Aide sur l'interface Web PAN-OS

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

June 29, 2020

Table of Contents

Bases d'interface Web....13
Vue d'ensemble du pare-feu....15
Fonctionnalités et avantages....16
Heure de la dernière connexion et tentatives de connexion échouées....17
Message du jour....18
Gestionnaire de tâches....19
Langue....21
Alarmes....22
Validation des modifications....23
Enregistrement des configurations candidates....28
Annuler les modifications....32
Configurations du verrouillage....36
Recherche globale....38
Détails de la menace....39
Récapitulatif d'AutoFocus Intelligence....41
Exportation du tableau de configuration....44

Tableau de bord....45
Widgets du tableau de bord....47

ACC....49
Aperçu de l'ACC....51
Onglets de l'ACC....53
Widgets de l'ACC....54
Actions de l'ACC....56
Utilisation des onglets et des widgets....56
Utilisation des filtres – Filtres locaux et filtres généraux....57

surveiller....61
Surveillance > Journaux....63
Types de journaux....63
Actions des journaux....68
Surveillance > External Logs....71
Surveillance > Moteur de corrélation automatique....73
Surveillance > Moteur de corrélation automatique > Objets de corrélation....73
Surveillance > Moteur de corrélation automatique > Événements corrélés....74
Surveillance > Capture de paquets....76
Aperçu de la capture de paquets....76
Blocs de construction d'une capture de paquets personnalisée....77
Activation de la capture de paquets de menaces....80
Surveillance > App-Scope....82
Aperçu de l'App-Scope....82
Rapport récapitulatif App-Scope....83
Rapport de surveillance des modifications App-Scope....83
Rapport de surveillance des menaces App-Scope....84
Rapport de la carte des menaces App-Scope....86
Rapport de surveillance du réseau App-Scope....87

Rapport de la carte du trafic App-Scope....88
Surveillance > Navigateur de session....90
Surveillance > Liste d'interdiction d'adresses IP....91
Entrées de la liste d'interdiction d'adresses IP....91
Afficher ou supprimer les entrées de la liste d'interdiction d'adresses IP....92
Surveillance > Botnet....94
Paramètres d'un rapport du Botnet....94
Paramètres de configuration d'un Botnet....95
Surveillance > Rapports au format PDF....97
Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF....97
Surveillance > Rapports au format'A0;PDF > Rapport d'activité des utilisateurs....98
Surveillance > Rapports PDF > Utilisation de l'application SaaS....100
Surveillance > Rapports au format'A0;PDF > Groupes de rapports....102
Surveillance > Rapports au format PDF > Planificateur de courrier électronique....103
Surveillance > Gérer des rapports personnalisés....105
Surveillance > Rapports....107

Politiques....109
Types de politique....111
Déplacement ou clonage d'une règle de politique....112
Archive des commentaires d'audit....113
Commentaires d'audit....113
Journaux de configuration (entre les validations)....113
Changements des règles....114
Requête sur le nombre d'utilisations de la règle....115
Requête sur le nombre d'utilisations de la règle du périphérique....115
Politiques > Sécurité....117
Présentation de la politique de sécurité....117
Blocs de construction dans une règle de politique de sécurité....118
Création et gestion des politiques....128
Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité....131
Applications et utilisation....134
Optimiseur de la politique de sécurité....137
Politiques > NAT....139
Onglet Général des politiques NAT....139
Onglet Paquet d'origine NAT....140
Onglet Paquet translaté NAT....141
Onglet Liaison HA Active / Active....144
Politiques > QoS....146
Politiques > Transfert basé sur une politique....150
Onglet Général du transfert basé sur une politique....150
Onglet Source du transfert basé sur une politique....151
Onglet Destination / Application / Service du transfert basé sur une politique....152
Onglet Transfert du transfert basé sur une politique....153
Politiques > Déchiffrement....155
Onglet Général du déchiffrement....155
Onglet déchiffrement de la source....156
Onglet Déchiffrement de la destination....157
Onglet Service de déchiffrement / catégorie d'URL....158
Onglet Options de Déchiffrement....158
Politiques > Inspection des tunnels....160
Blocs de construction dans une politique d'inspection des tunnels....160

Politiques > Contrôle prioritaire sur l'application 166
Onglet Général de contrôle prioritaire sur l'application 167
Onglet Source de contrôle prioritaire sur l'application 167
Onglet Destination de contrôle prioritaire sur l'application 168
Onglet Protocole / Application de contrôle prioritaire sur l'application 169
Politiques > Authentification 170
Blocs de construction d'une règle de politique d'authentification 170
Créer et gérer la politique d'authentification 175
Politiques > Protection'A0;DoS 178
Onglet Général de protection DoS ; 178
Onglet Source de protection DoS ; 179
Onglet Destination de protection DoS ; 180
Onglet Option / Protection de protection DoS 180
Politiques > SD-WAN 184
Onglet Général SD-WAN 184
Onglet Source SD-WAN 185
Onglet Destination SD-WAN 186
Onglet Application/Service SD-WAN 186
Onglet Sélection du chemin d'accès SD-WAN 188
Onglet Cible SD-WAN 188

Objets 191
Déplacement, clonage ou rétablissement des objets ou application d'un contrôle prioritaire sur ceux-ci 193
Déplacement ou clonage d'un objet 193
Contrôle prioritaire et rétablissement d'un objet 193
Objets > Adresses 195
Objets > Groupes d'adresses 197
Objets > Régions 200
Objets > Groupes d'utilisateurs dynamiques 201
Objets > Applications 203
Présentation des applications 203
Actions prises en charge sur les applications 207
Définition des applications 211
Objets > Groupes d'applications 215
Objets > Filtres d'applications 216
Objets > Services 217
Objets > Groupes de services 219
Objets > Étiquettes 220
Création d'étiquettes 220
Afficher la base de règles en tant que groupes 222
Gestion des étiquettes 225
Objets > Listes dynamiques externes 228
Objets > Objets personnalisés 233
Objets > Objets personnalisés > Modèles de données 233
Objets > Objets personnalisés > Logiciels espions / vulnérabilité 237
Objets > Objets personnalisés > Catégories d'URL 241
Objets > Profils de sécurité 243
Actions dans des profils de sécurité 243
Objets > Profils de sécurité > Antivirus 247
Objets > Profils de sécurité > Profil antispyware 249
Objets > Profils de sécurité > Protection contre les vulnérabilités 254
Objets > Profils de sécurité > Filtrage des URL 259
Paramètres généraux du filtrage des URL 259

Catégories de filtrage des URL....260
Paramètres de filtrage des URL....263
Détection des informations d'identification de l'utilisateur....264
Insertion de l'en-tête HTTP....266
Objets > Profils de sécurité > Blocage des fichiers....269
Objets > Profils de sécurité > Analyse WildFire....271
Objets > Profils de sécurité > Filtrage des données....273
Objets > Profils de sécurité > Protection DoS....275
Objets > Profils de sécurité > Protection GTP....279
Objets > Profils de sécurité > Protection SCTP....285
Objets > Groupes de profils de sécurité....291
Objets > Transfert des journaux....292
Objets > Authentification....296
Objets > Profils de déchiffrement....298
Paramètres généraux des profils de déchiffrement....298
Paramètres de contrôle du trafic SSL décrypté....299
Paramètres de contrôle du trafic non déchiffré....305
Paramètres de contrôle du trafic SSH déchiffré....306
Objets > Déchiffrement > Profil de transfert....308
Objets > Gestion des liens SD-WAN....311
Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès....311
Objets > Gestion des liens SD-WAN > Distribution du trafic....312
Objets > Calendriers....314

Réseau....315
Réseau > Interfaces....317
Présentation des interfaces de pare-feu....318
Composants communs des interfaces de pare-feu....318
Composants communs des interfaces de pare-feu PA-7000 Series....320
Interface Tap....320
Interface HD....321
Interface du câble virtuel....322
Sous-interface de câble virtuel....324
Interface de niveau 2 de la série PA-7000....324
Sous-interface de niveau 2 de la série PA-7000....326
Interface de niveau 3 de la série PA-7000....327
Interface de niveau 3....339
Sous-interface de couche 3....350
Interface de la carte de journal....360
Sous-interface de la carte de journal....361
Interface miroir de décryptage....362
Groupe d'interfaces Ethernet agrégées (AE)....363
Interfaces Ethernet agrégées (AE)....366
Réseau > Interfaces > VLAN....373
Réseau > Interfaces > En boucle....383
Réseau > Interfaces > De tunnel....386
Réseau > Interfaces > SD-WAN....388
Réseau > Zones....389
Présentation des zones de sécurité....389
Étapes de configuration des zones de sécurité....389
Réseau > VLAN....393
Réseau > Câbles virtuels....394
Réseau > Routeurs virtuels....395
Paramètres généraux d'un routeur virtuel....395

Itinéraires statiques ... 396
Redistribution d'itinéraire ... 399
RIP ... 401
OSPF ... 403
OSPFv3 ... 409
BGP ... 416
Multidiffusion IP ... 431
ECMP ... 435
Statistiques d'exécution supplémentaires d'un routeur virtuel ... 437
Réseau > Tunnels'A0;IPSec ... 449
Gestion d'un tunnel VPN IPSec ... 449
Onglet Général Tunnel IPSec ... 450
Onglet ID de proxy Tunnel IPSec ... 452
Statut du tunnel IPSec sur le pare-feu ... 453
Redémarrage ou actualisation d'un tunnel IPSec ... 453
Réseau > Tunnels GRE ... 454
Tunnels GRE ... 454
Réseau > DHCP ... 456
Présentation de DHCP ... 456
Adressage DHCP ... 456
Serveur DHCP ... 457
Relais DHCP ... 460
Client DHCP ... 461
Réseau > Proxy'A0;DNS ... 462
Présentation du proxy DNS ... 462
Paramètres du proxy DNS ... 463
Actions de proxy DNS supplémentaires ... 466
Réseau > QoS ... 467
Paramètres d'une interface de QoS ... 467
Statistique de l'interface QoS ... 469
Réseau > LLDP ... 471
Présentation de LLDP ... 471
Étapes de configuration de LLDP ... 471
Réseau > Profils réseau ... 474
Réseau > Profils réseau > Crypto IPSec GlobalProtect ... 474
Réseau > Profils réseau > Passerelles'A0;IKE ... 474
Réseau > Profils réseau > Crypto'A0;IPSec ... 482
Réseau > Profils réseau > Crypto IKE ... 483
Réseau > Profils réseau > Surveillance ... 484
Réseau > Profils réseau > Gestion de l'interface ... 485
Réseau > Profils réseau > Protection de zone ... 486
Réseau > Profils réseau > QoS ... 507
Réseau > Profils réseau > Profil LLDP ... 508
Réseau > Profils réseau > Profil BFD ... 509
Réseau > Profils réseau > Profil d'interface SD-WAN ... 512

Périphérique ... 515
Périphérique > Configuration ... 517
Périphérique > Configuration > Gestion ... 518
Périphérique > Configuration > Opérations ... 546
Activation de la surveillance SNMP ... 553
Périphérique > Configuration > Module de sécurité matériel ... 556
Paramètres du fournisseur du module matériel de sécurité ... 556
Authentication HSM ... 557

Opérations matérielles de sécurité....557
Configuration et état du fournisseur du module matériel de sécurité matériel....558
Statut du module matériel de sécurité....559
Périphérique > Configuration > Services....560
configuration des services pour les systèmes globaux et virtuels ;....560
Paramètres des services globaux....561
Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l'itinéraire de service....563
Route pour le service de destination....567
Périphérique > Configuration > Interfaces....568
Périphérique > Configuration > Télémesure....572
Périphérique > Configuration > Content-ID....575
Périphérique > Configuration > WildFire....581
Périphérique > Configuration > Session....585
Paramètres de session....585
Délais d'expiration de session....589
Paramètres TCP....591
Paramètres de décryptage : Vérification de la révocation du certificat....593
Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert....594
Paramètres de session VPN....595
Périphérique > Haute disponibilité....597
Considérations importantes pour la configuration HD....597
Configuration des paramètres HD....598
Périphérique > Carte de transfert des journaux....609
Périphérique > Audit de configuration....611
Périphérique > Profils de mot de passe....612
Exigences relatives au nom d'utilisateur et au mot de passe....613
Périphérique > Administrateurs....614
Périphérique > Rôles admin....617
Périphérique > Domaine d'accès....620
Périphérique > Profil d'authentification....621
Profil d'authentification....621
Exportation des métadonnées SAML à partir d'un Profil d'authentification....629
Périphérique > Séquence d'authentification....631
Périphérique > Sources d'informations de machine virtuelle....633
Paramètres pour activer les sources d'informations de machine virtuelle pour les Serveurs VMware ESXi et vCenter....635
Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC....636
Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine....637
Périphérique > Résolution des problèmes....640
Correspondance de la politique de sécurité....640
Correspondance de la politique QoS....642
Correspondance de la politique d'authentification....643
Correspondance politique SSL/déchiffrement....644
Correspondance de la politique NAT....645
Correspondance à la politique PBF (transfert basé sur une politique)....646
Correspondance de la politique DoS....647
Routage....649
Test WildFire....650
Archivage sécurisé des menaces....650
Ping....651
Trace Route....653

Connectivité du collecteur de journaux....654
Liste dynamique externe....655
Serveur de mises à jour....656
État du service de journalisation du cloud de test GP....656
État du service du cloud de test GP....656
Périphérique > Systèmes virtuels....658
Périphérique > Passerelles partagées....661
Périphérique > Gestion des certificats....662
Périphérique > Gestion des certificats > Certificats....663
Gestion des certificats du pare-feu et de Panorama....663
Gestion des autorités de certification de confiance par défaut....668
Périphérique > Gestion des certificats > Profil de certificat....670
Périphérique > Gestion des certificats > Répondeur'A0;OCSP....673
Périphérique > Gestion des certificats > Profil de service SSL/TLS....674
Périphérique > Gestion des certificats > SCEP....676
Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL....680
Périphérique > Pages de réponse....683
Périphérique > Paramètres des journaux....686
Sélection des destinations du transfert des journaux....686
Définition des paramètres d'alarme....689
Effacer les journaux....691
Périphérique > Profils de serveur....692
Périphérique > Profils de serveur > Piège'A0;SNMP....693
Périphérique > Profils de serveur > Syslog....696
Périphérique > Profils de serveur > Messagerie....698
Périphérique > Profils de serveur > HTTP....700
Périphérique > Profils de serveur > NetFlow....703
Périphérique > Profils de serveur > RADIUS....705
Périphérique > Profils de serveur > TACACS+....707
Périphérique > Profils de serveur > LDAP....709
Périphérique > Profils de serveur > Kerberos....712
Périphérique > Profils de serveur > Fournisseur d'identité SAML....713
Périphérique > Profils de serveur > DNS....717
Périphérique > Profils de serveur > Authentification multifacteur....718
Périphérique > Base de données d'utilisateurs locale > Utilisateurs....721
Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs....723
Périphérique > Exportation programmée des journaux....724
Périphérique > Logiciel....726
Périphérique > Mises à jour dynamiques....728
Périphérique > Licences....732
Périphérique > Support....734
Périphérique > Clé principale et diagnostics....735
Déployer la clé principale....736

Identification utilisateur....739
Périphérique > Identification utilisateur > Mappage d'utilisateur....741
Configuration de l'agent User-ID Palo Alto Networks....741
Surveillance des serveurs....751
Inclure ou exclure des sous-réseaux pour l'association d'utilisateur....754
Périphérique > Identification utilisateur > Sécurité de la connexion....756
Périphérique > Identification utilisateur > Agents User-ID....757
Configuration de l'accès aux agents User-ID....757
Gestion de l'accès aux agents User-ID....759
Périphérique > Identification utilisateur > Agents de Terminal Server....761

Périphérique > Identification utilisateur > Onglet Paramètres de mappage de groupe.....763
Périphérique > Identification utilisateur > Paramètres du portail captif.....768

GlobalProtect.....773
Réseau > GlobalProtect > Portails.....775
Onglet Général Portails GlobalProtect.....776
Onglet d'Authentification des portails GlobalProtect.....778
Onglet Collecte de données du portail GlobalProtect.....780
Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect).....781
Onglet des VPN sans client des portails GlobalProtect.....807
Onglet du satellite du portail GlobalProtect.....810
Réseau > GlobalProtect > Passerelles.....814
Onglet Général des passerelles GlobalProtect.....814
Onglet d'authentification de la passerelle GlobalProtect.....815
Onglet Agent de passerelles GlobalProtect.....817
Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect).....830
Réseau > GlobalProtect > Gestionnaire de périphériques mobiles.....833
Réseau > GlobalProtect > Liste de blocage de périphériques.....835
Réseau > GlobalProtect > Applications sans client.....836
Réseau > GlobalProtect > Groupes d'applications sans client.....837
Objets > GlobalProtect > Objets HIP.....838
Onglet Général des objets HIP.....838
Onglet Périphérique mobile des objets HIP.....840
Onglet Gestion des correctifs des objets HIP.....842
Onglet Pare-feu des objets HIP.....843
Onglet Anti-logiciels malveillants des objets HIP.....843
Onglet Sauvegarde du disque des objets HIP.....844
Onglet Cryptage du disque des objets HIP.....845
Onglet Prévention des pertes de données des objets HIP.....845
Onglet HIP Objects Certificate (Certificat d'objets HIP).....846
Onglet Vérifications personnalisées des objets HIP.....846
Objets > GlobalProtect > Profils HIP.....848
Périphérique > Client GlobalProtect.....850
Gestion du logiciel de l'application GlobalProtect.....850
Paramétrage de l'application GlobalProtect.....851
Utilisation de l'application GlobalProtect.....852

Interface Web de Panorama.....853
Utilisation de l'interface Web de Panorama.....855
Commutateur de contexte.....860
Opérations de validation de Panorama.....861
Définition des politiques sur Panorama.....871
Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité.....873
Panorama > Configuration > Interfaces.....875
Panorama > Haute disponibilité.....879
Panorama > Clusters WildFire gérés.....882
Tâches des clusters WildFire gérés.....882
Tâches de l'appareil WildFire géré.....883
Informations WildFire gérées.....884
Cluster WildFire géré et administration de l'appareil.....888
Panorama > Administrateurs.....900
Panorama > Rôles admin.....903
Panorama > Domaines d'accès.....905

Panorama > Périphériques gérés > Récapitulatif....907
Administration du pare-feu géré....907
Informations sur les pare-feu gérés....908
Mises à jour logicielles et de contenu du pare-feu....912
Sauvegardes du pare-feu....913
Panorama > Périphériques gérés > État....914
État détaillé des périphériques dans Panorama....916
Panorama > Modèles....920
Modèles....920
Piles de Modèles....921
Panorama > Modèles > Variables des modèles....922
Panorama > Groupes de périphériques....925
Panorama > Collecteurs gérés....927
Informations sur les collecteurs de journaux....927
Configuration du Collecteur de journaux....928
Mises à jour logicielles pour les collecteurs de journaux dédiés....937
Panorama > Groupes de collecteurs....939
Configuration du groupe de collecteurs....939
Information sur les groupes de collecteurs....946
Panorama > Plug-ins....947
Panorama > VMware NSX....948
Configuration d'un groupe de notification....948
Création de définitions de services....949
Configuration de l'accès à NSX Manager....950
Création de règles de redirection....952
Panorama > Profil d'ingestion des journaux....954
Panorama > Paramètres des journaux....955
Panorama > Exportation programmée des configurations....957
Panorama > Logiciel....959
Gestion des mises à jour logicielles Panorama....959
Affichage des informations sur les mises à jour logicielles Panorama....960
Panorama > Déploiement du périphérique....961
Gestion des mises à jour logicielles et de contenu....961
Affichage des informations sur les mises à jour logicielles et de contenu....964
Planification des mises à jour de contenu dynamiques....965
Rétablissement des versions de contenu précédentes de Panorama....966
Gestion des licences du pare-feu....967

Bases d’interface Web

Les rubriques suivantes fournissent un aperçu du pare-feu et décrivent les tâches administratives de base.

- Vue d’ensemble du pare-feu
- Fonctionnalités et avantages
- Heure de la dernière connexion et tentatives de connexion échouées
- Message du jour
- Gestionnaire de tâches
- Langue
- Alarmes
- Validation des modifications
- Enregistrement des configurations candidates
- Annuler les modifications
- Configurations du verrouillage
- Recherche globale
- Détails de la menace
- Récapitulatif d'AutoFocus Intelligence

© 2020 Palo Alto Networks, Inc.

Vue d’ensemble du pare-feu

Les pare-feu Palo Alto Networks® de nouvelle génération inspectent l'ensemble du trafic (y compris les applications, les menaces et les contenus) et l'associent à l'utilisateur, où qu'il se trouve et quel que soit le type de périphérique. L’utilisateur, l’application et les contenus, c'est-à-dire tout ce qui fait fonctionner votre entreprise, deviennent parties intégrantes de votre politique de sécurité d'entreprise. Cela vous permet d’harmoniser votre sécurité à vos politiques d’entreprises et de rédiger des règles qui sont faciles à comprendre et à préserver.

Dans le cadre de notre plate-forme d'exploitation de la sécurité, nos pare-feu de nouvelle génération fournissent à votre organisation la possibilité de :

- Activer les applications (y compris les applications en tant que service), les utilisateurs et le contenu en toute sécurité en classant tout le trafic (peu importe le port).
- Réduire le risque d’attaque à l’aide d’un modèle d’application positif, en autorisant toutes les applications désirées et en bloquant tout le reste.
- Appliquer les politiques de sécurité afin de bloquer les exploitations de vulnérabilités connues, les virus, les rançongiciels, les spyware, les botnets et les autres logiciels malveillants inconnus, comme les menaces persistantes avancées.
- Protéger vos centres de données (y compris les centres de données virtuels) en segmentant les données et les applications, ainsi qu’en appliquant le principe de confiance zéro.
- Appliquer une sécurité cohérente dans l'ensemble de vos établissements et de vos environnements infonuagiques.
- Adopter l'informatique mobile sécurisée en étendant la plateforme d’exploitation de sécurité aux utilisateurs et aux périphériques où qu'ils se trouvent.
- Obtenir un aperçu centralisé et simplifier la sécurité du réseau, ce qui rend vos données exploitables afin de pouvoir prévenir des cyberattaques réussies.
- Identifier et empêcher les tentatives de vol d'identifiants en arrêtant l’envoi d’identifiants d’entreprise valides à des sites Web illégitimes. Elle neutralise également la capacité d'un pirate informatique à utiliser des identifiants volés pour un mouvement latéral ou une compromission du réseau en appliquant des politiques d'authentification au niveau de la couche réseau.

© 2020 Palo Alto Networks, Inc.

Fonctionnalités et avantages

Les pare-feu Palo Alto Networks de dernière génération assurent un contrôle granulaire du trafic autorisé à accéder à votre réseau. Les fonctionnalités et avantages principaux incluent'A0;:

- **Mise en œuvre d'une politique basée sur une application (App-ID™)** – Le contrôle des accès selon le type d'application est beaucoup plus efficace lorsque l'identification d'une application ne se base pas uniquement sur le protocole et le numéro de port. Le service App-ID peut bloquer des applications à haut risque, ainsi que des comportements à haut risque, tels que le partage de fichiers, et le trafic crypté avec le protocole SSL (Secure Sockets Layer) peut être décrypté et inspecté.
- **Identification de l'utilisateur (User-ID™)** - La fonction User-ID permet aux administrateurs de configurer et d'appliquer des politiques de pare-feu basées sur des utilisateurs et des groupes d'utilisateurs, à la place de ou en plus des zones et adresses réseaux. Le pare-feu peut communiquer avec de nombreux serveurs d'annuaire, comme Microsoft Active Directory, eDirectory, SunOne, OpenLDAP et la plupart des autres serveurs d'annuaire basés sur le protocole LDAP afin de fournir au pare-feu des informations concernant un utilisateur et un groupe. Vous pouvez utiliser ces informations pour la mise en œuvre sécurisée d'applications qui peut être définie par utilisateur ou par groupe. Par exemple, l'administrateur peut autoriser une seule organisation de l'entreprise à utiliser une application Web. Vous pouvez également configurer le contrôle granulaire de certains composants d'une application en fonction des utilisateurs et des groupes (voir Identification utilisateur).
- **Prévention des menaces** – Les services de prévention des menaces qui protègent le réseau des virus, des vers, des logiciels espions et d'autres trafics malveillants peuvent varier selon la source de l'application et du trafic (voir Objets > Profils de sécurité).
- **Filtrage des URL** – Les connexions sortantes peuvent être filtrées pour empêcher l'accès à des sites Web inappropriés (voir Objets > Profils de sécurité > Filtrage des URL).
- **Visibilité du trafic** - Les rapports, journaux et mécanismes de notification étendus fournissent une visibilité détaillée dans le trafic des applications réseaux et des événements de sécurité. Le Centre de commande de l'application (ACC) de l'interface Web identifie les applications dont le trafic est le plus dense et les risques de sécurité les plus élevés (voir Surveillance).
- **Adaptabilité et vitesse du réseau** - Le pare-feu Palo Alto Networks peut développer ou remplacer votre pare-feu existant et peut être installé de façon transparente dans n'importe quel réseau ou configuré de sorte à prendre en charge un environnement ayant fait l'objet d'un basculement ou d'un routage. Des vitesses pouvant atteindre plusieurs gigaoctets et une architecture à accès unique permettent de vous fournir ces services avec peu, voire aucun impact sur les délais d'attente du réseau.
- **GlobalProtect** - Le logiciel GlobalProtect™ sécurise les systèmes clients, tels que les ordinateurs portables qui sont utilisés sur le terrain, grâce à une connexion simple et sécurisée où que vous soyez.
- **Fonctionnement à sécurité intégrée** – Un support haute disponibilité (HA) assure un basculement automatique en cas de défaillance matérielle ou logicielle (voir Périphérique > Systèmes virtuels).
- **Analyse de logiciels malveillants et création de rapports** – Le service d'analyse basé sur le cloud WildFire™ fournit une analyse détaillée et crée un rapport concernant les logiciels malveillants qui traversent le pare-feu. L'intégration avec le service de renseignement sur les menaces AutoFocus™ vous permet d'évaluer le risque associé au trafic de votre réseau à l'échelle organisationnelle, industrielle et mondiale.
- **Pare-feu série VM** – Un pare-feu série VM fournit une instance virtuelle de PAN-OS® pouvant être utilisée dans un environnement de centre de données virtualisé. Il est idéal pour les environnements publics, privés et hybrides du cloud.
- **Gestion et Panorama** – Vous pouvez gérer chaque pare-feu par l'intermédiaire d'une interface Web intuitive ou une interface de ligne de commande (CLI) ou tous les pare-feu peuvent être gérés de façon centralisée via le système de gestion centralisée de Panorama™ qui dispose d'une interface Web très similaire à celle des pare-feu Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Heure de la dernière connexion et tentatives de connexion échouées

Pour détecter l'utilisation malveillante et empêcher l'exploitation d'un compte privilégié, comme un compte administratif sur un pare-feu Palo Alto Networks ou sur Panorama, l'interface Web et l'interface de ligne de commande (CLI) affichent l'heure de la dernière connexion au compte et toute tentative de connexion échouée liée à votre nom d'utilisateur lorsque vous vous connectez. Cette information vous permet d'identifier facilement si quelqu'un utilise vos informations d'identification administratives pour lancer une attaque.

Une fois que vous êtes connecté à l'interface Web, l'heure de la dernière connexion au compte apparaît dans la portion inférieure gauche de la fenêtre. Si une ou plusieurs tentatives de connexion échouées se sont produites depuis la dernière connexion réussie, une icône de mise en garde apparaît à droite de l'information concernant la dernière connexion. Placez le curseur sur le symbole de mise en garde pour afficher le nombre de tentatives de connexion ayant échoué ou cliquez pour consulter la fenêtre **Récapitulatif des échecs de tentatives de connexion**, qui liste le nom du compte administrateur, l'adresse IP source et la raison de l'échec de connexion.

Si vous voyez plusieurs tentatives de connexion échouées dont vous n'êtes pas l'auteur, vous devez communiquer avec votre administrateur réseau pour localiser le système qui exécute l'attaque exhaustive, puis enquêtez sur l'utilisateur et l'ordinateur de l'hôte pour identifier et éradiquer toute activité malveillante. Si vous voyez que la date et l'heure de la dernière connexion au compte indiquent un compte compromis, vous devez immédiatement changer votre mot de passe, puis effectuer une vérification de la configuration pour déterminer si l'on a effectué des modifications de configuration suspectes. Si vous constatez que les journaux ont été effacés ou si vous avez des difficultés à déterminer si des modifications inappropriées ont été effectuées à l'aide de votre compte, rétablissez la configuration afin d'obtenir une bonne configuration.

© 2020 Palo Alto Networks, Inc.

Message du jour

Si un autre administrateur ou vous avez configuré un message du jour ou si Palo Alto Networks en a intégré un dans le cadre d'une nouvelle version du logiciel ou du contenu, une boîte de dialogue Message du jour s'affiche lorsque les utilisateurs se connectent à l'interface Web. Cela garantit que les utilisateurs voient l'information importante, comme un redémarrage imminent du système, qui affecte les tâches qu'ils souhaitent effectuer.

La boîte de dialogue affiche un message par page. Si la boîte de dialogue comprend l'option **Do not show again (Ne plus afficher)**, vous pouvez la sélectionner pour chaque message dont vous ne souhaitez pas que la boîte de dialogue s'affiche lors des prochaines connexions.

Chaque fois qu'une modification est apportée au Message of the Day (Message du jour), le nouveau message apparaît lors de votre prochaine connexion au compte, même si vous avez sélectionné l'option Do not show again (Ne plus afficher) lors d'une connexion précédente. Vous devez ensuite resélectionner cette option pour éviter de voir le message modifié lors de vos prochaines connexions.

Pour naviguer parmi les différentes boîtes de dialogue, cliquez sur les flèches droite ( ) et gauche ( ) situées sur les côtés de la boîte de dialogue ou cliquez sur un sélecteur de page ( ) le long de la portion inférieure de la boîte de dialogue. Après avoir cliqué sur **Close (Fermer)** dans la boîte de dialogue, vous pouvez l'ouvrir à nouveau manuellement en cliquant sur les messages ( ) au bas de l'interface Web.

Pour configurer un message du jour, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres des bannières et des messages.

© 2020 Palo Alto Networks, Inc.

Gestionnaire de tâches

Cliquez sur **Tâches** en bas de l'interface Web, pour afficher les opérations que d'autres administrateurs, PAN-OS ou vous avez lancées depuis le dernier redémarrage du pare-feu (par exemple, des validations manuelles ou des rafraîchissements automatiques du nom de domaine complet [FQDN]). Pour chaque tâche, le Gestionnaire des tâches fournit les informations et les actions décrites dans le tableau ci-dessous.

Par défaut, certaines colonnes sont masquées. Pour afficher ou masquer des colonnes spécifiques, ouvrez le menu déroulant dans n'importe quel en-tête de colonne, sélectionnez Colonnes, puis sélectionnez (afficher) ou effacer (masquer) les noms des colonnes.

Champ/Bouton	Description
	Pour filtrer les tâches, vous devez saisir une chaîne de texte basée sur une valeur dans l'une des colonnes et Appliquer le filtre ( ). Par exemple, saisir **`edl`** filtrera la liste pour afficher uniquement les tâches EDLFetch (récupérer les listes dynamiques externes). Pour supprimer le filtrage, cliquez sur Supprimer le filtre ( ).
Type	Le type de tâche, comme une demande de journaux, un rafraîchissement de la licence ou une validation. Si les informations relatives à la tâche (les avertissements par exemple) sont trop longues pour rentrer dans la colonne Messages, vous pouvez cliquer sur la valeur Type pour afficher tous les détails.
Status (État)	Indique si la tâche est en attente (comme les validations dont l'état est « File d'attente »), en cours (telles que les demandes de journaux dont l'état est « Actif »), terminée ou échouée. Pour les validations en cours, l'État indique le pourcentage d'achèvement.
ID de tâche	Un numéro qui identifie la tâche. À partir de la CLI, vous pouvez utiliser l'ID de tâche pour afficher les détails supplémentaires d'une tâche. Par exemple, vous pouvez consulter la position d'une tâche de validation dans la file d'attente de validation en saisissant : `> show jobs id <job-id>` Cette colonne est masquée par défaut.
Heure de fin	La date et l'heure de fin de la tâche. Cette colonne est masquée par défaut.
Heure de début	La date et l'heure de début de la tâche. Pour les tâches de validation, l'Heure de début indique le moment où une validation a été ajoutée à la file d'attente de validation.
Messages	Affichent des détails sur la tâche. Si l'entrée indique qu'il y a trop de messages, vous pouvez cliquer sur le Type de tâche pour voir les messages.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	En ce qui concerne les tâches de validation, les Messages comprennent le délai avant le retrait de la file d'attente pour indiquer quand PAN-OS a commencé à procéder à la validation. Pour voir la description qu'a saisie un administrateur relativement à une validation, cliquez sur **Commit Description (Description de validation)**. Pour plus d'informations, reportez-vous à la section Validation des modifications.
Action (Action)	Cliquez sur **x** pour annuler une validation en attente initiée par un administrateur ou par PAN-OS. Ce bouton est disponible uniquement pour les administrateurs qui ont l'un des rôles prédéfinis suivants : super utilisateur, administrateur du périphérique, administrateur du système virtuel ou administrateur de Panorama.
Montrer	Sélectionnez les tâches que vous souhaitez afficher : • **Toutes les tâches** (par défaut). • **Toutes** les tâches d'un certain type (**Tâches**, **Rapports** ou **Requêtes du journal**). • Toutes les tâches **En cours d'exécution** (en cours). • Toutes les tâches **En cours d'exécution** d'un certain type (**Tâches**, **Rapports** ou **Requêtes du journal**). • (Panorama uniquement) Utilisez la deuxième liste déroulante pour afficher les tâches de **Panorama** (par défaut) ou un pare-feu géré spécifique.
Effacer la file d'attente de validation	Annule toutes les validations en attente initiées par les administrateurs ou par PAN-OS. Ce bouton est disponible uniquement pour les administrateurs qui ont l'un des rôles prédéfinis suivants : super utilisateur, administrateur du périphérique, administrateur du système virtuel ou administrateur de Panorama.

© 2020 Palo Alto Networks, Inc.

Langue

Par défaut, la langue qui est définie sur l'ordinateur à partir duquel vous vous connectez au pare-feu détermine la langue qui s’affiche sur l'interface de gestion Web. Pour changer manuellement la langue, cliquez sur **Language (Langue)** (dans le coin inférieur droit de l'interface Web), sélectionnez la langue souhaitée dans le menu déroulant, puis cliquez sur **OK**. L’interface Web s’actualise et s’affiche dans la langue souhaitée.



Voici certaines langues prises en charge : français, japonais, espagnole, chinois simplifié et chinois traditionnel

© 2020 Palo Alto Networks, Inc.

Alarmes

Une alarme est un message généré par le pare-feu indiquant que le nombre d'événements d'un certain type (par exemple, les erreurs de cryptage et de décryptage) a dépassé le seuil configuré pour ce type d'événement (reportez-vous à la section Définitions des paramètres d'alarme). Lorsqu'il génère une alarme, le pare-feu crée un Journal des alarmes et ouvre la boîte de dialogue Alarmes du système pour afficher l'alarme en question. Après avoir fermé la boîte de dialogue, vous pouvez à tout moment la rouvrir en cliquant sur **Alarmes** () au bas de l'interface Web. Pour éviter que le pare-feu ouvre automatiquement la boîte de dialogue pour une alarme en particulier, sélectionnez Alarmes non acquittées, puis cliquez sur **Acknowledge (Acquitter)** pour ajouter les alarmes à la liste des Alarmes acquittées.

© 2020 Palo Alto Networks, Inc.

Validation des modifications

Cliquez sur **Commit (Valider)** dans le coin supérieur droit de l'interface Web et indiquez une opération à appliquer pour les modifications en attente relatives à la configuration du pare-feu : commit (activate) (activer), validate (valider) ou preview (prévisualiser). Vous pouvez filtrer les modifications en attente par l'administrateur ou l'*emplacement* et ensuite prévisualiser, valider et confirmer uniquement ces modifications. L'emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Le pare-feu met en attente les demandes de validation afin que vous puissiez lancer une nouvelle validation lorsqu'une validation précédente est en cours. Le pare-feu exécute les validations dans l'ordre dans lequel elles sont initiées, mais donne la priorité aux validations que le pare-feu initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d'attente possède déjà le nombre maximum de validations lancées par l'administrateur, vous devez attendre que le pare-feu termine le traitement d'une validation en attente avant d'en lancer une nouvelle.

Utilisez le Gestionnaire de tâches pour annuler des validations ou pour voir les détails des validations dont l'état est en attente, en cours, terminé ou échoué.

La boîte de dialogue Validation affiche les options décrites dans le tableau suivant.

Champ/Bouton	Description
Valider toutes les modifications	Confirme toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement le périmètre des modifications de configuration que le pare-feu valide lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l'étendue de validation : • **Rôle du super-utilisateur** – Le pare-feu valide les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent l'étendue de validation (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège **Valider pour d'autres administrateurs**, le pare-feu valide les modifications configurées par tous les administrateurs. Si votre profil de Rôle administrateur n'inclut pas le privilège **Valider pour les autres administrateurs**, le pare-feu ne valide que vos modifications et non celles d'autres administrateurs. Si vous avez mis en œuvre des domaines d'accès, le pare-feu applique automatiquement ces domaines pour filtrer le périmètre de validation (voir Périphérique > Domaine d'accès). Quel que soit votre rôle administrateur, le pare-feu ne valide que les modifications de configuration dans les domaines d'accès affectés à votre compte.
Valider les modifications effectuées par	Filtre le périmètre des modifications de configuration que le pare-feu valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle du super-utilisateur** – Vous pouvez limiter l'étendue de validation aux modifications apportées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation aux modifications configurées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtre l'étendue de validation comme suit : • **Filtrer par administrateur** – Même si votre rôle vous permet de valider les modifications effectuées par les autres administrateurs, par défaut, l'étendue de validation inclut uniquement vos modifications. Pour ajouter d'autres administrateurs à la portée de la validation, cliquez sur le lien **<usernames> (<noms d'utilisateur>)**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les emplacements spécifiques pour les modifications à Inclure dans la validation. Si vous avez mis en œuvre des domaines d'accès, le pare-feu filtre automatiquement le périmètre de validation en fonction de ces domaines (voir Périphérique > Domaine d'accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l'étendue de validation inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte. *Après avoir chargé une configuration (Périphérique > Configuration > Opérations), vous devez Valider toutes les modifications.* Lorsque vous validez des modifications apportées à un système virtuel, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce système virtuel.
Étendue de la validation	Répertorie les emplacements contenant des modifications à valider. Différents facteurs déterminent si la liste inclut toutes les modifications ou un sous-ensemble de modifications, comme il est décrit dans Valider toutes les modifications et Valider les modifications effectuées par. Les emplacements peuvent être l'un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l'emplacement Partagé. • **Politique et objets** – Règles de politique ou objets qui sont définis sur un pare-feu qui ne dispose pas de plusieurs systèmes virtuels. • **Périphérique et réseau** – Paramètres réseau et de périphériques globaux (tels que les profils de Gestion de l'interface) et non spécifiques à un système virtuel. Cela s'applique également aux

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	paramètres réseau et de périphériques sur un pare-feu qui ne dispose pas de plusieurs systèmes virtuels. • **<Virtual-system> (<système-virtuel>)** – Le nom du système virtuel dans lequel les règles de politique ou les objets sont définis sur un pare-feu comportant plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones).
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Systèmes virtuels** – Les paramètres qui sont définis dans un système virtuel spécifique. • **Autres modifications** – Les paramètres qui ne sont pas spécifiques à un système virtuel (comme les objets partagés).
Inclure dans la validation (Validation partielle uniquement)	Vous permet de sélectionner les modifications que vous souhaitez valider. Par défaut, toutes les modifications de l'**Étendue de validation** sont sélectionnées. Cette colonne s'affiche uniquement après que vous avez choisi de **Valider les modifications effectuées par** des administrateurs spécifiques. *Il peut y avoir des dépendances affectant les modifications que vous incluez dans une validation. Par exemple, si vous ajoutez un objet et qu'un autre administrateur modifie cet objet, vous ne pouvez pas valider la modification pour l'autre administrateur sans valider votre propre modification.*
Regrouper par type d'emplacement	Regroupe la liste des modifications de configuration de l'**Étendue de validation** par **Type d'emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans l'**Étendue de validation** de la configuration en cours d'exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l'interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d'exécution que vous comparez. *Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.*

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Modifier le récapitulatif	Répertorie les paramètres individuels pour lesquels vous effectuez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l'objet** – Le nom qui identifie la politique, l'objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d'emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L'administrateur qui a effectué la dernière modification du paramètre. • **Sera validé** – Indique si la validation inclut le paramètre actuellement. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**). Sélectionnez un objet dans la liste des changements pour afficher la **Différence au niveau de l'objet**.
Confirmer la validation	Vérifie que la syntaxe de la configuration du pare-feu est correcte et est complète d'un point de vue sémantique. Le résultat inclut les mêmes erreurs et avertissements qu'une validation afficherait, y compris la règle l'occultation et l'application des avertissements de dépendance. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d'exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d'erreur.
Description	Vous permet de saisir une description (comportant jusqu'à 512 caractères) pour aider les autres administrateurs à comprendre les modifications que vous avez effectuées. *Le Journal système pour un événement de validation tronquera la description si elle dépasse 512 caractères.*
Valider	Démarre la validation ou, si d'autres validations sont en attente, l'ajoute à la file d'attente de validation.
État de la validation	Fournit la progression pendant la validation et fournit ensuite les résultats après la validation. Les résultats de la validation indiquent la

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	réussite ou l'échec, les détails sur la validation des modifications et les avertissements de la validation. Les avertissements sont les suivants : • **Validation** – Répertorie les avertissements généraux sur la validation. • **Dépendance d'application** – Répertorie toutes les dépendances d'application requises pour les règles existantes. • **Règle ombragée** – Répertorie toutes les règles ombragées.

© 2020 Palo Alto Networks, Inc.

Enregistrement des configurations candidates

Sélectionnez **Config (Configuration)** > **Save Changes (Enregistrer les modifications)** en haut à droite du pare-feu ou de l'interface Web Panorama pour enregistrer un nouveau fichier instantané de configuration candidate ou pour écraser un fichier de configuration existant. Si le pare-feu ou Panorama redémarre avant que vous validiez vos modifications, vous pouvez rétablir la configuration candidate à l'instantané sauvegardé pour restaurer les modifications apportées après la dernière validation. Pour revenir à l'instantané, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**et **Load named configuration snapshot (Charger l'instantané de la configuration)**. Si l'instantané n'est pas rétabli après avoir effectué un redémarrage, la configuration candidate sera la même que la dernière configuration validée (la configuration active).

Vous pouvez filtrer les modifications de la configuration à enregistrer en fonction de l'administrateur ou de l'*emplacement*. L'emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.



Vous devez régulièrement enregistrer vos modifications afin de ne pas les perdre si le pare-feu ou Panorama redémarre.



L'enregistrement de vos modifications dans la configuration candidate n'active pas ces modifications ; vous devez Valider les modifications *pour les activer.*

La boîte de dialogue Enregistrer les modifications affiche les options décrites dans le tableau suivant :

Champ/Bouton	Description
Enregistrer toutes les modifications	Enregistre toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement la portée des modifications de configuration que le pare-feu enregistre lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine la portée de l'enregistrement : • **Rôle de super-utilisateur** – Le pare-feu enregistre les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affectés à votre compte déterminent la portée de l'enregistrement (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège d'**Enregistrer pour les autres administrateurs**, le pare-feu enregistre les modifications configurées par tous les administrateurs. Si votre profil de rôle administrateur n'inclut pas le privilège d'**Enregistrer pour les autres administrateurs**, le pare-feu n'enregistre que vos modifications et non celles des autres administrateurs. Si vous avez implémenté des domaines d'accès, le pare-feu applique automatiquement ces domaines pour filtrer la portée de l'enregistrement (voir Périphérique > Domaine d'accès). Indépendamment de votre rôle administratif, le pare-feu n'enregistre que les modifications de configuration dans les domaines d'accès affectés à votre compte.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Enregistrer les modifications effectuées par	Permet de filtrer la portée des modifications de configuration que le pare-feu valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle de super-utilisateur** – Vous pouvez limiter la portée de l'enregistrement aux modifications apportées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège d'**Enregistrer pour les autres administrateurs**, vous pouvez limiter la portée de l'enregistrement aux modifications configurées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège d'**Enregistrer pour les autres administrateurs**, vous pouvez limiter la portée de l'enregistrement uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtrez la portée de l'enregistrement comme suit : • **Filtrer par administrateur** – Même si votre rôle permet d'enregistrer les modifications d'autres administrateurs, la portée de l'enregistrement inclut uniquement vos modifications par défaut. Pour ajouter d'autres administrateurs à la portée de l'enregistrement, cliquez sur le lien **<usernames> (<noms d'utilisateur>)**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les modifications dans des emplacements spécifiques pour les Inclure dans l'enregistrement. Si vous avez implémenté des domaines d'accès, le pare-feu filtre automatiquement la portée de l'enregistrement en fonction de ces domaines (voir Périphérique > Domaine d'accès). Quels que soient votre rôle administratif et vos choix de filtrage, la portée de l'enregistrement inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte.
Enregistrer la portée	Énumère les emplacements contenant des modifications à enregistrer. Le fait que la liste comprenne toutes les modifications ou un sous-ensemble de modifications dépend de plusieurs facteurs, comme décrit pour les options Enregistrer toutes les modifications et Enregistrer les modifications effectuées par. Les emplacements peuvent être l'un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l'emplacement Partagé. • **policy-and-objects (politique et objets)** – (Pare-feu uniquement) Règles de politique ou objets définis sur un pare-feu qui ne possède pas plusieurs systèmes virtuels. • **device-and-network (périphérique et réseau)** – (Pare-feu uniquement) Paramètres réseau et périphériques qui sont globaux (tels que les profils de gestion d'interface) et non spécifiques à un système virtuel.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **<virtual-system> (<système-virtuel>)** – (Pare-feu uniquement) Le nom du système virtuel dans lequel les règles ou objets de stratégie sont définis sur un pare-feu doté de plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones). • **<device-group> (<groupe de périphériques>)** – (Panorama uniquement) Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • **<template> (<modèle>)** – (Panorama uniquement) Le nom du modèle ou de la pile de modèles dans lequel les paramètres sont définis. • **<log-collector-group> (<groupe de collecteurs de journaux>)** – (Panorama uniquement) Le nom du Groupe de collecteurs dans lequel les paramètres sont définis. • **<log-collector> (<collecteur de journaux>)** – (Panorama uniquement) Le nom du Collecteur de journaux dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements où les modifications ont été apportées : • **Systèmes virtuels** – (Pare-feu uniquement) Les paramètres définis dans un système virtuel spécifique. • **Groupes de périphériques** – (Panorama uniquement) Paramètres définis dans un groupe de périphériques spécifique. • **Modèles** – (Panorama uniquement) Paramètres définis dans un modèle spécifique ou une pile de modèles spécifique. • **Groupes de collecteurs** – (Panorama uniquement) Paramètres spécifiques à une configuration de Groupe de collecteurs.
Inclure dans Enregistrer (Enregistrement partiel uniquement)	Vous permet de sélectionner les modifications que vous souhaitez enregistrer. Par défaut, toutes les modifications contenues dans **Enregistrer la portée** sont sélectionnées. Cette colonne s'affiche uniquement après que vous avez choisi d'**Enregistrer les modifications effectuées par** des administrateurs spécifiques. *Il peut y avoir des dépendances qui affectent les modifications que vous incluez dans un enregistrement. Par exemple, si vous ajoutez un objet et qu'un autre administrateur modifie cet objet, vous ne pouvez pas enregistrer la modification pour l'autre administrateur sans enregistrer votre propre modification.*
Regrouper par type d'emplacement	Regroupe la liste des modifications de configuration dans le champ **Enregistrer la portée** par **Type d'emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans le champ **Enregistrer la portée** à la configuration en cours d'exécution. La fenêtre de prévisualisation utilise un code

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l'interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d'exécution que vous comparez. *Etant donné que les résultats de la prévisualisation s'affichent dans une nouvelle fenêtre, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant de débloquer l'ouverture des fenêtres contextuelles.*
Modifier le récapitulatif	Énumère les paramètres individuels pour lesquels vous enregistrez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l'objet** – Le nom qui identifie la politique, l'objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d'emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L'administrateur qui a effectué la dernière modification du paramètre. • **Sera enregistré** – Indique si l'opération d'enregistrement inclura le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Save (Enregistrer)	Enregistre les modifications sélectionnées dans un fichier instantané de configuration : • Si vous avez sélectionné **Enregistrer toutes les modifications**, le pare-feu écrase le fichier instantané de configuration par défaut (.snapshot.xml). • Si vous avez sélectionné **Enregistrer les modifications effectuées par**, spécifiez le **Nom** d'un nouveau fichier de configuration ou d'un fichier de configuration existant et cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

Annuler les modifications

Sélectionnez **Config (Configuration)** > **Revert Changes (Annuler les modifications)** en haut à droite du pare-feu ou de l'interface Web Panorama pour annuler les modifications apportées à la configuration candidate depuis la dernière validation. L'annulation des modifications restaure les paramètres en fonction des valeurs de la configuration en cours d'exécution. Vous pouvez filtrer les modifications de la configuration à annuler en fonction de l'administrateur ou de l'*emplacement*. L'emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Vous ne pouvez pas annuler les modifications jusqu'à ce que le pare-feu ou Panorama finisse de traiter tous les engagements en attente ou en cours. Après avoir lancé le processus d'annulation, le pare-feu ou Panorama verrouille automatiquement le candidat et exécute les configurations afin que les autres administrateurs ne puissent pas modifier les paramètres ou effectuer de modifications. Après avoir terminé le processus d'annulation, le pare-feu ou Panorama supprime automatiquement le verrouillage.

La boîte de dialogue Annuler les modifications affiche les options décrites dans le tableau suivant :

Champ/Bouton	Description
Annuler toutes les modifications	Annule toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement la portée des modifications de configuration que le pare-feu annule lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine la portée de l'annulation : • **Rôle de super-utilisateur** – Le pare-feu annule les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affectés à votre compte déterminent la portée de l'annulation (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège de **Valider pour les autres administrateurs**, le pare-feu annule les modifications configurées par tous les administrateurs. Si votre profil de rôle administrateur n'inclut pas le privilège de **Valider pour les autres administrateurs**, le pare-feu n'annule que vos modifications et non celles des autres administrateurs. *Dans les profils de rôle d'administrateur, les privilèges de validation s'appliquent également à l'annulation.* Si vous avez implémenté des domaines d'accès, le pare-feu applique automatiquement ces domaines pour filtrer la portée de l'annulation (voir Périphérique > Domaine d'accès). Indépendamment de votre rôle administratif, le pare-feu n'annule que les modifications de configuration dans les domaines d'accès affectés à votre compte.
Annuler les modifications effectuées par	Permet de filtrer la portée des modifications de configuration que le pare-feu annule. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle de super-utilisateur** – Vous pouvez limiter la portée de l'annulation aux modifications apportées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège de **Valider pour les autres administrateurs**, vous pouvez limiter la portée de l'annulation aux modifications configurées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège de **Valider pour les autres administrateurs**, vous pouvez limiter la portée de l'annulation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtrez la portée de l'annulation comme suit : • **Filtrer par administrateur** – Même si votre rôle permet d'annuler les modifications d'autres administrateurs, la portée de l'annulation inclut uniquement vos modifications par défaut. Pour ajouter d'autres administrateurs à la portée de l'annulation, cliquez sur le lien **<usernames> (<noms d'utilisateur>)**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les modifications dans des emplacements spécifiques pour les Inclure dans l'annulation. Si vous avez implémenté des domaines d'accès, le pare-feu filtre automatiquement la portée de l'annulation en fonction de ces domaines (voir Périphérique > Domaine d'accès). Quels que soient votre rôle administratif et vos choix de filtrage, la portée de l'annulation inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte.
Portée de l'annulation	Liste les emplacements qui ont des modifications à annuler. Que la liste inclue toutes les modifications ou un sous-ensemble de modifications dépend de plusieurs facteurs, comme décrit pour les options Annuler toutes les modifications et Annuler les modifications effectuées par. Les emplacements peuvent être l'un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l'emplacement Partagé. • **policy-and-objects (politique et objets)** – (Pare-feu uniquement) Règles de politique ou objets définis sur un pare-feu qui ne possède pas plusieurs systèmes virtuels. • **device-and-network (périphérique et réseau)** – (Pare-feu uniquement) Paramètres réseau et périphériques qui sont globaux (tels que les profils de gestion d'interface) et non spécifiques à un système virtuel. • **<virtual-system> (<système-virtuel>)** – (Pare-feu uniquement) Le nom du système virtuel dans lequel les règles ou objets de stratégie sont définis sur un pare-feu doté de plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones).

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **<device-group> (<groupe de périphériques>)** – (Panorama uniquement) Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • **<template> (<modèle>)** – (Panorama uniquement) Le nom du modèle ou de la pile de modèles dans lequel les paramètres sont définis. • **<log-collector-group> (<groupe de collecteurs de journaux>)** – (Panorama uniquement) Le nom du Groupe de collecteurs dans lequel les paramètres sont définis. • **<log-collector> (<collecteur de journaux>)** – (Panorama uniquement) Le nom du Collecteur de journaux dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements où les modifications ont été apportées : • **Systèmes virtuels** – (Pare-feu uniquement) Les paramètres définis dans un système virtuel spécifique. • **Groupe de périphériques** – (Panorama uniquement) Les paramètres définis dans un groupe de périphériques spécifique. • **Modèle** – (Panorama uniquement) Les paramètres définis dans un modèle ou une pile de modèles spécifiques. • **Groupe de collecteurs de journaux** – (Panorama uniquement) Les paramètres spécifiques à une configuration de Groupe de collecteurs. • **Collecteur de journaux** – (Panorama uniquement) Les paramètres spécifiques à une configuration de Collecteur de journaux. • **Autres changements** – Paramètres qui ne sont pas spécifiques à l'une des zones de configuration précédentes (telles que les objets partagés).
Inclure dans l'annulation (Annulation partielle uniquement)	Permet de sélectionner les modifications que vous souhaitez annuler. Par défaut, toutes les modifications de la **Portée d'annulation** sont sélectionnées. Cette colonne s'affiche uniquement après avoir choisi d'**Annuler les modifications effectuées par** des administrateurs spécifiques.  *Certaines dépendances peuvent affecter les modifications que vous incluez dans une annulation. Par exemple, si vous ajoutez un objet et un autre administrateur puis que vous modifiez cet objet, vous ne pouvez pas annuler votre modification sans annuler la modification pour l'autre administrateur.*
Regrouper par type d'emplacement	Liste les modifications de configuration dans la **Portée d'annulation** par **Type d'emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans la **Portée d'annulation** à la configuration en cours d'exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge).

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	Pour vous aider à faire correspondre les modifications aux sections de l'interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d'exécution que vous comparez. *Etant donné que les résultats de la prévisualisation s'affichent dans une nouvelle fenêtre, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant de débloquer l'ouverture des fenêtres contextuelles.*
Modifier le récapitulatif	Liste les paramètres individuels pour lesquels vous annulez les modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l'objet** – Le nom qui identifie la politique, l'objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d'emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L'administrateur qui a effectué la dernière modification du paramètre. • **Sera annulé** – Indique si l'opération d'annulation inclut le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Rétablir	Annule les modifications sélectionnées.

© 2020 Palo Alto Networks, Inc.

Configurations du verrouillage

Pour vous aider à coordonner les tâches de configuration avec d'autres administrateurs de pare-feu lors de sessions de connexion simultanées, l'interface Web vous permet de verrouiller la configuration ou la validation. Ainsi, aucun autre administrateur ne peut modifier la configuration ou valider des modifications jusqu'à suppression de ce verrou.

Dans le coin supérieur droit de l'interface Web, un cadenas verrouillé ( ) indique qu'un ou plusieurs verrous ont été activés (avec le nombre de verrous entre parenthèses) et un cadenas déverrouillé ( ) indique qu'aucun verrou n'a été activé. En cliquant sur le cadenas verrouillé ou déverrouillé, la boîte de dialogue Verrous s'ouvrira et fournira par le fait même les options et les champs suivants.

Pour configurer le pare-feu afin d'activer automatiquement un verrou de validation chaque fois qu'un administrateur modifie la configuration candidate, sélectionnez Device (Périphérique) > Setup (Configuration) > Management (Gestion), modifiez les Paramètres généraux, activez Automatically Acquire Commit Lock (Appliquer automatiquement un verrou de validation), puis cliquez sur OK et Commit (Valider).

Lorsque vous annulez les modifications (Config (Configuration) > Revert Changes (Annuler les modifications)), le pare-feu verrouille automatiquement la configuration candidate et active afin que les autres administrateurs ne puissent ni éditer les paramètres ni valider des modifications. Le pare-feu supprime automatiquement le verrou une fois l'annulation terminée.

Champ/Bouton	Description
Admin	Le nom d'utilisateur de l'administrateur qui a activé le verrou.
Location (Emplacement)	Sur un pare-feu possédant plus d'un système virtuel (vsys), la portée du verrou peut affecter un vsys spécifique ou l'emplacement Partagé.
Type	Voici les différents types de verrous : • **Verrou de configuration** : empêche d'autres administrateurs de modifier la configuration candidate. Seuls un super utilisateur ou l'administrateur qui a activé le verrou peuvent le retirer. • **Verrou de validation** – Empêche d'autres administrateurs de valider des modifications apportées à la configuration candidate. La file d'attente de validations n'accepte aucune nouvelle validation jusqu'à ce que tous les verrous aient été retirés. Ce verrou empêche l'occurrence de collisions qui peuvent se produire lorsque plusieurs administrateurs apportent des changements au cours de sessions de connexion simultanées, puis qu'un administrateur termine et lance une validation avant que les autres administrateurs aient terminé. Le pare-feu retire automatiquement le verrou après avoir terminé la validation pour laquelle l'administrateur avait activé le verrou. Un super utilisateur ou l'administrateur qui a activé le verrou peut également le retirer manuellement.

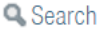
© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Commentaire	Saisissez un texte allant jusqu'à 256 caractères. Cette fonction est utile pour les autres administrateurs qui veulent connaître la raison de l'activation du verrou.
Créé à	La date et l'heure où un administrateur a activé le verrou.
Connecté(s)	Indique si l'administrateur ayant activé le verrou est actuellement connecté ou non.
Poser un verrou	Pour activer un verrou, cliquez sur **Take a Lock (Poser un verrou)**, sélectionnez le **Type**, sélectionnez le **Location (Emplacement)** (pare-feu à plusieurs systèmes virtuels), saisissez des **Comments (Commentaires)** facultatifs, cliquez sur **OK** puis vous pouvez **Close (Fermer)**.
Supprimer le verrouillage	Pour retirer un verrou, sélectionnez-le, cliquez sur **Remove Lock (Retirer le verrou)**, cliquez ensuite sur **OK**, puis sur **Close (Fermer)**.

© 2020 Palo Alto Networks, Inc.

Recherche globale

La recherche globale vous permet de rechercher une chaîne particulière, telle qu'une adresse IP, un nom d'objet, un nom de politique, un ID de menace, un UUID de règle ou un nom d'application, dans la configuration candidate sur un pare-feu ou Panorama. Les résultats de la recherche sont regroupés par catégorie et fournissent des liens vers l'emplacement de la configuration dans l'interface Web, de manière à pouvoir trouver facilement tous les endroits où la chaîne existe ou a été référencée.

Pour lancer la recherche globale, cliquez sur l'icône de **Recherche** 

située en haut à droite de l'interface Web. La Recherche globale est disponible à partir de toutes les pages et de tous les emplacements de l'interface Web. Voici une liste des fonctionnalités de la recherche globale qui vous permettront d'effectuer des recherches réussies :

- Si vous initiez une recherche sur un pare-feu avec plusieurs systèmes virtuels ou si les rôles administrateur sont définis, la Recherche globale renvoie uniquement les résultats pour les zones du pare-feu pour lesquelles vous disposez d'autorisations. Il en va de même pour les groupes de périphériques Panorama ; vous verrez les résultats de la recherche uniquement pour les groupes de périphériques pour lesquels vous disposez d'un accès administratif.
- Les espaces dans le texte de la recherche sont traités comme des opérations ET. Par exemple, si vous recherchez`corp policy`, à la fois **entreprise** et **politique** doivent exister dans l'élément de configuration pour qu'il soit inclus dans les résultats de la recherche.
- Pour rechercher une expression exacte, mettez-la entre guillemets.
- Pour relancer une recherche précédente, cliquez sur Recherche globale et une liste des 20 dernières recherches s'affiche. Cliquez sur un élément de la liste pour relancer cette recherche. La liste d'historique de recherche est unique pour chaque compte administrateur.

Recherche globale est disponible pour chaque champ qui peut faire l'objet d'une recherche. Par exemple, dans le cas d'une politique de sécurité, vous pouvez faire porter la recherche sur les champs suivants : Nom, Étiquettes, Zone, Adresse, Utilisateur, Profil HIP, Application, UUID et Service. Pour effectuer une recherche, cliquez sur la liste déroulante à côté de l'un de ces champs, puis sur **Recherche globale**. Par exemple, si vous cliquez sur **Recherche globale** dans une zone nommée l3-vlan-trust, la Recherche globale recherche cette zone dans l'ensemble de la configuration et les résultats pour chaque emplacement où la zone est référencée sont renvoyés. Les résultats de la recherche sont regroupés par catégorie et vous pouvez pointer chaque élément avec la souris pour en afficher les détails ou cliquer sur un élément pour accéder sa page de configuration.

La Recherche globale ne recherche pas de contenu dynamique que le pare-feu affecte aux utilisateurs (comme les journaux, les plages d'adresses ou les adresses DHCP individuelles). Dans le cas de DHCP, vous pouvez faire porter la recherche sur un attribut de serveur DHCP, tel que l'entrée NS, mais vous ne pouvez pas rechercher d'adresses émises pour les utilisateurs. Un autre exemple est les noms d'utilisateur que le pare-feu collecte lorsque vous activez la fonctionnalité User-ID ™. Dans ce cas, un nom d'utilisateur ou un groupe d'utilisateurs existant dans la base de données User-ID peut faire l'objet d'une recherche uniquement si le nom ou le groupe existe dans la configuration, comme lorsqu'un nom de groupe d'utilisateurs est défini dans une politique. En général, vous pouvez rechercher uniquement du contenu que le pare-feu écrit dans la configuration.

Vous souhaitez en savoir plus ?

En savoir plus sur l'utilisation de la Recherche globale pour rechercher la configuration du pare-feu ou de Panorama.

© 2020 Palo Alto Networks, Inc.

Détails de la menace

- Surveillance > Journaux > Menace
- ACC > Activité des menaces
- Objets > Profils de sécurité > Antispyware / Protection contre les vulnérabilités

Utilisez la boîte de dialogue Détails de la menace pour en savoir plus sur les signatures de menaces qui équipent le pare-feu et les événements qui déclenchent ces signatures. Les détails de la menace sont fournis pour :

- Les journaux de menace qui enregistrent les menaces détectées par le pare-feu (**Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**)
- Les principales menaces découvertes dans votre réseau (**ACC** > **Threat Activity (Activité des menaces)**)
- Les signatures de menaces que vous souhaitez modifier ou exclure de l'exécution (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware/Vulnerability Protection (Protection antispyware / contre les vulnérabilités)**)

Lorsque vous trouvez une signature de menace à propos de laquelle vous souhaitez en apprendre davantage, passez la souris sur le **Threat Name (Nom de la menace)** ou l'**ID** de menace et cliquez sur **Exception** pour examiner les détails de la menace. Les détails de la menace vous permettent de vérifier facilement si une signature de menace est configurée en tant qu'exception à votre politique de sécurité et de trouver les dernières informations relatives à l'Archivage sécurisé des menaces d'une menace spécifique. La base de données d'Archivage sécurisé des menaces de Palo Alto Networks est intégrée au pare-feu, ce qui vous permet de visualiser de plus amples détails sur les signatures de menaces dans le contexte du pare-feu ou de lancer une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur pour une menace enregistrée.

Selon le type de menace que vous visualisez, les détails incluent tous ou certains détails de la menace décrits dans le tableau suivant.

Détails de la menace	Description
Name (Nom)	Nom de la signature de menace.
ID	ID de signature de menace unique. Sélectionnez **View in Threat Vault (Afficher dans l'Archivage sécurisé des menaces)** pour ouvrir une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur et rechercher les dernières informations que la base de données des menaces de Palo Alto Networks détient pour cette signature. L'entrée d'Archivage sécurisé des menaces pour la signature de la menace peut inclure des détails supplémentaires, y compris les premières et dernières versions de contenu pour inclure les mises à jour de la signature et la version PAN-OS minimale requise pour prendre en charge la signature.
Description	Informations sur la menace qui déclenche la signature.
Sévérité	Le niveau de gravité de la menace : informations, faible, moyen, élevé ou critique.
CVE	Failles de sécurité connues associées à la menace. L'identifiant des Failles et vulnérabilités communes (CVE) est l'identifiant le plus utile pour trouver des informations sur les vulnérabilités uniques, car les ID spécifiques aux fournisseurs incluent généralement de multiples vulnérabilités.

© 2020 Palo Alto Networks, Inc.

Détails de la menace	Description
ID bugtraq	L'ID Bugtraq associée à la menace.
ID constructeur	L'identifiant spécifique au fournisseur d'une vulnérabilité. Par exemple, MS16-148 est l'ID de fournisseur pour une ou plusieurs vulnérabilités Microsoft et APBSB16-39 est l'ID de fournisseur pour une ou plusieurs vulnérabilités Adobe.
Référence	Les sources de recherche que vous pouvez utiliser pour en savoir plus sur la menace.
Profils d'exemption	Les profils de sécurité qui définissent une action d'application différente pour la signature de menace que l'action de signature par défaut. L'exception de menace n'est active que lorsque des profils d'exemption sont attachés à une règle de politique de sécurité (vérifiez si l'exception est Utilisée dans la règle de sécurité actuelle).
Utilisé dans la règle de sécurité en cours	Exceptions de menace actives – Une coche dans cette colonne indique que le pare-feu applique activement l'exception de menace (les Profils d'exemption qui définissent l'exception de menace sont attachés à une règle de politique de sécurité). Si cette colonne est décochée, le pare-feu applique la menace en se basant uniquement sur l'action de signature par défaut recommandée.
Exempter les adresses IP	Adresses IP d'exemption – Vous pouvez ajouter une adresse IP sur laquelle filtrer l'exception de menace ou afficher les **Exempt IP Addresses (Adresses IP d'exemption)** existantes. Cette option n'applique une exception de menace que lorsque la session associée comporte une adresse IP source ou de destination qui correspond à l'adresse IP d'exemption. Pour toutes les autres sessions, la menace est appliquée en fonction de l'action de signature par défaut.

Si vous rencontrez des difficultés pour afficher les détails de la menace, vérifiez les conditions suivantes :

- *La licence de Prévention contre les menaces du pare-feu est active (Device (Périphérique) > Licenses (Licences)).*
- *Les dernières mises à jour de contenu des Antivirus, des Menaces et des Applications sont installées.*
- *L'accès à l'Archivage sécurisé des menaces est activé (sélectionnez Device (Périphérique) > Setup (Configuration) > Management (Gestion) et modifier le paramètre Logging and Reporting (Journalisation et génération de rapports) sur Enable Threat Vault Access (Activer l'accès à l'archivage sécurisé des menaces)).*
- *Les valeurs par défaut (ou personnalisées) des profils de sécurité Antivirus, Antispyware et Contre les vulnérabilités sont appliquées à votre politique de sécurité.*

© 2020 Palo Alto Networks, Inc.

Récapitulatif d'AutoFocus Intelligence

Vous pouvez afficher un aperçu graphique des renseignements sur les menaces que AutoFocus compile pour vous aider à évaluer l'omniprésence et les risques des artefacts de pare-feu suivants :

- Adresse IP
- URL
- Domain (Domaine)
- agent utilisateur (trouvé dans la colonne Agent utilisateur des Journaux de filtrage des données) ;
- nom de la menace (uniquement pour les menaces des sous-types de virus et du virus détectés par WildFire) ;
- Filename
- hachage SHA-256 (trouvé dans la colonne Prétraitement de fichier des journaux Envois WildFire).

Pour consulter la fenêtre AutoFocus Intelligence Summary (Récapitulatif d'AutoFocus Intelligence), vous devez d'abord avoir un abonnement actif à AutoFocus et activez les renseignements de menaces AutoFocus (sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres AutoFocus).

Après avoir activé les renseignements AutoFocus, placez votre souris sur un artefact de journal ou de liste dynamique externe pour ouvrir le menu déroulant ( ), puis cliquez sur **AutoFocus** :

- afficher le Trafic, les Menaces, le Filtrage des URL, les Envois WildFire, le Filtrage des données et les Journaux unifiés (**Monitor (Surveillance)** > **Logs (Journaux)**).
- afficher les entrées de la liste dynamique externe.

Vous pouvez également lancer la recherche AutoFocus à partir du pare-feu pour étudier davantage les artefacts intéressants ou suspects que vous trouvez.

Champ/Bouton	Description
Rechercher l'AutoFocus pour...	Cliquez pour lancer une recherche AutoFocus pour l'artefact.
Onglet Informations d'analyse	
Sessions	Le nombre de sessions privées dans lesquelles WildFire a détecté l'artefact. Les sessions privées sont celles qui s'exécutent uniquement sur les pare-feu associés à votre compte de support. Placez le curseur sur une barre de session pour afficher le nombre de sessions par mois.
Échantillons	Organisation et échantillons globaux (fichiers et liens d'e-mail) associés à l'artefact et regroupés par verdict de WildFire (bénins, indésirables, malveillants, hameçonnage). *Global* fait référence à des échantillons provenant de tous les envois WildFire, alors que *organisation* se réfère uniquement aux échantillons soumis à WildFire par votre organisation. Cliquez sur un verdict de WildFire pour lancer une recherche AutoFocus pour l'artefact filtré par portée (organisation ou mondiale) et le verdict de WildFire.
Tags correspondantes	Tags AutoFocus qui correspondent à l'artefact : • **Tags privés** – Visibles uniquement pour les utilisateurs AutoFocus associés à votre compte de support.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **Tags publics** – Visibles pour tous les utilisateurs AutoFocus. • **Tags de l'Unité 42** – Identifient les menaces et les campagnes constituant un risque direct relatif à la sécurité. Ces tags sont créées par l'Unité 42 (l'équipe de recherche et de renseignement sur les menaces de Palo Alto Networks). • **Tags informationels** – Tags de l'Unité 42 qui identifient les menaces touchant les produits informatiques. Placez le curseur sur un tag pour afficher la description de le tag et d'autres détails concernant le tag. Cliquez sur un tag pour lancer une recherche AutoFocus pour ce tag. Pour afficher plus de tags correspondantes pour un artefact, cliquez sur le symbole (...) pour lancer une recherche AutoFocus pour cet artefact. La colonne Tags dans les résultats de recherche AutoFocus affiche plus de tags correspondantes pour l'artefact.
Onglet DNS passif L'onglet DNS passif affiche l'historique du DNS passif associé à l'artefact. Cet onglet affiche uniquement des informations correspondantes si l'artefact est une adresse IP, un domaine ou une URL.	
Requête	Le domaine qui a soumis une requête DNS. Cliquez sur le domaine pour lancer une recherche AutoFocus pour ce dernier.
Type	Le type de demande DNS (par exemple : A, NS, CNAME).
Réponse	L'adresse IP ou le domaine dont la requête DNS a pris la forme. Cliquez sur l'adresse IP ou le domaine pour lancer une recherche AutoFocus. *La colonne Réponse n'affiche pas d'adresses IP privées.*
Nombre	Le nombre de fois que la requête a été soumise.
Première apparition	La date et l'heure auxquelles la combinaison Requête, Réponse et Type a été vue pour la première fois en fonction de l'historique DNS passif.
Vu en dernier	La date et l'heure auxquelles la combinaison Requête, Réponse et Type a été vue le plus récemment en fonction de l'historique DNS passif.
Onglet Hachages correspondants L'onglet Hachages correspondants affiche les cinq échantillons privés les plus récents dans lesquels WildFire a détecté l'artefact. Les échantillons privés sont ceux qui sont détectés uniquement sur les pare-feu associés à votre compte de support.	
Sha256	Le hachage SHA-256 pour un échantillon. Cliquez sur le hachage pour lancer une recherche AutoFocus pour ce hachage.
Type de fichier	Le type de fichier de l'échantillon.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Date de création	La date et l'heure auxquelles WildFire a analysé un échantillon et lui a affecté un verdict de WildFire.
Date de la mise à jour	La date et l'heure auxquelles WildFire a mis à jour le verdict de WildFire pour un échantillon.
Verdict	Le verdict de WildFire pour un échantillon : bénin, indésirable, malveillant ou hameçonnage.

© 2020 Palo Alto Networks, Inc.

Exportation du tableau de configuration

Les utilisateurs administratifs peuvent exporter les données qui figurent dans les bases de règles de politiques, les objets, les périphériques gérés et les interfaces dans un format tabulaire, soit dans un fichier PDF, soit dans un fichier CSV. Les données exportées sont celles qui sont visibles sur l'interface Web. Dans le cas de données filtrées, seules les données correspondant au filtre sont exportées. Si vous n'appliquez aucun filtre, tous les données sont exportées.

Toutes les données de nature délicate, comme les mots de passe, sont masquées par des symboles génériques (*).

Un journal système et un lien de téléchargement sont générés lorsque l'exportation du tableau de configuration s'effectue avec succès. Utilisez le lien de téléchargement pour enregistrement le fichier PDF ou CSV localement. Après la fermeture de la fenêtre qui contient le lien de téléchargement, le lien de téléchargement de cette exportation n'est plus disponible.

Pour exporter des données du tableau, cliquez sur **PDF/CSV** et configurez les paramètres suivants :

Paramètres d'exportation	Description
File Name (Nom du fichier)	Saisissez un nom (maximum de 32 caractères) pour identifier les données exportées. Ce nom devient le nom du fichier téléchargé qui est généré lors de l'exportation.
Type de fichier	Sélectionnez le type de résultats d'exportation à générer. Vous pouvez choisir le format PDF ou CSV.
Taille de la page	Par défaut, la taille de la page est définie sur lettre (8,5 sur 11,0 po). Vous ne pouvez pas modifier la taille de la page. Par défaut, le PDF est généré en orientation portrait et passe à l'orientation paysage pour permettre l'intégration du nombre maximal de colonnes.
Description (PDF uniquement)	Saisissez une description (maximum de 255 caractères) pour fournir le contexte et des informations supplémentaires de l'exportation.
Données du tableau	Montre les données du tableau qui seront exportées. Si vous devez effacer les paramètres de filtrage qui vous avez définis précédemment, cliquez sur **Show All Columns (Afficher toutes les colonnes)** pour afficher toutes les règles de politique qui correspondent au type de politique sélectionné. Vous pouvez ensuite ajouter ou supprimer des colonnes et appliquer des filtres, au besoin.
Montrer toutes les colonnes	Supprime tous les filtres et affiche toutes les colonnes du tableau.

Cliquez sur **Export (Exporter)** pour générer le lien de téléchargement du tableau de configuration.

Tableau de bord

Les widgets du Tableau de bord affichent les informations générales concernant le pare-feu ou Panorama™, comme la version du logiciel, l'état de chaque interface, l'utilisation des ressources et jusqu'à 10 entrées pour chaque type de journaux ; les widgets de journaux affichent les entrées depuis la dernière heure.

Le sujet Widgets du tableau de bord décrit la manière d'utiliser le Tableau de bord et décrit les widgets disponibles.

© 2020 Palo Alto Networks, Inc.

Widgets du tableau de bord

Par défaut, le **Tableau de bord** affiche les widgets dans une **Structure** à **3 colonnes**, mais vous pouvez personnaliser les **Tableaux de bord** pour afficher uniquement **2 colonnes**.

Vous pouvez également choisir les widgets à afficher ou à masquer pour visualiser uniquement ceux que vous souhaitez contrôler. Pour afficher un widget, sélectionnez une catégorie de widget à partir du menu déroulant **Widgets** et sélectionnez-en un pour l'ajouter au Tableau de bord (les noms des widgets qui apparaissent comme grisés sont déjà affichés). Vous pouvez cacher (cesser l'affichage) un widget en fermant celui-ci ( dans l'en-tête du widget). Les pare-feu et Panorama sauvegardent vos paramètres d'affichage des widgets au cours des connexions (connexion séparée pour chaque administrateur).

Veuillez vous référer à l'horodatage de la **Dernière mise à jour** pour déterminer quand les données du tableau de bord ont été actualisées pour la dernière fois. Vous pouvez actualiser manuellement l'ensemble du **Tableau de bord** ( dans le coin supérieur droit du Tableau de bord) ou vous pouvez actualiser les widgets individuels ( dans chaque en-tête de widget). Utilisez le menu déroulant sans référence à côté de l'option d'actualisation manuelle du Tableau de bord () pour sélectionner l'intervalle d'actualisation automatique pour l'ensemble du **Tableau de bord** (en minutes) : **1 minute**, **2 minutes** ou **5 minutes.** Pour désactiver l'actualisation automatique de l'ensemble du **Tableau de bord**, sélectionnez **Actualisation manuelle**.

Widgets du tableau de bord	Description
Widgets Application	
Applications principales	Affiche les applications ayant le plus grand nombre de sessions. La taille du bloc indique le nombre relatif de sessions (passez la souris sur le bloc pour afficher le nombre correspondant) et la couleur indique les risques de sécurité ; vert pour des risques faibles et rouge pour des risques élevés. Cliquez sur une application pour afficher son profil d'application.
Applications principales à haut risque	Similaire à Principales applications, sauf que les applications présentant les risques les plus élevés avec la plupart des sessions sont affichées.
Facteur de risque de ACC	Affiche le facteur de risque moyen (entre 1 et 5) du trafic réseau traité au cours de la semaine passée. Plus la valeur est élevée, plus le risque est important.
Widgets Système	
Informations générales	Affiche le nom et le modèle du pare-feu ou de Panorama, le processeur et la mémoire vive de Panorama, le mode du système de Panorama, la version logicielle de PAN-OS® ou de Panorama, les informations de gestion IPv4 et IPv6, le numéro de série, l'ID de CPU et l'UUID, les versions des définitions des applications, du trafic, des menaces et du filtrage des URL, la date et l'heure actuelles et la période de temps depuis le dernier redémarrage.
Interfaces (Pare-feu uniquement)	Indique si chaque interface est active (vert), inactive (rouge) ou si son état est inconnu (gris).

© 2020 Palo Alto Networks, Inc.

Widgets du tableau de bord	Description
Ressources systèmes	Affiche la Gestion de l'utilisation du processeur, l'utilisation du Panneau de données et le Nombre de sessions (le nombre de sessions établies via le pare-feu ou Panorama).
Haute disponibilité	Si la haute disponibilité (HD) est activée, il indique l'état HD du pare-feu / Panorama local et homologue ; vert (actif), jaune (passif) ou noir (autre). Pour plus d'informations sur la HD, reportez-vous à la section Périphérique > Systèmes virtuels ou Panorama > Haute disponibilité.
Verrous	Montre les verrous de configuration qui ont été établis par les administrateurs.
Administrateurs connectés	Affiche l'adresse IP source, le type de session (interface Web ou CLI) et l'heure de début de session pour chaque administrateur actuellement connecté.
Widgets Journaux	
Journaux des menaces	Affiche l'ID de menace, l'application, ainsi que la date et l'heure des 10 dernières entrées du journal des menaces. L'ID de menace correspond à la description ou à l'URL d'un site malveillant qui va à l'encontre du profil de filtrage des URL. Seules les entrées des 60 dernières minutes sont affichées.
Journaux de filtrage des URL	Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des URL.
Journaux de filtrage des données	Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des données.
Journaux de configuration	Affiche le nom d'utilisateur de l'administrateur, le client (interface Web ou CLI), ainsi que la date et l'heure des 10 dernières entrées du journal de configuration. Seules les entrées des 60 dernières minutes sont affichées.
Journaux systèmes	Affiche la description, ainsi que la date et l'heure des 10 dernières entrées du journal système. *Une entrée « Configuration installée » indique que les modifications apportées à la configuration ont été correctement validées. Seules les entrées des 60 dernières minutes sont affichées.*

ACC

Le centre de commande de l'application (ACC) est un outil analytique qui fournit des renseignements exploitables concernant l'activité sur votre réseau. L'ACC utilise les journaux du pare-feu pour représenter graphiquement les tendances du trafic sur votre réseau. Cette représentation graphique vous permet d'interagir avec les données et de visualiser les relations entre les événements sur le réseau, notamment les modèles d'utilisation réseau, les modèles de trafic, les activités suspectes et les anomalies.

- Aperçu de l'ACC
- Onglets de l'ACC
- Widgets de l'ACC
- Actions de l'ACC
- Utilisation des onglets et des widgets
- Utilisation des filtres – Filtres locaux et filtres généraux

Vous souhaitez en savoir plus ?

Reportez-vous à la section Utilisation du centre de commande de l'application.

© 2020 Palo Alto Networks, Inc.

Aperçu de l’ACC

Le tableau suivant affiche l’onglet ACC et décrit chaque composant.

Aperçu de l’ACC


1	**Onglets**	L’ACC comprend des onglets prédéfinis qui offrent une visibilité sur le trafic réseau, l’activité des menaces, les activités bloquées, l’activité du tunnel, l’activité GlobalProtect et l’activité du réseau mobile (si la sécurité GTP est activée). Pour plus d’informations sur chaque onglet, reportez-vous à la section Onglets ACC.
2	**Widgets (Widgets)**	Chaque onglet inclut un ensemble de widgets par défaut qui représentent le mieux les événements et les tendances associés à l’onglet. Les widgets vous permettent d’examiner les données à l’aide des filtres suivants : nombre d’octets (entrants et sortants), sessions, contenu (fichiers et données), catégories d’URL, applications, utilisateurs, menaces (malveillantes, bénignes, indésirables, hameçonnage) et nombre. Pour plus d’informations sur chaque widget, reportez-vous à la section Widgets ACC.
3	**Période**	Les diagrammes et les graphiques de chaque widget fournissent un affichage en temps réel de l’historique. Vous pouvez choisir un intervalle personnalisé ou utiliser une période prédéfinie, allant des 15 dernières minutes aux 30 derniers jours ou aux 30 derniers jours calendaires. La période utilisée pour effectuer le rendu des données est, par défaut, la dernière heure. Les intervalles de date et d’heure sont affichés à l’écran. Par exemple : `11/11 10:30:00-01/12 11:29:59`

© 2020 Palo Alto Networks, Inc.

Aperçu de l'ACC		
4	**Filtres Globaux**	Les filtres généraux vous permettent de définir un filtre pour tous les onglets. Les diagrammes et les graphiques appliquent les filtres sélectionnés avant d'effectuer le rendu des données. Pour plus d'informations sur l'utilisation des filtres, reportez-vous à la section Actions ACC.
5	**Affichage des applications par**	L'affichage de l'application vous permet de filtrer la vue ACC soit par les applications approuvées et non approuvées utilisées sur votre réseau, soit par le niveau de risque des applications utilisées sur votre réseau. Le vert indique les applications approuvées, le bleu les applications non approuvées et le jaune indique les applications qui ont un état d'approbation différent au sein de différents systèmes virtuels ou groupes de périphériques.
6	**Échelle de risque**	L'échelle de risque allant de 1 (risque le plus faible) à 5 (risque le plus élevé) indique le risque de sécurité relatif sur votre réseau. L'échelle de risque utilise différents facteurs, tels que le type des applications vues sur le réseau et les niveaux de risque associés aux applications, l'activité des menaces et les logiciels malveillants via le nombre de menaces bloquées, ainsi que les hôtes compromis ou le trafic vers les hôtes et les domaines malveillants.
7	**Source**	Les données utilisées pour l'affichage varient entre le pare-feu et Panorama™. Les options suivantes sont à votre disposition pour sélectionner les données utilisées pour générer les vues sur l'ACC : **Système virtuel** : sur un pare-feu qui est activé pour plusieurs systèmes virtuels, vous pouvez utilisez le menu déroulant **Système virtuel** pour modifier l'affichage ACC pour inclure tous les systèmes virtuels ou seulement une sélection de systèmes virtuels. **Groupe de périphériques**: sur Panorama, vous pouvez utiliser le menu déroulant **Groupe de périphériques** pour modifier l'affichage ACC pour inclure des données provenant de tous les groupes de périphériques ou uniquement d'une sélection de groupes de périphériques. **Source de données** : sur Panorama, vous pouvez également modifier l'affichage pour utiliser **Panorama** ou les **Données du périphérique distant** (données du pare-feu géré). Lorsque la source de données est **Panorama**, vous pouvez filtrer l'affichage pour un groupe de périphériques spécifique.
8	**Export (Exporter)**	Vous pouvez exporter les widgets affichés dans l'onglet actif au format PDF.

© 2020 Palo Alto Networks, Inc.

Onglets de l'ACC

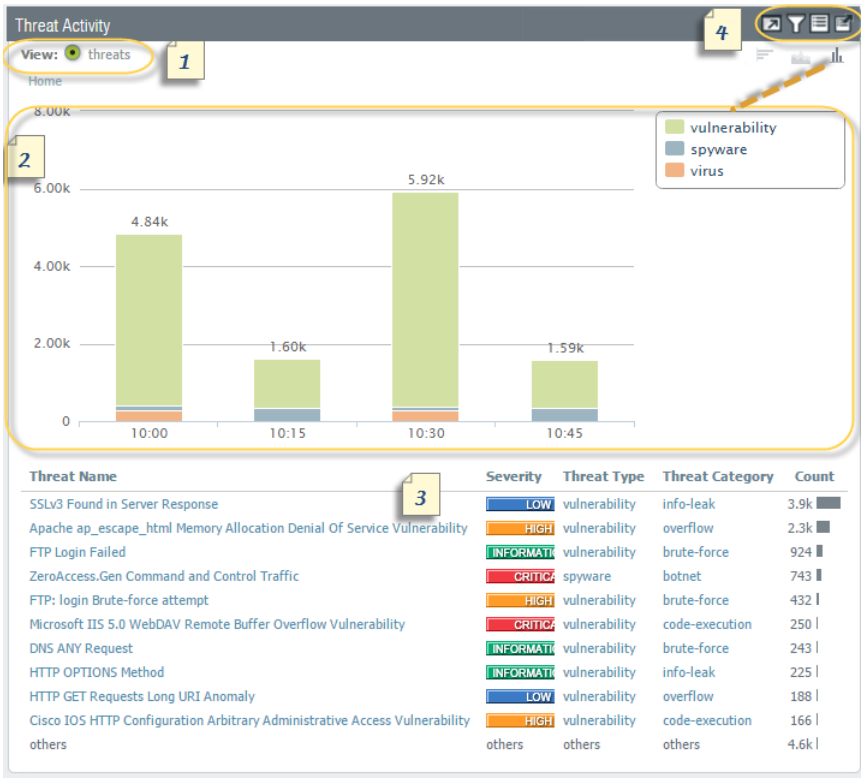
- **Network Activity (Activité du réseau)** – Affiche une vue d'ensemble du trafic et de l'activité des utilisateurs sur votre réseau. Cette vue se concentre sur les applications les plus utilisées, les principaux utilisateurs qui génèrent du trafic en examinant le nombre d'octets, le contenu, les menaces et les URL consultées par les utilisateurs, et les règles de politique de sécurité les plus utilisées auxquelles le trafic correspond. De plus, vous pouvez afficher l'activité réseau par zone source ou de destination, région, adresse IP, interface d'entrée ou de sortie et par information sur l'hôte, notamment les systèmes d'exploitation des périphériques les plus couramment utilisés sur le réseau.
- **Activité des menaces** – Affiche une vue d'ensemble des menaces sur le réseau. Il se concentre sur les principales menaces : vulnérabilités, logiciels espions, virus, hôtes visitant des domaines ou URL malveillants, principaux envois WildFire par type de fichier et application, et applications qui utilisent des ports non standard. Le widget Hôtes compromis complète la détection par de meilleures techniques de visualisation. Il utilise les informations de l'onglet Événements corrélés (Surveillance > Moteur de corrélation automatique > Événements corrélés) pour présenter une vue agrégée des hôtes compromis sur votre réseau par utilisateurs source ou adresses IP, triés par gravité.
- **Activités bloquées** – Se concentre sur le trafic dont l'entrée sur le réseau a été empêchée. Les widgets de cet onglet vous permettent d'afficher l'activité refusée par nom d'application, nom d'utilisateur, nom de menace, contenu (fichiers et données) et les principales règles de sécurité dont l'action de refus a bloqué le trafic.
- **Mobile Network Activity (Activité du réseau mobile)** – Affiche une représentation visuelle du trafic mobile sur votre réseau à l'aide des journaux GTP générés à partir de votre configuration de la règle de politique de sécurité. Cette vue comprend des widgets interactifs et personnalisables d'Événements GTP, d'Activité de l'abonné mobile et de Causes de rejet GTP auxquels vous pouvez appliquer des Filtres de l'ACC et descendre dans la hiérarchie pour isoler les informations dont vous avez besoin. Lorsque vous activez la Sécurité SCTP, les widgets de cet onglet affiche une représentation visuelle et les détails des événements SCTP sur le pare-feu, de même que le nombre de blocs envoyés et reçus par ID d'association SCTP.
- **Activité du tunnel** – Affiche l'activité du trafic du tunnel que le pare-feu a inspecté en fonction de vos politiques d'inspection du tunnel. Les informations incluent l'utilisation du tunnel en fonction de l'ID de tunnel, de la balise de surveillance, de l'utilisateur et des protocoles de tunnel tels que l'Encapsulation générique de routage (GRE), le Protocole de tunnel de type GPRS (General Packet Radio Service) pour les Données utilisateur (GTP-U) et le protocole IPSec non crypté.
- **Activité GlobalProtect** – Affiche une vue d'ensemble de l'activité des utilisateurs de votre déploiement GlobalProtect. Les informations incluent le nombre d'utilisateurs et le nombre de fois que les utilisateurs se sont connectés, les passerelles auxquelles les utilisateurs se sont connectés, le nombre d'échecs de connexion ainsi que la raison de l'échec, un récapitulatif des méthodes d'authentification et les versions de l'application GlobalProtect utilisées, ainsi que le nombre de postes en quarantaine.

Vous pouvez également personnaliser les onglets et les widgets, comme décrit dans la rubrique Utilisation des onglets et des widgets*.*

© 2020 Palo Alto Networks, Inc.

Widgets de l'ACC

Les widgets de chaque onglet sont interactifs. Vous pouvez définir des filtres et obtenir un affichage détaillé en la personnalisant et en l'axant sur les informations dont vous avez besoin.



Chaque widget est structuré pour afficher les informations suivantes :

1	**Vue**	Vous pouvez trier les données par nombre d'octets, sessions, menaces, nombre, utilisateurs, contenu, applications, URL, caractère malveillant, bénin, indésirable, de hameçonnage, (nom de)fichiers, données, profils et objets. Les options disponibles varient selon le widget.
2	**Graphique**	Les options d'affichage graphique sont treemap, graphique linéaire, graphique à barres horizontales, graphique à aires empilées, graphique à barres empilées et carte. Les options disponibles varient selon le widget et l'interactivité varie selon le type de graphique. Par exemple, le widget Applications utilisant des ports non standard vous permet de choisir entre une treemap et un graphique linéaire. Pour obtenir un affichage détaillé, cliquez sur le graphique. La zone sur laquelle vous cliquez devient un filtre et vous permet de faire un zoom avant et d'afficher des informations plus granulaires sur cette sélection.
3	**Table**	La vue détaillée des données utilisées pour effectuer un rendu du graphique s'affiche dans une table sous le graphique. Vous pouvez cliquer et définir un filtre local ou général pour les éléments de la table. Avec un filtre local le graphique est mis à jour et la table est triée selon ce filtre.

© 2020 Palo Alto Networks, Inc.

		Avec un filtre général, la vue de l'ACC pivote de manière à afficher uniquement les informations spécifiques à votre filtre.
4	**Actions**	Voici les actions disponibles dans la barre de titre d'un widget : • **Agrandir la vue** – Vous permet d'agrandir le widget et de l'afficher dans un espace écran plus large. Dans la vue agrandie, vous pouvez voir d'autres éléments que les dix principaux qui s'affichent dans l'écran du widget par défaut. • **Définir les filtres locaux** – Vous permet d'ajouter des filtres qui précisent l'affichage au sein du widget. Reportez-vous à Utilisation des filtres – Filtres locaux et filtres généraux. • **Accéder aux journaux** - Vous permet d'accéder directement aux journaux (**Monitor (Surveillance)** > **Logs (Journaux)** > **<log-type> (Type de journal)**). Les journaux sont filtrés selon la période pour laquelle le rendu du graphique est effectué. Si vous avez défini des filtres locaux et généraux, la requête de journal concatène la période et les filtres et affiche uniquement les journaux qui correspondent à votre ensemble de filtres. • **Exporter** : vous permet d'exporter le graphique au format PDF.

Pour une description de chaque widget, reportez-vous aux détails de la section utilisation de l'ACC.

© 2020 Palo Alto Networks, Inc.

Actions de l'ACC

Pour personnaliser et préciser l'affichage de l'ACC, vous pouvez ajouter et supprimer des onglets et des widgets, définir des filtres locaux et généraux, et interagir avec les widgets.

- Utilisation des onglets et des widgets
- Utilisation des filtres – Filtres locaux et filtres généraux

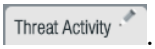
Utilisation des onglets et des widgets

Les options suivantes décrivent comment utiliser et personnaliser les onglets et les widgets.

- Ajout d'un onglet personnalisé.
  1. Sélectionnez Ajouter () dans la liste des onglets.
  2. Ajoutez un **View Name (Nom de vue)**. Ce nom sera utilisé comme nom d'onglet. Vous pouvez ajouter jusqu'à 10 onglets personnalisés.

- Modifier un onglet.

  Sélectionnez l'onglet et cliquez sur Modifier à côté du nom de l'onglet pour le modifier.

  Exemple : 

  .

- Définir l'onglet par défaut
  1. Modifier un onglet.
  2. Sélectionnez  pour définir l'onglet actuel comme valeur par défaut. Chaque fois que vous vous connectez au pare-feu, cet onglet s'affiche.

- Enregistrer l'état de l'onglet
  1. Modifier un onglet.
  2. Sélectionnez  pour enregistrer vos préférences dans l'onglet actuel en tant que valeurs par défaut.

     L'état de l'onglet, y compris les filtres que vous auriez pu configurer, est synchronisé entre les paires HD.

- Exporter un onglet
  1. Modifier un onglet.
  2. Sélectionnez  pour exporter l'onglet actuel. L'onglet se télécharge sur votre ordinateur en tant que fichier .txt. Vous devez activer les fenêtres contextuelles pour télécharger le fichier.

- Importer un onglet
  1. Ajout d'un onglet personnalisé.
  2. Sélectionnez  pour importer un onglet.
  3. Recherchez le fichier texte (.txt) et sélectionnez-le.

© 2020 Palo Alto Networks, Inc.

- Affichage des widgets inclus dans une vue.
  1. Sélectionnez la vue et cliquez sur Modifier ().
  2. Sélectionnez la liste déroulante **Add Widgets (Ajouter des widgets)** pour revoir les widgets sélectionnés.

- Ajout d'un widget ou d'un groupe de widgets
  1. Ajoutez un nouvel onglet ou modifiez un onglet prédéfini.
  2. Sélectionnez **Add Widget (Ajouter un widget)**, puis cochez la case correspondant au widget que vous souhaitez ajouter. Vous pouvez sélectionner un maximum de 12 widgets.
  3. (Facultatif) Pour créer un modèle à 2 colonnes, sélectionnez **Ajouter un Groupe de widgets**. Vous pouvez faire glisser et déposer des widgets dans l'affichage à deux colonnes. Lorsque vous faites glisser le widget sur le modèle, un espace réservé s'affiche et vous permet de déposer le widget.

     Vous ne pouvez pas nommer de groupe de widgets.

- Supprimer l'onglet, le widget ou le groupe de widgets.
  - Pour supprimer un onglet personnalisé, sélectionnez l'onglet et cliquez sur Supprimer (

).

    Vous ne pouvez pas supprimer d'onglet prédéfini.
  - Pour supprimer un widget ou un groupe de widgets, modifiez l'onglet, puis cliquez sur Supprimer ([X]). Vous ne pouvez pas annuler une suppression.

- Réinitialisation de la vue par défaut

  Dans une vue prédéfinie, telle que la vue **Blocked Activity (Activité bloquée)**, vous pouvez supprimer un ou plusieurs widgets. Si vous souhaitez réinitialiser le modèle pour inclure l'ensemble de widgets par défaut de l'onglet, modifiez l'onglet et cliquez sur **Reset View (Réinitialiser la vue)**.

Utilisation des filtres – Filtres locaux et filtres généraux

Pour accéder aux détails et contrôler avec précision l'affichage de l'ACC, vous pouvez utiliser les filtres.

- **Filtres locaux** - ils sont appliqués à un widget spécifique. Un filtre local vous permet d'interagir avec le graphique et de personnaliser l'affichage de manière à pouvoir accéder aux détails et accéder aux informations que vous souhaitez surveiller sur un widget spécifique. Vous pouvez appliquer un filtre local de deux façons : en cliquant sur un attribut dans le graphique ou la table, ou en sélectionnant l'option **Définir le filtre** dans un widget. **Définir un filtre** vous permet de définir un filtre local persistant au redémarrage.
- **Filtres généraux** - ils sont appliqués à l'ensemble de l'ACC. Un filtre général vous permet de pivoter l'affichage sur les détails qui vous importent le plus et d'exclure les informations sans rapport de l'affichage actif. Par exemple, pour afficher tous les éléments relatifs à un utilisateur et une application spécifiques, vous pouvez appliquer l'adresse IP de l'utilisateur et spécifier l'application pour créer un filtre général qui affiche uniquement les informations qui se rapportent à cet utilisateur et cette application via tous les onglets et les widgets dans l'ACC. Les filtres généraux ne sont pas persistants au cours des connexions.

  Les filtres généraux peuvent être appliqués de trois façons :

© 2020 Palo Alto Networks, Inc.

- **Définir un filtre général à partir d'une table** : sélectionnez un attribut dans la table d'un widget et appliquez-le comme filtre général.
- **Ajouter un filtre widget comme filtre général** – Placez la souris sur l'attribut et cliquez sur l'icône en forme de flèche qui se trouve à droite de l'attribut. Cette option vous permet d'élever un filtre local utilisé dans un widget et d'appliquer l'attribut globalement de sorte que l'affichage de l'ensemble des onglets de l'ACC soit mis à jour.
- **Définition d'un filtre général** : définissez un filtre à l'aide du volet **Global Filters (Filtres généraux)** de l'ACC.

- Définition d'un filtre local.

  Vous pouvez également cliquer sur un attribut dans la table sous le graphique pour l'appliquer comme filtre local.

  1. Sélectionnez un widget et cliquez sur Filtre ( ).
  2. Ajoutez ( ) les filtres que vous souhaitez appliquer.
  3. Cliquez sur **Apply (Appliquer)**. Ces filtres sont persistants au redémarrage.

  Le nombre de filtres locaux appliqués à un widget est indiqué en regard de son nom.

- Définissez un filtre général à partir d'une table.

  Placez la souris sur un attribut d'un tableau et cliquez sur la flèche qui apparaît à droite de l'attribut.

- Définissez un filtre général à l'aide du volet Filtres généraux.

  Ajoutez ( ) les filtres que vous souhaitez appliquer.

- Promotion d'un filtre local comme filtre général
  1. Dans n'importe quelle table d'un widget, sélectionnez un attribut pour le définir comme filtre local.
  2. Pour promouvoir le filtre comme filtre général, placez la souris sur l'attribut et cliquez sur la flèche qui se trouve à droite de l'attribut.

- Supprimez un filtre.

  Cliquez sur Supprimer ( ) pour supprimer un filtre.

  - **Filtres généraux** - Cette option se trouve dans le volet Filtres généraux.
  - **Filtres locaux** - Cliquez sur Filtre ( ) pour faire apparaître la boîte de dialogue Définir les filtres locaux, puis sélectionnez le filtre et supprimez-le.

- Effacez tous les filtres.

  - **Filtres généraux** - **Clear All (Effacer tous)** les filtres généraux.
  - **Filtres locaux** - Sélectionnez un widget et cliquez sur Filtre ( ). Puis cliquez sur **Clear All (Effacer tous)** dans le widget Définir les filtres locaux.

- Refus de filtres.

  Sélectionnez un attribut et Refusez ( ) un filtre.

© 2020 Palo Alto Networks, Inc.

- **Filtres généraux** - Cette option se trouve dans le volet Filtres généraux.
- **Filtres locaux** - Cliquez sur Filtre () pour faire apparaître la boîte de dialogue Définir les filtres locaux, ajoutez un filtre, puis refusez-le.

- Affichage des filtres en cours d'utilisation.
  - **Filtres généraux** - Le nombre de filtres généraux appliqués est affiché dans le volet de gauche sous Filtres généraux.
  - **Filtres locaux** - Le nombre de filtres locaux appliqués à un widget est affiché en regard de son nom. Pour afficher les filtres, cliquez sur **Définir les filtres locaux**.

© 2020 Palo Alto Networks, Inc.

surveiller

Les rubriques suivantes décrivent les journaux et les rapports du pare-feu que vous pouvez utiliser pour surveiller l'activité sur votre réseau :

- Surveillance > Journaux
- Surveillance > External Logs
- Surveillance > Moteur de corrélation automatique
- Surveillance > Capture de paquets
- Surveillance > App-Scope
- Surveillance > Navigateur de session
- Surveillance > Liste d'interdiction d'adresses IP
- Surveillance > Botnet
- Surveillance > Rapports au format PDF
- Surveillance > Gérer des rapports personnalisés
- Surveillance > Rapports

© 2020 Palo Alto Networks, Inc.

Surveillance > Journaux

Les rubriques suivantes fournissent des informations supplémentaires sur les journaux de surveillance.

Que voulez-vous savoir ?	Reportez-vous à la section :
Parlez-moi des différents types de journaux.	Types de journaux
Journaux de filtrage. Journaux d'exportation. Afficher les détails des entrées des journaux. Modifier l'affichage des journaux.	Actions des journaux
Vous souhaitez en savoir plus ?	Surveillance et gestion des journaux.

Types de journaux

- **Monitor (Surveillance)** > **Logs (Journaux)**

Le pare-feu affiche tous les journaux afin que les autorisations d'administration basées sur les rôles soient respectées. Seules les informations que vous avez la permission de voir sont visibles, ce qui varie selon les types de journaux que vous visualisez. Pour plus d'informations sur les autorisations d'administrateur, reportez-vous à Périphérique > Rôles administrateur.

Type de journal	Description
Trafic	Affiche une entrée au début et à la fin de chaque session. Chaque entrée contient la date et l'heure, les zones source et de destination, des adresses et des ports, le nom de l'application, le nom de la règle de sécurité appliquée au flux, l'action de la règle (**allow (autoriser)**, **deny (refuser)** ou **drop (supprimer)**), l'interface d'entrée et de sortie, ainsi que le nombre d'octets et le motif de fin de session. La colonne Type indique si l'entrée correspond au début ou à la fin d'une session, ou si la session a été refusée ou supprimée. Une « suppression » indique que la règle de sécurité qui bloquait le trafic a défini « n'importe quelle » application, alors qu'un « refus » indique que la règle a identifié une application spécifique. Si le trafic est supprimé avant d'avoir identifié l'application, comme lorsqu'une règle supprime l'ensemble du trafic d'un service spécifique, l'application affiche « non applicable ». Examinez les journaux du trafic pour obtenir plus de détails sur les entrées et les artefacts : • Cliquez sur Détails ( ) pour afficher des détails supplémentaires concernant une session, à savoir si une entrée

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
	ICMP regroupe plusieurs sessions entre une même source et destination (la valeur **Count (Nombre)** sera supérieure à 1). • Sur un pare-feu doté d'une licence AutoFocus™ active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante ( ) pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact.
Prévention	Affiche une entrée pour chaque alarme de sécurité générée par le pare-feu. Chaque entrée inclut la date et l'heure, le nom ou l'URL d'une menace, les zones sources et de destination, des adresses et des ports, le nom d'une application, le nom de la règle de sécurité appliquée au flux ainsi que l'action de l'alarme (**allow (autoriser)** ou **block (bloquer)**) et sa gravité. La colonne Type indique le type de menace, comme « virus » ou « logiciel espion ». La colonne Nom présente la description de la menace ou l'URL. Quant à la colonne Catégorie, elle correspond à la catégorie de menace (comme « un enregistreur de frappe ») ou la catégorie d'URL. Explorez les journaux des menaces pour obtenir de plus amples détails sur chaque entrée et artefact : • Cliquez sur ( ) pour afficher des détails supplémentaires concernant une menace, à savoir si une entrée regroupe plusieurs menaces du même type entre une même source et destination (la valeur **Count (Nombre)** sera supérieure à 1). • Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante ( ) pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact. • Si les captures de paquets locaux sont activées, cliquez sur Télécharger ( ) pour accéder aux paquets capturés. Pour activer les captures de paquets locaux, reportez-vous aux sous-sections dans **Objects (Objets)** > **Security Profiles (Profils de sécurité)**. • Pour afficher plus de détails à propos d'une menace ou pour configurer rapidement des exemptions de menace directement à partir des journaux de menaces, cliquez sur le nom de la menace dans la colonne **Name (Dénomination)**. La liste des Profils d'exemption affiche tous les profils personnalisés de protection Antivirus, Antispyware et Vulnérabilité. Pour configurer une exemption pour une signature de menace, cochez la case à gauche de la dénomination du profil de sécurité et enregistrez vos modifications. Pour ajouter des exemptions pour des adresses IP (jusqu'à 100 adresses IP par signature), surlignez le profil de sécurité, ajoutez la ou les adresse(s) IP dans la section Adresses IP exemptées et cliquez sur **OK** pour

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
	enregistrer. Pour afficher ou modifier l'exemption, reportez-vous au profil de sécurité associé et cliquez sur l'onglet **Exceptions**. Par exemple, si la menace relève de la catégorie vulnérabilité, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**, cliquez sur le profil associé, puis sur l'onglet **Exceptions**.
Filtrage des URL	Affiche les journaux pour les filtres des URL qui contrôlent l'accès à des sites Web et qui déterminent si les utilisateurs peuvent envoyer des informations d'identification à des sites Web. Sélectionnez Objets > Profils de sécurité > Filtrage des URL pour définir les paramètres de filtrage des URL, y compris les catégories d'URL à bloquer ou à autoriser et pour lesquelles vous souhaitez autoriser ou désactiver l'envoi d'informations d'identification. Vous pouvez également activer la journalisation des options d'en-tête HTTP pour l'URL. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact.
Envois WildFire	Affiche les journaux pour les fichiers et les liens d'e-mails que le pare-feu a transmis pour l'analyse WildFire™. Le cloud WildFire analyse l'échantillon et renvoie les résultats de l'analyse, y compris le verdict WildFire attribué à l'échantillon (bénin, malveillant, grayware ou hameçonnage). Vous pouvez confirmer si le pare-feu a autorisé ou bloqué un fichier en fonction des règles de politique de sécurité en consultant la colonne Actions. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage (dans la colonne Prétraitement des fichiers) contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact.
Filtrage des données	Affiche les journaux des politiques de sécurité ainsi que les profils de filtrage des données, pour empêcher les informations sensibles, comme les numéros de carte de crédit ou de sécurité sociale, de quitter la zone protégée par le pare-feu, et les profils de blocage des fichiers, qui empêchent le chargement ou le téléchargement de certains types de fichiers. Pour configurer la protection par mot de passe pour accéder aux détails d'une entrée de journal, cliquez sur . Saisissez un mot de passe et cliquez sur **OK**. Pour obtenir des instructions sur la modification ou la suppression d'un mot de passe pour la protection des données, reportez-vous à Périphérique > Pages de réponse.

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
	le système vous invite à saisir votre mot de passe une seule fois par session.
Correspondance HIP	Affiche toutes les correspondances HIP que la passerelle GlobalProtect™ identifie lors de la comparaison des données HIP brutes signalées par l'agent aux objets et aux profils HIP définis. Contrairement à d'autres journaux, une correspondance HIP est enregistrée même si elle ne correspond pas à une politique de sécurité. Pour davantage d'informations, reportez-vous à la section Réseau > GlobalProtect > Portails.
GlobalProtect	Affiche les journaux de connexions à GlobalProtect Utilise cette information pour identifier vos utilisateurs GlobalProtect et leur version de système d'exploitation client, résoudre les problèmes de connexion et de performance, ainsi qu'identifier le portail et les passerelles auxquels les utilisateurs se connectent.
Indicateur d'adresse IP	Affiche les informations sur la façon dont une étiquette a été appliquée à une adresse IP particulière et le moment où elle a été appliquée. Utilisez ces informations pour déterminer le moment où une adresse IP particulière a été placé dans un groupe d'adresses, et pourquoi, ainsi que pour déterminer les règles de politique qui influent sur cette adresse. Le journal comprend la réception de l'heure (la date et l'heure d'arrivée du premier et du dernier paquet de la session), le système virtuel, l'adresse IP source, l'étiquette, l'événement, le délai de temporisation, le nom de la source et le type de source.
User-ID™	Affiche des informations concernant les mappages d'adresse IP / nom d'utilisateur, comme la source des informations de mappage, la date à laquelle l'agent User-ID a effectué le mappage et le temps restant avant l'expiration des mappages. Vous pouvez utiliser ces informations pour résoudre les problèmes d'User-ID. Par exemple, si le pare-feu applique la mauvaise règle de politique pour un utilisateur, vous pouvez afficher les journaux pour vérifier si cet utilisateur est mappé à la bonne adresse IP et si les associations de groupe sont correctes.
GTP	Affiche les journaux d'événements comprenant des informations sur la large gamme d'attributs GTP. Ces informations incluent le type d'événement GTP, le type de message d'événement GTP, APN, IMSI, IMEI, l'adresse IP de l'utilisateur final, en plus des informations TCP/IP que le pare-feu de prochaine génération identifie, telles que l'application, la source, l'adresse de destination et l'horodatage.
Inspection des tunnels	Affiche une entrée au début et à la fin de chaque session de tunnel inspecté. Le journal comprend l'Heure de réception (date et heure d'arrivée du premier et du dernier paquet dans la session), ID du tunnel, Balise de suivi, ID de la session, Règle de sécurité appliquée

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
	au trafic du tunnel, etc. Voir Politiques > Inspection des tunnels pour davantage d'informations.
SCTP	Affiche les associations et événements SCTP selon les journaux générés par le pare-feu lors de l'inspection d'état, la validation du protocole et le filtrage du trafic SCTP. Les journaux SCTP comprennent des informations sur la large gamme d'attributs SCTP et de son protocole de charge utile, comme le type d'événement SCTP, le type de bloc, le « cause code, ID Diameter Application, Code de commande Diameter et les blocs. Ces informations SCTP sont fournis en plus des informations générales que le pare-feu identifie, comme l'adresse source et l'adresse de destination, le port source et le port de destination, la règle et l'horodatage. Reportez-vous à la section Objets > Profils de sécurité > Protection SCTP pour obtenir plus d'informations.
Configuration	Affiche une entrée pour chaque modification de la configuration. Chaque entrée inclut la date et l'heure, le nom d'utilisateur de l'administrateur, l'adresse IP correspondant à l'emplacement où la modification a été effectuée, le type de client (interface Web ou CLI), le type de commande exécutée, la réussite ou l'échec de la commande, le chemin de la configuration et les valeurs avant et après la modification.
system	Affiche une entrée pour chaque événement du système. Chaque entrée inclut la date et l'heure, la gravité de l'événement et sa description.
Alarmes	Le journal des alarmes enregistre des informations détaillées sur les alarmes qui sont générées par le système. Les informations figurant dans ce journal sont également indiquées dans Alarmes. Reportez-vous à la section Définir les paramètres d'alarme.
Authentification	Affiche des informations à propos des événements d'authentification qui se produisent lorsque les utilisateurs finaux essaient d'accéder aux ressources du réseau pour lesquelles l'accès est contrôlé par les Règles de la politique d'authentification. Vous pouvez utiliser ces informations pour résoudre les problèmes d'accès et pour adapter votre Politique d'authentification si nécessaire. En parallèle des objets de corrélation, vous pouvez également utiliser les Journaux d'authentification pour identifier les activités suspectes sur votre réseau, telles que les attaques par force brute. Vous pouvez éventuellement configurer les Règles d'authentification sur Délais d'expiration d'authentification du journal. Ces délais d'expiration font référence à la période pendant laquelle un utilisateur doit s'authentifier une seule fois pour une ressource, mais qu'il peut y accéder à plusieurs reprises. Consulter les informations à propos de ces délais d'expiration vous aide à décider s'il est nécessaire de les régler, et comment le faire.

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
	Les journaux système enregistrent les événements d'authentification liés à GlobalProtect et à l'accès administrateur à l'interface Web.
unified	Affiches les plus récentes entrées de journal relatives au trafic, aux menaces, au filtrage des URL, aux envois WildFire et au filtrage des données en une vue unifiée. Cette vue commune des journaux vous permet d'examiner conjointement ces différents types de journaux et de les filtrer (plutôt que de chercher chaque journal séparément). Ou, vous pouvez choisir les types de journaux à afficher : cliquez sur la flèche à gauche du champ de filtrage et sélectionnez **traffic (trafic)**, **threat (menace)**, **URL**, **data (données)** et/ou **wildfire** pour afficher seulement les types de journaux sélectionnés. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante ( ) pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact. Le pare-feu affiche tous les journaux afin que les autorisations d'administration basées sur les rôles soient respectées. Lorsque vous affichez des journaux unifiés, seuls les journaux que vous êtes autorisés à voir sont inclus. Par exemple, un administrateur qui n'est pas autorisé à visualiser les journaux des envois WildFire ne verra pas les entrées des journaux des envois WildFire lorsqu'il visualisera les journaux unifiés. Pour plus d'informations sur les autorisations d'administrateur, reportez-vous à Périphérique > Rôles administrateur. *Vous pouvez utiliser le Jeu de journaux unifié avec le portail de renseignement de menaces AutoFocus. Pour ajouter des filtres de recherche AutoFocus directement dans le champ de filtrage des journaux Unifiés, vous devez Définir une recherche AutoFocus.*

Actions des journaux

Le tableau suivant décrit les actions de journaux.

Action (Action)	Description
Journaux de filtrage	Chaque page du journal dispose d'un champ de filtrage situé en haut de la page. Vous pouvez ajouter des artefacts au champ, comme une adresse IP ou une plage horaire, pour trouver les entrées du journal correspondantes. Les icônes qui se situent à la droite du champ vous permettent d'appliquer, d'effacer, de créer, d'enregistrer et de charger des filtres.

© 2020 Palo Alto Networks, Inc.

Action (Action)	Description
	 • Créer un filtre : • Cliquez sur un artefact d'une entrée de journal pour ajouter cet artefact au filtre. • Cliquez sur **Add (Ajouter)** ( ) pour définir de nouveaux critères de recherche. Pour chaque critère, sélectionnez le **Connector (Connecteur)** qui définit le type de recherche (**and (et)** ou **or (ou)**), l'**Attribute (Attribut)** sur lequel se fonde la recherche, un **Operator (Opérateur)** pour définir la portée de la recherche ainsi qu'une **Value (Valeur)** pour l'évaluation par rapport aux entrées du journal. **Add (Ajoutez)** chaque critère au champ de filtrage et **Close (Fermez)** lorsque vous avez terminé. Vous pouvez ensuite appliquer ( ) le filtre. *Si la chaîne Value (Valeur) correspond à un Operator (Opérateur) (tel que has ou in), entrez la chaîne entre guillemets afin d'éviter une erreur de syntaxe. Par exemple, si vous filtrez par pays de destination et que vous utilisez* ***IN*** *en tant que Value (Valeur) pour préciser INDE, saisissez le filtre en tant que* ***(dstloc eq "IN")****.* *Le filtre des journaux* ***(receive_time in last-60-seconds)*** *entraîne l'augmentation ou la diminution du nombre d'entrées de journal (et de pages de journal) au fil du temps.* • Appliquer les filtres - Cliquez sur Appliquer les filtres ( ) pour afficher les entrées de journal qui correspondent au filtre actuel. • Supprimer les filtres - Cliquez sur Effacer les filtres ( ) pour effacer les valeurs inscrites dans le champ de filtrage. • Enregistrer un filtre - Cliquez sur Enregistrer un filtre ( ), saisissez un nom de filtre, puis cliquez sur **OK**. • Utiliser un filtre enregistré - Cliquez sur Charger un filtre ( ) pour ajouter un filtre enregistré dans le champ de filtrage.
Journaux d'exportation	Cliquez sur Exporter vers un fichier CSV ( ) pour exporter tous les journaux qui correspondent au filtre actuel vers un rapport au format CSV et continuer **Download file (Télécharger le fichier)**. Par défaut, le rapport comprend un maximum de 2 000 lignes de journal. Pour modifier le nombre maximum de lignes des rapports CSV générés, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation et génération de rapports de journaux)** et saisissez une nouvelle valeur **Max Rows in CSV Export (Nombre max. de lignes du rapport d'exportation CSV)**.
Mettre en surbrillance les actions de politique	Sélectionnez pour surligner les entrées des journaux qui correspondent à l'action. Les journaux filtrés sont surlignés dans les couleurs suivantes : • vert – autoriser ; • jaune – continuer ou forcer ; • rouge – refuser, abandonner, abandonner l'ICMP, réinitialiser le client, réinitialiser le serveur, réinitialiser les deux, bloquer-continuer, bloquer le forçage, bloquer l'URL, abandonner tout, entonnoir.

© 2020 Palo Alto Networks, Inc.

Action (Action)	Description
Modifier l'affichage des journaux	Pour personnaliser l'affichage des journaux : • Modifier l'intervalle d'actualisation automatique - Sélectionnez un intervalle dans la liste déroulante des intervalles (**60 seconds (60 secondes)**, **30 seconds (30 secondes)**, **10 seconds (10 secondes)** ou **Manual (Manuel)**). • Modifier le nombre d'entrées affichées par page ainsi que leur ordre de présentation - Les entrées de journaux sont extraites en blocs de 10 par page. • Utilisez les commandes de pagination situées en bas de la page pour naviguer dans la liste du journal. • Pour modifier le nombre d'entrées par page dans le journal, sélectionnez le nombre de lignes dans la liste déroulante Par page (**20**, **30**, **40**, **50**, **75**, ou **100**). • Pour trier les résultats par ordre croissant ou décroissant, utilisez la liste déroulante **ASC (Croissant)** ou **DESC (Décroissant)**. • Résoudre des adresses IP en noms de domaines – Sélectionnez **Resolve Hostname (Résolution du nom d'hôte)** pour commencer à résoudre des adresses IP externes en noms de domaines. • Changer l'ordre de présentation des journaux - Sélectionnez **DESC (Décroissant)** pour afficher les journaux en ordre décroissant, en commençant par les entrées de journaux ayant l'heure de réception la plus récente. Sélectionnez **ASC (Croissant)** pour afficher les journaux en ordre croissant, en commençant par les entrées de journaux ayant l'heure de réception la moins récente.
Afficher les détails des entrées des journaux.	Pour afficher des informations sur les détails des entrées des journaux : • Pour afficher des détails supplémentaires, cliquez sur Détails () d'une entrée. Si la source ou la destination a un mappage d'une adresse IP à un domaine ou à un nom d'utilisateur défini dans la page **Addresses (Adresses)**, ce nom s'affiche à la place de l'adresse IP. Pour afficher l'adresse IP associée, placez votre curseur sur le nom. • Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact.

© 2020 Palo Alto Networks, Inc.

Surveillance > External Logs

Utilisez cette page pour consulter les journaux ingérés depuis Endpoint Security Manager (ESM) de Traps™ vers les collecteurs de journaux gérés par Panorama™. Pour afficher les journaux du Traps ESM sur Panorama, procédez comme suit :

- Sur le serveur Traps ESM, configurez Panorama en tant que serveur Syslog et sélectionnez les événements de journalisation à transférer à Panorama. Les événements peuvent inclure des événements de sécurité ainsi que tout changement apporté à la stratégie, à l'état de l'agent ou du serveur ESM, et aux paramètres de configuration.
- Sur un Panorama déployé en mode Panorama avec un ou plusieurs Collecteurs de journaux gérés, configurez un profil d'ingestion des journaux (Panorama > Profil d'ingestion des journaux) et associez-le à un Groupe de collecteurs (Panorama > Groupes de collecteurs) dans lequel stocker les journaux du Traps ESM.

Les journaux externes ne sont pas associés à un groupe de périphériques et ne sont visibles que lorsque vous sélectionnez **Groupe de périphériques** : **Tous,** car les journaux ne sont pas transférés depuis les pare-feu.

Type de journal	Description
Monitor (Surveillance) > External Logs (Journaux externes) > Traps ESM > Threat (Menace)	Ces événements de menaces comprennent tous les événements de prévention, de notification, les événements provisoires et les événements de post-détection signalés par les agents Traps.
Monitor (Surveillance) > External Logs (Journaux externes) > Traps ESM > System (Système)	Les événements du système de serveur ESM incluent les modifications liées à l'état ESM, aux licences, aux fichiers de Support technique ESM et à la communication avec WildFire.
Monitor (Surveillance) > External Logs (Journaux externes) > Traps ESM > Policy (Politique)	Les événements de changement de politique incluent les modifications apportées aux règles, aux niveaux de protection, aux mises à jour de contenu, aux journaux de contrôle de hachage et aux verdicts.
Monitor (Surveillance) > External Logs (Journaux externes) > Traps ESM > Agent	Les événements de changement d'agent se produisent au niveau du point de terminaison et incluent les modifications apportées aux mises à jour de contenu, aux licences, au logiciel, à l'état de la connexion, aux règles d'actions ponctuelles, aux processus et aux services et aux fichiers mis en quarantaine.
Monitor (Surveillance) > External Logs (Journaux externes) >	Les événements de modification de la configuration ESM incluent les modifications à l'échelle du système pour les licences, les utilisateurs administratifs et les rôles administrateur, les processus, les paramètres de restriction et les conditions.

© 2020 Palo Alto Networks, Inc.

Type de journal	Description
Traps ESM > Config (Configuration)	

Panorama peut mettre en corrélation les événements de sécurité distincts au niveau des points de terminaison avec les événements sur le réseau pour détecter toute activité suspecte ou malveillante entre les points d'extrémité et le pare-feu. Pour afficher les événements mis en corrélation identifiés par Panorama, voir Surveillance > Moteur de corrélation automatique > Événements corrélés.

© 2020 Palo Alto Networks, Inc.

Surveillance > Moteur de corrélation automatique

Le moteur de corrélation automatique suit les modèles sur votre réseau et met en corrélation les événements qui indiquent une hausse des comportements suspects ou des événements représentant une activité malveillante. Le moteur fonctionne comme votre analyste de sécurité personnel qui examine les événements isolés dans les différents ensembles de journaux sur le pare-feu, interroge les données de modèles spécifiques et fait les liens afin de vous fournir des informations exploitables.

Le moteur de corrélation utilise des objets de corrélation qui génèrent des événements corrélés. Les événements corrélés collectent les preuves vous permettant de repérer les similitudes entre des événements réseau apparemment sans rapport et constituent une base de réponse en cas d'incident.

Les modèles suivants prennent en charge le moteur de corrélation automatique :

- Panorama - appareils et appareils virtuels de la série M
- Pare-feu PA-3200 Series
- Pare-feu de la série PA-5200
- Pare-feu PA-7000 Series

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les objets de corrélation ?	Surveillance > Moteur de corrélation automatique > Objets de corrélation
Qu'est-ce qu'un événement corrélé ? Où puis-je voir la preuve de correspondance d'une correspondance de corrélation ?	Surveillance > Moteur de corrélation automatique > Événements corrélés
Comment puis-je obtenir une vue graphique des correspondances de corrélation ?	Reportez-vous au widget Hôtes compromis dans la section ACC.
Vous souhaitez en savoir plus ?	Utilisation du moteur de corrélation automatique

Surveillance > Moteur de corrélation automatique > Objets de corrélation

Pour contrer la progression des méthodes de diffusion de logiciels malveillants et d'attaques, les objets de corrélation étendent les fonctionnalités de détection des logiciels malveillants basées sur les signatures sur le pare-feu. Ils fournissent des renseignements permettant l'identification de modèles de comportement suspect dans les différents ensembles de journaux et rassemblent les preuves requises pour l'examen et répondre rapidement à un événement.

Un objet de corrélation est un fichier de définition qui spécifie les modèles de correspondance, les sources de données à utiliser pour les recherches et la période de recherche de ces modèles. Un modèle est une structure booléenne de conditions qui interrogent les sources de données. Chaque modèle se voit affecté un niveau de gravité et un seuil, qui est le nombre de fois qu'une correspondance au modèle se produit dans

© 2020 Palo Alto Networks, Inc.

un délai imparti. Lorsqu'une correspondance au modèle survient, un événement de corrélation est consigné dans le journal.

Les sources de données utilisées pour effectuer des recherches peuvent inclure les journaux suivant : statistiques d'application, trafic, récapitulatif du trafic, récapitulatif des menaces, menaces, filtrage des données et filtrage des URL. Par exemple, la définition d'un objet de corrélation peut inclure un ensemble de modèles qui recherchent les preuves d'hôtes infectés, de modèles de logiciels malveillants ou de mouvement latéral de logiciels malveillants dans les journaux du trafic, de filtrage des URL et des menaces.

Les objets de corrélation sont définis par Palo Alto Networks® et sont fournis dans les mises à jour de contenu. Vous devez disposer d'une licence de prévention des menaces valide pour obtenir des mises à jour de contenu.

Tous les objets de corrélation sont activés par défaut. Pour désactiver un objet, sélectionnez-le et **Désactivez-le**.

Champs des objets de corrélation	Description
Nom et titre	L'étiquette indique le type d'activité que l'objet de corrélation détecte.
ID	Un nombre unique identifie l'objet de corrélation. Ce nombre se trouve dans la série 6000.
Catégorie	Un récapitulatif du type de menace ou nuisance qui pèse sur le réseau, l'utilisateur ou l'hôte.
État	L'état indique si l'objet de corrélation est activé (actif) ou désactivé (inactif).
Description	La description spécifie les conditions de correspondance pour lesquelles le pare-feu ou Panorama analysera les journaux. Elle décrit le modèle d'escalade ou le chemin de progression qui sera utilisé pour identifier toute activité malveillante ou comportement suspect de l'hôte.

Surveillance > Moteur de corrélation automatique > Événements corrélés

Les événements corrélés étendent les fonctionnalités de détection des menaces sur le pare-feu et Panorama. Ils rassemblent les preuves de comportement suspect ou inhabituel des utilisateurs ou des hôtes sur le réseau.

L'objet de corrélation permet de s'appuyer sur certains comportements ou conditions et de suivre les similitudes entre plusieurs sources de journaux. Lorsque l'ensemble des conditions spécifiées dans un objet de corrélation est observé sur le réseau, chaque correspondance est consignée dans le journal comme événement corrélé.

L'événement corrélé comprend les détails répertoriés dans le tableau suivant.

Champ	Description
Heure de correspondance	L'heure à laquelle l'objet de corrélation a déclenché une correspondance.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Heure de mise à jour	L'horodatage auquel la correspondance a été mise à jour pour la dernière fois.
Nom de l'objet	Le nom de l'objet de corrélation qui a déclenché la correspondance.
Source Address (Adresse source)	L'adresse IP de l'utilisateur d'où provient le trafic.
Source User (Utilisateur source)	Les informations sur l'utilisateur et le groupe d'utilisateurs du serveur d'annuaire, si User-ID™ est activé.
Sévérité	Un indice qui classe le risque en fonction de l'étendue du dommage causé.
Résumé	Une description qui récapitule les preuves rassemblées sur l'événement corrélé.

Pour afficher la vue détaillée du journal, cliquez sur Détails () d'une entrée. La vue détaillée du journal inclut toutes les preuves d'une correspondance :

Onglet	Description
Informations sur la correspondance	**Détails sur l'objet** - présente des informations sur l'objet de corrélation qui a déclenché la correspondance. Pour plus d'informations sur les objets de corrélation, reportez-vous à Surveillance > Moteur de corrélation automatique > Objets de corrélation.
	Détails de la correspondance - Un récapitulatif des détails de la correspondance, notamment l'heure de correspondance, l'heure de la dernière mise à jour selon la preuve de correspondance, le niveau de gravité de l'événement et un récapitulatif des événements.
Preuve de correspondance	Cet onglet inclut toutes les preuves qui corroborent l'événement corrélé. Il affiche des informations détaillées sur les preuves collectées pour chaque session.

L'onglet **Correlated Events (Événements corrélés)** permet de consulter un affichage graphique des informations, et l'onglet **ACC** > **Threat Activity (Activités des menaces)** permet de consulter le widget Hôtes compromis. Dans le widget Hôtes compromis, l'affichage est agrégé par adresse IP et utilisateur source, et trié par niveau de gravité.

Pour configurer les notifications lorsqu'un événement corrélé est consigné dans le journal, accédez à **Device (Périphérique)** > **Log Settings (Paramètres du journal)** ou à l'onglet **Panorama** > **Log Settings (Paramètres du journal)**.

© 2020 Palo Alto Networks, Inc.

Surveillance > Capture de paquets

Tous les pare-feu Palo Alto Networks disposent d'une fonctionnalité intégrée de capture de paquets que vous pouvez utiliser pour capturer des paquets qui traversent les interfaces réseau sur le pare-feu. Vous pouvez ensuite utiliser les données capturées à des fins de dépannage ou pour créer des signatures d'application personnalisées.

La fonctionnalité de capture de paquets est gourmande en ressources processeur et peut réduire les performances du pare-feu. Utilisez uniquement cette fonctionnalité lorsque cela est nécessaire et assurez-vous de la désactiver après avoir collecté les paquets requis.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quelles sont les différentes méthodes que le pare-feu peut utiliser pour capturer des paquets ?	Aperçu de la capture de paquets
Comment puis-je générer une capture de paquets personnalisée ?	Blocs de construction d'une capture de paquets personnalisée
Comment puis-je générer des captures de paquets lorsque le pare-feu détecte une menace ?	Activation de la capture de paquets de menaces
Comment puis-je télécharger une capture de paquets ?	Aperçu de la capture de paquets
Vous souhaitez en savoir plus ?	
• Activez la capture de paquets étendue pour les profils de sécurité.	Périphérique > Configuration > Content-ID
• Utilisez la capture de paquets pour écrire des signatures d'application personnalisées.	Reportez-vous à la section Signatures personnalisées.
• Empêcher un administrateur du pare-feu d'afficher les captures de paquets.	Définir l'accès administrateur à l'interface Web.
• Voir un exemple.	Voir Captures de paquets.

Aperçu de la capture de paquets

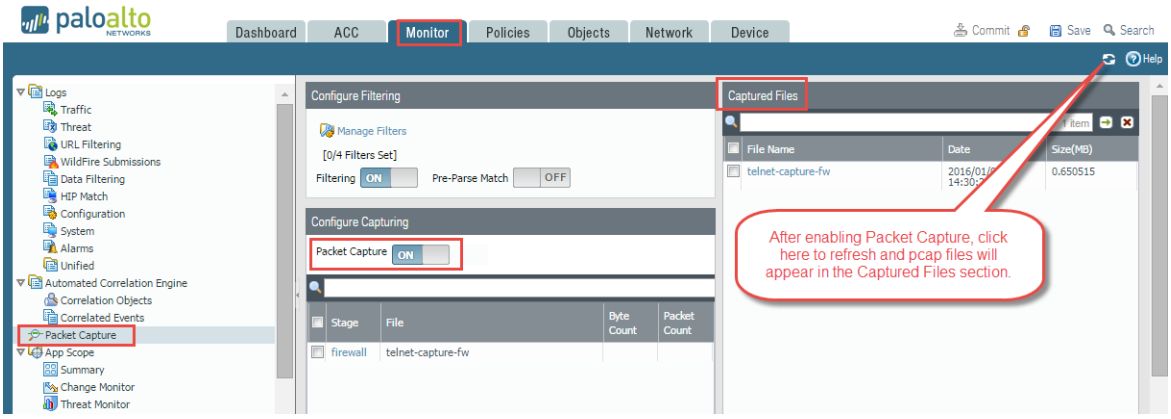
Vous pouvez configurer un pare-feu Palo Alto Networks pour effectuer une capture de paquets personnalisée ou une capture de paquets de menace.

© 2020 Palo Alto Networks, Inc.

- **Capture de paquets personnalisée** - Capturez des paquets pour l'ensemble du trafic ou le trafic en fonction des filtres définis. Par exemple, vous pouvez configurer le pare-feu pour capturer uniquement les paquets depuis et vers une adresse IP source et de destination ou un port spécifique. Utilisez ces captures de paquets pour résoudre les problèmes liés au trafic réseau ou pour collecter les attributs de l'application pour écrire des signatures d'applications personnalisées (**Monitor (Surveillance)** > **Packet Capture (Capture de paquets)**). Définissez le nom de fichier en fonction de l'étape (Supprimer, Pare-feu, Recevoir ou Transmettre). Une fois la capture de paquets terminée, vous pouvez la télécharger dans la section Fichiers capturés.
- **Capture de paquets de menace** - Capturez des paquets lorsque le pare-feu détecte un virus, un logiciel espion ou une vulnérabilité. Vous pouvez activer cette fonctionnalité dans les profils de sécurité Antivirus, Antispyware et Protection contre les vulnérabilités. Ces captures de paquets fournissent le contexte d'une menace qui vous permet de déterminer si une attaque est réussie ou d'en savoir plus sur les méthodes utilisées par une personne malveillante. L'action relative à la menace doit être définie sur Autoriser ou Alerter, sinon la menace est bloquée et les paquets ne peuvent pas être capturés. Vous pouvez configurer ce type de capture de paquets dans **Packet Capture (Objets)** > **Security Profiles (Profils de sécurité)**. Pour télécharger ( ) des captures de paquets, sélectionnez **Monitor (Surveillance)** > **Threat (Menaces)**.

Blocs de construction d'une capture de paquets personnalisée

Le tableau suivant décrit les composants de la page **Monitor (Surveillance)** > **Packet Capture (Capture de paquets)** utilisée pour configurer les captures de paquets, activer la capture de paquets et télécharger les fichiers de capture de paquets.



Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
Gérer les filtres	Configuration du filtrage	Lorsque vous activez la capture de paquets personnalisée, vous pouvez définir des filtres pour capturer uniquement les paquets correspondant à ces filtres. Cela facilitera la localisation d'informations dont vous avez besoin dans les captures de paquets et réduira la puissance de traitement requise par le pare-feu pour effectuer la capture de paquets. Cliquez sur **Add (Ajouter)** pour ajouter un nouveau filtre et configurez les champs suivants :

© 2020 Palo Alto Networks, Inc.

Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
		• **ID** - Saisissez ou sélectionnez un identifiant pour le filtre. • **Ingress Interface (Interface d'entrée)** - Sélectionnez l'interface d'entrée sur laquelle vous souhaitez capturer le trafic. • **Source** - Spécifiez l'adresse IP source du trafic à capturer. • **Destination** - Spécifiez l'adresse IP de destination du trafic à capturer. • **Src Port (Port source)** - Spécifiez le port source du trafic à capturer. • **Dest Port (Port de destination)** - Spécifiez le port de destination du trafic à capturer. • **Proto (Protocole)** - Spécifiez le numéro de protocole de filtrage (1-255). Par exemple, le numéro de protocole d'ICMP est 1. • **Non-IP (Non IP)** - Indiquez la méthode de traitement du trafic non IP (exclure tout le trafic IP, inclure tout le trafic IP, inclure uniquement le trafic IP ou n'inclure aucun filtre IP). Broadcast et AppleTalk sont des exemples de trafic non IP. • **IPv6** - Sélectionnez cette option pour inclure des paquets IPv6 dans le filtre.
Filtrage	Configuration du filtrage	Une fois les filtres définis, définissez le **Filtering (Filtrage)** sur **ON (activé)**. Si le filtrage est **OFF (désactivé)**, l'ensemble du trafic est capturé.
Correspondance avant analyse	Configuration du filtrage	Cette option est à des fins de dépannage avancé. Lorsqu'un paquet arrive au port d'entrée, il passe par plusieurs étapes de traitement avant d'être analysé pour identifier des correspondances par rapport aux filtres préconfigurés. Il est possible qu'un paquet, en raison d'un échec, n'atteigne pas à l'étape de filtrage. Ceci peut se produire, par exemple, lors de l'échec de la recherche d'un itinéraire. Placez le paramètre **Pre-Parse Match (Correspondance avant analyse)** sur **ON (Activé)** afin d'émuler une correspondance positive pour chaque paquet entrant dans le système. Ceci permet au pare-feu de capturer les paquets n'atteignant pas le processus de filtrage. Si un paquet peut arriver à l'étape de filtrage, il est ensuite traité en fonction de la configuration du filtre et supprimé s'il ne répond pas aux critères de filtrage.

© 2020 Palo Alto Networks, Inc.

Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
Capture de paquets	Configuration de la capture	Cliquez sur l'interrupteur à bascule pour **ACTIVER** ou **DÉSACTIVER** la capture de paquets. Vous devez sélectionner au moins une étape de capture. Cliquez sur **Add (Ajouter)** et indiquez les éléments suivants : • **Stage (Étape)** - Indique le point auquel les paquets doivent être capturés : • **drop (supprimer)** - Lorsque le traitement d'un paquet rencontre une erreur et que ce paquet est supprimé. • **firewall (pare-feu)** - Lorsqu'un paquet dispose d'une correspondance de session ou qu'un premier paquet doté est correctement créé avec une session. • **Receive (recevoir)** - Lorsqu'un paquet est reçu sur le processeur du panneau de données. • **transmit (transmettre)** - Lorsqu'un paquet doit être transmis au processeur du panneau de données. • **File (Fichier)** - Indiquez le nom du fichier de capture. Ce nom de fichier doit commencer par une lettre et peut inclure des lettres, des chiffres, des points, des caractères de soulignement ou des traits d'union. • **Packet Count (Nombre de paquets)** - Indiquez le nombre maximum de paquets au-delà desquels la capture s'arrête. • **Byte Count (Nombre d'octets)** – Indiquez le nombre maximum d'octets au-delà desquels la capture s'arrête.
Fichiers capturés	Fichiers capturés	Contient une liste de captures de paquets personnalisées précédemment générées par le pare-feu. Cliquez sur un fichier pour le télécharger sur votre ordinateur. Pour supprimer une capture de paquets, sélectionnez la capture de paquets, puis cliquez sur **Delete (Supprimer)**. • **File Name (Nom de fichier)** - Affiche les fichiers de capture de paquets. Les noms de fichiers sont basés sur le nom de fichier spécifié pour l'étape de capture. • **Date** - Date à laquelle le fichier a été généré. • **Size (MB) (Taille (Mo))** - Taille du fichier de capture. Une fois la capture de paquets activée puis désactivée, vous devez cliquez sur Actualiser ( ) pour afficher

© 2020 Palo Alto Networks, Inc.

Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
		tout nouveau fichier de capture de paquets dans cette liste.
Effacer tous les paramètres	Settings (Paramètres)	Cliquez sur **Clear All Settings (Effacer tous les paramètres)** pour désactiver la capture de paquets et effacer tous les paramètres de capture de paquets.  *Cela ne désactive pas la capture de paquets définie dans un profil de sécurité. Pour plus d'informations sur l'activation de la capture de paquets dans un profil de sécurité, reportez-vous à la section* Activation de la capture de paquets de menaces*.*

Activation de la capture de paquets de menaces

- Objets > Profils de sécurité

Pour permettre au pare-feu de capturer des paquets lorsqu'il détecte une menace, activez l'option de capture de paquets dans le profil de sécurité.

D'abord, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**, puis modifiez le profil souhaité comme décrit dans le tableau suivant :

Options de capture de paquets dans les Profils de sécurité	Location (Emplacement)
Antivirus	Sélectionnez un profil Antivirus personnalisé et, dans l'onglet **Antivirus**, sélectionnez **Packet Capture (Capture de paquets)**.
Antispyware	Sélectionnez un profil Antispyware personnalisé, cliquez sur l'onglet **DNS Signatures (Signatures DNS)** et, dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** ou **extended-capture (capture étendue)**.
Protection contre les vulnérabilités	Sélectionnez un profil Protection contre les vulnérabilités et, dans l'onglet **Rules (Règles)**, cliquez sur **Add (Ajouter)** pour ajouter une nouvelle règle ou choisissez-en une existante. Puis, cliquez sur la liste déroulante **Packet Capture (Capture de paquets)** et sélectionnez **single-packet (un seul paquet)** ou **extended-capture (capture étendue)**.

 *dans les profils Antispyware et Protection contre les vulnérabilités, vous pouvez également activer la capture de paquets pour les exceptions. Cliquez sur l'onglet Exceptions et, dans la*

© 2020 Palo Alto Networks, Inc.

colonne Capture de paquets d'une signature, cliquez sur la liste déroulante et sélectionnez single-packet (un seul paquet) ou extended-capture (capture étendue).

(Facultatif) Pour définir la longueur d'une capture de paquets de menaces en fonction du nombre de paquets capturés (basé sur un paramètre global), sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** et, dans la section Paramètres Content-ID™, modifiez la **Extended Packet Capture Length (packets) (Longueur de capture de paquets étendue)** (plage comprise entre 1 et 50, valeur par défaut : 5).

Une fois la capture de paquets activée dans un profil de sécurité, vous devez vérifier que celui-ci fait partie d'une règle de sécurité. Pour savoir comment ajouter un profil de sécurité à une règle de sécurité ; reportez-vous à Présentation de la politique de sécurité.

Toutes les fois qu'un pare-feu détecte une menace et que la capture des paquets est activée dans le profil de sécurité, vous pouvez télécharger ( ) ou exporter la capture de paquets.

© 2020 Palo Alto Networks, Inc.

Surveillance > App-Scope

Les rubriques suivantes décrivent les fonctionnalités d'App Scope.

- Aperçu de l'App-Scope
- Rapport récapitulatif App-Scope
- Rapport de surveillance des modifications App-Scope
- Rapport de surveillance des menaces App-Scope
- Rapport de la carte des menaces App-Scope
- Rapport de surveillance du réseau App-Scope
- Rapport de la carte du trafic App-Scope

Aperçu de l'App-Scope

Les rapports'A0;App-Scope fournissent une visibilité graphique des aspects suivants de votre réseau'A0;:

- Modifications au niveau de l'utilisation de l'application et de l'activité des utilisateurs
- Utilisateurs et applications monopolisant la bande passante du réseau
- Menaces du réseau

Les rapports'A0;App Scope vous permettent de voir rapidement si un comportement est inhabituel ou inattendu et d'identifier un comportement problématique'A0;; chaque rapport propose une fenêtre dynamique et personnalisable par l'utilisateur dans le réseau. Ces rapports contiennent des options permettant de sélectionner les données et les plages à afficher. Sur Panorama, vous pouvez également sélectionner la **Data Source (Source de données)** des informations affichées. La source de données par défaut (sur les nouvelles installations Panorama) utilise la base de données locale de Panorama, qui stocke les journaux transférés par les pare-feu gérés ; lors d'une mise à niveau, la source de données par défaut est **Remote Device Data (Données du périphérique distant)** (données du pare-feu géré). Pour afficher une vue agrégée des données directement depuis les périphériques gérés, vous devez faire basculer la source de **Panorama** sur **Données du périphérique distant**.

Pointez la souris et cliquez sur les lignes ou les barres des diagrammes pour accéder à l'ACC et afficher des informations détaillées sur l'application, la catégorie d'application, l'utilisateur ou la source spécifique.

Diagrammes du centre de commande de l'application	Description
Résumé	Rapport récapitulatif App-Scope
Surveillance des modifications	Rapport de surveillance des modifications App-Scope
Utilitaire de surveillance des menaces	Rapport de surveillance des menaces App-Scope
Carte des menaces	Rapport de la carte des menaces App-Scope
Surveillance réseau	Rapport de surveillance du réseau App-Scope
Carte du trafic	Rapport de la carte du trafic App-Scope

© 2020 Palo Alto Networks, Inc.

Rapport récapitulatif App-Scope

Le rapport récapitulatif affiche les diagrammes des cinq applications, catégories d'applications, utilisateurs et sources obtenant, perdant et consommant le plus de bande passante.

Pour exporter les diagrammes dans le rapport récapitulatif au format PDF, cliquez sur **Export (Exporter)** (Export:). Chaque diagramme est enregistré sous forme de page du fichier'A0;PDF.

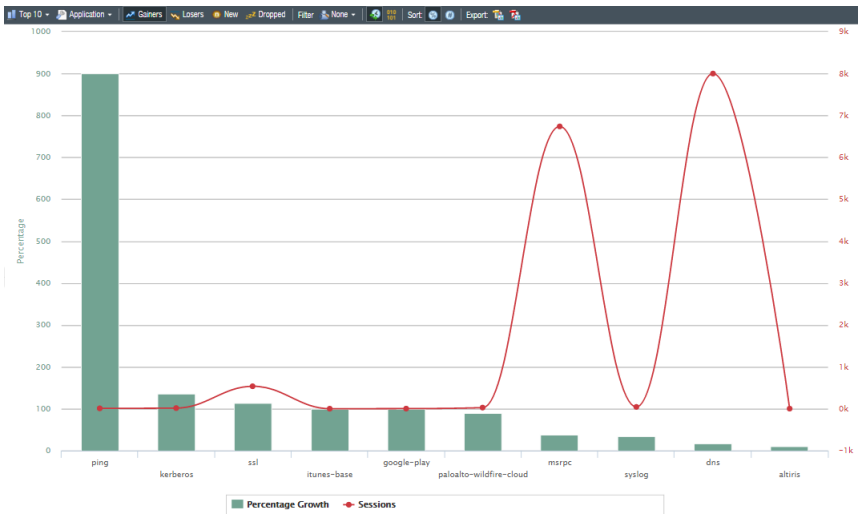
Rapport récapitulatif App-Scope



Rapport de surveillance des modifications App-Scope

Le rapport de surveillance des modifications affiche les modifications effectuées au cours d'une période définie. Par exemple, le diagramme ci-dessous affiche les applications les plus utilisées au cours de la dernière heure par rapport à la dernière période de 24 heures. Les principales applications sont définies par nombre de sessions et triées par pourcentage.

Rapport de surveillance des modifications App-Scope



Ce rapport contient les options suivantes.

© 2020 Palo Alto Networks, Inc.

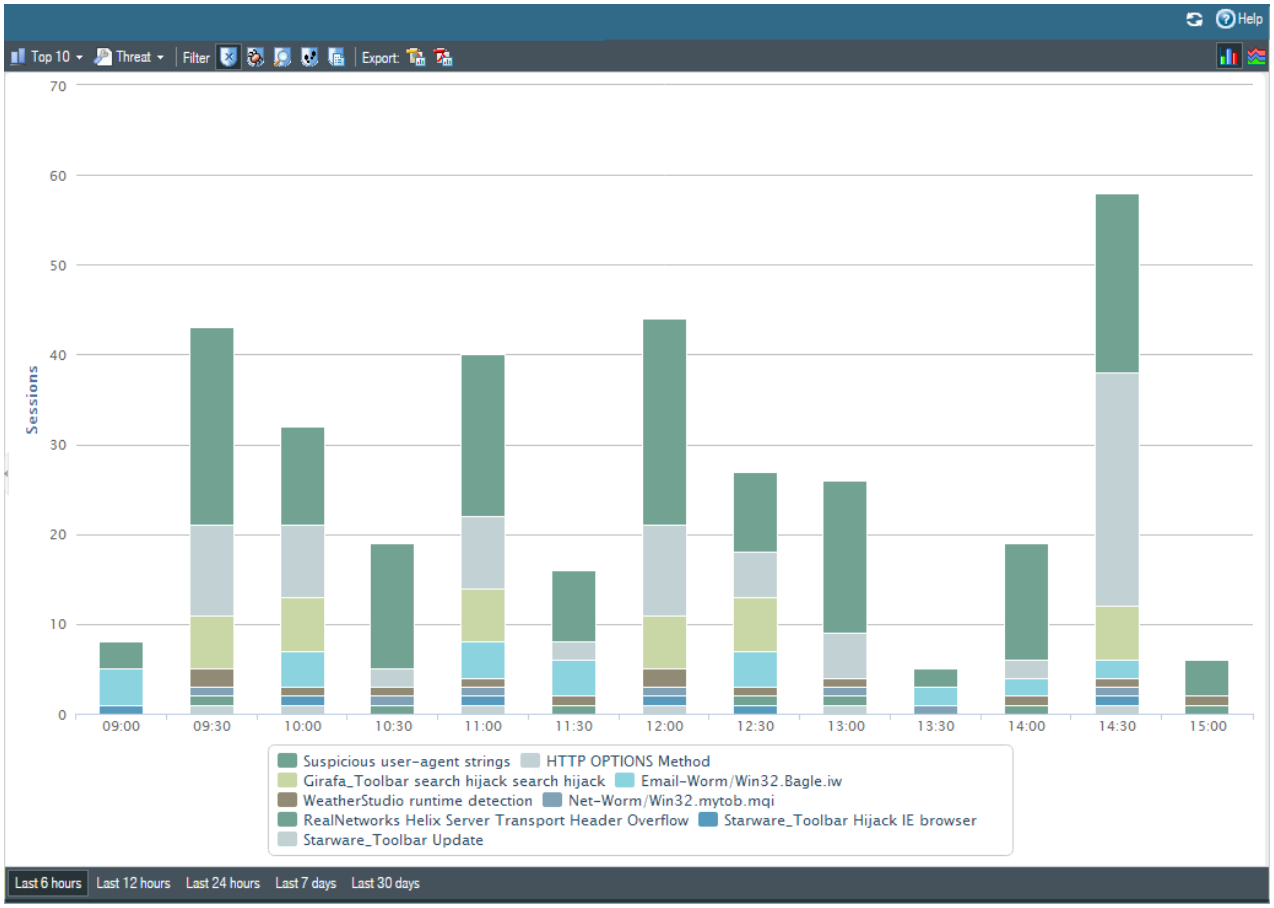
Options du rapport de surveillance des modifications	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Application	Détermine le type d'élément signalé : application, catégorie d'applications, source ou destination.
Gagnants	Affiche les mesures des éléments dont le nombre a augmenté au cours de la période évaluée.
Perdants	Affiche les mesures des éléments dont le nombre a baissé au cours de la période évaluée.
Nouveau	Affiche les mesures des éléments ajoutés au cours de la période évaluée.
Dropped	Affiche les mesures des éléments abandonnés au cours de la période évaluée.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné. Aucun affiche toutes les entrées.
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.
Trier	Indique si des entrées doivent être triées par pourcentage ou par croissance brute.
Export (Exporter)	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
Comparer (intervalle)	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

Rapport de surveillance des menaces App-Scope

Le rapport de surveillance des menaces affiche le nombre de menaces principales identifiées au cours de la période sélectionnée. Par exemple, la figure ci-dessous affiche les 10 types de menaces principales rencontrées au cours des 6 dernières heures.

Rapport de surveillance des menaces App-Scope

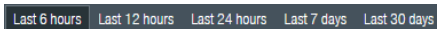
© 2020 Palo Alto Networks, Inc.



Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Ce rapport contient les options suivantes.

Options du rapport de surveillance des menaces	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Prévention	Détermine le type d'élément mesuré : menace, catégorie de menaces, source ou destination.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné.
	Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées.
Export (Exporter)	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	

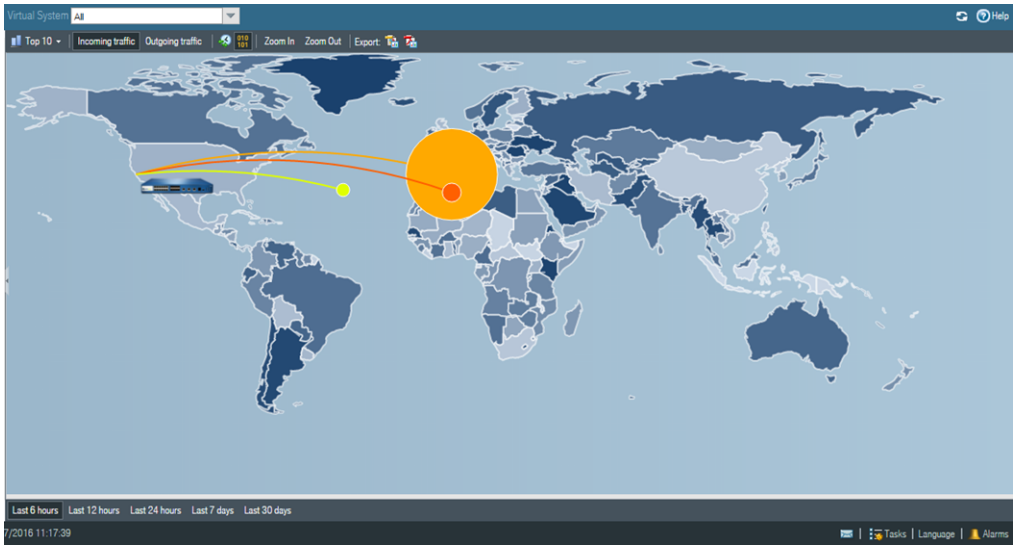
© 2020 Palo Alto Networks, Inc.

Options du rapport de surveillance des menaces	Description
	Indique la période au bout de laquelle des mesures sont réalisées.

Rapport de la carte des menaces App-Scope

Le rapport de la carte des menaces affiche une vue géographique des menaces, ainsi que leur gravité.

Rapport de la carte des menaces App-Scope



Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Cliquez sur un pays de la carte pour faire un **Zoom In (Zoom avant)**, puis un **Zoom Out (Zoom arrière)**, au besoin. Ce rapport contient les options suivantes.

Options du rapport de la carte des menaces	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Menaces entrantes	Affiche les menaces entrantes.
Menaces sortantes	Affiche les menaces sortantes.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné.
Zoom avant et zoom arrière	Zoom avant et zoom arrière de la carte.
Export (Exporter)	Exporte le graphique sous forme d'image .png ou au format PDF.

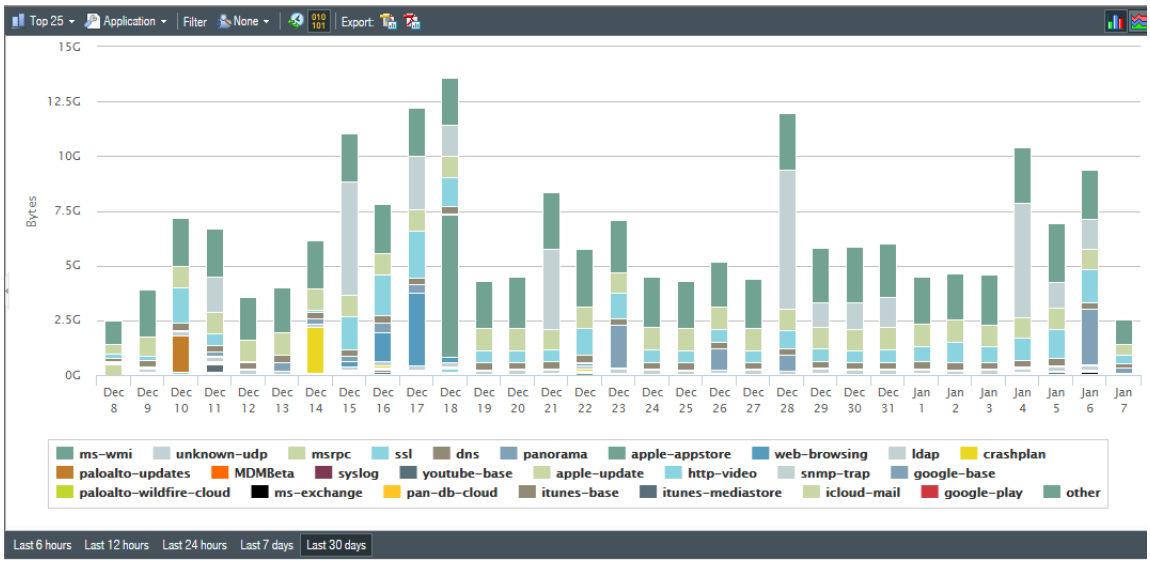
© 2020 Palo Alto Networks, Inc.

Options du rapport de la carte des menaces	Description
Barre du bas	
	Indique la période au bout de laquelle des mesures sont réalisées.

Rapport de surveillance du réseau App-Scope

Le rapport de surveillance du réseau affiche la bande passante dédiée aux différentes fonctions réseau au cours d'une période définie. Chacune de ces fonctions est représentée par une couleur, comme indiqué dans la légende située sous le diagramme. Par exemple, l'image ci-dessous montre la bande passante de l'application au cours des 7 derniers jours et se base sur des informations de session.

Rapport de surveillance du réseau App-Scope



Ce rapport contient les options suivantes.

Options du rapport de surveillance du réseau	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Application	Détermine le type d'élément signalé : application, catégorie d'applications, source ou destination.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné. **None (Aucun)** affiche toutes les entrées.
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.

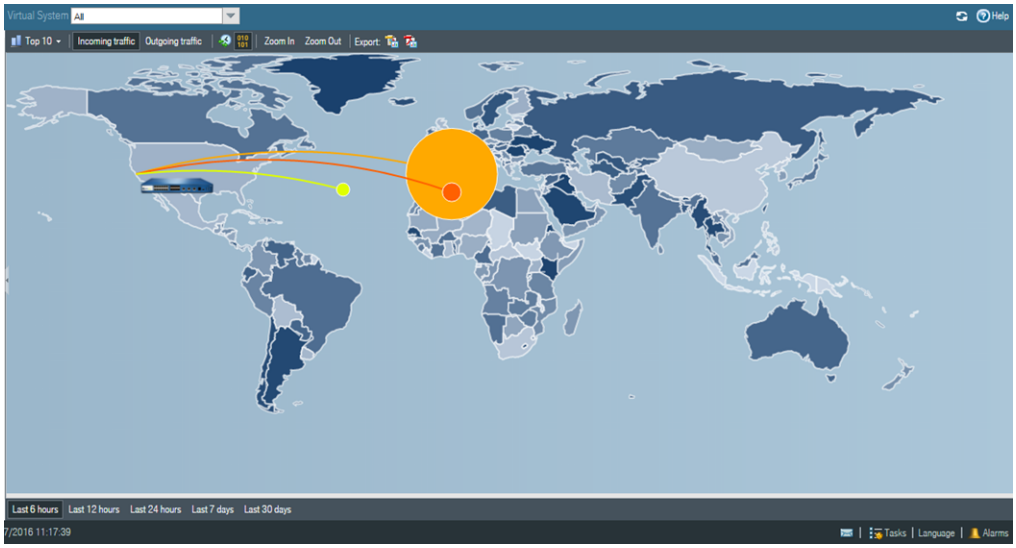
© 2020 Palo Alto Networks, Inc.

Options du rapport de surveillance du réseau	Description
	Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées.
Export (Exporter)	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

Rapport de la carte du trafic App-Scope

Le rapport de la carte du trafic affiche une vue géographique des flux de trafic en fonction des sessions ou des flux.

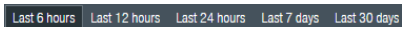
Rapport de la carte du trafic App-Scope



Chaque type de trafic est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Ce rapport contient les options suivantes.

Options du Rapport de la carte du trafic	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Trafic entrant	Affiche le trafic entrant.
Trafic sortant	Affiche le trafic sortant.

© 2020 Palo Alto Networks, Inc.

Options du Rapport de la carte du trafic	Description
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.
Zoom avant et zoom arrière	Zoom avant et zoom arrière de la carte.
Export (Exporter)	Exporte le graphique sous forme d’image .png ou au format PDF.
Barre du bas	
	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

© 2020 Palo Alto Networks, Inc.

Surveillance > Navigateur de session

Sélectionnez **Monitor (Surveillance)** > **Session Browser (Navigateur de session)** pour parcourir et filtrer les sessions en cours d'exécution sur le pare-feu. Pour plus d'informations sur les options de filtrage pour cette page, reportez-vous à la section Actions des journaux.

© 2020 Palo Alto Networks, Inc.

Surveillance > Liste d'interdiction d'adresses IP

Il existe plusieurs façons de configurer le pare-feu pour placer des adresses IP sur la liste d'interdictions, y compris les méthodes suivantes :

- Configurez une règle de politique de Protection DoS avec l'action **Protéger**, puis appliquez un profil de Protection DoS classé à cette règle. Le profil comprend la durée du blocage.
- Configurez une règle de politique de sécurité avec un profil de protection contre les vulnérabilités qui utilise une règle avec l'action **Bloquer IP**, puis appliquez la règle à une zone.

La liste d'interdiction d'adresses IP est prise en charge sur les pare-feux PA-3200 Series, PA-5200 Series et PA-7000 Series.

Que voulez-vous savoir ?	Reportez-vous à la section :
Que signifient les champs Liste d'interdiction d'adresses IP ?	Entrées de la liste d'interdiction d'adresses IP
Comment puis-je filtrer, naviguer ou supprimer les entrées de la liste d'interdiction d'adresses IP ?	Afficher ou supprimer les entrées de la liste d'interdiction d'adresses IP
Vous souhaitez en savoir plus ?	Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités Protection DoS contre la saturation de nouvelles sessions Surveiller les adresses IP bloquées

Entrées de la liste d'interdiction d'adresses IP

- **Surveiller** > **la liste d'interdiction d'adresses IP**

Le tableau suivant explique l'entrée de la liste d'interdiction pour une adresse IP source bloquée par le pare-feu.

Champ	Description
Délai de blocage	Mois/jour et heures:minutes:secondes lorsque l'adresse IP est placée dans la liste d'interdiction d'adresses IP.
Type	Type d'action de blocage : indique si le matériel (hw) ou le logiciel (sw) ont bloqué l'adresse IP. Lorsque vous configurez une politique de Protection DoS ou une politique de Sécurité qui utilise un profil de Protection contre les vulnérabilités pour bloquer les connexions à partir d'adresses sources IPv4, le pare-feu bloque automatiquement ce trafic dans le matériel avant que ces paquets n'utilisent des ressources du processeur ou de la mémoire tampon des paquets. Si le trafic d'attaque dépasse la capacité de blocage du matériel, le pare-feu utilise un logiciel pour bloquer le trafic.
Adresse IP source	Adresse IP source du paquet bloqué par le pare-feu.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Zone d'entrée	Zone de sécurité affectée à l'interface sur laquelle le paquet traverse le pare-feu.
Temps restant	Nombre de secondes restantes pour que l'adresse IP se retrouve sur la liste d'interdiction d'adresses IP.
Bloquer la source	Nom du profil de Protection DoS classé ou nom de l'objet de Protection contre les vulnérabilités sur lesquels vous avez indiqué l'action de blocage d'adresses IP.
Nombre total d'adresses IP bloquées : x sur un total de y (z % utilisés)	Nombre d'adresses IP bloquées (x) sur le nombre d'adresses IP bloquées prises en charge par le pare-feu (y) et le pourcentage correspondant d'adresses IP bloquées utilisé (z).

Afficher ou supprimer les entrées de la liste d'interdiction d'adresses IP

Accédez aux entrées de la liste d'interdiction d'adresses IP, visualisez les informations détaillées et supprimez une entrée si vous le souhaitez.

Afficher ou supprimer les entrées de la liste d'interdiction d'adresses IP	
Rechercher des informations spécifiques concernant la liste d'interdiction d'adresses IP	Sélectionnez une valeur dans une colonne, qui entre dans un filtre dans le champ **Filtres**, puis cliquez sur la flèche de droite pour initier la recherche d'entrées avec cette valeur. Cliquez sur le « X » pour supprimer un filtre.
Afficher les entrées de la liste d'interdiction d'adresses IP au-delà de l'écran actuel	Saisissez un numéro de page dans le champ **Page** ou cliquez sur les flèches simples pour afficher la Page suivante ou la Page précédente des entrées. Cliquez sur les flèches doubles pour afficher la Dernière page ou la Première page des entrées.
Afficher des informations détaillées sur une adresse IP de la liste d'interdiction d'adresses IP	Cliquez sur une Adresse IP source d'une entrée qui relie les Solutions réseau WhoIs avec des informations concernant l'adresse.
Supprimer les entrées de la liste d'interdiction d'adresses IP	Sélectionnez une entrée et cliquez sur **Supprimer**. *Uniquement la suppression d'entrées matérielles est prise en charge par l'interface web. Cependant, la suppression d'entrées matérielles et logicielles est prise en charge par la CLI.*

© 2020 Palo Alto Networks, Inc.

Afficher ou supprimer les entrées de la liste d'interdiction d'adresses IP	
Effacer toute la liste d'interdiction d'adresses IP	Cliquez sur **Effacer tout** pour supprimer définitivement toutes les entrées, ce qui signifie que ces paquets ne sont plus bloqués. *Uniquement la suppression de la liste d'adresses IP bloquées des entrées matérielles est prise en charge par l'interface web. Cependant, la suppression de la liste d'adresses IP bloquées des entrées matérielles et logicielles est prise en charge par la CLI.*

© 2020 Palo Alto Networks, Inc.

Surveillance > Botnet

Le rapport du Botnet vous permet d'utiliser des mécanismes comportementaux pour identifier d'éventuels hôtes infectés par un Botnet dans votre réseau. Le rapport attribue à chaque hôte une note de confiance de 1 à 5 pour indiquer la probabilité d'une infection par un Botnet ; une note de 5 correspond à la plus grande probabilité. Avant de programmer l'exécution du rapport ou de l'exécuter à la demande, vous devez le configurer pour identifier les types de trafic qui sont suspects. Le Guide de l'administrateur PAN-OS® fournit des détails sur l'Interprétation du résultat du rapport du Botnet.

- Paramètres d'un rapport du Botnet
- Paramètres de configuration d'un Botnet

Paramètres d'un rapport du Botnet

- Surveillance > Botnet > Paramètre du rapport

Avant de générer le rapport du Botnet, vous devez préciser les types du trafic qui peuvent indiquer l'activité d'un Botnet (reportez-vous à la section Configuration des rapports du Botnet). Pour programmer un rapport quotidien ou pour l'exécuter sur demande, cliquez sur **Report Setting (Paramètre du rapport)** et remplissez les champs suivants. Pour exporter un rapport, sélectionnez le rapport et**Exporter au format PDF**, **Exporter vers un fichier CSV** ou **Exporter au format XML**.

Paramètres d'un rapport du Botnet	Description
Délai d'exécution du test	Sélectionnez un délai pour le rapport - **Dernière 24 heures** (par défaut) or **Dernier jour calendaire**.
Lancer l'exécution	Cliquez sur **Run Now (Lancer l'exécution)** pour générer un rapport manuellement et immédiatement. Le rapport s'affiche dans un nouvel onglet de la boîte de dialogue du rapport Botnet.
Nbre de rangées	Indiquez le nombre de lignes à afficher dans le rapport (valeur par défaut : 100).
Planifié	Sélectionnez cette option pour générer automatiquement le rapport tous les jours. Cette option est activée par défaut.
Générateur de requêtes	(Facultatif) **Add (Ajoutez)** des requêtes au Générateur de requêtes pour filtrer les résultats du rapport par attributs tels que les adresses IP source / de destination, les utilisateurs ou les zones. Par exemple, si vous savez que le trafic ayant été initié à partir de l'adresse IP 192.0.2.0 ne possède aucun risque d'activité d'un Botnet, vous pouvez ajouter `not (addr.src in 192.0.2.0)` en tant que requête pour exclure cet hôte des résultats du rapport. • **Connector (Connecteur)** - Sélectionnez un connecteur logique (**and (et)** ou **or (ou)**). Si vous avez sélectionné **Negate (Ignorer)**, le rapport exclura les hôtes indiqués dans la requête. • **Attribute (Attribut)** - Sélectionnez une zone, une adresse ou un utilisateur qui est associé aux hôtes que le pare-feu évalue afin de détecter une activité du Botnet.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un rapport du Botnet	Description
	• **Operator (Opérateur)** - Sélectionnez un opérateur pour lier l'**Attribute (Attribut)** à une **Value (Valeur)**. • **Value (Valeur)** - Saisissez une valeur à faire correspondre avec la requête.

Paramètres de configuration d’un Botnet

- Surveillance > Botnet > Configuration

Pour préciser les types de trafic qui indiquent un risque d'activité d'un Botnet, cliquez sur **Configuration** du côté droit de la page **Botnet** et renseignez les champs suivants. Après avoir configuré le rapport, vous pouvez l’exécuter sur demande ou le programmer pour qu’il s’exécute quotidiennement (voir Surveillance > Rapports au format PDF > Gestion des rapports récapitulatifs au format PDF).

La configuration du rapport Botnet par défaut est optimale. Si vous croyez que les valeurs par défaut identifient des faux positifs, créez un billet d’assistance, pour que Palo Alto Networks puisse réévaluer les valeurs.

Paramètres de configuration d’un Botnet	Description
Trafic HTTP	Cliquez sur **Enable (Activer)** et définissez la valeur **Count (Nombre)** de chacun des types de trafic HTTP que le rapport doit inclure. Les valeurs **Count (Nombre)** que vous saisissez représentent le nombre minimum d'événements pour chaque type de trafic qui doivent survenir pour que l'hôte qui y est associé obtienne une note de confiance plus élevée dans le rapport (plus grand risque d'infection par un Botnet). Si le nombre d’événements est inférieur au **Nombre**, le rapport indiquera la note de confiance la plus basse ou (pour certains types de trafic) n’affichera pas d’entrée pour l’hôte. • **Malware URL visit (Visite de l'URL d'un site malveillant)** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Identifie les utilisateurs communiquant avec des URL de sites malveillants connus en fonction des catégories de filtrage des URL du Botnet et des sites malveillants. • **Use of dynamic DNS (Utilisation d'un DNS dynamique)** (intervalle compris entre 2 et1000 ; valeur par défaut : 5) - Recherche le trafic d'une requête DNS dynamique pouvant indiquer la présence d'un logiciel malveillant, de communications avec un Botnet ou de kits d'attaques. Il est généralement très risqué d'utiliser des domaines DNS dynamiques. Les logiciels malveillants se servent souvent des domaines DNS dynamiques pour éviter d'être mis sur une liste noire d'adresses IP. Envisagez d’utiliser le Filtrage des URL pour bloquer ce type de trafic. • **Browsing to IP domains (Navigation dans des domaines IP)** (intervalle compris entre 2 et 1000 ; valeur par défaut : 10) - Identifie les utilisateurs qui naviguent dans des domaines IP au lieu d'adresses URL. • **Browsing to recently registered domains (Navigation dans des domaines récemment enregistrés)** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Recherche du trafic dans les domaines ayant été enregistrés au cours des 30 derniers jours. Les pirates, les logiciels

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration d'un Botnet	Description
	malveillants et les kits d'attaques utilisent fréquemment les domaines nouvellement enregistrés. • **Executable files from unknown sites (Fichiers exécutables provenant de sites inconnus)** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Identifie les fichiers exécutables téléchargés à partir d'URL inconnues. Les fichiers exécutables jouent un rôle dans de nombreuses infections et, lorsqu'ils sont combinés à d'autres types de trafic suspect, peuvent vous aider à prioriser les analyses d'hôtes à effectuer.
Applications inconnues	Définissez les seuils permettant de déterminer si le rapport englobera le trafic associé aux applications TCP inconnu et UDP inconnu qui sont suspectes. • **Sessions Per Hour (Sessions par heure)** (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10) - Le rapport présente le trafic des applications ayant un nombre de sessions par heure inférieur ou égal à la valeur précisée. • **Destinations Per Hour (Destinations par heure)** (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10) - Le rapport présente le trafic des applications ayant un nombre de destinations par heure inférieur ou égal à la valeur précisée. • **Minimum Bytes (Nombre minimum d'octets)** (intervalle compris entre 1 et 200 ; valeur par défaut : 50) - Le rapport présente le trafic des applications dont la charge utile est égale ou supérieure à la taille précisée. • **Maximum Bytes (Nombre maximum d'octets)** (intervalle compris entre 1 et 200 ; valeur par défaut : 100) - Le rapport présente le trafic des applications dont la charge utile est égale ou inférieure à la taille précisée.
IRC	Sélectionnez cette option pour inclure le trafic faisant appel aux serveurs IRC.

© 2020 Palo Alto Networks, Inc.

Surveillance > Rapports au format PDF

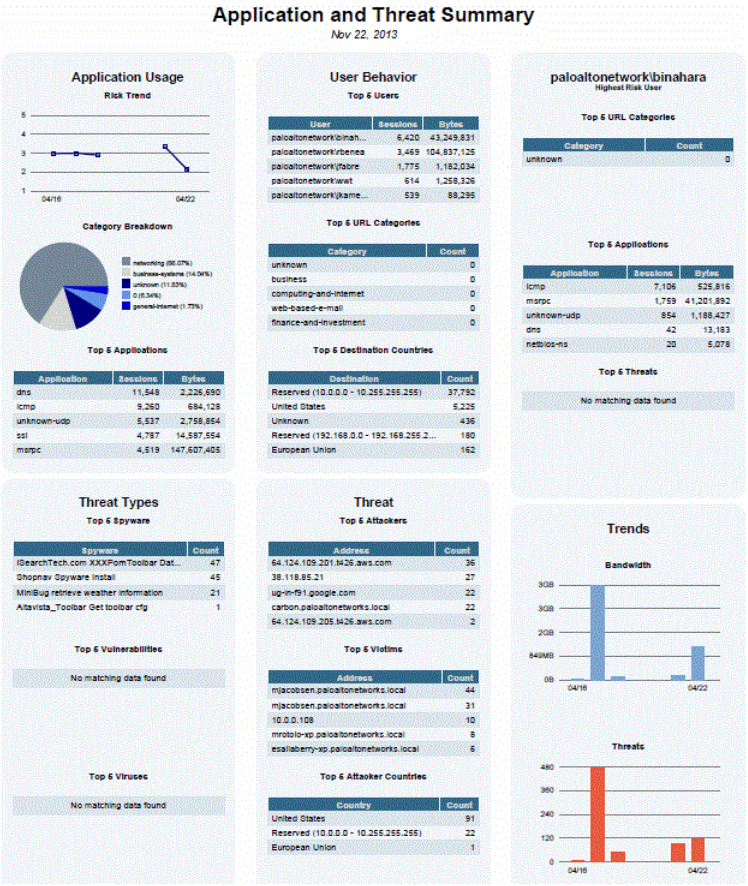
Les rubriques suivantes décrivent les rapports au format PDF.

- Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF
- Surveillance > Rapports au format'A0;PDF > Rapport d'activité des utilisateurs
- Surveillance > Rapports PDF > Utilisation de l'application SaaS
- Surveillance > Rapports au format'A0;PDF > Groupes de rapports
- Surveillance > Rapports au format PDF > Planificateur de courrier électronique

Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF

Les rapports récapitulatifs au format PDF contiennent des informations compilées à partir de rapports existants, en fonction des données figurant dans les 5 meilleurs de chaque catégorie (au lieu des 50 meilleurs). Ils contiennent également des diagrammes de tendance qui ne sont pas disponibles dans les autres rapports.

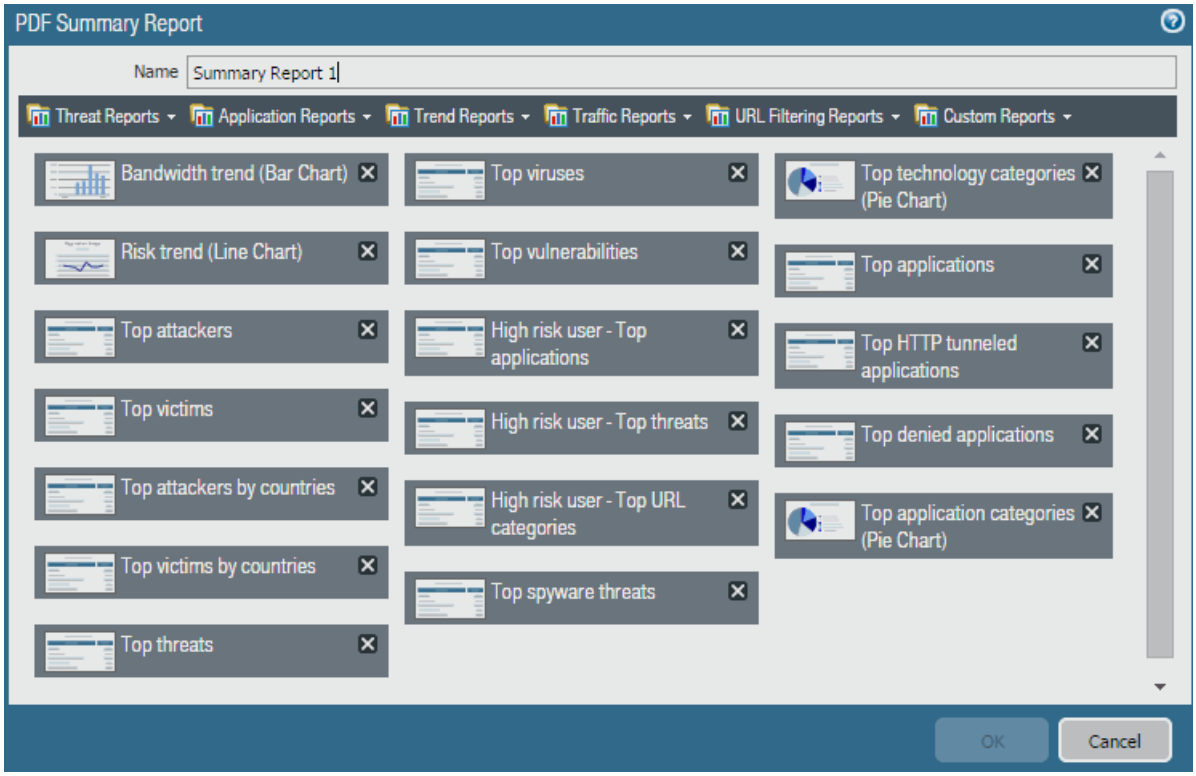
Rapport récapitulatif au format PDF



Pour créer des rapports récapitulatifs au format PDF, cliquez sur **Ajouter**. La page **PDF Summary Report (Rapport récapitulatif au format PDF)** s'ouvre pour afficher tous les éléments disponibles du rapport.

Gestion de rapports au format'A0;PDF

© 2020 Palo Alto Networks, Inc.



Utilisez une ou plusieurs de ces options pour élaborer un rapport :

- Pour supprimer un élément du rapport, cliquez sur Supprimer ([X]) ou désélectionnez l'élément de la liste déroulante pertinente.
- Sélectionnez des éléments supplémentaires dans la liste déroulante pertinente.
- Faites glisser et déposez un élément pour le déplacer vers une autre zone du rapport.

18 éléments de rapport au maximum sont autorisés. Si vous en avez déjà 18, vous devez supprimer certains éléments existants avant de pouvoir en ajouter des nouveaux.

Pour **Enregistrer** le rapport, saisissez un nom de rapport et cliquez sur **OK**.

Pour afficher les rapports PDF, sélectionnez **Monitor (Surveiller)** > **Reports (Rapports)**, cliquez sur **PDF Summary Report (Rapport récapitulatif au format PDF)** pour sélectionner un rapport et cliquez ensuite sur un jour dans le calendrier pour télécharger un rapport pour ce jour-là.

Les nouveaux rapports récapitulatifs au format PDF ne s'affichent qu'après l'exécution du rapport, ce qui se produit automatiquement toutes les 24 heures à 2 heures du matin.

Surveillance > Rapports au format'A0;PDF > Rapport d'activité des utilisateurs

Utilisez cette page pour créer des rapports qui récapitulent l'activité des utilisateurs individuels ou des groupes d'utilisateurs. Cliquez sur **Ajouter** et indiquez les informations suivantes.

© 2020 Palo Alto Networks, Inc.

Paramètres du rapport d'activité des utilisateurs / groupes	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Type	Pour le rapport d'activité des utilisateurs'A0;: sélectionnez **User (Utilisateur)**, puis saisissez l'**Username (Nom d'utilisateur)** ou l'**IP address (Adresse IP)** (IPv4 ou IPv6) de l'utilisateur qui sera le sujet du rapport.
	Pour le rapport d'activité des groupes'A0;: Sélectionnez un **Group (Groupe)** et saisissez le **Group Name (Nom du groupe)**.
Filtres supplémentaires	Sélectionnez **Filter Builder (Générateur de filtre)** pour créer des filtres à appliquer au rapport d'activité des utilisateurs / groupes.
Période de temps	Sélectionnez un délai pour le rapport dans la liste déroulante.
Inclure la navigation détaillée	(Facultatif) Sélectionnez cette option pour inclure pour inclure des journaux des URL détaillés dans le rapport. *les informations relatives à la navigation détaillée peuvent inclure un grand nombre de journaux (des milliers) pour l'utilisateur ou le groupe d'utilisateurs sélectionné et peuvent rendre le rapport très volumineux.*

Le rapport d'activité des groupes n'inclut pas l'option Parcourir le récapitulatif par catégorie d'URL ; toutes les autres informations sont communes aux rapports d'activité des utilisateurs et des groupes.

Pour exécuter le rapport sur demande, cliquez sur **Run Now (Lancer l'exécution)**. Pour modifier le nombre maximum de lignes affichées dans le rapport, reportez-vous à la section Paramètres de journalisation et de génération de rapports.

Pour enregistrer le rapport, cliquez sur **OK**. Vous pouvez ensuite planifier le rapport pour la distribution par courrier électronique (Surveillance > Rapports au format PDF > Planificateur de courrier électronique).

Ajouter un filtre de journal

Générez des filtres de journal à appliquer au rapport d'activité des utilisateurs ou au rapport d'activité des groupes pour personnaliser les rapports. Vous pouvez filtrer les rapports d'activité selon l'application, les caractéristiques d'application, etc. Par exemple, si vous vous intéressez à une application SaaS qui ne possèdent pas de certificats, vous pouvez générer un filtre selon cette caractéristique d'application.

Champ Ajouter un filtre de journal	Description
Zone de texte Filtre de journal	Inscrivez le filtre que vous aimeriez appliquer au journal. Vous pouvez en inscrire plus d'un.
Connecteur	Modifier le filtre pour y ajouter une option de filtrage supplémentaire. Cochez la case **Negate**

© 2020 Palo Alto Networks, Inc.

Champ Ajouter un filtre de journal	Description
	(Refuser) pour ne pas appliquer un filtre de connecteur que vous avez créé.
Attribut	Sélectionnez l'attribut que vous aimeriez ajouter à partir du menu.
Opérateur	Déterminez si l'Attribut doit être égal ou non à la Valeur.
Valeur	Définissez la Valeur de l'attribut. Lorsque possible, un menu déroulant dans lequel figureront des valeurs possibles s'affichera.

Sélectionnez **Apply (Appliquer)** pour appliquer le filtre généré au Rapport d'activités de l'utilisateur ou au Rapport d'activités du groupe.

Surveillance > Rapports PDF > Utilisation de l'application SaaS

Utilisez cette page pour générer un rapport d'utilisation de l'application Saas qui résume les risques de sécurité associés aux applications SaaS qui traversent votre réseau. Ce rapport prédéfini présente une comparaison des applications autorisées et des applications non autorisées, les applications SaaS risquées qui possèdent des caractéristiques d'hébergement défavorables ainsi que l'activité, l'utilisation et la conformité des applications en indiquant les principales applications de chaque catégorie sur les pages détaillées. Vous pouvez utiliser ces informations détaillées sur les risques pour appliquer une politique relative aux applications SaaS que vous souhaitez autoriser ou bloquer sur votre réseau.

Pour générer un rapport informatif et précis, vous devez étiqueter les applications approuvées sur votre réseau (reportez-vous à la section Génération du rapport d'utilisation de l'application SaaS). Le pare-feu et Panorama considère que toute application qui n'est pas dotée d'une telle étiquette prédéfini n'est pas approuvée sur le réseau. Il importe d'être au fait des applications approuvées et des applications non approuvées qui existent sur votre réseau puisque les applications SaaS non approuvées peuvent représenter une menace pour la sécurité de l'information ; elles ne sont pas autorisées à être utilisées sur votre réseau et peuvent entraîner une exposition à des risques ainsi que la perte de données privées et de nature délicate.

Assurez-vous d'étiqueter uniformément les applications sur tous les pare-feu ou les groupes de périphériques. Si la même application est étiquetée comme étant approuvée dans un système virtuel et comme étant non approuvée dans un autre système virtuel ou sur Panorama ou encore si une application n'est pas approuvée dans un groupe de périphériques parent mais qu'elle est approuvée dans un groupe de périphériques enfants (ou l'inverse), le rapport d'utilisation de l'application Saas générera des résultats non concordants.

Sur le ACC, définissez l'Affichage de l'application sur Par état approuvé pour identifier visuellement les applications qui ont un état approuvé différent dans les systèmes virtuels ou les groupes de périphériques. Le vert indique les applications approuvées, le bleu les applications non autorisées et le jaune indique les applications qui ont un état approuvé différent dans différents systèmes virtuels ou groupes de périphériques.

Pour configurer le rapport, cliquez sur **Add (Ajouter)** et indiquez les informations suivantes :

© 2020 Palo Alto Networks, Inc.

Paramètres du rapport d'utilisation de l'application SaaS	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Période de temps	Sélectionnez un délai pour le rapport dans la liste déroulante : **7 derniers jours**, **30 derniers jours** ou **90 derniers jours**. Le rapport comprend les données du jour actuel (le jour où le rapport est généré).
Inclure les journaux à partir de	Dans le menu déroulant, sélectionnez si vous souhaitez générer le rapport sur un groupe d'utilisateurs sélectionné, sur une zone sélectionnée ou pour tous les groupes d'utilisateurs et zones configurés sur le pare-feu ou Panorama. • **Pour un groupe d'utilisateurs sélectionné** – Sélectionnez le **Groupe d'utilisateurs** pour lequel le pare-feu ou Panorama filtrera les journaux. • **Pour une zone sélectionnée** – Sélectionnez la **Zone** pour laquelle le pare-feu ou Panorama filtrera les journaux. • **Pour tous les groupes d'utilisateurs et zones** – Vous pouvez générer des rapports sur tous les groupes ou choisir jusqu'à 25 groupes d'utilisateurs pour lesquels vous souhaitez obtenir une visibilité. Si vous avez plus de 25 groupes, le pare-feu ou Panorama affiche les 25 principaux groupes dans le rapport et affectez tous les groupes d'utilisateurs restants au groupe Autres.
Inclure les informations sur les groupes d'utilisateurs dans le rapport (Non disponible si vous choisissez de générer le rapport sur un **Groupe d'utilisateurs sélectionné**.)	Cette option filtre les journaux pour les groupes d'utilisateurs que vous souhaitez inclure dans le rapport. Sélectionnez le lien **Groupes de gestion** ou les **Groupes de gestion pour la zone sélectionnée** pour choisir jusqu'à 25 groupes d'utilisateurs pour lesquels vous souhaitez obtenir une visibilité. Lorsque vous générez un rapport pour des groupes d'utilisateurs spécifiques sur une zone sélectionnée, les utilisateurs qui ne sont membres d'aucun des groupes sélectionnés sont affectés à un groupe d'utilisateurs appelé Autres.
Groupe d'utilisateurs	Sélectionnez le ou les groupes d'utilisateurs pour lesquels vous souhaitez générer le rapport. Cette option s'affiche uniquement lorsque vous choisissez **Groupe d'utilisateurs sélectionné** dans le menu déroulant **Inclure les journaux à partir de**.
Employé	Sélectionnez la zone pour laquelle vous souhaitez générer le rapport. Cette option s'affiche uniquement lorsque vous choisissez **Zone sélectionnée** dans le menu déroulant **Inclure les journaux à partir de**. Vous pouvez ensuite sélectionner Inclure les informations sur les groupes d'utilisateurs dans le rapport.
Inclut des renseignements détaillés sur les catégories d'application dans le rapport	Le rapport d'utilisation de l'application SaaS au format PDF comprend deux sections. Les deux sections du rapport sont générées par défaut. La première section du rapport (dix pages) porte sur les applications SaaS utilisées sur votre réseau au cours de la période considérée.

© 2020 Palo Alto Networks, Inc.

Paramètres du rapport d'utilisation de l'application SaaS	Description
	Désélectionnez cette options si vous ne voulez pas que la seconde section du rapport comprenne des renseignements détaillés sur les applications SaaS et autres que SaaS pour chacune des sous-catégories d'applications figurant à la première section du rapport. Cette seconde section du rapport englobe les noms des principales applications de chacune des sous-catégories ainsi que des informations sur les utilisateurs, les groupes d'utilisateurs, les fichiers, les octets transférés et les menaces provenant de ces applications. Sans les informations détaillées, le rapport comprend dix pages.
Nombre max. de sous-catégories dans le rapport à	Sélectionnez si vous souhaitez utiliser toutes les sous-catégories d'applications dans le rapport d'Utilisation de l'application SaaS ou si vous souhaitez limiter le nombre maximum de 10, 15, 20 ou 25 sous-catégories. Lorsque vous réduisez le nombre maximum de sous-catégories, le rapport détaillé est plus court, car vous limitez les informations d'activité de l'application SaaS et non-SaaS incluses dans le rapport.

Cliquez sur **Run Now (Exécuter maintenant)** pour générer le rapport sur demande.

Vous pouvez générer ce rapport sur demande ou vous pouvez programmer sa génération quotidienne, hebdomadaire ou mensuelle. Pour programme la génération du rapport, reportez-vous à la section Planifier des rapports pour la livraison par courrier électronique.

Sur les pare-feu PA-220 et PA-220R, le rapport d'utilisation d'application SaaS n'est pas transmis en tant que fichier PDF joint à l'e-mail. L'e-mail contient plutôt un lien qui vous permettra d'ouvrir le rapport dans un navigateur Web.

Pour plus d'informations sur le rapport, consultez la section Gestion de la génération de rapports.

Surveillance > Rapports au format'A0;PDF > Groupes de rapports

Les groupes de rapports vous permettent de créer des ensembles de rapports que le système peut compiler et envoyer sous la forme d'un rapport unique agrégé au format PDF avec une page de titre facultative et tous les rapports constitutifs inclus.

Paramètres du groupe de rapports	Description
Name (Nom)	Donnez un nom au groupe de rapports (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Titre de la page	Sélectionnez cette option pour inclure une page de titre dans le rapport.
Title	Saisissez un nom qui va servir de titre au rapport.
Sélection du rapport / widgets	Pour chaque rapport à inclure dans le groupe, vous devez sélectionner le rapport dans la colonne de gauche et l'**Ajouter** à la colonne de droite. Vous pouvez sélectionner les types de rapports suivants : • Rapport prédéfini

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe de rapports	Description
	• Rapport personnalisé • Rapport récapitulatif au format PDF • Csv • Vue détaillée du journal – Chaque fois que vous créez un rapport personnalisé, le pare-feu crée automatiquement un rapport de Vue détaillée du journal portant le même nom. Le rapport Aperçu du journal affiche les journaux utilisés par le pare-feu pour générer le contenu du rapport personnalisé. Pour inclure les données de la vue détaillée du journal, lors de la création d'un groupe de rapports, ajoutez vos **Rapports personnalisés** puis ajoutez les rapports de **Vue détaillée du journal** correspondants. Le rapport agrégé généré pour le groupe de rapports affiche les données du rapport personnalisé suivies des données de journaux. Après l'enregistrement du groupe de rapports, la colonne Widgets de la page Groupes de rapports répertorie les rapports que vous avez ajoutés au groupe.

Pour utiliser le groupe de rapports, reportez-vous à Surveillance > Rapports au format PDF > Planificateur de courrier électronique.

Surveillance > Rapports au format PDF > Planificateur de courrier électronique

Utilisez le planificateur de courrier électronique pour planifier la distribution de rapports par courrier électronique. Avant d'ajouter un planning, vous devez définir des groupes de rapports et un profil de messagerie. Reportez-vous à Surveillance > Rapports au format PDF > Groupes de rapports et Périphérique > Profils de serveur > E-mail.

L'exécution des rapports planifiés commence à 2h00 et le transfert du courrier électronique s'effectue à la fin de l'exécution de tous les rapports planifiés.

Paramètres du planificateur de courrier électronique	Description
Name (Nom)	Saisissez un nom pour identifier le planning (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Groupe de rapports	Sélectionnez le groupe de rapports (Surveillance > Rapports au format PDF > Groupes de rapports) ou le rapport d'Utilisation de l'application SaaS (Surveillance > Rapports PDF > Utilisation de l'application SaaS) que vous souhaitez planifier.
Profil de messagerie	Sélectionnez le profil qui définit les paramètres de messagerie. Pour plus d'informations sur la définition des profils de messagerie, reportez-vous à Périphérique > Profils de serveur > E-mail.
Récurrence	Sélectionnez la fréquence à laquelle le rapport doit être généré et envoyé.

© 2020 Palo Alto Networks, Inc.

Paramètres du planificateur de courrier électronique	Description
Contrôle prioritaire sur les adresses électroniques	Saisissez une adresse de courrier électronique facultative à utiliser à la place du destinataire défini dans le profil de messagerie.
Envoyer le courrier électronique de test	Cliquez pour envoyer un courrier électronique de test à l'adresse de messagerie définie dans le **Profil de messagerie** sélectionné.

© 2020 Palo Alto Networks, Inc.

Surveillance > Gérer des rapports personnalisés

Vous pouvez créer des rapports personnalisés à exécuter sur demande ou selon la planification (chaque nuit). Pour les rapports prédéfinis, sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.

Une fois que le pare-feu a généré un rapport personnalisé planifié, vous risquez d'invalider les résultats antérieurs du rapport si vous modifiez sa configuration pour changer les résultats ultérieurs. Si vous devez modifier la configuration d'un rapport planifié, il est recommandé de créer un nouveau rapport.

Vous devez **Add (Ajouter)** un rapport personnalisé pour en créer un nouveau. Pour que le rapport se base sur un modèle existant, cliquez sur **Load Template (Charger un modèle)** et sélectionnez le modèle. Pour générer un rapport sur demande, au lieu de ou en plus du moment **Scheduled (Planifié)**, cliquez sur **Run Now (Exécuter maintenant)**. Indiquez les paramètres suivants pour définir un rapport.

Paramètres d'un rapport personnalisé	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description pour le rapport personnalisé.
Base de données	Sélectionnez la base de données à utiliser comme source de données pour le rapport.
Planifié	Sélectionnez cette option pour exécuter le rapport de nuit. Le rapport est rendu accessible en sélectionnant **Monitor (Surveillance)** > **Reports (Rapports)**.
Intervalle de temps	Sélectionnez un délai fixe ou choisissez **Custom (Personnalisé)** et indiquez une date et un délai.
Trier par	Sélectionnez des options de tri afin d'organiser le rapport, y compris la quantité d'informations à y inclure. Les options disponibles dépendent du choix de base de données.
Regrouper par	Sélectionnez des options de regroupement afin d'organiser le rapport, y compris la quantité d'informations à inclure dans le rapport. Les options disponibles dépendent du choix de base de données.
Colonnes	Sélectionnez les colonnes Disponible à inclure dans le rapport personnalisé et ajoutez-les (⊞) aux colonnes Sélectionné. Sélectionnez **Up (Déplacer en haut)**, **Down (Déplacer en bas)**, **Top (Monter)** et **Bottom (Descendre)** pour réorganiser les colonnes sélectionnées. Au besoin, vous pouvez également sélectionner et supprimer (⊟) les colonnes précédemment sélectionnées.

© 2020 Palo Alto Networks, Inc.

Paramètres d’un rapport personnalisé	Description
Générateur de requêtes	Pour générer une requête de rapport, indiquez les options suivantes et cliquez sur **Add (Ajouter)**. Répétez ces différentes étapes, le cas échéant, pour formuler une requête complète. • **Connector (Connecteur)** - Sélectionnez le connecteur (**and (et)** ou **or (ou)**) devant précéder l'expression que vous ajoutez. • **Negate (Refuser)** - Sélectionnez cette option pour interpréter la requête en tant que refus. Dans l'exemple précédent, l'option de refus fait correspondre des entrées qui ne figurent pas dans les dernières 24 heures ou qui ne proviennent pas d'une zone « non sécurisée ». • **Attribute (Attribut)** : sélectionnez un élément de donnée. Les options disponibles dépendent du choix de base de données. • **Operator (Opérateur)** : sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du choix de base de données. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre.

Pour plus d’informations, reportez-vous à la section Génération de rapports personnalisés.

© 2020 Palo Alto Networks, Inc.

Surveillance > Rapports

Le pare-feu fournit plusieurs rapports (les 50 principaux) concernant les statistiques du trafic pour le jour précédent ou un jour sélectionné au cours de la semaine précédente.

Pour afficher un rapport, développez une catégorie de rapport (comme Rapports personnalisés) sur le côté droit de la page et sélectionnez un nom de rapport. La page répertorie les rapports dans les sections. Vous pouvez afficher des informations dans chaque rapport pour la période sélectionnée.

Par défaut, le pare-feu affiche tous les rapports pour le jour calendaire précédent. Pour afficher les rapports d'un autre jour, sélectionnez une date de génération de rapport dans le calendrier dans le coin inférieur droit de la page.

Pour afficher les rapports sur un système autre que le pare-feu, sélectionnez une option d'exportation :

- **Exporter vers un fichier PDF**
- **Exporter vers un fichier CSV**
- **Exporter vers un fichier XML**

© 2020 Palo Alto Networks, Inc.

Politiques

Les rubriques suivantes décrivent les types de stratégie de pare-feu, la manière de déplacer ou cloner des stratégies et ainsi que les paramètres de stratégie :

- Types de politique
- Déplacement ou clonage d'une règle de politique
- Archive des commentaires d'audit
- Requête sur le nombre d'utilisations de la règle
- Politiques > Sécurité
- Politiques > NAT
- Politiques > QoS
- Politiques > Transfert basé sur une politique
- Politiques > Déchiffrement
- Politiques > Inspection des tunnels
- Politiques > Contrôle prioritaire sur l'application
- Politiques > Authentification
- Politiques > Protection'A0;DoS
- Politiques > SD-WAN

© 2020 Palo Alto Networks, Inc.

Types de politique

Les politiques vous permettent de contrôler le fonctionnement du pare-feu en mettant des règles en application et en automatisant des actions. Le pare-feu prend en charge les types de politiques suivantes :

- Les politiques de sécurité de base visant à bloquer ou autoriser une session réseau en fonction de l'application, des zones et adresses source et de destination ou, en option, du service (port et protocole). Les zones identifient les interfaces physiques ou logiques qui envoient ou reçoivent le trafic. Voir Politiques > Sécurité.
- Politiques de traduction des adresses réseau (Network Address Translation, NAT) visant à traduire des adresses et des ports. Voir Politiques > NAT.
- Politiques de qualité du service (QoS) visant à déterminer comment le trafic est classé en vue de son traitement lorsqu'il transite par une interface sur laquelle la QoS est activée. Voir Politiques > QoS.
- Politiques de transfert basé sur une politique visant à appliquer un contrôle prioritaire sur la table de routage et à indiquer une interface de trafic sortant. Voir Politiques > Transfert basé sur une politique (PBF).
- Politiques de déchiffrement visant à déchiffrer le trafic pour les politiques de sécurité. Chaque politique peut définir les catégories d'URL pour le trafic à déchiffrer. Le déchiffrement SSH est utilisé pour identifier et contrôler la tunnellisation SSH en plus de l'accès au shell SSH. Voir Politiques > Déchiffrement.
- Les politiques d'inspection des tunnels pour imposer la sécurité, la Protection DoS et les politiques QoS sur le trafic par tunnel et pour visualiser l'activité du tunnel. Voir Politiques > Inspection des tunnels.
- Politiques de contrôle prioritaire visant à appliquer un contrôle prioritaire sur les définitions d'applications fournies par le pare-feu. Voir Politiques > Contrôle prioritaire sur l'application.
- Les politiques d'authentification pour définir l'authentification pour les utilisateurs finaux qui ont accès aux ressources du réseau. Voir Politiques > Authentification.
- Politiques de déni de service (DoS) visant à assurer une protection contre les attaques'A0;DoS et à prendre des mesures de protection en cas de correspondance des règles. Voir Politiques > Protection DoS.
- Les politiques SD-WAN déterminent la gestion des chemins des liens entre la zone source et la zone de destination lorsque l'état des chemins des liens se dégrade sous le seuil établi par les mesures d'état approuvés et configurés. Voir Politiques > SD-WAN.

Les politiques partagées envoyées depuis Panorama ™ s'affichent en orange sur l'interface Web du pare-feu. Vous pouvez modifier ces politiques partagées uniquement sur Panorama ; vous ne pouvez pas les modifier sur le pare-feu.

Afficher la base de règles en tant que groupes pour afficher tous les groupes d'étiquettes d'une base de règles. Dans les bases de règles disposant de nombreuses règles, afficher la base de règles en tant que groupe simplifie l'affichage en présentant les étiquettes, le code de couleur et le nombre de règles contenu dans chaque groupe tout en préservant la hiérarchie des règles établie.

© 2020 Palo Alto Networks, Inc.

Déplacement ou clonage d'une règle de politique

Lorsque vous déplacez ou clonez des politiques, vous pouvez définir une **Destination** (un système virtuel sur un pare-feu ou un groupe de périphériques sur Panorama) pour laquelle vous disposez d'autorisations d'accès, y compris l'emplacement partagé.

Pour déplacer une règle de politique, sélectionnez-la dans l'onglet **Policies (Politiques)**, cliquez sur **Move (Déplacer)**, sélectionnez **Move to other vsys (Passer à un autre système virtuel)** (pare-feu uniquement) ou **Move to different rulebase or device group (Passer à une autre règle de base ou un autre groupe de périphériques)** (Panorama uniquement), spécifiez les champs dans le tableau suivant et cliquez sur **OK**.

Pour cloner une règle de politique, sélectionnez-la dans l'onglet **Policies (Politiques)**, cliquez sur **Clone (Cloner)**, renseignez les champs du tableau suivant, puis cliquez sur **OK**.

Paramètres de déplacement/ clonage	Description
Règles sélectionnées	Affiche le nom et l'emplacement actuel (système virtuel ou groupe de périphériques) des règles de politique que vous avez sélectionnées pour l'opération.
Destination	Sélectionnez le nouvel emplacement de la politique ou de l'objet : un système virtuel, un groupe de périphériques ou un emplacement partagé. La valeur par défaut est le **Virtual System (Système virtuel)** ou le **Device Group (Groupe de périphériques)** que vous avez sélectionné dans l'onglet **Policies (Politiques)** ou **Objects (Objets)**.
Ordre des règles	Sélectionnez la position de la règle par rapport aux autres règles : • **Move top (Monter)** - La règle va précéder toutes les autres règles. • **Move bottom (Descendre)** - La règle va suivre toutes les autres règles. • **Before rule (Avant la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle suivante. • **After rule (Après la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle précédente.
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option (sélectionnée par défaut) pour que le pare-feu ou Panorama affiche la première erreur trouvée et arrête de rechercher d'autres erreurs. Par exemple, une erreur se produit si la **Destination** ne contient aucun objet référencé dans la règle de la politique que vous déplacez. Si vous désélectionnez cette option, le pare-feu ou Panorama trouvera toutes les erreurs avant de les afficher.

© 2020 Palo Alto Networks, Inc.

Archive des commentaires d'audit

Sélectionnez **Audit Comment Archive (Archive des commentaires d'audit)** pour afficher l'historique des commentaires d'audit, les journaux de configuration et l'historique des changements apportés à une règle de politique sélectionnée.

- Commentaires d'audit
- Journaux de configuration (entre les validations)
- Changements des règles

Commentaires d'audit

Afficher l'historique des **Audit Comment (Commentaires d'audit)**applicable à une règle de politique sélectionnée. Appliquez et enregistrez les filtres pour identifier rapidement des commentaires d'audit spécifiques et pour exporter les commentaires d'audit affichés au format CSV.

Champ	Description
Moment de validation	Moment auquel le commentaire a été validé
Commentaire d'audit	Contenu du commentaire d'audit.
Administrateur	Utilisateur qui a ajouté ou modifié le commentaire d'audit.
Version de la configuration	Version de la révision de configuration. 0 indique la première fois que la règle de politique a été créée et validée dans Panorama.

Journaux de configuration (entre les validations)

Affichez le journal de configuration généré par la règle de politique sélectionnée entre les validations. Appliquez et enregistrez les filtres pour identifier rapidement des journaux de configuration spécifiques et pour exporter les journaux de configuration affichés au format CSV.

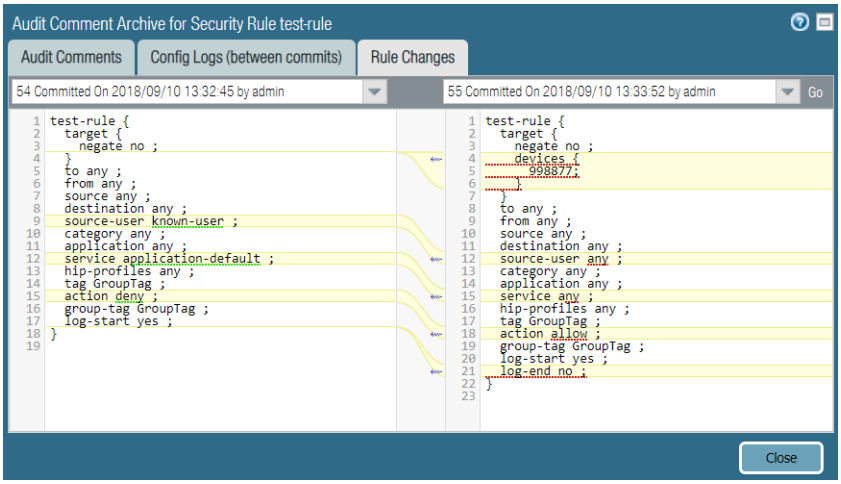
Champ	Description
Période	Moment auquel le commentaire a été validé
Administrateur	Contenu du commentaire d'audit.
Commande	Type de commande exécuté.
Avant les modifications	Informations relatives à la règle avant le changement. Par exemple, si vous renommez une règle, l'ancien nom s'affiche.
Après modification	Informations relatives à la règle après le changement. Par exemple, si vous renommez une règle, le nouveau nom s'affiche.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Nom du périphérique	Nom du périphérique avant la modification des commentaires d'audit.

Changements des règles

Afficher et comparer la version de la configuration de la règle de politique sélectionnée pour analyser les changements qui se sont produits. Dans le menu déroulant, sélectionnez les deux versions de configuration des règles de politique que vous souhaitez comparer.



© 2020 Palo Alto Networks, Inc.

Requête sur le nombre d'utilisations de la règle

- **Policies (Politiques)** > **Rule Usage (Utilisation d'une règle)**

Utilisez la requête sur le nombre d'utilisations de la règle pour filtrer la base de règle sélectionnée sur une période de temps donnée. La requête sur l'utilisation des règles vous permet de filtrer rapidement votre base de règles de politique pour identifier les règles non utilisées à des fins de suppression pour que vous puissiez réduire les points d'entrée ouverts aux pirates. Cliquez sur **PDF/CSV** pour exporter les règles filtrées au format PDF ou CSV. Pour utiliser la requête sur le nombre d'utilisations de la règle, vous devez activer le paramètre **Policy Rule Hit Count (Requête sur le nombre d'utilisation de la règle)** (Périphérique > Configuration > Gestion).

Par défaut, les colonnes **Name (Nom)**, **Location (Emplacement)**, **Created (Créé)**, **Modified (Modifié)** et **Rule Usage (Utilisation de la règle)** s'affichent lorsque vous interrogez l'utilisation de la règle dans votre base de règles de politique. Vous pouvez ajouter plus de colonnes pour afficher des renseignements supplémentaires sur les règles de politique.

Tâche	Description
Nombre de correspondances	
Délai	Indiquez le délai au cours duquel interroger la base de règles sélectionnée. Sélectionnez un délai prédéterminé ou définissez un délai **Custom (Personnalisé)**.
Usage	Sélectionnez l'utilisation de la règle à interroger : **Any (Indifférent)**, **Unused (Non utilisée)**, **Used (Utilisée)** ou **Partially Used (Partiellement utilisée)** (Panorama uniquement).
Depuis	(Délai personnalisé uniquement) Sélectionnez la date et l'heure de l'interrogation de la base de règles de politique.
Exclure la réinitialisation des règles au cours des _ derniers jours	Sélectionnez cette option pour exclure les règles qui ont été manuellement réinitialisées par un utilisateur au cours du nombre de jours indiqués.

Requête sur le nombre d'utilisations de la règle du périphérique

Vous pouvez afficher l'utilisation de la règle du système virtuel et du périphérique lorsque vous affichez l'utilisation de la règle d'une politique de Panorama ou du serveur de gestion. **Reset Rule Hit Counter (Réinitialiser le compteur d'une règle)** pour réinitialiser le nombre de correspondances, la première correspondance et la dernière correspondance.

Cliquez sur **PDF/CSV** pour exporter les règles filtrées au format PDF ou CSV.

Champ	Description
Groupe de périphériques	Le groupe de périphériques auquel le périphérique ou le système virtuel appartient.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Nom de périphérique/ Système virtuel	Nom du groupe de périphériques ou du système virtuel.
Nombre de correspondances	Nombre total de correspondances du trafic à la règle de politique.
Dernière correspondance	Date et heure de la dernière correspondance du trafic à la règle de politique.
Première correspondance	Date et heure de la première correspondance du trafic à la règle de politique.
Dernière mise à jour reçue	Date et heure des dernières informations d'utilisation de la règle reçues du pare-feu ou du serveur de gestion Panorama.
Créé	Date et heure de création de la règle de politique.
Modifié	Date et heure de la dernière modification de la règle de politique. La colonne est vide si la règle de politique n'a pas été modifiée.
État	L'état de la connexion du périphérique : `Connected` ou `Disconnected`.

© 2020 Palo Alto Networks, Inc.

Politiques > Sécurité

Les règles de politiques de sécurité référencent les zones de sécurité et vous permettent d'autoriser, de limiter et de suivre le trafic sur votre réseau en fonction des applications, des utilisateurs ou groupes d'utilisateurs et des services (port et protocole). Par défaut, le pare-feu inclut une règle de sécurité nommée *règle1* qui autorise tout trafic issu d'une zone approuvée vers une zone non approuvée.

Que voulez-vous savoir ?	Reportez-vous à la section :
Qu'est-ce qu'une politique de Sécurité ?	Présentation de la politique de sécurité Pour Panorama, reportez-vous à Déplacer ou cloner une règle de stratégie
Quels sont les champs disponibles pour créer une règle de politique de Sécurité ?	Blocs de construction dans une règle de politique de sécurité
Comment puis-je utiliser l'interface Web pour gérer des règles de politique de Sécurité ?	Création et gestion des politiques Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité Applications et utilisation Optimiseur de la politique de sécurité
Vous souhaitez en savoir plus ?	Politique de Sécurité

Présentation de la politique de sécurité

Les politiques de sécurité vous permettent d'appliquer des règles et d'agir. Elles peuvent être aussi générales ou spécifiques que vous le souhaitez. Les règles des politiques sont comparées au trafic entrant dans un ordre précis, et comme la première règle qui correspond au trafic est appliquée, les règles spécifiques doivent précéder les règles plus générales. Par exemple, une règle correspondant à une application unique doit précéder une règle correspondant à l'ensemble des applications si tous les autres paramètres relatifs au trafic sont identiques.



Pour s'assurer que les utilisateurs finaux s'authentifient lorsqu'ils essaient d'accéder à vos ressources réseau, le pare-feu évalue la politique d'Authentification avant la politique de Sécurité. Pour plus d'informations, voir Politiques > Authentification.

Pour le trafic qui ne correspond à aucune règle définie par l'utilisateur, les règles par défaut s'appliquent. Les règles par défaut, qui s'affichent en bas de la base des règles de sécurité, sont prédéfinies pour autoriser l'ensemble du trafic intra-zone (au sein de la zone) et refuser le trafic inter-zone (entre les zones). Bien que ces règles fassent partie de la configuration prédéfinie et soient en lecture seule par défaut, vous pouvez appliquer un **Override (Contrôle prioritaire)** afin de modifier un nombre limité de paramètres, notamment les étiquettes, l'action (autoriser ou refuser), les paramètres des journaux et les profils de sécurité.

L'interface contient les onglets suivants pour définir les règles de politique de Sécurité.

- **General (Général)** – Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la règle de politique de Sécurité.
- **Source** - Sélectionnez l'onglet **Source** pour définir la zone source ou l'adresse source qui génère le trafic.

© 2020 Palo Alto Networks, Inc.

- **User (Utilisateur)** - Sélectionnez l'onglet **User (Utilisateur)** pour appliquer la politique à des utilisateurs individuels ou à un groupe d'utilisateurs. Si vous utilisez GlobalProtect™ et que l'option profil d'informations sur l'hôte (HIP) est activée, vous pouvez également baser la politique sur les informations collectées par GlobalProtect. Par exemple, le niveau d'accès de l'utilisateur peut être déterminé par un HIP qui indique au pare-feu la configuration locale de l'utilisateur. Les informations HIP peuvent être utilisées pour un contrôle d'accès granulaire basé sur les programmes de sécurité exécutés sur l'hôte, les valeurs du registre et de nombreuses autres vérifications telles que l'installation ou non du logiciel antivirus sur l'hôte.
- **Destination** - Sélectionnez l'onglet **Destination** pour définir la zone de destination ou l'adresse de destination du trafic.
- **Application** – Sélectionnez l'onglet **Application** pour définir l'action de la politique en fonction d'une application ou d'un groupe d'applications. Un administrateur peut également utiliser une signature App-ID™ existante et la personnaliser pour détecter les applications propriétaires ou certains attributs d'une application existante. Les applications personnalisées sont définies dans **Objects (Objets)** > **Applications**.
- **Service/URL Category (Catégorie de Service / URL)** – Sélectionnez l'onglet **Service/URL Category (Catégorie de Service / URL)** pour indiquer un protocole TCP et/ou un numéro de port UDP ou une catégorie d'URL spécifique comme critère de correspondance dans la politique.
- **Action** - Sélectionnez l'onglet **Action** pour déterminer l'action qui sera prise en fonction du trafic correspondant aux attributs de la politique définie.
- **Usage (Utilisation)** - Sélectionnez l'onglet **Usage (Utilisation)** pour afficher l'utilisation d'une règle, y compris le nombre d'applications vues sur une règle, la dernière fois que des nouvelles applications ont été vues sur la règle, les données du Compteur d'accès, le trafic des 30 derniers jours, la date de création de la règle et la date de sa dernière modification.

Blocs de construction dans une règle de politique de sécurité

- Politiques > Sécurité

La section suivante décrit chaque composant d'une règle de politique de Sécurité. Lorsque vous créez une règle de politique de Sécurité, vous pouvez configurer les options décrites ici.

Éléments de base d'une politique de sécurité	Configuré dans	Description
Numéro de règle	S. O.	Le pare-feu numérote automatiquement chaque règle, et l'ordre change à mesure que les règles sont déplacées. Lorsque vous filtrez des règles pour rechercher des règles correspondant à un ou plusieurs filtre(s) spécifique(s), chaque règle s'affiche avec son numéro dans l'ensemble des règles de la base de règles et sa position dans l'ordre d'évaluation. Panorama numérote indépendamment les règles avant et les règles après. Lorsque Panorama transfère les règles à un pare-feu géré, la numérotation des règles intègre la hiérarchie dans les règles avant, les règles de pare-feu et les règles après d'une base de règles et reflète la séquence de règles et son ordre d'évaluation.
Name (Nom)	**Général**	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Rule Type (Type de règle)		Indique si la règle s'applique au trafic dans une zone, entre des zones ou aux deux'A0;: • **universal (universel)** (par défaut) : applique la règle à l'ensemble du trafic inter-zone et intra-zone correspondant dans les zones source et de destination indiquées. Par exemple, si vous créez une règle universelle pour les zones source A et B et de destination A et B, la règle s'applique à l'ensemble du trafic dans la zone A, dans la zone B, ainsi que de la zone A à la zone B et de la zone B à la zone A. • **intrazone (intra-zone)** : applique la règle à l'ensemble du trafic correspondant dans les zones source indiquées (vous ne pouvez pas indiquer de zone de destination pour les règles intra-zone). Par exemple, si vous définissez la zone source sur A et B, la règle s'applique à l'ensemble du trafic dans les zones'A0;A et B, mais pas entre les zones'A0;A et B. • **interzone (inter-zone)** : applique la règle à l'ensemble du trafic correspondant entre les zones source et de destination indiquées. Par exemple, si vous définissez la zone source sur A, B et C, et la zone de destination sur A et B, la règle s'applique à l'ensemble du trafic de la zone A à la zone B, de la zone B à la zone A, de la zone C à la zone A, de la zone C à la zone B, mais pas au trafic dans les zones A, B et C.
Description		Saisissez une description de la politique (1024 caractères maximum).
Étiquettes		Spécifiez l'étiquette pour la politique. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter des étiquettes à certaines règles avec des mots spécifiques, tels que Déchiffrement et Aucun déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement. Vous pouvez également ajouter des étiquettes aux règles par défaut.
Regrouper des règles par étiquette		Valeur par défaut : **None (Aucune)**.

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
Commentaire d'audit		
Archive des commentaires d'audit		
Journaux de configuration (entre les validations)		
Changements des règles		
Source Zone (Zone source)	**Source**	Il faut **Add (Ajouter)** des zones source (la valeur par défaut est **Any [N'importe laquelle]**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Source Address (Adresse source)		Cliquez sur **Add (Ajouter)** des adresses, des groupes d'adresses ou des régions source (la valeur par défaut est **Any [indifférent]**). Faites votre sélection dans la liste déroulante ou sélectionnez l'objet d'**Address (Adresse)**, le **Address Group (Groupe d'adresses)** ou les **Regions (Régions)** (en bas de la liste déroulante) pour définir les paramètres. Objets>Adresses et Objets>Groupes d'adresses décrivent les types d'objets d'adresses et les groupes d'adresses, respectivement, qu'une règle de politiques de sécurité prend en charge. Si vous sélectionnez l'option **Negate (Ignorer)**, la règle appliquera les adresses source de la zone spécifiée, à l'exception des adresses spécifiées.
Source User (Utilisateur source)	**Utilisateur**	**Add (Ajoutez)** les utilisateurs ou les groupes d'utilisateurs source soumis à la politique : • **indifférent** - Inclut tout trafic, quelles que soient les données utilisateur. • **pré-ouverture de session** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des terminaisons GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe d'utilisateurs du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option **Inconnu** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage utilisateur/adresse IP sur le pare-feu. • **Select (Sélection)** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement.  *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*
Profil HIP source	**Utilisateur**	**Add (Ajouter)** des profils HIP (profils d'informations sur l'hôte) vous permet de collecter des informations sur l'état de sécurité de vos hôtes, à savoir s'ils ont installé les derniers correctifs de sécurité et les dernières définitions antivirus. L'utilisation des profils d'informations sur l'hôte pour la mise en œuvre d'une stratégie active la sécurité granulaire qui garantit que les hôtes distants accédant à vos ressources vitales sont adéquatement maintenus et en conformité avec vos normes de sécurité avant de les autoriser à accéder à vos ressources réseau. Les profils HIP source suivants sont pris en charge : • **any (indifférent)** – Inclut tous les terminaux, quelles que soient les informations HIP. • **select (sélectionner)** – Inclut les profils HIP sélectionnés comme déterminé par votre configuration. Par exemple, vous pouvez ajouter un profil HIP, une liste de profils HIP ou ajouter des profils HIP manuellement. • **no-hip (pas de hip)** – Les informations HIP ne sont pas requises. Ce paramètre permet d'accéder à des clients

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		tiers qui ne peuvent pas collecter ou soumettre des informations HIP.
Destination Zone (Zone de destination)	**Destination**	Il faut **Add (Ajouter)** des zones de destination (la valeur par défaut est **any (n'importe laquelle)**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles. *Vous ne pouvez pas définir de zone de destination pour les règles intra-zone car ces types de règle s'appliquent uniquement au trafic disposant d'une source et d'une destination dans la même zone. Pour indiquer les zones qui correspondent à une règle intra-zone, vous devez définir uniquement la zone source.*
Adresse de destination		Cliquez sur **Add (Ajouter)** des adresses, des groupes d'adresses ou des régions de destination (la valeur par défaut est **any [indifférent]**). Faites votre sélection dans la liste déroulante ou cliquez sur l'objet d'**Address (Adresse)**, le **Address Group (Groupe d'adresses)** ou les **Regions (Régions)** (en bas de la liste déroulante) pour définir les paramètres d'adresses. Objets>Adresses et Objets>Groupes d'adresses décrivent les types d'objets d'adresses et les groupes d'adresses, respectivement, qu'une règle de politiques de sécurité prend en charge. Si vous sélectionnez l'option **Negate (Ignorer)**, la règle appliquera les adresses de destination de la zone spécifiée, à l'exception des adresses spécifiées.
Application	**Application**	**Add (Ajoutez)** des applications spécifiques pour la règle de politique de Sécurité. Si une application présente plusieurs fonctions, vous pouvez sélectionner l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans son ensemble, toutes les fonctions seront incluses et la définition de l'application sera automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou des conteneurs dans la règle de politique de Sécurité, vous pouvez en consulter les détails en passant la souris sur l'objet dans la colonne Application, en ouvrant la liste

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		déroulante et en sélectionnant **Valeur (Value)**. Ainsi, vous pourrez accéder aux membres des applications directement depuis la politique, sans passer par l'onglet **Object (Objet)**.  *Spécifiez toujours une ou plusieurs applications de sorte que seules les applications que vous voulez sur votre réseau sont autorisées, ce qui réduit la surface d'attaque et vous donne un plus grand contrôle du trafic réseau. Ne définissez pas l'application sur any (Indifférent), ce qui autorise le trafic de n'importe quelle application et augmente la surface d'attaque.*
Service (Service)	**Catégorie de service/URL**	Sélectionnez les services que vous souhaitez limiter à des numéros de ports TCP et/ou UDP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **any (indifférent)** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **Application-default (valeur par défaut de l'application)** - Les applications sélectionnées sont autorisées ou non seulement sur leurs **ports par défaut définis par Palo Alto Networks®**. Cette option est recommandée pour les politiques d'autorisation, car elle empêche l'exécution d'applications sur des ports ou protocoles inhabituels, qui, si elle n'est pas intentionnelle, peut être un signe de comportement et d'utilisation non souhaité des applications.  *Si vous utilisez cette option, le pare-feu vérifiera toujours les applications sur tous les ports, mais les applications seront autorisées uniquement sur leurs ports et protocoles par défaut.*  *Pour la plupart des applications, utilisez l'option application-default (application par défaut) pour empêcher l'application d'utiliser les ports non standard ou d'afficher d'autres comportements d'évitement. Si le port par défaut de l'application change, le pare-feu met automatiquement à jour la règle en utilisant le bon port par défaut. Pour les applications qui utilisent des ports non standard, comme les applications personnalisées internes, modifiez l'application ou créez une règle qui spécifie les ports non standard et appliquez*

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		la règle uniquement au trafic qui exige l'application. • **Select (Sélectionnez)** - **Add (Ajoutez)** un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée. (Ou sélectionnez Objets > Services et Objets > Groupes de services).
URL Category (Catégorie d'URL)		Sélectionnez des catégories d'URL pour la règle de sécurité. • Choisissez **any (indifférent)** pour autoriser ou non toutes les sessions, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, **Add (Ajoutez)** une ou plusieurs catégories spécifiques (y compris des catégories personnalisées) dans la liste déroulante. Sélectionnez Objets > Listes dynamiques externes pour définir des catégories personnalisées.
Paramètres d'action	**Actions**	Sélectionnez l'**Action** que le pare-feu prend à l'égard du trafic qui correspond aux attributs définis dans une règle : • **Allow (Autoriser)** - (par défaut) Autorise le trafic mis en correspondance. • **Deny (Refuser)** - Bloque le trafic mis en correspondance et applique l'*action Refuser* définie par défaut pour l'application refusée. Pour afficher l'action refuser définie par défaut pour une application, consultez les détails de l'application (**Objects (Objets)** > **Applications**). Étant donné que l'action Refuser par défaut varie d'une application à une autre, le pare-feu pourrait bloquer la session et envoyer une réinitialisation à une application, pendant qu'il abandonne silencieusement la session d'une autre application. • **Drop (Abandonner)** - Abandonne l'application sans aucune notification. Aucune réinitialisation TCP n'est envoyée à l'hôte ou à l'application, à moins d'avoir sélectionné **Send ICMP Unreachable (Envoyer ICMP inaccessible)**. • **Reset client (Réinitialiser le client)** - Envoie une réinitialisation TCP au périphérique côté client. • **Reset server (Réinitialiser le serveur)** - Envoie une réinitialisation TCP au périphérique côté serveur. • **Reset both (Réinitialiser les deux)** - Envoie une réinitialisation TCP aux périphériques côté client et côté serveur. • **Send ICMP Unreachable (Envoyer ICMP inaccessible)** – Uniquement disponible pour les interfaces de Couche 3. Lorsque vous configurez une règle de politique de Sécurité pour abandonner du trafic ou réinitialiser la

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		connexion, le trafic n'atteint pas l'hôte de destination. Dans ces cas-là, pour tout trafic UDP et TCP abandonné, vous pouvez activer le pare-feu pour qu'il envoie une réponse ICMP inaccessible à l'adresse IP source qui génère le trafic. L'activation de ce paramètre permet à la source de fermer ou d'arrêter facilement la session, évitant ainsi le plantage des applications. Pour afficher le taux de paquets ICMP inaccessibles configuré sur le pare-feu, consultez la section Paramètres de la session (**Device (Périphérique)** > **Setup (Configuration)** > **Session**). Pour appliquer un contrôle prioritaire sur l'action par défaut définie sur les règles interzones et intrazones prédéfinies : reportez-vous à la section Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité.
Paramètres du profil	**Actions**	Pour définir la vérification additionnelle que le pare-feu effectue sur les paquets qui correspondent à la règle de profil de Sécurité, sélectionnez les profils individuels Antivirus, Antispyware, Protection contre les vulnérabilités, Filtrage des URL, Blocage des fichiers, Filtrage des données, Analyse WildFire, Protection GTP et Protection SCTP. Pour définir un groupe de profils plutôt que des profils individuels, sélectionnez **Profile Type Group (Groupe de types de profil)**, puis sélectionnez un **Group Profile (Profil de groupe)**. Pour définir de nouveaux profils ou groupes de profils, cliquez sur **Nouveau** à côté du profil ou du groupe approprié (voir Objets > Profils de sécurité > Protection GTP). Vous pouvez également joindre des Profils de Sécurité (ou des groupes de profils) aux règles par défaut.
Paramètre des journaux et autres paramètres	**Actions**	Pour générer des entrées dans le journal du trafic local en cas de trafic correspondant à cette règle, sélectionnez les options suivantes'A0;: • **Log At Session Start (Se connecter au début de la session)** (option désactivée par défaut) – Génère une entrée dans le journal du trafic pour le début d'une session. *Évitez d'activer l'option Log at Session Start (Se connecter au début de la session) sauf à des fins de résolution de problèmes ou pour que les journaux de session de tunnel présentent les tunnels GRE actifs dans l'ACC. La journalisation à la fin de session*

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		consomme moins de ressources et identifie l'application exacte si l'application change après quelques paquets, par exemple, de facebook-base à facebook-chat. • **Log At Session End (Se connecter en fin de session)** (option activée par défaut) – Génère une entrée dans le journal du trafic pour la fin d'une session.  *Si des entrées pour le début ou la fin de la session sont journalisées, des entrées le sont également en cas d'abandon et de refus.* • **Log Forwarding Profile (Profil de transfert des journaux)** - Pour transférer des entrées du journal du trafic local et du journal des menaces vers des destinations distantes, comme des serveurs Panorama et Syslog, sélectionnez un **Log Forwarding Profile (Profil de transfert des journaux)**.  *La génération d'entrées du journal des menaces est déterminée par les Profils de Sécurité. Définissez de New (nouveaux profils) de journalisation, au besoin (voir Objets > Transfert des journaux).*  *Créez et activez des profils de transfert de journaux pour envoyer des journaux à des périphériques de stockage externes dédiés. Les journaux sont alors préservés, car le pare-feu dispose d'une capacité de stockage des journaux limitée et, lorsque l'espace est utilisé, le pare-feu supprime les journaux les plus vieux.* Vous pouvez également modifier les paramètres de journal dans les règles par défaut. Indiquez n'importe quelle combinaison des options suivantes'A0;: • **Schedule (Calendrier)** – Pour limiter les dates et les heures auxquelles la règle est en vigueur, sélectionnez un calendrier dans la liste déroulante. Définissez de **New (Nouveaux)** calendriers, au besoin (reportez-vous à Paramètres de contrôle du trafic SSL décrypté). • **QoS Marking (Marquage QoS)** – Pour modifier le paramètre de qualité du service (QoS) des paquets qui correspondent à la règle, sélectionnez **IP DSCP (Description IP)** ou **IP Precedence (Priorité IP)** et saisissez la valeur QoS au format binaire ou sélectionnez une valeur prédéfinie dans le menu déroulant. Pour plus

© 2020 Palo Alto Networks, Inc.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		d'informations sur la QoS, reportez-vous à la section Qualité de service. • **Disable Server Response Inspection (Désactiver l'inspection de la réponse du serveur)** – Désactive l'inspection des paquets entre le serveur et le client. L'option est désactivée par défaut.  *Pour une sécurité optimale, n'activez pas Disable Server Response Inspection (Désactiver l'inspection de la réponse du serveur). Lorsque cette option est sélectionnée, le pare-feu n'inspecte que les flux de données client-à-serveur. Il n'inspecte pas les flux de données serveur-à-client et, par conséquent, ne peut déterminer si ces flux de trafic comportent des menaces.*
De Base	**Rule Usage (Utilisation d'une règle)**	• **Rule Created (Règle créée)** : date et heure de création de la règle. • **Last Edited (Dernière modification)** : date et heure de la dernière modification de la règle.
Activité	**Rule Usage (Utilisation d'une règle)**	• **Hit Count (Nomre de correspondances)** : nombre total de fois que le trafic a été mis en correspondance avec la règle. • **First Hit (Première correspondance)** : moment de la première correspondance. • **Last Hit (Dernière correspondance)** : moment de la dernière correspondance.
Applications	**Rule Usage (Utilisation d'une règle)**	• **Applications Seen (Applications vues)** : le nombre d'applications que la règle autorise. • **Last App Seen (Dernière application vue)** : le nombre de jours depuis que la dernière nouvelle application (une application jamais vue jusqu'à présent) a été vue sur la règle. • **Compare Applications & Applications Seen (Comparer les applications et les applications vues)** : Cliquez sur cette option pour comparer les applications configurées sur la règle aux applications vues dans la règle. Utilisez cette outil pour découvrir les applications qui correspondent à la règle et pour ajouter des applications à la règle.
Traffic (des 30 derniers jours)	**Rule Usage (Utilisation d'une règle)**	• **Bytes (Octets)** : la quantité, en octets, de trafic de la règle au cours des 30 derniers jours.  *Si la période de temps dépasse 30 jours, les plus vieilles règles demeureraient*

© 2020 Palo Alto Networks, Inc.

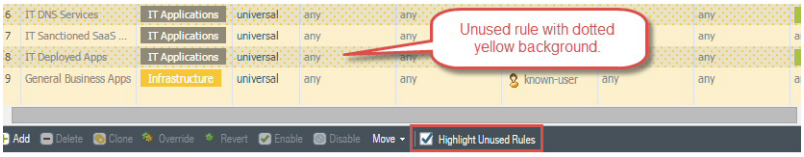
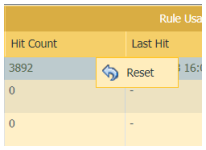
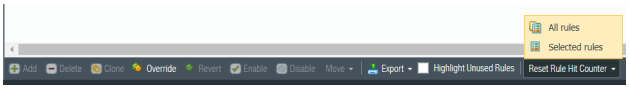
Éléments de base d'une politique de sécurité	Configuré dans	Description
		au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.

Création et gestion des politiques

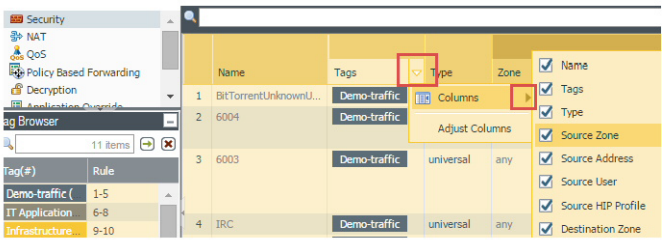
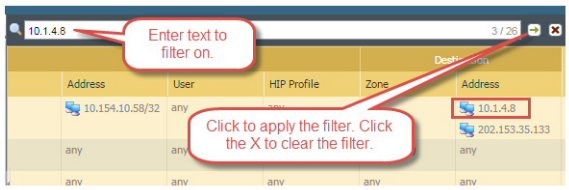
Sélectionnez la page **Policies (Politiques)** > **Security (Sécurité)** pour ajouter, modifier et gérer les politiques de sécurité :

Tâche	Description
Ajouter	**Add** (Ajoutez) une nouvelle règle de politique ou sélectionnez une règle sur laquelle fonder une nouvelle règle et **Clone Rule (Clonez la règle)**. La règle copiée « règle*n* », où *n* représente le premier nombre entier disponible qui caractérise le nom de la règle, est insérée sous la règle sélectionnée. Pour plus d'informations sur le clonage, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Modifier	Sélectionnez une règle pour en modifier les paramètres. Si la règle est transmise par Panorama, elle est en lecture seule sur le pare-feu et vous ne pouvez la modifier localement.
	Les actions **Override (Contrôle prioritaire)** et **Revert (Rétablir)** ne concernent que les règles par défaut affichées en bas de la base des règles de Sécurité. Ces règles prédéfinies, autorisant l'ensemble du trafic intra-zone et refusant l'ensemble du trafic inter-zone, indiquent au pare-feu comment gérer le trafic qui ne correspond à aucune autre règle dans la base de règles. Comme elles font partie de la configuration prédéfinie, vous devez appliquer un **Override (Contrôle prioritaire)** afin de modifier les paramètres de politique sélectionnés. Si vous utilisez Panorama, vous pouvez également **Override (Forcer)** les règles par défaut et les appliquer sur les pare-feu dans un Groupe de périphériques ou un Contexte partagé. Vous pouvez également **Revert (Rétablir)** les règles par défaut afin de restaurer les paramètres prédéfinis ou les paramètres transmis par Panorama. Pour plus d'informations, reportez-vous à la section Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité.
Se déplacer	Les règles sont évaluées de haut en bas et telles qu'elles apparaissent dans la page **Policies (Politiques)**. Pour modifier l'ordre d'évaluation des règles par rapport au trafic réseau, sélectionnez une règle et cliquez sur **Move Up (Déplacer en haut)**, **Move Down (Déplacer en bas)**, **Move Top (Déplacer vers le haut)**, **Move Bottom (Déplacer vers le bas)** ou **Move to a different rulebase or device group (Déplacer vers une autre base de règles ou un autre groupe de périphériques.)**. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Copiez l'UUID.	Copiez l'UUID de la règle au presse-papiers aux fins d'utilisation lors de la recherche de la configuration ou des journaux.

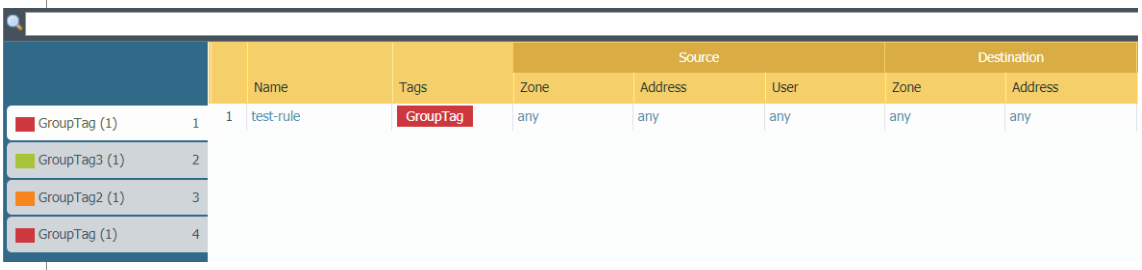
© 2020 Palo Alto Networks, Inc.

Tâche	Description
Supprimer	Sélectionnez et **Delete (Supprimer)** une règle existante.
Activer/ désactiver	Pour désactiver une règle, sélectionnez-la et **Disable (Désactivez)**-la ; pour activer une règle qui est désactivée, sélectionnez-la et **Enable (Activez)**-la.
Surveiller l'utilisation d'une règle	Pour identifier les règles qui n'ont pas été utilisées depuis le dernier redémarrage du pare-feu, sélectionnez **Highlight Unused Rules (Mettre en évidence les règles non utilisées)**. Vous pourrez ensuite décider de la **Disable (Désactiver)** ou de la **Delete (Supprimer)**. Les règles qui ne servent pas à l'heure actuelle s'affichent sur un fond jaune pointillé. Lorsque le compteur d'accès à une règle de politique est activé, les données du Compteur d'accès sont utilisées pour déterminer si une règle est inutilisée. *Chaque pare-feu garde un indicateur de trafic pour les règles ayant une correspondance. Comme l'indicateur est réinitialisé à l'occasion de la réinitialisation du panneau de données au moment d'un redémarrage, dans le cadre des meilleures pratiques, contrôlez cette liste régulièrement pour déterminer si la règle a eu une correspondance depuis le dernier contrôle avant de la supprimer ou de la désactiver.* 
Réinitialiser le Compteur d'accès	Le **Hit Count (Compteur d'accès)** suit le trafic total qui correspond à la règle de politique. Ce chiffre demeure après le redémarrage, la mise à niveau et le redémarrage du panneau de données. Pour réinitialiser le compteur d'une règle donnée, développez la liste déroulante et **Reset (Réinitialiser)** le compteur.  Vous pouvez également **Reset Rule Hit Counter (Réinitialiser le Compteur d'accès)** (menu du bas). Pour effacer les statistiques du compteur d'accès, sélectionnez **All Rules (Toutes les règles)** ou sélectionnez des règles précises et réinitialiser les statistiques du compteur pour les **Selected rules (Règles sélectionnées)** uniquement.  Consultez le **First Hit (Premier accès)** pour déterminer la première utilisation de la politique de sécurité. La date est indiquée au format hh:mm:ss année. Vous ne pouvez pas réinitialiser cette valeur. Consultez le **Last Hit (Dernier accès)** pour déterminer la dernière utilisation de la politique de sécurité. La date est indiquée au format hh:mm:ss année. Vous ne pouvez pas réinitialiser cette valeur.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
Afficher/ Masquer les colonnes	Montrer ou masquer les colonnes qui s'affichent sous **Policies (Politiques)**. Sélectionnez le nom de la colonne pour faire basculer l'affichage. 
Appliquer des filtres	Pour appliquer un filtre à la liste, faites votre choix parmi la liste déroulante **Filter Rules (Règles de filtrage)**. Pour définir un filtre, choisissez **Filter (Filtre)** dans le menu déroulant des éléments. *Les règles par défaut ne font pas partie du filtrage de la base de règles et s'affichent toujours dans la liste des règles filtrées.*
	Pour afficher les sessions réseau consignées comme correspondances par rapport à la politique, sélectionnez **Log Viewer (Afficheur de journaux)** dans le menu déroulant des noms de règles.
	Pour afficher la valeur actuelle, sélectionnez **Value (Valeur)** dans le menu déroulant des entrées. Vous pouvez également modifier, filtrer ou supprimer les éléments directement depuis le menu de la colonne. Par exemple, pour afficher les adresses incluses dans un groupe d'adresses, placez votre souris sur l'objet dans la colonne **Address (Adresse)**, puis sélectionnez **Value (Valeur)** dans la liste déroulante. Ainsi, les membres et les adresses IP correspondantes du groupe d'adresses s'affichent rapidement, sans devoir accéder à l'onglet **Object (Objet)**.
	Pour rechercher des objets qui sont utilisés dans une politique basée sur leur nom ou adresse IP, utilisez le filtre. Après avoir appliqué le filtre, vous ne verrez que les éléments qui correspondent à ce dernier. Le filtre fonctionne également avec les objets imbriqués. Par exemple, si vous filtrez 10.1.4.8, seule la politique qui contient cette adresse s'affiche : 
Prévisualiser les règles (Panorama uniquement)	Cliquez sur l'option **Preview Rules (Prévisualiser les règles)** pour afficher une liste des les règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de règles, la hiérarchie des règles est marquée visuellement pour chaque groupe de périphériques (et pare-feu géré), afin de faciliter l'analyse d'un grand nombre de règles.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
Exporter le tableau de configuration	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter la base de règles de politique au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, au besoin, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.
Surligner la règle inutilisée	Surlignez une règle de politique sans correspondances de trafic dans la colonne **Rule Usage (Utilisation d'une règle)**.
Group (Groupe)	Gérez les groupes d'étiquettes lorsque la case **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** est cochée. Vous pouvez effectuer les actions suivantes : • **Move rules in group to different rulebase or device group (Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques)** : déplacez le groupe d'étiquettes sélectionné vers un autre groupe de périphériques. • **Change group of all rules (Modifier le groupe de toutes les règles)** : déplacez les règles du groupe d'étiquettes sélectionné vers un autre groupe d'étiquettes dans la base de règles • **Delete all rules in group (Supprimer toutes les règles du groupe)** : supprime toutes les règles d'un groupe d'étiquettes sélectionné. • **Clone all rules in group (Cloner toutes les règles du groupe)** : clone toutes les règles d'un groupe d'étiquettes sélectionné vers un groupe de périphériques.
Afficher la base de règles en tant que groupes	Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher la base de règles de la politique au moyen de l'étiquette utilisée dans **Group Rules by Tag (Règles de groupe par étiquette)**. Les règles de politique visibles sont celles qui appartiennent au groupe d'étiquettes sélectionné. 
Tester la correspondance de la politique	Effectuez un test des politiques de protection pour la base de règles de politique sélectionnée pour vérifier que le bon trafic est refusé et autorisé.

Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité

Les règles de sécurité par défaut, inter-zone (par défaut) et intra-zone (par défaut), disposent de paramètres prédéfinis qui peuvent avoir un contrôle prioritaire sur un pare-feu ou sur Panorama. Si un pare-feu reçoit les règles par défaut d'un groupe de périphériques, vous pouvez également appliquer un contrôle prioritaire sur les paramètres du groupe de périphériques. Le pare-feu ou le système virtuel sur lequel vous appliquez un contrôle prioritaire stocke une version locale de la configuration de la règle. Les paramètres sur lesquels

© 2020 Palo Alto Networks, Inc.

vous pouvez appliquer un contrôle prioritaire sont un sous-ensemble de l'ensemble complet (le tableau suivant affiche une liste du sous-ensemble des règles de sécurité). Pour plus d'informations sur les règles de sécurité par défaut, consultez la section Politiques > Sécurité.

Pour appliquer un contrôle prioritaire sur une règle, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur un pare-feu ou **Policies (Politiques)** > **Security (Sécurité)** > **Default Rules (Règles par défaut)** sur Panorama. La colonne Nom affiche une icône représentant les éléments hérités () pour les règles sur lesquelles vous pouvez appliquer un contrôle prioritaire. Sélectionnez la règle, cliquez sur **Override (Contrôle prioritaire)** et modifiez les paramètres dans le tableau suivant.

Pour rétablir les paramètres prédéfinis d'une règle ayant été forcée ou les paramètres transmis par un groupe de périphériques Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur un pare-feu ou **Policies (Politiques)** > **Security (Sécurité)** > **Default Rules (Règles par défaut)** sur Panorama. La colonne Nom affiche une icône représentant le contrôle prioritaire () pour les règles contenant des valeurs qui ont été forcées. Sélectionnez la règle, cliquez sur **Revert (Rétablir)** et cliquez sur **Yes (Oui)** pour confirmer l'opération.

Champs pour appliquer un contrôle prioritaire d'une règle de sécurité par défaut	Description
Onglet Général	
Name (Nom)	Le **Name (Nom)** indique que la règle est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.
Rule Type (Type de règle)	Le **Rule Type (Type de règle)** est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.
Description	La **Description** est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.
Étiquette	Sélectionnez **Tags (Étiquettes)** dans la liste déroulante. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, ajouter une étiquette avec les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement spécifiques ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement.
Onglet Actions	
Paramètres d'action	Sélectionnez l'**Action** appropriée pour le trafic correspondant à la règle. • **Allow (Autoriser)** - (par défaut) Autorise le trafic. • **Deny (Refuser)** - Bloque le trafic et applique l'action Refuser définie par défaut pour l'application refusée par le pare-feu. Pour afficher l'action Refuser définie par défaut pour une application, consultez les détails de l'application dans **Objects (Objets)** > **Applications**.

© 2020 Palo Alto Networks, Inc.

Champs pour appliquer un contrôle prioritaire d'une règle de sécurité par défaut	Description
	• **Drop (Abandonner)** - Abandonne l'application sans aucune notification. Le pare-feu n'envoie aucun message de réinitialisation TCP à l'hôte ou à l'application. • **Reset client (Réinitialiser le client)** - Envoie un message de réinitialisation TCP au périphérique côté client. • **Reset server (Réinitialiser le serveur)** - Envoie un message de réinitialisation TCP au périphérique côté serveur. • **Reset both (Réinitialiser les deux)** - Envoie un message de réinitialisation TCP aux périphériques côté client et côté serveur.
Paramètres du profil	**Profile Type (Type de profil)** - Affectez des profils ou groupes de profils à la règle de sécurité : • Pour définir la vérification que les profils de sécurité effectuent par défaut, sélectionnez **Profiles (Profils)**, puis sélectionnez un ou plusieurs profils individuels **Antivirus**, **Vulnerability Protection (Protection contre les vulnérabilités)**, **Anti-Spyware (Antispyware)**, **URL Filtering (Filtrage des URL)**, **File Blocking (Blocage de fichiers)**, **Data Filtering (Filtrage des données)** et/ou **WildFire Analysis (Analyse WildFire)**. • Pour assigner un groupe de profils plutôt que des profils individuels, sélectionnez **Group (Groupe)**, puis sélectionnez **Group Profile (Profil de groupe)** dans la liste déroulante. • Pour définir de nouveaux profils(Objets > Profils de sécurité) ou groupes de profils (Objets > Profils de sécurité > Protection GTP), cliquez sur **New (Nouveau)** dans la liste déroulante pour le profil ou le groupe correspondant.
Paramètre des journaux	Indiquez n'importe quelle combinaison des options suivantes'A0;: • **Log Forwarding (Transfert des journaux)** - Pour transférer des entrées du journal du trafic local et du journal des menaces vers des destinations distantes, comme des serveurs Panorama et Syslog, sélectionnez un profil **Log Forwarding (Transfert des journaux)** dans la liste déroulante. Les profils de sécurité déterminent la génération d'entrées dans le journal des menaces. Pour définir un nouveau profil de **Log Forwarding (Transfert des journaux)**, sélectionnez **Profile (Profil)** dans la liste déroulante (reportez-vous à la section Objets > Transfert de journaux). • Pour générer des entrées dans le journal du trafic local en cas de trafic correspondant à cette règle, sélectionnez les options suivantes'A0;: • **Log at Session Start (Se connecter au début de la session)** - Génère une entrée dans le journal du trafic pour le début d'une session (sélectionné par défaut). • **Log at Session End (Se connecter en fin de session)** - Génère une entrée dans le journal du trafic pour la fin d'une session (désactivé par défaut).

© 2020 Palo Alto Networks, Inc.

Champs pour appliquer un contrôle prioritaire d'une règle de sécurité par défaut	Description
	Si vous configurez le pare-feu afin qu'il inclue des entrées au début et à la fin de la session dans le journal du Trafic, il va également inclure des entrées d'abandon et de refus.

Applications et utilisation

- Politiques > Sécurité > Optimiseur de politique > Aucune application spécifiée > Comparer (ou cliquer sur le nombre indiqué dans **Apps Seen [Applications vues])**
- Politiques > Sécurité > Optimiseur de politique > Applications inutilisées > Comparer (ou cliquer sur le nombre indiqué dans **Apps Seen [Applications vues])**
- Politiques > Sécurité et cliquer sur le nombre indiqué dans **Apps Seen (Applications vues)**

Avec l'onglet Usage (Utilisation) de la règle de politique de sécurité, vous pouvez aussi **Compare Applications & Applications Seen (Comparer les applications et les applications vues)** pour accéder aux outils qui vous aident à passer de règles de politique de sécurité basées sur les ports à des règles de politique de sécurité basées sur les applications et à éliminer les applications non utilisées des règles sous **Applications & Usage (Applications et utilisation)**.

Champ	Description
Délai	La période de temps pour les informations d'application : • **Anytime (En tout temps)** : affiche les applications vues au cours de la durée de vie de la règle. • **Past 7 days (7 derniers jours)** : affiche uniquement les applications vues au cours des 7 derniers jours. • **Past 15 days (15 derniers jours)** : affiche uniquement les applications vues au cours des 15 derniers jours. • **Past 30 days (30 derniers jours)** : affiche uniquement les applications vues au cours des 30 derniers jours.
Applications d'une règle	Les applications configurées dans la règle ou **Any (n'importe laquelle)** si aucune application spécifique n'est configurée dans la règle. Vous pouvez **Browse (Parcourir)**, **Add (Ajouter)** et **Delete (Supprimer)** les applications, au besoin, et les applications sont configurées dans une règle. Le chiffre entouré d'un cercle qui figure à côté de Apps on Rule (Applications d'une règle) indique le nombre d'applications. L'ajout d'applications à partir de cet emplacement revient à ajouter des applications dans la règle de politique de sécurité à l'onglet **Application**.
Applications vues	Toutes les applications vues et autorisées sur le pare-feu qui correspondent à la règle. Le chiffre entouré d'un cercle qui figure à côté de Apps Seen (Applications vues) indique le nombre d'applications vues dans la règle. • **Applications** : les applications vues dans la règle. Par exemple, si une règle autorise le trafic de navigation Web (Applications

© 2020 Palo Alto Networks, Inc.

Champ	Description
	d'une règle), il se peut que vous voyiez de nombreuses applications dans la liste, car il existe de nombreuses applications de navigation Web. • **Subcategory (Sous-catégorie)** : la sous-catégorie de l'application. • **Risk (Risque)** : la cote de risque de l'application. • **First Seen (Première apparition)** : le premier jour où l'application a été vue sur le réseau. • **Last Seen (Dernière apparition)** : la dernière journée à laquelle l'application a été vue sur le réseau.  *La granularité de la mesure des options First Seen (Première apparition) et Last Seen (Dernière apparition) est d'une journée. Ainsi, au cours de la journée où vous définissez une règle, les journées indiquées dans First Seen (Première apparition) et Last Seen (Dernière apparition) sont identiques.* • **Traffic (30 days) (Trafic [30 jours])** : la quantité de trafic, en octets, vue au cours des 30 derniers jours.  *Si la période de temps était plus longue, les plus vieilles règles demeureraient au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.*
Actions des applications vues	Actions que vous pouvez exécuter à l'option **Apps Seen (Applications vues)** : • **Create Cloned Rule (Créer une règle clonée)** : clone la règle actuelle. Lors de la migration de règles basées sur les ports à et des règles basées sur les applications, clonez d'abord la règle basée sur les ports, puis modifiez la règle clonée pour créer la règle de mise sur la liste blanche basée sur les applications. La règle clonée est insérée au-dessus de la règle basée sur les ports dans la liste de politiques. Utilisez cette méthode de migration afin de veiller à ne pas refuser par inadvertance le trafic que vous souhaitez autoriser ; si la règle clonée n'autorise pas toutes les applications dont vous avez besoin, la règle basée sur les ports qui suit les autorise. Surveillez la règle basée sur les ports et ajustez la règle basée sur les applications (clonée), au besoin. Lorsque vous avez la certitude que la règle basée sur les applications autorise le trafic que vous souhaitez et que seul le trafic non désire passe à la règle basée sur les ports, vous pouvez supprimer cette dernière en toute sécurité. • **Add to This Rule (Ajouter à cette règle)** : ajoute des applications vues à une règle. L'ajout d'applications à la règle transforme une règle configurée pour qu'elle corresponde à **Any (N'importe quelle)** application (une règle basée sur les ports) en une règle basée sur les applications qui met les

© 2020 Palo Alto Networks, Inc.

Champ	Description
	applications que vous spécifiez sur la liste blanche (la nouvelle règle basée sur les applications remplace la règle basée sur les ports). Toutes les applications que n'ajoutez pas à la règle sont refusées, comme c'est le cas pour toutes les règles de mise sur la liste blanche basée sur les applications. Veillez à identifier toutes les applications que vous souhaitez autoriser et ajoutez-les à la règle, afin d'éviter de refuser accidentellement une application. • **Add to Existing Rule (Ajouter à une règle existante)** : ajoute des applications vues à une règle existante basée sur les applications (App-ID). Ceci vous permet de cloner une règle basée sur App-ID à partir d'une règle basée sur un port, puis d'ajouter d'autres applications vues dans les règles sur les ports à l'application basée sur App-ID par la suite. • **Match Usage (mise en correspondance de l'utilisation)** : déplace toutes les applications vues dans la règle (elles sont répertoriées sous Applications d'une règle après avoir **mis en correspondance l'utilisation**). Si vous êtes certain que la règle devrait autoriser *toutes* les applications indiquées, la **Match Usage (mise en correspondance de l'utilisation)** est très pratique. Vous devez toutefois être certain que toutes les applications indiquées sont des applications que vous souhaitez autoriser sur votre réseau. Si de nombreuses applications ont été vues dans la règle (par exemple, dans une règle qui autorise la navigation Web), il vaut mieux cloner la règle et passer à une règle basée sur les applications. La **Match Usage (Mise en correspondance de l'utilisation)** fonctionne bien pour des règles simples disposant d'applications bien connues. Par exemple, si une règle basée sur les ports associée au port 22 n'a vu que du trafic SSH (et que c'est le seul trafic qu'elle devrait voir), il est sécuritaire de **Match Usage (Mettre l'utilisation en correspondance)**.
Boîte de dialogue Cloner Boîte de dialogue Ajouter à cette règle Boîte de dialogue Ajouter des applications à une règle existante	Lorsque vous sélectionnez des applications dans **Apps Seen (Applications vues)** et **Create Cloned Rule (Créer une règle clonée)** ou **Add to Rule (Ajouter à la règle)** qui ont des applications associées, ces boîtes de dialogue énumèrent ce qui suit : • **Name (Nom)** (Boîtes de dialogue Cloner et Ajouter des applications à une règle existante seulement). • Clone (Cloner) : saisir le nom de la nouvelle règle clonée. • Add Apps to Existing Rule (Ajouter des applications à une règle existante) : Sélectionner la règle à laquelle ajouter des applications dans le menu déroulant ou saisir le nom de la règle. • **Applications** : • Ajouter une application conteneur (par défaut) : coche les cases de toutes les applications conteneur, les applications vues dans la règle et les applications conteneur qui n'ont pas été vues dans la règle.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• Add specific apps seen (Ajouter des applications vues spécifiques) : sélectionne seulement les applications qui ont été vues dans la règle et désélectionne toutes les autres. (Vous pouvez sélectionner manuellement les applications conteneur et les autres applications.) • **Application** : • Les applications sélectionnées qui ont été vues dans la règle, surlignées en vert. • Applications incorporantes, surlignées en gris, et les applications individuelles sont indiquées ci-dessous. • Applications individuelles incorporées qui ont été vues dans la règle, mais qui n'ont pas été sélectionnées dans **Applications & Usage (Application et utilisation)** (texte normal). • Applications individuelles incorporées qui n'ont pas été vues dans la règle (*italiques*). • La date à laquelle les applications ont été **Last Seen (Vues en dernier)** dans la règle. • **Dependent Application (Applications dépendantes)** : • La case d'ajout des dépendances d'application est cochée par défaut, car ces applications sont requises pour que l'application sélectionnée s'exécute. • **Depends On (Dépend de)** : la liste des applications dépendantes des applications sélectionnées. Les applications que vous avez sélectionnées ont besoin de ces applications pour s'exécuter. • **Required By (Requise par)** : liste des applications qui exigent l'application dépendante (**Depends On [Dépend de]**). (Parfois une application dépendante exige à son tour une autre application dépendante.) Les boîtes de dialogue **Clone (Cloner)**, **Add to Rule (Ajouter à la règle)** et **Add Apps to Existing Rule (Ajouter des applications à une règle existante)** permettent de garantir que les applications ne s'interrompent pas et vous permettent de protéger la règle à l'épreuve du temps en incluant des applications individuelles pertinentes qui sont associées aux applications que vous clonez ou ajoutez à une règle.

Optimiseur de la politique de sécurité

- Politiques > Sécurité > Optimiseur de politique

Policies (Politiques) > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** affiche :

- **Aucune application spécifiée** : règles dont l'application est définie sur **any (Indifférent)**, pour que vous puissiez identifier les règles basées sur le port pour convertir les règles basées sur l'application.
- **Applications non utilisées** : règles qui incluent les applications qui n'ont jamais été mises en correspondance avec la règle.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Name (Nom)	Le nom de la règle de politique de sécurité.
Service (Service)	Tous les services associés avec la règle de politique de sécurité.
Traffic (octets, 30 jours)	**Traffic (30 days) (Trafic [30 jours])** : la quantité de trafic, en octets, vue au cours des 30 derniers jours.  *Si la période de temps était plus longue, les plus vieilles règles demeureraient au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.*
Applications autorisées	Les applications que la règle autorise. Ouvrez la boîte de dialogue **Application** à partir de laquelle vous pouvez ajouter et supprimer des applications sur la règle.
Applications vues	Le nombre d'applications vues dans la règle. Cliquez sur le nombre pour ouvrir la boîte de dialogue **Applications & Usage (Applications et utilisation)**, qui vous permet de comparer les applications configurées sur la règle aux applications vues dans la règle et de modifier les applications.
Journée sans nouvelles applications	Le nombre de jours depuis la dernière fois que des nouvelles applications ont été vues dans la règle.
Comparer	Ouvrez la boîte de dialogue **Applications & Usage (Applications et utilisation)** pour comparer les applications configurées sur la règle aux applications vues dans la règle et modifier la règle.
Dernière correspondance	La dernière correspondance du trafic à la règle.
Première correspondance	La première correspondance du trafic à la règle.
Modifié	La date et l'heure de modification de la règle.
Créé	La date et l'heure de création de la règle.

© 2020 Palo Alto Networks, Inc.

Politiques > NAT

Si vous définissez des interfaces de Niveau 3 sur le pare-feu, vous pouvez configurer une politique de traduction des adresses réseau (NAT pour « Network Address Translation ») pour préciser si les adresses IP et les ports source ou de destination doivent être convertis en adresses et ports publics ou privés. Par exemple, des adresses source privées peuvent être traduites en adresses publiques sur le trafic envoyé depuis une zone interne (de confiance) vers une zone publique (non approuvée). La traduction des adresses réseau est également prise en charge sur les interfaces de câble virtuel.

Les règles de traduction des adresses réseau (NAT) sont basées sur les zones source et de destination, les adresses source et de destination et le service de l'application (HTTP par exemple). Comme les politiques de sécurité, les règles des politiques NAT sont comparées au trafic entrant dans un ordre précis et la première règle qui correspond au trafic est appliquée.

En fonction de vos besoins, ajoutez des itinéraires statiques vers le routeur local afin que le trafic vers l'ensemble des adresses publiques soit acheminé au pare-feu. Il peut également être nécessaire d'ajouter des itinéraires statiques vers l'interface de réception sur le pare-feu pour réacheminer le trafic vers l'adresse privée.

Les tableaux suivants décrivent les paramètres NAT et NPTv6 (traduction de préfixe réseau entre IPv6 et IPv6) :

- Onglet Général des politiques NAT
- Onglet Paquet d'origine NAT
- Onglet Paquet translaté NAT
- Onglet Liaison HA Active / Active

Vous souhaitez en savoir plus ?

Voir NAT

Onglet Général des politiques NAT

- **Policies (Politiques)** > **NAT** > **General (Général)**

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique NAT ou NPTv6. Vous pouvez configurer une étiquette afin que vous puissiez trier ou filtrer les politiques lorsqu'il en existe un grand nombre. Sélectionnez le type de politique NAT que vous voulez créer et qui va affecter les champs disponibles sur les onglets **Original Packet (Paquet d'origine)** et **Translated Packet (Paquet translaté)**.

Règle NAT - Paramètres généraux	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquette	Si vous avez voulez étiqueter la politique, cliquez sur **Ajouter** et indiquer l'étiquette.

© 2020 Palo Alto Networks, Inc.

Règle NAT - Paramètres généraux	Description
	Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Type NAT	Indiquez le type de traduction : • **ipv4** - traduction effectuée entre des adresses IPv4. • **nat64** - traduction effectuée entre des adresses IPv6 et IPv4. • **nptv6** - traduction effectuée entre des préfixes IPv6. Vous ne pouvez pas combiner des plages d'adresses IPv4 et IPv6 dans une même règle NAT.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Paquet d'origine NAT

- Politiques > NAT > Paquet d'origine

Sélectionnez l'onglet **Original Packet (Paquet d'origine)** pour définir les zones de paquets source et de destination qui seront tranlsatées par le pare-feu, ainsi que l'interface de destination et le type de service. Vous pouvez configurer plusieurs zones source et de destination de même type et vous pouvez appliquer la règle à des réseaux donnés ou à des adresses IP données.

Règle NAT - Paramètres du paquet d'origine	Description
Zone source / zone de destination	Sélectionnez une ou plusieurs zones source et de destination pour le paquet (non NAT) d'origine (valeur par défaut : **Any (Indifférent)**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Pour faciliter la gestion, vous pouvez préciser de multiples zones. Par exemple, vous pouvez configurer les paramètres afin que plusieurs adresses NAT internes renvoient vers la même adresse IP externe.
Interface de destination	Indiquez l'interface de destination des paquets que traduit le pare-feu. Vous pouvez utiliser l'interface de destination pour traduire des adresses

© 2020 Palo Alto Networks, Inc.

Règle NAT - Paramètres du paquet d'origine	Description
	IP différemment dans le cas où le réseau est connecté à deux fournisseurs d'accès avec des pools d'adresses IP différents.
Service (Service)	Précisez le service pour lequel le pare-feu traduit l'adresse source ou de destination. Pour définir un nouveau groupe de services, sélectionnez Objets > Groupes de service.
Adresse source / adresse de destination	Indiquez une combinaison d'adresses source et de destination que doit traduire le pare-feu. Pour NPTv6, les préfixes configurés pour l'**Adresse source** et l'**Adresse de destination** doivent être au format xxxx:xxxx::/yy. L'adresse ne peut pas contenir une partie de l'identifiant d'interface (hôte) défini. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64.

Onglet Paquet translaté NAT

- Politique > NAT > Paquet translaté

Aux fins de la traduction de l'adresse source, sélectionnez l'onglet **Translated Packet (Paquet traduit)** pour déterminer le type de traduction à effectuer sur la source et l'adresse et, éventuellement, sur le port auxquels la source est traduite.

Vous pouvez également activer la Translation d'une adresse de destination pour un hôte interne afin de le rendre accessible à une adresse IP publique. Dans ce cas, définissez une adresse source publique et une adresse de destination pour un hôte interne dans l'onglet **Original Packet (Paquet d'origine)**, puis à l'onglet **Translated Packet (Paquet translaté)**, vous configurez la **Static IP (Adresse IP statique)** ou **Dynamic IP (with session distribution) (Adresse IP dynamique (avec distribution de sessions)** et saisissez la **Translated Address (Adresse traduite)**. Ensuite, lorsque l'hôte interne accède à l'adresse publique, celle-ci est translatée vers l'adresse (de destination) interne de l'hôte interne.

Règle NAT - Paramètres du paquet translaté	Description
Traduction de l'adresse source	Sélectionnez le **Translation Type (type de translation)** (pool d'adresses dynamiques ou statiques) et saisissez une adresse IP ou une plage d'adresses (adresse1-adresse2) vers laquelle l'adresse source sera translatée (**Translated Address (Adresse translatée)**). La taille de la plage d'adresses est limitée par le type de pool d'adresses'A0;: • **Dynamic IP And Port (IP et port dynamiques)** - La sélection de l'adresse est basée sur un hachage de l'adresse IP source. Pour une adresse IP source donnée, le pare-feu utilise la même adresse source translatée pour toutes les sessions. Le NAT source d'adresses IP et de ports dynamiques prend en charge environ 64 000 sessions simultanées sur chaque adresse IP du pool NAT. Certains modèles prennent en charge la sursouscription, ce qui permet à une seule adresse IP d'héberger plus de 64 000 sessions simultanées. La translation des adresses IP / ports dynamiques de Palo Alto Networks® prend en charge plus de sessions NAT que d'adresses IP et ports disponibles. Grâce à la sursouscription, le pare-feu peut utiliser les combinaisons d'adresses IP et de

© 2020 Palo Alto Networks, Inc.

Règle NAT - Paramètres du paquet translaté	Description
	ports jusqu'à deux fois en simultané sur les pare-feux PA-220, PA-820, PA-850, VM-50, VM300 et VM-1000-HV, jusqu'à quatre fois en simultané sur les pare-feux PA-5220 et de la série PA-3200, et jusqu'à huit fois en simultané sur les pare-feux PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-500 et VM-700 lorsque les adresses IP de destination sont uniques. • **Dynamic IP (IP dynamique)** - Translate à la prochaine adresse disponible dans la plage définie, mais le numéro de port ne change pas. Jusqu'à 32 000 adresses IP consécutives sont prises en charge. Un pool d'adresses IP dynamiques peut contenir plusieurs sous-réseaux, donc vous pouvez traduire vos adresses réseau internes vers deux ou plusieurs sous-réseaux publics distincts. • **Advanced (Dynamic IP/Port Fallback) (Avancé (IP dynamique / port dynamique de secours))** - Utilisez cette option pour créer un pool de secours qui assure la translation des adresses IP et des ports si le pool principal est à court d'adresses. Vous pouvez définir des adresses pour le pool en utilisant l'option **Translated Address (Adresse traduite)** ou l'option **Interface Address (Adresse de l'interface)** ; la dernière option est réservée aux interfaces qui reçoivent une adresse IP de manière dynamique. Lors de la création d'un pool de secours, vérifiez que les adresses ne coïncident pas avec celles du pool principal.
Traduction de l'adresse source (suite)	• **Static IP (IP statique)** - La même adresse est toujours utilisée pour la translation et le port ne change pas. Par exemple, si la plage source est 192.168.0.1 - 192.168.0.10 et que la plage de translation est 10.0.0.1 - 10.0.0.10, l'adresse 192.168.0.2 est toujours translatée en 10.0.0.2. La taille de la plage d'adresses est quasi-illimitée. Vous devez utiliser une translation **Static IP (IP statique)** pour la translation de l'adresse source. Pour NPTv6, les préfixes configurés pour **Translated Address (Adresse translatée)** doivent être au format xxxx:xxxx::/yy et l'adresse ne peut pas contenir une partie de l'identifiant d'interface (hôte) définie. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64. • **None (Aucune)** - Aucune translation n'est effectuée.
Bidirectionnel	(Facultatif) Activez la translation bidirectionnelle pour la translation d'une adresse **Static IP (IP statique)** source pour que le pare-feu puisse créer une translation correspondante (NAT ou NPTv6) dans le sens opposé de la translation que vous configurez. *Si vous activez la traduction bidirectionnelle, vous devez vous assurer d'avoir mis en place des politiques de sécurité pour contrôler le trafic dans les deux sens. En l'absence de telles politiques, la fonctionnalité de traduction bidirectionnelle autorise la traduction automatique des paquets dans les deux directions.*
Traduction de l'adresse de destination	Configure les options suivantes pour que le pare-feu exécute la règle NAT de destination. Généralement, vous utilisez le NAT de destination pour autoriser l'accès à un serveur interne, tel qu'un serveur de messagerie, depuis le réseau public.
Type de translation	Sélectionnez le type de translation effectuée par le pare-feu sur l'adresse de destination :

© 2020 Palo Alto Networks, Inc.

Règle NAT - Paramètres du paquet translaté	Description
et adresse translatée	• **None (Aucune)** (par défaut) • **Static IP (IP statique)** : saisissez une **Translated Address (Adresse translatée)** comme adresse IP ou plage d'adresses IP et un numéro de **Translated Port (Port translaté)** (de 1 à 65535) pour la translation de l'adresse de destination et du numéro de port initiaux. Si le champ **Translated Port (Port translaté)** n'est pas renseigné, le port de destination n'est pas modifié. Pour NPTv6, les préfixes configurés pour le préfixe de Destination et la **Translated Address (Adresse translatée)** doivent être au format xxxx:xxxx::/yy. L'adresse ne peut pas contenir une partie de l'identifiant d'interface (hôte) défini. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64. *Le port translaté n'est pas pris en charge pour NPTv6 car NPTv6 sert strictement à la translationde préfixe. La section de l'adresse du port et de l'hôte est simplement transférée telle quelle.* *La translation d'adresses IP statiques pour IPv4 vous permet aussi de Enable DNS Rewrite (Activer la réécriture DNS) (tel que décrit ci-dessous)* • **Dynamic IP (with session distribution) (IP dynamique (avec distribution de sessions)** : sélectionnez ou saisissez une **Translated Address (Adresse translatée)** qui est un FQDN, un objet d'adresse ou un groupe d'adresses à partir duquel le pare-feu sélectionne l'adresse translatée. Si le serveur DNS renvoie plus d'une adresse pour un FQDN ou si l'objet d'adresse ou le groupe d'adresses se translate en plus d'une adresse IP, le pare-feu distribue les sessions parmi ces adresses en utilisant la **Session Distribution Method (Méthode de distribution de sessions)** définie.
Méthode de Distribution de Sessions	Si vous sélectionnez de translater le NAT de destination vers **Dynamic IP (with session distribution) (Adresse IP dynamique (avec distribution de session)**, il est possible que l'adresse de destination translatée (vers un nom de domaine complet (FQDN), un objet d'adresse ou un groupe d'adresses) peut se résoudre en plus d'une adresse. Vous pouvez choisir la manière dont le pare-feu distribue (affecte) les sessions par ces adresses pour équilibrer la distribution des sessions : • **Round Robin (Pondération comparative)** : (par défaut) affecte de nouvelles sessions à des adresses IP en ordre rotatif. Sauf si votre environnement vous force à choisir l'une des autres méthodes de distribution, utilisez cette méthode. • **Source IP Hash (Hachage IP source)** : affecte de nouvelles sessions en fonction du hachage des adresses IP source. Si vous avez du trafic entrant provenant d'une seule adresse IP source, sélectionnez une autre méthode que le **Source IP Hash (Hachage IP source)**. • **IP Modulo (Modulo IP)** : Le pare-feu tient compte de l'adresse IP source et de destination du paquet entrant ; le pare-feu effectue une opération XOR et une opération modulo. Le résultat détermine à quelle adresse IP le pare-feu affecte les nouvelles sessions. • **IP Hash (Hachage IP)** : affecte de nouvelles sessions au moyen d'un hachage d'adresses IP source et de destination. • **Least Sessions (Le moins de sessions)** : affecte de nouvelles sessions à l'adresse IP qui possède le moins de sessions concurrentes. Si vous disposez

© 2020 Palo Alto Networks, Inc.

Règle NAT - Paramètres du paquet translaté	Description
	de nombreuses sessions de courte durée, l'option **Least Sessions (le moins de sessions)** vous fournit une distribution plus équilibrée des sessions.
Activer la réécriture DNS :	Dans PAN-OS 9.0.2 et versions 9.0 ultérieurs, si la règle de politique NAT de destination est de type **ipv4**et que la translation de l'adresse de destination est de type **Static IP (IP statique), l'option Enable DNS Rewrite (Activer la réécriture DNS)** est disponible. Vous pouvez activer la réécriture DNS si vous utiliser un NAT de destination ainsi que les services DNS sur un côté du pare-feu pour résoudre les FQDN d'un client qui se trouve de l'autre côté du pare-feu. Lorsque la réponse DNS traverse le pare-feu, le pare-feu réécrit l'adresse IP dans la réponse DNS par rapport à l'adresse de destination originale ou à l'adresse de destination translatée qui correspond à la réponse DNS dans la règle de politique NAT. Une seule règle de politique NAT permet au pare-feu d'effectuer la NAT sur les paquets qui correspondent à la règle et d'effectuer la NAT sur les IP addresses in DNS responses that match the rule (adresses IP dans les réponses DNS qui correspondent à la règle). Vous devez spécifier la manière dont le pare-feu effectue la NAT sur une adresse IP dans une réponse DNS relative à la règle NAT : inverse ou directe. • **reverse (inverse)** - (par défaut) Si le paquet est une réponse DNS qui correspond à l'adresse de destination translatée dans la règle, la réponse DNS est translatée en utilisant la translation inverse de la règle utilisée. Par exemple, si la règle translate 1.1.1.10 en 192.168.1.10, le pare-feu réécrit la réponse DNS 192.168.1.10 en 1.1.1.10. • **forward (directe)** - Si le paquet est une réponse DNS qui correspond à l'adresse de destination originale dans la règle, la réponse DNS est translatée en utilisant la même translation que la règle utilise. Par exemple, si la règle translate 1.1.1.10 en 192.168.1.10, le pare-feu réécrit la réponse DNS 1.1.1.10 en 192.168.1.10.

Onglet Liaison HA Active / Active

- Politiques > NAT > Liaison HA Active/Active

L'onglet Liaison HA Active / Active n'est disponible que si le pare-feu est dans une configuration haute disponibilité (HD) active / active. Dans cette configuration, vous devez lier chaque règle NAT source (qu'elle soit statique ou dynamique) à l'ID de périphérique 0 ou à l'ID de périphérique 1 ; vous devez lier chaque règle NAT de destination à l'ID de périphérique **0**, à l'ID de périphérique **1**, **aux deux** (ID de périphérique 0 et ID de périphérique 1) ou au pare-feu actif-**principal**.

Sélectionnez les paramètres d'une **Liaison HA Active/Active** pour lier une règle NAT à un pare-feu HA comme suit :

- **0** - Lie la règle NAT au pare-feu qui possède l'ID du périphérique HA 0.
- **1** - Lie la règle NAT au pare-feu qui possède l'ID du périphérique HA 1.
- **both (aux deux)** - Lie la règle NAT aux deux pare-feu qui ont l'ID du périphérique HA 0 et l'ID du périphérique HA 0. Ce paramètre ne prend pas en charge la traduction d'adresses IP dynamiques ni la traduction d'adresses IP dynamiques et de ports NAT.
- **primary (principal)** - Lie la règle NAT au pare-feu à l'état HA actif/principal. Ce paramètre ne prend pas en charge la traduction d'adresses IP dynamiques ni la traduction d'adresses IP dynamiques et de ports NAT.

Généralement, les règles NAT spécifiques au périphérique sont configurées lorsque les deux homologues HA possèdent des pools d'adresses IP NAT uniques.

© 2020 Palo Alto Networks, Inc.

Lorsque le pare-feu crée une nouvelle session, la liaison HA détermine les règles NAT qui peuvent être mises en correspondance avec la session. La liaison doit comprendre le propriétaire de la session pour la mise en correspondance de la règle. Le pare-feu configuré pour la session effectue la mise en correspondance de la règle NAT, mais la session est comparée aux règles NAT qui sont liées au propriétaire de la session et traduite selon l'une des règles. En cas de règles spécifiques au périphérique, le pare-feu ignore toutes les règles NAT qui ne sont pas associées au propriétaire de la session. Par exemple, supposons que le pare-feu ayant le périphérique 1 est le propriétaire de la session et le pare-feu configuré pour la session. Lorsque le périphérique 1 tente de mettre en correspondance une session et une règle NAT, il ignore toutes les règles liées au périphérique ID 0.

En cas d'échec de l'un des homologues, le second homologue continue de traiter le trafic des sessions synchronisées du premier homologue, y compris les traductions NAT. Palo Alto Networks recommande la création d'une règle NAT double qui est liée à l'ID du second périphérique. Il y a ainsi deux règles NAT pour des adresses translatées source et des adresses translatées de destination identiques, soit une règle liée à chacun des ID du périphérique. Cette configuration permet à l'homologue HA de procéder aux taches de configuration d'une nouvelle session et d'effectuer la mise en correspondance de la règle NAT pour les règles NAT qui sont liées à son ID du périphérique. Sans une règle NAT double, l'homologue actif tentera d'effectuer la mise en correspondance de la politique NAT, mais la session ne correspondra pas aux règles propres au périphérique du pare-feu et le pare-feu sautera toutes les règles NAT qui ne sont pas liées à son ID du périphérique.

Vous souhaitez en savoir plus ?

Reportez-vous à la section NAT en mode HA active/active.

© 2020 Palo Alto Networks, Inc.

Politiques > QoS

Ajoutez des règles de politique QoS pour définir le trafic qui reçoit un traitement QoS spécifique et affecter une classe QoS à chaque règle de politique QoS afin de spécifier que la classe de service affectée s'applique à tous les trafics correspondants à la règle associée lorsqu'elle sort d'une interface sur laquelle la QoS est activée.

Les règles de politique de QoS transférées de Panorama vers un pare-feu s'affichent en orange et ne peuvent pas être modifiées au niveau du pare-feu.

De plus, pour permettre complètement au pare-feu d'assurer la QoS :

- Définissez des limites de bande passante pour chaque classe de service QoS (sélectionnez Réseau > Profils réseau > QoS pour ajouter ou modifier un profil QoS).
- Activez la QoS sur une interface (sélectionnez Réseau > QoS).

Référez-vous à la Qualité de service pour des flux de travail, des concepts et des cas pratiques relatifs à la QoS.

Vous devez **Ajouter** une nouvelle règle ou cloner une règle existante, puis définir les champs suivants.

Paramètres d'une règle de politique de QoS	
Onglet Général	
Name (Nom)	Saisissez un nom pour identifier la règle (63 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description (facultatif).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une règle de politique de QoS	
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.
Onglet Source	
Source Zone (Zone source)	Sélectionnez une ou plusieurs zones sources (la valeur par défaut est « **Indifférent** »). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel).
Source Address (Adresse source)	Indiquez une combinaison d'adresses IPv4 ou IPv6 sources dont l'application identifiée peut être écrasée. Pour sélectionner des adresses spécifiques, choisissez **select (sélectionner)** dans la liste déroulante et procédez de l'une des manières suivantes : • Sélectionnez cette option à côté des adresses  et/ou des groupes d'adresses  appropriés dans la colonne Disponible et cliquez sur **Ajouter** pour ajouter vos sélections à la colonne Sélectionnée. • Saisissez les premiers caractères d'un nom dans le champ Rechercher pour afficher toutes les adresses et tous les groupes d'adresses commençant par ces caractères. La sélection d'un élément dans la liste active cette option dans la colonne Disponibles. Répétez ce processus aussi souvent que nécessaire, puis cliquez sur **Add (Ajouter)**. • Saisissez une ou plusieurs adresses IP (une par ligne), avec ou sans masque réseau. Le format courant est : *<adresse_ip>/<masque>* • Pour supprimer des adresses, sélectionnez-les (colonne Sélectionné) et cliquez sur **Delete (Supprimer)** et cliquez sur Supprimer ou sélectionnez **any (indifférent)** pour effacer toutes les adresses et tous les groupes d'adresses. Pour ajouter de nouvelles adresses pouvant être utilisées dans cette politique ou dans d'autres politiques, cliquez sur **New Address (Nouvelle adresse)**. Pour définir de nouveaux groupes d'adresses, sélectionnez Objets > Groupes d'adresses.
Source User (Utilisateur source)	Indiquez les utilisateurs et groupes sources auxquels la politique de QoS va s'appliquer.
Inverser	Sélectionnez cette option pour que la politique s'applique en cas de non-correspondance des informations spécifiées dans cet onglet.
Onglet Destination	
Destination Zone (Zone de destination)	Sélectionnez une ou plusieurs zones de destination (la valeur par défaut est **any (indifférent)**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel).
Adresse de destination	Indiquez une combinaison d'adresses IPv4 ou IPv6 sources dont l'application identifiée peut être écrasée. Pour sélectionner des adresses spécifiques, choisissez **select (sélectionner)** dans la liste déroulante et procédez de l'une des manières suivantes :

© 2020 Palo Alto Networks, Inc.

Paramètres d'une règle de politique de QoS	
	• Sélectionnez cette option à côté des adresses  et/ou des groupes d'adresses  appropriés dans la colonne Disponible et cliquez sur **Ajouter** pour ajouter vos sélections à la colonne Sélectionnée. • Saisissez les premiers caractères d'un nom dans le champ Rechercher pour afficher toutes les adresses et tous les groupes d'adresses commençant par ces caractères. La sélection d'un élément dans la liste active cette option dans la colonne Disponibles. Répétez ce processus aussi souvent que nécessaire, puis cliquez sur **Add (Ajouter)**. • Saisissez une ou plusieurs adresses IP (une par ligne), avec ou sans masque réseau. Le format courant est : *<adresse_ip>/<masque>*. • Pour supprimer des adresses, sélectionnez-les (colonne Sélectionné) et cliquez sur **Delete (Supprimer)** et cliquez sur Supprimer ou sélectionnez **any (indifférent)** pour effacer toutes les adresses et tous les groupes d'adresses. Pour ajouter de nouvelles adresses pouvant être utilisées dans cette politique ou dans d'autres politiques, cliquez sur **New Address (Nouvelle adresse)**.
Inverser	Sélectionnez cette option pour que la politique s'applique en cas de non-correspondance des informations spécifiées dans cet onglet.
Onglet Application	
Application	Sélectionnez des applications spécifiques pour la règle de QoS. Pour définir de nouvelles applications ou de nouveaux groupes d'applications, sélectionnez **Objects (Objets)** > **Applications**. Si une application présente plusieurs fonctions, vous pouvez sélectionner l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans son ensemble, toutes les fonctions sont incluses et la définition de l'application est automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou un conteneur dans la règle de QoS, vous pouvez afficher les détails de ces objets en passant la souris sur l'objet qui figure dans la colonne Application, cliquez sur la flèche vers le bas et sélectionnez **Value (Valeur)**. Ainsi, vous pouvez facilement accéder aux membres des applications directement depuis la politique sans passer par l'onglet **Objets**.
Onglet Service / Catégorie d'URL	
Service (Service)	Sélectionnez des services à limiter à des numéros de ports TCP et/ou UDP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **any (indifférent)** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **application-default (par défaut de l'application)** - Les applications sélectionnées sont autorisées ou non seulement sur leurs **ports par défaut définis par Palo Alto Networks**. Cette option est recommandée pour les politiques d'autorisation.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une règle de politique de QoS	
	• **Select (Sélection)** - Cliquez sur **Add (Ajouter)**. Choisissez un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée.
URL Category (Catégorie d'URL)	Sélectionnez des catégories d'URL pour la règle de QoS. • Sélectionnez **Any (Indifférent)** pour vous assurer qu'une session peut correspondre à cette règle de QoS, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, cliquez sur **Add (Ajouter)** et sélectionnez une catégorie spécifique (y compris une catégorie personnalisée) dans la liste déroulante. Vous pouvez ajouter plusieurs catégories. Reportez-vous à Objets > Listes dynamiques externes pour des informations sur la définition des catégories personnalisées.
Onglet DSCP/TOS	
indifférent	Sélectionnez **Any (Indifférent)** (défini par défaut) pour autoriser la politique à être mise en correspondance avec le trafic, quel que soit la valeur DSCP (Differentiated Services Code Point/code d'accès aux services différenciés) ou ToS (type de service)/de priorité des adresses IP définie pour le trafic.
Points de code	Sélectionnez l'option **Codepoints (Points de code)** pour activer le trafic pour recevoir le traitement de la QoS en fonction de la valeur DSCP ou ToS définie dans l'en-tête IP d'un paquet. Les valeurs DSCP et ToS permettent d'indiquer le niveau de service demandé pour le trafic, tel que la remise au mieux. L'utilisation de points de code comme critère de correspondance dans une politique de QoS permet à une session de recevoir le traitement de la QoS en fonction du point de code détecté au début de la session. Continuez d'**Ajouter** des points de code pour faire correspondre le trafic à la politique de QoS : • Donnez un **Name (Nom)** descriptif aux entrées de point de code. • Sélectionnez le **Type** de point de code que vous souhaitez utiliser comme critère de correspondance pour la politique de QoS, puis sélectionnez une valeur **Codepoint (Point de code)** spécifique. Vous pouvez également créer un **Custom Codepoint (Point de code personnalisé)** en saisissant un **Codepoint Name (Nom de point de code)** et une **Binary Value (Valeur binaire)**.
Onglet Autres paramètres	
class	Sélectionnez la classe de QoS à assigner à la règle et cliquez sur **OK**. Les caractéristiques d'une classe sont définies dans le profil de QoS. Reportez-vous à Réseau > Profils réseau > QoS pour des informations sur la configuration de paramètres pour les classes de QoS.
Programmer	• Sélectionnez **None (Aucun)** pour que la règle de politique soit active en tout temps. • À partir du menu déroulant, sélectionnez **Schedule (Calendrier)** (icône du calendrier) pour définir une plage horaire fixe ou récurrente pendant laquelle la règle est active.

© 2020 Palo Alto Networks, Inc.

Politiques > Transfert basé sur une politique

Normalement, lorsque le trafic entre dans le pare-feu, l'interface d'entrée du routeur virtuel dicte l'itinéraire qui détermine l'interface de sortie et la zone de sécurité de destination en se basant sur l'adresse IP de destination. En créant une règle de transfert basé sur une politique (Policy-based Forwarding, PBF), vous pouvez préciser d'autres informations pour déterminer l'interface de sortie, y compris la zone source, l'adresse source, l'utilisateur source, l'adresse de destination, l'application de destination et le service de destination. La session initiale sur une adresse IP de destination et un port donnés associés à une application ne correspondra à aucune règle spécifique à l'application et sera transférée conformément aux règles PBF subséquentes (qui ne précisent aucune application) ou à la table de transfert du routeur virtuel. Toutes les sessions subséquentes sur cette adresse IP de destination et ce port pour la même application correspondront à une règle spécifique à l'application. Pour assurer le transfert via des règles PBF, il est déconseillé d'utiliser des règles spécifiques à une application.

Si nécessaire, des règles PBF peuvent être utilisées pour forcer le passage du trafic dans un système virtuel supplémentaire à l'aide de l'action Transférer à Vsys. Dans ce cas, il est nécessaire de définir une règle PBF supplémentaire qui transférera le paquet depuis le système virtuel de destination vers une interface de sortie spécifique sur le pare-feu.

Les tableaux suivants décrivent les paramètres de transfert basé sur une politique'A0;:

- Onglet Général du transfert basé sur une politique
- Onglet Source du transfert basé sur une politique
- Onglet Destination / Application / Service du transfert basé sur une politique
- Onglet Transfert du transfert basé sur une politique

Vous souhaitez en savoir plus ?

Référez-vous au Transfert basé sur une politique

Onglet Général du transfert basé sur une politique

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique PBF. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la politique (1024 caractères maximum).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez

© 2020 Palo Alto Networks, Inc.

Champ	Description
	ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Source du transfert basé sur une politique

L'onglet **Source** vous permet de définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique de transfert est appliquée.

Champ	Description
Source Zone (Zone source)	Pour choisir des zones source (valeur par défaut : indifférent), cliquez sur **Add (Ajouter)** et faites votre sélection dans la liste déroulante. Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles. *seules les zones de type Couche'A0;3 sont prises en charge pour le transfert basé sur la politique.*
Source Address (Adresse source)	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions source (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres.
Source User (Utilisateur source)	Cliquez sur **Add (Ajouter)** pour choisir les utilisateurs ou les groupes d'utilisateurs source soumis à la politique. Les types d'utilisateur source suivants sont pris en charge'A0;: • **any (indifférent)** - Inclut tout trafic, quelles que soient les données utilisateur.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect™ mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **known-user (utilisateur connu)** - Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option Inconnu pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Select (Sélection)** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination / Application / Service du transfert basé sur une politique

Sélectionnez l'onglet **Destination/Application/Service** pour définir les paramètres de destination qui seront appliqués au trafic correspondant à la règle de transfert.

Champ	Description
Adresse de destination	Cliquez sur **Add (Ajouter)** pour ajouter des adresses de destination ou des groupes d'adresses (valeur par défaut : indifférent). Par défaut, la règle s'applique à **Any (Toute)** adresse IP. Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)** ou sur **Address Group (Groupe d'adresses)** en bas de la liste déroulante et définissez les paramètres.
Application/Service	Sélectionnez des applications ou des services spécifiques pour la règle PBF. Pour définir de nouvelles applications, reportez-vous à la Définition des applications. Pour définir des groupes d'applications, reportez-vous à Objets > Groupes d'applications. *Il n'est pas recommandé d'utiliser les règles propres à une application avec le transfert basé sur une politique (PBF).*

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Lorsque cela est possible, utilisez un objet de service, qui est le port de couche 4 (TCP ou UDP) utilisé par le protocole ou l'application. Vous pouvez consulter les détails sur ces applications en passant la souris sur l'objet dans la colonne **Application**, en cliquant sur la flèche vers le bas et en sélectionnant **Value (Valeur)**. Ainsi, vous pouvez facilement accéder aux informations des applications directement depuis la politique sans passer par les onglets Objet. *Vous ne pouvez pas utiliser d'applications personnalisées, de filtres d'applications ou de groupes d'applications dans les règles PBF*

Onglet Transfert du transfert basé sur une politique

Sélectionnez l'onglet **Forwarding (Transfert)** pour définir les informations relatives aux actions et au réseau appliquées au trafic correspondant à la règle de transfert. Le trafic peut être transféré vers une adresse IP de saut suivant, un système virtuel ou être abandonné.

Champ	Description
Action (Action)	Sélectionnez l'une des options suivantes : • **Forward (Transférer)** - Précisez l'adresse IP du saut suivant et l'interface de sortie (l'interface prise par le paquet pour accéder au saut suivant spécifié). • **Forward To VSYS (Transférer à VSYS)** - Choisissez le système virtuel vers lequel effectuer le transfert dans la liste déroulante. • **Discard (Supprimer)** : abandonne le paquet. • **No PBF (Aucun PBF)** - Pas de modification du chemin que le paquet suivra. Cette option exclut les paquets qui correspondent aux critères de la source/de la destination/de l'application/du service définis dans la règle. Les paquets correspondants utilisent la table de routage au lieu du transfert basé sur une politique ; le pare-feu utilise la table de routage pour exclure le trafic correspondant du port redirigé. *Utilisez Forward (Transfert) ou Forward to VSYS (Transfert au système virtuel) en tant qu'action, pour que vous puissiez appliquer un profil de surveillance au trafic. (Vous ne pouvez appliquer un profil de surveillance lorsque l'action ne transfère par le trafic.) Les profils de surveillance surveillent l'adresse IP. En cas d'échec de la connectivité à l'adresse IP, les profils de surveillance précisent l'action.*
Interface de trafic sortant	Dirige le paquet vers une interface de sortie spécifique
Saut suivant	Si vous dirigez le paquet vers une interface spécifique, indiquez l'adresse IP du saut suivant du paquet de l'une des façons suivantes :

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• **IP Address (Adresse IP)** : Sélectionnez l'adresse IP et sélectionnez un objet d'adresse (ou créez un nouvel objet d'adresse) qui utilise une adresse IPv4 ou IPv6. • **FQDN** : Sélectionnez FQDN et sélectionnez un objet d'adresse (ou créez un nouvel objet d'adresse) qui utilise un FQDN. • **None (Aucun)** : Il n'y a pas de saut suivant ; le paquet est abandonné.
surveiller	Activez la surveillance pour vérifier la connexion à une **IP Address (Adresse IP)** cible ou à l'adresse IP de **Next Hop (Saut suivant)**. Sélectionnez **Monitor (Surveillance)** et associez un **Profile (Profil)** de surveillance (par défaut ou personnalisé, **Network [Réseau]** > **Network Profiles [Profils réseau]** > **Monitor [Surveillance]**) qui indique l'action lorsque l'adresse IP est inaccessible.  *Configurez les profils de surveillance et activez la surveillance pour que, en cas d'échec de l'interface de sortie ou de l'itinéraire, le pare-feu suit l'action du profil et minimise ou empêche l'interruption du service.*
Appliquer le retour symétrique	(Obligatoire pour les environnements de routage asymétrique) Sélectionnez **Appliquer le retour symétrique**, puis saisissez une ou plusieurs adresses IP dans la Liste d'**Adresses du saut suivant**. L'activation du retour symétrique permet de s'assurer que le trafic de retour (par exemple, depuis la zone approuvée sur le réseau local vers Internet) est transféré via la même interface que celle au niveau de laquelle le trafic arrive d'Internet.
Programmer	Pour limiter les dates et les heures auxquelles la règle est en vigueur, sélectionnez un calendrier dans la liste déroulante. Pour définir de nouveaux calendriers, reportez-vous à Paramètres pour contrôler le trafic SSL déchiffré.

© 2020 Palo Alto Networks, Inc.

Politiques > Déchiffrement

Vous pouvez configurer le pare-feu de manière à déchiffrer le trafic à des fins de visibilité, de contrôle et de sécurité granulaire. Les politiques de chiffrement peuvent s'appliquer au protocole SSL (Secure Sockets Layer/couche de sockets sécurisés), notamment les protocoles encapsulés SSL tels que IMAP(S), POP3(S), SMTP(S), FTP(S) et le trafic SSH (Secure Shell). L'option SSH vous permet de déchiffrer le trafic SSH sortant et entrant pour vous assurer que des protocoles sécurisés ne sont pas utilisés pour établir un tunnel pour des applications et du contenu non autorisés.

Ajoutez une règle de politiques de déchiffrement pour définir le trafic que vous voulez déchiffrer (par exemple, vous pouvez déchiffrer le trafic en fonction de la catégorisation d'URL). Les règles des politiques de déchiffrement sont comparées au trafic dans un ordre précis, donc les règles les plus spécifiques doivent précéder les règles plus générales.

Le déchiffrement du proxy de transfert SSL nécessite la configuration d'un certificat de confiance qui est présenté à l'utilisateur si le serveur auquel il se connecte possède un certificat signé par une autorité de certification de confiance. Créez un certificat sur la page **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis cliquez sur le nom du certificat et sélectionnez **Forward Trust Certificate (Transférer le certificat sécurisé)**.

Le pare-feu ne déchiffre par les applications qui interrompent le déchiffrement techniquement, par exemple, parce qu'elles utilisent des certificats épinglés ou l'authentification du client.

Reportez-vous à la Liste des applications exclues du déchiffrement SSL.

Les tableaux suivants décrivent les paramètres d'une politique de déchiffrement :

- Onglet Général du déchiffrement
- Onglet déchiffrement de la source
- Onglet Déchiffrement de la destination
- Onglet Service de déchiffrement / catégorie d'URL
- Onglet Options de Déchiffrement

Vous souhaitez en savoir plus ?

Voir déchiffrement

Onglet Général du déchiffrement

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique de déchiffrement. Vous pouvez également configurer une étiquette afin de pouvoir trier ou filtrer les politiques lorsqu'il existe un grand nombre de politiques.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).

© 2020 Palo Alto Networks, Inc.

Champ	Description
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet déchiffrement de la source

Sélectionnez l'onglet **Source** pour définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique de déchiffrement est appliquée.

Champ	Description
Source Zone (Zone source)	Cliquez sur **Add (Ajouter)** pour choisir des zones source (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Source Address (Adresse source)	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions source (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Source User (Utilisateur source)	Cliquez sur **Add (Ajouter)** pour choisir les utilisateurs ou les groupes d'utilisateurs source soumis à la politique. Les types d'utilisateur source suivants sont pris en charge'A0;: • **any (indifférent)** - Inclut tout trafic, quelles que soient les données utilisateur. • **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **known-user (utilisateur connu)** - Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option Inconnu pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Select (Sélection)** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement.  *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Déchiffrement de la destination

Sélectionnez l'onglet **Destination** pour définir la zone ou l'adresse de destination qui définit le trafic de destination auquel la politique sera appliquée.

Champ	Description
Destination Zone (Zone de destination)	Cliquez sur **Add (Ajouter)** pour choisir des zones de destination (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées

© 2020 Palo Alto Networks, Inc.

Champ	Description
	à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse de destination	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions de destination (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Service de déchiffrement / catégorie d'URL

Sélectionnez l'onglet **Service/URL Category (Service/Catégorie d'URL)** pour appliquer la politique de déchiffrement au trafic en fonction de numéros de ports TCP ou à n'importe quelle catégorie d'URL (ou une liste de catégories).

Champ	Description
Service (Service)	Appliquez la politique de déchiffrement au trafic en fonction de numéros de ports TCP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **any (indifférent)** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **application-default (application-défaut)** - Les applications sélectionnées sont décryptées (ou non) seulement sur les ports des applications définis par défaut par Palo Alto Networks. • **Select (Sélection)** - Cliquez sur **Add (Ajouter)**. Sélectionnez un service existant ou indiquez un nouveau **Service** ou **Service Group (Groupe de services)**. (Ou sélectionnez Objets > Services et Objets > Groupes de services).
Catégorie d'URL	Sélectionnez des catégories d'URL pour la règle de déchiffrement. • Choisissez **any (indifférent)** pour appliquer la règle à toutes les sessions, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, cliquez sur **Add (Ajouter)** et sélectionnez une catégorie spécifique (y compris une catégorie personnalisée) dans la liste déroulante. Vous pouvez ajouter plusieurs catégories. Pour plus d'informations sur la définition de catégories personnalisées, reportez-vous à cette section.

Onglet Options de Déchiffrement

Sélectionnez l'onglet **Options** pour déterminer si le trafic correspondant doit être décrypté ou non. Si l'option **Decrypt (Déchiffrer)** est définie, indiquez le type de déchiffrement. Vous pouvez également ajouter des fonctions de déchiffrement supplémentaires en configurant ou en sélectionnant un profil de déchiffrement.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Action (Action)	Sélectionnez **decrypt (déchiffrement)** ou **no-decrypt (aucun déchiffrement)** pour le trafic.
Type	Sélectionnez le type de trafic à déchiffrer dans la liste déroulante : • **SSL Forward Proxy (Proxy de transfert SSL)** - Précise que la politique déchiffrera le trafic client destiné à un serveur externe • **SSH Proxy (Proxy SSH)** - Précise que la politique déchiffrera le trafic SSH. Cette option vous permet de contrôler la tunnellisation SSH dans les politiques en précisant l'App-ID ssh-tunnel. • **SSL Inbound Inspection (Inspection SSL entrante)** - Précise que la politique déchiffrera le trafic d'inspection SSL entrante.
Profil de décryptage	Associez un profil de déchiffrement à une règle de politique afin de bloquer et de contrôler certains aspects du trafic. Pour plus d'informations concernant la création d'un profil de déchiffrement, sélectionnez Objets > Profils de déchiffrement.

© 2020 Palo Alto Networks, Inc.

Politiques > Inspection des tunnels

Vous pouvez configurer le pare-feu pour inspecter le contenu du trafic des protocoles de tunnel de texte en clair suivants :

- encapsulation générique de routage (GRE) ;
- protocole de tunnellisation du service général de radiocommunication par paquets (GPRS Tunneling Protocol) pour les données utilisateur (GTP-U) ; pris en charge uniquement par les pare-feu qui prennent en charge GTP.
- trafic IPSec non crypté (Algorithme de cryptage NULL pour IPSec et mode de transport IPSec AH) ;
- Réseau local (LAN) virtuel extensible (VXLAN)

Vous pouvez utiliser l'inspection du contenu du tunnel pour appliquer les règles de sécurité, la Protection DoS et les politiques de trafic QoS dans ces types de tunnels et sur le trafic imbriqué dans un autre tunnel de texte en clair (par exemple, IPSec crypté Null à l'intérieur d'un tunnel GRE).

Créez une politique d'Inspection de tunnel qui, lorsqu'elle correspond à un paquet entrant, détermine les protocoles de tunnel dans le paquet que le pare-feu inspectera et spécifie les conditions dans lesquelles le pare-feu supprime ou continue à traiter le paquet. Vous pouvez consulter les journaux d'inspection de tunnel et l'activité du tunnel dans l'ACC pour vérifier que le trafic par tunnel est conforme aux politiques de sécurité et d'utilisation de votre entreprise.

Le pare-feu supporte l'inspection du contenu du tunnel sur les interfaces et les sous-interfaces Ethernet, les interfaces AE, les interfaces VLAN et les tunnels VPN et LSVPN. La fonctionnalité est prise en charge dans les interfaces de niveau 3, de niveau 2, le câble virtuel et les déploiements Tap. L'inspection du contenu du tunnel fonctionne sur les passerelles partagées et sur les communications de système vers système virtuel.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les champs disponibles pour créer une politique d'Inspection des tunnels ?	Blocs de construction dans une politique d'inspection des tunnels
Comment puis-je consulter les journaux d'inspection du tunnel ?	Types de journaux et Niveaux de gravité
Vous souhaitez en savoir plus ?	Inspection du contenu du tunnel

Blocs de construction dans une politique d'inspection des tunnels

Sélectionnez **Policies (Politiques)** > **Tunnel Inspection (Inspection des tunnels)** pour ajouter une règle de politique d'inspection des tunnels. Vous pouvez utiliser le pare-feu pour inspecter le contenu des protocoles de tunnel de texte en clair (GRE, GTP-U, protocole IPSec non crypté et VXLAN) et utiliser l'inspection du contenu du tunnel pour appliquer les politiques de sécurité, de Protection DoS et de trafic QoS sur le trafic de ces types de tunnels. Tous les modèles de pare-feu prennent en charge l'inspection du contenu du tunnel des tunnels GRE et IPSec non cryptés, mais seuls les pare-feu qui prennent en charge GTP prennent en charge l'inspection du contenu des tunnels GTP-U. Le tableau suivant décrit les champs que vous configurez pour une politique d'Inspection des tunnels.

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
Name (Nom)	**Général**	Saisissez un nom pour la politique d'Inspection des tunnels, commençant par un caractère alphanumérique et pouvant contenir des zéros ou d'autres caractères alphanumériques, des traits de soulignement, des traits d'union, des points et des espaces.
Description		(Facultatif) Saisissez une description de la politique d'inspection des Tunnels.
Étiquettes		(Facultatif) Saisissez un ou plusieurs tags pour la journalisation et la génération de rapports qui identifient les paquets soumis à la politique d'Inspection des tunnels.
Regrouper des règles par étiquette		Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit		Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit		Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.
Source Zone (Zone source)	**Source**	Veuillez **Add (Ajouter)** une ou plusieurs zones sources de paquets auxquelles s'applique la politique d'Inspection des tunnels (la valeur par défaut est **Any (Indifférent)**).
Source Address (Adresse source)		(Facultatif) Veuillez **Ajouter** les adresses sources IPv4 ou IPv6, les groupes d'adresses ou les objets d'adresse de la Région géographique des paquets auxquels s'applique la politique d'Inspection des tunnels (la valeur par défaut est **Indifférent**).
Source User (Utilisateur source)		(Facultatif) Veuillez **Ajouter** les utilisateurs sources de paquets auxquels s'applique la politique d'Inspection des tunnels (la valeur par défaut est **indifférent**).
Inverser		(Facultatif) Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles étant spécifiées.

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
Destination Zone (Zone de destination)	**Destination**	Veuillez **Ajouter** une ou plusieurs zones de destination de paquets auxquelles s'applique la politique d'Inspection des tunnels (la valeur par défaut est **Indifférent**).
Adresse de destination		(Facultatif) Veuillez **Ajouter** les adresses de destination IPv4 ou IPv6, les groupes d'adresses ou les objets d'adresse de la Région géographique des paquets auxquels s'applique la politique d'Inspection des tunnels (la valeur par défaut est **Indifférent**).
Inverser		(Facultatif) Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles étant spécifiées.
Protocole de tunnel	**Inspection**	Veuillez **Add (Ajouter)** un ou plusieurs **Protocols (Protocoles)** de tunnels que vous souhaitez que le pare-feu inspecte : • **GRE (GRE)** – Le pare-feu inspecte les paquets qui utilisent l'Encapsulation générique de routage dans le tunnel. • **GTP-U (GTP-U)** – Le pare-feu inspecte les paquets qui utilisent le protocole de tunnellisation General Packet Radio Service (service général de radiocommunication par paquets ; GPRS) dans le tunnel. • **Non-encrypted IPSec (IPSec non crypté)** – Le pare-feu inspecte les paquets qui utilisent le protocole IPSec non crypté (IPSec non crypté ou mode de transport AH IPSec) dans le tunnel. • **VXLAN** – Le pare-feu inspecte la charge utile VXLAN pour déceler le contenu encapsulé ou les applications du tunnel. Pour supprimer un protocole de votre liste, sélectionnez-le et cliquez sur **Delete (Supprimer)** pour le supprimer.
Niveaux maximums d'inspection des tunnels	**Inspection** > **Inspect Options (Options d'inspection)**	Précisez si le pare-feu inspectera **One Level (Un niveau)** (par défaut) ou **Two Levels (Tunnel In Tunnel) (Deux niveaux (Un tunnel dans un tunnel))** d'encapsulation. Pour VXLAN, sélectionnez **One Level (Un niveau)**, car l'inspection ne se produit que sur la couche externe.
Abandonner le paquet en cas de dépassement du niveau maximum d'inspection des tunnels		(Facultatif) Abandonnez les paquets qui contiennent plus de niveaux d'encapsulation que ceux indiqués pour les Niveaux maximums d'inspection des tunnels.
Abandonner le paquet en cas		(Facultatif) Abandonnez les paquets qui contiennent un protocole de tunnel qui utilise un en-tête qui n'est pas

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
d'échec de la vérification stricte de l'en-tête pour le protocole de tunnel		conforme au document RFC pour ce protocole. Les en-têtes non conformes indiquent des paquets suspects. Cette option permet au pare-feu de vérifier les en-têtes par rapport au document RFC 2890. *N'activez pas cette option si votre pare-feu met GRE en tunnel avec un périphérique qui met en œuvre une version de GRE plus ancienne que le document RFC 2890.*
Abandonner le paquet en cas de protocole inconnu dans le tunnel		(Facultatif) Abandonnez les paquets contenant un protocole dans le tunnel que le pare-feu ne parvient pas à identifier.
Retourner le tunnel VXLAN analysé vers la source		(Facultatif) Activez cette option pour retourner le trafic au point de terminaison du tunnel VXLAN(VTEP) d'origine. Par exemple, utilisez cette option pour retourner le paquet encapsulé au VTEP source. Pris en charge uniquement sur la couche 3, la sous-interface de couche 3, l'interface agrégée de couche 3 et VLAN.
Activer les options de sécurité	**Inspection** > **Security Options (Options de sécurité)**	(Facultatif) Veuillez **Enable Security Options (Activer les options de sécurité)** pour affecter des zones de sécurité pour un traitement du contenu du tunnel par chaque politique de Sécurité. Le contenu source interne appartient à la **Tunnel Source Zone (Zone source du tunnel)** que vous indiquez et le contenu de destination interne appartient à la **Tunnel Destination Zone (Zone de destination du tunnel)** que vous indiquez. Si vous n'effectuez pas l'action consistant à **Enable Security Options (Activer les options de sécurité)**, le contenu source interne appartient par défaut à la même zone que la source extérieure du tunnel et le contenu de destination interne appartient à la même zone que la destination extérieure du tunnel. Par conséquent, tant le contenu source interne que le contenu de destination interne sont soumis aux mêmes politiques de Sécurité qui s'appliquent aux zones source et de destination du tunnel extérieur.
Zone source du tunnel		Si vous **Enable Security Options (Activer les options de sécurité)**, sélectionnez une zone du tunnel que vous avez créée, et le contenu interne utilisera cette zone source pour l'application de la politique. Autrement, le contenu source interne appartient par défaut à la même zone que la source extérieure du tunnel

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
		et les politiques de la zone de la source extérieure du tunnel s'appliquent également à la zone de contenu source interne.
Zone de destination du tunnel		Si vous **Enable Security Options (Activer les options de sécurité)**, sélectionnez une zone du tunnel que vous avez créée, et le contenu interne utilisera cette zone de destination pour l'application de la politique. Autrement, le contenu de destination interne appartient par défaut à la même zone que la destination extérieure du tunnel et les politiques de la zone de la destination extérieure du tunnel s'appliquent également à la zone de contenu de destination interne.
Nom de la surveillance	**Inspection (Inspection)** > **Monitor Options (Options de surveillance)**	(Facultatif) Saisissez un nom de surveillance pour regrouper le trafic similaire afin de surveiller le trafic dans les journaux et les rapports.
Balise de surveillance (numéro)		(Facultatif) Saisissez un numéro de balise de surveillance qui peut regrouper le trafic similaire pour la journalisation et la génération de rapports (plage de 1 à 16 777 215). Le numéro de tag est défini de manière globale. *Ce champ ne s'applique pas au protocole VXLAN. Les journaux VXLAN utilisent automatiquement le VXLAN Network Identifier (Identificateur réseau VXLAN ; VNI) dans l'en-tête VXLAN.*
Se connecter au début de la session		(Facultatif) Sélectionnez cette option pour générer un journal au début de la session de tunnel de texte en clair qui correspond à la politique d'inspection des tunnels. Ce paramètre remplace le paramètre Log at Session Start (Se connecter au début de la session) qui figure dans la règle de Politique de Sécurité qui s'applique à la session. Les journaux de tunnel sont stockés séparément des journaux de trafic. Les informations de la session de tunnel extérieur (GRE, protocole IPSec non crypté ou GTP-U) sont stockées dans les journaux de tunnel et les flux de trafic intérieur, dans les journaux de trafic. Cette séparation permet de facilement faire état de l'activité du tunnel (par opposition à l'activité du contenu interne) avec l'ACC et ses fonctions de production de rapports. *Pour ce qui est des journaux de tunnel, il est recommandé de Journaliser au début de la session et de Journaliser en fin de la session, puisque, aux fins*

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
		de la journalisation, les tunnels peuvent avoir une très longue durée de vie. Par exemple, les tunnels GRE peuvent être créés lors du démarrage du routeur pour prendre fin uniquement au redémarrage du routeur. Si vous ne sélectionnez pas Journaliser au début de la session, vous ne verrez jamais qu'il y a un tunnel GRE actif dans l'ACC.
Se connecter en fin de session		(Facultatif) Sélectionnez cette option pour générer un journal en fin de session de tunnel de texte en clair qui correspond à la politique d'inspection des tunnels. Ce paramètre remplace le paramètre Journaliser en fin de session qui figure dans la règle de Politique de Sécurité qui s'applique à la session.
Transfert des journaux		(Facultatif) Sélectionnez un profil de Transfert des journaux dans la liste déroulante pour préciser l'endroit où transférer les journaux d'inspection des tunnels. (Ce paramètre est distinct du paramètre de Transfert des journaux d'une règle de politique de Sécurité, qui s'applique aux journaux de trafic.)
Name (Nom)	**ID de tunnel** Par défaut, si vous ne configurez **pas** d'ID VXLAN, tout le trafic est inspecté. Si vous configurez un ID VXLAN, vous pouvez l'utiliser comme critère de correspondance pour restreindre l'inspection du trafic à des VNI précis.	(Facultatif) Un nom commence par un caractère alphanumérique et pouvant contenir des zéros ou d'autres caractères alphanumériques, des traits de soulignement, des traits d'union, des points et des espaces. Le **Name (Nom)** décrit les VNI que vous regroupez. Le nom sert d'élément pratique, mais ne sert pas de facteur dans la journalisation, la surveillance ou l'établissement de rapports.
ID VXLAN (VNI)		(Facultatif) Saisissez un seul VNI, une liste de VNI séparés par des virgules, une plage d'un maximum de 16 millions de VNI (un tiret faisant office de séparateur), ou une combinaison de ces éléments. Par exemple : 1-54,1024,1677011-1677038,94 Les ID VXLAN maximum par politique sont 4 096. Pour préserver la mémoire de configuration, utilisez les plages lorsque possible.

© 2020 Palo Alto Networks, Inc.

Politiques > Contrôle prioritaire sur l'application

Pour modifier la manière dont le pare-feu classe le trafic réseau par application, vous pouvez définir des politiques de contrôle prioritaire sur l'application. Par exemple, si vous voulez contrôler l'une de vos applications personnalisées, une politique de contrôle prioritaire sur l'application peut être utilisée pour identifier le trafic pour cette application en fonction de la zone, de l'adresse source et de destination, du port et du protocole. Si certaines de vos applications réseau sont classées comme « inconnues », vous pouvez créer de nouvelles définitions d'application qui leur correspondent (reportez-vous à la section Définition des applications).

Si possible, évitez d'utiliser des politiques de contrôle prioritaire sur l'application, car elles empêchent le pare-feu d'utiliser App-ID pour identifier les applications et d'effectuer l'inspection de couche 7 pour y déceler des menaces. Pour soutenir les applications propriétaires internes, il est préférable de créer des applications personnalisées *qui incluent la signature d'application pour que le pare-feu effectue l'inspection de couche 7 et analyse le trafic d'applications pour y déceler des menaces. Si une application commerciale ne dispose pas d'un App-ID,* soumettez une demande de nouvel App-ID*. Si la définition d'une application publique (ports ou signature par défaut) change et que le pare-feu n'identifie plus correctement l'application, créez un billet d'assistance pour que Palo Alto Networks puisse mettre à jour la définition. Entre-temps, créez une application personnalisée pour que le pare-feu continue d'effectuer l'inspection de la couche 7 du trafic.*

Comme les politiques de sécurité, les politiques de contrôle prioritaire sur l'application peuvent avoir une portée générale ou spécifique, selon les besoins. Les règles des politiques sont comparées au trafic dans un ordre précis, donc les règles les plus spécifiques doivent précéder les règles plus générales.

Étant donné que le moteur App-ID de PAN-OS classe le trafic en identifiant le contenu spécifique aux applications dans le trafic réseau, les définitions d'application personnalisées ne peuvent se contenter d'utiliser un numéro de port comme identifiant. Elles doivent également inclure le trafic (restreint par zone source, adresse IP source, zone de destination et adresse IP de destination).

Pour créer une application personnalisée avec contrôle prioritaire sur l'application'A0;:

- Créer une application personnalisée (voir Définition des applications). Il n'est pas nécessaire de définir des signatures pour l'application si celle-ci est utilisée uniquement dans des règles de contrôle prioritaire sur l'application.
- Définissez une politique de contrôle prioritaire sur l'application qui précise quand l'application personnalisée doit être invoquée. En général, une politique inclut l'adresse IP du serveur exécutant l'application personnalisée et un ensemble limité d'adresses IP source ou une zone source.

Les tableaux suivants vous permettent de configurer une règle de contrôle prioritaire sur l'application.

- Onglet Général de contrôle prioritaire sur l'application
- Onglet Source de contrôle prioritaire sur l'application
- Onglet Destination de contrôle prioritaire sur l'application
- Onglet Protocole / Application de contrôle prioritaire sur l'application

Vous souhaitez en savoir plus ?

Voir Utilisation des objets application dans une politique.

© 2020 Palo Alto Networks, Inc.

Onglet Général de contrôle prioritaire sur l'application

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique de contrôle prioritaire sur l'application. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez choisir de regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. L'archive des commentaires d'audit peut être exportée au format CSV.

Onglet Source de contrôle prioritaire sur l'application

Sélectionnez l'onglet **Source** pour définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique de contrôle prioritaire sur l'application est appliquée.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Source Zone (Zone source)	Il faut **Ajouter** des zones source (la valeur par défaut est **n'importe laquelle**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Source Address (Adresse source)	Cliquez sur **Ajouter** des adresses, des groupes d'adresses ou des régions source (la valeur par défaut est **indifférent**). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Destination de contrôle prioritaire sur l'application

Sélectionnez l'onglet **Destination** pour définir la zone ou l'adresse de destination qui définit le trafic de destination auquel la politique sera appliquée.

Champ	Description
Destination Zone (Zone de destination)	Cliquez sur **Add (Ajouter)** pour choisir des zones de destination (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse de destination	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions de destination (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

© 2020 Palo Alto Networks, Inc.

Onglet Protocole / Application de contrôle prioritaire sur l'application

Sélectionnez l'onglet **Protocol/Application (Protocole/Application)** pour définir le protocole (TCP ou UDP), le port et l'application qui précisent les attributs de l'application correspondants à la politique.

Champ	Description
Protocole	Sélectionnez le protocole (**TCP** ou **UDP**) pour lequel autoriser le contrôle prioritaire sur l'application.
Port	Saisissez le numéro de port (de 0 à 65535) ou la plage de numéros de ports (port1-port2) pour les adresses de destination définies. Utilisez des virgules pour séparer les ports ou les plages.
Application	Sélectionnez l'application contrôle prioritaire pour les flux de trafic qui remplissent les critères de la règle. Lors du contrôle prioritaire d'une application personnalisée, aucune inspection des menaces n'est effectuée, sauf si le contrôle prioritaire porte sur une application prédéfinie qui prend en charge l'inspection des menaces. Pour définir de nouvelles applications, reportez-vous à la section Objets > Applications.

© 2020 Palo Alto Networks, Inc.

Politiques > Authentification

Votre politique d'Authentification vous permet d'authentifier les utilisateurs finaux avant qu'ils puissent accéder aux ressources du réseau.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les champs disponibles pour créer une règle d'Authentification ?	Blocs de construction d'une règle de politique d'authentification
Comment puis-je utiliser l'interface Web pour gérer les politiques d'Authentification ?	Créer et gérer la politique d'authentification Pour Panorama, reportez-vous à Déplacer ou cloner une règle de stratégie
Vous souhaitez en savoir plus ?	Politique d'authentification

Blocs de construction d'une règle de politique d'authentification

Chaque fois qu'un utilisateur demande une ressource (par exemple lorsqu'il se rend sur une page Web), le pare-feu évalue la politique d'Authentification. En fonction de la règle de la politique de correspondance, le pare-feu invite alors l'utilisateur à répondre à une ou plusieurs demandes provenant de divers facteurs (types), comme la connexion et le mot de passe, la voix, le SMS, la fonction push ou l'authentification du mot de passe à usage unique (OTP). Une fois que l'utilisateur répond à tous les facteurs, le pare-feu évalue la politique de Sécurité (voir Politiques > Sécurité) pour déterminer s'il faut autoriser l'accès à la ressource.

Le pare-feu n'invite pas les utilisateurs à s'authentifier s'ils ont accès à des ressources non basées sur le Web (comme une imprimante) par le biais d'une passerelle GlobalProtect™, c'est-à-dire en mode interne ou en mode tunnel. Au lieu de cela, les utilisateurs voient des messages indiquant l'échec de connexion. Pour s'assurer que les utilisateurs peuvent accéder à ces ressources, configurez un portail d'authentification et formez les utilisateurs à le consulter lorsqu'ils remarquent des échecs de connexion. Consultez votre service informatique pour configurer un portail d'authentification.

La table suivante décrit chaque bloc de construction ou composant d'une règle de politique d'Authentification. Avant d'Ajouter une règle, exécutez les tâches préalables décrites dans Créer et gérer la politique d'authentification.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
Numéro de règle	S. O.	Chaque règle est automatiquement numérotée et son ordre change à mesure que les règles sont déplacées. Lorsque vous filtrez des règles pour qu'elles correspondent à des filtres spécifiques, la page des **Policies (Politiques)** > **Authentication (Authentification)** répertorie chaque règle avec son numéro dans le

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
		contexte de l'ensemble des règles de la base de règles et sa position dans l'ordre d'évaluation. Pour plus d'information, reportez-vous à la section séquence de règles et son ordre d'évaluation.
Name (Nom)	**Général**	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description		Saisissez une description de la règle (1024 caractères maximum).
Étiquette		Sélectionnez une étiquette pour trier et filtrer les règles (voir Objets > Étiquettes).
Regrouper des règles par étiquette		Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit		Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit		Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.
Source Zone (Zone source)	**Source**	Veuillez **Ajouter** des zones pour appliquer la règle uniquement au trafic provenant des interfaces dans les zones que vous indiquez (la valeur par défaut est **indifférent**). Pour définir de nouvelles zones, voir Réseau > Zones.
Source Address (Adresse source)		Veuillez **Ajouter** les adresses ou les groupes d'adresses pour appliquer la règle uniquement au trafic provenant des sources que vous indiquez (la valeur par défaut est **indifférent**).

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
		Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles qui sont sélectionnées. Pour définir de nouvelles adresses ou de nouveaux groupes d'adresses, voir Objets > Adresses et Objets > Groupes d'adresses.
Source User (Utilisateur source)	**Utilisateur**	Sélectionnez les utilisateurs sources ou les groupes d'utilisateurs auxquels s'applique la règle : • **any (indifférent)** – Inclut tout trafic, quel que soit l'utilisateur source. • **pre-logon (préouverture de session)** – Inclut les utilisateurs distants qui ne sont pas connectés à leurs systèmes client, mais dont les systèmes client se connectent au réseau par le biais de la fonctionnalité de préouverture de session GlobalProtect. • **known-user (utilisateur connu)** – Inclut tous les utilisateurs pour lesquels le pare-feu possède déjà des mappages adresse IP / nom d'utilisateur avant que la règle évoque l'authentification. • **unknown (inconnu)** – Inclut tous les utilisateurs pour lesquels le pare-feu ne dispose pas de mappages adresse IP / nom d'utilisateur. Une fois que la règle évoque l'authentification, le pare-feu crée des mappages d'utilisateurs pour les utilisateurs inconnus en fonction des noms d'utilisateur qu'ils ont saisis. • **Select (Sélectionner)** – Inclut uniquement les utilisateurs et les groupes d'utilisateurs que vous avez décidé d'**Ajouter** à la liste Utilisateur source. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*
Profil HIP source		**Add (Ajouter)** des profils HIP (profils d'informations sur l'hôte) vous permet de collecter des informations sur l'état de sécurité de vos hôtes, à savoir s'ils ont installé les derniers correctifs de sécurité et les dernières définitions antivirus. Pour plus d'informations et pour définir de nouveaux profils HIP, voir Objets > GlobalProtect > Profils HIP.

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
Destination Zone (Zone de destination)	**Destination**	Veuillez **Ajouter** des zones pour appliquer la règle uniquement au trafic à destination des interfaces dans les zones que vous indiquez (la valeur par défaut est **indifférent**). Pour définir de nouvelles zones, voir Réseau > Zones.
Adresse de destination		Veuillez **Ajouter** les adresses ou les groupes d'adresses pour appliquer la règle uniquement aux destinations que vous indiquez (la valeur par défaut est **indifférent**). Sélectionnez **Negate (Refuser)** pour choisir n'importe quelle adresse sauf celles qui sont sélectionnées. Pour définir de nouvelles adresses ou de nouveaux groupes d'adresses, voir Objets > Adresses et Objets > Groupes d'adresses.
Service (Service)	**Catégorie de service/URL**	Choisissez une option parmi les options suivantes pour appliquer la règle uniquement aux services sur les numéros de ports TCP et UDP spécifiques : • **any (indifférent)** – Indique les services sur n'importe quel port utilisant n'importe quel protocole. • **default (par défaut)** – Indique les services uniquement sur les ports par défaut définis par Palo Alto Networks. • **Select (Sélectionner)** – Vous permet d'**Ajouter** des services ou des groupes de services. Pour créer de nouveaux services et de nouveaux groupes de services, voir Objets > Services et Objets > Groupes de services.  *La sélection par défaut est service-http. Lorsque vous utilisez la politique d'authentification pour le portail captif, activez également service-https pour veiller à ce que le pare-feu découvre le mappage utilisateur/adresse ip pour tout le trafic Web.*
URL Category (Catégorie d'URL)		Sélectionnez les catégories d'URL auxquelles la règle s'applique : • Sélectionnez **any (indifférent)** pour indiquer tout le trafic indépendamment de la catégorie d'URL. • Vous devez **Ajouter** des catégories. Pour définir des catégories personnalisées, voir Objets > Objets personnalisés > Catégorie d'URL.

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
Application de l'authentification	**Actions**	Sélectionnez l'objet d'application de l'authentification (Objets > Authentification) qui indique la méthode (comme le portail captif ou le défi de navigation) et le profil d'authentification que le pare-feu utilise pour authentifier les utilisateurs. Le profil d'authentification définit si les utilisateurs répondent à une seul demande d'authentification ou à une authentification multifacteur (voir Périphérique > Profil d'authentification). Vous pouvez sélectionner un objet d'application d'authentification prédéfini ou personnalisé. *Si vous devez exclure des hôtes ou des serveurs d'une politique de portail captif, ajoutez-les à un profil d'authentification qui spécifie no-captive-portal (aucun portail captif) en tant que Authentication Enforcement (Application de l'authentification). Cependant, les politiques du portail captif aident le pare-feu à découvrir le mappage utilisateur/adresse IP. On devrait les utiliser lorsque possible.*
délai d'expiration		Pour réduire la fréquence des demandes d'authentification qui interrompent le flux de travail de l'utilisateur, vous pouvez indiquer l'intervalle en minutes (60 étant la valeur par défaut) auquel le pare-feu invite l'utilisateur à s'authentifier une seule fois pour un accès répété aux ressources. Si l'objet de l'**Authentication Enforcement (Application de l'authentification)** indique l'authentification multifacteur, l'utilisateur doit s'authentifier une fois pour chaque facteur. Le pare-feu enregistre un horodatage et republie une demande uniquement lorsque le délai d'expiration d'un facteur expire. La Redistribution des horodatages vers d'autres pare-feu vous permet d'appliquer le délai d'expiration même si le pare-feu qui autorise initialement l'accès à un utilisateur n'est pas le même pare-feu qui contrôle ultérieurement l'accès pour cet utilisateur. *Le Timeout (Délai d'expiration) est un compromis entre une sécurité plus stricte (période plus courte entre les invites d'authentification) et l'expérience utilisateur (période plus longue entre les invites d'authentification). Une authentification plus fréquente est*

© 2020 Palo Alto Networks, Inc.

Blocs de construction dans une règle d'authentification	Configuré dans	Description
		souvent le choix le plus indiqué pour accéder aux systèmes critiques et aux zones sensibles, comme un centre de données. Une authentification moins fréquente est souvent indiquée au périmètre du réseau de même que pour les entreprises pour lesquelles l'expérience utilisateur est clé. *Définissez la valeur des ressources du périmètre sur 480 minutes (8 heures) et définissez une valeur plus faible, comme 60 minutes, pour les ressources du centre de données et les systèmes critiques pour renforcer la sécurité. Surveillez et ajustez les valeurs, au besoin.*
Délais d'authentification des journaux		Sélectionnez cette option (désactivée par défaut) si vous souhaitez que le pare-feu génère des journaux d'Authentification chaque fois que le **Timeout (Délai d'expiration)** associé à un facteur d'authentification expire. L'activation de cette option fournit plus de données pour résoudre les problèmes d'accès. En conjonction avec les objets de corrélation, vous pouvez également utiliser les journaux d'Authentification pour identifier l'activité suspecte sur votre réseau (comme les attaques par force brute). *L'activation de cette option augmente le trafic de journaux.*
Transfert des journaux		Sélectionnez un profil de Transfert des journaux si vous souhaitez que le pare-feu transfère des journaux d'Authentification à Panorama ou à des services externes comme un serveur Syslog (voir Objets > Transfert de journaux).

Créer et gérer la politique d'authentification

Sélectionnez la page **Policies (Politiques)** > **Authentication (Authentification)** pour créer et gérer les règles de la politique d'Authentification :

Tâche	Description
Ajouter	Effectuez les tâches préalables suivantes avant de créer les règles de la politique d'Authentification :

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	❑ Configurez les paramètres du Portail captif User-ID™ (voir Périphérique > Identification de l'utilisateur > Paramètres du portail captif). Le pare-feu utilise le Portail captif pour afficher le premier facteur d'authentification requis par la règle d'Authentification. Le Portail captif permet également au pare-feu d'enregistrer l'horodatage associé aux délais d'expiration d'authentification et de mettre à jour les mappages d'utilisateurs. ❑ Configurez un profil de serveur qui précise la manière dont le pare-feu peut accéder au service qui authentifiera les utilisateurs (se reporter à la section Périphérique > Profils de serveur). ❑ Affectez le profil de serveur à un profil d'authentification qui indique les paramètres d'authentification (voir Périphérique > Profil d'authentification). ❑ Affectez le profil d'authentification à un objet d'application d'authentification qui indique le mode d'authentification (voir Objets > Authentification). Pour créer une règle, effectuez l'une des étapes suivantes, puis renseignez les champs décrits dans Blocs de construction d'une règle de politique d'authentification : • Cliquez sur **Add (Ajouter)**. • Sélectionnez une règle sur laquelle baser la nouvelle règle et cliquez sur **Cloner la règle**. Le pare-feu insère la règle copiée, appelée <rulename># sous la règle sélectionnée, où « # » représente le premier nombre entier disponible qui caractérise le nom de la règle et génère un nouvel UUID pour la règle clonée. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Modifier	Pour modifier une règle, cliquez sur la règle Nom et modifiez les champs décrits dans Blocs de construction d'une règle de politique d'authentification.  *Si le pare-feu a reçu la règle de Panorama, la règle est en lecture seule ; vous ne pouvez l'éditer que sur Panorama.*
Se déplacer	Lors de la correspondance du trafic, le pare-feu évalue les règles de haut en bas dans l'ordre dans lequel la page **Policies (Politiques)** > **Authentication (Authentification)** les répertorie. Pour modifier l'ordre d'évaluation, sélectionnez une règle et cliquez sur **Move Up (Déplacer en haut)**, **Move Down (Déplacer en bas)**, **Move Top (Déplacer vers le haut)** ou **Move Bottom (Déplacer vers le bas)**. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Supprimer	Pour supprimer une règle existante, vous devez la sélectionner et l'**Effacer**.
Activer/ désactiver	Pour désactiver une règle, vous devez la sélectionner et la **Désactiver**. Pour réactiver une règle désactivée, vous devez la sélectionner et l'**Activer**.
Surligner les règles inutilisées	Pour identifier les règles qui n'ont pas correspondu au trafic depuis le dernier redémarrage du pare-feu, sélectionnez **Highlight Unused Rules (Surligner les règles inutilisées)**. Vous pourrez ensuite décider de désactiver ou de supprimer les règles inutilisées. La page met en évidence les règles inutilisées sur un arrière-plan jaune pointillé.
Prévisualiser les règles	Cliquez sur l'option **Preview Rules (Prévisualiser les règles)** pour afficher une liste des règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de

© 2020 Palo Alto Networks, Inc.

Tâche	Description
(Panorama uniquement)	règles, la page délimite visuellement la hiérarchie des règles pour chaque groupe de périphériques (et pare-feu géré) pour faciliter la numérisation de nombreuses règles.

© 2020 Palo Alto Networks, Inc.

Politiques > Protection'A0;DoS

Une politique de Protection DoS vous permet de protéger les ressources critiques individuelles contre les attaques DoS en spécifiant s'il faut refuser ou autoriser les paquets qui correspondent à une interface, une zone, une adresse ou un utilisateur source et/ou une interface, une zone ou un utilisateur de destination.

Vous pouvez également choisir l'action de Protection et spécifier un profil DoS où vous définissez les seuils (sessions ou paquets par seconde) qui déclenchent une alarme, activent une mesure de protection et indiquent le taux maximum au-dessus duquel toutes les nouvelles connexions sont abandonnées. Ainsi, vous pouvez contrôler le nombre de sessions entre des interfaces, des zones, des adresses et des pays en vous basant sur des sessions ou des adresses IP source et/ou de destination agrégées. Par exemple, vous pouvez contrôler le trafic depuis et vers certaines adresses ou groupes d'adresses, de certains utilisateurs et pour certains services.

Le pare-feu applique les règles de la politique de Protection DoS avant les règles de politique de Sécurité afin de s'assurer que le pare-feu utilise ses ressources de la manière la plus efficace. Si une règle de politique de Protection DoS refuse un paquet, ce paquet n'atteint jamais de règle de politique de Sécurité.

Les tableaux suivants décrivent les paramètres des politiques de Protection DoS :

- Onglet Général de protection DoS ;
- Onglet Source de protection DoS ;
- Onglet Destination de protection DoS ;
- Onglet Option / Protection de protection DoS.

Vous souhaitez en savoir plus ?

Voir Profils de protection DoS et Objets > Profils de sécurité > Protection DoS.

Onglet Général de protection DoS ;

- **Policies (Politiques)** > **DoS Protection (Protection DoS)** > **General (Général)**

Sélectionnez l'onglet **Général** pour configurer un nom et une description pour la politique de Protection DoS. Vous pouvez également configurer une étiquette afin de pouvoir trier ou filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Saisissez un nom pour identifier la règle de politique de Protection DoS. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquettes	Si vous avez voulez étiqueter la politique, cliquez sur **Ajouter** et indiquer l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Une étiquette est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, il se peut que vous souhaitiez ajouter une étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, ajouter une étiquette avec les mots Déchiffrement ou Aucun déchiffrement aux politiques de

© 2020 Palo Alto Networks, Inc.

Champ	Description
	déchiffrement ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Source de protection DoS ;

Sélectionnez l'onglet **Source** pour définir l'interface ou les interfaces source ou la/les zone(s) source, et éventuellement l'adresse ou les adresses source et le/les utilisateurs source qui définissent le trafic entrant auquel s'applique la règle de la politique DoS.

Champ	Description
Type	Sélectionnez le type de source à laquelle s'applique la règle de politique de Protection DoS : • **Interface** – Appliquez la règle au trafic en provenance de l'interface spécifiée ou du groupe d'interfaces spécifié. • **Zone** – Applique la règle au trafic provenant de n'importe quelle interface dans une zone spécifiée. Cliquez sur **Ajouter** pour sélectionner plusieurs interfaces ou zones.
Source Address (Adresse source)	Sélectionnez **Tout** ou **Ajouter** et spécifiez une ou plusieurs adresses sources auxquelles s'applique la règle de politique de Protection DoS. (Facultatif) Sélectionnez **Refuser** pour spécifier que la règle s'applique à toutes les adresses, à l'exception de celles qui sont spécifiées.
Source User (Utilisateur source)	Spécifiez un ou plusieurs utilisateurs source auxquels s'applique la règle de la politique de Protection DoS : • **Tout** – Inclut les paquets sans tenir compte de l'utilisateur source. • **Pré-ouverture de session** – Inclut les paquets provenant des utilisateurs distants connectés au réseau à l'aide de GlobalProtect, mais qui ne sont pas connectés à leur système. Lorsque l'option **pre-logon (pré-ouverture de session)** est configurée sur le Portail des applications GlobalProtect, tout utilisateur actuellement non connecté à sa machine est identifié avec la pré-ouverture de session avec le nom d'utilisateur. Vous pouvez ensuite créer des politiques pour les utilisateurs en pré-ouverture de session. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option **Inconnu** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Sélectionner** – Inclut les utilisateurs spécifiés dans cette fenêtre. Par exemple, vous pouvez sélectionner un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination de protection DoS ;

Sélectionnez l'onglet **Destination** pour définir la zone ou l'interface et l'adresse de destination qui définissent le trafic de destination auquel la politique s'applique.

Champ	Description
Type	Sélectionnez le type de destination auquel s'applique la règle de politique de protection DoS : • **Interface** – Appliquez la règle aux paquets destinés à l'interface spécifiée ou au groupe d'interfaces spécifié. Cliquez sur **Ajouter** et sélectionnez une ou plusieurs interfaces. • **Zone** – Appliquez la règle aux paquets destinés à n'importe quelle interface de la zone spécifiée. Cliquez sur **Ajouter** et sélectionnez une ou plusieurs zones.
Adresse de destination	Sélectionnez **Tout** ou **Ajouter** et spécifiez une ou plusieurs adresses de destination auxquelles s'applique la règle de politique de Protection DoS. (Facultatif) Sélectionnez **Refuser** pour spécifier que la règle s'applique à toutes les adresses, à l'exception de celles qui sont spécifiées.

Onglet Option / Protection de protection DoS.

Sélectionnez l'onglet **Option/Protection (Option/protection)** pour configurer des options pour la règle de politique de Protection DoS, notamment le type de service auquel la règle s'applique, l'action à effectuer par rapport aux paquets qui correspondent à la règle et le déclenchement ou non du transfert des journaux pour le trafic correspondant. Vous pouvez définir un calendrier afin d'indiquer quand la règle est active.

Vous pouvez également sélectionner un Profil de protection DoS agrégé et/ou un Profil de protection DoS classé qui déterminent les taux de seuils qui, lorsqu'ils sont dépassés, incitent le pare-feu à prendre des

© 2020 Palo Alto Networks, Inc.

mesures de protection, comme déclencher une alarme, activer une action telle que Random Early Drop, et supprimer les paquets qui dépassent le taux de seuil maximal.

Champ	Description
Service (Service)	Cliquez sur **Ajouter** et sélectionnez un ou plusieurs services auxquels s'applique la politique de Protection DoS. La valeur par défaut est **Tout** service. Par exemple, si la politique DoS protège les serveurs Web, spécifiez HTTP, HTTPS et les autres ports de service appropriés pour les applications Web.  *Pour les serveurs critiques, créez des règles de protection DoS distinctes pour protéger les ports de service non utilisés afin d'empêcher les attaques ciblées.*
Action (Action)	Sélectionnez l'action que le pare-feu effectue sur les paquets qui correspondent à la règle de la politique de Protection DoS : • **Refuser** – Désélectionnez tous les paquets qui correspondent à la règle. • **Autoriser** – Autorisez tous les paquets qui correspondent à la règle. • **Protect (Protéger)** – Appliquez les protections précisées dans le profil de protection DoS aux paquets qui correspondre à la règle. Les paquets qui correspondent à la règle sont comptabilisés en fonction des taux de seuil dans le profil de Protection DoS qui, à son tour, déclenche une alarme, active une autre action et déclenche des suppressions de paquets lorsque le taux maximal est dépassé.  *L'application de la protection DoS vise à vous protéger des attaques DoS. Vous devriez donc normalement utiliser l'option Protect (Protéger). Deny (Refuser) abandonne le trafic légitime et le trafic DoS et Allow (Autoriser) n'arrête pas les attaques DoS. Utilisez Deny (Refuser) et Allow (Autoriser) uniquement pour faire des exceptions au sein d'un groupe. Par exemple, vous pouvez refuser le trafic provenant de la plupart des groupes, mais autoriser un sous-réseau de ce trafic, ou autoriser le trafic provenant de la plupart des groupes, mais refuser un sous-réseau de ce trafic.*
Programmer	Spécifiez le calendrier durant lequel la règle de la politique de protection DoS est en vigueur. Le paramètre par défaut **Aucun** indique l'absence de calendrier ; la politique est toujours en vigueur. Autrement, sélectionnez un calendrier ou créez un nouveau calendrier pour contrôler le moment où la règle de la politique de Protection DoS est en vigueur. Saisissez un **Nom** pour identifier le calendrier. Sélectionnez **Partagé** pour partager ce calendrier avec chaque système virtuel d'un pare-feu à plusieurs systèmes virtuels. Sélectionnez une **Récurrence** parmi **Quotidien**, **Hebdomadaire**, ou **Non récurrent**. Ajoutez une **Heure de début** et une **Heure de fin** dans heures:minutes, en fonction d'une horloge de 24 heures.
Transfert des journaux	Si vous souhaitez déclencher le transfert des entrées du journal des menaces pour le trafic correspondant vers un service externe, comme un serveur Syslog ou Panorama, sélectionnez un profil de Transfert des journaux ou cliquez sur **Profil** pour en créer un nouveau.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Le pare-feu journalise et transfère uniquement le trafic qui correspond à une action de la règle. *Pour faciliter la gestion, transférez les journaux DoS séparément des autres journaux des menaces. Transmettez-les tous deux directement aux* administrateurs par e-mail et à serveur de journaux*.*
Agréger	Les profils de protection DoS agrégés définissent les seuils qui s'appliquent au groupe combiné de périphériques précisés dans la règle de protection DoS pour protéger ces groupes de serveur. Par exemple, si vous définissez un seuil de taux d'alarme de 10 000 CPS, cela signifie que lorsque le nouveau CPS total de l'ensemble du groupe dépasse 10 000 CPS, le pare-feu déclenche un message d'alarme. Sélectionne un profil de protection DoS agrégé qui spécifie les taux de seuil auxquels les connexions entrantes par seconde déclenchent une alarme, activent une action et dépassent un taux maximal. Toutes les connexions entrantes (agrégé) sont prises en compte dans les seuils spécifiés dans un profil de protection DoS agrégé. Le paramètre de profil agrégé **Aucun** signifie qu'il n'y a pas de paramètres de seuil en place pour le trafic agrégé. Voir Objets > Profils de sécurité > Protection DoS.
Classés	Les profils de protection DoS classés définissent les seuils qui s'appliquent à chaque périphérique individuel précisé dans la règle de protection DoS pour protéger des serveurs critiques individuel ou de petits groupes de serveurs critiques. Par exemple, si vous définissez un seuil de taux d'alarme de 10 000 CPS, cela signifie que lorsque le nouveau CPS total d'un serveur individuel précisé dans la règle dépasse 10 000 CPS, le pare-feu déclenche un message d'alarme. Sélectionnez cette option et indiquez les éléments suivants : • **Profil** – Sélectionnez un profil de protection DoS classé pour appliquer cette règle. • **Adresse** – Choisissez si les connexions entrantes sont prises en compte pour les seuils du profil si elles correspondent **uniquement à l'IP source**, **uniquement à l'IP de destination**, ou **à la fois à l'IP source et à l'IP de destination**. *Le pare-feu consomme plus de ressources pour suivre le compteur src-dest-ip-both (à la fois à l'IP source et à l'IP de destination) que pour suivre uniquement les compteurs d'adresses IP source ou d'adresses IP de destination.* Si vous spécifiez un profil de Protection DoS classé, seules les connexions entrantes qui correspondent à une adresse IP source, une adresse IP de destination ou une paire d'adresses IP source et de destination sont prises en compte dans les seuils spécifiés dans le profil. Par exemple, vous pouvez indiquer un profil de Protection DoS classé avec un **Taux max.** de 100 cps et indiquer un paramètre **Adresse** dans la règle à définir sur **adresse IP source uniquement**. Vous obtenez alors une limite de 100 connexions par seconde cette adresse IP source en particulier. *N'utilisez pas source-ip-only (ip source uniquement) ou src-dest-ip-both (à la fois à l'IP source et à l'IP de destination) pour les zones Internet, car le pare-feu ne peut pas stocker des compteur pour toutes les adresses IP Internet possibles. Utilisez destination-ip-only (ip de destination uniquement) dans les zones du périmètre.*

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Utilisez destination-ip-only (ip de destination uniquement) pour protéger les périphériques critiques individuels. *Utilisez source-ip-only (ip source uniquement) et le seuil d'Alarm (alarme) pour surveiller les hôtes suspects dans des zones qui ne sont pas connectées à l'Internet.* Voir Objets > Profils de sécurité > Protection DoS.

© 2020 Palo Alto Networks, Inc.

Politiques > SD-WAN

Créez une règle de politique SD-WAN avec des critères de correspondance qui comprend une ou des applications, ainsi qu'un profil de qualité du chemin d'accès qui spécifie les mesures d'état de la gigue, de la latence et de la perte de paquets que vous indiquez. Quand les chemins d'accès entre la source et la destination des applications sensibles et critiques subissent une dégradation, la règle de politique SD-WAN utilise le profil de distribution du trafic associé pour sélectionner de manière dynamique un nouveau chemin d'accès optimal pour les applications. La règle de politique SD-WAN indique également les périphériques cibles auxquels Panorama applique la règle.

- Onglet Général SD-WAN
- Onglet Source SD-WAN
- Onglet Destination SD-WAN
- Onglet Application/Service SD-WAN
- Onglet Sélection du chemin d'accès SD-WAN
- (Panorama uniquement) Onglet Cible SD-WAN

Onglet Général SD-WAN

- **Politiques** > **SD-WAN** > **Général**

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique SD-WAN. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1 024 caractères maximum).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, il se peut que vous souhaitiez ajouter des étiquettes uniques à certaines politiques SD-WAN pour identifier leurs hubs ou branches spécifiques auxquelles les règles s'appliquent.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez choisir de regrouper les règles en fonction d'une **Tag (Étiquette)**.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. L'archive des commentaires d'audit peut être exportée au format CSV.

Onglet Source SD-WAN

- **Politiques** > **SD-WAN** > **Source**

Sélectionnez l'onglet **Source** pour définir les zones sources, les adresses sources et les utilisateurs sources qui définissent les paquets entrants auxquels la politique SD-WAN s'applique.

Champ	Description
Source Zone (Zone source)	Pour spécifier une zone source, sélectionnez **Add (Ajouter)** et sélectionnez une ou plusieurs zones, ou sélectionnez **Any (N'importe quelle)** zone. Spécifier plusieurs zones peut simplifier la gestion. Par exemple, si vous avez trois branches dans différentes zones et vous voulez que les critères de correspondance ainsi que la sélection du chemin d'accès soient les mêmes pour les trois branches, vous pouvez créer une règle SD-WAN et spécifier les trois zones sources pour couvrir les trois branches. *Seules les zones de type Couche 3 sont prises en charge par les règles de politique SD-WAN.*
Source Address (Adresse source)	Pour spécifier des adresses sources, **Add (Ajoutez)** des adresses sources ou des listes dynamiques externes (EDL), sélectionnez dans le menu déroulant ou sélectionnez **Address (adresse)** et créez un nouvel objet adresse. Vous pouvez également sélectionner **Any (n'importe quelle)** adresse source (par défaut).
Source User (Utilisateur source)	Pour spécifier certains utilisateurs, sélectionnez **Add (ajouter)** (le type indique ensuite **select [sélectionner]**) et saisissez un utilisateur, une liste d'utilisateurs ou des groupes d'utilisateurs. Vous pouvez également sélectionner un type d'utilisateur : • **any (indifférent)** - (par défaut) Inclut tout utilisateur, quelles que soient les données utilisateur. • **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect™ mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez sélectionner l'option **unknown (inconnu)** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage utilisateur/adresse IP sur le pare-feu.  *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination SD-WAN

- **Politique** > **SD-WAN** > **Destination**

Sélectionnez l'onglet **Destination** pour définir la ou les zones de destination ou la ou les adresses de destination qui définissent le trafic auquel la règle de politique SD-WAN s'applique.

Champ	Description
Destination Zone (Zone de destination)	**Add (Ajoutez)** des zones de destination (la valeur par défaut est any [n'importe laquelle]). Les zones doivent être de Couche 3. Pour définir de nouvelles zones, voir Réseau > Zones. Ajoutez plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse de destination	**Add (Ajoutez)** des adresses, des groupes d'adresses, des listes dynamiques externes (EDL) ou des régions de destination (valeur par défaut : **any [indifférent]**). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)** ou sur **Address Group (Groupe d'adresses)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Application/Service SD-WAN

- **Politiques** > **SD-WAN** > **Application/Service**

© 2020 Palo Alto Networks, Inc.

Sélectionnez l'onglet **Application/Service** pour spécifier les applications ou les services auxquels la règle de politique SD-WAN s'applique.

Champ	Description
Path Quality Profile (Profil de qualité du chemin d'accès)	Sélectionnez un profil de qualité du chemin d'accès qui détermine le pourcentage maximum de gigue, de latence et de perte de paquets que vous voulez appliquer aux applications et aux services spécifiés. Si un profil de qualité du chemin d'accès n'a pas encore été créé, vous pouvez créer un **New SD-WAN Path Quality (Nouveau profil de qualité du chemin d'accès SD-WAN** à partir de cet onglet.
Applications	**Add (Ajoutez)** des applications spécifiques pour la règle de politique SD-WAN ou sélectionnez **Any (toutes)**. Si une application présente plusieurs fonctions, sélectionnez l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans son ensemble, toutes les fonctions seront incluses et la définition de l'application sera automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou des conteneurs dans la règle de politique SD-WAN, consultez les détails en passant la souris sur l'objet dans la colonne Application, en ouvrant la liste déroulante et en sélectionnant **Valeur (Value)**. Ainsi, vous pourrez accéder aux membres des applications directement depuis la politique, sans passer par l'onglet **Object (Objet)**. *Ajoutez uniquement les services critiques à l'entreprise qui sont affectés par la latence, la gigue et la perte de paquets. Évitez d'ajouter des catégories ou des sous-catégories d'applications, car celles-ci sont trop générales et ne permettent par le contrôle par application.*
Service (Service)	**Add (Ajoutez)** des services spécifiques à la règle de politique SD-WAN et sélectionnez les ports qui autorisent ou non les paquets de ces services : • **any (indifférent)** - Les services sélectionnés sont autorisés ou non sur n'importe quel protocole ou port. • **Application-default (valeur par défaut de l'application)** - Les services sélectionnés sont autorisés ou non seulement sur leurs **ports par défaut définis par Palo Alto Networks®**. Cette option est recommandée pour les politiques qui permettent de spécifier l'action **allow (autoriser)**, car elle empêche l'exécution de services sur des ports ou protocoles inhabituels, qui, si elle n'est pas intentionnelle, peut être un signe de comportement et d'utilisation non souhaité des services. *Si vous utilisez cette fonction, uniquement le port par défaut correspond à la politique SD-WAN et l'action de la politique est appliquée. D'autres services, qui ne sont pas sur le port par défaut, peuvent être autorisés en fonction de la règle de politique de sécurité, mais*

© 2020 Palo Alto Networks, Inc.

Champ	Description
	ils ne correspondent pas avec la politique SD-WAN et aucune action n'est prise dans la règle de politique SD-WAN. *Pour la plupart des services, utilisez l'option application-default (application par défaut) pour empêcher le service d'utiliser les ports non standard ou d'afficher d'autres comportements d'évitement. Si le port par défaut du service change, le pare-feu met automatiquement à jour la règle en utilisant le bon port par défaut. Pour les services qui utilisent des ports non standard, comme les services personnalisés internes, modifiez le service ou créez une règle qui spécifie les ports non standard et appliquez la règle uniquement au trafic qui exige le service.* • **Select (Sélectionnez)** - **Add (Ajoutez)** un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée. (Ou sélectionnez Objets > Services et Objets > Groupes de services).

Onglet Sélection du chemin d'accès SD-WAN

- **Politiques** > **SD-WAN** > **Sélection du chemin d'accès**

Sélectionnez l'onglet **Path Selection (sélection du chemin d'accès)** pour spécifier le profil de distribution du trafic qui contrôle comment le pare-feu sélectionne un nouveau chemin d'accès pour le trafic des applications ou des services lorsque l'une des mesures de l'état du chemin souhaité dépasse le seuil configuré dans le profil de qualité du chemin d'accès dans la règle de politique SD-WAN.

Champ	Description
Profil de distribution du trafic	Dans la liste déroulante, sélectionnez un profil de distribution du trafic afin de déterminer comment le pare-feu sélectionne un autre chemin d'accès pour le trafic des applications ou des services lorsque les mesures d'état d'un des chemins d'accès privilégiés dépassent le seuil configuré dans le profil de qualité du chemin d'accès dans la règle.

Onglet Cible SD-WAN

- **Politiques** > **SD-WAN** > **Cible**

Sélectionnez l'onglet **Target (Cible)** pour sélectionner les périphériques gérés auxquels Panorama appliquera la règle de politique SD-WAN. Cet onglet est pris en charge uniquement sur le serveur de gestion Panorama.

Champ	Description
Tous (cible tous les périphériques)	Activez (cochez) pour appliquer la règle de politique SD-WAN à tous les périphériques gérés par le serveur de gestion Panorama.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Périphériques	1. Dans l'onglet Périphériques, sur le côté gauche, vous pouvez sélectionner un ou plusieurs filtres pour filtrer les éléments à afficher du côté droit dans la section **Name (Nom)**. 2. Dans la section **Name (Nom)**, sélectionnez un ou plusieurs périphériques auxquels Panorama applique la règle de politique SD-WAN. 3. Activez (cochez) **Filter Selected (Filtres sélectionnés)** pour afficher seulement les périphériques sélectionnés ainsi que le nombre de périphériques.
Étiquettes	Dans l'onglet Étiquettes, **Add (Ajoutez)** une ou plusieurs **Tags (Étiquettes)** qui ont été appliquées aux périphériques. Panorama appliquera la règle SD-WAN aux périphériques identifiés avec les étiquettes spécifiées.  *Pour spécifier où Panorama applique la règle, vous pouvez utiliser soit l'onglet Devices (Périphériques), soit l'onglet Tags (Étiquettes), mais pas les deux.*
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour appliquer la règle de politique SD-WAN à tous les périphériques, sauf les **Devices (Périphériques)** sélectionnés ou les périphériques avec les **Tags (Étiquettes)** spécifiées.

© 2020 Palo Alto Networks, Inc.

Objets

Les objets sont les éléments qui vous permettent de construire, de programmer et de chercher des règles de politique, et les profils de sécurité fournissent une protection contre les menaces dans les règles de sécurité.

Cette section décrit la configuration des profils de sécurité et des objets que vous pouvez utiliser avec les politiques :

- Déplacement, clonage ou rétablissement des objets ou application d'un contrôle prioritaire sur ceux-ci
- Objets > Adresses
- Objets > Groupes d'adresses
- Objets > Régions
- Objets > Applications
- Objets > Groupes d'applications
- Objets > Filtres d'applications
- Objets > Services
- Objets > Groupes de services
- Objets > Étiquettes
- Objets > GlobalProtect > Objets HIP
- Objets > GlobalProtect > Profils HIP
- Objets > Listes dynamiques externes
- Objets > Objets personnalisés
- Objets > Profils de sécurité
- Objets > Profils de sécurité > Protection GTP
- Objets > Profils de sécurité > Protection SCTP
- Objets > Groupes de profils de sécurité
- Objets > Transfert de journaux
- Objets > Authentification
- Objets > Profil de déchiffrement
- Objets > Calendriers

© 2020 Palo Alto Networks, Inc.

Déplacement, clonage ou rétablissement des objets ou application d'un contrôle prioritaire sur ceux-ci

Consultez les rubriques suivantes pour connaître les options qui s'offrent à vous pour modifier les objets existants :

- Déplacement ou clonage d'un objet
- Contrôle prioritaire et rétablissement d'un objet

Déplacement ou clonage d'un objet

Lorsque vous déplacez ou clonez des objets, vous pouvez définir une **Destination** (un système virtuel sur un pare-feu ou un groupe de périphériques sur Panorama™) pour laquelle vous disposez d'autorisations d'accès, y compris l'emplacement partagé.

Pour déplacer un objet, sélectionnez-le dans l'onglet **Objects (Objets)**, cliquez sur **Move (Déplacer)**, sélectionnez **Move to other vsys (Déplacer vers d'autres vsys)** (pare-feu uniquement) ou **Move to other device group (Déplacer vers un autre groupe de périphériques)** (Panorama uniquement), remplissez les champs du tableau suivant, puis cliquez sur **OK**.

Pour cloner un objet, sélectionnez-le dans l'onglet **Objects (Objets)**, cliquez sur **Clone (Cloner)**, remplissez les champs du tableau suivant, puis cliquez sur **OK**.

Paramètres de déplacement/ clonage	Description
Objets sélectionnés	Affiche le nom et l'emplacement actuel (système virtuel ou groupe de périphériques) des politiques ou objets que vous avez sélectionnés pour l'opération.
Destination	Sélectionnez le nouvel emplacement de la politique ou de l'objet : un système virtuel, un groupe de périphériques ou un emplacement partagé. La valeur par défaut est le **Virtual System (Système virtuel)** ou le **Device Group (Groupe de périphériques)** que vous avez sélectionné dans l'onglet **Policies (Politiques)** ou **Objects (Objets)**.
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option (sélectionnée par défaut) pour que le pare-feu ou Panorama affiche la première erreur trouvée et arrête de rechercher d'autres erreurs. Par exemple, une erreur se produit si la **Destination** ne contient aucun objet référencé dans la règle de la politique que vous déplacez. Si vous désélectionnez cette option, le pare-feu ou Panorama trouvera toutes les erreurs avant de les afficher.

Contrôle prioritaire et rétablissement d'un objet

Dans Panorama, vous pouvez imbriquer des groupes de périphériques dans une arborescence pouvant contenir jusqu'à quatre niveaux. Au niveau inférieur, un groupe de périphériques peut avoir des groupes

© 2020 Palo Alto Networks, Inc.

de périphériques parents, grands-parents et arrière-grands-parents à des niveaux supérieurs successifs (collectivement appelés *anciens*) dont le groupe de périphériques de niveau inférieur hérite des politiques et objets. Au niveau supérieur, un groupe de périphériques peut avoir des groupes de périphériques enfants, petits-enfants et arrière-petits-enfants — collectivement appelés *descendants*. Vous pouvez appliquer un contrôle prioritaire sur un objet dans un descendant afin que ses valeurs soient différentes de celles d'un ancien Cette capacité de contrôle prioritaire est activée par défaut. Toutefois, vous ne pouvez pas appliquer un contrôle prioritaire sur des objets partagés ou par défaut (préconfigurés). L'interface Web affiche l'icône  pour indiquer qu'un objet a hérité des valeurs et affiche l'icône  pour indiquer qu'un objet hérité contient des valeurs qui ont été forcées.

- **Appliquer un contrôle prioritaire sur un objet** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le descendant **Device Group (Groupe de périphériques)** qui contiendra la version forcée, sélectionnez l'objet, cliquez sur **Override (Contrôle prioritaire)** et modifiez les paramètres. Vous ne pouvez pas appliquer un contrôle prioritaire sur les paramètres **Name (Nom)** ou **Shared (Partagé)**.
- **Rétablir les valeurs héritées d'un objet dont les valeurs ont été forcées** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le **Device Group (Groupe de périphériques)** contenant la version forcée, sélectionnez l'objet, cliquez sur **Revert (Rétablir)**, puis sur **Yes (Oui)** pour confirmer l'opération.
- **Désactiver le contrôle prioritaire des valeurs d'un objet** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le **Device Group (Groupe de périphériques)** dans lequel se trouve l'objet, cliquez sur le nom de l'objet pour le modifier, sélectionnez l'option **Disable override (Désactiver le contrôle prioritaire)** et cliquez sur **OK**. Les contrôles prioritaires pour cet objet sont alors désactivés dans tous les groupes de périphériques qui héritent de l'objet du **Groupe de périphériques** sélectionné.
- **Rétablir les valeurs héritées de l'emplacement partagé ou des groupes de périphériques anciens des objets dont les valeurs ont eu un contrôle prioritaire dans Panorama** - Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les paramètres de Panorama, sélectionnez **Ancestor Objects Take Precedence (Les objets anciens sont prioritaires)** et cliquez sur **OK**. Vous devez ensuite les valider dans Panorama et dans les groupes de périphériques contenant des valeurs de contrôle prioritaire pour transmettre les valeurs héritées.

© 2020 Palo Alto Networks, Inc.

Objets > Adresses

Un objet d'adresse peut inclure une adresse IPv4 ou une adresse IPv6 (une adresse IP unique, une plage d'adresses ou un sous-réseau), un FQDN ou une adresse générique (une adresse IPv4 suivie d'une barre oblique et d'un masque générique). Un objet d'adresse vous permet de réutiliser cette même adresse ou ce même groupe d'adresses comme adresse source ou de destination dans les règles de politique, les filtres et les autres fonctions du pare-feu sans ajouter chaque adresse manuellement pour chaque instance. Vous créez un objet d'adresses à l'aide de l'interface Web ou de la CLI. Par ailleurs, les modifications doivent faire l'objet d'une opération de validation pour que l'objet soit intégré à la configuration.

Vous devez d'abord **Add (Ajouter)** un nouvel objet d'adresse, puis préciser les valeurs suivantes :

Paramètres de l'objet de l'adresse	Description
Name (Nom)	Saisissez un nom (maximum de 63 caractères) qui décrit les adresses que vous intégrerez à cet objet. Ce nom apparaît dans la liste d'adresses lors de la définition des règles de politique de sécurité. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez partager cet objet d'adresse avec : • **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - Si vous ne sélectionnez pas cette option, l'objet d'adresse est disponible uniquement pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • **Every device group on Panorama (Tous les groupes de périphériques sur Panorama)** - Si vous ne sélectionnez pas cette option, l'objet d'adresse sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet d'adresse dans les groupes de périphériques qui héritent de cet objet. Cette sélection est désactivée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Description	Saisissez une description de l'objet (1 023 caractères maximum).
Type	Spécifiez le type d'objet d'adresses et l'entrée : • **IP Netmask (Masque réseau IP)** - Saisissez l'adresse'A0;IPv4 ou IPv6 ou la plage d'adresses'A0;IP selon la notation suivante : *adresse_ip/masque* or *adresse_IP* où le masque correspond au nombre de valeurs binaires les plus significatives utilisées pour la portion réseau de l'adresse. Idéalement, pour les adresses IPv6, vous indiquez uniquement la partie réseau et non la partie hôte. Par exemple : • **192.168.80.150/32** - indique une adresse. • **192.168.80.0/24** - indique toutes les adresses comprises entre 192.168.80.0 et 192.168.80.255 • **2001:db8::/32**

© 2020 Palo Alto Networks, Inc.

Paramètres de l'objet de l'adresse	Description
	• **2001:db8:123:1::/64** • **IP Range (Plage d'adresses IP)** - Saisissez une plage d'adresses en utilisant le format suivant : *ip_address–ip_address* où les deux extrémités de la plage sont des adresses IPv4 ou des adresses IPv6. Par exemple : 2001:db8:123:1::1-2001:db8:123:1::22 • **Masque générique IP** saisissez une adresse IP générique au format d'une adresse IPv4 suivie d'une barre oblique et d'un masque (qui doivent commencer par zéro) ; par exemple, 10.182.1.1/0.127.248.0. Dans le masque générique, un zéro (0) indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le 0. Dans le masque générique, un bit de un (1) est un bit générique, ce qui indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le 1. Convertissez l'adresse IP et le masque générique en binaire. Pour illustrer la correspondance : sur le fragment de code binaire 0011, un masque générique de 1010 résultats en quatre correspondances (0001, 0011, 1001 et 1011). *Vous pouvez utiliser un objet d'adresse de type Masque générique IP uniquement dans une règle de politique de sécurité.* • **FQDN** : saisissez le nom de domaine. Le FQDN est résolu au moment de la validation. Le FQDN est ultérieurement actualisé selon la TTL du FQDN, si la TTL est supérieure ou égale à la Minimum FQDN Refresh Time (Fréquence d'actualisation minimale du FQDN) ; autrement, le FQDN est actualisé selon la Fréquence d'actualisation minimale du FQDN. Le FQDN est résolu par le serveur DNS du système ou un objet proxy DNS, si un proxy est configuré.
Résoudre	Après avoir sélectionné le type d'adresse et saisi une adresse IP ou un FQDN, cliquez sur **Resolve (Résoudre)** pour voir les FQDN ou les adresses IP associés, respectivement (selon la configuration DNS du pare-feu ou de Panorama). Vous pouvez faire passer un objet d'adresse d'un FQDN à un masque réseau IP et vice-versa. Pour passer d'un FQDN à un Masque réseau IP, cliquez sur **Resolve (Résoudre)** pour voir les adresses IP auxquelles le FQDN est résolu, sélectionnez en une, puis cliquez sur **Use this address (Utiliser cette adresse)**. Le Type d'objet d'adresse est modifié de manière dynamique en un Masque réseau IP et l'adresse IP que vous avez sélectionnée apparaît dans le champ texte. De même, pour que l'objet d'adresse passe d'un Masque réseau IP à un FQDN, cliquez sur **Resolve (Résoudre)** pour voir le nom DNS auquel le Masque réseau est résolu, puis sélectionnez le FQDN et cliquez sur **Use this FQDN (Utiliser ce FQDN)**. Le Type passe à FQDN et le FQDN apparaît dans le champ texte.
Étiquettes	Sélectionnez ou saisissez les étiquettes que vous souhaitez appliquer à cet objet d'adresse. Vous pouvez définir une étiquette ici ou utiliser l'onglet Objets > Étiquettes pour créer de nouvelles étiquettes.

© 2020 Palo Alto Networks, Inc.

Objets > Groupes d'adresses

Pour simplifier la création des politiques de sécurité, les adresses qui requièrent les mêmes paramètres de sécurité peuvent être combinées en groupes d'adresses. Un groupe d'adresses peut être statique ou dynamique.

- Groupes d'adresses dynamiques : un groupe d'adresses dynamique charge ses membres de manière dynamique à l'aide de recherches d'étiquettes et de filtres par étiquette. Les groupes d'adresses dynamiques sont très utiles si vous disposez d'une infrastructure virtuelle étendue, dans laquelle les changements d'emplacement des machines virtuelles et d'adresse'A0;IP sont fréquents. Par exemple, vous avez une configuration de basculement sophistiquée ou configurez fréquemment de nouvelles machines virtuelles et souhaitez appliquer la politique au trafic depuis ou vers la nouvelle machine, sans modifier la configuration/les règles sur le pare-feu.

  Pour utiliser un groupe d'adresses dynamique dans une politique, vous devez effectuer les tâches suivantes :

  - Définissez un groupe d'adresses dynamique et faites-y référence dans une règle de politique.
  - Informez le pare-feu des adresses'A0;IP et des étiquettes correspondantes, de manière à ce que les membres du groupe d'adresses dynamique puissent être formés. Pour ce faire, vous pouvez utiliser des scripts externes qui appellent l'API XML sur le pare-feu ou, si vous disposez d'un environnement VMware, vous pouvez sélectionner **Device (Périphérique)** > **VM Information Sources (Sources d'informations de machine virtuelle)** pour configurer les paramètres du pare-feu.

  les groupes d'adresses dynamiques peuvent également inclure des objets d'adresse définis de manière statique. Si vous créez un objet d'adresse et que vous appliquez les mêmes étiquettes que vous avez affectées à un groupe d'adresses dynamiques, ce dernier inclura tous les objets statiques et dynamiques correspondant aux étiquettes. Vous pouvez ainsi utiliser les étiquettes pour rassembler les objets statiques et dynamiques dans le même groupe d'adresses.
- Groupes d'adresses statiques : Un groupe d'adresses statiques peut inclure des objets d'adresse statiques, des groupes d'adresses dynamiques ou être une combinaison d'objets d'adresses statiques et de groupes d'adresses dynamiques.

  Pour créer un groupe d'adresses, cliquez sur **Add (Ajouter)** et renseignez les champs suivants :

Paramètres du groupe d'adresses	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d'adresses (**63** caractères maximum). Ce nom apparaît dans la liste d'adresses lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe d'adresses soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe d'adresses sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe d'adresses sera uniquement disponible pour

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe d'adresses	Description
	le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce groupe d'adresses dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Description	Saisissez une description de l'objet (1023 caractères maximum).
Type	Sélectionnez **Static (Statique)** ou **Dynamic (Dynamique)**. Pour créer un groupe d'adresses dynamique, utilisez les critères de correspondance pour rassembler les membres à inclure dans le groupe. Définissez les critères **Match (Correspondance)** à l'aide des opérateurs **AND (ET)** et **OR (OU)**. *pour afficher la liste des attributs des critères de correspondance, vous devez avoir configuré le pare-feu pour accéder et récupérer les attributs de la source/ l'hôte. Chaque machine virtuelle sur la(les) source(s) d'informations configurée(s) est enregistrée auprès du pare-feu ; le pare-feu peut sonder la machine pour récupérer les changements d'adresse IP ou de configuration, sans qu'aucune modification ne soit effectuée sur le pare-feu.* Pour un groupe d'adresses statiques, cliquez sur **Add (Ajouter)** et sélectionnez une ou plusieurs **Addresses (Adresses)**. Cliquez sur **Add (Ajouter)** pour ajouter un objet ou un groupe d'adresses au groupe d'adresses. Ce groupe peut contenir des objets d'adresse, ainsi que des groupes d'adresses statiques et dynamiques.
Étiquettes	Sélectionnez ou saisissez les étiquettes que vous souhaitez appliquer à ce groupe d'adresses. Pour plus d'informations sur les étiquettes, voir Objets > Étiquettes.
Nombre de membres et adresses	Après avoir ajouté un groupe d'adresses, la colonne Nombre de membres sur la page **Objects (Objets)** > **Address Groups (Groupes d'adresses)** indique si les objets du groupe sont renseignés dynamiquement ou statiquement. • Pour un groupe d'adresses statiques, vous pouvez afficher le nombre de membres dans le groupe d'adresses. • Pour un groupe d'adresses utilisant des étiquettes pour remplir dynamiquement les membres ou ayant des membres statiques et dynamiques, cliquez sur le lien **More... (Plus...)** dans la colonne Adresse pour afficher les membres. Vous pouvez maintenant visualiser les adresses IP qui sont enregistrées dans le groupe d'adresses. • Le type indique si l'adresse IP est un objet d'adresse statique ou si elle est enregistrée dynamiquement et affiche l'adresse IP.

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe d'adresses	Description
	• L'action vous permet d'**Annuler l'enregistrement des étiquettes** à partir d'une adresse IP. Cliquez sur le lien pour **Ajouter** la source d'enregistrement et spécifier les étiquettes dont il faut annuler l'enregistrement.

© 2020 Palo Alto Networks, Inc.

Objets > Régions

Le pare-feu prend en charge la création de règles de politique qui s'appliquent à des pays spécifiques ou à d'autres régions. L'option région est disponible lors de la définition de la source et de la destination des politiques de sécurité, des politiques de déchiffrement et des politiques DoS. Vous pouvez faire votre choix parmi une liste standard de pays ou utiliser les paramètres régionaux décrits dans cette section pour définir des régions personnalisées à inclure sous forme d'options dans les règles des politiques de sécurité.

Les tableaux suivants décrivent les paramètres régionaux'A0;:

Paramètres régionaux	Description
Name (Nom)	Sélectionnez un nom qui décrit la région. Ce nom apparaît dans la liste d'adresses lors de la définition de politiques de sécurité.
Emplacement géographique	Pour indiquer la latitude et la longitude, sélectionnez cette option et renseignez les valeurs (format xxx.xxxxxx). Ces informations sont utilisées dans les cartes du trafic et des menaces pour définir la portée d'application. Voir Surveillance > Journaux.
Adresses	Renseignez une adresse'A0;IP, une plage d'adresses'A0;IP ou un sous-réseau pour identifier la région, en respectant les formats suivants'A0;: x.x.x.x x.x.x.x-a.a.a.a x.x.x.x/n

© 2020 Palo Alto Networks, Inc.

Objets > Groupes d’utilisateurs dynamiques

Pour créer un groupe d’utilisateurs dynamiques, sélectionnez **Objects (Objets)** > **Dynamic User Groups (Groupes d’utilisateurs dynamiques)**, **Add (Ajoutez)** un nouveau groupe d’utilisateurs dynamiques et configurez les paramètres suivants :

Paramètres de groupe d’utilisateurs dynamiques	Description
Name (Nom)	Saisissez un **Name (Nom)** qui décrit le groupe d'utilisateurs dynamiques (63 caractères maximum). Ce nom apparaît dans la liste d’utilisateurs sources lors de la définition des règles de politique de sécurité. Le nom doit être unique et utiliser uniquement des caractères alphanumériques, des espaces, des traits d'union et des traits de soulignement.
Description	Saisissez une **Description** de l'objet (1 023 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous voulez que les critères de correspondance du groupe d’utilisateurs dynamiques soient disponibles pour tous les groupes de périphériques sur Panorama. *Panorama ne partage pas l’information des membres du groupe avec les groupes de périphériques.* Si vous désélectionnez cette option, les critères de correspondance du groupe d’utilisateurs dynamiques seront uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce groupe d’utilisateurs dynamiques dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Correspondance	**Add Match Criteria (Ajoutez des critères de correspondance)** pour définir les membres dans le groupe d’utilisateurs dynamiques en utilisant les opérateurs **AND (ET)** ou **OR (OU)** pour inclure plusieurs étiquettes. *Lorsque vous Add Match Criteria (Ajoutez des critères de correspondance), uniquement les étiquettes existantes s’afficheront. Vous pouvez sélectionner une étiquette existante ou créer de nouvelles étiquettes.*
Étiquettes	(Optional [Facultatif]) Sélectionnez ou saisissez les étiquettes d’objet statique que vous voulez appliquer sur l’objet de groupe d’utilisateurs dynamiques. Ceci permet d’étiqueter l’objet de groupe d’utilisateurs dynamiques lui-même et non les membres du groupe. Les étiquettes que vous sélectionnez vous permettent de group related items (regrouper des éléments associés) et ne sont pas reliées aux critères de correspondance. Pour plus d’informations sur les étiquettes, voir Objets > Étiquettes.

© 2020 Palo Alto Networks, Inc.

Après avoir ajouté un groupe d'utilisateurs dynamiques, vous pouvez afficher les informations suivantes pour le groupe :

Colonne des groupes d'utilisateurs dynamiques	Description
Location (Emplacement) (Panorama uniquement)	Identifie si les critères de correspondance du groupe d'utilisateurs dynamiques sont disponibles pour tous les groupes d'appareils sur Panorama (**Shared [Partagé]**) ou seulement pour le groupe d'appareils sélectionné.
Users (Utilisateurs)	Sélectionnez **more (plus)** pour voir la liste des utilisateurs dans le groupe d'utilisateurs dynamiques. • Pour ajouter des étiquettes aux utilisateurs pour leur intégration dans le groupe, **Register Users (Enregistrez les utilisateurs)**, puis sélectionnez **Registration Source (Source d'enregistrement)** et les **Tags (Étiquettes)** que vous voulez appliquez à l'utilisateur. Lorsque les étiquettes d'un utilisateur correspondent aux critères de correspondance d'un groupe, le pare-feu ajoute l'utilisateur au groupe d'utilisateurs dynamiques. • (Optional [Facultatif]) Spécifiez un **Timeout (Délai d'expiration)** en minutes (par défaut : 0 ; plage comprise entre 0 et 43 200) pour supprimer les utilisateurs d'un groupe quand le délai spécifié expire. • (Optional [Facultatif]) **Add (Ajoutez)** des **Users (Utilisateurs)** au groupe ou **Delete (Supprimez)** des utilisateurs du groupe. • Pour supprimer des étiquettes des utilisateurs et les empêcher de devenir des membres d'un groupe, sélectionnez les utilisateurs et cliquez sur **Unregister Users (Annuler l'enregistrement des utilisateurs)**, puis sélectionnez **Registration Source (Source d'enregistrement)** et **Tags (Étiquettes)**. • Lorsque vous avez terminer de vérifier ou de modifier la liste des utilisateurs du groupes d'utilisateurs dynamiques, cliquez sur **Close (Fermer)**.

© 2020 Palo Alto Networks, Inc.

Objets > Applications

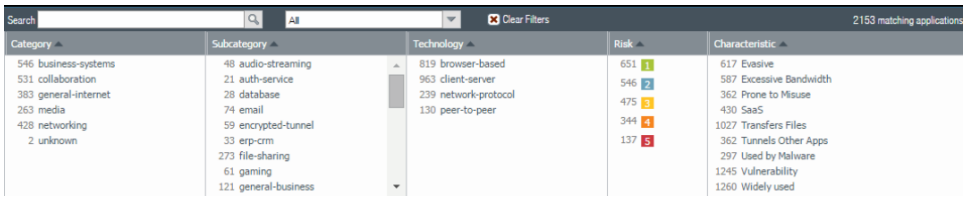
Les rubriques suivantes décrivent la page **Applications**.

Que voulez-vous faire ?	Reportez-vous à la section
Comprendre les paramètres et les attributs de l'application affichés sur la page Applications.	Présentation des applications Actions prises en charge sur les applications
Ajouter une nouvelle application ou modifier une application existante.	Définition des applications

Présentation des applications

La page Applications dresse la liste des divers attributs de chaque définition d'application, tels que le risque relatif pour la sécurité que présente l'application (de 1 à 5). Le risque est évalué sur des critères tels que la capacité de l'application à partager des fichiers, le fait qu'elle soit sujette à une utilisation frauduleuse ou tente de contourner les pare-feu. Plus la valeur est élevée, plus le risque est important.

La partie supérieure de la page affiche une liste des attributs que vous pouvez utiliser pour filtrer la liste, comme illustré ci-dessous. Le nombre à gauche de chaque entrée représente le nombre total d'applications dotées de cet attribut.



Toutes les semaines, le contenu affiche de nouveaux décodeurs et contextes pour lesquels vous pouvez développer des signatures.

Le tableau suivant décrit les détails de l'application (les applications personnalisées et les applications de Palo Alto® Networks peuvent afficher certains ou tous ces champs).

Détails de l'application	Description
Name (Nom)	Nom de l'application.
Description	Description de l'application (255 caractères maximum).
Informations complémentaires	Liens vers des sources en ligne (Wikipédia, Google et Yahoo!) qui présentent des informations supplémentaires sur l'application.
Ports standard	Ports que l'application utilise pour communiquer avec le réseau.
Dépend de	Liste d'autres applications qui sont nécessaires pour que cette application fonctionne. Lors de la création d'une règle de politique

© 2020 Palo Alto Networks, Inc.

Détails de l'application	Description
	pour autoriser l'application sélectionnée, vous devez aussi vérifier que vous autorisez toutes les autres applications dont l'application dépend.
Utilise implicitement	Les autres applications dont dépend l'application sélectionnée, mais que vous n'avez pas besoin d'ajouter à vos règles de politique de Sécurité pour autoriser l'application sélectionnée, car ces applications sont implicitement prises en charge.
Précédemment identifié en tant que	Pour les nouveaux App-ID™ ou les App-ID ayant été modifiés, cet élément indique que l'application a été précédemment identifiée en tant que. Il vous permet d'évaluer si une politique doit être modifiée en fonction des modifications apportées à l'application. Si un App-ID est désactivé, les sessions associées à cette application vont correspondre à la politique de l'application précédemment identifiée. De même, les App-ID désactivés vont apparaître dans les journaux tels qu'ils étaient précédemment identifiés dans l'application.
Refuser l'action	Les App-ID sont développés avec une action de refus par défaut qui dicte la manière dont le pare-feu répond lorsque l'application est incluse dans une règle de politique de sécurité avec une action de refus. L'action de refus par défaut peut indiquer un abandon silencieux ou une réinitialisation TCP. Vous pouvez appliquer un contrôle prioritaire sur cette action par défaut dans la politique de Sécurité.
Caractéristiques	
Évasif	Utilise un port ou un protocole dans un but autre que celui visé initialement et dans l'espoir qu'il traverse un pare-feu.
Bande passante excessive	Utilise de manière régulière 1'A0;Mbit/s minimum dans des conditions normales d'utilisation.
Sujet à une utilisation frauduleuse	Généralement utilisé à des fins malveillantes ou peut être facilement configuré afin d'exposer d'autres utilisateurs en plus de celui visé.
SaaS	Sur le pare-feu, le SaaS (Software as a Service/logiciel à la demande) se caractérise comme service sur lequel le fournisseur de services de l'application détient et gère le logiciel et l'infrastructure mais sur lequel vous gardez un contrôle intégral sur les données, y compris les personnes pouvant créer, accéder, partager et transférer ces données. N'oubliez pas que dans le contexte de caractérisation d'une application, les applications SaaS sont différentes des services Web. Les services Web sont des applications hébergées dont l'utilisateur n'est pas propriétaire des données (par exemple, Pandora) ou dont le service consiste principalement à partager des données fournies par de nombreux abonnés à des fins sociales (par exemple : LinkedIn, Twitter ou Facebook).
Peut transférer des fichiers	Est en mesure de transférer un fichier entre deux systèmes d'un réseau.

© 2020 Palo Alto Networks, Inc.

Détails de l'application	Description
Véhicule d'autres applications	Est en mesure de transporter d'autres applications sur son protocole.
Utilisé par un logiciel malveillant	Un programme malveillant est connu pour utiliser l'application à des fins de propagation, d'attaque ou de vol de données ou est intégré à un programme malveillant.
Contient des vulnérabilités connues	Comporte des vulnérabilités rendues publiques.
Répandue	Concerne plus de 1'A0;000'A0;000 d'utilisateurs.
Poursuivre l'analyse d'autres applications	Indique au pare-feu de continuer à essayer de faire correspondre d'autres signatures d'applications. Si cette option n'est pas sélectionnée, le pare-feu arrêtera de rechercher des correspondances pour l'application dès la première mise en correspondance de la signature.
Caractéristiques SaaS	
Violations des données	Applications qui pourraient avoir divulgué des informations sécurisées à une source non fiables au cours des trois dernières années.
Conditions d'utilisation insuffisantes	Applications offrant de piètres modalités de service qui pourraient compromettre les données de l'entreprise.
Absence de certification	Applications dont la conformité aux programmes ou aux certifications du section, comme SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA ou FEDRAMP est insuffisante.
Faible viabilité financière	Applications qui pourraient cesser leurs activités au cours des 18 à 24 prochains mois.
Aucune restriction IP	Applications sans restrictions IP pour l'accès utilisateur.
par application	
Catégorie	La catégorie de l'application sera l'une des suivantes : • systèmes professionnels • collaboration • Internet grand public • multimédia • réseautage • inconnue
subcategory	Sous-catégorie dans laquelle l'application est classée. Différentes catégories contiennent différentes sous-catégories qui lui sont associées. Par exemple, les sous-catégories de la catégorie Collaboration contiennent E-mail, Partage de fichiers, Messagerie instantanée, Conférence par Internet, Entreprise sociale, Réseau social, Vidéo VoIP et Annonce Web. Alors que les sous-catégories de la catégorie Systèmes professionnels contiennent Service

© 2020 Palo Alto Networks, Inc.

Détails de l'application	Description
	d'autorisation, Base de données, CRM ERP, Activité générale, Gestion, Programmes de bureaux, Mise à jour logicielle et Sauvegarde de la mémoire.
TECHNOLOGIES	La technologie de l'application sera l'une des suivantes : • client/serveur : Une application qui utilise un modèle client/serveur dans lequel un ou plusieurs clients communiquent avec un serveur du réseau. • protocole réseau : Une application qui est généralement utilisée pour la communication entre systèmes et qui simplifie le fonctionnement du réseau. Ceci inclut la plupart des protocoles IP. • poste à poste : Une application qui communique directement avec d'autres clients pour transférer des informations, plutôt que de recourir à un serveur central, afin de simplifier la communication. • basé sur navigateur : Une application dont le fonctionnement dépend d'un navigateur Web.
Risque	Risque affecté à l'application. Pour personnaliser ce paramètre, cliquez sur le lien **Personnaliser**, saisissez une valeur (entre 1 et 5) et cliquez sur **OK**.
Étiquettes	Étiquettes attribuées à une application. **Edit Tags (Modifier les étiquettes)** pour ajouter ou supprimer les étiquettes attribuées à une application.
Options (Options)	
Délai d'expiration de la session	Délai, en secondes, au bout duquel la session de l'application expire en cas d'inactivité (plage allant de 1 à 604 800 secondes). Ce délai d'expiration concerne les protocoles autres que TCP ou UDP. Pour ces derniers, reportez-vous aux lignes suivantes dans ce tableau. Pour personnaliser ce paramètre, cliquez sur le lien **Customize (Personnaliser)**, saisissez une valeur et cliquez sur **OK**.
Délai d'attente TCP (secondes)	Délai d'expiration, en secondes, requis pour mettre fin au débit d'une application TCP (plage allant de 1 à 604 800 secondes). Pour personnaliser ce paramètre, cliquez sur le lien **Customize (Personnaliser)**, saisissez une valeur et cliquez sur **OK**. Une valeur de 0 indique que le minuteur de session général sera utilisé, à savoir 3 600 secondes pour TCP.
Délai d'attente UDP (secondes)	Délai d'expiration, en secondes, requis pour mettre fin au débit d'une application UDP (plage allant de 1 à 604 800 secondes). Pour personnaliser ce paramètre, cliquez sur le lien **Customize (Personnaliser)**, saisissez une valeur et cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

Détails de l'application	Description
Délai d'attente des sessions TCP à moitié fermées (en secondes)	Durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, entre la réception du premier paquet FIN et celle du second paquet FIN ou RST. Si le délai expire, la session sera fermée (plage allant de 1 à 604 800 secondes). Par défaut : si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé. Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre **TCP Half Closed (Délai d'attente des sessions TCP à moitié fermées)** global.
Délai d'attente des sessions TCP en état time_wait (en secondes)	Durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, après la réception du second paquet FIN ou RST. Si le délai expire, la session sera fermée (plage allant de 1 à 600 secondes). Par défaut : si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé. Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre **TCP Time Wait (Délai d'attente des sessions TCP en état time_wait)** global.
compatible App-ID	Indique si l'App-ID est activé ou désactivé. Si un App-ID est désactivé, le trafic de cette application sera traité comme l'App-ID **Previously Identified As (Précédemment identifié en tant que)** dans la politique de sécurité et dans les journaux. Pour les applications ajoutées après la version 490 du contenu, vous pouvez les désactiver pendant que vous passez en revue l'impact de la politique de la nouvelle application. Après avoir passé en revue la politique, vous pouvez **enable (activer)** l'App-ID. Vous pouvez également **disable (désactiver)** une application que vous avez précédemment activée. Sur un pare-feu en mode multi-vsys, vous pouvez désactiver les App-ID séparément dans chaque système virtuel.

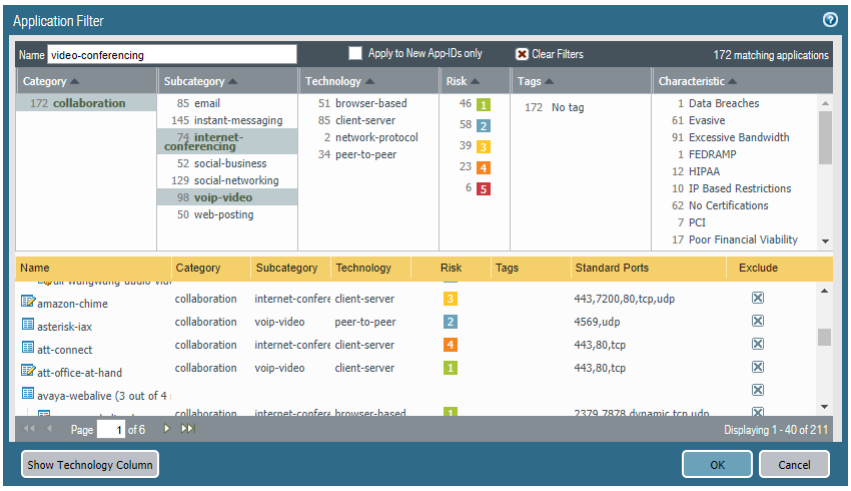
Lorsque le pare-feu n'est pas capable d'identifier une application à l'aide de l'App-ID, le trafic sera classé comme inconnu (« unknown ») : « unknown-tcp » ou « unknown-udp ». Ce comportement s'applique à toutes les applications inconnues, à l'exception de celles qui émule complètement le protocole HTTP. Pour en savoir plus, reportez-vous à la section Surveillance > Botnet.

Vous pouvez créer de nouvelles définitions pour les applications inconnues, puis définir des politiques de sécurité correspondantes. En outre, les applications qui nécessitent les mêmes paramètres de sécurité peuvent être combinées en groupe d'applications pour simplifier la création des politiques de sécurité.

Actions prises en charge sur les applications

Sur cette page, vous pouvez effectuer les actions suivantes :

© 2020 Palo Alto Networks, Inc.

Actions prises en charge pour les applications	Description
Filtrer par application	• Pour rechercher une application spécifique, saisissez le nom ou la description de l'application dans le champ **Rechercher** et appuyez sur **Entrée**. La liste déroulante vous permet de rechercher et de filtrer une application donnée ou d'afficher **All (Toutes)** les applications, les **Custom applications (applications personnalisées)**, les **Disabled applications (applications désactivées)** ou les **Tagged applications (applications étiquetées)**. L'application apparaît dans la liste et les colonnes de filtrage sont mises à jour pour afficher des statistiques relatives aux applications qui correspondent à la recherche. La recherche fonctionne avec des chaînes partielles. Lorsque vous définissez des politiques de sécurité, vous pouvez rédiger des règles qui s'appliquent à toutes les applications correspondant à un filtre sauvegardé. Ces règles sont mises à jour de manière dynamique lorsqu'une nouvelle application est ajoutée par le biais d'une mise à jour du contenu qui correspond au filtre. • Pour filtrer par attributs de l'application affichés sur la page, cliquez sur un élément qui servira de base pour le filtrage. Par exemple, pour limiter la liste à la catégorie Collaboration, cliquez sur **Collaboration (Collaboration)** pour que la liste n'affiche que les applications correspondantes.  • Pour filtrer la liste en fonction d'autres colonnes, sélectionnez une entrée dans ces colonnes. Le filtrage est appliqué selon un ordre précis : Les filtres Catégorie sont appliqués en premier, suivis des filtres Sous-catégorie, puis des filtres Technologie et, enfin, des filtres Charactéristiques. Par exemple, si vous appliquez les filtres Catégorie, Sous-catégorie et Risque, la colonne Technologie sera automatiquement limitée aux technologies correspondant aux catégories et sous-catégories sélectionnées, même si un filtre Technologie n'est pas explicitement appliqué. Lorsque vous appliquez un filtre, la liste des applications sera automatiquement mise à jour. Pour créer un nouveau filtre d'application, voir Objets > Filtres d'application.

© 2020 Palo Alto Networks, Inc.

Actions prises en charge pour les applications	Description
Ajouter une nouvelle application.	Pour ajouter une nouvelle application, reportez-vous à la section Définition des applications.
Afficher ou personnaliser les détails de l'application.	Cliquez sur le lien du nom de l'application pour afficher la description de l'application, y compris le port standard et les caractéristiques de l'application ainsi que le risque. Pour plus d'informations sur les paramètres de l'application, consultez la section Définition des applications. Si l'icône située à gauche du nom de l'application comporte un crayon jaune (), l'application est une application personnalisée.
Désactiver une application	Vous pouvez **Désactiver** une application (ou plusieurs applications) de sorte que la signature de l'application ne corresponde pas au trafic. Les règles de sécurité définies pour bloquer, autoriser ou mettre en œuvre une application correspondante ne sont pas appliquées au trafic de l'application si celle-ci est désactivée. Vous pouvez choisir de désactiver une application incluse avec une nouvelle version du contenu car la mise en œuvre de la politique dans l'application risque de changer lorsque celle-ci est uniquement identifiée. Par exemple, le pare-feu autorise une application identifiée en tant que trafic de type navigation Web avant l'installation d'une nouvelle version du contenu ; après avoir installé la mise à jour du contenu, l'application uniquement identifiée ne correspondra plus à la règle de Sécurité autorisant le trafic de type navigation Web. Dans ce cas, vous pouvez choisir de désactiver l'application afin que le trafic correspondant à la signature de l'application continue d'être classé en tant que trafic de type navigation Web et soit autorisé.
Activer une application	Vous pouvez sélectionner une application désactivée et la **Enable (Activer)** de sorte que le pare-feu puisse gérer l'application conformément à vos politiques de sécurités configurées.
Importer une application	Pour importer une application, cliquez sur **Import (Importer)**. Accédez au fichier et sélectionnez le système virtuel cible dans la liste déroulante **Destination**.
Exporter une application	Pour exporter une application, sélectionnez cette option correspondant à l'application et cliquez sur **Export (Exporter)**. Suivez les invites pour sauvegarder le fichier.
Exporter un tableau de configuration des applications.	Exportez les informations sur les applications au format **PDF/CSV**. Seules les colonnes qui sont visibles dans l'interface Web sont exportées. Consultez la section Exportation des données du tableau de configuration.
Évaluer l'impact des politiques après l'installation d'une nouvelle version du contenu	Il est nécessaire de **Réviser les politiques** pour évaluer la mise en œuvre basée sur les politiques pour les applications avant et après l'installation d'une version du contenu. La boîte de dialogue Évaluer les politiques permet d'évaluer l'impact d'une politique sur les nouvelles applications incluses dans une version téléchargée du contenu. Cette boîte de

© 2020 Palo Alto Networks, Inc.

Actions prises en charge pour les applications	Description
	dialogue vous permet d'ajouter ou de supprimer une application en attente (une application téléchargée avec une version du contenu, mais qui n'est pas installée sur le pare-feu) dans ou depuis une règle de politique de Sécurité existante. Les modifications apportées aux politiques d'applications en attente ne seront effectives qu'après avoir installé la version du contenu correspondant. Vous pouvez également accéder à la boîte de dialogues Réviser les politiques lors du téléchargement et de l'installation de versions de contenu sur la page **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
Étiqueter une application	Une étiquette prédéfinie nommée **sanctioned (approuvée)** est disponible pour que vous étiquetiez des applications SaaS. Bien qu'une application SaaS soit identifiée en tant que **Saas=yes (Saas=oui)** dans caractéristiques de l'application, vous pouvez utiliser l'étiquette approuvée pour n'importe quelle application. *Étiquetez l'application en tant que sanctioned (approuvée) pour permettre de distinguer le trafic des applications SaaS approuvées du trafic des applications SaaS non approuvées, par exemple, lorsque vous examinez le rapport d'utilisation d'application SaaS ou lorsque vous évaluez les applications sur votre réseau.* Sélectionnez une application, cliquez sur **Edit Tags (Modifier les étiquettes)** et à partir de la liste déroulante, sélectionnez l'étiquette **Sanctioned (approuvée)** prédéfinie pour identifier toute application que vous souhaitez explicitement autoriser sur votre réseau. Lorsque vous générez le rapport d'utilisation de l'application SaaS (voir Surveillances > Rapports au format PDF > Utilisation de l'application SaaS), vous pouvez comparer les statistiques sur l'application que vous avez approuvée par rapport aux applications SaaS non approuvées qui sont utilisées sur votre réseau. Lorsque vous étiquetez une application comme étant approuvée, les restrictions suivantes s'appliquent : • L'étiquette Approuvée ne peut être appliquée à un groupe d'applications. • L'étiquette Approuvée ne peut être appliquée au niveau **Shared (Partagé)** ; vous ne pouvez étiqueter une application que par groupe de périphériques ou par système virtuel. • L'étiquette Approuvée ne peut être utilisée pour étiqueter des applications comprises dans une application incorporante, comme facebook-mail, qui fait partie de l'application incorporante Facebook. Vous pouvez également **Remove tag (Supprimer l'étiquette)** ou **Override tag (Appliquer un contrôle prioritaire sur l'étiquette)**. L'option de contrôle prioritaire n'est offerte que sur un pare-feu qui a hérité de paramètres d'un groupe de périphériques qui ont été transmis par Panorama.

© 2020 Palo Alto Networks, Inc.

Définition des applications

Sélectionnez **Objects (Objets)** > **Applications** pour **Add (Ajouter)** une nouvelle application personnalisée à évaluer par le pare-feu lors de l'exécution de politiques.

Paramètres de la nouvelle application	Description
Onglet Configuration	
Name (Nom)	Saisissez le nom de l'application (31 caractères maximum). Ce nom apparaît dans la liste d'applications lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des points, des tirets et des caractères de soulignement. Le caractère final doit être une lettre.
Partagé	Sélectionnez cette option si vous souhaitez que l'application soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'application sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, l'application sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet applicatif pour les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Description	Saisissez une description de l'application à titre de référence générale (255 caractères maximum).
Catégorie	Sélectionnez la catégorie de l'application, par exemple **email (courrier électronique)** ou **database (base de données)**. La catégorie est utilisée pour générer le diagramme du Top 10 des catégories d'applications et à des fins de filtrage (reportez-vous à la section ACC).
subcategory	Sélectionnez la sous-catégorie de l'application, par exemple **email (courrier électronique)** ou **database (base de données)**. La sous-catégorie est utilisée pour générer le diagramme du Top 10 des catégories d'applications et à des fins de filtrage (reportez-vous à la section ACC).
TECHNOLOGIES	Sélectionnez la technologie de l'application.
App parent	Désignez une application parent pour cette application. Ce paramètre s'applique lorsqu'une session correspond à la fois à l'application parent et à l'application personnalisée'A0;; toutefois, l'application personnalisée est reportée car elle est plus spécifique.

© 2020 Palo Alto Networks, Inc.

Paramètres de la nouvelle application	Description
Risque	Sélectionnez le niveau de risque associé à cette application (1 = le plus faible, 5 = le plus élevé).
Caractéristiques	Sélectionnez les caractéristiques de l'application qui peuvent présenter un risque pour cette dernière. Pour obtenir une description de chaque caractéristique, reportez-vous à la section Caractéristiques.
Onglet Avancé	
Port	Si l'application utilise le protocole TCP et/ou UDP, sélectionnez **Port** et saisissez une ou plusieurs combinaisons de protocole et de numéro de port (une entrée par ligne). Le format courant est : *<protocole>/<port>* où le *<port>* est un numéro de port unique, ou **dynamic (dynamique)** en cas d'attribution de port dynamique. Exemples'A0;: TCP/dynamic ou UDP/32. Ce paramètre est appliqué lors de l'utilisation de la valeur **app-default (app-défaut)** dans la colonne Service d'une règle de sécurité.
Protocole IP	Pour indiquer un protocole IP autre que TCP ou UDP, sélectionnez **IP Protocol (Protocole IP)** et saisissez le numéro de protocole (de 1 à 255).
Type ICMP	Pour spécifier un type Internet Control Message Protocol version 4 (ICMP), sélectionnez **ICMP Type (Type ICMP)** et saisissez le numéro de type (plage 0-255).
Type ICMP6	Pour spécifier un type ICMPv6 (Internet Control Message Protocol/ protocole de message de contrôle Internet version 6), sélectionnez **ICMP6 Type (Type ICMP6)** et saisissez le numéro de type (plage 0-255).
None	Pour spécifier des signatures indépendantes de tout protocole, sélectionnez **None (Aucun)**.
délai d'expiration	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé. Cette valeur est utilisée pour les protocoles autres que TCP et UDP dans tous les cas et pour les délais d'attente TCP et UDP lorsque ces derniers ne sont pas définis.
Délai d'attente TCP	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application TCP inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé.
Délai d'attente UDP	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application UDP inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé.

© 2020 Palo Alto Networks, Inc.

Paramètres de la nouvelle application	Description
Délai d'attente des sessions TCP à moitié fermées	Saisissez la durée maximale pendant laquelle une session reste dans la table des sessions, entre la réception du premier FIN et celle du second FIN ou RST. Si le délai expire, la session est fermée. Par défaut : Si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé (intervalle compris entre 1 et 604 800 secondes). Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre global Délai d'attente des sessions TCP à moitié fermées.
Délai d'attente des sessions TCP en état time_wait	Saisissez la durée maximale pendant laquelle une session reste dans la table des sessions, après la réception du second FIN ou RST. Si le délai expire, la session est fermée. Par défaut : Si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé (intervalle compris entre 1 et 600 secondes). Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre global Délai d'attente des sessions TCP en état time_wait.
Analyse en cours	Sélectionnez les types d'analyse que vous voulez autoriser, en fonction des profils de sécurité (types de fichier, modèles de données et virus).
Onglet Signatures	
Signatures	Cliquez sur **Add (Ajouter)** pour ajouter une nouvelle signature, et renseignez les informations suivantes : • **Signature Name (Nom de la signature)** - Saisissez un nom permettant d'identifier la signature. • **Comment (Commentaire)** - Saisissez une description (facultatif). • **Ordered Condition Match (Correspondance de l'état ordonné)** - Indiquez si l'ordre dans lequel les conditions de la signature sont définies a son importance. • **Scope (Portée)** - Indiquez s'il faut appliquer cette signature à la **Transaction** en cours seulement pendant toute la **Session** utilisateur. Précisez les conditions qui identifient la signature. Ces conditions servent à générer la signature que le pare-feu utilise pour faire correspondre les modèles de l'application et contrôler le trafic : • Pour ajouter une condition, sélectionnez **Add And Condition (Ajouter une condition AND)** ou **Add Or Condition (Ajouter une condition OR)**. Pour ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Add Condition (Ajouter une condition)**. • Sélectionnez un **Operator (Opérateur)** dans la liste déroulante. Les options sont les suivantes : **Pattern Match (Correspondance des modèles)**, **Greater Than (Supérieur à)**, **Less Than (Inférieur à)** et **Equal To (Egal à)**, et précisez les options suivantes : (Pour la correspondance des modèles uniquement)

© 2020 Palo Alto Networks, Inc.

Paramètres de la nouvelle application	Description
	• **Context (Contexte)** - Choisissez parmi les contextes disponibles. Ces contextes sont mis à jour à l'aide des mises à jour de contenu dynamiques. • **Pattern (Modèle)** - Indiquez une expression régulière pour préciser des valeurs de chaîne uniques qui s'appliquent à l'application personnalisée. *Exécutez une capture de paquets pour identifier le contexte. Reportez-vous à la section Syntaxe des règles des modèles pour connaître les règles concernant les expressions régulières.* (Pour les options Supérieur à, Inférieur à) • **Context (Contexte)** - Choisissez parmi les contextes disponibles. Ces contextes sont mis à jour à l'aide des mises à jour de contenu dynamiques. • **Value (Valeur)** - Précisez une valeur pour la mise en correspondance (intervalle compris entre 0 et 4 294 967 295). • **Qualifier and Value (Qualificatif et Valeur)** - (Facultatif) Ajoutez des paires qualificatif/valeur. (Pour l'option Égal à uniquement) • **Context (Contexte)** – Sélectionnez parmi les requêtes inconnues et les réponses pour le protocole TCP ou UDP (par exemple, unknown-req-tcp) ou parmi les autres contextes disponibles via les mises à jour du contenu dynamiques (par exemple, dnp3-req-func-code). Pour les requêtes inconnues et les réponses pour le protocole TCP ou UDP, précisez : • **Position** - Faites votre choix parmi les quatre premiers ou les quatre seconds octets de la charge utile. • **Mask (Masque)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xffffff00. • **Value (Valeur)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xaabbccdd. Pour tous les autres contextes, précisez une **Value (Valeur)** qui est pertinente à l'application. Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.

Il n'est pas nécessaire de définir des signatures pour l'application si celle-ci est utilisée uniquement dans des règles de contrôle prioritaire sur l'application.

© 2020 Palo Alto Networks, Inc.

Objets > Groupes d'applications

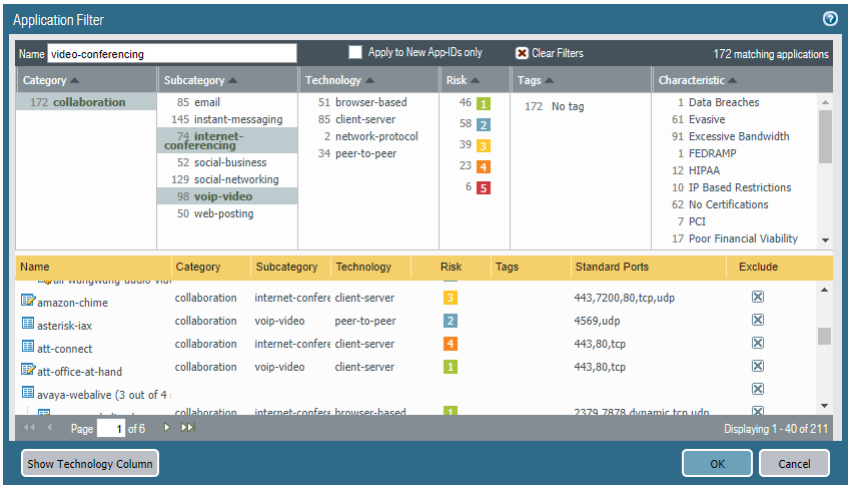
Pour simplifier la création de politiques de sécurité, les applications qui requièrent les mêmes paramètres de sécurité peuvent être combinées en créant un groupe d'applications. (Pour définir une nouvelle application, reportez-vous à la section Définition des applications.)

Paramètres du nouveau groupe d'applications	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d'applications (31 caractères maximum). Ce nom apparaît dans la liste d'applications lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe d'applications soit disponible pour : Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe d'applications sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe d'applications sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de groupe d'applications dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Applications	Cliquez sur **Add (Ajouter)** et sélectionnez des applications, des filtres d'applications et/ou d'autres groupes d'applications à inclure dans ce groupe.

© 2020 Palo Alto Networks, Inc.

Objets > Filtres d'applications

Les filtres d'application permettent de simplifier les recherches répétées. Pour définir un filtre d'application, vous devez **Ajouter** et saisir un nom pour votre nouveau filtre. Dans la partie supérieure de la fenêtre, cliquez sur un élément qui servira de base pour le filtrage. Par exemple, pour limiter la liste à la catégorie Collaboration, cliquez sur **collaboration**.



Pour filtrer la liste en fonction d'autres colonnes, sélectionnez une entrée dans ces colonnes. Le filtrage est successif : d'abord par catégorie, suivi du filtrage par sous-catégorie, par technologie, par risque, par étiquette et enfin par caractéristique.

Lorsque vous sélectionnez les filtres, la liste des applications qui s'affichent sur la page est automatiquement mise à jour.

© 2020 Palo Alto Networks, Inc.

Objets > Services

Lorsque vous définissez des politiques de sécurité pour des applications spécifiques, vous pouvez sélectionner un ou plusieurs services pour limiter les numéros de ports que les applications peuvent utiliser. Le service par défaut est **indifférent**, ce qui autorise tous les ports TCP et UDP. Les services HTTP et HTTPS sont prédéfinis, mais vous pouvez ajouter des définitions supplémentaires. Les services qui sont souvent affectés ensemble peuvent être combinés en groupe de services pour simplifier la création de politiques de sécurité (reportez-vous à la section Objets > Groupes de services).

Par ailleurs, vous pouvez utiliser ces objets de services pour définir des délai d'expiration de session selon le service, ce qui veut dire que vous pouvez appliquer différents délai d'expiration à différents groupes d'utilisateurs, et ce, même lorsque ces groupes utilisent le même service TCP ou UDP ou, si vous passez d'une politique de sécurité basée sur les ports avec applications personnalisées à une politique de sécurité basée sur les applications, vous pouvez facilement conserver vos délai d'expiration d'applications personnalisés.

Le tableau suivant décrit les paramètres des services'A0;:

Paramètres des services	Description
Name (Nom)	Saisissez un nom pour le service (**63** caractères maximum). Ce nom apparaît dans la liste de services lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du service (1023 caractères maximum).
Partagé	Sélectionnez cette option si vous souhaitez que l'objet de service soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'objet de service sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, l'objet de service sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de service dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Protocole	Sélectionnez le protocole utilisé par le service (**TCP** ou **UDP**).
Port de destination	Saisissez le numéro de port de destination (de 0 à 65535) ou la plage de numéros de ports (port1-port2) utilisé(e) par le service. Utilisez des virgules pour séparer les ports ou les plages. Le port de destination doit être renseigné.

© 2020 Palo Alto Networks, Inc.

Paramètres des services	Description
Port source	Saisissez le numéro de port source (de 0 à 65535) ou la plage de numéros de ports (port1-port2) utilisé(e) par le service. Utilisez des virgules pour séparer les ports ou les plages. Le port source est facultatif.
Délai d'expiration de la session	Définissez le délai d'expiration de la session pour le service : • **Inherit from application (Hériter de l'application)** (par défaut) : aucun délai d'expiration basé sur le service n'est appliqué ; c'est le délai d'expiration des applications qui est appliqué. • **Override (Exercer un contrôle prioritaire)** : définissez un délai d'expiration de la session personnalisé pour le service. Continuez à renseigner les champs Délai d'expiration TCP, Délai d'attente des sessions TCP à moitié fermées et Délai d'attente TCP.
Les paramètres suivants ne s'affichent que si vous choisissez de remplacer les délais d'expiration des applications et de créer des délais d'expiration de session personnalisés pour un service :	
Délai d'attente TCP	Définissez la durée maximale, en secondes, pendant laquelle une session TCP peut demeurer ouverte après le début de la transmission des données. Lorsque ce délai expire, la session est fermée. La plage est comprise entre 1 et 604 800. La valeur par défaut est de 3 600 secondes.
Délai d'attente des sessions TCP à moitié fermées	Définissez la durée maximale, en secondes, pendant laquelle une session demeure ouverte lorsqu'un seul côté de la connexion a tenté de mettre fin à la connexion. Ce paramètre s'applique à : • La période de temps après que le pare-feu a reçu le premier paquet FIN (ce qui indique qu'un côté de la connexion tente de mettre fin à la session), mais avant qu'il ne reçoive le second paquet FIN (ce qui indique que l'autre côté de la connexion met fin à la session) • La période de temps avant la réception d'un paquet RST (ce qui indique une tentative de rétablir la connexion). Si le délai expire, la session est fermée. La plage est comprise entre 1 et 604 800. La valeur par défaut est de 120 secondes.
Délai d'attente TCP	Définissez la durée maximale, en secondes, pendant laquelle une session demeure ouverte après la réception du second paquet FIN requis pour mettre fin à la session ou après réception d'un paquet RST visant à rétablir une connexion. Lorsque le délai expire, la session est fermée. La plage est comprise entre 1 et 600. La valeur par défaut est de 15 secondes.

© 2020 Palo Alto Networks, Inc.

Objets > Groupes de services

Pour simplifier la création de politiques de sécurité, vous pouvez combiner les services qui disposent des mêmes paramètres de sécurité en groupes de services. Pour définir de nouveaux services, reportez-vous à la section Objets > Services.

Le tableau suivant décrit les paramètres des groupes de services'A0;:

Paramètres des groupes de services	Description
Name (Nom)	Saisissez un nom pour le groupe de services (**63** caractères maximum). Ce nom apparaît dans la liste de services lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe de services soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe de services sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe de services sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de groupe de service dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Service (Service)	Cliquez sur **Add (Ajouter)** pour ajouter des services au groupe. Faites votre sélection dans la liste déroulante ou cliquez sur **Service** en bas de la liste déroulante et renseignez les paramètres. Reportez-vous à la section Objets > Services pour obtenir une description des paramètres.

© 2020 Palo Alto Networks, Inc.

Objets > Étiquettes

Les étiquettes vous permettent de regrouper des objets à l'aide de mots-clés ou d'expressions. Vous pouvez appliquer des étiquettes à des objets d'adresse, à des groupes d'adresses (statiques et dynamiques), à des applications, à des zones, à des services, à des groupes de services et à des règles de politique. Vous pouvez aussi utiliser un profil d'interface SD-WAN pour appliquer une étiquette de liens à une interface Ethernet. Vous pouvez utiliser des étiquettes pour trier ou filtrer des objets, mais aussi pour distinguer visuellement des objets selon leurs couleurs. Lorsque vous appliquez une couleur à une étiquette, l'onglet **Policy (Politique)** affiche l'objet avec sa couleur d'arrière-plan.

Vous devez créer une étiquette avant de pouvoir regrouper des règles à l'aide de cette étiquette. Après avoir affecté des règles regroupées par étiquette, **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher une représentation visuelle de votre base de règles de politique selon les étiquettes affectées. Lorsque vous affichez votre base de règles en tant que groupes, l'ordre de la politique et la priorité sont maintenus. Dans cette vue, sélectionnez l'étiquette de groupe pour afficher toutes les règles groupées en fonction de cette étiquette.

Une étiquette prédéfinie nommée **Sanctioned (Sanctionné)** est disponible pour les applications d'étiquetage (**Objects (Objets)** > **Applications**). Ces étiquettes sont requises pour suivre avec précision (Surveillance > Rapports PDF> Utilisation de l'application SaaS).

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment créer des étiquettes ?	Création d'étiquettes
Comment puis-je afficher la base de règles en tant que groupes ?	Afficher la base de règles en tant que groupes
Rechercher des règles contenant des étiquettes. Regrouper des règles en utilisant des étiquettes. Afficher les étiquettes d'une politique. Appliquer les étiquettes à la politique.	Gestion des étiquettes
Vous souhaitez en savoir plus ?	Reportez-vous à la section Politique. Reportez-vous à la section Créer une étiquette de liens pour un lien SD-WAN.

Création d'étiquettes

- **Objects (Objets)** > **Tags (Étiquettes)**

Sélectionnez **Tags (Étiquettes)** pour créer une étiquette, affecter une couleur ou supprimer, renommer et cloner des étiquettes. Chaque objet peut comporter jusqu'à 64 étiquettes ; lorsqu'un objet dispose de plusieurs étiquettes, il affiche la couleur de la première étiquette appliquée.

Sur le pare-feu, l'onglet **Tags (Étiquettes)** affiche les étiquettes que vous avez définies localement sur le pare-feu ou transférées depuis Panorama vers le pare-feu. Sur Panorama, l'onglet **Tags (Étiquettes)**

© 2020 Palo Alto Networks, Inc.

affiche les étiquettes que vous définissez sur Panorama. Cet onglet n'affiche pas les étiquettes qui sont dynamiquement récupérées des sources d'informations VM définies sur le pare-feu pour former des groupes d'adresses dynamiques et n'affiche pas les étiquettes qui sont définies à l'aide de l'API XML ou REST.

Lorsque vous créez une nouvelle étiquette, elle est automatiquement créée dans le système virtuel ou dans le groupe de périphériques actuellement sélectionné sur le pare-feu ou sur Panorama.

Paramètres des étiquettes	Description
Name (Nom)	Saisissez un nom de tag unique (127 caractères maximum). Ce nom n'est pas sensible à la casse.
Partagé	Sélectionnez cette option si vous souhaitez que l'étiquette soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'étiquette est uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez (décochez) cette option, l'étiquette sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette étiquette dans les groupes de périphériques qui héritent de l'étiquette. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'étiquette.
Couleur	Sélectionnez une couleur de la palette de couleurs dans la liste déroulante (la valeur par défaut est None [Aucune]).
Commentaires	Ajoutez une étiquette ou une description pour décrire l'utilisation à laquelle l'étiquette est destinée.

- Ajouter une étiquette : **Add (Ajoutez)** une étiquette, puis remplissez les champs suivants :

  Vous pouvez également créer une nouvelle étiquette lors de la création ou de la modification d'une politique dans l'onglet **Policies (Politiques)**. L'étiquette est automatiquement créée dans le groupe de périphériques ou dans le système virtuel actuellement sélectionné.
- Modifier une étiquette : Cliquez sur une étiquette pour modifier ou renommer une étiquette ou pour les affecter une couleur.
- Supprimer une étiquette : Cliquez sur **Delete (Supprimer)**, puis sélectionnez l'étiquette. Vous ne pouvez pas supprimer d'étiquette prédéfinie.
- Déplacer ou cloner une étiquette : Les options permettant de déplacer ou de cloner une étiquette vous permettent de copier une étiquette ou da le déplacer vers un autre Groupe de périphériques ou vers un autre Système virtuel sur les pare-feu pouvant comporter plusieurs systèmes virtuels.

  Déplacez ou clonez et sélectionnez l'étiquette. Sélectionnez l'emplacement de **Destination** (Groupe de périphériques ou Système virtuel). Désélectionnez (décochez) l'option **Error out on first detected error in validation (Erreur sortante dès la première erreur détectée lors de la validation)** pour que le processus de validation identifie toutes les erreurs de l'objet avant de les afficher. Cette option est activée par

© 2020 Palo Alto Networks, Inc.

défaut, et le processus de validation s'arrête dès la détection de la première erreur et affiche uniquement l'erreur.

- Appliquer un contrôle prioritaire ou Rétablir un tag (Panorama uniquement) : L'option **Override (Contrôle prioritaire)** est disponible uniquement si vous n'aviez pas sélectionné l'option **Disable override (Désactiver le contrôle prioritaire)** lors de la création de l'étiquette. L'option **Override (Contrôle prioritaire)** vous permet d'appliquer un contrôle prioritaire sur la couleur assignée à l'étiquette qui a été héritée d'un groupe de périphériques partagés ou ancêtres. Le champ **Location (Emplacement)** correspond au groupe de périphériques actuel. Vous pouvez également **Disable override (Désactiver le contrôle prioritaire)** pour empêcher les tentatives ultérieures d'exercer un contrôle prioritaire.

  Revert (Annulez) les modifications pour annuler les récentes modifications apportées à une étiquette. Lors du rétablissement d'une étiquette, le champ **Location (Emplacement)** affiche le groupe de périphériques ou le système virtuel ayant transmis l'étiquette.

Afficher la base de règles en tant que groupes

- **Policies (Politique)** > **<Rulebase Type> (<Type de base de règles>)**

Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher la base de règles de la politique au moyen de l'étiquette de groupe. Lorsque vous affichez votre base de règles en tant que groupes, l'ordre de la politique et la priorité sont maintenus. Dans cette vue, sélectionnez l'étiquette de groupe pour afficher toutes les règles groupées en fonction de cette étiquette.

Lorsque vous affichez votre base de règle en tant que groupes, cliquez sur **Group (Groupe)** pour déplacer, modifier, supprimer ou cloner toutes les règles dans le groupe d'étiquettes sélectionné. Le tableau suivant décrit les options de gestion des règles qui sont disponibles lorsque vous affichez votre base de règle en tant que groupes.

Option	Description
Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques	Déplace toutes les règles de politique du groupe d'étiquettes sélectionné vers une autre base de règles ou groupe de périphériques.
Modifier le groupe de toutes les règles	Déplace toutes les règles du groupe d'étiquettes sélectionné vers un autre groupe d'étiquettes.
Déplacer toutes les règles du groupe	Déplace toutes les règles du groupe d'étiquettes sélectionné au sein de la base de règles.
Supprimer toutes les règles du groupe	Supprimer toutes les règles du groupe d'étiquettes sélectionné.
Cloner toutes les règles du groupe	Clone toutes les règles du groupe d'étiquettes sélectionné.

Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques

Si vous devez réorganiser votre base de règles, sélectionnez le groupe d'étiquettes qui contient les règles que vous souhaitez déplacer et **Move Rules in Group to Different Rulesbase or Device Group (Déplacez les règles du groupe vers une autre base de règles ou un autre groupe de périphériques)** pour les réaffecter

© 2020 Palo Alto Networks, Inc.

à une autre base de règles ou à un autre groupe de périphériques (plutôt que de déplacer chaque règle individuellement). Le groupe de périphériques doit déjà exister (vous ne pouvez le créer lors du processus) avant de déplacer les règles d'un groupe d'étiquettes vers un autre groupe de périphériques. De plus, vous pouvez déplacer les règles d'un groupe d'étiquettes vers une autre base de règles faisant partie du même groupe de périphériques.

Pour déplacer les règles vers une autre base de règles ou vers un autre groupe de périphériques, saisissez les informations suivantes :

Champ	Description
Destination	Le groupe de périphériques cible pour le déplacement des règles de politique.
(Panorama uniquement) Type de destination	Sélectionnez si vous souhaitez modifier les règles vers la **Pre-Rulebase (Base de règles avant)** ou vers la **Post-Rulebase (Base de règles après)** du groupe de périphériques de destination.
Ordre des règles	Sélectionnez l'endroit de la base de règles où modifier les règles. Vous avez le choix entre les actions suivantes'A0;: • **Move Top (Déplacer vers le haut)** : déplacez les règles clonées au haut de la base de règles du groupe de périphériques de destination. • **Move Bottom (Déplacer vers le bas)** : déplacez les règles à la fin de la base de règles du groupe de périphériques de destination. • **Before Rule (Avant la règle)** : déplacez les règles avant la règle sélectionnée de la base de règles du groupe de périphériques de destination. • **After Rule (Après la règle)** : déplacez les règles après la règle sélectionnée de la base de règles du groupe de périphériques de destination.
Erreur sortante dès la première erreur détectée lors de la validation	Cochez la case pour déterminer comment les erreurs décelées au cours de la validation s'affichent. Si elle est cochée, chaque erreur s'affiche individuellement. Si elle est décochée, les erreurs sont groupées et s'affichent en tant qu'une seule erreur. Les erreurs détectées au cours de la validation entraînent l'échec du déplacement. Aucune règle n'est ainsi déplacée dans le groupe de périphériques de destination.

Modifier le groupe de toutes les règles

Plutôt que de modifier chaque règle, **Change Group of All Rules (Modifiez le groupe de toutes les règles)** pour déplacer un ensemble complet de règles de politique d'un groupe d'étiquettes à un autre groupe d'étiquettes existant. L'ordre des règles au sein du groupe d'étiquettes est maintenu lorsque celles-ci sont déplacées vers le nouveau groupe d'étiquettes. Vous avez toutefois le choix de placer les nouvelles règles devant les règles du groupe d'étiquettes de destination, ou après.

Pour déplacer les règles vers un autre groupe d'étiquettes, précisez le groupe d'étiquettes de destination et l'endroit où placer les règles déplacées.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Sélectionner un groupe pour son ordre d'apparition	Sélectionnez le groupe d'étiquettes de destination.
Déplacer vers le haut	**Move Top (Déplacer vers le haut)** insère les règles au haut du groupe d'étiquettes de destination.
Déplacer vers le bas	**Move botton (Déplacer vers le bas)** insère les règles au bas du groupe d'étiquettes de destination.

Déplacer toutes les règles du groupe

Plutôt que de réorganiser chaque règle individuellement, **Move All Rules in Group (Déplacer toutes les règles du groupe)** pour déplacer toutes les règles dans le groupe d'étiquettes sélectionné vers le haut ou le bas de la hiérarchie de la règle. L'ordre des règles déplacées au sein du groupe d'étiquettes est maintenu lorsque vous déplacez le groupe d'étiquettes. Vous avez toutefois le choix de placer les règles devant les règles du groupe d'étiquettes de destination, ou après.

Pour déplacer les règles, précisez le groupe d'étiquettes de destination et l'endroit où placer les règles déplacées.

Champ	Description
Sélectionner un groupe pour son ordre d'apparition	Sélectionnez le groupe d'étiquettes de destination.
Déplacer vers le haut	**Move Top (Déplacer vers le haut)** insère les règles avant le groupe d'étiquettes de destination.
Déplacer vers le bas	**Move botton (Déplacer vers le bas)** insère les règles après le groupe d'étiquettes de destination.

Supprimer toutes les règles du groupe

Pour simplifier la gestion des règles, vous pouvez **Delete All Rules in Group (Supprimer toutes les règles du groupe)** afin de réduire vos risques de sécurité et de maintenir la base de règles de politique organisée en supprimant les règles non voulues ou non utilisées qui sont associées à un groupe d'étiquettes sélectionné.

Cloner toutes les règles du groupe

Plutôt que de recréer manuellement des règles de politique existantes dans un groupe d'étiquettes, **Clone All Rules in Group (Clonez toutes les règles du groupe)** pour rapidement reproduire les règles du groupe d'étiquettes sélectionné du groupe de périphériques et de la base de règles de votre choix. Le groupe de périphériques doit déjà exister (vous ne pouvez le créer lors du processus) avant de cloner les règles d'un groupe d'étiquettes vers un autre groupe de périphériques. De plus, vous pouvez cloner les règles d'un groupe d'étiquettes vers une autre base de règles faisant partie du même groupe de périphériques.

Le nom de la règle est ajouté aux règles clonées, selon le format suivant : `<nom-de-la-règle>-1`. Si une règle clonée se trouve au même emplacement que la première règle et que le nom ne change pas, le nom est alors joint. Par exemple, `<nom-de-la-règle>-2`, `<nom-de-la-règle>-3` et ainsi de suite.

© 2020 Palo Alto Networks, Inc.

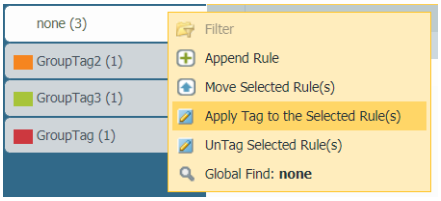
Pour cloner des règles, configurez les champs suivants.

Champ	Description
Destination	Le groupe de périphériques cible des règles de politique clonées.
(Panorama uniquement) Type de destination	Sélectionnez si vous souhaitez cloner les règles vers la **Pre-Rulebase (Base de règles avant)** ou vers la **Post-Rulebase (Base de règles après)** du groupe de périphériques de destination.
Ordre des règles	Sélectionnez l'endroit de la base de règles où cloner les règles. Vous avez le choix entre les actions suivantes'A0;: • **Move Top (Déplacer vers le haut)** : insérez les règles clonées au haut de la base de règles du groupe de périphériques de destination. • **Move Bottom (Déplacer vers le bas)** : insérez les règles clonées au bas de la base de règles du groupe de périphériques de destination. • **Before Rule (Avant la règle)** : insérez les règles clonées avant la règle sélectionnée de la base de règles du groupe de périphériques de destination. • **After Rule (Après la règle)** : insérez les règles clonées après la règle sélectionnée de la base de règles du groupe de périphériques de destination.
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option pour déterminer comment les erreurs décelées au cours de la validation s'affichent. Si elle est activée, chaque erreur s'affiche individuellement. Si elle est désactivée (décochée), les erreurs sont groupées et s'affichent en tant qu'une seule erreur. Les erreurs détectées au cours de la validation entraînent l'échec du clonage. Aucune règle n'est ainsi clonée dans le groupe de périphériques de destination.

Gestion des étiquettes

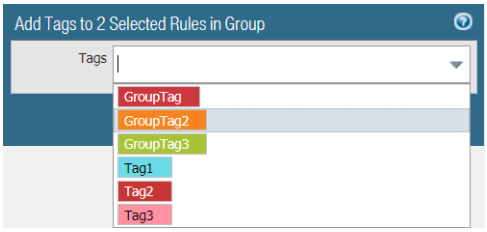
Le tableau suivant répertorie les actions que vous pouvez effectuer lorsque vous regroupez des règles par étiquettes de groupes.

- Attribuer une étiquette à une règle.
  1. Sélectionnez **View Rules as Groups (Afficher les règles en tant que groupes)**.
  2. Sélectionnez une ou plusieurs règles dans le volet de droite.
  3. Dans le menu déroulant dans étiquettes de groupes, **Apply Tag to the Selected Rules (Appliquez les étiquettes aux groupes sélectionnés)**.



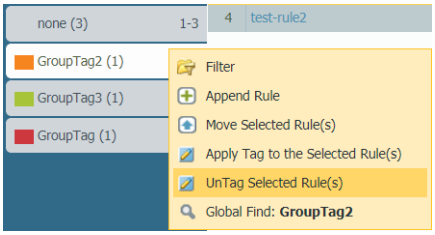
  4. Ajoutez des étiquettes aux règles sélectionnées.

© 2020 Palo Alto Networks, Inc.

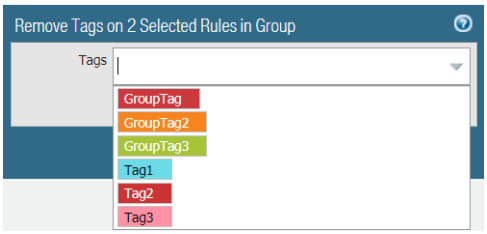


- Affichez les règles affectées à un groupe d'étiquettes.
  1. Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher les étiquettes de groupes auxquelles vos règles sont affectées.
  2. Le volet de droite se met à jour et affiche les étiquettes de groupe contenant n'importe lesquelles des étiquettes sélectionnées.
  3. Sélectionnez l'étiquette de groupes pour afficher les règles associées à ce groupe. Les règles qui ne sont pas affectées à une étiquette de groupes sont répertoriées dans le groupe **none (aucune)**.

- Annuler l'attribution d'une étiquette à une règle.
  1. Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher les étiquettes de groupes auxquelles vos règles sont affectées.
  2. Sélectionnez une ou plusieurs règles dans le volet de droite.
  3. Dans le menu déroulant dans étiquettes de groupes, **Apply Tag to the Selected Rules (Appliquez les étiquettes aux groupes sélectionnés)**.



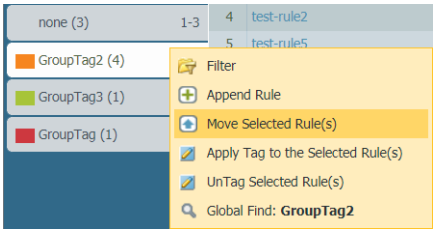
  4. Supprimez les étiquettes des règles sélectionnées. De plus, vous pouvez **Delete All (supprimer toutes)** les étiquettes affectées à la règle.



- Réorganiser une règle en utilisant des étiquettes.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, sélectionnez une ou plusieurs règles d'une étiquette de groupes, glissez la souris sur le numéro de la règle et sélectionnez **Move Selected Rule(s) (Déplacer la règle sélectionnée(s) dans la liste)** dans le menu déroulant. Ne sélectionnez aucune règle si vous souhaitez déplacer toutes les règles dans l'étiquette de groupe sélectionnée.

© 2020 Palo Alto Networks, Inc.



Sélectionnez une étiquette de groupe dans la liste déroulante de la fenêtre Déplacer une règle et indiquez si vous voulez **Move Before (Avancer)** ou **Move After (Reculer)** l'étiquette sélectionnée dans la liste déroulante.

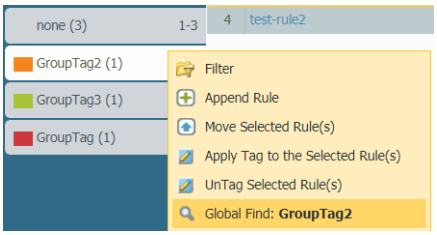
- Ajouter une nouvelle règle qui s'applique aux étiquettes sélectionnées.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, glissez la souris sur l'étiquette de groupe et sélectionnez l'option **Append Rule (Ajouter la règle)** dans le menu déroulant.

  La nouvelle règle est ajoutée à la fin de la liste de règles affectées à l'étiquette de groupe.

- Rechercher une étiquette de groupe.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, glissez la souris sur l'étiquette de groupe et sélectionnez l'option **Global Find (Recherche générale)** dans le menu déroulant.



- Exporter le tableau de configuration des étiquettes.

  Les rôles administrateurs peuvent exporter le tableau de configuration des objets au format **PDF/CSV** et peuvent appliquer des filtres pour personnaliser les sorties du tableau afin qu'elles n'intègrent que les colonnes dont vous avez besoin. Seules les colonnes qui sont visibles dans le dialogue d'Exportation sont exportées. Consultez la section Exportation des données du tableau de configuration.

© 2020 Palo Alto Networks, Inc.

Objets > Listes dynamiques externes

Une liste dynamique externe est un objet d'adresse basé sur une liste importée d'adresses IP, d'URL ou de noms de domaine que vous pouvez utiliser dans les règles de politique pour bloquer ou autoriser le trafic. Cette liste doit être un fichier texte enregistré sur un serveur Web accessible par le pare-feu. Le pare-feu utilise l'interface de gestion (MGT) par défaut pour récupérer cette liste.

Avec une licence de prévention des menaces active, Palo Alto Networks® fournit plusieurs listes d'adresses IP dynamiques intégrées que vous pouvez utiliser pour bloquer des hôtes malveillants. Les listes sont mises à jour quotidiennement en fonction de nos plus récentes recherches sur les menaces.

Vous pouvez utiliser une liste d'adresses IP comme objet d'adresse dans la source et la destination de vos règles de politique. Vous pouvez utiliser une liste des URL dans un profil de filtrage des URL (Objets > Profils de sécurité > Filtrage des URL) ou comme critère de correspondance dans les règles de politique de sécurité. Vous pouvez également utiliser une liste des domaines dans Objets > Profils de sécurité > Profil antispyware pour les noms de domaines pièges spécifiés.

Sur chaque modèle de pare-feu, vous pouvez utiliser jusqu'à 30 listes dynamiques externes avec des sources uniques à travers toutes les règles des politiques de Sécurité. Le nombre maximal d'entrées que le pare-feu prend en charge pour chaque type de liste varie en fonction du modèle de pare-feu (reportez-vous aux différentes limites de pare-feu pour chaque type de liste dynamique externe). Les entrées de la liste ne sont comptabilisées que dans la limite maximale si la liste dynamique externe est utilisée dans la politique. Si vous dépassez le nombre maximal d'entrées qui sont prises en charge sur un modèle, le pare-feu génère un journal système et ignore toutes les entrées qui dépassent cette limite. Pour vérifier le nombre d'adresses IP, de domaines et d'URL actuellement utilisés dans la politique et le nombre total pris en charge sur le pare-feu, cliquez sur **Capacités de la liste** (pare-feu uniquement).

Les listes dynamiques externes sont présentées en ordre d'évaluation, de haut en bas. Utilisez les commandes directionnelles (bas de la page) pour changer l'ordre de la liste. Ces commandes vous permettent de réorganiser l'ordre des listes pour vous assurer que les entrées les plus importantes d'une EDL sont validées avant d'atteindre les limites de capacité.



Vous ne pouvez changer l'ordre de la EDL lorsque les listes sont regroupées selon le type.

Pour récupérer la dernière version de la liste dynamique externe à partir du serveur qui l'héberge, sélectionnez une liste dynamique externe et cliquez sur **Import Now (Importer maintenant)**.



Vous ne pouvez pas supprimer, cloner ou modifier les paramètres des flux d'adresses IP malveillantes de Palo Alto Networks.

Add (Ajoutez) une nouvelle liste dynamique externe et configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la liste dynamique externe	Description
Name (Nom)	Saisissez un nom pour identifier la liste dynamique externe (32 caractères maximum). Ce nom identifie la liste lorsque vous utilisez celle-ci pour appliquer la politique.
Partagé	Sélectionnez cette option si vous souhaitez que la liste dynamique externe soit disponible pour :

© 2020 Palo Alto Networks, Inc.

Paramètres de la liste dynamique externe	Description
	• Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, la liste dynamique externe sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, la liste dynamique externe sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette liste dynamique externe dans les groupes de périphériques qui héritent de l'objet. Cette option est désactivée (décochée) par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Vérifier l'URL source (pare-feu uniquement)	Cliquez pour vérifier que le pare-feu peut se connecter au serveur qui héberge la liste dynamique externe. *Ce test ne vérifie pas si le serveur est authentifié avec succès.*
Onglet Créer liste	
Type *Vous ne pouvez mélanger les adresses IP, les URL et les noms de domaine dans une seule liste. Chaque liste doit comprendre des entrées d'un seul type.*	Faites votre sélection à partir des types de listes dynamiques externes suivants : • **Predefined IP List (Liste des adresses IP prédéfinies)** – Les listes de ce type utilisent un flux d'adresses IP malveillantes ou à haut risque de Palo Alto Networks comme source d'entrées de liste (une licence de Prévention des menaces active est requise). • **IP List (Liste IP)** - Chaque liste peut inclure des plages IP et des sous-réseaux IP dans l'espace d'adresse IPv4 et IPv6. La liste doit contenir une seule adresse IP, une seule plage ou un seul sous-réseau par ligne. Exemple : `192.168.80.150/32` `2001:db8:123:1::1 or 2001:db8:123:1::/64` `192.168.80.0/24 (this indicates all addresses from 192.168.80.0 through 192.168.80.255)` `2001:db8:123:1::1 - 2001:db8:123:1::22` Un sous-réseau ou une plage d'adresses IP comme 92.168.20.0/24 ou 192.168.20.40-192.168.20.50, sont comptabilisés comme une entrée d'adresse IP et pas comme plusieurs adresses IP. • **Domain List (Liste des domaines)** - Chaque liste ne peut posséder qu'une seule entrée de nom de domaine par ligne. Exemple : `www.p301srv03.paloalonetworks.com` `ftp.example.co.uk` `test.domain.net`

© 2020 Palo Alto Networks, Inc.

Paramètres de la liste dynamique externe	Description
	Pour la liste des domaines compris dans la liste dynamique externe, le pare-feu crée un ensemble de signatures personnalisées des logiciels espions et un niveau de gravité moyen, pour que vous puissiez utiliser l'action Entonnoir pour une liste de domaines personnalisée. • **URL List (Liste des URL)** - Chaque liste ne peut posséder qu'une seule entrée d'URL par ligne. Exemple : `financialtimes.co.in` `www.wallaby.au/joey` `www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx` `*.example.com/*` Pour chaque liste d'URL, l'action par défaut est définie sur Autoriser. Pour modifier l'action par défaut, voir Objets > Profils de sécurité > Filtrage des URL.
Description	Saisissez une description de la liste dynamique externe (255 caractères maximum).
Source	Saisissez une URL d'accès HTTP ou HTTPS vers le fichier texte. Par exemple, http://192.0.2.20/myfile.txt. • Si la liste dynamique externe est une liste des adresses IP prédéfinies, sélectionnez **Palo Alto Networks - High risk IP addresses (Palo Alto Networks- Adresse IP à haut risque)** ou **Palo Alto Networks - Known malicious IP addresses (Palo Alto Networks - Adresses IP malveillantes connues)** en tant que source de la liste. • Si la liste externe dynamique est une liste de domaines, le paramètre est défini par défaut sur **Automatically expand to include subdomains (Élargir automatiquement sur l'inclusion de sous-domaines)**. Cette option permet à PAN-OS d'évaluer tous les composants de niveau inférieur des noms de domaines indiqués dans le fichier d'EDL. *Si votre EDL contient des sous-domaines, ces entrées étendues sont incluses dans le calcul de la capacité du modèle de votre appareil. Vous pouvez désactiver cette fonction si vous souhaitez définir manuellement des sous-domaines. Cependant, les sous-domaines qui ne sont pas explicitement définis dans la liste ne sont pas évalués par les règles de politique.*
Profil du certificat	Si la liste dynamique externe comporte une URL d'accès HTTPS, sélectionnez un profil de certificat existant (pare-feu et Panorama) ou créez un nouveau **Profil de certificat** (pare-feu uniquement) pour authentifier le serveur Web qui héberge la liste. Pour plus d'informations sur la configuration d'un profil de certificat, voir Périphérique > Gestion des certificats > Profil du certificat. Par défaut : **Aucun (Désactiver le profil de certificat)**

© 2020 Palo Alto Networks, Inc.

Paramètres de la liste dynamique externe	Description
	Pour maximiser le nombre de listes dynamiques externes que vous pouvez utiliser pour appliquer la stratégie, utilisez le même profil de certificat pour authentifier les listes dynamiques externes qui utilisent la même URL source afin que les listes ne comptent que pour une seule liste dynamique externe. Les listes dynamiques externes provenant de la même URL source qui utilisent différents profils de certificats sont comptabilisées comme des listes dynamiques externes uniques.
Authentification du client	Sélectionnez cette option (désactivée par défaut) pour ajouter un nom d'utilisateur et un mot de passe au pare-feu qui sera utilisé pour accéder à une source de listes dynamiques externes nécessitant une authentification HTTP basique. Ce paramètre n'est disponible que lorsque la liste dynamique externe possède une URL HTTPS. • **Nom d'utilisateur** – Saisissez un nom d'utilisateur valide pour accéder à la liste. • **Mot de passe / Confirmer le mot de passe** - Saisissez, puis confirmez le mot de passe du nom d'utilisateur.
Rechercher des mises à jour	Spécifiez la fréquence à laquelle le pare-feu récupère la liste du serveur Web. Vous pouvez définir l'intervalle à laquelle le pare-feu récupère la liste sur **Hourly (Toutes les heures)** (par défaut), **Five Minute (Toutes les cinq minutes)**, **Daily (Quotidienne)**, **Weekly (Hebdomadaire)** ou **Monthly (Mensuelle)**. Le pare-feu valide automatiquement les changements et les intègre immédiatement à la configuration si la dernière validation n'a pas été effectuée au cours des 15 dernières minutes ; si la dernière modification a eu lieu au cours des 15 dernières minutes, la validation se produit 15 minutes après la dernière validation. Toutes les règles de politique qui font référence à la liste sont mises à jour afin que le pare-feu puisse appliquer comme il se doit la politique. *Vous n'avez pas à configurer une fréquence pour une liste prédéfinie d'adresses IP parce que le pare-feu reçoit dynamiquement des mises à jour de contenu avec une licence active de prévention des menaces.*
Onglet des entrées et des exceptions de la liste	
Entrées de la liste	Affiche les entrées dans la liste dynamique externe. • Ajouter une entrée en tant qu'exception de liste – Sélectionnez jusqu'à 100 entrées et cliquez sur Envoyer (). • Affichez un récapitulatif des renseignements sur les menaces AutoFocus™ pour un objet – Passez sur une entrée, cliquez sur le menu déroulant et cliquez sur **Autofocus**. Vous devez avoir une licence AutoFocus et activer les renseignements de menaces AutoFocus pour afficher un récapitulatif des objets (sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres **AutoFocus**).

© 2020 Palo Alto Networks, Inc.

Paramètres de la liste dynamique externe	Description
	• Vérifiez si une adresse IP, un domaine ou une URL se trouve dans la liste dynamique externe – Saisissez une valeur dans le champ de filtrage et cliquez sur Appliquer le filtre (). Effacez le filtre ([X]) pour revenir à l'affichage de la liste complète.
Exceptions manuelles	Affiche les exceptions de la liste dynamique externe. • Modifier une exception – Cliquez sur une exception et faites vos modifications. • Saisir manuellement une exception – Cliquez sur **Ajouter** une nouvelle exception manuellement. • Supprimer une exception de la liste des Exceptions manuelles – Sélectionnez une exception et cliquez sur **Effacer**. • Vérifiez si une adresse IP, un domaine ou une URL se trouve dans la liste des Exceptions manuelles – Saisissez une valeur dans le champ de filtrage et cliquez sur Appliquer le filtre (). Effacez le filtre ([X]) pour revenir à l'affichage de la liste complète. Vous ne pouvez pas enregistrer vos modifications dans la liste dynamique externe si vous avez des entrées en double dans la liste des Exceptions manuelles.

© 2020 Palo Alto Networks, Inc.

Objets > Objets personnalisés

Créez des modèles de données, des signatures contre les logiciels malveillants ou contre les vulnérabilités ainsi que des catégories d'URL personnalisées à utiliser avec les politiques :

- Objets > Objets personnalisés > Modèles de données
- Objets > Objets personnalisés > Logiciels espions / vulnérabilité
- Objets > Objets personnalisés > Catégories d'URL

Objets > Objets personnalisés > Modèles de données

Les rubriques suivantes décrivent les modèles de données.

Que voulez-vous faire ?	Reportez-vous à la section :
Créer un modèle de données.	Paramètres des modèles de données
En savoir plus sur la syntaxe des expressions régulières pour les modèles de données et voir quelques exemples.	Syntaxe pour les modèles de données d'expression régulière Exemples de modèles de données d'expression régulière

Paramètres des modèles de données

Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **Data Patterns (Modèles de données)** pour définir les catégories d'informations sensibles que vous souhaitez filtrer. Pour plus d'informations sur la définition des profils de filtrage de données, sélectionnez Objets > Profils de sécurité> Filtrage des données.

Vous pouvez créer trois types de modèles de données pour le pare-feu. Vous pourrez utiliser ces modèles lors de la recherche d'informations sensibles :

- **Predefined (Prédéfini)** – Utilise les modèles de données prédéfinis pour analyser les fichiers de la sécurité sociale et les numéros des cartes de crédit.
- **Regular Expression (Expression régulière)** – Crée des modèles de données personnalisés en utilisant des expressions régulières.
- **File Properties (Propriétés du fichier)** – Analyse les fichiers pour les propriétés et les valeurs de fichiers spécifiques.

Paramètres des modèles de données	Description
Name (Nom)	Saisissez le nom du modèle de données (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du modèle de données (255 caractères maximum).
Partagé	Sélectionnez cette option si vous souhaitez que le modèle de données soit disponible pour :

© 2020 Palo Alto Networks, Inc.

Paramètres des modèles de données	Description
	• Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le modèle de données sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le modèle de données sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres du modèle de données de l'objet pour les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Type de modèle	Sélectionnez le type de modèle de données que vous voulez créer : • Modèle prédéfini • Expression régulière • Propriétés du fichier
Modèle prédéfini	Palo Alto Networks fournit des modèles de données prédéfinis pour analyser certains types de renseignements dans les fichiers comme, par exemple, les numéros de carte de crédit ou les numéros de sécurité sociale. Pour configurer le filtrage des données en fonction d'un modèle prédéfini, cliquez sur **Add (Ajouter)** un motif et sélectionnez ce qui suit : • **Name (Nom)** – Sélectionnez le modèle prédéfini qui sera utilisé pour filtrer les données sensibles. Lorsque vous choisissez un modèle prédéfini, le champ **Description** se remplit automatiquement. • Sélectionnez le **File Type (Type de fichier)** dans lequel vous souhaitez détecter le modèle prédéfini.
Expression régulière	Cliquez sur **Add (Ajouter)** un modèle de données personnalisé. Donnez au modèle un **Nom** descriptif, configurez le **Type de fichier** que vous souhaitez analyser pour le motif de données et saisissez l'expression régulière qui définit le **Modèle de données**. Pour les détails et les exemples de syntaxe des modèles d'informations d'expression régulière, veuillez vous référer aux sections suivantes : • Syntaxe pour les modèles de données d'expression régulière • Exemples de modèles de données d'expression régulière
Propriétés du fichier	Créez un modèle de données pour analyser les propriétés du fichier et les valeurs associées. Par exemple, cliquez sur **Add (Ajouter)** un modèle de données pour filtrer les documents Microsoft Word et les fichiers PDF lorsque le titre du document comprend les mots « sensible », « interne » ou « confidentiel ». • Donnez un **Nom** descriptif au modèle de données. • Sélectionnez le **Type de fichier** que vous souhaitez analyser.

© 2020 Palo Alto Networks, Inc.

Paramètres des modèles de données	Description
	• Sélectionnez la **Propriété de fichier** que vous souhaitez analyser pour une valeur spécifique. • Saisissez la **Valeur de propriété** que vous souhaitez analyser.

Syntaxe pour les modèles de données d'expression régulière

Lorsque vous créez un modèle de données d'expression régulière, les exigences générales suivantes s'appliquent :

- Le modèle doit se composer d'une chaîne d'au moins 7 octets avec des valeurs fixes. Les 7 octets ne peuvent pas contenir de point (`.`), d'astérisque (`*`), de signe plus (`+`) ou de plage (`[a-z]`).
- Lorsque vous avez besoin que les valeurs soient sensibles à la casse, définissez des modèles pour toutes les chaînes possibles pour qu'elles correspondent à toutes les variations d'un terme. Par exemple, si vous voulez que des documents désignés comme étant confidentiels s'affichent dans les correspondances, vous devrez créer un modèle pour « confidentiel », « Confidentiel » et « CONFIDENTIEL ».

La syntaxe des expressions régulières dans PAN-OS® est similaire à celle des moteurs traditionnels, mais chaque modèle est unique. Le tableau suivant décrit la syntaxe prise en charge dans PAN-OS.

Syntaxe des règles des modèles	Description
.	Renvoie n'importe quel caractère unique.
?	Renvoie le caractère ou l'expression qui précède 0 ou 1 fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : (abc)?
*	Renvoie le caractère ou l'expression qui précède 0 ou plusieurs fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : (abc)*
+	Renvoie le caractère ou l'expression régulière qui précède une ou plusieurs fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : (abc)+
|	Spécifie un autre « ou ». Exemple : ((bif)|(scr)|(exe)) renvoie « bif », « scr » ou « exe ». *Vous devez inclure les sous-chaînes alternatives entre parenthèses.*
-	Spécifie une plage. Exemple : [c-z] renvoie tout caractère entre c et z inclus.
[ ]	Renvoie n'importe quel caractère spécifié.

© 2020 Palo Alto Networks, Inc.

Syntaxe des règles des modèles	Description
	Exemple : [abz] renvoie n'importe lequel des caractères a, b ou z.
^	Renvoie n'importe quel caractère à l'exception des caractères spécifiés. Exemple : [^abz] renvoie n'importe quel caractère à l'exception des caractères a, b ou z.
{ }	Renvoie une chaîne qui contient un minimum et un maximum. Exemple : {10-20} renvoie n'importe quelle chaîne comprise entre 10 et 20 octets inclus. Vous devez spécifier ceci directement devant une chaîne fixe et vous ne pouvez utiliser que le trait d'union (–).
\	Effectue une correspondance littérale sur n'importe quel caractère ci-dessus. Vous devez faire précéder le caractère spécifié d'une barre oblique inversée (\).
&amp	La perluète (&) est un caractère spécial, donc si vous recherchez & dans une chaîne, vous devez plutôt utiliser **&amp**».

Exemples de modèles de données d'expression régulière

Voici des exemples de modèles personnalisés valides'A0;:

- .*((Confidentiel)|(CONFIDENTIEL))
  - Recherche le mot « Confidentiel » ou « CONFIDENTIEL » partout
  - « .* » indique que la recherche porte sur n'importe quelle partie de la chaîne
  - Selon que votre décodeur est sensible à la casse ou pas, le terme « confidentiel » (en minuscules) risque de ne pas faire partie des correspondances.
- .*((Exclusif &amp Confidentiel)|(Exclusif et Confidentiel))
  - Recherche « Exclusif & Confidentiel » ou « Exclusif et Confidentiel »
  - Plus précis que « Confidentiel »
- .*(Communiqué de presse).*((Ebauche)|(EBAUCHE)|(ébauche))
  - Recherche « Communiqué de presse », suivi par diverses formes du mot « ébauche », ce qui peut indiquer que le communiqué de presse n'est pas prêt à être divulgué
- .*(Trinidad)
  - Recherche un nom de code de projet, par exemple « Trinidad »

© 2020 Palo Alto Networks, Inc.

Objets > Objets personnalisés > Logiciels espions / vulnérabilité

Le pare-feu prend en charge la création de signatures personnalisées contre les logiciels espions et les vulnérabilités grâce à son moteur de détection des menaces. Vous pouvez rédiger des modèles d'expressions régulières personnalisés pour identifier les communications 'AB; phone home 'BB; des logiciels espions ou les exploitations de vulnérabilités. Les modèles obtenus peuvent être utilisés dans n'importe quel profil personnalisé de protection contre les vulnérabilités. Le pare-feu recherche les modèles personnalisés dans le trafic réseau et prend l'action définie pour lutter contre l'exploitation de la vulnérabilité détectée.



Toutes les semaines, le contenu affiche de nouveaux décodeurs et contextes pour lesquels vous pouvez développer des signatures.

En option, vous pouvez inclure un attribut de temps dans la définition des signatures personnalisées, en précisant un seuil par intervalle pour le déclenchement des actions possibles en réponse à une attaque. L'action n'est prise qu'une fois le seuil atteint.

La page **Custom Spyware Signature (Signatures personnalisées contre les logiciels espions)** permet de définir des signatures pour les profils de protection contre les logiciels espions. La page **Custom Vulnerability Signature (Signatures personnalisées contre les vulnérabilités)** permet de définir des signatures pour les profils de protection contre les vulnérabilités.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
Onglet Configuration	
ID de menace	Saisissez un identifiant numérique pour la configuration (l'intervalle des signatures contre les logiciels espions est compris entre 15 000 et 18 000 ; l'intervalle des signatures contre les vulnérabilités est compris entre 41 000 et 45 000).
Name (Nom)	Indiquez le nom de la menace.
Partagé	Sélectionnez cette option si vous souhaitez que la signature personnalisée soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, la signature personnalisée sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, la signature personnalisée sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.

© 2020 Palo Alto Networks, Inc.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette signature dans les groupes de périphériques qui héritent de la signature. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de la signature.
Commentaire	Saisissez un commentaire (facultatif).
Sévérité	Affectez un niveau qui indique la gravité de la menace.
Action par défaut	Affectez l'action par défaut à prendre si les conditions de la menace sont réunies. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité.
Direction	Indiquez si la menace est évaluée depuis le client vers le serveur, depuis le serveur vers le client ou les deux.
Système affecté	Indiquez si la menace implique le client, le serveur ou les deux. S'applique aux signatures contre les vulnérabilités, mais non aux signatures contre les logiciels espions.
CVE	Indiquez l'identifiant CVE à titre de référence externe pour une analyse plus approfondie.
Constructeur	Indiquez l'identifiant du constructeur à titre de référence externe pour une analyse plus approfondie.
Bugtraq	Indiquez le bugtraq (similaire à l'identifiant CVE) à titre de référence externe pour une analyse plus approfondie.
Référence	Ajoutez tout lien qui permet une analyse plus approfondie. Ces informations s'affichent lorsqu'un utilisateur clique sur la menace depuis l'ACC, les journaux ou le profil de protection contre les vulnérabilités.
Onglet Signatures	
Signature standard	Sélectionnez **Standard**, puis **Ajoutez** une nouvelle signature. Renseignez les informations suivantes'A0;: • **Standard** - Saisissez un nom permettant d'identifier la signature. • **Comment (Commentaire)** - Saisissez une description (facultatif). • **Ordered Condition Match (Correspondance de l'état ordonné)** - Indiquez si l'ordre dans lequel les conditions de la signature sont définies a son importance. • **Scope (Portée)** - Indiquez s'il faut appliquer cette signature à la transaction en cours seulement pendant toute la session utilisateur. Ajoutez une condition en cliquant sur **Add Or Condition (Ajouter une condition OU)** ou **Add And Condition (Ajouter une condition ET)**. Pour

© 2020 Palo Alto Networks, Inc.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Add Condition (Ajouter une condition)**. Ajoutez une condition à une signature afin que celle-ci soit générée pour le trafic lorsque les paramètres que vous avez définis pour la condition sont vrais. Sélectionnez un **Operator (Opérateur)** dans la liste déroulante. L'opérateur définit le type de condition qui doit être vrai pour que la signature personnalisée corresponde au trafic. Faites votre sélection parmi les opérateurs **Less Than (Inférieur à)**, **Equal To (Égal à)**, **Greater Than (Supérieur à)** ou **Pattern Match (Correspondance des modèles)**. • Si vous avez choisi un opérateur **Pattern Match (Correspondance des modèles)**, alors les éléments suivants devront être vrais pour que la signature corresponde au trafic : • **Context (Contexte)** - Choisissez parmi les contextes disponibles. • **Pattern (Modèle)** - Précisez une expression régulière. Reportez-vous à la section Syntaxe des règles des modèles pour connaître les règles concernant les expressions régulières. • **Qualifier and Value (Qualificatif et Valeur)** - Ajoutez des paires qualificatif/valeur (facultatif). • **Negate (Ignorer)** - Sélectionnez l'option **Negate (Ignorer)** pour que la signature personnalisée corresponde au trafic uniquement lorsque la condition Correspondance des modèles définie n'est pas vraie. Ceci permet de vous assurer que la signature personnalisée ne se déclenche pas sous certaines conditions. *Une signature personnalisée ne peut pas uniquement être créée avec les conditions Ignorer ; au moins une condition positive doit être incluse pour qu'une condition Ignorer puisse être définie. De même, si l'étendue de la signature est définie sur Session, une condition Ignorer ne peut pas être configurée comme dernière condition pour pouvoir correspondre au trafic.* Vous pouvez définir des exceptions pour les signatures personnalisées contre les logiciels malveillants ou contre les vulnérabilités en utilisant la nouvelle option permettant d'ignorer la génération de signatures lorsque le trafic correspond à une signature et l'exception à la signature. Cette option permet d'autoriser un trafic donné dans votre réseau qui, autrement, serait classé en tant qu'exploitation de vulnérabilité ou de logiciel malveillant. Dans ce cas, la signature est générée pour le trafic correspondant au modèle, le trafic correspondant au modèle mais aussi à l'exception du modèle qui est exclu de la génération de signature et de toute action de la politique associée (comme une interdiction ou un abandon). Par exemple, vous pouvez choisir de générer une signature pour des URL redirigées. Cependant, vous pouvez désormais créer une exception dans laquelle aucune signature ne sera générée pour les URL redirigeant vers un domaine de confiance.

© 2020 Palo Alto Networks, Inc.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	• Si vous avez choisi un opérateur **Equal To (Égal à)**, **Less Than (Inférieur à)** ou **Greater Than (Supérieur à)**, alors les éléments suivants devront être vrais pour que la signature corresponde au trafic : • **Context (Contexte)** - Faites votre choix parmi les requêtes inconnues et les réponses pour le protocole TCP ou UDP. • **Position** - Faites votre choix parmi les quatre premiers ou les quatre seconds octets de la charge utile. • **Mask (Masque)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xffffff00. • **Value (Valeur)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xaabbccdd.
Association de signatures	Sélectionnez **Combination (Association)** et indiquez les informations suivantes : Sélectionnez l'option **Combination Signatures (Association de signatures)** pour indiquer les conditions de définition des signatures : • Ajoutez une condition en cliquant sur **Add AND Condition (Ajouter une condition AND)** ou **Add OR Condition (Ajouter une condition OR)**. Pour ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Add Condition (Ajouter une condition)**. • Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre. Sélectionnez l'option **Time Attribute (Attribut temporel)** pour indiquer les informations suivantes : • **Number of Hits (Nombre d'accès)** - Spécifiez le seuil de déclenchement d'une action basée sur une politique sous la forme d'un nombre d'accès (1-1000) dans un certain nombre de secondes (1-3600). • **Aggregation Criteria (Critères d'agrégation)** - Précisez si les accès sont comptabilisés par adresse IP source, adresse IP de destination, ou une combinaison des deux. • Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.

© 2020 Palo Alto Networks, Inc.

Objets > Objets personnalisés > Catégories d'URL

Utilisez la page Catégorie d'URL personnalisée pour créer votre liste d'URL personnalisée et utilisez-la dans un profil de filtrage des URL ou en tant que critères de correspondance dans les règles de la politique. Dans une catégorie d'URL personnalisée, vous pouvez ajouter des entrées d'URL individuellement ou vous pouvez importer un fichier texte qui contient une liste d'URL.



Les URL ajoutées aux catégories personnalisées sont sensibles à la casse.

Le tableau suivant décrit les paramètres des URL personnalisées.

Paramètres de la catégorie d'URL personnalisée	Description
Name (Nom)	Saisissez un nom pour identifier la catégorie d'URL personnalisée (31 caractères maximum). Ce nom apparaît dans la liste de catégories pour la définition de politiques de filtrage des URL ainsi que dans les critères de correspondance des catégories d'URL définies dans les règles de la politique. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description de la catégorie d'URL (255 caractères maximum).
Type	Sélectionnez le type de catégorie : • **Category Match (Correspondance à la catégorie)** - Sélectionnez **Category match (Correspondance à la catégorie)** afin de définir une nouvelle catégorie personnalisée contenant les URL correspondants à toutes les catégories de URL spécifiées (un URL doit correspondre à toutes les catégories dans la liste). Spécifiez de 2 à 4 catégories. • **URL List (Liste des URL)** - Sélectionnez **URL List (Liste de URLS)** pour ajouter ou importer une liste de URL dans la catégorie. Ce type de catégorie contient aussi des URL ajoutés avant PAN-OS 9.0.
Partagé	Sélectionnez cette option si vous souhaitez que la catégorie d'URL soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez (décochez) cette option, la catégorie d'URL est uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez (décochez) cette option, la catégorie d'URL est uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.

© 2020 Palo Alto Networks, Inc.

Paramètres de la catégorie d'URL personnalisée	Description
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet des URL personnalisées dans les groupes de périphériques qui héritent de l'objet. Cette sélection est décochée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Sites	Gérez les sites pour la catégorie des URL personnalisées (chaque URL ajouté ou importé est limité à 255 caractères). • **Add (Ajoutez)** : **Add (Ajoutez)** des URL, mais une seule par ligne. Chaque URL peut être au format « www.example.com » ou peut inclure des caractères génériques, comme « *.example.com ». Pour obtenir plus d'informations sur les formats pris en charge, consultez la liste d'interdictions à la section Objets > Profils de sécurité > Filtrage des URL. • **Import (Importer)** : **Import (Importez)** et accédez au fichier texte qui contient la liste des URL. Ne saisissez qu'un seul URL par ligne. Chaque URL peut être au format « www.example.com » ou peut inclure des caractères génériques, comme « *.example.com ». Pour obtenir plus d'informations sur les formats pris en charge, consultez la liste d'interdictions à la section Objets > Profils de sécurité > Filtrage des URL. • **Export (Exporter)** : **Export (Exportez)** les entrées d'URL personnalisées comprises dans la liste (exportées sous forme de fichier texte). • **Delete (Supprimer)** - **Delete (Supprimez)** une entrée pour supprimer l'URL de la liste. *Pour supprimer une catégorie personnalisée que vous avez utilisée dans un profil de filtrage des URL, vous devez définir l'action sur Aucun avant de pouvoir procéder. Consultez les actions de la Catégorie dans la section* Objets > Profils de sécurité > Filtrage des URL.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité

Les profils de sécurité fournissent une protection contre les menaces dans les politiques de sécurité. Chaque règle de politique de sécurité peut inclure un ou plusieurs profils de sécurité. Les types de profil disponibles sont les suivants :

- Profils antivirus visant à assurer une protection contre les vers, les virus et les chevaux de Troie, mais aussi à bloquer les téléchargements de logiciels espions. Reportez-vous à la section Objets > Profils de sécurité > Antivirus.
- Profils Antispyware visant à bloquer les tentatives de communications phone-home ou de signalement sur les serveurs (C2) de commande et de contrôle externes par les logiciels espions sur les hôtes compromis. Reportez-vous à la section Objets > Profils de sécurité > Profil antispyware.
- Profils de protection contre les vulnérabilités visant à bloquer les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes. Reportez-vous à la section Objets > Profils de sécurité > Protection contre les vulnérabilités.
- Profils de filtrage des URL visant à limiter l'accès des utilisateurs à des sites Web et/ou des catégories de sites Web spécifiques, tels que les sites commerciaux ou de jeux d'argent. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des URL.
- Profils de blocage des fichiers visant à bloquer les types de fichiers sélectionnés et dans le sens spécifié du flux de la session (entrant et/ou sortant). Reportez-vous à la section Objets > Profils de sécurité > Blocage des fichiers.
- Profils d'analyse WildFire™ visant à indiquer le fichier à analyser localement sur l'équipement WildFire ou dans le Cloud WildFire. Reportez-vous à la section Objets > Profils de sécurité > Analyse WildFire.
- Profils de filtrage des données visant à empêcher les informations sensibles, telles que les numéros de carte de crédit ou de sécurité sociale, de quitter un réseau protégé. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des données.
- Les profils de protection DoS sont utilisés avec les règles de politique de protection DoS pour protéger le pare-feu contre les attaques à volume élevé à l'encontre d'une session et de plusieurs sessions. Voir Objets > Profils de sécurité > Protection DoS.
- Les profils de protection GTP permettent au pare-feu d'inspecter, de valider et de filtrer le trafic GTP. Reportez-vous à la section Objets > Profils de sécurité > Protection GTP.

Outre les profils individuels, vous pouvez combiner des profils qui sont souvent appliqués ensemble et ainsi créer des groupes de profils de sécurité (**Objects (Objets)** > **Security Profile Groups (Groupes de profils de sécurité)**).

Actions dans des profils de sécurité

Une action indique la manière dont le pare-feu répond à une menace. Chaque signature de menace ou de virus définie par Palo Alto Networks contient une action par défaut, généralement définie sur **Alerter**, qui vous indique d'utiliser l'option que vous avec activée pour les notifications ou sur **Réinitialiser les deux**, qui réinitialise les deux côtés de la connexion. Cependant, vous pouvez définir ou appliquer un contrôle prioritaire sur l'action sur le pare-feu. Les actions suivantes peuvent être appliquées lors de la définition de profils Antivirus, de profils Antispyware, de profils de Protection contre les vulnérabilités, d'objets Logiciels espions personnalisés, d'objets Vulnérabilité personnalisés ou de Protection DoS.

© 2020 Palo Alto Networks, Inc.

Action (Action)	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilité	Objet personnalisé - Logiciels espions et Vulnérabilité	profil de protection du dos
Default (Par défaut)	L'action par défaut définie en interne est appliquée pour chaque signature de menace. Pour les profils antivirus, l'action par défaut est appliquée pour la signature de virus.	✓	✓	✓	—	Abandon anticipé aléatoire
allow (autoriser)	Autorise le trafic de l'application. *L'action Allow (Autoriser) ne génère pas de journaux associés aux signatures ou aux profils.*	✓	✓	✓	✓	—
alert (alerter)	Génère une alerte pour chaque flux de trafic de l'application. L'alerte est sauvegardée dans le journal des menaces.	✓	✓	✓	✓	✓ Génère une alerte lorsque le volume d'attaque (cps) atteint le Seuil d'alarme défini dans le profil.
Chutes	Abandonne le trafic de l'application.	✓	✓	✓	✓	—
Réinitialiser le client	Pour le protocole TCP, la connexion côté client est réinitialisée.	✓	✓	✓	✓	—

© 2020 Palo Alto Networks, Inc.

Action (Action)	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilité	Objet personnalisé - Logiciels espions et Vulnérabilité	profil de protection du dos
	Pour le protocole UDP, la connexion est abandonnée.					
Réinitialiser le serveur	Pour le protocole TCP, la connexion côté serveur est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.	✓	✓	✓	✓	–
Réinitialiser les deux	Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur. Pour le protocole UDP, la connexion est abandonnée.	✓	✓	✓	✓	–
Bloquer IP	Bloque le trafic d'une source ou d'une paire source-destination ; configurable pendant une durée déterminée.	–	–	–	–	✓
Entonnoir	Cette action dirige les requêtes DNS provenant de domaines malveillants vers une adresse IP entonnoir. Cette action est disponible pour les signatures DNS Palo Alto Networks et pour les domaines personnalisés inclus dans Objets > Listes dynamiques externes.	–	–	–	–	–
Abandon anticipé aléatoire	Amène le pare-feu à supprimer les paquets de manière aléatoire lorsque les connexions	–	–	–	–	✓

© 2020 Palo Alto Networks, Inc.

Action (Action)	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilité	Objet personnalisé - Logiciels espions et Vulnérabilité	profil de protection du dos
	par seconde atteignent le seuil de Taux d'activation dans un profil de Protection DoS appliqué à une règle de Protection DoS.					
cookies SYN ;	Amène le pare-feu à générer des cookies SYN pour authentifier un SYN envoyé par un client lorsque les connexions par seconde atteignent le seuil du Taux d'activation dans un profil de Protection DoS appliqué à une règle de Protection DoS.	—	—	—	—	✓

Vous ne pouvez pas supprimer un profil utilisé dans une règle de politique ; vous devez d'abord supprimer le profil de la règle de politique.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Antivirus

La page **Antivirus Profiles (Profils antivirus)** vous permet de configurer pour le pare-feu des options d'analyse antivirus du trafic défini. Définissez les applications qui doivent être analysées et l'action à effectuer lorsqu'un virus est détecté. Le profil par défaut inspecte l'ensemble des décodeurs de protocole répertoriés à la recherche de virus, génère des alertes pour les protocoles Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP) et Post Office Protocol Version 3 (POP3) et prend l'action par défaut pour d'autres applications (alerte ou refus), en fonction du type de virus détecté. Le profil est ensuite associé à une règle de politique de sécurité pour déterminer le trafic traversant certaines zones à inspecter.

Il est possible d'utiliser des profils personnalisés pour limiter les inspections antivirus sur le trafic entre des zones de sécurité de confiance ou au contraire les renforcer sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs.

Pour ajouter un nouveau profil antivirus, sélectionnez l'option Ajouter et saisissez les paramètres suivants :

Champ	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils antivirus pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil antivirus dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Onglet Antivirus Précisez l'action à effectuer pour les différents types de trafic, tels que FTP et HTTP.	
Capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés.
Décodeurs et actions	Pour chaque type de trafic que vous voulez inspecter, choisissez une action dans la liste déroulante. Vous pouvez définir différentes actions pour les signatures antivirus standard (colonne Action) et les signatures générées par le système'A0;WildFire (colonne Action'A0;WildFire).

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Il se peut que certains environnements exigent une durée d'exposition plus longue pour les signatures antivirus'A0;; par conséquent, cette option vous permet de définir des actions pour les deux types de signature antivirus fournis par Palo Alto Networks. Par exemple, les signatures antivirus standard passent par une période d'exposition plus longue avant d'être publiées (24'A0;heures), tandis que les signatures'A0;WildFire peuvent être générées et publiées dans les 15'A0;minutes suivant la détection d'une menace. Vous pouvez alors choisir l'action Alerte au lieu de Bloquer en cas de signature'A0;WildFire. *Pour accroître la sécurité, clonez le profil antivirus par défaut et définissez l'action et l'action WildFire de tous les décodeurs sur reset-both (réinitialiser les deux) et associez le profil à toutes les règles de politiques de sécurité qui autorisent le trafic.*
Exceptions d'applications et actions	La table **Applications Exception (Exceptions d'applications)** vous permet de définir les applications à ne pas inspecter. Par exemple, pour bloquer l'ensemble du trafic HTTP excepté pour une application spécifique, vous pouvez définir un profil antivirus pour lequel l'application est une exception. L'action **Block (Bloquer)** est utilisée pour le décodeur HTTP, et l'action **Allow (Autoriser)** pour faire de l'application une exception. Pour chaque exception d'application, sélectionnez l'action à prendre lorsqu'une menace est détectée. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité. Pour trouver une application, commencez à saisir le nom de l'application dans la zone de saisie. Une liste d'applications correspondantes s'affiche pour vous permettre de faire votre choix. *Si vous croyez qu'une application légitime est mal identifiée comme portant un virus (faux positif), ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre le virus incorrectement identifié. Une fois le problème réglé, supprimez l'exception du profil.*

Onglet Exception de virus

Utilisez l'onglet **Virus Exceptions (Exceptions de virus)** pour définir une liste de menaces que le profil antivirus ignorera.

Créez une exception uniquement si vous êtes certain qu'un virus identifié n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre la signature de virus incorrectement identifiée. Une fois le problème réglé, supprimez immédiatement l'exception du profil.

ID de menace	Pour ajouter des menaces précises que vous souhaitez ignorer, saisissez un ID de menace à la fois et cliquez sur **Add (Ajouter)**. Les ID de menace figurent dans le journal des menaces. Voir Surveillance > Journaux.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Profil antispyware

Vous pouvez joindre un profil antispyware à une règle de politique de sécurité pour détecter des connexions initiées par des logiciels espions et des logiciels malveillants de commande et de contrôle (C2) installés sur les systèmes de votre réseau. Vous pouvez choisir l'un des deux profils antispyware prédéfinis à associer à une règle de politique de sécurité. Chaque profil présente un ensemble de règles prédéfinies (avec des signatures de menaces) classées en fonction de la gravité de la menace ; chaque signature de menace contient une action par *défaut* définie par Palo Alto Networks.

- Par défaut : le profil par défaut utilise l'action par défaut pour chaque signature, comme indiqué par Palo Alto Networks, lors de la création d'une signature.
- Strict : le profil strict applique un contrôle prioritaire sur l'action définie dans le fichier de signature, dans le cas de menaces présentant un niveau de gravité critique, élevé et moyen, par une action **reset-both (réinitialiser les deux)**. L'action par défaut est exécutée dans le cas de menaces présentant un niveau de gravité moyen et informatif.
- Vous pouvez également créer des profils personnalisés. Par exemple, vous pouvez diminuer la rigueur de l'inspection antispyware pour le trafic entre des zones de sécurité de confiance et maximiser l'inspection du trafic reçu d'Internet ou du trafic envoyé à des actifs protégés, tels que les fermes de serveurs.

Les tableaux suivants décrivent les paramètres des profils antispyware :

Paramètres des profils antispyware	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils antispyware lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil antispyware dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

Onglet Règles

Les règles antispyware vous permettent de définir une action et un niveau de gravité personnalisés à l'égard des menaces, un nom de menace contenant le texte que vous saisissez et/ou une catégorie de menace, comme les logiciels publicitaires.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils antispyware	Description
Cliquez pour **Ajouter** une nouvelle règle, ou vous pouvez sélectionner une règle existante et sélectionnez **Rechercher des signatures correspondantes** pour filtrer les signatures de menaces en fonction de cette règle.	
Nom de la règle	Indiquez le nom de la règle.
Nom de la menace	Saisissez **any (indifférent)** pour que toutes les signatures soient vérifiées, ou saisissez du texte pour vérifier les signatures dont le nom contient le texte saisi.
Catégorie	Choisissez une catégorie ou choisissez **any (n'importe laquelle)** pour faire correspondre toutes les catégories.
Action (Action)	Sélectionnez une action pour chaque menace. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité.  *Pour accroître la sécurité, utilisez les paramètres d'action du profil strict prédéfini.*
Capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés. Sélectionnez **single-packet (un seul paquet)** pour capturer un seul paquet lorsqu'une menace est détectée, ou **extended-capture (capture étendue)** pour capturer de 1 à 50 paquets (la valeur par défaut est de 5 paquets). La capture étendue détaille le contexte de la menace, lors de l'analyse des journaux des menaces. Pour visualiser la capture de paquets, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**, puis recherchez l'entrée du journal qui vous intéresse et cliquez sur la flèche vers le bas de couleur verte dans la seconde colonne. Pour définir le nombre de paquets à capturer, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID**, puis modifiez les paramètres Content-ID™. Les paquets sont capturés uniquement si l'action affiche **allow (autoriser)** ou **alert (alerter)**. Si l'action **block (bloquer)** est définie, la session est immédiatement fermée.  *Activez la capture étendue pour les événements présentant un niveau de gravité critique, élevé et moyen. Utilisez la valeur de capture étendue par défaut de 5 paquets, qui procure suffisamment d'informations pour analyser la menace dans la plupart des cas. (Un trafic de capture de paquets trop important peut entraîner l'abandon des capture de paquets.) N'activez pas la capture étendue pour les événements informatifs et présentant un niveau de gravité faible, car elle n'est pas très utile comparativement à la capture d'informations sur les événements présentant une gravité plus élevée et crée un volume relativement élevé de trafic de faible valeur.*
Sévérité	Choisissez un niveau de gravité (**critical (critique)**, **high (élevé)**, **medium (moyen)**, **low (faible)** ou **informational (informations)**).
Onglet Exceptions	

© 2020 Palo Alto Networks, Inc.

Paramètres des profils antispyware	Description
Cet onglet vous permet de modifier l'action d'une signature spécifique. Par exemple, vous pouvez générer des alertes pour un ensemble spécifique de signatures et bloquer tous les paquets correspondant à toutes les autres signatures. Les exceptions de menaces sont généralement configurées lorsque des faux positifs se produisent. Pour faciliter la gestion des exceptions de menaces, vous pouvez les ajouter directement depuis la liste **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**. Vérifiez que vous disposez des dernières mises à jour afin d'être protégé contre de nouvelles menaces. Vérifiez également que vous disposez des nouvelles signatures contre tout faux positif.	
Exceptions	Sélectionnez **Enable (Activer)** pour chaque menace à laquelle vous voulez affecter une action, ou sélectionnez **All (Tout)** pour répondre à toutes les menaces répertoriées. La liste dépend de l'hôte, de la catégorie et du niveau de gravité sélectionnés. Si la liste est vide, il n'existe aucune menace pour les sélections en cours. Utilisez les exemptions d'adresses IP pour ajouter des filtres d'adresse IP à une exception de menace. Si des adresses IP sont ajoutées à une exception de menace, l'action d'exception pour cette signature ne l'emporte sur l'action de la règle que si la signature est déclenchée par une session dont l'adresse IP source ou de destination correspond à une adresse IP de l'exception. Vous pouvez ajouter jusqu'à 100 adresses IP par signature. Avec cette option, vous n'avez pas besoin de créer une nouvelle règle de politique et un nouveau profil de vulnérabilité pour créer une exception pour une adresse IP spécifique. *Créez une exception uniquement si vous êtes certain qu'un signature identifiée en tant que spyware n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre la signature incorrectement identifiée. Une fois le problème réglé, supprimez l'exception du profil.*
Onglet DNS Signatures (Signatures DNS) Le paramètre **DNS Signatures (Signatures DNS)** offre un moyen supplémentaire d'identifier les hôtes infectés sur un réseau. Ces signatures détectent les requêtes DNS de noms d'hôte associés à des logiciels malveillants.	
Onglet Policies & Settings (Politiques et paramètres) Les **DNS Signature Policies (Politiques de signature DNS)**vous permettent de sélectionner et de configurer des sources de politique de signature DNS de manière à autoriser ou bloquer ces requêtes, à les placer dans un entonnoir ou à générer une alerte, comme dans le cas des signatures antivirus courantes. Les hôtes qui lancent des requêtes DNS associées à des sites malveillants figureront dans le rapport du Botnet. De plus, vous pouvez spécifier les adresses IP entonnoirs dans les **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)** si vous mettez en entonnoir des requêtes DNS malveillantes.	
Signature DNS source	Cette option vous permet de sélectionner les listes auxquelles vous voulez affecter une action lorsqu'une requête DNS survient. Il existe deux options de politique de signature DNS source par défaut : • **Signature DNS de contenu Palo Alto Networks** : une liste de signatures téléchargeable locale qui est mise à jour par les mises à jour de contenu dynamiques.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils antispyware	Description
	• **Sécurité DNS de Palo Alto Networks** : un service de sécurité DNS basé sur le nuage qui effectue l'analyse proactive des données DNS et qui fournit un accès complet à la base de données des signatures DNS de Palo Alto Networks. *Le service exige l'achat et l'activation de la licence de sécurité DNS en plus de la licence de prévention des menaces.* Par défaut, les signatures DNS de contenu Palo Alto Networks accessibles localement sont mises en entonnoir, tandis que la sécurité DNS basée sur le cloud est définie sur autoriser. Si vous souhaitez activer la mise en entonnoir à l'aide de la sécurité DNS, vous devez configurer l'action des requêtes DNS pour la mise en entonnoir. L'adresse par défaut utilisée pour la mise en entonnoir appartient à Palo Alto Networks (sinkhole.paloaltonetworks.com). Cette adresse n'est pas statique et ne peut être modifiée par l'intermédiaire d'une mise à jour de contenu sur le pare-feu ou Panorama. **Add (Ajoutez)** une nouvelle liste dynamique externe correspondant au type de domaine que vous avez créé. Pour créer une nouvelle liste, voir Objets > Listes dynamiques externes.
Action pour les requêtes DNS	Choisissez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées. Les options sont les suivantes : **alert (alerte)**, **allow (autoriser)**, **block (bloquer)** ou **sinkhole (mise en entonnoir)**. La **sinkhole (mise en entonnoir)** est l'action par défaut pour les signatures DNS de Palo Alto Networks. L'action DNS Sinkhole (piège DNS) permet aux administrateurs d'identifier les hôtes infectés sur le réseau à l'aide du trafic DNS, même lorsque le pare-feu est au nord d'un serveur DNS local (le pare-feu ne peut pas voir l'auteur de la requête DNS). Lorsqu'une licence de prévention des menaces est installée et qu'un profil antispyware est activé dans un profil de sécurité, une signature DNS se déclenche en cas de requête DNS dirigée vers des domaines malveillants. Dans un déploiement type où le pare-feu est au nord du serveur DNS local, le journal des menaces identifie le résolveur DNS local comme la source du trafic plutôt que l'hôte réellement infecté. La mise en entonnoir des requêtes DNS malveillantes résout ce problème de visibilité en falsifiant des réponses aux requêtes dirigées vers des domaines malveillants, de manière à ce que les clients tentant de se connecter à ces domaines (pour la commande et le contrôle, par exemple) se connectent plutôt à une adresse IP définie par l'administrateur. Les hôtes infectés peuvent ensuite être facilement identifiés dans les journaux du trafic, car tout hôte tentant de se connecter à l'adresse IP entonnoir est probablement infecté par des logiciels malveillants. *Activez la mise en entonnoir DNS lorsque le pare-feu ne peut pas voir l'auteur de la requête DNS (normalement lorsque le pare-feu est au nord d'un serveur DNS local) afin de pouvoir identifier les hôtes infectés. Si vous ne pouvez mettre le trafic en entonnoir, bloquez-le.*
Capture de paquets	Sélectionnez cette option pour une source donnée pour capturer des paquets identifiés.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils antispyware	Description
	Activez la capture de paquets sur le trafic mis en entonnoir afin de pouvoir l'analyser et d'obtenir des renseignements sur l'hôte infecté.
Paramètres de la mise en entonnoir DNS	Après que l'action Entonnoir est définie pour une source de signature DNS, précisez l'adresse IPv4 ou IPv6 qui sera utilisée pour la mise en entonnoir. Par défaut, l'adresse IP entonnoir est définie sur un serveur de Palo Alto Networks. Vous pouvez ensuite utiliser les journaux du trafic ou concevoir un rapport personnalisé qui filtre l'adresse IP entonnoir afin d'identifier les clients infectés. Voici la séquence d'événements qui se produit lorsqu'une requête DNS est mise en entonnoir : Un logiciel malveillant se trouvant sur un ordinateur client infecté envoie une requête'A0;DNS pour résoudre un hôte malveillant sur Internet. La requête DNS du client est envoyée à un serveur DS interne, qui interroge ensuite un serveur DNS public de l'autre côté du pare-feu. La requête DNS correspond à une entrée DNS dans la base de données de signatures DNS précisée ; ainsi l'action Entonnoir sera effectuée dans le cas de cette requête. Le client infecté tente ensuite de démarrer une session avec l'hôte, mais utilise l'adresse IP falsifiée à la place. L'adresse IP falsifiée est l'adresse définie dans l'onglet Signatures DNS des profils antispyware, lorsque l'action Entonnoir est sélectionnée. L'administrateur est alerté lors de la présence d'une requête DNS malveillante dans le journal des menaces. Il peut alors rechercher l'adresse IP entonnoir dans les journaux du trafic et facilement localiser l'adresse IP du client qui tente de démarrer une session avec l'adresse IP entonnoir.
Onglet Exceptions Les **Exceptions** à la signature DNS vous permettent d'exclure les ID des menaces de l'application de la politique. Pour ajouter des menaces spécifiquesque vous souhaitez exclure de la politique, sélectionnez ou cherchez un **Threat ID (ID de menace)**, puis cliquez sur **Enable (Activer)**. Chaque entrée fournit l'**ID** de menace, le **Name (Nom)** et le **FQDN** de l'objet.	

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Protection contre les vulnérabilités

Une règle de politique de sécurité peut inclure la définition d'un profil de protection contre les vulnérabilités qui détermine le niveau de protection en fonction d'un dépassement de capacité de la mémoire tampon, de l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités du système. Il existe deux profils prédéfinis disponibles pour la fonction Protection contre les vulnérabilités'A0;:

- Le profil **default (par défaut)** applique l'action par défaut à l'ensemble des vulnérabilités du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Il ne détecte pas les événements de protection contre les vulnérabilités dont le niveau de gravité est faible et informations.
- Le profil **strict** applique la réponse de blocage à l'ensemble des événements de protection contre les logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Par ailleurs, il utilise l'action par défaut pour les événements de protection contre les vulnérabilités dont le niveau de gravité est faible et informations.

Il est possible d'utiliser des profils personnalisés pour limiter les inspections de vulnérabilité sur le trafic entre des zones de sécurité de confiance ou au contraire renforcer la protection sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs. Pour appliquer des profils de protection contre les vulnérabilités à des politiques de sécurité, reportez-vous à la section Politiques > Sécurité.



Appliquez un profil de protection contre les vulnérabilités à chaque règle de politique de sécurité qui autorise le trafic en vue d'assurer la protection contre le dépassement de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités côté client et côté serveur.

Les paramètres Règles définissent des ensembles de signatures à activer, ainsi que des actions à prendre lorsqu'une signature est déclenchée.

Le paramètre Exceptions vous permet de modifier la réponse à une signature spécifique. Par exemple, vous pouvez bloquer tous les paquets qui correspondent à une signature à l'exception de celui sélectionné, ce qui génère une alerte. L'onglet **Exception** offre des fonctions de filtrage.

La page **Vulnerability Protection (Protection contre les vulnérabilités)** présente un ensemble de colonnes par défaut. D'autres colonnes d'informations sont disponibles depuis le sélecteur de colonnes. Cliquez sur la flèche à droite de l'en-tête d'une colonne et faites votre sélection dans le sous-menu Colonnes.

Les tableaux suivants décrivent les paramètres des profils de protection contre les vulnérabilités :

Paramètres des profils de protection contre les vulnérabilités	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de protection contre les vulnérabilités pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection contre les vulnérabilités	Description
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Protection contre la vulnérabilité dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Onglet Règles	
Nom de la règle	Indiquez un nom permettant d'identifier la règle.
Nom de la menace	Indiquez une chaîne textuelle à vérifier. Le pare-feu applique un ensemble de signatures à la règle en recherchant cette chaîne textuelle dans les noms des signatures.
Liste CVE	Indiquez quelles sont les failles et vulnérabilités communes (CVE) si vous voulez limiter les signatures à celles qui correspondent également aux CVE définies. Chaque CVE se présente sous le format CVE-aaaa-xxxx, où aaaa correspond à l'année et xxxx est son identifiant unique. Vous pouvez effectuer une recherche de chaîne dans ce champ. Par exemple, pour trouver les vulnérabilités correspondant à l'année 2011, saisissez « 2011 ».
Type d'hôte	Précisez s'il faut limiter les signatures pour la règle à celles qui se trouvent du côté du client, à celles qui se trouvent du côté du serveur ou aux deux (**any (indifférent)**).
Sévérité	Sélectionnez le niveau de gravité à vérifier (**informational (informations)**, **low (faible)**, **medium (moyen)**, **high (élevé)** ou **critical (critique)**) si vous voulez limiter les signatures à celles qui correspondent également au niveau de gravité spécifié.
Action (Action)	Sélectionnez l'action à appliquer lors du déclenchement d'une règle. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité. L'action **Default (Par défaut)** est basée sur l'action prédéfinie incluse dans chaque signature fournie par Palo Alto Networks. Pour afficher l'action par défaut correspondant à une signature, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection**

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection contre les vulnérabilités	Description
	contre les vulnérabilités) et cliquez sur **Add (Ajouter)** ou sélectionnez un profil existant. Cliquez sur l'onglet **Exceptions** puis sur **Show all signatures (Montrer toutes les signatures)** pour voir une liste de toutes les signatures et l'**Action** associée. *Pour renforcer la sécurité, définissez l'action des événements du client et du serveur dont le niveau de gravité est critique, élevé et moyen sur reset-both (réinitialiser les deux événements) et utilisez l'action par défaut pour les événements informatifs et présentant un niveau de gravité faible.*
Capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés. Sélectionnez **single-packet (un seul paquet)** pour capturer un seul paquet lorsqu'une menace est détectée, ou **extended-capture (capture étendue)** pour capturer de 1 à 50 paquets (la valeur par défaut est de 5 paquets). La capture étendue détaille le contexte de la menace, lors de l'analyse des journaux des menaces. Pour visualiser la capture de paquets, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**, puis recherchez l'entrée du journal qui vous intéresse et cliquez sur la flèche vers le bas de couleur verte dans la seconde colonne. Pour définir le nombre de paquets à capturer, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** puis modifiez les paramètres Content-ID. Les paquets sont capturés uniquement si l'action affiche **allow (autoriser)** ou **alert (alerter)**. Si l'action **block (bloquer)** est définie, la session est immédiatement fermée. *Activez la capture étendue pour les événements présentant un niveau de gravité critique, élevé et moyen et la capture d'un seul paquet pour les événements présentant un niveau de gravité faible. Utilisez la valeur de capture étendue par défaut de 5 paquets, qui procure suffisamment d'informations pour analyser la menace dans la plupart des cas. (Un trafic de capture de paquets trop important peut entraîner l'abandon des capture de paquets.) N'activez pas la capture des paquets pour les événements informatifs, car elle n'est pas très utile comparativement à la capture d'informations sur les événements présentant une gravité plus élevée et crée un volume relativement élevé de trafic de faible valeur.* *Appliquez la capture des paquets étendue en utilisant la même logique que vous utilisez pour décider du trafic à journaliser ; prenez des captures étendues du trafic que vous journalisez, y compris le trafic que vous bloquez.*
Onglet Exceptions	

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection contre les vulnérabilités	Description
Threats	*Créez une exception uniquement si vous êtes certain qu'une menace identifiée n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse enquêter sur la menace incorrectement identifiée. Une fois le problème réglé, supprimez immédiatement l'exception du profil.* Sélectionnez **Enable (Activer)** pour chaque menace à laquelle vous voulez affecter une action, ou sélectionnez **All (Tout)** pour répondre à toutes les menaces répertoriées. La liste dépend de l'hôte, de la catégorie et du niveau de gravité sélectionnés. Si la liste est vide, il n'existe aucune menace pour les sélections en cours. Choisissez une action dans la liste déroulante ou dans le menu **Action** en haut de la liste pour appliquer la même action à l'ensemble des menaces. Si vous avez sélectionné **Show All (Montrer toutes les signatures)**, la liste de toutes les signatures est alors affichée. Sinon, seules les signatures qui sont des exceptions sont affichées. Sélectionnez **Packet Capture (Capture de paquets)** pour capturer des paquets identifiés. La base de données des signatures contre les vulnérabilités contient des signatures qui indiquent une attaque par force brute ; par exemple, l'ID de menace 40001 est déclenché par une attaque FTP par force brute. Les signatures de force brute sont déclenchées lorsqu'un événement survient au-delà d'un seuil temporel donné. Les seuils sont préconfigurés pour les signatures de force brute et peuvent être modifiés en cliquant sur modifier ( ) à côté du nom de la menace sous l'onglet **Vulnerability (Vulnérabilité)** (avec sélection de l'option **Custom (Personnaliser)**). Vous pouvez définir le nombre d'accès par unité de temps et si le seuil s'applique à la source, la destination ou les deux. Des seuils peuvent être appliqués à une adresse IP source, une adresse IP de destination ou à une combinaison d'adresses IP source et de destination. l'action par défaut est indiquée entre parenthèses. La colonne CVE affiche les identifiants correspondant aux failles et vulnérabilités communes (CVE). Ces identifiants uniques concernent les vulnérabilités de sécurité informatique courantes. Cliquez sur la colonne Exemptions d'adresses IP pour **ajouter** des filtres d'adresse IP à une exception de menace. Lorsque vous ajoutez une adresse IP à une exception de menace, l'action d'exception pour cette signature ne l'emportera sur l'action de la règle que si la signature est déclenchée par une session dont l'adresse IP source ou de destination correspond à une adresse IP de l'exception. Vous pouvez ajouter jusqu'à 100 adresses IP par signature. Vous devez entrer une adresse IP unicast (c'est-à-dire une adresse sans masque de réseau), telle que 10.1.7.8 ou 2001:db8:123:1::1. En ajoutant des exemptions d'adresses IP, vous n'avez pas besoin de créer

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection contre les vulnérabilités	Description
	une nouvelle règle de politique et un nouveau profil de vulnérabilité pour créer une exception pour une adresse IP spécifique.
ID constructeur	Indiquez des ID constructeur si vous voulez limiter les signatures à celles correspondant également aux ID constructeur définis. Par exemple, les ID constructeur correspondant à Microsoft se présentent sous la forme MSaa-xxx, où aa correspond à l'année au format deux chiffres et xxx est son identifiant unique. Pour trouver le constructeur Microsoft pour l'année 2009, saisissez « MS09 » dans le champ de recherche.
Catégorie	Sélectionnez une catégorie de vulnérabilité si vous voulez limiter les signatures à celles correspondant à cette catégorie.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Filtrage des URL

Vous pouvez utiliser les profils de URL filtering (filtrage des URL) pour non seulement contrôler l'accès au contenu Web, mais également pour contrôler l'interaction des utilisateurs avec le contenu Web.

Que voulez-vous faire ?	Reportez-vous à la section :
Contrôler l'accès aux sites Web en fonction de la catégorie URL.	Catégories de filtrage des URL
Détectez les envois d'informations d'identification d'entreprise, puis décidez les catégories d'URL auxquelles les utilisateurs peuvent soumettre des informations d'identification.	Détection des informations d'identification de l'utilisateur Catégories de filtrage des URL
Bloquez les résultats de la recherche si l'utilisateur final n'utilise pas les paramètres de recherche sécurisée les plus stricts dans la recherche.	Paramètres de filtrage des URL
Activer la journalisation des en-têtes HTTP.	Paramètres de filtrage des URL
Contrôler l'accès aux sites Web au moyen d'en-têtes HTTP personnalisés.	Insertion de l'en-tête HTTP
Vous souhaitez en savoir plus ?	• En savoir plus sur la configuration du filtrage des URL. • Utilisez les catégories d'URL pour empêcher l'hameçonnage des informations d'identification. • Pour créer des catégories d'URL personnalisées, voir Objets > Objets personnalisés > Catégorie d'URL. • Pour importer une liste d'URL que vous souhaitez appliquer, sélectionnez Objets > Listes dynamiques externes.

Paramètres généraux du filtrage des URL

Le tableau suivant décrit les paramètres généraux de filtrage des URL.

Paramètres généraux	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de filtrage des URL pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).

© 2020 Palo Alto Networks, Inc.

Paramètres généraux	Description
Partagé	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de filtrage des URL dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

Catégories de filtrage des URL

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)** > **Categories (Catégories)** pour contrôler l'accès aux sites Web en fonction des catégories d'URL.

Paramètres de catégories	Description
Catégorie	Affiche les catégories d'URL et les listes pour lesquelles vous pouvez définir l'accès Web et la politique d'utilisation. Par défaut, les autorisations **Site Access (Accès au site)** et **User Credential Submission (Envoi des informations d'identification de l'utilisateur)** pour toutes les catégories sont définies sur **Allow (Autoriser)**. Les catégories d'URL et les listes sont groupées dans trois menus déroulants : • **Custom URL Categories (Catégories d'URL personnalisées)** : Sélectionnez Objets > Objets personnalisés > Catégories d'URL pour définir une catégorie d'URL personnalisée. Vous pouvez fonder les catégories d'URL personnalisées sur une liste d'URL ou sur plusieurs catégories prédéfinies. • **External Dynamic URL Lists (Listes d'URL dynamiques externes)** : Sélectionnez Objets > Listes dynamiques externes pour permettre au pare-feu d'importer une liste d'URL d'un serveur Web. • **Pre-defined Categories (Catégories prédéfinies)** : Dresse la liste de toutes les catégories d'URL définies par PAN-DB, l'URL Palo Alto Networks et la base de données IP du cloud.  *Block (Bloquez) toutes les catégories d'URL dangereuses qui sont connues pour vous protéger contre l'infiltration d'exploitations, le téléchargement de fichiers malveillants, les activités de commande et de contrôle et l'exfiltration de données : command-and-control (commande et contrôle), copyright-infringement (violation des droits d'auteur), dynamic-dns (DNS dynamique), extremism (extrémisme), malware (logiciel malveillant), phishing (hameçonnage), proxy-avoidance-and-anonymizers (évitement de proxy*

© 2020 Palo Alto Networks, Inc.

Paramètres de catégories	Description
	et anonymiseurs), unknown (inconnu), newly-registered-domain (domaine nouvellement enregistré), grayware (logiciel indésirable) et parked (parqué). *Pour introduire graduellement une politique d'interdiction, définissez les catégories sur Continuer et créez une page de réponse personnalisée pour informer vos utilisateurs de vos politiques d'utilisation et les prévenir qu'ils consultent un site qui pourrait présenter une menace. À l'issue d'une période de temps appropriée, passez à une politique qui bloque ces sites éventuellement malveillants.*
Accès au site	Pour chaque catégorie d'URL, sélectionnez la mesure à prendre si un utilisateur tente d'accéder à une URL de cette catégorie : • **alert (alerte)** - Autorise l'accès au site Web, mais ajoute une alerte dans le journal des URL chaque fois qu'un utilisateur accède à cette URL.  *Définissez la valeur d'alert (alerte) en tant qu'action pour les catégories de trafic que vous ne bloquez pas. Ainsi, il journalise les tentatives d'accès et procure un aperçu du trafic.* • **allow (autoriser)** - Autorise l'accès au site Web.  *Comme l'option allow (autoriser) ne journalise pas le trafic non bloqué, définissez alert (alerter) en tant qu'action pour les catégories de trafic que vous ne bloquez pas si vous voulez journaliser les tentatives d'accès et obtenir un aperçu du trafic.* • **block (bloquer)** - Interdit l'accès au site Web. Si l'Accès au site à une catégorie d'URL est défini sur bloqué, les autorisations d'Envoi des informations d'identification de l'utilisateur sont également automatiquement définies sur bloquer. • **Continue (continuer)** : affiche aux utilisateurs une page d'avertissement pour les décourager d'accéder au site Web. L'utilisateur doit alors **Continue (continuer)** vers le site Web s'il décide d'ignorer l'avertissement.  *Les pages continue (avertissement) ne s'affichent pas correctement sur les machines client configurées pour utiliser un serveur proxy.* • **override (remplacer)** : affiche une page de réponse qui invite l'utilisateur à saisir un mot de passe valide afin d'accéder au site. Configurez les paramètres de Contrôle prioritaire sur l'URL par l'administrateur (**Device (Périphérique)** > **Setup (Configuration)** > **Content ID (ID de contenu)**) pour gérer le mot de passe et les autres paramètres de contrôle prioritaire. (Reportez-vous également au tableau Paramètres de gestion dans Périphérique > Configuration > Content-ID).  *Les pages Override (Contrôle prioritaire) ne s'affichent pas correctement sur les machines client configurées pour utiliser un serveur proxy.*

© 2020 Palo Alto Networks, Inc.

Paramètres de catégories	Description
	• **none (aucun)** (catégorie d'URL personnalisée uniquement) – Si vous avez créé des catégories d'URL personnalisées, définissez l'action sur **none (aucun)** pour autoriser le pare-feu à hériter de la catégorie de filtrage des URL que lui a assignée votre fournisseur de base de données d'URL. La définition de l'action sur **none (aucune)** vous donne la souplesse d'ignorer des catégories personnalisées dans votre profil de filtrage des URL tout en vous permettant d'utiliser la catégorie d'URL personnalisée en tant que critère de correspondance dans les règles de politique (sécurité, déchiffrement et de QoS) afin d'effectuer des exceptions ou d'affecter diverses actions. Pour supprimer une catégorie d'URL personnalisée, vous devez définir l'action sur **none (aucune)** dans tous les profils où la catégorie personnalisée est utilisée. Pour plus d'informations sur les catégories d'URL personnalisées, voir Objets > Objets personnalisés > Catégorie d'URL.
Envoi des informations d'identification de l'utilisateur	Pour chaque catégorie d'URL, sélectionnez les **User Credential Submissions (Envois des informations d'identification de l'utilisateur)** pour autoriser les utilisateurs à saisir des informations d'identification d'entreprise valides sur une URL de cette catégorie ou le leur interdire. Avant de pouvoir contrôler les envois des informations d'identification de l'utilisateur en fonction de la catégorie d'URL, vous devez activer la détection d'envoi d'informations d'identification (sélectionnez l'onglet **Détection des informations d'identification de l'utilisateur**). Les catégories d'URL avec **Site Access (Accès au site)** défini sur bloquer sont automatiquement configurées pour bloquer les envois d'informations d'identification de l'utilisateur. • **alert (alerter)** – Autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal de Filtrage des URL chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie. • **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web. • **block (bloquer)** - Empêche les utilisateurs de saisir des informations d'identification sur le site Web. Une page de réponse antihameçonnage par défaut bloque les envois d'informations d'identification de l'utilisateur. • **continue (continuer)** – Affiche une page de réponse aux utilisateurs qui les invite à sélectionner Continuer pour saisir des informations d'identification sur le site. Par défaut, une page de poursuite antihameçonnage s'affiche pour avertir les utilisateurs lorsqu'ils tentent de saisir des informations d'identification sur des sites pour lesquels la saisie d'informations d'identification n'est pas recommandée. Vous pouvez choisir de créer une page de réponse personnalisée pour avertir les utilisateurs contre les tentatives d'hameçonnage ou pour leur apprendre à ne pas réutiliser des informations d'identification d'entreprise valides sur d'autres sites Web.
Vérifier la catégorie d'URL	Cliquez pour accéder à la base de données PAN-DB URL Filtering où vous pouvez saisir une URL ou une adresse IP pour afficher les informations de catégorisation.

© 2020 Palo Alto Networks, Inc.

Paramètres de catégories	Description
Filtrage dynamique des URL (activé par défaut) (Configurable pour BrightCloud uniquement)	Sélectionnez cette option pour activer la recherche sur le Cloud afin de catégoriser l'URL. Cette option est appelée si la base de données locale ne parvient pas à catégoriser l'URL. Si l'URL n'est pas résolue au bout de 5 secondes, la réponse qui s'affiche est `Not resolved URL`. *Pour PAN-DB, cette option est activée par défaut et n'est pas configurable.*

Paramètres de filtrage des URL

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)** > **URL Filtering Settings (Paramètres de filtrage des URL)** pour appliquer des paramètres de recherche sécurisés et pour activer la journalisation des en-têtes HTTP.

Paramètres de filtrage des URL	Descriptions
Consigner la page de conteneur uniquement Par défaut : Activé	Sélectionnez cette option pour ne consigner que les URL qui correspondent au type de contenu défini. Le pare-feu ne journalise pas les liens Web liés aux journaux au cours de la session, comme les liens de publicités et de contenu, qui réduit la journalisation et la charge mémoire tout en journalisant les URL pertinents. *Si vous utilisez des proxys qui masquent l'adresse IP initiale de la source, activez l'option X-Forwarded-For de la journalisation de l'en-tête HTTP pour préserver l'adresse IP initiale de l'utilisateur qui initie la requête de la page Web.*
Activer la mise en œuvre de la recherche sécurisée Par défaut : Désactivé Une licence de filtrage des URL n'est pas requise pour utiliser cette fonctionnalité.	Sélectionnez cette option pour mettre en œuvre le filtrage strict de la recherche sécurisée. De nombreux moteurs de recherche incluent un paramètre de recherche sécurisée qui filtre les images et vidéos réservées aux adultes dans le trafic renvoyé d'une recherche. Lorsque vous sélectionnez le paramètre pour Activer la mise en œuvre de la recherche sécurisée, le pare-feu bloque les résultats de la recherche si l'utilisateur final n'utilise pas les paramètres de recherche sécurisée les plus stricts dans sa recherche. Le pare-feu peut appliquer la recherche sécurisée pour les moteurs de recherche suivants : Google, Yahoo, Bing, Yandex et YouTube. Il s'agit d'un paramètre visant à fournir le meilleur résultat possible et les moteurs de recherche ne garantissent nullement que son fonctionnement soit compatible avec tous les sites Web. Pour utiliser la mise en œuvre de la recherche sécurisée, vous devez activer ce paramètre, puis associer le profil de filtrage des URL à une règle de politique de Sécurité. Le pare-feu bloquera alors tout trafic renvoyé d'une recherche correspondant qui n'utilise pas les paramètres de recherche sécurisée les plus stricts.

© 2020 Palo Alto Networks, Inc.

Paramètres de filtrage des URL	Descriptions
	Si vous effectuez une recherche sur Yahoo'A0;Japan (yahoo.co.jp) alors que vous êtes connecté à votre compte'A0;Yahoo, l'option de verrouillage du paramètre de recherche doit également être activée. *Pour empêcher les utilisateurs de contourner cette fonction en utilisant d'autres moteurs de recherche, configurez le profil de filtrage des URL pour bloquer la catégorie Moteurs de recherche et autoriser l'accès à Google, Bing, Yahoo, Yandex et YouTube.*
Journalisation de l'en-tête HTTP	L'activation de la journalisation de l'en-tête'A0;HTTP fournit une visibilité des attributs inclus dans la demande'A0;HTTP envoyée à un serveur. Lorsque cette option est activée, une ou plusieurs des paires attributs/valeurs suivantes sont enregistrées dans le journal de filtrage des URL'A0;: • User-Agent : le navigateur Web utilisé par l'utilisateur pour accéder à l'URL. Ces informations sont incluses dans la demande HTTP envoyée au serveur. Par exemple, la valeur'A0;User-Agent dans le journal peut être Internet'A0;Explorer ou Firefox. Celle-ci peut contenir 1'A0;024'A0;caractères maximum. • Referer : l'URL de la page Web associée qui relie l'utilisateur à une autre page Web ; il s'agit de la source qui a redirigé (référé) l'utilisateur vers (à) la page Web demandée. La valeur Referer peut contenir 256'A0;caractères maximum. • X-Forwarded-For : champ d'en-tête qui conserve l'adresse IP de l'utilisateur ayant demandé la page Web. Elle vous permet d'identifier l'adresse IP de l'utilisateur, ce qui est particulièrement utile si vous disposez d'un serveur proxy sur votre réseau ou que vous avez mis en œuvre la traduction NAT source, qui masque l'adresse IP de l'utilisateur de telle manière que toutes les demandes semblent provenir de l'adresse IP du serveur proxy ou d'une adresse IP commune. La valeur X-Forwarded-For peut contenir 128'A0;caractères maximum.

Détection des informations d'identification de l'utilisateur

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)** > **User Credential Detection(Détection des informations d'identification de l'utilisateur)** pour que le pare-feu détecte les situations où les utilisateurs soumettent leurs informations d'identification d'entreprise.

Configurez la détection des informations d'identification de l'utilisateur pour que les utilisateurs puissent transmettre leurs informations d'identification uniquement aux sites qui correspondent à des catégories d'URL spécifiées, ce qui permet de réduire la surface d'attaque en empêchant la soumission d'informations d'identification à des sites appartenant à des catégories non approuvées. Si vous bloquez toutes les catégories d'URL dans un profil de filtrage des URL pour la soumission des informations d'identification, vous n'avez pas à vérifier les informations d'identification.

Le pare-feu utilise une des trois méthodes pour détecter les informations d'identification valides saisies sur ces pages Web. Chaque méthode nécessite l'utilisation de User-ID™ qui permet au pare-feu de comparer les envois de nom d'utilisateur et de mot de passe aux pages Web et des informations d'identification

© 2020 Palo Alto Networks, Inc.

d'entreprise valides. Sélectionnez une de ces méthodes pour ensuite continuer à Empêcher l'hameçonnage des informations d'identification en fonction de la catégorie d'URL.

Vous devez configurer le pare-feu pour decrypt (déchiffrer) le trafic que vous voulez surveiller pour les informations d'identification des utilisateurs.

Paramètres de Détection des informations d'identification de l'utilisateur	Description
Utilisateur IP	Cette méthode de détection des informations d'identification vérifie les envois de noms d'utilisateur valides. Vous pouvez utiliser cette méthode pour détecter les envois d'informations d'identification incluant un nom d'utilisateur d'entreprise valide (quel que soit le mot de passe qui l'accompagne). Le pare-feu détermine une correspondance de nom d'utilisateur en vérifiant que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour utiliser cette méthode, le pare-feu fait correspondre le nom d'utilisateur saisi à la table de mappage adresse IP / nom d'utilisateur. Pour utiliser cette méthode, vous pouvez utiliser n'importe laquelle des méthodes de mappage d'utilisateur décrites dans Mappage d'adresses IP à des utilisateurs.
mappage de groupe	Le pare-feu détermine si le nom d'utilisateur qu'un utilisateur saisit sur un site restreint correspond à un nom d'utilisateur d'entreprise valide. Pour ce faire, le pare-feu fait correspondre le nom d'utilisateur saisi à la liste des noms d'utilisateur dans sa table de mappage utilisateur / groupe pour détecter quand les utilisateurs saisissent un nom d'utilisateur sur un site d'une catégorie restreinte. Cette méthode ne vérifie que les envois de noms d'utilisateur d'entreprise en fonction de l'appartenance à un groupe LDAP, ce qui simplifie la configuration, mais l'expose davantage aux faux positifs. Vous devez activer le mappage de groupe pour utiliser cette méthode.
Informations d'identification du domaine	Cette méthode de détection des informations d'identification permet au pare-feu de vérifier un nom d'utilisateur d'entreprise valide et le mot de passe y étant associé. Le pare-feu détermine si le nom d'utilisateur et le mot de passe saisis par un utilisateur correspondent au nom d'utilisateur d'entreprise et au mot de passe de ce même utilisateur. Pour ce faire, le pare-feu doit être capable de faire correspondre les envois d'informations d'identification à des noms d'utilisateur et des mots de passe d'entreprise valides et vérifier que le nom d'utilisateur saisi correspond à l'adresse IP de l'utilisateur connecté. Ce mode est pris en charge uniquement avec l'agent User-ID basé sur Windows et exige que l'agent User-ID soit installé sur un contrôleur de domaine en lecture seule (RODC) et équipé de l'Extension service d'informations d'identification User-ID. Pour utiliser cette méthode, vous devez également activer l'option permettant à User-ID d'effectuer le Mappage d'adresses IP à des utilisateurs en utilisant l'une des méthodes de mappage d'utilisateur prises en charge, y compris la Politique d'authentification, Captive Portal et GlobalProtect™. Reportez-vous à la section Empêcher le hameçonnage des informations d'identification pour plus d'informations sur chacune des méthodes que le

© 2020 Palo Alto Networks, Inc.

Paramètres de Détection des informations d'identification de l'utilisateur	Description
	pare-feu peut utiliser pour vérifier les envois d'informations d'identification d'entreprise valides et sur les étapes permettant d'activer la prévention contre l'hameçonnage.
Gravité des journaux détectée par un nom d'utilisateur valide	Définissez la gravité pour les journaux qui indiquent que le pare-feu a détecté une saisie de nom d'utilisateur valide sur un site Web. Cette gravité des journaux est associée à des événements où un nom d'utilisateur valide est saisi sur des sites Web avec des autorisations d'envoi des informations d'identification pour alerter, bloquer ou continuer. Les journaux qui enregistrent quand un utilisateur saisit un nom d'utilisateur valide sur un site Web pour lequel les envois d'informations d'identification sont autorisés ont une gravité de niveau information. Sélectionnez **Catégories** pour vérifier ou ajuster les catégories d'URL auxquelles les envois d'informations d'identification sont autorisés et bloqués. *Définissez la gravité des journaux sur moyenne ou plus.*

Insertion de l'en-tête HTTP

Pour activer la gestion de l'accès aux applications Web par le pare-feu en insérant des en-têtes HTTP et leurs valeurs dans des requêtes HTTP, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)** > **HTTP Header Insertion (Insertion de l'en-tête HTTP)**.

Le pare-feu prend en charge l'insertion d'en-têtes pour le trafic HTTP/1.x uniquement ; le pare-feu ne prend pas en charge l'insertion d'en-têtes pour trafic HTTP/2.

Vous pouvez créer des entrées d'insertion en fonction d'un type d'insertion d'en-tête HTTP prédéfini ou vous pouvez créer votre propre type personnalisé. L'insertion d'en-têtes s'effectue généralement pour les en-têtes HTTP personnalisés, mais vous pouvez également insérer des en-têtes HTTP standard.

L'insertion d'un en-tête se produit lorsque :

1. Une requête HTTP correspond à une règle de politique de sécurité qui possède une ou plusieurs entrées d'insertion d'un en-tête HTTP configurées.
2. Un domaine spécifié correspond à un domaine qui se trouve dans l'en-tête Hôte HTTP.
3. L'action est tout sauf `block (bloquer)`.

Le pare-feu peut procéder à l'insertion de l'en-tête HTTP seulement pour les méthodes GET, POST, PUT et HEAD.

Si vous activez l'insertion de l'en-tête HTTP et que l'en-tête identifié est absent d'une requête, le pare-feu insère l'en-tête. Si l'en-tête identifié existe déjà dans la requête, le pare-feu remplace alors les valeurs de l'en-tête par celles que vous avez indiquées.

Add (Ajoutez) une entrée d'insertion ou sélectionnez une entrée d'insertion existante pour la modifier. Au besoin, vous pouvez également sélectionner une entrée d'insertion et la **Delete (Supprimer)**.

© 2020 Palo Alto Networks, Inc.

L'action de la liste d'interdictions prise par défaut à l'égard d'une nouvelle entrée d'insertion d'en-tête HTTP est Block (Bloquer). Si vous souhaitez qu'une action différente soit prise, allez à Catégories de filtrage des URL et sélectionnez l'action appropriée. Vous pouvez également ajouter l'entrée d'insertion à un profil pour lequel l'action souhaitée est configurée.

Paramètres d'insertion de l'en-tête HTTP	Description
Name (Nom)	Le **Name (Nom)** de cette entrée d'insertion de l'en-tête HTTP.
Type	Le **Type** d'entrée que vous voulez créer. Les entrées peuvent être prédéfinies ou personnalisées. Le pare-feu utilise les mises à jour du contenu pour remplir et maintenir les entrées prédéfinies. Si vous souhaitez inclure le nom d'utilisateur dans l'en-tête HTTP, sélectionnez **Dynamic Fields (Champs dynamiques)**.
Domaines	L'insertion d'un en-tête se produit lorsqu'un domaine de cette liste correspond à l'en-tête Hôte de la requête HTTP. Si vous créez une entrée prédéfinie, la liste des domaines est prédéfinie dans une mise à jour de contenu. Cette façon de faire suffit pour la plupart des cas pratiques, mais vous pouvez ajouter ou supprimer des domaines, au besoin. Si vous voulez créer une entrée personnalisée, **Add (Ajouter)** au moins un domaine à la liste. Chaque nom de domaine peut comporter un maximum de 256 caractères et vous pouvez identifier un maximum de 50 domaines pour chaque entrée. Vous pouvez utiliser un astérisque (*) comme caractère générique pour trouver une correspondance avec toute requête de domaine spécifié (par exemple, *.etrade.com).
En-tête	Lorsque vous créez une entrée prédéfinie, la liste des en-têtes est renseignée dans le cadre d'une mise à jour de contenu. Cette façon de faire suffit pour la plupart des cas pratiques, mais vous pouvez ajouter ou supprimer des en-têtes, au besoin. Lorsque vous créez une entrée personnalisée, ajoutez un ou plusieurs en-têtes (maximum de cinq) à cette liste. Les noms des en-têtes peuvent comporter un maximum de 100 caractères, mais ne peuvent inclure d'espace. Si vous souhaitez inclure le nom d'utilisateur dans l'en-tête HTTP, sélectionnez **X-Authenticated-User** puis sélectionnez la **Value (Valeur)**, ou **Add (Ajoutez)** un nouvel en-tête.
Valeur	Configurez la **Value (Valeur)** en utilisant un maximum de 512 caractères. La valeur d'en-tête varie selon l'information que vous désirez inclure dans l'en-tête HTTP pour les domaines spécifiés. Par exemple, manage user access to SaaS applications (gérez l'accès des utilisateurs aux applications SaaS) en sélectionnant des predefined types (types prédéfinis) ou en utilisant des custom entries (saisies personnalisées). Pour inclure le nom d'utilisateur dans l'en-tête HTTP, sélectionnez le domaine et le format du nom d'utilisateur que l'appareil de sécurité nécessite :

© 2020 Palo Alto Networks, Inc.

Paramètres d'insertion de l'en-tête HTTP	Description
	• **`($domain)\($user)`** • **`WinNT://($domain)/($user)`** Vous pouvez également saisir un format personnalisé en utilisant les jetons dynamiques **`($user)`** et **`($domain)`** (par exemple, **`($user)@($domain)`**). Le pare-feu remplit les jetons dynamiques de l'utilisateur et du domaine en utilisant le nom d'utilisateur principal dans le profil de mappage de groupe. *Utilisez chaque jeton dynamique **`($user)`** et **`($domain)`** une seule fois par valeur.*
Journaux	Sélectionnez **Log (Journal)** pour activer la journalisation de cette entrée d'insertion d'en-tête.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Blocage des fichiers

Vous pouvez joindre un profil de blocage des fichiers à une règle de politique de sécurité (Politiques > Sécurité) pour empêcher les utilisateurs de charger ou de télécharger des types de fichiers donnés ou de générer une alerte lorsqu'un utilisateur tente de charger ou de télécharger des types de fichiers donnés.



Pour accroître la sécurité, appliquez le profil strict prédéfini. Si vous devez prendre en charge des applications critiques qui utilisent un type de fichier que le profil strict bloque, clonez le profil strict et n'apportez que les exceptions de type de fichier dont vous avez besoin. Appliquez le profil cloné à une règle de politique de sécurité qui restreint l'exception uniquement aux sources, aux destinations et aux utilisateurs qui doivent utiliser le type de fichier. Vous pouvez également utiliser la Direction pour restreindre l'exception au chargement ou au téléchargement.

Si vous ne bloquez pas l'ensemble des fichiers PE Windows, envoyez tous les fichiers inconnus à WildFire pour qu'ils soient analysés. Pour les comptes d'utilisateur, définissez l'action sur continue (continuer) pour empêcher les téléchargements drive-by dans le cadre desquels des sites Web, des courriels ou des fenêtres contextuelles malveillants amènent les utilisateurs à télécharger des fichiers malveillants par inadvertance. Informez les utilisateurs qu'une invite à continuer le transfert d'un fichier qui a été lancé à leur insu pourrait indiquer qu'ils sont en train d'effectuer un téléchargement malveillant.

Les tableaux suivants décrivent les paramètres des profils de blocage des fichiers.

Paramètres des profils de blocage des fichiers	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de blocage des fichiers pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de blocage des fichiers dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut,

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de blocage des fichiers	Description
	ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Règles	Définissez une ou plusieurs règles pour préciser l'action à prendre (le cas échéant) pour les types de fichier sélectionnés. Pour ajouter une règle, renseignez les informations suivantes et cliquez sur **Add (Ajouter)** : • **Name (Nom)** - Saisissez un nom pour la règle (31 caractères maximum). • **Applications** - Sélectionnez les applications auxquelles la règle s'applique ou sélectionnez **any (indifférent)**. • **File Types (Types de fichier)** - Cliquez dans le champ Types de fichier, puis cliquez sur **Add (Ajouter)** pour afficher une liste des types de fichier pris en charge. Cliquez sur un type de fichier pour l'ajouter au profil ; continuez à ajouter d'autres types de fichier, au besoin. Si vous sélectionnez **any (indifférent)**, l'action définie est prise à l'égard de tous les types de fichier pris en charge. • **Direction** - Sélectionnez la direction du transfert de fichiers (**Upload (Charger)**, **Download (Télécharger)** ou **Both (Les deux)**). • **Action** - Sélectionnez l'action à prendre lorsque les types de fichier sélectionnés sont détectés : • **alert (alerte)** - Une entrée est ajoutée dans le journal des menaces. • **continue (continuer)** - Un message indique à l'utilisateur qu'un téléchargement a été demandé et exige sa confirmation. L'objectif est de prévenir l'utilisateur d'un possible téléchargement effectué à son insu (téléchargement 'AB; drive-by 'BB;) et de lui donner l'opportunité de poursuivre ou d'arrêter le téléchargement. Lorsque vous créez un profil de blocage des fichiers à l'aide de l'action **continue (continuer)**, vous pouvez uniquement choisir l'application **web-browsing (navigation-web)**. Si vous choisissez une autre application, le trafic correspondant à la règle de politique de sécurité ne traverse pas le pare-feu car aucune page vous invitant à continuer ne s'affiche. • **block (bloquer)** - Le fichier est bloqué.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Analyse WildFire

Utilisez un profil d'analyse WildFire pour indiquer le fichier WildFire à analyser localement sur l'équipement WildFire ou dans le Cloud WildFire. Vous pouvez indiquer le trafic à transférer vers le Cloud public ou privé en fonction du type de fichier, de l'application ou du sens de transmission du fichier (chargement ou téléchargement). Après avoir créé un profil d'analyse WildFire, l'ajout de ce profil à une politique (**Policies (Politiques)** > **Security (Sécurité)**) vous permettra d'appliquer les paramètres du profil à n'importe quel trafic correspondant à cette politique (par exemple, une catégorie d'URL définie dans la politique).



Utilisez le profil par défaut prédéfini pour transférer tous les fichiers inconnus à WildFire à des fins d'analyse. De plus, définissez les mises à jour de contenu des appareils WildFire pour qu'elles soient téléchargées et installées toutes les minutes. Vous disposerez ainsi du soutien le plus récent.

Paramètres du profil d'analyse WildFire	
Name (Nom)	Donnez un nom descriptif au profil d'analyse WildFire (31 caractères maximum). Ce nom apparaîtra dans la liste des profils d'analyse WildFire disponibles au moment de la définition d'une règle de politique de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Décrivez éventuellement les règles du profil ou l'utilisation prévue du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Protection contre la vulnérabilité dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Règles	Définissez une ou plusieurs règles pour indiquer le trafic à transférer vers le Cloud public WildFire ou vers l'équipement WildFire (Cloud privé) pour analyse. • Donnez un **Name (Nom)** descriptif aux règles que vous ajoutez au profil (31 caractères maximum). • Ajoutez une **Application** afin que le trafic de l'application corresponde à la règle et qu'il soit transféré vers la destination d'analyse définie. • Sélectionnez un **File Type (Type de fichier)** à analyser dans la destination d'analyse définie de la règle.

© 2020 Palo Alto Networks, Inc.

Paramètres du profil d'analyse WildFire	
	 *Un cloud privé Wildfire (hébergé par un appareil WildFire) ne prend pas en charge l'analyse des fichiers APK, Mac OS X, d'archivage ou linux.* • Appliquez la règle au trafic en fonction du **Direction (Sens)** du transfert. Vous pouvez appliquer la règle pour charger du trafic et/ou télécharger du trafic. • Sélectionnez la **Destination** du trafic à transférer pour analyse : • Sélectionnez Cloud public afin que l'ensemble du trafic correspondant à la règle soit transféré vers le Cloud public WildFire pour analyse. • Sélectionnez Cloud privé afin que l'ensemble du trafic correspondant à la règle soit transféré vers l'équipement WildFire pour analyse.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Filtrage des données

Le filtrage de données permet au pare-feu de détecter des informations sensibles, telles que les numéros de carte de crédit ou de sécurité sociale ou les documents internes de l'entreprise, et d'empêcher ces données de quitter un réseau sécurisé. Avant d'activer le filtrage des données, sélectionnez Objets > Objets personnalisés > Modèles de données pour définir le type de données que vous souhaitez filtrer (comme les numéros de sécurité sociale ou les titres des documents contenant le mot « confidentiel »). Vous pouvez ajouter plusieurs objets de modèle de données à un seul profil de filtrage des données et, lorsqu'il est joint à une règle de politique de sécurité, le pare-feu analyse le trafic autorisé pour chaque motif de données et bloque le trafic correspondant en fonction des paramètres du profil de filtrage de données.

Paramètres des profils de filtrage des données	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de filtrage des données dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Capture de données	Sélectionnez cette option pour collecter automatiquement les données bloquées par le filtre.  *Indiquez un mot de passe pour l'option Gérer la protection des données à la page Paramètres pour afficher vos données capturées. Reportez-vous à la section Périphérique > Configuration > Gestion.*

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de filtrage des données	Description
Modèle de données	Ajoutez un modèle de données existant qui sera utilisé pour filtrer ou sélectionnez **Nouveau** pour configurer un nouvel objet de modèle de données (Objets > Objets personnalisés > Modèles de données).
Applications	Désignez les applications à inclure dans la règle de filtrage'A0;: • Choisissez **any (indifférent)** pour appliquer le filtre à toutes les applications répertoriées. Cette sélection ne bloque pas toutes les applications possibles, mais seulement celles qui sont répertoriées. • Cliquez sur **Add (Ajouter)** pour désigner des applications individuelles.
Types de fichier	Indiquez les types de fichier à inclure dans la règle de filtrage : • Choisissez **any (indifférent)** pour appliquer le filtre à tous les types de fichier répertoriés. Cette sélection ne bloque pas tous les types de fichier possibles mais seulement ceux qui sont répertoriés. • Cliquez sur **Add (Ajouter)** pour désigner des types de fichier individuels.
Direction	Précisez si le filtre doit être appliqué dans la direction du chargement, du téléchargement ou dans les deux directions.
Seuil d'alerte	Précisez combien de fois le modèle de données doit être détecté dans un fichier pour déclencher une alerte.
Seuil de blocage	Bloquez les fichiers qui contiennent de nombreux exemples du modèle de données.
Gravité des journaux	Définissez la gravité du journal enregistrée pour les événements qui correspondent à cette règle de profil du filtrage des données.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Protection DoS

Les profils de protection DoS permettent le ciblage de haute précision et l'amélioration des profils de protection de zone. Un profil de protection DoS indique les taux de seuil auxquels les nouvelles connexions par seconde (cps) déclenchent une alarme et une mesure (indiquée dans la politique de protection DoS). Le profil de protection DoS indique également le taux maximal de connexions par seconde et la durée pendant laquelle une adresse IP bloquée reste sur la liste des adresses IP bloquées. Vous spécifiez un profil de protection DoS dans une règle de politique de protection DoS, dans laquelle vous spécifiez les critères selon lesquels les paquets correspondent à la règle, et la règle de politique détermine les périphériques auxquels le profil s'applique.



Créez les profils et politiques de protection DoS visant à protéger les périphériques individuels critiques ou les petits groupes de périphériques, particulièrement les périphériques Internet, comme les serveurs Web et les serveurs de bases de données.

Vous pouvez configurer des profils de protection DoS agrégés et classés. Vous pouvez appliquer un profil agrégé, un profil classé ou un profil de chaque type à une règle de politique de protection DoS. Si vous appliquez les deux types de profil à une règle, le pare-feu applique d'abord le profil agrégé, puis applique le profil classé, au besoin.

- Dans un profil de protection DoS classé, **Classified (Classé)** est sélectionné en tant que **Type**. Lorsque vous appliquez un profil de protection DoS classé à une règle de protection DoS dont l'action est définie sur **Protect (Protéger)**, le pare-feu compte les connexions vers les seuils cps du profil si le paquet répond au type d'adresse spécifié : source-ip-only, destination-ip-only ou src-dest-ip-both.
- L'option **Aggregate (Agrégé)** d'un profil de protection DoS est sélectionnée en tant que **Type**. Lorsque vous appliquez un profil de protection DoS agrégé à une règle de protection DoS dont l'action est définie sur **Protect (Protéger)**, le pare-feu compte toutes les connexions (le nombre combiné de connexions pour le groupe de périphériques spécifiés dans la règle) qui répondent aux critères de la règle vers les seuils CPS du profil.

Pour appliquer un profil de protection DoS à une politique de protection DoS, voir Politiques > Protection DoS.



Si vous disposez d'un environnement de systèmes virtuels multiples (multi-vsys) et que vous avez configuré les paramètres suivants :

- *les zones externes pour permettre la communication entre les systèmes virtuels et*
- *les passerelles partagées pour permettre aux systèmes virtuels de partager une interface commune et une adresse IP unique pour les communications externes, alors*

Les mécanismes de protection DoS et de zone suivants sont désactivés dans la zone externe :

- *Cookies SYN*
- *Fragmentation IP*
- *ICMPv6*

Pour activer la fragmentation IP et la protection ICMPv6, vous devez créer un profil de protection de zone distinct pour la passerelle partagée.

Pour protéger la passerelle partagée contre la saturation SYN, vous pouvez appliquer un profil de protection contre la saturation SYN avec l'abandon anticipé aléatoire ou les cookies SYN. Sur une zone externe, seul Abandon anticipé aléatoire est disponible pour la protection contre la saturation SYN.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection DoS	
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de protection DoS dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Type	Sélectionnez l'un des types de profil suivants : • **Aggregate (Agrégé)** - Appliquez les seuils DoS configurés dans le profil à l'ensemble des connexions qui correspondent aux critères de la règle à laquelle ce profil est appliqué. Par exemple, une règle agrégée disposant d'un **Alarm Rate (taux d'alarme)** de saturation SYN de 10 000 CPS compte les connexions combinées de tous les périphériques correspondant à la règle DoS. Lorsque le CPS du groupe est supérieur à 10 000 CPS, l'alarme est alors déclenchée, peu importe la répartition des CPS parmi les périphériques. • **Classified (Classé)** - Appliquez les seuils DoS configurés dans le profil à chaque connexion individuelle qui correspond aux critères de classification (adresse IP source, adresse IP de destination ou paire d'adresses IP source et de destination). Par exemple, une règle classée comportant un **Alarm Rate (Taux d'alarme)** de saturation SYN de 10 000 CPS permet un maximum de 10 000 CPS par périphérique et déclenche une alarme lorsqu'un périphérique individuel spécifié dans la règle DoS dépasse 10 000 CPS.
Onglet Protection contre la saturation	
Onglet Saturation SYN Onglet Saturation UDP Onglet Saturation ICMP Onglet Saturation ICMPv6	Sélectionnez cette option pour activer le type de protection contre la saturation indiqué sur l'onglet et précisez les paramètres suivants : • **Action** – (**Saturation SYN** uniquement) Action que le pare-feu effectue si l'action de la politique de protection DoS est **Protégée** et si les CPS atteignent le **Activate Rate (Taux d'activation)**. Choisissez l'une des options suivantes :

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection DoS	
Onglet Saturation Autre IP	• **Abandon anticipé aléatoire** – Abandonne des paquets de façon aléatoire lorsque les connexions par seconde atteignent le seuil du **Taux d'activation**. • **Cookies SYN** - Utilisation de cookies SYN pour indiquer qu'il n'est pas nécessaire d'abandonner des connexions face à une attaque par saturation SYN.  *Commencez par les cookies SYN, qui traitent le trafic légitime équitablement, mais consomment plus de ressources du pare-feu. Surveillez le processus et l'utilisation de la mémoire, et si les cookies SYN consomment un trop grand nombre de ressources, passez à RED. Utilisez toujours RED si vous ne disposez pas d'un périphérique de prévention DDoS dédié devant le réseau (Internet) pour vous protéger d'attaques DoS de grand volume.* • **Alarm Rate (Taux d'alarme)** - Indiquez le taux de seuil (cps) pour générer une alarme DoS (plage de 0 à 2 000 000 cps ; valeur par défaut de 10 000 cps). Pour les profils classés, la meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen du périphérique afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes. Pour les profils agrégés, la meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen. Surveillez et ajustez les seuils selon vos besoins. • **Taux d'activation** - Indiquez le taux de seuil (cps) auquel une réponse DoS est activée. La réponse DoS est configurée dans le champ **Action** du profil de protection DoS (abandon anticipé aléatoire ou cookies SYN). La plage du **Taux d'activation** est comprise entre 0 et 2 000 000 cps. La valeur par défaut est 10 000 cps. Si le profil **Action** est défini sur **Abandon anticipé aléatoire** (RED), lorsque les connexions entrantes par seconde atteignent le seuil du **Taux d'activation**, RED se produit. Si le taux de cps augmente, le taux RED augmente en fonction d'un algorithme. Le pare-feu continue avec RED jusqu'à ce que le taux de cps atteigne le seuil du **Max Rate (Taux max)**. Les profils classés appliquent des limites CPS exactes à des périphériques individuels et vous fondez ces limites sur la capacité des périphériques protégés. Ainsi, vous n'avez donc pas à limiter le CPS graduellement et vous pouvez définir le **Activate Rate (Taux d'activation)** au même seuil que le **Max Rate (Taux max.)**. Définissez le **Activate Rate (Taux d'activation)** sur une valeur plus faible que celle du **Max Rate (Taux max.)** uniquement si vous souhaitez commencer à abandonner le trafic en direction d'un serveur individuel avant qu'il n'atteigne le **Max Rate (Taux max.)**. Pour les profils agrégés, fixez le seuil juste au-dessus du taux de CPS du groupe. Surveillez et ajustez les seuils selon vos besoins. • **Taux max.** - Indiquez le taux de seuil des connexions entrantes par seconde autorisées par le pare-feu. Lorsque le seuil du **Taux max** est atteint, le pare-feu abandonne l'ensemble des nouvelles connexions (la

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection DoS	
	plage est comprise entre 2 et 2 000 000 cps ; la valeur par défaut est 40 000 cps). Pour les profils classés, fondez le **Max Rate (Taux max)** sur la capacité des périphériques que vous protégez afin d'éviter leur saturation. Pour les profils agrégés, fixez le **Max Rate (Taux max.)** sur une valeur allant de 80 à 90 % de la capacité du groupe. Surveillez et ajustez les seuils selon vos besoins. • **Durée du blocage** – Indiquez la durée (secondes) pendant laquelle l'adresse IP offensante reste sur la liste des adresses IP bloquées et pendant laquelle les connexions avec l'adresse IP sont bloquées. Le pare-feu ne compte pas les paquets qui arrivent pendant la durée du blocage à l'égard des seuils du Taux d'alarme, du Taux d'activation ou du Taux max (la plage est comprise entre 1 et 21 600 secondes ; la valeur par défaut est 300 secondes).
Onglet Protection des ressources	
Sessions	Sélectionnez cette option pour activer la protection des ressources.
Limite max. de sessions simultanées	Indiquez le nombre maximum de sessions simultanées. • Pour le type de profil **agrégé**, cette limite s'applique à l'ensemble du trafic correspondant à la règle de protection DoS à laquelle le profil de protection DoS est appliqué. • Pour le type de profil **classé**, cette limite s'applique au trafic classé (IP source, IP de destination ou les deux) correspondant à la règle de protection DoS à laquelle le profil de protection DoS est appliqué.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Protection GTP

Le profil de protection GTP permet au pare-feu d'inspecter le trafic GTP. Pour afficher ce profil, vous devez activer la sécurité GTP dans Périphérique > Configuration > Gestion.

Les options du profil vous permettent d'activer l'inspection d'état de GTP v1-C, GTP v2-C et GTP-U, d'activer la validation du protocole pour GTPv1-C, GTP v2-C et GTP-U, d'activer l'inspection du contenu de GTP-U pour analyser les données utilisateur dans les tunnels GTP-U. Elles vous permettent également de filtrer les sessions GTP en fonction de l'APN, du préfixe IMSI et du RAT, et d'éviter l'usurpation de l'adresse IP de l'utilisateur final pour protéger les abonnés mobiles contre la surfacturation.

Paramètres d'un profil d'inspection GTP	
Inspection GTP	
GTP-C	• Sélectionnez **Inspection d'état** pour permettre au pare-feu d'inspecter **GTPv1-C**, **GTPv2-C** ou les deux. Lorsque vous activez l'inspection d'état, le pare-feu utilise l'adresse IP source, le port source, l'adresse IP de destination, le port de destination, le protocole et les identifiants du point d'extrémité du tunnel (TEID) pour assurer le suivi d'une session GTP. Il vérifie et valide également l'ordre des différents types de messages GTP qui sont utilisés pour établir un tunnel GTP. Le TEID identifie de manière unique les points d'extrémité du tunnel GSN. Les tunnels pour une liaison montante et une liaison descendante sont séparés et utilisent un TEID différent. • Sélectionnez l'**Action Blocage** ou **Alerte** prise par le pare-feu pour répondre à une absence de vérification de la validité. L'action d'alerte permet le trafic, mais génère un journal tandis que l'action de blocage rejette le trafic et génère un journal. • Indiquez les contrôles de validité que le pare-feu doit effectuer sur un en-tête GTP et sur les éléments d'informations (IE) d'une charge utile. Le pare-feu utilise l'action de blocage ou d'alerte que vous sélectionnez ci-dessous pour gérer l'erreur. Vous pouvez configurer le pare-feu pour valider : • **Éléments d'informations réservés** – Vérifie les messages GTPv1-C ou GTPv2-C qui utilisent des valeurs d'IE réservés. • **Out of Order IE (Éléments d'informations hors commande)** (GTPv1-C uniquement) – Vérifie que l'ordre des IE dans les messages GTPv1-C est exact. • **Longueur des éléments d'informations** – Vérifie les messages GTPv1-C ou GTPv2-C ayant une longueur d'IE invalide. • **Champ réservé dans l'en-tête** – Vérifie les paquets mal formés qui utilisent des valeurs invalides ou des valeurs réservées dans un en-tête. • **Type de message non pris en charge** – Vérifie les types de messages inconnus ou incorrects.
GTP-U	L'activation de l'inspection par état pour GTPv1-C et/ou GTPv20C active automatiquement l'inspection par état GTP-U.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil d'inspection GTP	
	Vous pouvez spécifier les contrôles de validité suivants pour les charges utiles GTP-U. • **Éléments d'informations réservés** – Vérifie les messages GTP-U qui utilisent des valeurs d'IE réservés. • **Éléments d'informations hors ligne** – Vérifie que l'ordre des IE dans les messages GTP-U est correct. • **Longueur des éléments d'informations** – Vérifie les messages ayant une longueur d'IE incorrecte. • **Champ réservé dans l'en-tête** – Vérifie les paquets mal formés qui utilisent des valeurs invalides ou des valeurs réservées dans un en-tête. • **Type de message non pris en charge** – Vérifie les types de messages inconnus ou incorrects. De plus, vous pouvez également configurer une action d'autorisation, de blocage ou d'alerte pour : • **Usurpation de l'adresse IP de l'utilisateur final** – Configurez le pare-feu pour bloquer ou émettre une alerte lorsque l'adresse IP source dans un paquet GTP-U de l'équipement utilisateur de l'abonné n'est pas identique à l'adresse IP dans le message GTP-C correspondant échangé pendant la configuration du tunnel. • **GTP dans GTP –** Vous pouvez configurer le pare-feu pour bloquer ou émettre une alerte lorsqu'il détecte un message GTP dans GTP. Lors de la détection, le pare-feu génère un journal GTP avec un niveau de gravité critique. • Activez l'**Inspection du contenu GTP-U** si vous souhaitez inspecter et appliquer la politique à la charge utile des données utilisateur dans un paquet GTP-U. L'inspection du contenu GTP-U vous permet de mettre en corrélation les informations IMSI et les informations IMEI issues des messages GTP-C avec le trafic IP encapsulé dans les paquets GTP-U.
Options de filtrage	
Filtrage RAT	Par défaut, toutes les technologies d'accès radioélectrique (RAT) sont autorisées. Les messages GTP-C de demande de création de PDF et de demande de création de sessions sont filtrés ou autorisés en fonction du filtre RAT. Vous pouvez indiquer s'il faut autoriser, bloquer ou alerter les technologies d'accès à distance (RAT) suivantes que l'équipement utilisateur utilise pour accéder au réseau mobile principal : • **UTRAN** • **GERAN** • **RÉSEAU LOCAL SANS FIL** • **GAN** • **Évolution HSPA** • **EUTRAN** • **Virtuel** • **EUTRAN-NB-IoT**
Filtrage IMSI	L'IMSI (International Mobile Subscriber Identity) est une identification unique associée à un abonné aux réseaux GSM, UMTS et LTE qui est approvisionné par la carte du module d'identification de l'abonné (SIM).

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil d'inspection GTP	
	Une IMSI est généralement présentée comme un nombre long de 15 chiffres (8 octets), mais elle peut être plus courte. L'IMSI se compose de trois parties : • Code mobile de pays (MCC) composé de trois chiffres. Le MCC identifie uniquement le pays de domicile de l'abonné mobile. • Code de réseau mobile (MNC) composé de deux ou trois chiffres ; 2 chiffres standard européens ou 3 chiffres standard nord-américains. Le MNC identifie le PLMN domestique de l'abonné mobile. • Numéro d'identification de l'abonné mobile (MSIN) identifiant l'abonné mobile dans un PLMN. Le **IMSI Prefix (Préfixe IMSI)** combine le MCC et le MNC et vous permet d'**allow (autoriser)**, de **block (bloquer)** ou d'**alert (émettre une alerte)** concernant le trafic GTP d'un PLMN spécifique. Par défaut, tous les IMSI sont autorisés. Vous pouvez saisir manuellement ou importer un fichier csv avec un IMSI ou des préfixes IMSI dans le pare-feu. L'IMSI peut comprendre des caractères génériques, par exemple, 310* ou 240011*. Le pare-feu prend en charge, au maximum, 5 000 IMSI ou préfixes IMSI.
Filtrage APN	Le point d'accès du réseau (APN) est le point de référence entre le GGSN et le PGW dont un équipement utilisateur a besoin pour se connecter à Internet. L'APN se compose de deux parties : • L'identificateur réseau APN qui définit le réseau externe auquel le GGSN/PGW est connecté et éventuellement un service requis par la station mobile. Cette partie de l'APN est obligatoire. • L'identificateur de l'opérateur APN qui définit dans quelle ossature PLMN GPRS/EPS est situé le GGSN/PGW. Cette partie de l'APN est facultative. Par défaut, tous les APN sont autorisés. Le filtre APN vous permet d'autoriser, de bloquer ou d'émettre une alerte sur le trafic GTP en fonction de la valeur APN. Les messages GTP-C de demande de création de PDF et de demande de création de sessions sont filtrés ou autorisés en fonction des règles définies pour le filtre APN. Vous pouvez ajouter manuellement ou importer une liste de filtres APN dans le pare-feu. La valeur pour l'APN doit inclure l'ID du réseau ou le nom de domaine du réseau (par exemple, exemple.com) et, le cas échéant, l'ID de l'opérateur. Pour le filtrage APN, le caractère générique * vous permet de chercher tous les APN. Une combinaison de * et d'autres caractères n'est pas prise en charge pour les caractères génériques. Par exemple, « internet.mnc* » est traité comme un APN ordinaire et ne filtrera pas toutes les entrées qui commencent par internet.mnc. Le pare-feu prend en charge, au maximum, 1 000 filtres APN.
Nombre max. de tunnels GTP	

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil d'inspection GTP	
Nombre max. de tunnels simultanés autorisés par destination	Vous permet de limiter le nombre maximal de tunnels GTP-U à une adresse IP de destination, par exemple pour le GGSN. Plage entre 0 à 100 000 000 tunnels.
Alerte lorsque le nombre max. de tunnels simultanés par destination est atteint	Spécifiez le seuil auquel le pare-feu déclenche une alerte lorsque le nombre de tunnels GTP-U maximum à destination a été établi. Un message de journal GTP de gravité critique est généré lorsque la limite configurée pour le tunnel est atteinte.
Fréquence de journalisation	Le nombre d'événements comptés par le pare-feu avant que ce dernier génère un journal lorsque les limites configurées pour le tunnel GTP sont dépassées. Ce paramètre vous permet de réduire le volume aux messages enregistrés. Par défaut : 100 ; plage : 1-100000000
Protection contre la surfacturation	Sélectionnez le système virtuel qui sert de pare-feu Gi/SGi sur votre pare-feu. Le pare-feu Gi/SGi inspecte le trafic IP de l'abonné mobile qui parcourt l'interface Gi/SGi depuis le PGW/GGSN vers le PDN externe (réseau de données par paquets), comme Internet, et sécurise l'accès à Internet pour les abonnés mobiles. La surfacturation peut survenir lorsqu'un GGSN attribue une adresse IP précédemment utilisée depuis le pool d'adresses IP de l'utilisateur final à un abonné mobile. Lorsqu'un serveur malveillant sur Internet continue à envoyer des paquets à cette adresse IP, car il n'a pas fermé la session initiée pour l'abonné précédent et que la session est encore ouverte sur le pare-feu Gi. Pour interdire la livraison des données, chaque fois qu'un tunnel GTP est supprimé (détecté par le message de suppression du PDP ou le message de suppression de la session) ou expiré, le pare-feu activé pour la protection contre la surfacturation informe le pare-feu Gi/SGi qu'il doit supprimer toutes les sessions qui appartiennent à l'abonné de la table de session. La sécurité GTP et le pare-feu SGi/Gi doivent être configurés sur le même pare-feu physique, mais ils peuvent être dans des systèmes virtuels différents. Afin de supprimer des sessions en fonction des événements GTP-C, le pare-feu doit disposer de toutes les informations de session pertinentes, ce qui n'est possible que lorsque vous gérez le trafic à partir des interfaces SGi, S11 ou S5 pour GTPv2 et les interfaces Gi et Gn pour GTPv1 dans le réseau mobile principal.
Autres paramètres des journaux Par défaut, le pare-feu ne consigne pas les messages GTP autorisés. Vous pouvez activer de manière sélective la journalisation des messages GTP autorisés lorsque cela est nécessaire à des fins de dépannage puisque cela générera un important volume de journaux. En plus des messages des journaux autorisés, cet onglet vous permet également d'activer de manière sélective l'enregistrement des informations de localisation des utilisateurs.	
Messages GTPv1-C autorisés	Cet onglet vous permet d'activer de manière sélective la journalisation des messages GTPv1-C autorisés, si vous avez activé l'inspection d'état pour GTPv1?C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil d'inspection GTP	
	Par défaut, le pare-feu ne consigne pas les messages autorisés. Les options de journalisation pour les messages GTPv1-C autorisés sont les suivantes : • **Tunnel Management (Gestion du tunnel)** – Ces messages GTPv1-C sont utilisés pour gérer les tunnels GTP-U qui acheminent des paquets IP encapsulés et des messages de signalisation entre une paire donnée de nœuds de réseau tels que SGSN et GGSN. Il comprend des messages, tels que Créer une demande contextuelle PDP, Créer une réponse contextuelle PDP, Mettre à jour la demande contextuelle PDP, Mettre à jour la réponse contextuelle PDP, Supprimer la demande contextuelle PDP, Supprimer la réponse contextuelle PDP. • **Path Management (Gestion des chemins)** – Ces messages GTPv1?C sont généralement envoyés par le GSN ou le Contrôleur de réseau radio (RNC) à un autre GSN ou RNC pour savoir si la paire est active. Il comporte des messages tels que Demande / Réponse d'écho. • **Others (Autres)** – Ces messages incluent la gestion des emplacements, la gestion de la mobilité, la gestion des informations RAN et les messages du service de diffusion / multidiffusion de multimédia (MBMS).
Emplacement de l'utilisateur du journal	Vous permet d'inclure les informations de localisation de l'utilisateur, comme le code de zone et l'ID de cellule, dans les journaux GTP.
Capture de paquets	Vous permet de capturer des événements GTP.
Messages GTPv2-C autorisés	Cet onglet vous permet d'activer de manière sélective la journalisation des messages GTPv2-C autorisés, si vous avez activé l'inspection d'état pour GTPv2?C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin. Par défaut, le pare-feu ne consigne pas les messages autorisés. Les options de journalisation pour les messages GTPv2-C autorisés sont les suivantes : • **Tunnel Management (Gestion du tunnel)** – Ces messages GTPv2-C sont utilisés pour gérer les tunnels GTP-U qui acheminent des paquets IP encapsulés et des messages de signalisation entre une paire donnée de nœuds de réseau tels que SGW et PGW. Il comprend les types de messages suivants : Créer une demande de session, Créer une réponse de session, Créer une demande de porteur, Créer une réponse de porteur, Modifier la demande de porteur, Modifier la réponse du porteur, Supprimer une demande de session, Supprimer la réponse de session. • **Path Management (Gestion des chemins)** – Ces messages GTPv2-C sont généralement envoyés par un nœud de réseau comme SGW ou PGW à un autre PGW ou SGW pour savoir si l'homologue est actif. Il comporte des messages tels que Demande / Réponse d'écho. • **Others (Autres)** – Ces messages incluent les messages de gestion de la mobilité et les messages liés à l'accès non-3GPP.
Messages GTP-U autorisés	Cet onglet vous permet d'activer de manière sélective la journalisation des messages GTPv2-C autorisés, si vous avez activé l'inspection d'état pour GTPv1?C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil d'inspection GTP	
	Les options de journalisation pour les messages GTP-U autorisés sont les suivantes : • **Tunnel Management (Gestion du tunnel)** – Il s'agit de messages de signalisation GTP-U tels que l'Indication d'erreur. • **Path Management (Gestion des chemins)** – Ces messages GTP-U sont envoyés par un nœud de réseau (tel que eNodeB) à un autre nœud de réseau (comme SGW) pour voir si la paire est active. Il comporte des messages tels que Demande / Réponse d'écho. • **G-PDU** – Le G-PDU (GTP-U PDU) est utilisé pour transférer des paquets de données utilisateur au sein des nœuds de réseau dans le réseau de base mobile ; il se compose d'un en-tête GTP et d'un T-PDU.
Paquets G-PDU consignés par nouveau tunnel GTP-U	Activez cette option pour vérifier que le pare-feu inspecte les PDU GTP-U. Le pare-feu génère un journal pour le nombre spécifié de paquets G-PDU dans chaque nouveau tunnel GTP-U. Par défaut : Plage entre 1-10.

© 2020 Palo Alto Networks, Inc.

Objets > Profils de sécurité > Protection SCTP

Créez un profil de protection Stream Control Transmission Protocol (protocole de transmission de contrôle de flux ; SCTP) pour préciser comment le pare-feu doit valider et filtrer les blocs SCTP. Vous devez d'abord activer la Sécurité SCTP (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**) pour voir ce type de profil sous Security Profiles (Profils de sécurité). Vous pouvez également restreindre le nombre d'adresses IP par point de terminaison SCTP dans un environnement à connexions multiples et vous pouvez préciser les situations dans lesquelles le pare-feu journalise les événements SCTP. Après avoir créé un profil de protection SCTP, vous devez appliquer le profil à une règle de politique de Sécurité d'une zone.

Les modèles de pare-feu qui prennent en charge la sécurité SCTP disposent d'un profil de protection SCTP prédéfini (*default-ss7*) que vous pouvez utiliser tel quel ou que vous pouvez cloner pour vous servir de base pour la création d'un nouveau profil de protection SCTP. Sélectionnez **Object (Objets)** > **Security Profiles (Profils de sécurité)** > **SCTP Protection (Protection SCTP)**, puis sélectionnez **default-ss7** pour voir les Codes d'opération qui déclenchent une alerte pour ce profil prédéfini.

Paramètres des profils de protection SCTP	
Name (Nom)	Donnez un nom au profil de protection SCTP.
Description	Saisissez une description pour le profil de protection SCTP.
Inspection SCTP	
Bloc inconnu	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un paquet SCTP avec un bloc inconnu (le bloc n'est pas défini dans RFC3758, dans RFC4820, dans RFC4895, RFC4960, dans RFC5061 ni dans RFC 6525) : • **allow (autoriser)** (par défaut) : autorise le paquet à passer sans modification. • **alert (alerter)** : autorise le paquet à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : invalide le bloc avant de faire passer le paquet et génère un journal SCTP.
Indicateurs de blocs	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un paquet SCTP avec un indicateur de blocs qui ne correspond pas à RFC4960 : • **allow (autoriser)** (par défaut) : autorise le paquet à passer sans modification. • **alert (alerter)** : autorise le paquet à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le paquet et génère un journal SCTP.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection SCTP	
Longueur non valide	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un bloc SCTP avec une longueur non valide : • **allow (autoriser)** (par défaut) : autorise le paquet ou le bloc à passer sans modification. • **block (bloquer)** : abandonne le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux.
Limite d'adresses IP pour le multihébergement	Saisissez le nombre maximal d'adresses IP que vous pouvez configurer pour un point de terminaison SCTP avant que le pare-feu ne génère un message d'alerte (plage est comprise entre 1 et 8 ; par défaut 4). Le multihébergement SCTP est la capacité d'un point de terminaison à prendre en charge plus d'une adresse IP pour une association avec un homologue. En cas d'échec d'un chemin vers un point de terminaison, SCTP sélectionne l'une des autres adresses IP de destination fournies pour cette association.
Paramètres des journaux	Sélectionnez n'importe quelle combinaison de paramètres pour générer les journaux SCTP, soit selon les blocs autorisés, le début et la fin d'une association et les événements d'échec d'un état : • **Journaliser au début de la session** • **Journaliser en fin de session** • **Journaliser les blocs d'initialisation d'association autorisés** • **Journaliser les blocs de pulsation autorisés** • **Journaliser les blocs de fin d'association autorisés** • **Journaliser tous les blocs de contrôle** • **Journaliser les événements d'échec d'un état** Pour que le pare-feu stocke les journaux SCTP, vous devez allouer de l'espace au stockage des journaux SCTP (reportez-vous à l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
Options de filtrage	
Filtrage SCTP	
Name (Nom)	Saisissez un nom à donner au filtre SCTP.
PPID	Précisez un PPID pour le filtre SCTP : • **any (indifférent)** : amène le pare-feu à prendre l'Action que vous avez définie pour tous les blocs de données SCTP qui contiennent un PPID. • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA**

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection SCTP	
	• **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • Entrez une valeur PPID valide (une valeur qui ne se trouve pas dans la liste déroulante). Par exemple, la valeur PPID de H.323 est 13. Chaque filtre SCTP ne peut définir qu'un seul PPID. Vous pouvez toutefois définir plusieurs filtres SCTP pour un profil de Protection SCTP.
Action (Action)	Définissez l'action que le pare-feu doit prendre à l'égard des blocs de données qui contiennent le PPID indiqué : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
Les paquets SCTP sont mis en correspondance avec les filtres de la liste, de haut en bas. Si vous créez plus d'un filtre SCTP pour un profil, l'ordre dans lequel les filtres SCTP apparaissent importe. Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour modifier sa priorité relative au sein de la liste de Filtrage SCTP.	
Filtrage Diameter	
Name (Nom)	Saisissez un nom à donner au filtre Diameter.
Action (Action)	Définissez l'action que prend le pare-feu à l'égard des blocs Diameter qui contiennent les ID d'application Diameter, les codes de commande et les AVP définis. Si les blocs faisant l'objet d'une inspection comprennent l'ID d'application Diameter défini *et* n'importe lequel des Codes de commande Diameter définis *et* n'importe laquelle des AVP Diameter définies, alors : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection SCTP	
	journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
ID d'application Diameter	Définissez l'ID d'application Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. • **Indifférent** • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • **Diameter Base Accounting** • **Diameter Common Messages** • **Diameter Credit Control** Vous pouvez également entrer une valeur numérique pour un ID d'application Diameter (la plage est comprise entre 0 et 4 294 967 295). Un filtre Diameter ne peut posséder qu'un seul ID d'application.
Code de commande Diameter	Définissez les Codes de commande Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **any (indifférent)**, sélectionnez un Code de commande Diameter dans la liste déroulante et saisissez une valeur donnée (la plage est comprise entre 0 et 16 777 215). La liste déroulante n'inclut que les codes de commande qui s'appliquent à l'ID d'application Diameter sélectionné. Vous pouvez ajouter plusieurs Codes de commande Diameter dans un filtre Diameter.
AVP Diameter	Définissez la Attribute-Value Pair (paire attribut-valeur ; AVP) Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. Saisissez un ou plusieurs codes ou valeurs AVP (la plage est comprise entre 1 et 16 777 215).
Si vous créez plus d'un filtre Diameter pour un profil, l'ordre dans lequel les filtres Diameter apparaissent importe. Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour régler sa priorité relative au sein de la liste de Filtrage Diameter.	
Filtrage SS7	
Name (Nom)	Saisissez un nom à donner au filtre SS7.
Action (Action)	Définissez l'action que le pare-feu doit prendre à l'égard des blocs SS7 qui contiennent les éléments de filtrage SS7 définis. Si le bloc faisant l'objet de l'inspection contient le SSN du demandeur du sous-système de commande de connexions sémaphores *et*

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection SCTP	
	n'importe laquelle des valeurs Global Title (appellation globale ; GT) du demandeur du sous-système de commande de connexions sémaphores définies *et* n'importe lequel des Codes d'opération définis, alors : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
SSN du demandeur du sous-système de commande de connexions sémaphores	Définissez le SSN du demandeur du sous-système de commande de connexions sémaphores d'application pour un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **any-map (indifférent-mappage)** ou **Add (Ajoutez)** un des SSN de demandeur du sous-système de commande de connexions sémaphores à partir de la liste déroulante : • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **Gestion SCCP** Un filtre SS7 ne peut posséder qu'un seul SSN du demandeur du sous-système de commande de connexions sémaphores.
GT du demandeur du sous-système de commande de connexions sémaphores	Définissez la valeur GT du demandeur du sous-système de commande de connexions sémaphores d'application pour un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **Any (Indifférent)** ou **Add (Ajoutez)** une valeur numérique comportant jusqu'à 15 chiffres. Vous pouvez également saisir un groupe de valeurs GT du demandeur du sous-système de commande de connexions sémaphores à l'aide d'un préfixe. Par exemple : 876534*. Vous pouvez ajouter plusieurs valeurs GT du demandeur du sous-système de commande de connexions sémaphores dans un filtre SS7.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de protection SCTP	
	Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **INAP** et **SCCP Management (Gestion SCCP)**, cette option est désactivée.
Code d'opération	Définissez le code d'opération d'un bloc à l'égard duquel le pare-feu prend l'action définie. Pour les SSN de demandeur du sous-système de commande de connexions sémaphores suivants, sélectionnez **any (indifférent)** ou un code d'opération dans la liste déroulante, ou saisissez une valeur précise (plage comprise entre 1 et 255) : • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **CAP**, saisissez une valeur (plage comprise entre 1 et 255). Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **INAP** et **SCCP Management (Gestion SCCP)**, cette option est désactivée. Vous pouvez ajouter plusieurs Codes d'opération dans un filtre SS7.
Si vous créez plus d'un filtre SS7 pour un profil, l'ordre dans lequel les filtres SS7 apparaissent importe. Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour régler sa priorité relative au sein de la liste de Filtrage SS7.	

© 2020 Palo Alto Networks, Inc.

Objets > Groupes de profils de sécurité

Le pare-feu prend en charge la création de groupes de profils de sécurité, ce qui permet de définir des ensembles de profils de sécurité pouvant être traités en tant qu'unités, puis ajoutés aux politiques de sécurité. Par exemple, vous pouvez créer un groupe de profils de sécurité « *menaces* » qui inclut des profils antivirus, antispyware et de protection contre les vulnérabilités, puis créer une politique de sécurité comprenant ce profil « menaces ».

Les profils antivirus, antispyware, de protection contre les vulnérabilités, de filtrage des URL et de blocage des fichiers qui sont souvent appliqués ensemble peuvent être combinés en groupes de profils pour simplifier la création de politiques de sécurité.

Pour définir un nouveau profil de sécurité, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**.

Le tableau suivant décrit les paramètres des profils de sécurité :

Paramètres des groupes de profils de sécurité	Description
Name (Nom)	Saisissez un nom pour le groupe de profils (31 caractères maximum). Ce nom apparaît dans la liste de profils lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le groupe de profils soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe de profils sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe de profils sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de Groupes de profils de sécurité dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Profils	Sélectionnez un profil antivirus, antispyware, de protection contre les vulnérabilités, de filtrage des URL et/ou de blocage des fichiers à inclure dans ce groupe. Les profils de filtrage des données peuvent également figurer dans les groupes de profils de sécurité. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des données.

© 2020 Palo Alto Networks, Inc.

Objets > Transfert des journaux

Par défaut, les journaux générés par le pare-feu demeurent uniquement dans leur stockage local. Toutefois, vous pouvez utiliser Panorama™, le Service de journalisation ou des services externes (tel qu'un serveur Syslog) pour surveiller centralement les informations du journal en définissant un profil de Transfert des journaux et en l'affectant aux règles de politique de sécurité, d'authentification, de protection DoS et d'inspection des tunnels. Les profils de transfert de journaux définissent les destinations de transfert pour les Types de journaux suivants : Authentification, Filtrage des données, GTP, SCTP, Menaces, Trafic, Tunnel, Filtrage des URL et envois WildFire®.

Vous devriez transférer les journaux à Panorama ou au stockage externe pour diverses raisons, y compris la conformité, la redondance, l'exécution d'analyses, la surveillance centralisée et l'examen des comportements des menaces et des tendances à long terme. De plus, le pare-feu dispose d'une capacité de stockage des journaux limitée et supprime les plus vieux journaux au fur et à mesure que l'espace est plein. Veillez donc à transférer les journaux des menaces et les journaux WildFire.

Pour transférer d'autres types de journaux, voir Périphérique > Paramètres des journaux.

Pour activer le transfert à WildFire® des journaux ou des fichiers sur un pare-feu PA-7000 Series, vous devez d'abord configurer une Interface de carte de journal sur le pare-feu PA-7000 Series. Dès que vous configurez cette interface, le pare-feu utilise automatiquement ce port. Aucune configuration spéciale n'est requise. Vous n'avez qu'à configurer un port de données sur l'une des Network Processing Cards (cartes de traitement réseau ; NPC) du pare-feu de la série PA-7000 comme interface de type carte de journal et à vous assurer que le réseau que vous utilisez communique avec vos serveurs de journaux. Pour le transfert WildFire, le réseau doit communiquer correctement avec le cloud ou l'équipement WildFire (ou les deux).

Le tableau suivant décrit les paramètres du profil de transfert des journaux :

Paramètres des profils de transfert des journaux	Description
Name (Nom)	Saisissez un nom (jusqu'à 64 caractères) pour identifier le profil. Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de règles de politiques de sécurité. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - Si vous désactivez (décochez) cette option, le profil est disponible uniquement dans le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • **Tous les groupes de périphériques sur Panorama** - Si vous désactivez (décochez) cette option, le profil est disponible uniquement dans le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de transfert des journaux	Description
Permettre la journalisation améliorée des applications au service de journalisation (y compris les journaux de trafic et les journaux URL)	Les journaux améliorés des applications pour les services de cloud Palo Alto Networks sont disponibles avec un abonnement au Service de journalisation. La journalisation améliorée des applications permet au pare-feu de collecter les données spécialement conçues pour accroître la visibilité des activités réseau pour les applications exécutant dans l'environnement des Services de cloud Palo Alto Networks.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de transfert de journaux dans les groupes de périphériques qui héritent du profil. Cette sélection est désactivée (décochée) par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Description	Saisissez une description pour expliquer le but de ce profil de transfert des journaux.
Liste de correspondance (non étiquetée)	Il vous faut **Ajouter** un ou plusieurs profils de liste de correspondance (jusqu'à 64) qui spécifient les destinations de transfert, les filtres de journal avec attributs pour contrôler quels journaux sont transférés par le pare-feu, et les mesures à prendre pour les journaux (tel que l'étiquetage automatique). Complétez les deux champs suivants (Nom et Description) pour chaque profil de liste de correspondance.
Nom (profil de liste de correspondance)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance.
Description (profil de liste de correspondance)	Saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but de ce profil de liste de correspondance.
Type de journal	Sélectionnez le type de journal auquel profil de liste de correspondance s'applique : authentification (**auth**), **data (données)**, **gtp**, **sctp**, **threat (menaces)**, **traffic (trafic)**, **tunnel**, **URL** ou **WildFire**.
Filtre	Par défaut, le pare-feu transfère **Tous les journaux** des **Types de journaux** sélectionnés. Pour transférer un sous-ensemble des journaux, sélectionnez un filtre existant dans le menu déroulant ou sélectionnez **Générateur de filtre** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez le connecteur logique (et/ou) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les attributs disponibles dépendent du **Type de journal**.

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de transfert des journaux	Description
	• **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les critères disponibles dépendent du **Type de journal**. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. Pour display or export (afficher ou exporter) les journaux que le filtre met en correspondance, sélectionnez l'option **View Filtered Logs (Afficher les journaux filtrés)**, qui fournit les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (comme **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).
Panorama Panorama/Service de journalisation	Sélectionnez **Panorama** si vous souhaitez transmettre des journaux aux collecteurs de journaux, au serveur de gestion Panorama ou au Service de journalisation. Si vous activez cette option, vous devez configurer le transfert des journaux vers Panorama. Pour utiliser le Service de journalisation, vous devez également **Enable (Activer)** le Service de journalisation sous Périphérique > Configuration > Gestion.
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).
Actions intégrées	Cliquez pour **Ajouter** l'action à exécuter. Vous pouvez choisir entre deux types : Étiquetage et Intégration. • **Étiquetage** : Ajoutez ou supprimez automatiquement une étiquette à l'adresse IP source ou de destination dans une entrée de journal et enregistrez l'adresse IP et le mappage des étiquettes pour l'agent User-ID sur le pare-feu ou Panorama ou pour un agent User-ID distant afin que vous puissiez répondre à un événement et que vous puissiez appliquer dynamiquement la politique de sécurité. La possibilité d'étiqueter une adresse IP et d'appliquer dynamiquement une politique à l'aide de groupes d'adresses dynamiques vous offre une meilleure visibilité, un meilleur contexte et un meilleur contrôle pour appliquer de manière cohérente la politique de sécurité indépendamment de l'endroit où l'adresse IP se déplace sur votre réseau. Configurez les paramètres suivants'A0;:

© 2020 Palo Alto Networks, Inc.

Paramètres des profils de transfert des journaux	Description
	• Cliquez pour **Ajouter** une action et saisissez un nom pour la décrire. • Sélectionnez l'adresse IP cible que vous souhaitez étiqueter – **Adresse source** ou **Adresse de destination**. Vous pouvez prendre une mesure pour tous les types de journaux qui incluent une adresse IP source ou de destination dans l'entrée de journal. Vous pouvez uniquement étiqueter l'adresse IP source, dans les journaux de corrélation et les journaux de correspondance HIP. Vous ne pouvez pas configurer une action pour les journaux système et les journaux de configuration, car le type de journal ne comporte pas une adresse IP dans l'entrée de journal. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez enregistrer l'adresse IP et étiqueter le mappage sur l'agent **Local User-ID (User-ID local)** sur ce pare-feu ou Panorama, ou sur un agent **Remote User-ID (User-ID à distance)**. • Pour enregistrer l'adresse IP et étiqueter le mappage sur un agent **User-ID à distance**, sélectionnez le profil de serveur HTTP (Périphérique > Profils de serveur > HTTP) qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de l'indicateur d'adresse IP n'expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l'action Add Tag (Ajouter une étiquette).* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination. • **Intégration** : disponible uniquement pour les pare-feu VM-Series dans Azure. Cette option vous permet de transférer les journaux sélectionnés au Centre de sécurité Azure via l'action **Azure-Security-Center-Integration (Intégration au Centre de sécurité Azure)**.

© 2020 Palo Alto Networks, Inc.

Objets > Authentification

Un objet d'application d'authentification indique la méthode et le service à utiliser pour les utilisateurs finaux s'authentifiant qui accèdent à vos ressources réseau. Vous affectez l'objet aux règles de la politique d'Authentification qui appellent la méthode d'authentification et le service lorsque le trafic correspond à une règle (voir Politiques > Authentification).

Le pare-feu possède les objets d'application d'authentification prédéfinis suivants (en lecture seule) :

- **Défi de navigation par défaut** - Le pare-feu obtient de façon transparente les informations d'identification d'authentification de l'utilisateur. Si vous sélectionnez cette action, vous devez activer l'ouverture de session unique (SSO) Kerberos ou l'authentification NTLM (NT LAN Manager) lors de la Configuration du portail captif. En cas d'échec de l'authentification SSO Kerberos, le pare-feu revient à l'authentification NTLM. Si vous n'avez pas configuré NTLM, ou si l'authentification NTLM échoue, le pare-feu revient à la méthode d'authentification spécifiée dans l'objet **formulaire Web par défaut** prédéfini.
- **Formulaire Web par défaut** – Pour authentifier les utilisateurs, le pare-feu utilise le profil de certificat ou le profil d'authentification que vous avez spécifié lors de la configuration du portail captif. Si vous avez indiqué un profil d'authentification, le pare-feu ignore tous les paramètres Kerberos SSO du profil et présente une page du Portail captif pour que l'utilisateur saisisse ses informations d'authentification.
- **Aucun portail captif par défaut** – Le pare-feu évalue la politique de Sécurité sans authentifier les utilisateurs.

Avant de créer un objet d'application d'authentification personnalisé :

- Configurez un profil de serveur qui spécifie la façon de se connecter au service d'authentification (reportez-vous à la section Périphérique > Profils de serveur).
- Affectez le profil de serveur à un profil d'authentification qui indique les paramètres d'authentification comme les paramètres d'ouverture de session Kerberos unique (voir Périphérique > Profil d'authentification).

Pour créer un objet d'application d'authentification personnalisé, cliquez sur **Ajouter** et remplissez les champs suivants :

Paramètres de l'application d'authentification	Description
Name (Nom)	Saisissez un nom descriptif (jusqu'à 31 caractères) pour vous aider à identifier l'objet lors de la définition des règles d'Authentification. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que l'objet soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le **Système virtuel** sélectionné dans l'onglet **Objets**. • Chaque groupe de périphériques sur Panorama. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le **Groupe de périphériques** sélectionné dans l'onglet **Objets**.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'application d'authentification	Description
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet d'application d'authentification dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Méthode d'authentification	Sélectionnez une méthode : • **Défi de navigation** - Le pare-feu obtient de façon transparente les informations d'identification d'authentification de l'utilisateur. Si vous sélectionnez cette action, Kerberos SSO doit être activé sur le **Profil d'authentification** que vous sélectionnez ou bien vous devez avoir configuré NTLM dans les Paramètres du portail captif. En cas d'échec de l'authentification SSO Kerberos, le pare-feu revient à l'authentification NTLM. Si vous n'avez pas configuré NTLM, ou si l'authentification NTLM échoue, le pare-feu revient à l'authentification **formulaire Web**. • **Formulaire Web** – Pour authentifier les utilisateurs, le pare-feu utilise le profil de certificat que vous avez indiqué lors de la configuration du portail captif ou le **Profil d'authentification** que vous sélectionnez dans l'objet d'application d'authentification. Si vous avez sélectionné un **Profil d'authentification**, le pare-feu ignore tous les paramètres Kerberos SSO du profil et présente une page du Portail captif pour que l'utilisateur saisisse ses informations d'authentification. • **Aucun portail captif** – Le pare-feu évalue la politique de Sécurité sans authentifier les utilisateurs.
Profil d'authentification	Sélectionnez le profil d'authentification qui indique le service à utiliser pour valider l'identité des utilisateurs.
Message	Saisissez les instructions qui indiquent aux utilisateurs comment répondre à la première demande d'authentification qu'ils voient lorsque leur trafic déclenche la règle d'Authentification. Le message s'affiche dans la **Page Confort du portail captif**. Si vous ne saisissez pas de message, la page **Captive Portal Comfort Page (Page Confort du portail captif)** par défaut s'affiche (voir Périphérique > Pages de réponse). *Le pare-feu affiche la Captive Portal Comfort Page (Page Confort du portail captif) uniquement pour la première demande d'authentification (facteur) que vous définissez dans l'onglet Authentication (Authentification) du Authentication Profile (Profil d'authentification) (voir Périphérique > Profil d'authentification). Pour les demandes d'authentification multifacteur (MFA) que vous définissez dans l'onglet Facteurs du profil, le pare-feu affiche la Page de connexion MFA.*

© 2020 Palo Alto Networks, Inc.

Objets > Profils de déchiffrement

Les profils de déchiffrement vous permettent de bloquer et de contrôler des aspects précis du trafic SSL et SSH devant être déchiffré ainsi que du trafic que vous avez explicitement exclu du déchiffrement. Après avoir créé un profil de déchiffrement, vous pourrez ensuite l'ajouter à une politique de déchiffrement ; tout trafic correspondant à cette politique de déchiffrement est mis en œuvre selon les paramètres du profil.

Un profil de déchiffrement par défaut est configuré sur le pare-feu et est automatiquement inclus dans les nouvelles politiques de déchiffrement (vous ne pouvez pas modifier le profil de déchiffrement par défaut). Cliquez sur **Add (Ajouter)** pour créer un nouveau profil de déchiffrement ou sélectionnez un profil existant et cliquez sur **Clone (Cloner)** pour le cloner ou le modifier.

Que voulez-vous faire ?	Reportez-vous à la section :
Ajouter un nouveau profil de déchiffrement. Activer la mise en miroir des ports pour le trafic déchiffré.	Paramètres généraux des profils de déchiffrement
Bloquer et contrôler le trafic SSL déchiffré.	Paramètres de contrôle du trafic SSL décrypté
Bloquer et contrôler le trafic que vous avez exclu du déchiffrement (par exemple, le trafic classé comme services relatifs à la santé, au domaine médical et à la finance).	Paramètres de contrôle du trafic non déchiffré
Bloquer et contrôler le trafic SSH déchiffré.	Paramètres de contrôle du trafic SSH déchiffré

Paramètres généraux des profils de déchiffrement

Le tableau suivant décrit les paramètres généraux des profils de déchiffrement.

Profil de déchiffrement – Paramètres généraux	Description
Name (Nom)	Saisissez un nom pour le profil (**31** caractères maximum). Ce nom apparaît dans la liste des profils de déchiffrement lors de la définition des politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**.

© 2020 Palo Alto Networks, Inc.

Profil de déchiffrement – Paramètres généraux	Description
	• Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Décryptage pour les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Interface de mise en miroir du déchiffrement (Prise en charge sur tous les modèles, sauf le pare-feu VM-Series sur AWS, sur Azure, sur Édition NSX, sur Citrix SDX.)	Sélectionnez une **Interface** à utiliser pour la Mise en miroir du port de déchiffrement. *Avant d'activer la mise en miroir du port de déchiffrement, vous devez obtenir une licence Mise en miroir du port de déchiffrement, l'installer et redémarrer le pare-feu.*
Transmis uniquement (Prise en charge sur tous les modèles, sauf le pare-feu VM-Series sur AWS, sur Azure, sur Édition NSX, sur Citrix SDX.)	Sélectionnez **Forwarded Only (Transmis uniquement)** pour mettre en miroir le trafic décrypté uniquement après la mise en œuvre de la politique de sécurité. Avec cette option, seul le trafic qui est transféré vers le pare-feu est mis en miroir. Cette option est utile si vous transférez le trafic décrypté vers d'autres périphériques de détection des menaces, tels qu'un périphérique DLP (prévention des fuites de données) ou un autre système de prévention des intrusions (IPS). Si vous désélectionnez cette option (paramètre par défaut), le pare-feu mettra en miroir tout le trafic décrypté sur l'interface avant de rechercher des politiques de sécurité, ce qui vous permettra de rejouer les événements et d'analyser le trafic qui génère une menace ou déclenche une action d'abandon.

Paramètres de contrôle du trafic SSL décrypté

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour contrôler le trafic SSL qui a été déchiffré à l'aide du déchiffrement du proxy de transfert SSL ou de l'inspection SSL entrante. Vous pouvez utiliser ces paramètres pour limiter ou bloquer des sessions SSL basées sur des critères, notamment l'état du certificat du serveur externe, l'utilisation de suites de chiffrement ou de versions de protocoles non prises en charge ou la disponibilité de ressources système pour traiter le déchiffrement.

Paramètres de l'onglet Déchiffrement SSL	Description
ONGLET PROXY DE TRANSFERT SSL	
Sélectionnez des options pour limiter ou bloquer le trafic SSL décrypté à l'aide du proxy de transfert SSL.	

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
Validation des certificats du serveur – Sélectionnez des options pour contrôler les certificats du serveur dans le trafic SSL décrypté.	
Bloquer les sessions avec un certificat expiré	Mettez fin à la connexion SSL si le certificat du serveur a expiré. Cela empêche les utilisateurs d'accepter des certificats expirés et de poursuivre une session SSL.  *Bloquez les sessions avec des certificats expirés pour empêcher l'accès aux sites éventuellement non sécuritaires.*
Bloquer les sessions avec des émetteurs non approuvés	Mettez fin à la session SSL si l'émetteur des certificats du serveur n'est pas approuvé.  *Bloquez les sessions avec des émetteurs non approuvés, car un émetteur non approuvé peut indiquer la présence d'une attaque par hôte interposé, d'une attaque par rejeu ou d'un autre type d'attaque.*
Bloquer les sessions dont l'état du certificat est inconnu	Mettez fin à la session SSL si un serveur renvoie l'état « inconnu » pour la révocation d'un certificat. L'état de révocation du certificat indique si la confiance d'un certificat a été révoquée ou pas.  *Pour disposer de la sécurité la plus stricte, bloquez les sessions dont l'état du certificat est inconnu. Cependant, comme l'état des certificats peut être inconnu pour une diversité de raisons, la sécurité pourrait être trop stricte. Si le blocage de l'état des certificats inconnu affecte des sites que vous devez utiliser à des fins commerciales, ne bloquez pas les sessions dont l'état du certificat est inconnu.*
Bloquer les sessions dont le délai d'attente de vérification de l'état du certificat a expiré	Mettez fin à la session SSL si l'état du certificat ne peut pas être récupéré lors du délai pendant lequel le pare-feu est configuré pour arrêter d'attendre la réponse d'un service de rapport sur l'état du certificat. Vous pouvez configurer la valeur de **Certificate Status Timeout (Délai d'expiration du statut du certificat)** lors de la création ou de la modification d'un profil de certificat (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**). Le blocage des sessions lors de la temporisation de la vérification de l'état est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si les serveurs de révocation du certificat répondent lentement, le blocage lors de l'expiration du délai peut bloquer des sites qui disposent de certificats valides. Vous pouvez augmenter la valeur de délai d'attente de la vérification de la révocation du certificat et du protocole OCSP si vous vous préoccupez des certificats valides arrivant à expiration.
Limiter les extensions de certificat	Limite les extensions de certificat utilisées pour le certificat du serveur dynamique à l'utilisation de la clé et à l'utilisation améliorée de la clé.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
	Restreignez les extensions de certificat si votre déploiement exige aucune autre extension de certificat.
Ajouter la valeur CN du certificat à l'extension SAN	Permettez au pare-feu d'ajouter une extension Subject Alternative Name (autre nom de l'objet ; SAN) au certificat d'emprunt d'identité qu'il présente au client dans le cadre du déchiffrement de proxy de transfert SSL. Lorsqu'un certificat du serveur ne contient qu'un Common Name (nom commun ; CN), le pare-feu ajoute une extension SAN au certificat d'emprunt d'identité selon le CN du certificat du serveur. Cette option est utile dans les situations où les navigateurs exigent que les certificats des serveurs utilisent un SAN et ne prennent plus en charge la correspondance des certificats en fonction des CN. Elle garantit que les utilisateurs puissent continuer à accéder aux ressources Web qu'ils demandent et que le pare-feu puisse continuer à déchiffrer des sessions même si un certificat du serveur ne contient qu'un CN. *Ajoutez la valeur CN du certificat à l'extension SAN pour garantir l'accès aux ressources Web demandées.*
Vérifications des modes non pris en charge – Sélectionnez des options pour contrôler les applications SSL non prises en charge.	
Bloquer les sessions avec une version non prise en charge	Mettez fin à la session si PAN-OS ne prend pas en charge le message « client hello ». PAN-OS prend en charge SSLv3, TLS1.0, TLS1.1 et TLS1.2. *Bloquez toujours les sessions avec une version non prise en charge pour empêcher l'accès à des sites disposant de protocoles faibles. À l'onglet SSL Protocol Settings (Paramètres du protocole SSL), définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s'applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des suites de cryptage non prises en charge	Mettez fin à la session si la suite de chiffrement définie dans la négociation SSL n'est pas prise en charge par PAN-OS. *Bloquez les sessions qui utilisent des suites de chiffrement que vous ne prenez pas en charge. Vous configurez les suites de chiffrement (algorithmes de chiffrement) à autoriser à l'onglet SSL Protocol Settings (Paramètres du protocole SSL). N'autorisez pas les utilisateurs à se connecter à des sites ayant des suites de chiffrement faibles.*

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
Bloquer les sessions avec authentification du client	Mettez fin aux sessions avec authentification du client pour le trafic du proxy de transfert SSL. *Bloquez les sessions avec authentification du client sauf si une application importante l'exige. Dans ce cas, vous devriez créer un profil de déchiffrement distinct et l'appliquer uniquement au trafic qui exige l'authentification du client.*
Vérification des échecs – Sélectionnez la mesure à prendre si les ressources du système ne sont pas disponibles pour traiter le décryptage.	
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n'arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur l'expérience utilisateur, car les sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.
Bloquer les sessions si HSM n'est pas disponible	Mettez fin aux sessions si aucun module de sécurité matériel n'est disponible pour signer les certificats. La décision de bloquer les sessions si le HSM n'est pas disponible dépend de vos règles de conformité sur la provenance de vos clés privés et de votre manière de gérer le trafic chiffré si le HSM n'est pas disponible.
Extension client	
Enlever l'ALPN	Le pare-feu traite et inspecte le trafic HTTP/2 par défaut. Cependant, vous pouvez désactiver l'inspection HTTP/2 en indiquant que le pare-feu doit **Strip ALPN (Enlever l'ALPN)**. Lorsque cette option est sélectionnée, le pare-feu supprime la valeur contenue dans l'extension TLS Application-Layer Protocol Negotiation (ALPN)). Comme ALPN est utilisé pour sécuriser les connexions HTTP/2 connections, lorsqu'aucune valeur n'est indiquée pour cet extension TLS, le pare-feu déclasse le trafic HTTP/2 en HTTP/1.1 ou le classe en tant que trafic TCP inconnu.

pour les modes et les défaillances non pris en charge, les informations de session sont mises en cache pendant 12'A0;heures'A0;; par conséquent, les sessions à venir entre les mêmes paires d'hôtes et de serveurs ne sont pas décryptées. Activez plutôt les options pour bloquer ces sessions.

ONGLET INSPECTION SSL ENTRANTE

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
Sélectionnez les options pour limiter ou bloquer le trafic SSL décrypté à l'aide de l'inspection SSL entrante.	
Vérifications des modes non pris en charge – Sélectionnez ces options pour contrôler des sessions si des modes non pris en charge sont détectés dans le trafic SSL.	
Bloquer les sessions avec une version non prise en charge	Mettez fin à la session si PAN-OS ne prend pas en charge le message « client hello ». PAN-OS prend en charge SSLv3, TLS1.0, TLS1.1 et TLS1.2.  *Bloquez toujours les sessions avec une version non prise en charge pour empêcher l'accès à des sites disposant de protocoles faibles. À l'onglet SSL Protocol Settings (Paramètres du protocole SSL), définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s'applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des suites de cryptage non prises en charge	Mettez fin à la session si la suite de chiffrement utilisée n'est pas prise en charge par PAN-OS.  *Bloquez les sessions qui utilisent des suites de chiffrement que vous ne prenez pas en charge. Vous configurez les suites de chiffrement (algorithmes de chiffrement) à autoriser à l'onglet SSL Protocol Settings (Paramètres du protocole SSL). N'autorisez pas les utilisateurs à se connecter à des sites ayant des suites de chiffrement faibles.*
Vérification des échecs – Sélectionnez la mesure à prendre si les ressources du système ne sont pas disponibles.	
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n'arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur l'expérience utilisateur, car les sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.
Bloquer les sessions si HSM n'est pas disponible	Mettez fin aux sessions si aucun module de sécurité matériel n'est disponible pour déchiffrer la clé de session.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
	La décision de bloquer les sessions si le HSM n'est pas disponible dépend de vos règles de conformité sur la provenance de vos clés privés et de votre manière de gérer le trafic chiffré si le HSM n'est pas disponible.
ONGLET DES PARAMÈTRES DU PROTOCOLE SSL Sélectionnez les paramètres suivants pour mettre en œuvre les versions de protocole et les suites de déchiffrement du trafic de la session SSL.	
Versions du protocole	Imposez l'utilisation des versions minimales et maximales du protocole pour la session SSL.
Version min	Définissez la version minimale du protocole qui peut être utilisée pour établir la connexion SSL.  *Définissez la version minimale sur TLSv1.2 afin de fournir la sécurité la plus forte. Passez en revue les sites qui ne prennent pas en charge TLSv1.2 pour voir s'ils ont un véritable objectif commercial. Pour les sites auxquels vous devez accéder qui ne prennent pas en charge TLSv1.2, créez un profil de déchiffrement distinct qui spécifie la version la plus forte du protocole qu'ils prennent en charge et appliquez-le à une règle de politique de déchiffrement qui restreint l'utilisation de la version faible uniquement aux sites nécessaires, provenant uniquement des sources nécessaires (zones, adresses, utilisateurs).*
Version max	Définissez la version maximale du protocole qui peut être utilisée pour établir la connexion SSL. Vous pouvez choisir l'option Max où aucune version maximale n'est spécifiée ; dans ce cas, les versions du protocole qui sont équivalentes ou ultérieures à la version minimale sélectionnée sont prises en charge.  *Définissez la version maximale sur Max, pour que, lorsque les protocoles s'améliorent, le pare-feu les prend automatiquement en charge.*
Algorithmes d'échange de clés	Imposez l'utilisation des algorithmes d'échange de clés sélectionnés pour la session SSL. Les trois algorithmes (**RSA**, **DHE** et **ECDHE**) sont activés par défaut. Le **DHE** (Diffie-Hellman) et le **ECDHE** (Diffie-Hellman basé sur les courbes elliptiques) activent le Perfect Forward Secrecy (PFS) pour le déchiffrement du proxy de transfert SSL ou de l'inspection sortante.
Algorithmes de chiffrement	Imposez l'utilisation des algorithmes de chiffrement sélectionnés pour la session SSL.  *Ne prenez pas en charge les algorithmes de chiffrement 3DES ou RC4. (Le pare-feu bloque automatiquement ces deux algorithmes lorsque vous utilisez TLSv1.2 comme version de protocole minimale.) Si vous devez faire une*

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Déchiffrement SSL	Description
	exception et que vous devez prendre en charge une version de protocole plus faible, décochez 3DES et RC4 dans le profil de déchiffrement. S'il y a des sites auxquels vous devez accéder à des fins professionnelles qui utilisent les algorithmes de chiffrement 3DES ou RC4, créez un profil de déchiffrement distinct et appliquez-le à une règle de politique de déchiffrement qui s'applique uniquement à ces sites.
Algorithmes d'authentification	Imposez l'utilisation des algorithmes d'authentification sélectionnés pour la session SSL.  *Bloquez l'ancien algorithme MD5 plus faible (bloqué par défaut). Si aucun site nécessaire n'utilise l'authentification SHA1, bloquez SHA1. S'il y a des sites auxquels vous devez accéder à des fins professionnelles qui utilisent SHA1, créez un profil de déchiffrement distinct et appliquez-le à une règle de politique de déchiffrement qui s'applique uniquement à ces sites.*

Paramètres de contrôle du trafic non déchiffré

Vous pouvez utiliser l'onglet **No Decryption (Aucun déchiffrement)** pour que les paramètres bloquent le trafic correspondant à une politique de déchiffrement configurée avec l'action **No Decrypt (Aucun décryptage)** (**Policies (Politiques)** > **Decryption (Déchiffrement)** > **Action**). Ces options permettent de contrôler les certificats des serveurs de la session, bien que le pare-feu ne décrypte et n'inspecte pas le trafic de la session.

Paramètres de l'onglet Aucun déchiffrement	Description
Bloquer les sessions avec un certificat expiré	Mettez fin à la connexion SSL si le certificat du serveur a expiré. Cela empêche les utilisateurs d'accepter des certificats expirés et de poursuivre une session SSL.  *Bloquez les sessions avec des certificats expirés pour empêcher l'accès aux sites éventuellement non sécuritaires.*
Bloquer les sessions avec des émetteurs non approuvés	Mettez fin à la session SSL si l'émetteur des certificats du serveur n'est pas approuvé.  *Bloquez les sessions avec des émetteurs non approuvés, car un émetteur non approuvé peut indiquer la présence d'une attaque par hôte interposé, d'une attaque par rejeu ou d'un autre type d'attaque.*

© 2020 Palo Alto Networks, Inc.

Paramètres de contrôle du trafic SSH déchiffré

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour contrôler le trafic SSH déchiffré entrant et sortant. Ces paramètres vous permettent de limiter ou de bloquer le trafic SSH tunnellisé en fonction de critères, notamment l'utilisation d'algorithmes non pris en charge, la détection d'erreurs SSH ou la disponibilité des ressources pour traiter le déchiffrement du proxy SSH.

Paramètres de l'onglet Proxy SSH	Description
Vérifications des modes non pris en charge – Utilisez ces options pour contrôler des sessions si des modes non pris en charge sont détectés dans le trafic SSH. La version SSH prise en charge est SSH version 2.	
Bloquer les sessions avec une version non prise en charge	Mettez fin aux sessions si le message « client hello » n'est pas pris en charge par PAN-OS. *Bloquez toujours les sessions avec une version non prise en charge pour empêcher l'accès à des sites disposant de protocoles faibles. À l'onglet SSL Protocol Settings (Paramètres du protocole SSL), définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s'applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des algorithmes non pris en charge	Mettez fin aux sessions si l'algorithme défini par le client ou le serveur n'est pas pris en charge par PAN-OS. *Bloquez toujours les sessions avec des algorithmes non pris en charge pour empêcher l'accès à des sites disposant des algorithmes faibles.*
Vérification des échecs – Sélectionnez les actions à prendre si des erreurs SSH surviennent et si les ressources du système ne sont pas disponibles.	
Bloquer les sessions avec des erreurs SSH	Mettez fin aux sessions si des erreurs SSH surviennent.
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n'arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur

© 2020 Palo Alto Networks, Inc.

Paramètres de l'onglet Proxy SSH	Description
	l'expérience utilisateur, car les sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.

© 2020 Palo Alto Networks, Inc.

Objets > Déchiffrement > Profil de transfert

Vous pouvez définir un profil de déchiffrement de transfert pour permet au pare-feu de faire office d'agent de déchiffrement. Un pare-feu qui agit en tant qu'agent de déchiffrement transfère le trafic qu'il a déjà déchiffré et inspecté à une chaîne de sécurité (une ensemble d'appareils de sécurité tiers en ligne) pour procurer une mise en œuvre supplémentaire. Vous pouvez également configurer le pare-feu pour qu'il distribue les sessions de la chaîne de sécurité afin de veiller à ce que les appareils de la chaîne de sécurité ne soient pas sursouscrits. Lorsque le pare-feu reçoit le trafic de la chaîne de sécurité, il le chiffre de nouveau et le transfère à la destination appropriée.

Avant de créer un profil de déchiffrement de transfert pour permettre au pare-feu de faire office d'agent de déchiffrement, vous devez :

- Activez le décryptage du proxy de transfert SSL.
- Dédiez au moins deux interfaces de couche 3 du pare-feu au transfert du trafic déchiffré à la chaîne de sécurité (sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, modifiez une interface, sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**, puis activez le Déchiffrement des transferts). Répétez cette tâche pour activer une deuxième interface comme interface de Déchiffrement des transferts.

Une fois cette tâche accomplie, créez un profil de Déchiffrement des transferts afin de jumeler les deux interfaces et définissez les paramètres de la chaîne de sécurité à laquelle le pare-feu transfèrera le trafic déchiffré.

Reportez-vous à la section Agent de déchiffrement pour en apprendre davantage sur les déploiements d'agent de déchiffrement et de chaîne de sécurité pris en charge et pour obtenir le flux de travail complet vous permettant de définir un pare-feu en tant qu'agent de déchiffrement.

Paramètres de Déchiffrement des transferts	Description
Name (Nom)	Donnez un nom descriptif au profil.
Description	Vous pouvez décrire les paramètres du profil.
Onglet Général	
Type de chaîne de sécurité	Sélectionnez le type de chaîne de sécurité à laquelle le pare-feu transfère le trafic déchiffré : • **Routed (Layer 3) (Acheminé (de couche 3)** : Les périphériques de ce type de chaîne de sécurité utilisent des interfaces de couche 3 pour se connecter au réseau de la chaîne de sécurité. Chaque interface doit disposer d'une adresse IP et d'un masque de sous-réseau qui lui ont été affectés. Les périphériques d'une chaîne de sécurité sont configurés avec des itinéraires statiques (ou le routage dynamique) pour acheminer le trafic entrant et sortant au prochain périphérique de la chaîne de sécurité et le retourner au pare-feu. • **Transparent Bridge (Pont transparent)** : Dans un réseau de chaîne de sécurité en pont transparent, tous les périphériques de la chaîne de sécurité sont configurés avec deux interfaces connectées au réseau de la chaîne de sécurité. Selon leur configuration, ces deux interfaces de plan de données sont en mode Pont transparent ; aucune adresse IP, masque

© 2020 Palo Alto Networks, Inc.

Paramètres de Déchiffrement des transferts	Description
	de sous-réseau, passerelle par défaut ou table de routage local ne leur sont attribués. Les périphériques d'une chaîne de sécurité en mode Pont transparent reçoivent le trafic sur une interface, puis analysent et appliquent le trafic avant qu'il ne sorte de l'autre interface pour se rendre vers le prochain périphérique de la chaîne de sécurité en ligne.
Sens du flux	Précisez la manière dont le pare-feu dirige les sessions entrantes et sortantes déchiffrées via une chaîne de sécurité : dans le même sens (unidirectionnel) ou dans des sens opposés (bidirectionnel). Le sens du flux que vous choisissez dépend du type de périphériques qui constituent votre chaîne de sécurité. Par exemple, si une chaîne de sécurité se compose de périphériques sans état qui peuvent examiner les deux côtés d'une session, vous choisiriez le flux unidirectionnel.
Interface principale	Sélectionnez l'interface principale et l'interface secondaire que le pare-feu utilisera pour transmettre le trafic à une chaîne de sécurité. Ensemble, les interfaces principale et secondaire forment une paire d'interfaces de déchiffrement de transferts. Seules les interfaces que vous configurez en tant qu'interfaces de déchiffrement de transferts sont affichées.
Interface secondaire	
Onglet Chaînes de sécurité	
Activer	Activez la chaîne de sécurité.
Name (Nom)	Donnez un nom descriptif à la chaîne de sécurité.
Premier périphérique	Sélectionnez l'adresse IPv4 du premier périphérique et du dernier périphérique de la chaîne de sécurité ou définissez un nouvel Objet d'adresse pour facilement faire référence au périphérique.
Dernier périphérique	
Méthode de Distribution de Sessions	Lors du transfert à plusieurs chaînes de sécurité acheminées (de couche 3), choisissez la méthode que le pare-feu utilisera pour distribuer les sessions déchiffrées parmi les chaînes de sécurité : • **IP Modulo (Modulo IP)** : le pare-feu attribue les sessions selon le hachage module des adresses IP source et de destination. • **IP Hash (Hachage IP)** : le pare-feu attribue les sessions selon le hachage IP des adresses IP source et de destination et des numéros de port. • **Round Robin (Permutation circulaire)** : le pare-feu alloue les sessions également entre les chaînes de sécurité. • **Lowest Latency (Plus faible latence)** : le pare-feu alloue un plus grand nombre de sessions à la chaîne de sécurité ayant la plus faible latence. Pour que cette méthode fonctionne comme prévu, vous devez également activer la Surveillance de la latence et la Surveillance HTTP (sélectionnez **Health Monitor (Contrôle de fonctionnement)**).
Onglet Contrôle de fonctionnement	
Sur échec du contrôle de fonctionnement	Choisissez si le pare-feu doit **Bypass Security Chain (Ignorer la chaîne de sécurité)** (autoriser le trafic de la session) ou **Block Session (Bloquer**

© 2020 Palo Alto Networks, Inc.

Paramètres de Déchiffrement des transferts	Description
	la session) si toutes les chaînes de sécurité associées à ce profil de déchiffrement de transferts échouent un contrôle de fonctionnement. Cela veut dire que lorsque la configuration d'un profil de déchiffrement prévoit plusieurs chaînes de sécurité, si une seule chaîne de sécurité échoue un contrôle de fonctionnement, le pare-feu distribue les sessions aux chaînes de sécurité qui sont fonctionnelles selon la méthode indiquée à l'onglet **Security Chains (Chaînes de sécurité)** ; il ne bloque ou n'autorise le trafic selon ce paramètre que si toutes les chaînes échouent.
Condition d'échec du contrôle de fonctionnement	Définissez un échec du contrôle de fonctionnement en tant qu'événement qui se produit lorsqu'une des conditions de contrôle de fonctionnement est remplie (une **OR Condition (Condition OU)**) ou lorsque toutes les conditions sont remplies (une **AND Condition** (Condition ET)).
Surveillance des chemins Surveillance de la latence Surveillance HTTP	Activez la surveillance HTTP, de la latence et des chemins, ou toute combinaison des trois, pour identifier les situations où les chaînes de sécurité ne traitent pas efficacement le trafic déchiffré. Pour chaque type de surveillance que vous activez, définissez les durées et les nombres qui déclencheront un échec du contrôle de fonctionnement. Activer : • La surveillance des chemins pour vérifier la connectivité des périphériques. • La surveillance de la latence pour vérifier la vitesse et l'efficacité de traitement des périphériques. • La surveillance HTTP pour vérifier la disponibilité des périphériques et les temps de réponse.

© 2020 Palo Alto Networks, Inc.

Objets > Gestion des liens SD-WAN

Créez des profils de qualité du chemin d'accès SD-WAN et des profils de distribution du trafic SD-WAN à utiliser avec les règles de politique SD-WAN.

- Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès
- Objets > Gestion des liens SD-WAN > Profil de distribution du trafic

Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès

SD-WAN vous permet de créer un profil de qualité de chemin d'accès pour chaque ensemble d'applications, les filtres d'applications, les groupes d'applications, les services, les objets de services et les objets de groupes de services qui ont des besoins de qualité de réseau uniques et ensuite de référencer le profil dans une règle de politique SD-WAN. Dans le profil, vous définissez le seuil maximum de trois paramètres : la latence, la gigue et la perte de paquets. Lorsqu'un lien SD-WAN dépasse un de ces seuils, le pare-feu sélectionne un meilleur chemin d'accès pour les paquets qui correspond à la règle SD-WAN où vous avez appliquer ce profil.

Un réglage de sensibilité pour chaque paramètre de qualité du chemin vous permet d'indiquer au pare-feu quel paramètre est plus important (préféré) pour les applications auxquelles le profil s'applique. Le pare-feu accorde plus d'importance à un paramètre avec un réglage élevé plutôt qu'un paramètre avec un réglage moyen ou bas. Par exemple, certaines applications sont plus sensibles à la perte de paquets qu'à la gigue ou la latence, donc vous pouvez régler la sensibilité à la perte de paquets à « élevée » pour le profil associé à ces applications et le pare-feu examinera la perte de paquets en premier.

Si vous laissez les réglages de sensibilité de la latence, de la gigue et de la perte de paquets au paramètre par défaut (moyen) ou si vous réglez les trois paramètres au même niveau de sensibilité, l'ordre de préférence du profil est comme suit : la perte de paquets, puis la latence et enfin la gigue.

Par défaut, le pare-feu mesure la latence et la gigue toutes les 200 ms et fait une moyenne des trois dernières mesures pour évaluer la qualité du chemin sur une fenêtre glissante. Vous pouvez modifier ce comportement en sélectionnant une surveillance des chemins agressive ou souple lorsque vous configurez un profil d'interface SD-WAN.

	Réglages du profil de qualité du chemin d'accès
Name (Nom)	Saisissez un **Name (Nom)** pour le profil de qualité du chemin d'accès en utilisant une combinaison de caractères alphanumériques, de traits de soulignement, de traits d'union, d'espaces et de points, pour un maximum de 31 caractères.
Latence (ms)	**Threshold (Seuil)** - Saisissez le nombre de millisecondes autorisées pour qu'un paquet quitte le pare-feu, arrive à l'extrémité opposée du tunnel SD-WAN et qu'un paquet de réponse soit renvoyé au pare-feu avant que le seuil ne soit dépassé (la plage est comprise entre 10 et 2 000 ; par défaut : 100).
	Sensitivity (Sensibilité) - Sélectionnez **high (élevée)**, **medium (moyenne)** (par défaut) ou **low (faible)**.
Gigue (ms)	**Threshold (Seuil)** - Saisissez la variation moyenne, en millisecondes, selon laquelle la latence des paquets SD-WAN peut varier (la plage est comprise entre 10 et 1 000 ; par défaut : 100). Le seuil de gigue par défaut de 100 ms

© 2020 Palo Alto Networks, Inc.

	Réglages du profil de qualité du chemin d'accès
	signifie que les mesures de latence peuvent varier d'une moyenne de 100 ms avant que le seuil de gigue ne soit dépassé.
	Sensitivity (Sensibilité) - Sélectionnez **high (élevée)**, **medium (moyenne)** (par défaut) ou **low (faible)**.
Perte de paquets (%)	**Threshold (Seuil)** - Saisissez le pourcentage de perte de paquets sur le lien avant que le seuil ne soit dépassé (la plage est comprise entre 1 et 100 ; par défaut : 1).
	Sensitivity (Sensibilité) - Sélectionnez **high (élevée)**, **medium (moyenne)** (par défaut) ou **low (faible)**.

Objets > Gestion des liens SD-WAN > Distribution du trafic

Pour ce profil de distribution du trafic, sélectionnez la méthode utilisée par le pare-feu pour distribuer les sessions et basculer vers un meilleur chemin lorsque la qualité du chemin se détériore. Ajoutez les étiquettes de liens que le pare-feu doit considérer lorsqu'il détermine le lien par lequel il transfère le trafic SD-WAN. Vous appliquez un profil de distribution du trafic à chaque règle de politique SD-WAN que vous créez.

	Profil de distribution du trafic
Name (Nom)	Saisissez un **Name (Nom)** pour le profil de distribution du trafic en utilisant une combinaison d'un maximum de 31 caractères composée de caractères alphanumériques, de traits d'union, d'espaces, de traits de soulignement et de points.
Meilleur chemin disponible	Si le coût n'est pas un facteur déterminant et les applications peuvent utiliser n'importe quel chemin d'accès sur la branche sélectionnez **Best Available Path (Meilleur chemin disponible)**. Le pare-feu distribue le trafic et bascule sur un des liens appartenant aux étiquettes de liens dans la liste basée sur les mesures de la qualité d'un chemin d'accès pour ainsi fournir la meilleure expérience de l'application aux utilisateurs.
Priorité descendante	Si vous avez des liens onéreux ou à faible capacité et vous souhaitez qu'ils soient utilisés uniquement en dernier ressort ou comme liens de secours, utilisez la méthode de **Top Down Priority (Priorité descendante)** et placez les étiquettes qui comprennent ces liens en dernier dans la liste des **Link Tags (étiquettes de liens)** dans ce profil. Le pare-feu utilise la première étiquette de liens de la liste en premier pour déterminer sur quels liens charger le trafic de la session et sur lesquels basculer. Si aucun des liens de la première étiquette de liens n'est qualifié, le pare-feu sélectionne un lien dans la deuxième étiquette de liens dans la liste. Si aucun des liens de la deuxième étiquette de liens n'est qualifié, la procédure continue aussi longtemps que nécessaire jusqu'à ce que le pare-feu trouve un lien qualifié. Si tous les liens associés sont surchargés et qu'aucun lien ne respecte les seuils de qualité, le pare-feu utilise la méthode du meilleur chemin disponible pour sélectionner un lien vers lequel transférer le trafic. Si la gigue, la latence ou la perte de paquets pour une application dépasse le seuil configuré, le pare-feu commence en haut de la liste de priorité descendante des étiquettes de liens pour trouver un lien sur lequel basculer.

© 2020 Palo Alto Networks, Inc.

	Profil de distribution du trafic
Distribution pondérée de sessions	Sélectionnez la méthode **Weighted Session Distribution (Distribution de session pondérée)** si vous souhaitez charger le trafic (qui correspond à la règle) manuellement vers votre ISP et vos liens WAN et que vous n'avez pas besoin de basculer lors de conditions de dégradation Vous indiquez manuellement la charge du lien lorsque vous appliquez un pourcentage statique de nouvelles sessions que les interfaces regroupées avec une seule étiquette obtiendront. Par exemple, sélectionnez cette méthode pour les applications qui ne sont pas sensibles à la latence et qui ont besoin d'une grande capacité de bande passante du lien, comme des sauvegardes importantes de branche et des transferts de gros fichiers. Cependant, si le lien subit une panne, le pare-feu ne redirigera pas le trafic correspondant vers un lien différent.
Étiquettes de liens	Ajoutez les **Link Tags (Étiquettes de liens)** que vous voulez que le pare-feu considère lors du processus de sélection du lien que vous avez choisi pour ce profil. L'ordre des étiquettes est importante si vous choisissez la méthode **Top Down Priority (Priorité descendante)** ; vous pouvez cliquer sur **Move Up (Monter)** ou **Move Down (Descendre)** pour changer l'ordre des étiquettes.
Poids	Si vous choisissez la méthode de distribution pondérée de sessions, saisissez un pourcentage pour chaque étiquette de liens que vous ajoutez. La somme des valeurs en pourcentage doit être égale à 100 %.

© 2020 Palo Alto Networks, Inc.

Objets > Calendriers

Par défaut, les règles des politiques de sécurité sont en vigueur en tout temps (toutes les dates et heures). Pour limiter l'application d'une règle de politique de sécurité à des horaires spécifiques, vous pouvez définir des calendriers puis les appliquer aux politiques concernées. Pour chaque calendrier, vous pouvez définir une date et une plage horaire fixes ou récurrentes. Pour appliquer des calendriers à des politiques de sécurité, reportez-vous à la section Politiques > Sécurité.

Lorsqu'une règle de politique de sécurité est invoquée par un calendrier défini, seules les nouvelles sessions sont affectées par la règle de politique de sécurité appliquée. Les sessions existantes ne sont pas affectées par la politique planifiée.

Paramètres des calendriers	Description
Name (Nom)	Saisissez un nom pour le calendrier (31 caractères maximum). Ce nom apparaît dans la liste de calendriers lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le calendrier soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le calendrier sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le calendrier sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette planification dans les groupes de périphériques qui héritent de la planification. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de la planification.
Récurrence	Sélectionnez le type de calendrier (**Quotidien**, **Hebdomadaire** ou **Non récurrent**).
Quotidien	Cliquez sur **Ajouter** et renseignez une **Heure de début** et une **Heure de fin** au format 24 heures (HH:MM).
Hebdomadaire	Cliquez sur **Ajouter**, sélectionnez un **Jour de la semaine**, et précisez une **Heure de début** et une **Heure de fin** au format 24 heures (HH:MM).
Non récurrent	Cliquez sur **Ajouter** et indiquez une **Date de début**, une **Heure de début**, une **Date de fin** et une **Heure de fin**.

Réseau

Les rubriques suivantes décrivent les paramètres réseau du pare-feu.

- Réseau > Câbles virtuels
- Réseau > Interfaces
- Réseau > Routeurs virtuels
- Réseau > Zones
- Réseau > VLAN
- Réseau > Tunnels'A0;IPSec
- Réseau > Tunnels GRE
- Réseau > DHCP
- Réseau > Proxy'A0;DNS
- Réseau > QoS
- Réseau > LLDP
- Réseau > Profils réseau

© 2020 Palo Alto Networks, Inc.

Réseau > Interfaces

Les interfaces de pare-feu (ports) permettent à un pare-feu de se connecter à d'autres périphériques réseau, ainsi qu'à d'autres interfaces du pare-feu. Les rubriques suivantes expliquent les types d'interfaces et comment les configurer :

Que voulez-vous faire ?	Reportez-vous à la section
Quelles sont les interfaces de pare-feu ?	Présentation des interfaces de pare-feu
Je ne connais pas les interfaces de pare-feu ; quels sont les composants d'une interface de pare-feu ?	Composants communs des interfaces de pare-feu Composants communs des interfaces de pare-feu PA-7000 Series
Je connais déjà les interfaces de pare-feu ; comment puis-je trouver des informations sur la configuration d'un type d'interface spécifique ?	**Interfaces physiques (Ethernet)** Interface Tap Interface HD Interface du câble virtuel Sous-interface de câble virtuel Interface de niveau 2 de la série PA-7000 Sous-interface de niveau 2 de la série PA-7000 Interface de niveau 3 de la série PA-7000 Interface de niveau 3 Sous-interface de couche 3 Interface de la carte de journal Sous-interface de la carte de journal Interface miroir de décryptage Groupe d'interfaces Ethernet agrégées (AE) Interfaces Ethernet agrégées (AE) **Interfaces logiques** Réseau > Interfaces > VLAN Réseau > Interfaces > En boucle Réseau > Interfaces > De tunnel Réseau > Interfaces > SD-WAN
Vous souhaitez en savoir plus ?	Mise en réseau

© 2020 Palo Alto Networks, Inc.

Présentation des interfaces de pare-feu

Les configurations d'interface des ports de données du pare-feu permettent au trafic d'entrer et de sortir du pare-feu. Un pare-feu Palo Alto Networks® peut fonctionner simultanément dans plusieurs déploiements, car vous pouvez configurer les interfaces pour prendre en charge différents déploiements. Par exemple, vous pouvez configurer les interfaces Ethernet d'un pare-feu pour le câble virtuel, le niveau 2, le niveau 3 et le mode Tap. Les interfaces prises en charge par le pare-feu sont les suivantes :

- **Interfaces physiques** – Le pare-feu prend en charge deux types de supports (cuivre et fibre optique) qui peuvent envoyer et recevoir du trafic à différents taux de transmission. Vous pouvez configurer des interfaces Ethernet selon les types suivants : Tap, HA (haute disponibilité, carte de journal (interface et sous-interface), miroir de déchiffrement, câble virtuel (interface et sous-interface), couche 2 (interface et sous-interface), couche 3 (interface et sous-interface) et Ethernet agrégée. Les types d'interfaces disponibles et les taux de transmission varient selon le modèle matériel.
- **Interfaces logiques** - Ce sont notamment les interfaces de réseau local virtuel (VLAN), les interfaces en boucle, les interfaces de tunnel et les interface SD-WAN. Vous devez configurer l'interface physique avant de définir une interface VLAN, une interface SD-WAN ou une interface de tunnel.

Composants communs des interfaces de pare-feu

Sélectionnez **Network (Réseau)** > **Interfaces** pour afficher et configurer les composants qui sont communs à la plupart des types d'interfaces.

Pour obtenir la description des composants uniques ou différents lors de la configuration d'interfaces sur un pare-feu de la série PA-7000 ou lors de l'utilisation de Panorama™ pour configurer des interfaces sur un pare-feu, reportez-vous à la section Composants communs des interfaces de pare-feu PA-7000 Series*.*

Étapes de Configuration de l'interface de pare-feu	Description
Interface (nom de l'interface)	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier. Vous pouvez toutefois ajouter un suffixe numérique aux sous-interfaces, interfaces agrégées, interfaces VLAN, interfaces en boucle, interfaces de tunnel et interfaces SD-WAN.
Type d'interface	Pour les interfaces Ethernet (**Network (Réseau)** > **Interfaces** > **Ethernet**), vous pouvez sélectionner le type d'interface : • **Tap** • **HA** • **Decrypt Mirror (Miroir de déchiffrement)** (Pris en charge sur tous les pare-feu, à l'exception des pare-feu pare-feu VM-Series Édition NSX, Citrix SDX, AWS et Azure.) • **Virtual Wire** • **Couche 2** • **Couche 3** • **Log Card (Carte de journal)** (pare-feu de la série PA-7000 uniquement) ; • **Aggregate Ethernet**
Profil de gestion	Sélectionnez un **Management Profile (Profil de gestion)** (**Network (Réseau)** > **Interfaces (Interfaces)** > **<if-config (if-config)** > **Advanced (Avancé)** > **Other**

© 2020 Palo Alto Networks, Inc.

Étapes de Configuration de l'interface de pare-feu	Description
	Info (Autres informations) qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface.
état des liaisons	Pour les interfaces Ethernet, l'état des liaisons indique si l'interface est actuellement accessible et peut recevoir du trafic sur le réseau : • **Vert** - configurée et active • **Rouge** - Configurée, mais inactive ou désactivée • **Gris** - non configurée Pointez l'état des liaisons pour afficher une infobulle qui indique les paramètres duplex et de vitesse de liaison de l'interface.
Adresse IP	(Facultatif) Configurez l'adresse IPv4 ou IPv6 de l'interface Ethernet, VLAN ou de tunnel. Pour une adresse IPv4, vous pouvez également sélectionner le mode d'adressage (**Type**) de l'interface : **Static (Statique)**, **DHCP Client (client DHCP)** ou **PPPoE**.
Virtual Router (routeur virtuel - VR)	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Étiquette (sous-interface uniquement)	Saisissez l'étiquette VLAN (1-4 094) de la sous-interface.
Réseau local virtuel	Vous devez sélectionner **Network (Réseau)** > **Interfaces (Interfaces)** > **VLAN (VLAN)**, puis modifier un **VLAN (VLAN)** existant ou **Add (Ajouter)** un nouveau (reportez-vous à la section Réseau > VLANs). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de l'interface. Pour activer le basculement entre les interfaces de couche 2 ou pour activer le routage via une interface VLAN, vous devez configurer un objet VLAN.
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une **Security Zone (Zone de sécurité)** (**Réseau (Network)** > **Interfaces (Interfaces)** > **<if-config (if config)** > **Config (Configuration)**)pour l'interface ou sélectionnez **Zone (Zone)** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Caractéristiques	Pour les interfaces Ethernet, cette colonne indique si les fonctions suivantes sont activées :  Client DHCP  Proxy DNS

© 2020 Palo Alto Networks, Inc.

Étapes de Configuration de l'interface de pare-feu	Description
	Passerelle GlobalProtect™ activée LACP (Link Aggregation Control Protocol/protocole d'agrégation de liaisons) LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) Surveillance NDP Profil NetFlow Profil de qualité de service (QoS) SD-WAN
Commentaire	Une description de la fonction de l'interface.

Composants communs des interfaces de pare-feu PA-7000 Series

Le tableau suivant décrit les composants de la page **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** qui sont uniques ou différents lors de la configuration d'interfaces sur un pare-feu de la série PA-7000 ou lors de l'utilisation de Panorama pour configurer des interfaces sur n'importe quel pare-feu. Cliquez sur **Add Interface (Ajouter une interface)** pour créer une nouvelle interface ou sélectionnez une interface existante (Ethernet1/1, par exemple) pour la modifier.

Sur les pare-feu de la série PA-7000, vous devez configurer une Interface de la carte de journal *sur un seul port de données.*

Étapes de Configuration de l'interface de pare-feu de la série PA-7000	Description
Logement	Sélectionnez le numéro de logement (1-12) de l'interface. Seuls les pare-feu PA-7000 Series disposent de plusieurs logements. Si vous utilisez Panorama pour configurer une interface pour n'importe quel autre modèle de pare-feu, sélectionnez le **Slot 1 (Logement 1)**.
Interface (nom de l'interface)	Choisissez le nom d'une interface associée au **Slot (logement)** sélectionné.

Interface Tap

- Réseau > Interfaces > Ethernet

Vous pouvez utiliser une interface Tap pour surveiller le trafic sur un port.

© 2020 Palo Alto Networks, Inc.

Pour configurer une interface Tap, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d'une interface Tap	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Tap**.
profil NetFlow ;		Si vous souhaitez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil NetFlow)** pour en définir un nouveau (reportez-vous à la section Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Virtual System (système virtuel - vsys)	**Ethernet Interface (Interface Ethernet)** > **Config (Configuration)**	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)**	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).

Interface HD

- Réseau > Interfaces > Ethernet

Chaque interface haute disponibilité (HA) a une fonction spécifique : une interface sert à synchroniser la configuration et les pulsations, et l'autre sert à synchroniser l'état. Si la HA active/active est activée, le pare-feu peut utiliser une interface HA tierce pour transférer les paquets.



Certains pare-feu Palo Alto Networks contiennent des ports physiques dédiés à l'utilisation dans des déploiements HA (l'un pour la liaison de contrôle et l'autre pour la liaison de données). Pour les pare-feu n'incluant pas de ports dédiés, vous devez définir des ports de

© 2020 Palo Alto Networks, Inc.

données qui vont être utilisés pour la HA. Pour plus d'informations sur HA, reportez-vous à « Périphérique > Systèmes virtuels ».

Pour configurer une interface HA, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d'une interface HA	Description
Nom de l'interface	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire	Saisissez une description de l'interface (facultatif).
Type d'interface	Sélectionnez **HA**.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).

Interface du câble virtuel

- Réseau > Interfaces > Ethernet

Un câble virtuel relie logiquement deux interfaces Ethernet, ce qui permet d'autoriser la circulation de l'ensemble du trafic entre les interfaces ou uniquement le trafic doté des étiquettes VLAN sélectionnées (aucun autre service de basculement ou de routage n'est disponible). Vous pouvez créer des sous-interfaces de câble virtuel pour classer le trafic en fonction d'une adresse IP, d'une plage d'adresses IP ou d'un sous-réseau. Un câble virtuel n'exige aucune modification des périphériques réseau adjacents. Un câble virtuel peut relier deux interfaces Ethernet de matériel analogue (deux interfaces en cuivre ou deux interfaces en fibre optique), ou relier une interface en cuivre à une interface en fibre optique.

Pour établir un câble virtuel, vous devez décider quelles sont les deux interfaces à relier(**Network (Réseau)** > **Interfaces** > **Ethernet**) et configurer leurs paramètres comme le décrit la table suivante.

Si vous utilisez une interface existante pour le câble virtuel, retirez d'abord l'interface de n'importe quelle zone de sécurité associée.

Paramètre d'une Interface de câble virtuel	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.

© 2020 Palo Alto Networks, Inc.

Paramètre d'une Interface de câble virtuel	Configuré dans	Description
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Virtual Wire (Câble virtuel)**.
Virtual Wire	**Ethernet Interface (Interface Ethernet)** > **Config (Configuration)**	Sélectionnez un câble virtuel ou cliquez sur **Virtual Wire (Câble virtuel)** pour en définir un nouveau (Réseau > Câbles virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de câble virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)**	Sélectionnez une vitesse d'interface en Mbits/s ou sélectionnez **auto (auto)** pour que le pare-feu détermine automatiquement la vitesse. Les deux interfaces du câble virtuel doivent avoir la même vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**). Les deux interfaces du câble virtuel doivent avoir le même mode de transmission.
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Activer LLDP	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.
Profil		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l'interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau > Profil LLDP). Sélectionnez **None (Aucun)** pour configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez pour configurer un pare-feu HA passif pour qu'il prénégocie LLDP avec son homologue avant que le pare-feu devienne actif. Si LLDP n'est pas activé, sélectionnez pour configurer un pare-feu HA passif pour qu'il ne fasse que passer les paquets LLDP à travers du pare-feu.

© 2020 Palo Alto Networks, Inc.

Sous-interface de câble virtuel

- Réseau > Interfaces > Ethernet

Les sous-interfaces de câble virtuel vous permettent de séparer le trafic par étiquette VLAN ou une combinaison d'étiquette VLAN et de classificateur d'adresses IP, d'affecter le trafic étiqueté à une zone et à un système virtuel différents, puis d'appliquer les politiques de sécurité relatives au trafic correspondant aux critères définis.

Pour ajouter Interface du câble virtuel, sélectionnez la ligne pour cette interface, cliquez sur **Add Subinterface (Ajouter une sous-interface)** et spécifiez les informations suivantes.

Paramètres d'une sous-interface de câble virtuel	Description
Nom de l'interface	**Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface de câble virtuel sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de la sous-interface (facultatif).
Étiquette	Saisissez le l'étiquette) VLAN (0-4 094) de la sous-interface.
profil NetFlow ;	Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil NetFlow)** pour en définir un nouveau (reportez-vous à la section Périphérique > Profils de serveur > NetFlow). Sélectionnez**None (Aucun)** pour supprimer l'affectation de serveur NetFlow de la sous-interface.
Classificateur IP	Cliquez sur **Add (Ajouter)** et saisissez une adresse IP, une plage d'adresses IP ou un sous-réseau pour classer le trafic sur cette sous-interface de câble virtuel.
Virtual Wire	Sélectionnez un câble virtuel ou cliquez sur **Virtual Wire (Câble virtuel)** pour en définir un nouveau (reportez-vous à la section Réseau > Câbles virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de câble virtuel de la sous-interface.
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.

Interface de niveau 2 de la série PA-7000

- Réseau > Interfaces > Ethernet

Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** pour configurer une interface de niveau 2, puis cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de niveau 2	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Layer2 (IPv6)**.
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Réseau local virtuel	**Ethernet Interface (Interface Ethernet)** > **Config (Configuration)**	Pour activer le basculement entre des interfaces de niveau 2 ou pour activer le routage via une interface VLAN, sélectionnez un VLAN existant ou cliquez sur **VLAN** pour définir un nouveau VLAN (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une **Security Zone (Zone de sécurité)** pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)**	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Activer LLDP	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.
Profil		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l'interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau >

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de niveau 2	Configuré dans	Description
		Profil LLDP). Sélectionnez **None (Aucun)** pour configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez cette option pour permettre à un pare-feu HA passif de prénégocier LLDP avec son homologue avant que le pare-feu ne devienne actif.

Sous-interface de niveau 2 de la série PA-7000

- Réseau > Interfaces > Ethernet

Pour chaque port Ethernet configuré en tant qu'interface physique de couche 2, vous pouvez définir une interface de couche 2 logique supplémentaire (sous-interface) pour chaque étiquette VLAN assignée au trafic reçu par le port. Pour activer le basculement entre les sous-interfaces de couche 2, assignez-leur le même objet VLAN.

Pour configurer une Interface de niveau 2 de la série PA-7000, sélectionnez la ligne de cette interface physique, puis cliquez sur **Ajouter une sous-interface** et indiquez les informations suivantes.

Paramètres d'une sous-interface de couche 2	Description
Nom de l'interface	Le Nom de l'interface en lecture seule affiche le nom de l'interface physique sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de la sous-interface (facultatif).
Étiquette	Saisissez l'étiquette VLAN (1-4 094) de la sous-interface.
profil NetFlow ;	Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Profil NetFlow** pour définir un nouveau profil (voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de la sous-interface.
Réseau local virtuel	Pour activer le basculement entre des interfaces de niveau 2 ou pour activer le routage via une interface VLAN, sélectionnez un VLAN ou cliquez sur **VLAN** pour définir un nouveau VLAN (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de la sous-interface.
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de couche 2	Description
Zone de sécurité	Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.

Interface de niveau 3 de la série PA-7000

- Réseau > Interfaces > Ethernet

Pour configurer une interface de niveau 3, sélectionnez une interface (Ethernet1/1, par exemple) et indiquez les informations suivantes.

Paramètres d'une interface de couche 3	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Layer3 (Couche 3)**.
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Virtual Router (routeur virtuel - VR)	**Ethernet Interface (Interface Ethernet)** > **Config (Configuration)**	Sélectionnez un routeur virtuel ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (reportez-vous à la section Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Ethernet Interface (Interface Ethernet)** >	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1 000**) ou sélectionnez **Auto**.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
Mode duplex de la liaison	**Advanced (Avancé)**	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Profil de gestion	**VLAN Interface (Interface VLAN)** > **Advanced (Avancé)** > **Other Info (Autres informations)**	Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (intervalle compris entre 576 et 9 192 ; valeur par défaut : 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l'interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Sous-interface non étiquetée		Indique que toutes les sous-interfaces appartenant à cette interface de couche 3 ne sont pas étiquetées. PAN-OS® sélectionne une sous-interface non étiquetée comme interface d'entrée en fonction de la destination du paquet. Si la destination est l'adresse IP d'une sous-interface non étiquetée, il effectue un mappage vers la sous-interface. Cela signifie aussi que l'adresse source des paquets allant dans la direction inverse doit être traduite en adresse IP de la sous-interface non étiquetée. Une conséquence indirecte de ce mécanisme de classification est

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
		que tous les paquets multicast et de diffusion sont assignés à l'interface de base et non à l'une des sous-interfaces. Comme OSPF (Open Shortest Path First/premier chemin ouvert le plus court) utilise le multicast, le pare-feu ne le prend pas en charge sur les sous-interfaces non étiquetées.
Adresse IP Adresse MAC	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **ARP Entries (Entrées ARP)**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol / protocole de résolution d'adresse) statiques, cliquez sur **Add (Ajouter)**, puis saisissez une adresse IP et son adresse matérielle associée (MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques minimisent le traitement ARP et protègent des attaques par hôte interposé pour les adresses définies.
Adresse IPv6 Adresse MAC	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **ND Entries (Entrées ND)**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) cliquez sur **Add (Ajouter)** et saisissez l'adresse IP et l'adresse MAC du voisin.
Activer le proxy NDP	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **NDP Proxy (Proxy NDP)**	Sélectionnez cette option pour activer le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l'interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface pour indiquer qu'il agira en tant que proxy en répondant aux paquets destinés à ces adresses. Il est recommandé de sélectionner l'option **Enable NDP Proxy (Activer le proxy NDP)** si vous utilisez NPTv6 (Network Prefix Translation/traduction de préfixe réseau IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées d'adresse en saisissant une chaîne de recherche et en cliquant sur Appliquer le filtre ( ).
Adresse		Cliquez sur **Add (Ajouter)** pour saisir une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
		voisins IPv6 du pare-feu et de sélectionner **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** en regard d'une adresse afin d'empêcher le proxy NDP pour cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Activer LLDP	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.
LLDP Profile (profil LLDP)		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l'interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau > Profil LLDP). Sélectionnez **None (Aucun)** pour configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez cette option pour permettre au pare-feu défini comme pare-feu HA passif de prénégocier LLDP avec son homologue avant que le pare-feu devienne actif.
Type	**Ethernet Interface (Interface Ethernet)** > **IPv4**	Sélectionnez la méthode d'affectation d'un type d'adresse IPv4 à l'interface : • **Static (Statique)** - Vous devez indiquer manuellement l'adresse IP. • **PPPoE** - Le pare-feu utilisera l'interface pour le protocole PPPoE (Point-to-Point Protocol over Ethernet/protocole point à point sur Ethernet). • **DHCP Client (Client DHCP)** - Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique.  *Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge PPPoE ni le client DHCP.* Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
Settings (Paramètres)	**Ethernet Interface (Interface Ethernet)** > **Advanced**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
	(Avancé) > **DDNS**	DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur		Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si vous sélectionnez une version antérieure d'un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s'il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l'interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
Onglet IPv6 - IPv6		Ajoutez les adresses IPv6 configurées sur l'interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l'inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l'état de la mise à jour du nom d'hôte et une date de retour à des fins de résolution de problèmes.
Type d'adresse IPv4 = **Static (Statique)**		
Adresse IP	**Ethernet Interface (Interface Ethernet)** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre pare-feu détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Type d'adresse IPV4 = **PPPoE**		
Activer	**Ethernet Interface (Interface Ethernet)** > **IPv4** > **PPPoE** > **General (Général)**	Sélectionnez cette option pour activer l'interface de la terminaison PPPoE.
Username (Nom d'utilisateur)		Saisissez le nom d'utilisateur pour la connexion de point à point.
Mot de passe/ Confirmer le mot de passe		Saisissez, puis confirmez le mot de passe du nom d'utilisateur.
Afficher les informations d'exécution du client PPPoE		(Facultatif) Une fenêtre de dialogue s'ouvre pour afficher les paramètres que le pare-feu a négociés avec le fournisseur de services Internet pour établir une connexion. Les informations affichées dépendent du fournisseur de services Internet.
Authentification	**Ethernet Interface**	Sélectionnez le protocole d'authentification des communications PPPoE : **CHAP** (Challenge-Handshake

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
	(Interface Ethernet) > **IPv4** > **PPPoE** > **Advanced (Avancé)**	Authentication Protocol/protocole d'authentification par défi-réponse), **PAP** (Password Authentication Protocol/ protocole d'authentification de mot de passe) ou la valeur **Auto (Automatique)** par défaut (le pare-feu détermine le protocole). Sélectionnez **None (Aucun)** pour supprimer l'affectation de protocole de l'interface.
Adresse statique		Suivez l'une des étapes ci-dessous pour indiquer l'adresse IP assignée par le fournisseur de services Internet (aucune valeur par défaut) : • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. • Sélectionnez **None (Aucune)** pour supprimer l'affectation d'adresse de l'interface.
Créer automatiquement un itinéraire par défaut en direction de l'homologue		Sélectionnez cette option pour créer automatiquement un itinéraire par défaut pointant vers l'homologue PPPoE lorsqu'il est connecté.
Mesure d'itinéraire par défaut		(Facultatif) Pour l'itinéraire entre le pare-feu et le fournisseur de services Internet, saisissez une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Accéder au concentrateur		(Facultatif) Saisissez le nom du concentrateur d'accès se trouvant à l'extrémité du fournisseur de services Internet auquel le pare-feu se connecte (aucune valeur par défaut).
Service (Service)		(Facultatif) Saisissez la chaîne de service (aucune valeur par défaut).
Passif		Sélectionnez cette option pour utiliser le mode passif. En mode passif, un point d'extrémité PPPoE attend que le concentrateur d'accès envoie la première trame.
Type d'adresse IPv4 = **DHCP**		
Activer	**Ethernet Interface (Interface**	Sélectionnez pour activer le client DHCP sur l'interface.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur	**Ethernet)** > **IPv4**	Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.
Envoyer le nom d'hôte		Choisissez si le pare-feu (en tant que client DHCP) doit envoyer le nom d'hôte de l'interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte le nom d'hôte du pare-feu est alors le choix indiqué dans le champ Nom d'hôte par défaut. Vous pouvez envoyer ce nom ou saisir un nom d'hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou minuscules, des chiffres, des points, des tirets et des traits de soulignement).
Mesure d'itinéraire par défaut		Pour l'itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535, aucune valeur par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Activer IPv6 sur l'interface	**Ethernet Interface (Interface Ethernet)** > **IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
		• **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche. • **Send Router Advertisement (Envoyer la publication de routeur)** - Sélectionnez pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d'informations sur la RA, reportez-vous à la section Activation de la publication de routeur. Les champs restants s'appliquent uniquement si vous activez la RA. • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)** (valeur par défaut de 2 592 000). • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que **Valid Lifetime (Durée de vie valide** expire (valeur par défaut de 604 800). • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
Activer la détection des doublons d'adresses	**Ethernet Interface (Interface Ethernet)** > **IPv6** > **Address Resolution (Résolution de l'adresse)**	Sélectionnez pour activer la Détection des doublons d'adresses (DAD) puis configurez les autres champs de cette section.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 10 à 36 000 ; valeur par défaut de 30).
Intervalle NS (neighbor solicitation interval/intervalle de sollicitation de voisins)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Une fois activé, vous pouvez sélectionner Surveillance NDP ( dans la colonne Fonctions) et visualiser des informations sur un voisin que le pare-feu a découvert, comme l'adresse IPv6, l'adresse MAC correspondante et l'ID utilisateur (selon le cas).
Activer la publication des routeurs	**Ethernet Interface (Interface Ethernet) > IPv6 > Router Advertisement (Publication de routeurs)**	Pour réaliser une SLAAC (stateless address auto-configuration / autoconfiguration d'adresse sans état) sur les interfaces IPv6, sélectionnez cette option et renseignez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s'agit d'un paramètre global de l'interface. Si vous souhaitez définir des options de publication de routeur pour les adresses IP individuelles, cliquez sur **Add (Ajouter)** dans la table d'adresses IP et configurez l'adresse. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez sélectionner l'option **Enable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)		Indiquez l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Intervalle max. (s)		Indiquez l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez 0 pour indiquer l'absence de limite de saut.
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Vérification de cohérence	**Ethernet Interface (Interface Ethernet)** > **IPv6** > **Router Advertisement (cont)** **(Publication**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
	de routeurs (suite))	
Inclure les informations DNS dans la publication de routeur	**Etherne Interface (Interface Ethernet)** > **IPv6** > **DNS Support (Prise en charge DNS)**	Sélectionnez pour permettre au pare-feu d'envoyer des informations DNS dans les messages de publication de routeur (RA) NDP à partir de cette interface Ethernet IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option.
Serveur		Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie, dans l'ordre indiqué de haut en bas, dans une publication de routeur NDP au destinataire, qui utilise ensuite ces adresses dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser les serveurs RDNS afin de résoudre les noms de domaine (la plage est la valeur d'Intervalle max. (sec) jusqu'à deux fois l'intervalle maximal, la valeur par défaut est de 1 200).
Suffixe		Il vous faut **Ajouter** et configurer un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour « qualité » sans suffixe, le routeur ajoute une période et le premier suffixe DNS du DNS cherche ce nom dans la liste puis transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le FQDN. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit réussie (ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Configuré dans	Description
		Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l'ordre ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximal de secondes après que le client DNS IPv6 reçoit la publication du routeur lui indiquant qu'il peut utiliser un nom de domaine (suffixe) sur la Liste de recherche DNS (la plage est comprise entre la valeur de l'Intervalle max. [sec] et deux fois l'intervalle maximal ; la valeur par défaut est 1 200).

Interface de niveau 3

- **Network (Réseau)** > **Interfaces** > **Ethernet**

Configurez une interface Ethernet de couche 3 à laquelle vous pouvez acheminer le trafic.

Paramètres d'une interface de couche 3	Description
Nom de l'interface	Le **Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface physique sélectionnée.
Commentaire	Saisissez une description conviviale pour l'interface.
Type d'interface	Sélectionnez **Layer3 (Couche 3)**.
Profil NetFlow	Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez un profil NetfFlow existant ou cliquez sur **Netflow Profile (Profil Netflow)** pour créer un nouveau profil NetFlow (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Onglet Configuration	
Virtual Router (routeur virtuel - VR)	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) existant pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une zone de sécurité existante pour l'interface ou définissez une nouvelle **Zone**. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Onglet IPv4	
Activer SD-WAN	Sélectionnez **Enable SD-WAN (Activer SD-WAN)** pour activer la fonctionnalité SD-WAN de l'interface Ethernet.
Type d'IPv4 = Statique	
Adresse IP	Ajoutez et suivez l'une des étapes ci-dessous pour indiquer une adresse IP statique et un masque réseau de l'interface. • Utilisez la notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d'**Address (Adresse)** de type **IP netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre pare-feu détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n'en avez plus besoin.
Passerelle du saut suivant	Si vous avez utilisé la fonction **Enable SD-WAN (Activer SD-WAN)**, saisissez l'adresse IPv4 de la passerelle du saut suivant.
Type d'IPv4 = PPPoE, onglet Général	
Activer	Sélectionnez **Enable (Activer)** pour activer l'interface pour la terminaison PPPoE (Point-to-Point Protocol over Ethernet/protocole point à point sur Ethernet). L'interface en tant que point de terminaison Point-to-Point Protocol over Ethernet (protocole point-à-point sur Ethernet ; PPPoE) prend en charge la connectivité dans un environnement Digital Subscriber Line (ligne d'accès numérique ; DSL) où se trouve un modem DSL, mais aucun autre périphérique PPPoE pour terminer la connexion.
Username (Nom d'utilisateur)	Saisissez le nom d'utilisateur fourni par votre ISP pour la connexion de point à point.
Mot de passe et confirmation de mot de passe	Saisissez le mot de passe et confirmez le mot de passe.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Afficher les informations d'exécution du client PPPoE	Consultez les informations de l'interface PPPoE.
Type d'IPv4 = PPPoE, onglet Avancé	
Authentification	Sélectionnez la méthode d'authentification : • **None (Aucune)** (par défaut) - Il n'y a aucune authentification pour l'interface PPPoE. • **CHAP** - Le pare-feu utilise le Challenge Handshake Authentication Protocol (protocole d'authentification de négociation par défi, CHAP) - RFC-1994 - sur l'interface PPPoE. • **PAP** - Le pare-feu utilise le Password Authentication Protocol (protocole d'authentification par mot de passe, PAP) sur l'interface PPPoE. Le PAP est moins sécuritaire que le CHAP ; le PAP envoie les noms d'utilisateur et les mots de passe en texte brut. • **auto** - Le pare-feu négocie la méthode d'authentification (CHAP ou PAP) avec le serveur PPPoE.
Adresse statique	Demandez une adresse IPv4 souhaitée au serveur PPPoE et celui-ci peut attribuer cette adresse ou une autre adresse.
Créer automatiquement un itinéraire par défaut en direction de l'homologue	Sélectionnez cette option pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur PPPoE.
Mesure d'itinéraire par défaut	Saisissez la mesure d'itinéraire par défaut (niveau de priorité) pour la connexion PPPoE (par défaut : 10). Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, le pare-feu utilise un itinéraire avec une valeur de mesure de 10 avant un itinéraire avec une valeur de mesure de 100.
Accéder au concentrateur	Si votre ISP vous a fourni le nom d'un concentrateur d'accès, saisissez ce nom. Le pare-feu se connectera à ce concentrateur d'accès du côté de l'IPS. Ceci est une valeur de chaîne de 0 à 255 caractères.
Service (Service)	Le pare-feu (client PPPoE) peut fournir la demande de service désirée au serveur PPPoE. Ceci est une valeur de chaîne de 0 à 255 caractères.
Passif	Le pare-feu (client PPPoE) attend que le serveur PPPoE initie la connexion. Si l'option n'est pas activée, le pare-feu initie la connexion.
Onglet IPv4, type = client DHCP	
Activer	Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
	Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur	Indique au pare-feu de créer une route statique vers une passerelle par défaut. La passerelle par défaut est utile lorsque les clients tentent d'accéder à de nombreuses destinations qui n'ont pas besoin de conserver des itinéraires dans une table de routage sur le pare-feu.
Envoyer le nom d'hôte	Sélectionnez cette option pour affecter un nom d'hôte à l'interface du client DHCP et envoyer ce nom d'hôte (option 12) à un serveur DHCP. qui peut enregistrer le nom d'hôte auprès du serveur DNS. Le serveur DNS peut ensuite gérer automatiquement les résolutions de nom d'hôte/adresse IP dynamique. Les hôtes externes peuvent identifier l'interface par son nom d'hôte. La valeur par défaut indique **system-hostname (nom de l'hôte système)**, qui correspond au nom d'hôte du pare-feu que vous avez configuré sous **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**. Vous pouvez également saisir un nom d'hôte pour l'interface, d'un maximum de 64 caractères, y compris des lettres majuscules et minuscules, des chiffres, des points, des tirets et des traits de soulignement.
Mesure d'itinéraire par défaut	Saisissez une mesure d'itinéraire par défaut (niveau de priorité) pour l'itinéraire entre le pare-feu et le serveur DHCP (plage comprise entre 1 et 65 535 ; aucune valeur de mesure par défaut). Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, le pare-feu utilise un itinéraire avec une valeur de mesure de 10 avant un itinéraire avec une valeur de mesure de 100.
Afficher les informations d'exécution du client DHCP	Affichez tous les paramètres du client reçus par son serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle et les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Onglet IPv6	
Activer IPv6 sur l'interface	Sélectionnez pour activer l'adressage IPv6 sur l'interface.
ID de l'interface	Saisissez l'identifiant unique étendu sur 64 bits (**EUI-64**) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous utilisez l'option **Utiliser l'ID de l'interface comme partie hôte** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de cette adresse.
Adresse	Ajoutez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou en créer un nouveau.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Activer l'adresse sur l'interface	Activez l'adresse IPv6 sur l'interface.
Utiliser l'ID de l'interface comme partie hôte.	Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6.
Anycast	Sélectionnez cette option pour inclure le routage via le nœud le plus proche.
Envoyer la publication des routeurs	Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d'informations sur la RA, reportez-vous à la section Activer la publication de routeur dans ce tableau. Les champs suivants s'appliquent uniquement si vous **Enable Router Advertisement (Activez la publication du routeur)** : • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que la **Valid Lifetime (Durée de vie valide)** expire. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
Onglet IPv6, onglet Résolution d'adresse	
Activer la fonction Duplicate Address Detection (détection des doublons d'adresses ; DAD).	Sélectionnez cette option pour activer la détection des doublons d'adresses (DAD), puis configurez les tentatives DAD, la durée d'accessibilité (s) et l'intervalle NS.
Tentatives DAD	Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité (s)	Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Intervalle (s)	Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP	Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Lorsque cette option est activée, vous pouvez sélectionner **NDP** (dans la colonne Caractéristiques) pour visualiser des informations sur un voisin détecté par le pare-feu, comme l'adresse IPv6, l'adresse MAC correspondante et l'User-ID (dans le meilleur des cas).
Onglet IPv6, onglet Publication des routeurs	
Activer la publication des routeurs	Pour assurer la Découverte des voisins sur les interfaces IPv6, sélectionnez et configurez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s'agit d'un paramètre global de l'interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Add (Ajouter)** et configurer une adresse IPv6 dans la table d'adresses IP. Si vous définissez des options de publication de routeur pour une adresse IPv6, vous devez **Enable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)	Indiquez l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
Intervalle max. (s)	Indiquez l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
Limite de saut	Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
MTU de liaison	Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients (la plage est comprise entre 1 280 et 1 500) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée d'accessibilité (ms)	Indiquez la durée d'accessibilité, en millisecondes, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité (la plage est comprise entre 0 et 3 600 000), ou

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
	indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de retransmission (ms)	Indiquez le minuteur de retransmission, en millisecondes, qui détermine la durée d'attente du client avant la retransmission des messages de sollicitation de voisins. (la plage est comprise entre 0 et 4 294 967 295) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de vie du routeur (s)	Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur	Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée	Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration	Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consignera toutes les incohérences dans un journal système de type **Ipv6nd**.
L'onglet **DNS Support Tab (Onglet Prise en charge DNS)** est disponible si vous sélectionnez l'option **Enable Router Advertisement (Activer la publication du routeur)** dans l'onglet **Router Advertisement (Publication du routeur)**.	
Inclure les informations DNS dans la publication de routeur	Sélectionnez le pare-feu pour transmettre des informations DNS vers les publications du routeur NDP à partir de cette interface Ethernet IPv6. Les autres champs de Prise en charge DNS (serveur, durée de vie, suffixe et durée de vie) ne sont visibles qu'après sélection de cette option.
Serveur	Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de demandes de recherche DNS aux serveurs DNS racine et aux serveurs DNS autoritaires pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l'ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Durée de vie	Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser un serveur RDNS afin de résoudre les noms de domaine (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Suffixe	Il vous faut **ajouter** un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur utilise les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour l'option de liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l'ordre ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie	Saisissez le nombre maximal de secondes après que le client DNS IPv6 reçoit la publication du routeur lui indiquant qu'il peut utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Onglet SD-WAN	
État d'une interface SD-WAN	Si vous avez sélectionné **Enable SD-WAN (Activer SD-WAN)** dans l'onglet **IPv4**, le pare-feu indique `l'état de l'interface SD-WAN. Activé`. Si vous n'avez pas sélectionné **Enable SD-WAN (Activer SD-WAN)**, le pare-feu indique que l'état de SD-WAN est **Disabled (Désactivé)**.
Profil d'interface SD-WAN	Sélectionnez un profil d'interface SD-WAN existant pour l'appliquer à cette interface Ethernet ou ajoutez un nouveau profil d'interface SD-WAN.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
	Vous devez Enable SD-WAN (Activer SD-WAN) pour l'interface avant que vous ne puissiez appliquer un profil d'interface SD-WAN.
Onglet Avancé	
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1 000**) ou sélectionnez **Auto**.
Mode duplex de la liaison	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Onglet Avancé. Onglet Autres informations	
Profil de gestion	Sélectionnez un profil de gestion qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de `fragmentation ICMP obligatoire` indiquant que le paquet est trop volumineux.
Ajuster TCP MSS	Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l'interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Sous-interface non étiquetée	Sélectionnez cette option si les sous-interfaces correspondantes à cette interface ne sont pas étiquetées.
Onglet Avancé, onglet Entrées ARP	

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Adresse IP Adresse MAC	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol/ protocole de résolution d'adresse) statiques, **Add (Ajoutez)** une adresse IP et son adresse matérielle associée (Media Access Control/commande d'accès au support ou MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques réduisent le traitement ARP.
Onglet Avancé, onglet Entrées ND	
Adresse IPv6 Adresse MAC	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol/protocole de découverte des voisins), **Add (Ajoutez)** l'adresse IPv6 et l'adresse MAC du voisin.
Onglet Avancé, onglet Proxy NDP	
Activer le proxy NDP	Activez le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l'interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface de manière à recevoir les paquets destinés aux adresses de la liste. Il est recommandé d'activer le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** en saisissant un filtre et ensuite en cliquant sur Appliquer le filtre (la flèche grise).
Adresse	Vous devez **Add (Ajouter)** une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a aucune importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour ignorer ces voisins pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser	Sélectionnez **Negate (Ignorer)** une adresse afin d'empêcher le proxy NDP d'opérer sur cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Onglet Avancé, onglet LLDP	
Activer LLDP	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/ protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques avoisinants et leurs fonctionnalités en envoyant des unités de données LLDP aux périphériques avoisinants et en recevant des unités de données LLDP de ceux-ci.
LLDP Profile (profil LLDP)	Sélectionnez un profil LLDP existant ou créez un nouveau LLDP Profile (profil LLDP). Le profil vous permet de configurer le mode LLDP, d'activer les

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
	notifications SNMP et Syslog, ainsi que de configurer les éléments TLV (Type-Longueur-Valeur) que vous souhaitez transmettre aux homologues LLDP.
Onglet Avancé, onglet DDNS	
Settings (Paramètres)	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer	Activez DDNS sur l'interface - vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)	Saisissez l'intervalle. en jours, entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat	Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte	Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur	Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** *Si vous sélectionnez une version antérieure d'un service DDNS et le pare-feu indique que la version sera supprimée avant une date donnée, sélectionnez plutôt la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s'il ne reçoit pas de réponse du service DDNS.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de couche 3	Description
Onglet IPv4	Ajoutez les adresses IPv4 configurées sur l'interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d'adresses IPv4 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6	Ajoutez les adresses IPv6 configurées sur l'interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d'adresses IPv6 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info	Affiche l'inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l'état de la mise à jour du nom d'hôte et une date de retour à des fins de résolution de problèmes.

Sous-interface de couche 3

- **Réseau** > **Interfaces** > **Ethernet**

Vous pouvez définir des interfaces logiques de couche 3 (sous-interfaces) supplémentaires pour chaque port Ethernet configuré comme interface physique de couche 3.

Pour configurer une Interface de niveau 3 de la série PA-7000, sélectionnez une interface physique, puis cliquez sur **Add Subinterface (Ajouter une sous-interface)** et indiquez les informations suivantes.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
Nom de l'interface	**Sous-interface de couche 3**	Le champ **Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface physique sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier la sous-interface.
Commentaire		Saisissez une description de la sous-interface (facultatif).
Étiquette		Saisissez l'étiquette VLAN (1 à 4 094) de la sous-interface.
profil NetFlow ;		Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Profil NetFlow** pour définir un nouveau profil (voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de la sous-interface.
Virtual Router (routeur virtuel - VR)	**Layer3 Subinterface (Sous-interface de couche**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
Virtual System (système virtuel - vsys)	**3) > Config (Configuration)**	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.
Type	**Layer3 Subinterface (Sous-interface de couche 3) > IPv4**	Sélectionnez la méthode d'affectation d'un type d'adresse IPv4 à la sous-interface : • **Static (Statique)** - Vous devez indiquer manuellement l'adresse IP. • **DHCP Client (Client DHCP)** - Permet à la sous-interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol) et de recevoir une adresse IP assignée de façon dynamique. *Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP.* Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
Adresse IP	**Layer3 Subinterface (Sous-interface de couche 3) > IPv4, Type = Static (IPv4, Type = Statique)**	Cliquez sur **Add (Ajouter)** et suivez l'une des étapes ci-dessous pour indiquer une adresse IP statique et un masque réseau de l'interface. • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d'**Address (Adresse)** de type **IP netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n'en avez plus besoin.
Activer	**Layer3 Subinterface (Sous-interface de couche 3) >**	Sélectionnez pour activer le client DHCP sur l'interface.
Créer automatiquement un itinéraire par défaut en direction		Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
de la passerelle par défaut fournie par le serveur	**IPv4, Type = DHCP**	
Envoyer le nom d'hôte		Choisissez si le pare-feu (en tant que client DHCP) doit envoyer le nom d'hôte de l'interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte, par défaut, le nom d'hôte du pare-feu est alors le choix indiqué dans le champ Nom d'hôte par défaut. Vous pouvez envoyer ce nom ou saisir un nom d'hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou minuscules, des chiffres, des points, des tirets et des traits de soulignement).
Mesure d'itinéraire par défaut		(Facultatif) Pour l'itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535 ; il n'y a aucune valeur par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez **Show DHCP Client Runtime Info (Afficher les informations d'exécution du client DHCP)** pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Activer IPv6 sur l'interface	**Layer3 Subinterface (Sous-interface de couche 3)** > **IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
		• **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche. • **Send Router Advertisement (Envoyer la publication de routeur)** - Sélectionnez pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d'informations sur la RA, reportez-vous à la section Activer la publication de routeur dans ce tableau. Les champs restants s'appliquent uniquement si vous activez la RA. • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que **Valid Lifetime (Durée de vie valide)** expire. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d'adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
Activer la détection des doublons d'adresses	**Layer3 Subinterface (Sous-interface de niveau 3 > IPv6 > Address Resolution (Résolution d'adresse)**	Sélectionnez pour activer la Détection des doublons d'adresses (DAD) puis configurez les autres champs de cette section.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
Intervalle NS (neighbor solicitation interval/intervalle de sollicitation de voisins)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Lorsque cela est activé, vous pouvez sélectionner NDP (dans la colonne Caractéristiques) pour visualiser des informations sur un voisin détecté par le pare-feu, comme l'adresse IPv6, l'adresse MAC correspondante et l'User-ID (dans le meilleur des cas).
Activer la publication des routeurs	**Layer3 Subinterface (Sous-interface de niveau 3) > IPv6 > Router Advertisement (Publication de routeur)**	Pour assurer la Découverte des voisins sur les interfaces IPv6, sélectionnez et configurez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s'agit d'un paramètre global de l'interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Ajouter** et configurer une Adresse dans la table d'adresses IP. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)		Indiquez l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Intervalle max. (s)		Indiquez l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez 0 pour indiquer l'absence de limite de saut.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence	**Layer3 Subinterface (Sous-interface de couche 3)** > **IPv6** > **Router Advertisement (cont)** **(Publication**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
	de routeur (suite))	
Inclure les informations DNS dans la publication de routeur	**Layer3 Subinterface (Sous-interface de couche 3)** > **IPv6** > **DNS Support (Prise en charge DNS)**	Sélectionnez le pare-feu pour transmettre des informations DNS vers les publications du routeur NDP à partir de cette sous-interface Ethernet IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option.
Serveur		Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de demandes de recherche DNS aux serveurs DNS racine et aux serveurs DNS autoritaires pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit Serveurs RDNS que le pare-feu envoie (dans l'ordre de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser un serveur RDNS afin de résoudre les noms de domaine (la plage est la valeur d'Intervalle max. (sec) jusqu'à deux fois l'intervalle maximal, la valeur par défaut est de 1 200).
Suffixe	**Layer3 Subinterface (Sous-interface de couche 3)** > **IPv6** > **DNS Support (Prise en charge DNS)** (suite)	Il vous faut **ajouter** un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur utilise les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
		Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l'ordre ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie	**Layer3 Subinterface (Sous-interface de couche 3)** > **IPv6** > **DNS Support (Prise en charge DNS)** (suite)	Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).
Profil de gestion	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **Other Info (Autres informations)**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **Other Info (Autres informations)**	Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l'interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
		L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Adresse IP Adresse MAC	**Layer3 Subinterface (Sous-interface de couche 3) > Advanced (Avancé) > ARP Entries (Entrées ARP)**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol/protocole de résolution d'adresse) statiques, **Add (Ajoutez)** une adresse IP et son adresse matérielle associée (Media Access Control/commande d'accès au support ou MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques réduisent le traitement ARP.
Adresse IPv6 Adresse MAC	**Layer3 Subinterface (Sous-interface de couche 3) > Advanced (Avancé) > ND Entries (Entrées ND)**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol/protocole de découverte des voisins), **Add (Ajoutez)** l'adresse IP et l'adresse MAC du voisin.
Activer le proxy NDP	**Layer3 Subinterface (Sous-interface de couche 3) > Advanced (Avancé) > NDP Proxy (Proxy NDP)**	Activez le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l'interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface de manière à recevoir les paquets destinés aux adresses de la liste. Il est recommandé d'activer le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** en saisissant un filtre et en cliquant sur Appliquer le filtre (la flèche grise).
Adresse		Vous devez **Add (Ajouter)** une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
Inverser		Sélectionnez **Negate (Ignorer)** une adresse afin d'empêcher le proxy NDP d'opérer sur cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Settings (Paramètres)	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **DDNS**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **DDNS**	Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **DDNS**	Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si vous sélectionnez une version antérieure d'un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
		se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s'il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l'interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d'adresses IPv4 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6 - IPv6		Ajoutez les adresses IPv6 configurées sur l'interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d'adresses IPv6 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info	**Layer3 Subinterface (Sous-interface de couche 3)** > **Advanced (Avancé)** > **DDNS**	Affiche l'inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l'état de la mise à jour du nom d'hôte et une date de retour à des fins de résolution de problèmes.

Interface de la carte de journal

- Réseau > Interfaces > Ethernet

Si vous configurez le transfert des journaux sur un pare-feu de la série PA-7000 doté d'une carte de traitement des journaux (LPC), vous devez configurer un port de données comme type **Log Card (Carte de journal)**. Vous devez effectuer cette action car les fonctions de trafic et de journalisation de ce modèle de pare-feu dépassent les fonctions de l'interface de gestion (MGT). Un port de données de carte de journal effectue le transfert des journaux pour Syslog, la messagerie, SNMP (Simple Network Management Protocol), le transfert des journaux Panorama et le transfert de fichiers WildFire™.

Vous ne pouvez configurer qu'un seul port sur le pare-feu comme type Log Card (Carte de journal). Si vous activez le transfert des journaux mais ne configurez aucune interface avec le type de Log Card (Carte de journal), une erreur de validation se produit.

Pour configurer une interface de carte de journal, sélectionnez une interface non configurée (Ethernet1/16, par exemple) et configurez les paramètres décrits dans le tableau suivant.

Paramètres d'une interface de carte de journal	Configuré dans	Description
Logement	**Interface Ethernet**	Sélectionnez le numéro de logement (1-12) de l'interface.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de carte de journal	Configuré dans	Description
Nom de l'interface		Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Log Card (Carte de journal)**.
IPv4	**Ethernet Interface (Interface Ethernet)** > **Log Card Forwarding (Transfert de la carte de journal)**	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6		Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.
Vitesse de liaison	**Ethernet Interface (Interface Ethernet)** > **Advanced (Avancé)**	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **Auto** (par défaut) pour que le pare-feu détermine automatiquement la vitesse en fonction de la connexion. **Auto** est la seule option possible pour les interfaces dont la vitesse ne peut être configurée. *La vitesse minimale recommandée pour la connexion est 1 000 (Mbits/s).*
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié en fonction de la connexion (**auto**). La valeur par défaut est **auto**.
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé en fonction de la connexion (**auto**). La valeur par défaut est **auto**.

Sous-interface de la carte de journal

- Réseau > Interfaces > Ethernet

Pour ajouter Interface de la carte de journal, sélectionnez la ligne pour cette interface, cliquez sur **Add Subinterface (Ajouter une sous-interface)** et spécifiez les informations suivantes.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une sous-interface de carte de journal	Configuré dans	Description
Nom de l'interface	**Sous-interface LPC**	**Interface Name (Nom de l'interface)** (en lecture seule) affiche le nom de l'interface de carte de journal sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire		Saisissez une description de l'interface (facultatif).
Étiquette		Saisissez le **Tag (Étiquette)** VLAN (0-4 094) de la sous-interface.  *Donnez à l'étiquette le même numéro que la sous-interface pour simplifier son utilisation.*
Virtual System (système virtuel - vsys)	**LPC Subinterface (Sous-interface LPC) > Config (Configuration)**	Sélectionnez le système virtuel auquel la sous-interface LPC (Log Processing Card/carte de traitement de journal) est affectée. Sinon, vous pouvez cliquer sur **Virtual Systems (Systèmes virtuels)** pour ajouter un nouveau système virtuel. Une fois qu'une sous-interface LPC est affectée à un système virtuel, cette interface est utilisée comme interface source pour tous les services qui transfèrent les journaux (Syslog, messagerie, SNMP) depuis la carte de journal.
IPv4	**Ethernet Interface (Interface Ethernet) > Log Card Forwarding (Transfert de la carte de journal)**	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6		Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.

Interface miroir de décryptage

- Réseau > Interfaces > Ethernet

Pour pouvoir utiliser la fonction Mise en miroir du port de déchiffrement, vous devez sélectionner le type d'interface **Decrypt Mirror (Miroir de déchiffrement)**. Cette fonction permet de créer une copie du trafic décrypté provenant d'un pare-feu et de l'envoyer à un outil de collecte du trafic, tel que NetWitness ou Solera, capable de recevoir des captures de paquets bruts, en vue de leur archivage et de leur analyse. Cette fonction est nécessaire pour les entreprises qui ont besoin de captures de données complètes à des fins médico-légales ou historiques, ou de la fonctionnalité de prévention des fuites de données (DLP). Pour activer cette fonction, vous devez acquérir et installer la licence gratuite.

© 2020 Palo Alto Networks, Inc.

La Mise en miroir du port de déchiffrement n'est pas offerte sur les pare-feu VM-Series pour plateformes de cloud public (AWS, Azure, Google Cloud Platform), VMware NSX et Citrix SDX.

Pour configurer une interface miroir de déchiffrement, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d'une interface miroir de déchiffrementge	Description
Nom de l'interface	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire	Saisissez une description de l'interface (facultatif).
Type d'interface	Sélectionnez **Decrypt Mirror (Miroir de déchiffrement)**.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).

Groupe d'interfaces Ethernet agrégées (AE)

- Réseau > Interfaces > Ethernet

Un groupe d'interfaces Ethernet agrégé se base sur la norme IEEE 802.1AX d'agrégation de liens pour combiner de multiples interfaces Ethernet en une seule interface virtuelle qui connecte un pare-feu à un autre périphérique ou à un autre pare-feu. Un groupe d'interfaces Ethernet agrégées augmente la bande passante qui existe entre des homologues en équilibrant la charge du trafic qui passe par les interfaces combinées. Ce dernier assure également la redondance ; en cas de défaillance d'une interface, les autres interfaces continuent de prendre en charge le trafic.

Avant de configurer un groupe d'interfaces Ethernet agrégées, vous devez d'abord configurer les interfaces qui le composent. Parmi les interfaces affectées à un groupe agrégé donné, le matériel peut différer (par exemple, vous pourriez allier la fibre optique et le cuivre), mais la bande passante (10 Gbit/s, 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s) et le type d'interface (HA3, câble virtuel, couche 2 ou couche 3) doivent être identiques. Vous pouvez ajouter un maximum de huit groupes d'interfaces Ethernet agrégées par pare-feu ; chaque groupe peut être composé d'un maximum de huit interfaces.

Tous les pare-feu Palo Alto Networks, à l'exception des modèles VM-Series, prennent en charge les groupes d'interfaces Ethernet agrégées.

Vous pouvez agréger les interfaces HA3 (transfert de paquets) dans une configuration haute disponibilité (HD) active / active, mais uniquement sur les modèles de pare-feu suivants :

- *PA-220*
- *PA-800 Series*
- *PA-3200 Series*

© 2020 Palo Alto Networks, Inc.

- *PA-5200 Series*

Pour configurer un groupe d'interfaces AE, vous devez **Ajouter un groupe agrégé**, configurer les paramètres décrits dans le tableau suivant, puis affecter les interfaces au groupe (reportez-vous à la section Interface Ethernet agrégée [AE]).

Paramètres d'un groupe d'interfaces agrégées	Configuré dans	Description
Nom de l'interface	**Agréger via l'interface Ethernet**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **ae**. Dans le champ adjacent, saisissez un suffixe numérique (compris entre 1 et 8) pour identifier le groupe d'interfaces Ethernet agrégées.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez le type d'interface, qui contrôle les exigences et les options de configuration restantes'A0;: • **HD** – Sélectionnez uniquement si l'interface est une liaison HA3 entre deux pare-feu et un déploiement actif/actif. Sélectionnez facultativement un **Profil Netflow** et configurez l'onglet **LACP** (reportez-vous à la section Activation de LACP). • **Câble virtuel** – Sélectionnez facultativement un **Profil Netflow** et configurer les onglets **Configuration** et **Avancé** comme décrit dans les Paramètres d'un câble virtuel. • **Niveau 2** – Sélectionnez facultativement un **Profil Netflow**, configurez les onglets **Configuration** et **Avancé** comme décrit dans les Paramètres d'une interface de niveau 2. Configurez facultativement l'onglet **LACP** (reportez-vous à la section Activation de LACP). • **Niveau 3** – Sélectionnez facultativement un **Profil Netflow**, configurez les onglets **Configuration, IPv4, IPv6** et **Avancé** comme décrit dans les Paramètres d'une interface de niveau 3. Configurez facultativement l'onglet **LACP** (reportez-vous à la section Activation de LACP).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow du groupe d'interfaces Ethernet agrégées.
Activer LACP	**Agréger via l'interface Ethernet > LACP**	Sélectionnez si vous souhaitez activer LACP (Link Aggregation Control Protocol, protocole d'agrégation de liens) pour le groupe d'interfaces Ethernet agrégées. LACP est désactivé par défaut. Si vous activez LACP, la détection des échecs de l'interface se fait automatiquement aux niveaux de la liaison de données et physique, peu importe si le pare-feu et son homologue LACP sont connectés directement. (Sans LACP, la détection des échecs de l'interface est

© 2020 Palo Alto Networks, Inc.

Paramètres d'un groupe d'interfaces agrégées	Configuré dans	Description
		automatique uniquement au niveau physique entre des homologues connectés directement.) LACP assure également un basculement automatique aux interfaces qui sont en veille si vous configurez des disques de secours (reportez-vous à la section Nombre maximum de ports).
Mode		Sélectionnez le mode LACP du pare-feu. Si vous disposez de deux homologues LACP, il est recommandé que l'un soit actif et l'autre passif. LACP ne peut pas fonctionner si les deux homologues sont passifs. • **Active (Actif)** - Le pare-feu interroge de façon active l'état LACP (disponible ou non réactif) des périphériques homologues. • **Passive (Passif)** par défaut) - Le pare-feu répond de façon passive aux requêtes d'état LACP des périphériques homologues.
Taux de transmission		Sélectionnez le taux auquel le pare-feu échange des requêtes et des réponses avec les périphériques homologues'A0;: • **Fast (Élevé)** - Toutes les secondes. • **Slow (Faible)** - Toutes les 30 secondes (il s'agit du paramètre par défaut).
Basculement rapide		Sélectionnez cette option si, en cas de défaillance d'une interface, vous souhaitez que le pare-feu bascule vers une interface opérationnelle en une seconde. Sinon, le basculement se produit à la vitesse définie par la norme'A0;IEEE'A0;802.1AX (au moins trois secondes).
Priorité du système	**Aggregate Ethernet Interface (Interface Ethernet agrégée) > LACP (cont) (LACP (suite))**	Ce nombre détermine si le pare-feu ou son homologue a un contrôle prioritaire sur l'autre en ce qui concerne les priorités de port (reportez-vous à la description du champ **Max Ports (Nombre maximum de ports)** ci-dessous). *Veuillez noter que plus le nombre est petit, plus la priorité est grande (plage comprise entre 1 et 65 535 ; valeur par défaut : 32 768).*
Nombre maximum de ports		Le nombre d'interfaces (1 à 8) qui peuvent être actives à un moment donné dans un groupe LACP agrégé. Cette valeur ne peut pas dépasser le nombre d'interfaces affectées au groupe. Si le nombre d'interfaces affectées dépasse le nombre d'interfaces actives, le pare-feu utilise les priorités de port LACP des interfaces pour déterminer celles qui sont en mode veille. Vous définissez les priorités de port LACP lors de la configuration de chaque interface du groupe (reportez-vous à la section Interface Ethernet agrégée [EA]).

© 2020 Palo Alto Networks, Inc.

Paramètres d'un groupe d'interfaces agrégées	Configuré dans	Description
Activation à l'état HA passif		Si les pare-feu sont déployés dans une configuration haute disponibilité (HD) active/passive, sélectionnez pour permettre au pare-feu passif de prénégocier LACP avec son homologue actif avant qu'un basculement ait lieu. Cette négociation préalable accélère le basculement, puisque le pare-feu actif n'a plus à négocier LACP avant de devenir actif.
Même adresse MAC système pour la haute disponibilité active/passive		Ceci ne s'applique qu'aux pare-feu déployés dans une configuration haute disponibilité (HD) active/passive ; les pare-feu qui sont déployés dans une configuration HD active/active nécessitent des adresses MAC uniques. Les pare-feu homologues HA ont la même valeur de priorité système. Cependant, dans un déploiement HA active/passive, l'ID système de chacun peut être identique ou différent, selon que vous affectiez la même adresse MAC ou non. *Lorsque les homologues LACP (également en mode HA) sont virtualisés (apparaissent sur le réseau comme périphérique unique), l'utilisation de la même adresse MAC système pour les pare-feu réduit la latence lors du basculement. Lorsque les homologues LACP ne sont pas virtualisés, l'utilisation de l'adresse MAC unique de chaque pare-feu réduit la latence lors du basculement.* LACP utilise l'adresse MAC afin de dériver un ID système pour chaque homologue LACP. Si la paire de pare-feu et la paire d'homologues ont les mêmes valeurs de priorité système, LACP utilise les valeurs d'ID système afin de déterminer celle qui a un contrôle prioritaire sur l'autre en ce qui concerne les priorités de port. Si les deux pare-feu ont la même adresse MAC, ils ont également le même ID système, qui est supérieur ou inférieur à l'ID système des homologues LACP. Si les pare-feu HA ont chacun une adresse MAC unique, l'un peut avoir un ID système supérieur à celui des homologues LACP, tandis que l'autre a un ID système inférieur. Dans le dernier cas, lorsqu'un basculement se produit sur les pare-feu, les priorités de port basculent entre les homologues LACP et le pare-feu qui devient actif.
Adresse MAC		Si vous avez activé l'option **Use Same System MAC Address (Utiliser la même adresse MAC système)**, sélectionnez une adresse MAC générée par le système, ou saisissez votre propre adresse, pour les deux pare-feu de la paire haute disponibilité (HA) active/passive. Vous devez vérifier que l'adresse est globalement unique.

Interfaces Ethernet agrégées (AE)

- Réseau > Interfaces > Ethernet

© 2020 Palo Alto Networks, Inc.

Pour configurer une Interface Ethernet agrégée (AE), configurez d'abord un Groupe d'interfaces Ethernet agrégées (AE), puis cliquez sur le nom de l'interface que vous souhaitez affecter à ce groupe. Parmi les interfaces que vous affectez à un groupe donné, le matériel peut différer (par exemple, vous pourriez allier la fibre optique et le cuivre), mais la bande passante et le type d'interface (comme Couche 3) doivent être identiques. De plus, l'interface doit être du même type que celle définie pour le groupe d'interfaces Ethernet agrégées ; vous modifierez toutefois le type en **Aggregate Ethernet (Ethernet agrégée)** lorsque vous configurerez chaque interface. Précisez les informations suivantes pour chaque interface que vous affectez au groupe.



Si vous avez activé LACP (Link Aggregation Control Protocol) pour le groupe d'interfaces AE, sélectionnez la même Vitesse de liaison et le même Modèle duplex de la liaison pour chaque interface de ce groupe. Lorsque les valeurs ne correspondent pas, l'opération de validation affiche un avertissement et PAN-OS utilise la vitesse la plus élevée et le duplex intégral.

Paramètres d'une interface agrégée	Configuré dans	Description
Nom de l'interface	**Agréger via l'interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		(Facultatif) Saisissez une description de l'interface.
Type d'interface		Sélectionnez **Aggregate Ethernet (Ethernet agrégée)**.
Groupe agrégé		Affectez l'interface à un groupe agrégé.
Vitesse de liaison		Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Priorité du port LACP		Le pare-feu utilise ce champ uniquement si vous avez activé LACP (Link Aggregation Control Protocol/protocole d'agrégation de liens) pour le groupe agrégé. Si le nombre d'interfaces que vous affectez au groupe dépasse le nombre d'interfaces actives (le champ Nombre maximum de ports), le pare-feu utilise les priorités de port LACP des interfaces pour déterminer celles qui sont en mode veille. Plus le nombre est petit, plus la priorité est grande (intervalle compris entre 1 et 65 535 ; valeur par défaut : 32 768).
Virtual Router (routeur virtuel - VR)	**Agréger via l'interface Ethernet** > **Configuration**	Sélectionnez le routeur virtuel auquel vous affectez l'interface Ethernet agrégée.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface agrégée	Configuré dans	Description
Zone de sécurité		Sélectionnez la zone de sécurité à laquelle vous affectez l'interface Ethernet agrégée.
Activer IPv6 sur l'interface	**Agréger via l'interface Ethernet > IPv6**	Sélectionnez pour activer IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous utilisez l'option **Utiliser l'ID de l'interface comme partie hôte** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de cette adresse.
Adresse		Il vous faut **Ajouter** une adresse IPv6 et configurer les paramètres suivants : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Adresse** pour en créer un. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche. • **Send RA (Envoyer la publication de routeur)** – Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. Lorsque vous sélectionnez cette option, vous devez également **Enable Router Advertisement (Activer la publicité du routeur)** sur l'interface de manière globale. Pour plus d'informations sur la RA, reportez-vous à la section Activation de la publication de routeur. Les autres champs ne sont visibles qu'après activation de la RA : • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface agrégée	Configuré dans	Description
		valide jusqu'à ce qu'elle dépasse la **Valid Lifetime (Durée de vie valide)**. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** – Sélectionnez cette option si les systèmes dont les adresses IP sont comprises dans le préfixe publié sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
Activer la détection des doublons d'adresses	**Aggregate Ethernet Interface (Interface Ethernet agrégée)** > **IPv6** > **Address Resolution (Résolution d'adresse)**	Sélectionnez cette option pour activer la détection des doublons d'adresses (DAD), ce qui vous permet ensuite d'indiquer le nombre de **Tentatives DAD**.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).
Intervalle NS (neighbor solicitation interval/ intervalle de sollicitation de voisins)		Indiquez la durée, en secondes, avant indication d'un échec d'une tentative DAD (plage de 1 à 10 ; par défaut 1).
Activer la surveillance NDP		Sélectionnez cette option pour activer la surveillance du Protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner le NDP ( dans la colonne Fonctions) et afficher des informations telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC et User-ID correspondants (selon la situation la plus favorable).
Activer la publication des routeurs	**Interface Ethernet agrégée** > **IPv6** > **Publication de routeur**	Sélectionnez cette option pour assurer la Découverte de voisins sur les interfaces IPv6 et configurer les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface agrégée	Configuré dans	Description
		Il s'agit d'un paramètre global de l'interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Ajouter** et configurer une Adresse dans la table d'adresses IP. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)		Indiquez l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Intervalle max. (s)		Indiquez l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez **0** pour indiquer l'absence de limite de saut.
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité, en millisecondes, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client, en millisecondes, avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface agrégée	Configuré dans	Description
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez cette option pour indiquer au client que d'autres informations d'adresse (comme les paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence	**Aggregate Ethernet Interface (Interface Ethernet agrégée) > IPv6 > Router Advertisement (cont) (Publication de routeur (suite))**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Inclure les informations DNS dans la publication de routeur	**Interface Ethernet agrégée > IPv6 > Prise en charge DNS**	Sélectionnez cette option pour que le pare-feu envoie des informations DNS dans les messages de publication de routeur (RA) NDP à partir de cette interface Ethernet agrégée IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option.
Serveur		Il faut **Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet agrégée IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie, dans l'ordre indiqué de haut en bas, dans une publication de routeur NDP au destinataire, qui utilise ensuite ces adresses dans le même ordre. Sélectionnez un serveur et utilisez les options **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser les Serveurs RDNS pour résoudre les noms de domaine (l'intervalle est la valeur de

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface agrégée	Configuré dans	Description
		l'Intervalle max. [s] jusqu'à deux fois l'Intervalle maximal ; la valeur par défaut est 1 200).
Suffixe		Il vous faut **Ajouter** et configurer un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). La longueur de suffixe maximale est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des suffixes ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie	**Aggregate Ethernet Interface (Interface Ethernet agrégée)** > **IIPv6** > **DNS Support (cont) (Prise en charge DNS (suite))**	Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).

© 2020 Palo Alto Networks, Inc.

Réseau > Interfaces > VLAN

Une interface VLAN peut fournir un routage dans un réseau de couche 3 (IPv4 ou IPv6). Vous pouvez ajouter un ou plusieurs ports Ethernet de niveau 2 (reportez-vous à la section Interface de niveau 2 de la série PA-7000) à une interface VLAN.

Paramètres d'une interface VLAN	Configuré dans	Description
Nom de l'interface	**Interface VLAN**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **vlan**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Réseau local virtuel	**VLAN Interface (Interface VLAN) > Config (Configuration)**	Sélectionnez une VLAN ou cliquez sur **VLAN** pour en définir une nouvelle (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de l'interface.
Virtual Router (routeur virtuel - VR)		Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Profil de gestion	**VLAN Interface (Interface VLAN) > Advanced (Avancé) > Other Info (Autres informations)**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l'interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Adresse IP Adresse MAC Interface	**VLAN Interface (Interface VLAN) > Advanced (Avancé) > ARP Entries (Entrées ARP)**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol) statiques, cliquez sur **Add (Ajouter)**, saisissez une adresse IP et son adresse matérielle associée (MAC) et sélectionnez une interface de niveau 3 pouvant accéder à l'adresse matérielle. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques minimisent le traitement ARP et protègent des attaques par hôte interposé pour les adresses définies.
Adresse IPv6 Adresse MAC	**VLAN Interface (Interface VLAN) > Advanced (Avancé) > ND Entries (Entrées ND)**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) cliquez sur **Ajouter** et saisissez l'adresse IPv6 et l'adresse Mac du voisin.
Activer le proxy NDP	**VLAN Interface (Interface VLAN) > Advanced (Avancé) > NDP Proxy (Proxy NDP)**	Sélectionnez cette option pour activer le proxy NDP (Neighbor Discovery Protocol) sur l'interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface et demande tous les paquets destinés à ces adresses. (**Recommandé**) Activez le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation/traduction de préfixe réseau IPv6).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** : saisissez d'abord un filtre et appliquez-le (la flèche verte).
Adresse		**Add (Ajoutez)** une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** en regard d'une adresse afin d'empêcher le proxy NDP pour cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Settings (Paramètres)	**VLAN Interface (Interface VLAN)** > **Advanced (Avancé)** > **DDNS**	Sélectionnez les paramètres pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Sélectionnez un profil de certificat que vous avez créé (ou créez-en un nouveau) pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
Constructeur		Sélectionnez le fournisseur DDNS (et le numéro de version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si vous sélectionnez une version antérieure d'un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Certains champs sont en lecture seule pour vous aviser des paramètres que le pare-feu utiliser pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s'il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l'interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6 - IPv6	**VLAN Interface (Interface VLAN)** > **Advanced (Avancé)** > **DDNS**	Ajoutez les adresses IPv6 configurées sur l'interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l'inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l'état de la mise à jour du nom d'hôte et une date de retour à des fins de résolution de problèmes.
Pour une adresse IPv4		
Type	**VLAN Interface (Interface VLAN)** > **IPv4**	Sélectionnez la méthode d'affectation d'un type d'adresse IPv4 à l'interface : • **Static (Statique)** - Vous devez indiquer manuellement l'adresse IP. • **DHCP Client (Client DHCP)** - Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/ protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP. Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
• **Type** d'adresse IPv4 = **Static (Statique)**		
Adresse IP	**VLAN Interface (Interface VLAN)** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d'**Address (Adresse)** de type **IP netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n'en avez plus besoin.
Type d'adresse IPv4 = **DHCP**		
Activer	**VLAN Interface (Interface VLAN)** > **IPv4**	Sélectionnez pour activer le client DHCP sur l'interface.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur		Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.
Envoyer le nom d'hôte		Sélectionnez cette option pour configurer le pare-feu (en tant que client DHCP) pour l'envoie du nom d'hôte de l'interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte, par défaut, le nom d'hôte du pare-feu est alors le choix indiqué dans le champ Nom d'hôte. Vous pouvez envoyer ce nom ou saisir un nom d'hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou minuscules, des chiffres, des points, des tirets et des traits de soulignement).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
Mesure d'itinéraire par défaut		Pour l'itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (plage de 1 à 65 535 ; il n'y a aucune valeur définie par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Pour une adresse IPv6		
Activer IPv6 sur l'interface	**VLAN Interface (Interface VLAN) > IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse	**VLAN Interface (Interface VLAN) > IPv6**	Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche. • **Send RA (Envoyer la publication de routeur)** – Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. Lorsque vous sélectionnez cette option, vous devez également **Enable Router Advertisement (Activer la publicité du routeur)** sur l'interface de manière globale. Pour plus d'informations sur la RA, reportez-vous à la section Activation de la publication de routeur. Les champs restants s'appliquent uniquement si vous activez la RA.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		• **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l'adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l'adresse valide est préférée, ce qui signifie que le pare-feu peut l'utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce qu'elle dépasse la **Valid Lifetime (Durée de vie valide)**. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** – Sélectionnez cette option si les systèmes dont les adresses IP sont comprises dans le préfixe publié sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l'ID d'une interface.
Activer la détection des doublons d'adresses	**VLAN Interface (Interface VLAN)** > **IPv6** > **Address Resolution (Résolution d'adresse)**	Sélectionnez cette option pour activer la détection des doublons d'adresses (DAD), ce qui vous permet d'indiquer le nombre de **Attempts (Tentatives) DAD**.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).
Intervalle NS (neighbor solicitation interval/ intervalle de sollicitation de voisins)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez cette option pour activer la surveillance du Protocole de découverte des voisins. Lorsqu'il est activé, vous pouvez sélectionner le NDP (dans la colonne Fonctions) et afficher des informations telles que l'adresse IPv6 d'un voisin découverte par le pare-feu, l'adresse MAC et User-ID correspondants (selon la situation la plus favorable).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
Activer la publication des routeurs	**VLAN Interface (Interface VLAN)** > **IPv6** > **Router Advertisement (Publication de routeur)**	Sélectionnez cette option pour assurer la Découverte de voisins sur les interfaces IPv6 et configurer les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s'agit d'un paramètre global de l'interface. Si vous souhaitez définir des options de publication de routeur pour les adresses IP individuelles, vous devez **Ajouter** une Adresse dans la table d'adresses IP et la configurer. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)		Indiquez l'intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Intervalle max. (s)		Indiquez l'intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez **0** pour indiquer l'absence de limite de saut.
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité, en millisecondes, que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified**

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		(non spécifiée) pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence	**VLAN Interface (Interface VLAN)** > **IPv6** > **Router Advertisement (cont) (Publication de routeur (suite))**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Inclure les informations DNS dans la publication de routeur	**VLAN Interface (Interface VLAN** > **IPv6** > **DNS Support (Prise en charge DNS)**	Sélectionnez cette option pour que le pare-feu envoie des informations DNS dans les publications du routeur NDP à partir de cette interface VLAN IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option.
Serveur		Il faut **Add (Ajouter)** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface VLAN IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l'ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface VLAN	Configuré dans	Description
		et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser les serveurs RDNS pour résoudre les noms de domaine (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'Intervalle maximal ; la valeur par défaut est 1 200).
Suffixe		Il vous faut **Ajouter** et configurer un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). La longueur de suffixe maximale est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet ensuite la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier l'ordre des suffixes ou **Delete (Supprimer)** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).

© 2020 Palo Alto Networks, Inc.

Réseau > Interfaces > En boucle

Utilisez les champs suivants pour configurer une interface en boucle :

Paramètres d'une interface en boucle	Configuré dans	Description
Nom de l'interface	**Interface en boucle**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **en boucle**. Dans le champ adjacent, saisissez un suffixe numérique (1-9999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Virtual Router (routeur virtuel - VR)	**Loopback Interface (Interface en boucle)** > **Config (Configuration)**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Profil de gestion	**Tunnel Interface (Interface de tunnel)** > **Advanced (Avancé)** > **Other Info (Autres informations)**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (intervalle compris entre 576 et 9 192, valeur par défaut : 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l'interface. La taille en octets de la MTU moins

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface en boucle	Configuré dans	Description
		la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv6)** - Intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv6)** - Intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Pour une adresse IPv4		
Adresse IP	**Loopback Interface (Interface en boucle)** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez une adresse IPv4 avec un masque de sous-réseau de /32, par exemple, 192.168.2.1/32. Seul le masque de sous-réseau /32 est pris en charge. • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Pour une adresse IPv6		
Activer IPv6 sur l'interface	**Loopback Interface (Interface en boucle)** > **IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface en boucle	Configuré dans	Description
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche.

© 2020 Palo Alto Networks, Inc.

Réseau > Interfaces > De tunnel

Utilisez les champs suivants pour configurer une interface de tunnel :

Paramètres d'une interface de tunnel	Configuré dans	Description
Nom de l'interface	**en texte clair**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **tunnel**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Virtual Router (routeur virtuel - VR)	**Tunnel Interface (Interface de tunnel)** > **Config (Configuration)**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Profil de gestion	**Tunnel Interface (Interface de tunnel)** > **Advanced (Avancé)** > **Other Info (Autres informations)**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; valeur par défaut de 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Pour une adresse IPv4		

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de tunnel	Configuré dans	Description
Adresse IP	**Tunnel Interface (Interface de tunnel)** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage interdomaine sans classes) : adresse_ip/masque (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Pour une adresse IPv6		
Activer IPv6 sur l'interface	**Tunnel Interface (Interface de tunnel)** > **IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface	**Tunnel Interface (Interface de tunnel)** > **IPv6**	Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche.

© 2020 Palo Alto Networks, Inc.

Réseau > Interfaces > SD-WAN

Créez une interface virtuelle SD-WAN et ajoutez des membres d'une ou plusieurs interfaces Ethernet physiques qui vont vers la même destination.

Paramètres d'une interface SD-WAN	
Nom de l'interface	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **sdwan**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface virtuelle SD-WAN.
Commentaire	Saisissez une description conviviale pour l'interface, telle que **`to internet (vers internet)`** ou **`to Western USA hub (vers un hub de l'ouest des USA)`**. Vos commentaires faciliteront l'identification des interfaces plutôt que d'essayer de décrypter des noms générés automatiquement dans les journaux et les rapports.
profil NetFlow ;	Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou définissez un nouveau **Netflow Profile (Profil Netflow)** (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Onglet Configuration	
Virtual Router (routeur virtuel - VR)	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou définissez un nouveau **Virtual System (Système virtuel)**.
Zone de sécurité	Sélectionnez une zone de sécurité pour l'interface ou définissez une nouvelle **Zone**. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface. L'interface virtuelle SD-WAN et tous les membres de l'interface doivent être dans la même zone de sécurité afin d'assurer que les mêmes règles de politique de sécurité s'appliquent à tous les chemins depuis la branche jusqu'à la même destination.
Onglet Avancé	
Interfaces	Sélectionnez les interfaces Ethernet Couche 3 (pour l'accès direct à internet [DIA]) ou les interfaces virtuelles de tunnel VPN (pour le hub) qui constituent cette interface virtuelle SD-WAN. Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN à un emplacement DIA ou de hub. Les interfaces peuvent avoir des étiquettes différentes. Cependant, si vous saisissez plus d'une interface, elles doivent toutes être du même type (tunnel VPN ou DIA).

© 2020 Palo Alto Networks, Inc.

Réseau > Zones

Les rubriques suivantes décrivent les zones de sécurité réseau.

Que voulez-vous faire ?	Reportez-vous à la section :
Quel est le but d'une zone de sécurité ?	Présentation des zones de sécurité
Quels sont les champs disponibles pour configurer des zones de sécurité ?	Étapes de configuration des zones de sécurité
Vous souhaitez en savoir plus ?	Segmentation de votre réseau via les interfaces et les zones

Présentation des zones de sécurité

Les zones de Sécurité sont une façon logique de regrouper des interfaces physiques et virtuelles sur le pare-feu afin de contrôler et de journaliser le trafic qui passe par toutes des interfaces spécifiques sur votre réseau. Une interface sur le pare-feu doit être affectée à une zone de sécurité avant que l'interface puisse traiter le trafic. De multiples interfaces de même type (par exemple, tap, niveau 2, niveau 3) peuvent être affectées à une zone, mais une interface ne peut appartenir qu'à une seule zone.

Les règles des politique sur le pare-feu font appel aux zones de sécurité pour identifier l'origine du trafic et sa destination. Le trafic peut circuler librement dans une zone, mais il ne peut pas circuler entre des zones différentes jusqu'à ce que vous définissiez une règle de politique de Sécurité qui l'autorise. Pour autoriser ou refuser le trafic intrazone, les règles de politique de Sécurité doivent faire référence à une zone source et à une zone de destination (pas des interfaces) et les zones doivent être du même type ; c'est-à-dire qu'une règle de politique de Sécurité peut autoriser ou refuser le trafic d'une zone de niveau 2 uniquement vers une autre zone de niveau 2.

Étapes de configuration des zones de sécurité

Pour définir une zone de sécurité, cliquez sur **Ajouter** et renseignez les informations suivantes.

Paramètres d'une zone de sécurité	Description
Name (Nom)	Saisissez un nom pour la zone (31 caractères maximum). Ce nom apparaît dans la liste des zones lors de la définition des politiques de sécurité et de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique au sein du routeur virtuel. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Location (Emplacement)	Ce champ n'est présent que si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée. Sélectionnez le système virtuel auquel la zone s'applique.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une zone de sécurité	Description
Type	Sélectionnez un type de zone (**Tap**, **Câble virtuel**, **Couche2**, **Couche3**, **Externe** ou **Tunnel**) pour afficher toutes les **Interfaces** de ce type qui n'ont pas été affectées à une zone. Les types de zones de couche 2 et de couche 3 répertorient toutes les interfaces et sous-interfaces Ethernet de ce type. **Add (Ajoutez)** les interfaces que vous souhaitez assigner à la zone. La zone externe est utilisée pour contrôler le trafic entre les systèmes virtuels multiples d'un seul pare-feu. Elle s'affiche uniquement si les pare-feu prennent en charge les systèmes virtuels multiples et uniquement si **Multi Virtual System Capability (Fonctionnalité de systèmes virtuels multiples)** est activé. Pour obtenir des informations sur les zones externes, reportez-vous à la section Trafic inter-VSYS restant au sein du pare-feu. Une interface peut appartenir à une seule zone dans un système virtuel.
Interfaces	Ajoutez une ou plusieurs interfaces à cette zone.
Profils de protection de zone	Sélectionnez un profil indiquant la manière dont le pare-feu répond aux attaques provenant de cette zone. Pour créer un nouveau profil, voir Réseau > Profils réseau > Protection de zone. Il est recommandé de défendre chaque zone avec un profil de protection de zone.
Activer la protection de la mémoire tampon des paquets	Configurez la protection de la mémoire tampon des paquets (Périphérique > Configuration > Session) de manière globale et appliquez-la à chaque zone. Le pare-feu applique la protection de la mémoire tampon des paquets à la zone d'entrée uniquement. Bien que la protection de la mémoire tampon des paquets soit désactivée par défaut, il est recommandé d'activer la protection de la mémoire tampon des paquets sur chaque zone pour protéger les mémoires tampons des pare-feu.
Paramètre des journaux	Sélectionnez un Profil de Transfert de journal pour transférer les journaux de protection de zone vers un système externe. Si vous disposez d'un profil de Transfert des journaux nommé par défaut, ce profil est automatiquement sélectionné pour ce menu déroulant lors de la définition d'une nouvelle zone de sécurité. Vous pouvez appliquer un contrôle prioritaire pour ce paramètre par défaut à tout moment en poursuivant la sélection d'un autre Profil de Transfert des journaux lors de la configuration d'une nouvelle zone de sécurité. Pour définir ou ajouter un nouveau profil de Transfert des journaux (et pour nommer un profil par défaut pour que ce menu déroulant soit automatiquement renseigné), cliquez sur **Nouveau** (voir Objets > Transfert des journaux). *Si vous configurez la zone dans un modèle Panorama, le menu déroulant Paramètres des journaux répertorie uniquement les profils de transfert des journaux partagés ; pour indiquer un profil non partagé, vous devez saisir son nom.*
Activer l'identification des utilisateurs	Si vous avez configuré User-ID™ pour effectuer un mappage nom d'utilisateur / adresse IP (détection), il est recommandé de **Enable User Identification (Activer l'identification des utilisateurs)** pour appliquer les

© 2020 Palo Alto Networks, Inc.

Paramètres d’une zone de sécurité	Description
	informations de mappage au trafic de cette zone. Si vous désactivez cette option, les rapports, les politiques et les journaux du pare-feu excluront les informations de mappage utilisateur du trafic de cette zone. Par défaut, si vous sélectionnez cette option, le pare-feu applique les informations de mappage utilisateur au trafic de tous les sous-réseaux de la zone. Pour limiter les informations à des sous-réseaux spécifiques de la zone, utilisez la **Include List (Liste d'inclusion)** et la **Exclude List (Liste d'exclusion)**. *Activez User-ID uniquement sur les zones approuvées. Si vous activez User-ID et le sondage du client sur une zone externe non approuvée (comme Internet), des sondages pourraient être envoyés en dehors de votre réseau protégé, ce qui entraînerait une divulgation des informations du nom de compte du service de l’agent User-ID, du nom de domaine et du hachage du mot de passe crypté, ce qui pourrait permettre à un pirate d’obtenir un accès non autorisé aux ressources protégées.* *User-ID effectue la détection dans la zone uniquement si elle se trouve dans la plage réseau surveillée. Si la zone est à l'extérieur de la plage, le pare-feu n'applique pas les informations de mappage utilisateur au trafic de la zone, même si vous sélectionnez Enable User Identification (Activer l'identification des utilisateurs). Pour plus d’informations, reportez-vous à la section* Inclure ou exclure des sous-réseaux pour le mappage d’utilisateur.
Liste d’inclusion de contrôle d’accès d’identification utilisateur	Par défaut, si vous ne spécifiez pas de sous-réseau dans cette liste, le pare-feu applique les informations de mappage utilisateur détectées à l'ensemble du trafic de cette zone de manière à ce qu'elles soient utilisées dans les journaux, les rapports et les politiques. Pour limiter les informations de mappage utilisateur à des sous-réseaux spécifiques de la zone, cliquez sur **Add (Ajouter)** et sélectionnez un objet d'adresse (ou de groupe d'adresses) ou saisissez la plage d'adresses IP (par exemple, 10.1.1.1/24) pour chaque sous-réseau. L'exclusion de tous les autres sous-réseaux est implicite, car la **Include List (Liste d’inclusion)** est une liste blanche. Vous n'avez donc pas besoin de les ajouter à la **Exclude List (liste d'exclusion)**. Ajoutez des entrées à **Exclude List (liste d'exclusion)** uniquement pour exclure les informations de mappage utilisateur d'un sous-ensemble des sous-réseaux de **Include List (liste d'inclusion)**. Par exemple, si vous ajoutez 10.0.0.0/8 à **Include List (liste d'inclusion)** et 10.2.50.0/22 à **Exclude List (liste d'exclusion)**, le pare-feu inclut les informations de mappage utilisateur de tous les sous-réseaux de 10.0.0.0/8 de la zone, excepté 10.2.50.0/22, et exclut les informations de tous les sous-réseaux de la zone se trouvant à l'extérieur de 10.0.0.0/8.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une zone de sécurité	Description
	Vous pouvez inclure uniquement des sous-réseaux qui se trouvent dans la plage réseau surveillée par User-ID. Pour plus d'informations, reportez-vous à la section Inclure ou exclure des sous-réseaux pour le mappage d'utilisateur*.*
Liste d'exclusion de contrôle d'accès d'identification utilisateur	Pour exclure les informations de mappage utilisateur d'un sous-ensemble de sous-réseaux de la **Liste d'inclusion**, cliquez sur **Ajouter** un objet d'adresse (ou de groupe d'adresses) ou saisissez la plage d'adresses IP pour chaque sous-réseau à exclure. *Si vous ajoutez des entrées à Exclude List (liste d'exclusion) mais pas à Include List (liste d'inclusion), le pare-feu exclut les informations de mappage utilisateur de tous les sous-réseaux de la zone, pas uniquement de ceux ajoutés.*

© 2020 Palo Alto Networks, Inc.

Réseau > VLAN

Le pare-feu prend en charge les VLAN qui respectent la norme IEEE 802.1Q. Chaque interface de couche 2 définie sur le pare-feu peut être associée à un VLAN. Ce même VLAN peut être assigné à plusieurs interfaces de couche 2, mais chaque interface peut appartenir à un seul VLAN.

Paramètres VLAN	Description
Name (Nom)	Saisissez un nom VLAN (31 caractères maximum). Ce nom apparaît dans la liste des VLAN lors de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Interface VLAN	Sélectionnez un Réseau > Interfaces > VLAN pour autoriser le routage du trafic hors du VLAN.
Interfaces	Indiquez les interfaces de pare-feu du VLAN.
Configuration MAC statique	Indiquez l'interface via laquelle une adresse MAC est accessible. Un contrôle prioritaire sera appliqué sur tout mappage de l'interface vers MAC appris.

© 2020 Palo Alto Networks, Inc.

Réseau > Câbles virtuels

Sélectionnez **Network (Réseau)** > **Virtual Wires (Câbles virtuels)** pour définir des câbles virtuels après avoir défini deux interfaces de câbles virtuels sur le réseau (Réseau > Interfaces).

Paramètres d'un câble virtuel	Description
Nom du câble virtuel	Saisissez un nom pour le câble virtuel (**31** caractères maximum). Il apparaît dans la liste des câbles virtuels lors de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Interfaces	Pour configurer un câble virtuel, sélectionnez deux interfaces Ethernet dans la liste affichée. Les interfaces sont répertoriées ici uniquement si elles disposent du type d'interface de câble virtuel et qu'elles n'ont pas été assignées à un autre câble virtuel. Pour plus d'informations sur les interfaces de câbles virtuels, consultez la section Interface du câble virtuel.
Etiquette autorisée	Saisissez un numéro d'étiquette (compris entre 0 et 4094) ou une plage de numéros d'étiquettes (étiquette1 - étiquette2) pour le trafic autorisé sur le câble virtuel. Une valeur d'étiquette de 0 indique un trafic non étiqueté (valeur par défaut). Plusieurs étiquettes ou plages doivent être séparées par des virgules. Tout trafic affichant une valeur d'étiquette exclue est supprimé. *Les valeurs d'étiquettes ne sont pas modifiées sur des paquets entrants ou sortants.* Lorsque vous utilisez des sous-interfaces de câble virtuel, la liste **Tag Allowed (Étiquettes autorisées)** va classer le trafic contenant les étiquettes répertoriées dans le câble virtuel parent. Les sous-interfaces de câble virtuel doivent utiliser des étiquettes qui n'existent pas dans la liste **Tag Allowed (Étiquettes autorisées)** du parent.
Pare-feu multicast	Sélectionnez cette option si vous voulez appliquer des règles de sécurité au trafic multicast. Si ce paramètre n'est pas appliqué, le trafic multicast est transféré dans le câble virtuel.
Transmission de l'état des liaisons	Sélectionnez cette option pour supprimer l'autre interface d'un câble virtuel en cas de détection d'un état de liaison inactif. Si vous ne sélectionnez pas cette option ou si vous la désactivez, l'état des liaisons n'est pas propagé dans le câble virtuel.

© 2020 Palo Alto Networks, Inc.

Réseau > Routeurs virtuels

Le pare-feu a besoin d'un routeur virtuel pour disposer d'itinéraires vers d'autres sous-réseaux, soit via des itinéraires statiques définis manuellement, soit via l'application de protocoles de routage de couche 3 (itinéraires dynamiques). Chaque interface de Couche 3, interface en boucle et interface VLAN définie sur le pare-feu doit être associée à un routeur virtuel. Chacune d'entre elles ne peut appartenir qu'à un seul routeur virtuel.

Pour définir un routeur virtuel, il faut des paramètres généraux et une combinaison d'itinéraires statiques ou de protocoles de routage dynamiques, selon les exigences de votre réseau. Vous pouvez également configurer d'autres fonctionnalités, comme la redistribution des itinéraires et les itinéraires ECMP.

Que voulez-vous faire ?	Reportez-vous à la section
Quels sont les éléments nécessaires d'un routeur virtuel ?	Paramètres généraux d'un routeur virtuel
Configurer :	Itinéraires statiques Redistribution d'itinéraire RIP OSPF OSPFv3 BGP Multidiffusion IP ECMP
Consulter les informations d'un routeur virtuel.	Statistiques d'exécution supplémentaires d'un routeur virtuel
Vous souhaitez en savoir plus ?	Mise en réseau

Paramètres généraux d'un routeur virtuel

- Réseau > Routeurs virtuels > Paramètres de routeur > Général

Tous les routeurs virtuels nécessitent l'assignation d'interfaces de couche 3 et de mesures de distance administrative, comme décrit dans le tableau suivant.

Paramètres généraux du routeur virtuel	Description
Name (Nom)	Saisissez un nom pour décrire le routeur virtuel (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Interfaces	Sélectionnez les interfaces à inclure dans le routeur virtuel. Ainsi, ils peuvent être utilisés comme interfaces sortantes dans la table de routage du routeur virtuel.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux du routeur virtuel	Description
	Pour spécifier le type d'interface, reportez-vous à Réseau > Interfaces. lors de l'ajout d'une interface, ses itinéraires connectés sont automatiquement ajoutés.
Distances administratives	Indiquez les distances administratives suivantes'A0;: • **Static routes (Itinéraires statiques)** - Intervalle compris entre 10 et 240 ; valeur par défaut : 10). • **OSPF Int** - Intervalle compris entre 10 et 240 ; valeur par défaut : 30). • **OSPF Ext** - Intervalle compris entre 10 et 240 ; valeur par défaut : 110). • **IBGP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 200). • **EBGP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 20). • **RIP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 120).

Itinéraires statiques

- Réseau > Routeurs virtuels > Itinéraires statiques

Vous pouvez ajouter un ou plusieurs itinéraires statiques. Cliquez sur l'onglet **IP** ou **IPv6** pour spécifier l'itinéraire utilisant une adresse IPv4 ou IPv6. Dans ce cas, vous devez généralement configurer des itinéraires par défaut (0.0.0.0/0). Ces derniers sont appliqués pour les destinations qui seraient alors introuvables dans la table de routage du routeur virtuel.

Paramètres d'Itinéraire statique	Description
Name (Nom)	Saisissez un nom pour identifier l'itinéraire statique (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Destination	Saisissez une adresse IP et un masque réseau en notation CIDR (Classless Inter-domain Routing/routage interdomaine sans classes) : *ip_address*mask (par exemple, 192.168.2.0/24 pour IPv4 ou 2001:db8::/32 pour IPv6). Vous pouvez également créer un objet d'adresse de type Masque réseau IP.
Interface	Sélectionnez l'interface pour transférer des paquets vers leur destination et/ou configurer les paramètres du saut suivant.
Saut suivant	Sélectionnez l'une des options suivantes : • **IP Address** (Adresse IP) : sélectionnez pour saisir l'adresse IP du routeur du saut suivant, ou sélectionnez ou créez un objet d'adresse de type Masque réseau IP. L'objet d'adresse doit avoir un masque réseau de /32 pour IPv4 ou de /128 pour IPv6. • **Next VR (Routeur virtuel suivant)** - Sélectionnez cette option pour sélectionner un routeur virtuel dans le pare-feu en tant que saut suivant. Cela vous permet d'effectuer un routage en interne entre des routeurs virtuels dans un pare-feu unique.

© 2020 Palo Alto Networks, Inc.

Paramètres d'Itinéraire statique	Description
	• **FQDN** : sélectionnez cette option pour identifier le saut suivant par FQDN. Sélectionnez ensuite un objet d'adresse de type FQDN ou créez un nouvel objet d'adresse de type FQDN. • **Discard (Supprimer)** - Indiquez si vous voulez arrêter le trafic vers cette destination. • **None (Aucun)** : sélectionnez cette option s'il n'existe aucun saut suivant pour l'itinéraire.
Distance admin	Indiquez la distance administrative de l'itinéraire statique (de 10 à 240, valeur par défaut : 10).
Mesure	Indiquez une mesure valide pour l'itinéraire statique (1 à 65 535).
Table d'itinéraires	Sélectionnez la table de routage dans laquelle le pare-feu installe l'itinéraire statique : • **Unicast** – Installe l'itinéraire dans la table de routage unicast. • **Multicast** – Installe l'itinéraire dans la table de routage multicast. • **Both (Les deux)** – Installe l'itinéraire dans la table de routage unicast et multicast. • **No Install (Aucune installation)** – N'installe pas l'itinéraire dans la table de routage (RIB) ; le pare-feu conserve l'itinéraire statique pour référence ultérieure jusqu'à ce que vous supprimiez cet itinéraire.
Profil BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) pour un itinéraire statique sur un pare-feu série PA-3200, série PA-5200, série PA-7000 ou série VM, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD pour cet itinéraire statique. Pour utiliser la BFD sur un itinéraire statique : • Le pare-feu et l'homologue qui se trouvent aux extrémités de l'itinéraire statique doivent prendre en charge les sessions BFD. • Le type de **Next Hop (Saut suivant)** de l'itinéraire statique doit correspondre à l'**IP Address (Adresse IP)**, et vous devez saisir une adresse IP valide. • Le paramètre de l'**Interface** ne peut correspondre à **None (Aucun)** ; vous devez sélectionner une interface (même si vous utilisez une adresse DHCP).
Surveillance des chemins	Sélectionnez cette option pour activer la surveillance des chemins pour l'itinéraire statique.

© 2020 Palo Alto Networks, Inc.

Paramètres d'Itinéraire statique	Description
Condition d'échec	Sélectionnez la condition selon laquelle le pare-feu considère le chemin surveillé comme inactif et considère donc l'itinéraire statique comme inactif : • **Any (N'importe laquelle)** – Si n'importe laquelle des destinations surveillées pour l'itinéraire statique n'est pas accessible par ICMP, le pare-feu supprime l'itinéraire statique de la RIB et de la FIB et ajoute l'itinéraire dynamique ou statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB. • **All (Toutes)** – Si toutes les destinations surveillées pour l'itinéraire statique ne sont pas accessibles par ICMP, le pare-feu supprime l'itinéraire statique de la RIB et de la FIB et ajoute l'itinéraire dynamique ou statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB. Sélectionner **All (Tout)** pour éviter toute éventualité d'une seule destination surveillée signalant une défaillance d'itinéraire statique lorsque cette destination surveillée est simplement hors ligne pour maintenance, par exemple.
Délai de maintien préemptif	Saisissez le nombre de minutes pendant lesquelles une surveillance des chemins inactifs doit conserver l'état Active (la surveillance des chemins évalue toutes les destinations surveillées de ses membres et doit rester Active avant que le pare-feu ne réinstalle l'itinéraire statique dans la RIB). Si le minuteur expire sans que la liaison devienne inactive ou instable, la liaison est jugée stable, la surveillance des chemins peut rester Active et le pare-feu peut ajouter l'itinéraire statique à la RIB. Si la liaison devient inactive ou instable pendant le délai de maintien, la surveillance des chemins échoue et le minuteur redémarre lorsque la surveillance désactivée reprend l'état Actif. Un **Preemptive Hold Time (Délai de maintien de préemption)** de zéro permet au pare-feu de réinstaller l'itinéraire statique dans la RIB immédiatement après l'activation de la surveillance des chemins. La plage est comprise entre 0 et 1 440 ; la valeur par défaut est 2.
Name (Nom)	Saisissez un nom pour la destination surveillée (31 caractères maximum).
Activer	Sélectionnez cette option pour activer la surveillance des chemins de cette destination spécifique pour l'itinéraire statique ; le pare-feu envoie des requêtes ping ICMP à cette destination.
IP source	Sélectionnez l'adresse IP que le pare-feu utilisera en tant que source dans la requête ping ICMP vers la destination surveillée : • Si l'interface possède plusieurs adresses IP, sélectionnez-en une. • Si vous sélectionnez une interface, le pare-feu utilise la première adresse IP affectée à l'interface par défaut. • Si vous sélectionnez **DHCP (Use DHCP Client address) (DHCP (Utiliser l'adresse du client DHCP))**, le pare-feu utilise l'adresse que DHCP a affectée à l'interface. Pour consulter l'adresse DHCP, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet** et dans la ligne de l'interface Ethernet, cliquez sur **Dynamic DHCP Client (Client DHCP**

© 2020 Palo Alto Networks, Inc.

Paramètres d'Itinéraire statique	Description
	dynamique). L'adresse IP s'affiche dans la fenêtre Statut de l'interface IP dynamique.
IP de destination	Saisissez une adresse IP fiable et stable ou un objet d'adresse pour lequel le pare-feu surveillera les chemins. La destination surveillée et la destination de l'itinéraire statique doivent utiliser la même famille d'adresses (IPv4 ou IPv6)
Intervalle des requêtes ping (sec)	Indiquez l'intervalle de la requête ping ICMP en secondes pour déterminer la fréquence à laquelle le pare-feu surveille les chemins (effectue un test ping sur la destination surveillée ; la plage est comprise entre 1 et 60 ; la valeur par défaut est 3).
Nombre de requêtes ping	Indiquez le nombre de paquets de requêtes ping ICMP consécutifs qui ne sont pas renvoyés par la destination surveillée avant que le pare-feu ne considère la liaison comme inactive. En fonction de la condition d'échec **Any (Indifférente)** ou **All (Toutes)**, si la surveillance des chemins est en état d'échec, le pare-feu supprime l'itinéraire statique de la RIB (la plage est comprise entre 3 et 10 et la valeur par défaut est 5). Par exemple, un Intervalle des requêtes ping de 3 secondes et un Nombre de requêtes ping de 5 requêtes ping manquées (le pare-feu ne reçoit pas de requêtes ping au cours des 15 dernières secondes) signifient que la surveillance des chemins détecte un échec de la liaison. Si la surveillance des chemins est en état d'échec et que le pare-feu reçoit une requête ping après 15 secondes, la liaison est considérée comme active ; en fonction de la condition d'échec **Any (Indifférente)** ou **All (Toutes)**, la surveillance des chemins de **Any (N'importe laquelle)** ou de **All (Toutes)** les destinations surveillées peut être considérée comme activée et le Délai de maintien de préemption commence.

Redistribution d'itinéraire

- Réseau > Routeur virtuel > Profils de redistribution

Les profils de redistribution orientent le pare-feu dans le filtrage, définissent des priorités et réalisent des actions en fonction du comportement souhaité du réseau. Cette redistribution permet à des itinéraires statiques et à des itinéraires acquis par d'autres protocoles d'être publiés via des protocoles de routage définis.

Les profils de redistribution doivent être appliqués aux protocoles de routage afin d'être effectifs. En l'absence de règles de redistribution, chaque protocole s'exécute séparément et ne communique pas au-delà de son domaine. Des profils de redistribution peuvent être ajoutés ou modifiés une fois tous les protocoles de routage configurés et la topologie de réseau résultante établie.

Appliquez des profils de redistribution aux protocoles'A0;RIP et OSPF en définissant des règles d'exportation. Appliquez des profils de redistribution au protocole BGP dans l'onglet **Règles de redistribution (Redistribution Rules)**. Consultez le tableau suivant.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de redistribution	Description
Name (Nom)	Vous pouvez **Ajouter** un **Profil de redistribution** et saisir le nom du profil.
Priorité	Saisissez une priorité (comprise entre 1 et 255) pour ce profil. Les profils sont classés dans l'ordre (valeur la plus basse en premier).
Redistribuer	Indiquez si la redistribution des itinéraires doit s'effectuer en fonction des paramètres de cette fenêtre. • **Redist** - Permet de redistribuer les itinéraires candidats correspondants. Si vous sélectionnez cette option, saisissez une nouvelle valeur de mesure. Une valeur de mesure inférieure correspond à un itinéraire préféré. • **No Redist (Ne pas redist)** - Sélectionnez cette option afin de ne pas redistribuer les itinéraires candidats correspondants.
Onglet Filtre général	
Type	Sélectionnez les types d'itinéraires de l'itinéraire candidat.
Interface	Sélectionnez des interfaces pour indiquer les interfaces de transfert d'un itinéraire candidat.
Destination	Pour indiquer la destination d'un itinéraire candidat, saisissez l'adresse IP ou le sous-réseau de destination (au format x.x.x.x ou x.x.x.x/n) et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Saut suivant	Pour indiquer la passerelle d'un itinéraire candidat, saisissez l'adresse IP ou le sous-réseau (au format x.x.x.x ou x.x.x.x/n) qui représente le saut suivant et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Onglet Filtre OSPF	
Type de chemin	Sélectionnez les types d'itinéraires de l'itinéraire OSPF candidat.
nominale	Indiquez l'identifiant de zone de l'itinéraire OSPF candidat. Entrez l'**OSPF area ID (ID de zone OSPF)** (au format x.x.x.x) et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Étiquette	Indiquez des valeurs pour les étiquettes OSPF. Saisissez une valeur d'étiquette numérique (1 à 255) et cliquez sur Ajouter. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Onglet Filtre BGP	
Communauté	Indiquez une communauté pour la politique de routage BGP.
Communauté étendue	Indiquez une communauté étendue pour la politique de routage BGP.

© 2020 Palo Alto Networks, Inc.

RIP

- Réseau > Routeurs virtuels > RIP

La définition d'un protocole RIP (Routing Information Protocol/protocole de routage Internet) comprend la configuration des paramètres généraux suivants :

Paramètres RIP	Description
Activer	Sélectionnez pour activer RIP.
Rejeter les itinéraires par défaut	(Recommandé) Sélectionnez si vous ne voulez pas apprendre d'itinéraires via RIP par défaut.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour RIP pour le routeur virtuel sur un pare-feu PA-5200 Series, PA-7000 Series, ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (profil ayant les paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver BFD)** pour désactiver BFD pour toutes les interfaces RIP du routeur virtuel ; vous ne pouvez activer BFD pour une seule interface RIP.

Les paramètres RIP des onglets suivants doivent également être configurés :

- **Interfaces** : Voir Onglet Interfaces RIP.
- **Timers (Minuteurs)** : Voir Onglet Minuteurs RIP.
- **Auth Profiles (Profils d'authentification)** : Voir l'Onglet Profils d'authentification RIP.
- **Export Rules (Règles d'exportation)** : Voir l'Onglet Règles d'exportation RIP.

Onglet Interfaces RIP

- Réseau > Routeurs virtuels > RIP > Interfaces

Utilisez les champs suivants pour configurer les interfaces RIP :

RIP – Paramètres de l'interface	Description
Interface	Sélectionnez une interface exécutant le protocole RIP.
Activer	Sélectionnez cette option pour activer ces paramètres.
Publier	Sélectionnez cette option pour activer la publication d'un itinéraire par défaut dans les homologues RIP avec la valeur la mesure spécifiée.
Mesure	Indiquez une valeur de mesure pour la publication d'un routeur. Ce champ n'est visible que si vous activez l'option **Advertise (Publier)**.

© 2020 Palo Alto Networks, Inc.

RIP – Paramètres de l'interface	Description
Profil d'authentification	Sélectionnez un profil.
Mode	Sélectionnez **normal**, **passive (passif)** ou **send-only (envoyer seulement)**.
BFD	Pour activer BFD pour une interface RIP (et ainsi appliquer un contrôle prioritaire sur le paramètre BFD pour RIP, pourvu que BFD ne soit pas activé pour RIP au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (profil ayant les paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour l'interface RIP.

Onglet Minuteurs RIP

- Réseau > Routeur virtuel > RIP > Minuteurs

Le tableau suivant décrit les minuteurs qui contrôlent les mises à jour et les périodes d'expiration des itinéraires RIP.

RIP – Paramètres du minuteur	Description
Timing RIP	
Intervalle en secondes (s)	Définissez la longueur de l'intervalle du minuteur en secondes. Ce délai est utilisé pour les champs restants du minuteur RIP (intervalle compris entre 1 et 60).
Intervalles de mise à jour	Saisissez le nombre d'intervalles entre les annonces de mise à jour des itinéraires (intervalle compris entre 1 et 3 600).
Intervalles d'expiration	Saisissez le nombre d'intervalles entre l'heure à laquelle l'itinéraire a été mis à jour pour la dernière fois et son expiration (intervalle compris entre 1 et 3 600).
Intervalles de suppression	Saisissez le nombre d'intervalles entre l'heure d'expiration de l'itinéraire et sa suppression (intervalle compris entre 1 et 3 600).

Onglet Profils d'authentification RIP

- Réseau > Routeur virtuel > RIP > Profils d'authentification

Par défaut, le pare-feu n'authentifie pas les messages RIP entre des voisins. Pour authentifier des messages RIP entre voisins, créez un profil d'authentification et appliquez-le à une interface qui exécute un protocole

© 2020 Palo Alto Networks, Inc.

RIP sur un routeur virtuel. Le tableau suivant décrit les paramètres de l'onglet **Auth Profiles (Profils d'authentification)**.

RIP – Paramètres du profil d'authentification	Description
Nom du profil	Saisissez un nom pour le profil d'authentification afin d'authentifier des messages RIP.
Type de mot de passe	Sélectionnez le type de mot de passe (simple ou MD5). • Si vous sélectionnez **Simple**, saisissez le mot de passe simple et confirmez-le. • Si vous sélectionnez **MD5**, saisissez une ou plusieurs entrées de mot de passe, notamment **Key-ID (ID-Clé)** (0 à 255), **Key (Clé)** et éventuellement le statut **Preferred (Préféré)**. Cliquez sur **Add (Ajouter)** pour chaque entrée, puis cliquez sur **OK**. Pour indiquer la clé à utiliser afin d'authentifier le message sortant, sélectionnez l'option **Preferred (Préféré)**.

Onglet Règles d'exportation RIP

- Réseau > Routeur virtuel > RIP > Règles d'exportation

Les règles d'exportation RIP vous permettent de contrôler quels sont les itinéraires que le routeur virtuel distribue aux homologues.

RIP – Paramètres des règles d'exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez pour autoriser le pare-feu à redistribuer son itinéraire par défaut vers des homologues.
Profil de redistribution	Cliquez sur **Add (Ajouter)** et sélectionnez ou créez un profil de redistribution vous permettant de modifier la redistribution, les filtres, la priorité et l'action d'un itinéraire en fonction du comportement réseau souhaité. Voir Redistribution de route.

OSPF

- Réseau > Routeur virtuel > OSPF

La définition du protocole OSPF (Open Shortest Path First / premier chemin ouvert le plus court) nécessite la configuration des paramètres généraux suivants (à l'exception de la BFD, qui est facultative) :

Paramètres OSPF	Description
Activer	Sélectionnez cette option pour activer le protocole OSPF.
Rejeter les itinéraires par défaut	(Recommandé) Sélectionnez cette option si vous ne voulez pas apprendre des itinéraires via OSPF par défaut.

© 2020 Palo Alto Networks, Inc.

Paramètres OSPF	Description
ID de routeur	Indiquez l'ID du routeur associé à l'instance OSPF dans ce routeur virtuel. Le protocole OSPF utilise l'ID du routeur pour identifier uniquement l'instance OSPF.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour OSPF pour le routeur virtuel sur un pare-feu PA-5200 Series, PA-7000 Series, PA-7000 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver BFD))** pour désactiver BFD pour toutes les interfaces OSPF du routeur virtuel ; vous pouvez activer BFD pour une seule interface OSPF.

De plus, vous devez configurer les paramètres OSPF dans les onglets suivants :

- **Areas (Zones)** : Voir Onglet des zones OSPF.
- **Auth Profiles (Profils d'authentification)** : Reportez-vous à la section Onglet Profils d'authentification OSPF.
- **Export Rules (Règles d'exportation)** : Reportez-vous à la section Onglet Règles d'exportation OSPF.
- **Advanced (Avancé)** : Voir Onglet avancé OSPF.

Onglet des zones OSPF

- Réseau > Routeur virtuel > OSPF > Zones

Les champs suivants décrivent les paramètres de la zone OSPF :

OSPF – Paramètres des zones	Description
Zones	
ID de zone	Configurez la zone sur laquelle les paramètres OSPF peuvent être appliqués. Saisissez un identifiant pour la zone au format x.x.x.x. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
Type	Sélectionnez l'une des options suivantes. • **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA (Link State Advertisement/annonce d'état de liaison) de la part des autres zones. Indiquez également si vous

© 2020 Palo Alto Networks, Inc.

OSPF – Paramètres des zones	Description
	souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale avec la valeur de mesure associée (plage de 1 à 255). Si l'option **Accept Summary (Accepter un récapitulatif)** est désactivée dans l'interface ABR (Area Border Router/routeur de bordure de zone) d'une zone terminale, la zone OSPF va agir en tant que zone TSA (Totally Stubby Area/zone complètement terminale) et l'interface ABR ne va propager aucune publication LSA récapitulative. • **NSSA** (Not-So-Stubby Area) - Il est possible de quitter directement la zone, mais uniquement par des itinéraires autres que des itinéraires OSPF. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA. Sélectionnez **Advertise Default Route (Publier l'itinéraire par défaut)** si vous souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale ainsi que la valeur de mesure associée (1 à 255). Sélectionnez également le type d'itinéraire utilisé pour publier la LSA par défaut. Cliquez sur **Add (Ajouter)** dans la section **External Ranges (Intervalles externes)** et saisissez des intervalles pour activer ou supprimer des itinéraires externes de publication appris via la zone NSSA vers d'autres zones.
Intervalle	Cliquez sur **Add (Ajouter)** pour agréger les adresses de destination LSA d'une zone dans des sous-réseaux. Activez ou supprimez des publications LSA correspondant au sous-réseau et cliquez sur **OK**. Répétez cette étape pour ajouter des plages supplémentaires.
Interface	Cliquez pour **Add (Ajouter)** une interface à inclure dans la zone et saisissez les informations suivantes : • **Interface** - Sélectionnez l'interface. • **Enable (Activer)** - Applique les paramètres de l'interface OSPF. • **Passive (Passif)** : sélectionnez cette option si vous ne voulez pas que l'interface OSPF envoie ou reçoive des paquets OSPF. Bien qu'aucun paquet OSPF ne soit envoyé ou reçu si vous choisissez cette option, l'interface est incluse dans la base de données LSA. • **Link type (Type de liaison)** : sélectionnez **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. Sélectionnez **p2p** (point-to-point/point à point) pour détecter automatiquement un voisin. Sélectionnez **p2mp** (point-to-multipoint/point-multipoint) lorsque les voisins doivent être définis manuellement. La définition manuelle des voisins est uniquement autorisée pour le mode p2mp. • **Metric (Mesure)** - Saisissez la mesure OSPF pour cette interface (0 à 65 535). • **Priority (Priorité)** - Saisissez la priorité OSPF pour cette interface (0 à 255). Il s'agit de la priorité d'élection d'un routeur en tant que routeur désigné (DR) ou en tant que DR de secours (BDR) conformément au protocole OSPF. Lorsque la valeur affiche 0, le routeur ne sera pas élu en tant que DR ou BDR.

© 2020 Palo Alto Networks, Inc.

OSPF – Paramètres des zones	Description
	• **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini. • **BFD** - Pour activer BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) pour une interface OSPF homologue (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour OSPF, pourvu que **BFD** ne soit pas activé pour OSPF au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD • Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour l'interface OSPF homologue. • **Hello Interval (sec) (Intervalle Hello (s))** - Intervalle, en secondes, auquel le processus OSPF envoie des paquets Hello à ses voisins directement connectés (intervalle compris entre 0 et 3 600 ; valeur par défaut : 10). • **Dead Counts (Nombre de pertes)** - Nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif. L'**intervalle Hello** multiplié par le **nombre de pertes** est égal à la valeur du minuteur d'inactivité (intervalle compris entre 3 et 20 ; valeur par défaut : 4). • **Retransmit Interval (sec) (Intervalle de retransmission (s))** - Durée, en secondes, pendant laquelle OSPF attend de recevoir une publication LSA (link-state advertisement) d'un voisin avant de la retransmettre (plage de 0 à 3 600 ; valeur par défaut de 10). • **Transit Delay (sec) (Délai de transit (s))** - Durée, en secondes, pendant laquelle une publication LSA est différée avant d'être envoyée d'une interface (plage de 0 à 3 600 ; valeur par défaut de 1).
Interface (suite)	• **Graceful Restart Hello Delay (sec) (Temporisation de redémarrage en douceur Hello (s))** - S'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. **La temporisation de redémarrage en douceur Hello** est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la **Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello)**. Par exemple, un **Intervalle Hello** de 10 secondes et un **Nombre de pertes** de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la **Temporisation de redémarrage en douceur Hello** est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive (plage de 1 à 10 ; valeur par défaut de 10).

© 2020 Palo Alto Networks, Inc.

OSPF – Paramètres des zones	Description
Liaison virtuelle	Configurez les paramètres de liaison virtuelle ou améliorez la connectivité de la zone du segment principal. Ces paramètres doivent être définis pour les routeurs de bordure de zone et à l'intérieur de la zone du segment principal (0.0.0.0). Cliquez sur **Add (Ajouter)**, saisissez les informations suivantes pour chaque liaison virtuelle à inclure dans la zone du segment principal et cliquez sur **OK**. • **Name (Nom)** : donnez un nom à la liaison virtuelle. • **Neighbor ID (ID du voisin)** : saisissez un ID de routeur (voisin) situé de l'autre côté de la liaison virtuelle. • **Transit Area (Zone de transit)** : saisissez l'ID de la zone de transit qui contient physiquement la liaison virtuelle. • **Enable (Activer)** : sélectionnez cette option pour activer la liaison virtuelle. • **Timing (Minutage)** : il est recommandé de conserver les paramètres de minutage par défaut. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.

Onglet Profils d'authentification OSPF

- Réseau > Routeur virtuel > OSPF > Profils d'authentification

Les champs suivants décrivent les paramètres des profils d'authentification OSPF :

OSPF – Paramètres des profils d'authentification	Description
Nom du profil	Donnez un nom au profil d'authentification. Pour authentifier les messages OSPF, commencez par définir les profils d'authentification, puis appliquez-les aux interfaces dans l'onglet **OSPF**.
Type de mot de passe	Sélectionnez le type de mot de passe (simple ou MD5). • Si vous sélectionnez **Simple**, saisissez le mot de passe. • Si vous sélectionnez **MD5**, saisissez une ou plusieurs entrées de mot de passe, notamment **Key-ID (ID-Clé)** (0 à 255), **Key (Clé)** et éventuellement le statut **Preferred (Préféré)**. Cliquez sur **Add (Ajouter)** pour chaque entrée, puis cliquez sur **OK**. Pour indiquer la clé à utiliser afin d'authentifier le message sortant, sélectionnez l'option **Preferred (Préféré)**.

Onglet Règles d'exportation OSPF

- Réseau > Routeur virtuel > OSPF > Règles d'exportation

Le tableau suivant décrit les champs utilisés pour exporter les itinéraires OSPF :

© 2020 Palo Alto Networks, Inc.

OSPF – Paramètres des règles d'exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez cette option pour autoriser la redistribution des itinéraires par défaut via OSPF.
Name (Nom)	Sélectionnez le nom d'un profil de redistribution. La valeur doit être un sous-réseau'A0;IP ou un nom de profil de redistribution valide.
Nouveau type de chemin	Sélectionnez le type de mesure à appliquer.
Nouvelle étiquette	Indiquez une étiquette pour l'itinéraire correspondant dont la valeur est de 32 bits.
Mesure	(Facultatif) Indiquez la mesure de l'itinéraire à associer à l'itinéraire exporté et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535).

Onglet Avancé OSPF

- Réseau > Routeur virtuel > OSPF > Avancé

Les champs suivants décrivent la compatibilité RFC 1583, les minuteurs OSPF et le redémarrage en douceur :

OSPF – Paramètres avancés	Description
Compatibilité avec RFC 1583	Sélectionnez pour garantir la compatibilité avec RFC 1583 (OSPF version 2).
Minuteurs	• **SPF Calculation Delay (sec) (Délai du calcul SPF (s))** - Vous permet d'ajuster le délai écoulé entre la réception de nouvelles informations sur la topologie et la réalisation d'un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent être ajustés de la même manière afin d'optimiser les délais de convergence. • **LSA Interval (sec) (Intervalle LSA (s))** - Indique le délai minimum écoulé entre les transmissions de deux instances du même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
Redémarrage sans échec	• **Enable Graceful Restart (Activer le redémarrage en douceur)** (option activée par défaut) - Un pare-feu activé pour cette fonction indique aux routeurs voisins de continuer à utiliser un itinéraire via le pare-feu, lorsque qu'une transition se produit et rend le pare-feu temporairement inactif. • **Enable Helper Mode (Activer le mode Aide)** (option activée par défaut) - Un pare-feu activé pour ce mode poursuit le transfert vers un périphérique adjacent lors du redémarrage du périphérique.

© 2020 Palo Alto Networks, Inc.

OSPF – Paramètres avancés	Description
	• **Enable Strict LSA Checking (Activer la vérification LSA stricte)** (option activée par défaut) - Cette fonction amène un pare-feu activé en mode Aide OSPF à quitter ce mode, en cas de modifications de topologie. • **Grace Period (sec) (Délai supplémentaire (s))** - Période en secondes pendant laquelle les périphériques homologues doivent poursuivre le transfert vers le pare-feu lorsque la contiguïté est rétablie ou lorsque le routeur est redémarré (plage de 5 à 1 800 ; valeur par défaut de 120). • **Max Neighbor Restart Time (Délai de redémarrage max. du voisin)** - Délai supplémentaire maximal en secondes que le pare-feu accepte en tant que routeur en mode Aide. Si les périphériques homologues offrent une période de grâce plus longue dans leur LSA de grâce, le pare-feu ne bascule pas en mode Aide (intervalle compris entre 5 et 1 800 ; valeur par défaut : 140).

OSPFv3

- Réseau > Routeur virtuel > OSPFv3

La configuration du protocole Open Shortest Path First v3 (OSPFv3) nécessite la configuration des trois premiers paramètres dans le tableau suivant (BFD est optionnel) :

Paramètres OSPFv3	Description
Activer	Sélectionnez cette option pour activer le protocole OSPF.
Rejeter les itinéraires par défaut	Sélectionnez cette option si vous ne voulez pas apprendre des itinéraires via OSPF par défaut.
ID de routeur	Indiquez l'ID du routeur associé à l'instance OSPF dans ce routeur virtuel. Le protocole OSPF utilise l'ID du routeur pour identifier uniquement l'instance OSPF.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour OSPFv3 pour le routeur virtuel sur un pare-feu PA-5200 Series, PA-7000 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour toutes les interfaces OSPFv3 sur le routeur virtuel. Vous ne pouvez pas activer la BFD pour une seule interface OSPFv3.

De plus, vous devez configurer les paramètres OSPFv3 dans les onglets suivants :

- **Areas (Zones)** : Voir Onglet des zones OSPFv3.

© 2020 Palo Alto Networks, Inc.

- **Auth Profiles (Profils d'authentification)** : Reportez-vous à la section Onglet Profils d'authentification OSPFv3.
- **Export Rules (Règles d'exportation)** : Reportez-vous à la section Onglet Règles d'exportation OSPFv3.
- **Advanced (Avancé)** : Voir Onglet avancé OSPFv3.

Onglet des zones OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Zones

Utilisez les champs suivants pour configurer les zones OSPFv3.

OSPv3 – Paramètres des zones	Description
Authentification	Sélectionnez le nom du profil d'authentification que vous souhaitez définir pour cette zone'A0;OSPF.
Type	Sélectionnez l'une des options suivantes : • **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA (Link State Advertisement/annonce d'état de liaison) de la part des autres zones. Indiquez également si vous souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale avec la valeur de mesure associée (1 à 255). Si l'option **Accept Summary (Accepter un récapitulatif)** est désactivée dans l'interface ABR (Area Border Router/routeur de bordure de zone) d'une zone terminale, la zone OSPF va agir en tant que zone TSA (Totally Stubby Area/zone complètement terminale) et l'interface ABR ne va propager aucune publication LSA récapitulative. • **NSSA** (Not-So-Stubby Area) - Il est possible de quitter directement la zone, mais uniquement par des itinéraires autres que des itinéraires OSPF. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA. Indiquez si vous souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale avec la valeur de mesure associée (1 à 255). Sélectionnez également le type d'itinéraire utilisé pour publier la LSA par défaut. Cliquez sur **Add (Ajouter)** dans la section **External Ranges (Intervalles externes)** et saisissez des intervalles pour activer ou supprimer des itinéraires externes de publication appris via la zone NSSA vers d'autres zones.
Intervalle	Cliquez sur **Add (Ajouter)** pour agréger les adresses IPv6 de destination LSA d'une zone par sous-réseau. Activez ou supprimez

© 2020 Palo Alto Networks, Inc.

OSPv3 – Paramètres des zones	Description
	des publications LSA correspondant au sous-réseau et cliquez sur **OK**. Répétez cette étape pour ajouter des plages supplémentaires.
Interface	Cliquez sur **Add (Ajouter)** et saisissez les informations suivantes pour chaque interface à inclure dans la zone et cliquez sur **OK**. • **Interface** - Sélectionnez l'interface. • **Enable (Activer)** - Applique les paramètres de l'interface OSPF. • **Instance ID (ID d'instance)** - Saisissez un numéro d'identification d'instance OSPFv3. • **Passive (Passif)** - Sélectionnez cette option si vous ne voulez pas que l'interface OSPF envoie ou reçoive des paquets OSPF. Bien qu'aucun paquet OSPF ne soit envoyé ou reçu si vous choisissez cette option, l'interface est incluse dans la base de données LSA. • **Link type (Type de liaison)** : sélectionnez **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. Sélectionnez **p2p** (point-to-point/point à point) pour détecter automatiquement un voisin. Sélectionnez **p2mp** (point-to-multipoint/point-multipoint) lorsque les voisins doivent être définis manuellement. La définition manuelle des voisins est uniquement autorisée pour le mode p2mp. • **Metric (Mesure)** - Saisissez la mesure OSPF pour cette interface (0 à 65 535). • **Priority (Priorité)** - Saisissez la priorité OSPF pour cette interface (0 à 255). Il s'agit de la priorité d'élection d'un routeur en tant que routeur désigné (DR) ou en tant que DR de secours (BDR) conformément au protocole OSPF. Lorsque la valeur affiche 0, le routeur ne sera pas élu en tant que DR ou BDR. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini. • **BFD** - Pour activer BFD (Bidirectional Forwarding Detection/ détection de transmission bidirectionnelle) pour une interface OSPFv3 homologue (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour OSPFv3, pourvu que **BFD** ne soit pas activé pour OSPFv3 au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD pour l'interface OSPFv3 homologue. • **Hello Interval (sec) (Intervalle Hello (s))** - Intervalle, en secondes, auquel le processus OSPF envoie des paquets Hello à ses voisins directement connectés (intervalle compris entre 0 et 3 600 ; valeur par défaut : 10).

© 2020 Palo Alto Networks, Inc.

OSPv3 – Paramètres des zones	Description
	• **Dead Counts (Nombre de pertes)** - Nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif. L'**intervalle Hello** multiplié par le **nombre de pertes** est égal à la valeur du minuteur d'inactivité (intervalle compris entre 3 et 20 ; valeur par défaut : 4). • **Retransmit Interval (sec) (Intervalle de retransmission (s))** - Durée, en secondes, pendant laquelle OSPF attend de recevoir une publication LSA (link-state advertisement) d'un voisin avant de la retransmettre (plage de 0 à 3 600 ; valeur par défaut de 10). • **Transit Delay (sec) (Délai de transit (s))** - Durée, en secondes, pendant laquelle une publication LSA est différée avant d'être envoyée d'une interface par le pare-feu (plage de 0 à 3 600 ; valeur par défaut de 1).
Interface (suite)	• **Graceful Restart Hello Delay (sec) (Temporisation de redémarrage en douceur Hello (s))** - S'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. **La temporisation de redémarrage en douceur Hello** est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la **Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello)**. Par exemple, un **Intervalle Hello** de 10 secondes et un **Nombre de pertes** de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la **Temporisation de redémarrage en douceur Hello** est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive (plage de 1 à 10 ; valeur par défaut de 10). • **Neighbors (Voisins)** - Pour les interfaces p2pmp, saisissez l'adresse IP de tous les voisins accessibles via cette interface.
Liaisons virtuelles	Configurez les paramètres de liaison virtuelle ou améliorez la connectivité de la zone du segment principal. Ces paramètres doivent être définis pour les routeurs de bordure de zone et à l'intérieur de la zone du segment principal (0.0.0.0). Cliquez sur **Add (Ajouter)**, saisissez les informations suivantes pour chaque liaison virtuelle à inclure dans la zone du segment principal et cliquez sur **OK**. • **Name (Nom)** : donnez un nom à la liaison virtuelle.

© 2020 Palo Alto Networks, Inc.

OSPv3 – Paramètres des zones	Description
	• **Instance ID (ID d'instance)** - Saisissez un numéro d'identification d'instance OSPFv3. • **Neighbor ID (ID du voisin)** : saisissez un ID de routeur (voisin) situé de l'autre côté de la liaison virtuelle. • **Transit Area (Zone de transit)** : saisissez l'ID de la zone de transit qui contient physiquement la liaison virtuelle. • **Enable (Activer)** : sélectionnez cette option pour activer la liaison virtuelle. • **Timing (Minutage)** : il est recommandé de conserver les paramètres de minutage par défaut. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.

Onglet Profils d'authentification OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Profils d'authentification

Utilisez les champs suivants pour configurer l'authentification pour OSPFv3.

OSPFv3 – Paramètres des profils d'authentification	Description
Nom du profil	Donnez un nom au profil d'authentification. Pour authentifier les messages OSPF, commencez par définir les profils d'authentification, puis appliquez-les aux interfaces dans l'onglet **OSPF**.
SPI	Indiquez l'index de paramètres de sécurité (SPI) pour le parcours du paquet entre le pare-feu distant et l'homologue.
Protocole	Indiquez l'un des protocoles suivants : • **ESP** - Protocole Encapsulating Security Payload/Encapsulation sécurisée de la charge utile • **AH** - Protocole Authentication Header
Algorithme de chiffrement	Indiquez l'un des suivants : • **None (Aucun)** - Aucun algorithme de chiffrement n'est utilisé. • **SHA1** (par défaut) - Algorithme SHA 1. • **SHA256** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 256 bits. • **SHA384** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 384 bits. • **SHA512** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 512 bits.

© 2020 Palo Alto Networks, Inc.

OSPFv3 – Paramètres des profils d'authentification	Description
	• **MD5** - Algorithme Message Digest 5 (algorithme de condensé de message 5).
Clé/Confirmer la clé	Saisissez et confirmez la clé d'authentification.
Chiffrement (protocole ESP uniquement)	Indiquez l'un des suivants : • **3des** (par défaut) – applique l'algorithme de chiffrement de données triple (3DES) à l'aide de trois clés cryptographiques de 56 bits. • **aes-128-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l'aide de clés cryptographiques de 128 bits. • **aes-192-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l'aide de clés cryptographiques de 192 bits. • **aes-256-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l'aide de clés cryptographiques de 256 bits. • **null (aucun)** - Aucun chiffrement n'est utilisé.
Clé/Confirmer la clé	Saisissez et confirmez la clé de chiffrement.

Onglet Règles d'exportation OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Règles d'exportation

Utilisez les champs suivants pour exporter les itinéraires OSPFv3.

OSPFv3 – Paramètres des règles d'exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez cette option pour autoriser la redistribution des itinéraires par défaut via OSPF.
Name (Nom)	Sélectionnez le nom d'un profil de redistribution. La valeur doit être un sous-réseau'A0;IP ou un nom de profil de redistribution valide.
Nouveau type de chemin	Sélectionnez le type de mesure à appliquer.
Nouvelle étiquette	Indiquez une étiquette pour l'itinéraire correspondant dont la valeur est de 32 bits.

© 2020 Palo Alto Networks, Inc.

OSPFv3 – Paramètres des règles d'exportation	Description
Mesure	(Facultatif) Indiquez la mesure de l'itinéraire à associer à l'itinéraire exporté et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535).

Onglet Avancé OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Avancé

Utilisez les champs suivants pour désactiver le routage de transit pour les calculs SPF, configurer les minuteurs OSPFv3 et configurer un redémarrage en douceur pour OSPFv3.

OSPFv3 – Paramètres avancés	Description
Désactiver le routage de l'acheminement pour le calcul SPF	Sélectionnez cette option si vous souhaitez définir le bit R dans les LSA de routeur envoyés par ce pare-feu pour indiquer que le pare-feu n'est pas actif. Lorsqu'il est dans cet état, le pare-feu prend part à OSPFv3 mais les autres routeurs n'envoient pas le trafic de l'acheminement. Dans cet état, le trafic local est transféré au pare-feu. Cela est utile lors de la maintenance sur un réseau à double interface, car le trafic peut être encore atteint lorsqu'il est réacheminé vers le pare-feu.
Minuteurs	• **SPF Calculation Delay (sec) (Délai du calcul SPF (s))** - Cette option est un temporisateur vous permettant d'ajuster le délai écoulé entre la réception de nouvelles informations sur la topologie et la réalisation d'un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent être ajustés de la même manière afin d'optimiser les délais de convergence. • **LSA Interval (sec) (Intervalle LSA (s))** - Cette option indique le délai minimum écoulé entre les transmissions de deux instances du même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
Redémarrage sans échec	• **Enable Graceful Restart (Activer le redémarrage en douceur)** (option activée par défaut) - Un pare-feu activé pour cette fonction indique aux routeurs voisins de continuer à utiliser un itinéraire via le pare-feu, lorsque qu'une transition se produit et rend le pare-feu temporairement inactif. • **Enable Helper Mode (Activer le mode Aide)** (option activée par défaut) - Un pare-feu activé pour ce mode poursuit le transfert vers un périphérique adjacent lors du redémarrage du périphérique.

© 2020 Palo Alto Networks, Inc.

OSPFv3 – Paramètres avancés	Description
	• **Enable Strict LSA Checking (Activer la vérification LSA stricte)** (option activée par défaut) - Cette fonction amène un pare-feu activé en mode Aide OSPF à quitter ce mode, en cas de modifications de topologie. • **Grace Period (sec) (Délai supplémentaire (s))** - Période, en secondes, pendant laquelle les périphériques homologues doivent poursuivre le transfert vers le pare-feu lorsque la contiguïté est rétablie ou lorsque le routeur est redémarré (plage de 5 à 1 800 ; valeur par défaut de 120). • **Max Neighbor Restart Time (Durée maximale de redémarrage des voisins)** - Période de grâce maximale en secondes que le pare-feu accepte en tant que routeur en mode Aide. Si les périphériques homologues offrent une période de grâce plus longue dans leur LSA de grâce, le pare-feu ne bascule pas en mode Aide (intervalle compris entre 5 et 800 ; valeur par défaut : 140).

BGP

- Réseau > Routeur virtuel > BGP

La configuration du Protocole de passerelle frontière (BGP) vous oblige à configurer Paramètres BGP de base pour activer BGP et configurer l'ID du routeur et le Numéro AS comme décrit dans le tableau suivant. En outre, vous devez configurer un homologue BGP dans le cadre d'un groupe d'homologues BGP.

Configurez les paramètres BGP restants dans les onglets suivants, si nécessaire pour votre réseau :

- **General (Général)** : voir Onglet Général BGP ;
- **Advanced (Avancé)** : voir Onglet Avancé BGP ;
- **Peer Group (Groupe d'homologues)** : voir Onglet Groupe d'homologues BGP.
- **Import (Importer)** : voir Onglets d'Importation et d'Exportation BGP.
- **Export (Exporter)** : voir Onglets d'Importation et d'Exportation BGP.
- **Conditional Adv (Publication condit.)** : voir Onglet Avancé Publication conditionnelle BGP.
- **Aggregate (Agréger)** : voir Onglet Agrégation BGP ;
- **Redist Rules (Règles de redistribution)** : voir Onglet Règles de redistribution BGP.

Paramètres BGP de base

Pour utiliser BGP sur un routeur virtuel, vous devez activer BGP et configurer l'ID du routeur et le Numéro AS ; l'activation de BFD est facultative.

Paramètres BGP	Configuré dans	Description
Activer	**BGP**	Sélectionnez cette action pour activer BGP.
ID de routeur		Saisissez l'adresse IP à assigner à un routeur virtuel.
Numéro AS		Saisissez le numéro de l'AS auquel appartient un routeur virtuel, en fonction de l'ID du routeur (compris entre 1 et 4 294 967 295).

© 2020 Palo Alto Networks, Inc.

Paramètres BGP	Configuré dans	Description
BFD		Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour BGP pour le routeur virtuel sur un pare-feu PA-5200 Series, PA-7000 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD existant sur le pare-feu • création d'un **nouveau profil BFD**. Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver BFD pour toutes les interfaces BGP du routeur virtuel ; vous ne pouvez activer la BFD pour une seule interface BGP. *Si vous activez ou désactivez la BFG globalement, toutes les interfaces qui exécutent BGP seront désactivées et réactivées avec la fonctionnalité BFD, ce qui peut interrompre le trafic BGP. Par conséquent, activez la BFD sur les interfaces BGP lors des périodes creuses où une conversion n'influe pas sur le trafic de production.*

Onglet Général BGP

- Réseau > Routeur virtuel > BGP > Général

Utilisez les champs suivants pour configurer les paramètres généraux de BGP.

Paramètres généraux de BGP	Configuré dans	Description
Rejeter les itinéraires par défaut	**Général** > **BGP**	Sélectionnez pour ignorer les itinéraires par défaut publiés par les homologues BGP.
Installer un itinéraire		Sélectionnez pour installer des itinéraires BGP dans la table de routage générale.
Agréger MED		Sélectionnez cette option pour activer l'agrégation d'un itinéraire, même lorsque des itinéraires affichent différentes valeurs MED (Multi-Exit Discriminator/discriminateur Multi-Sortie).
Préférence locale par défaut		Indique une valeur que le pare-feu peut utiliser pour déterminer les préférences entre différents chemins.
Format AS		Sélectionnez le format 2 octets (par défaut) ou 4 octets. Ce paramètre peut être configuré à des fins d'interopérabilité.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux de BGP	Configuré dans	Description
Toujours comparer MED		Activez la comparaison MED des chemins de voisins situés dans différents systèmes autonomes.
Comparaison MED déterministe		Activez la comparaison MED afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues iBGP (homologues BGP figurant dans le même système autonome).
Profils d'authentification		Vous devez **Add (Ajouter)** un profil d'authentification et configurer les paramètres suivants : • **Profile Name (Nom du profil)** - Saisissez un nom pour identifier le profil. • **Secret/Confirm Secret (Phrase secrète/Confirmer une phrase secrète)** - Saisissez et confirmez une phrase secrète pour les communications d'homologues BGP. Supprimez (⊖) les profils vous n'en avez plus besoin.

Onglet Avancé BGP

- Réseau > Routeur virtuel > BGP > Avancé

Les paramètres avancés de BGP incluent une multitude de fonctionnalités. Vous pouvez exécuter ECMP sur plusieurs systèmes BGP autonomes. Vous pouvez exiger de la part des homologues eBGP qu'ils énumèrent leur propre AS comme premier AS dans un attribut AS_PATH (pour éviter les paquets de Mise à jour usurpés). Vous pouvez configurer le redémarrage en douceur de BGP, un moyen au moyen duquel les homologues BGP indiquent s'ils peuvent conserver l'état du transfert lors d'un redémarrage de BGP afin de minimiser les conséquences des itinéraires instables (qui montent et qui descendent). Vous pouvez configurer les réflecteurs d'itinéraires et les confédérations d'AS ; deux méthodes qui permettent d'éviter un maillage complet des appairages BGP dans un AS. Vous pouvez configurer le blocage de l'itinéraire pour éviter la convergence inutile du routeur lorsqu'un réseau BGP est instable et que les itinéraires sont instables.

Paramètres avancés BGP	Configuré dans	Description
Support de multiples AS dans ECMP	**BGP** > **Advanced (avancé)**	Sélectionnez si vous activez ECMP pour un routeur virtuel et que vous souhaitez exécuter ECMP sur plusieurs systèmes BGP autonomes.
Appliquer le premier AS pour EBGP		Amène le pare-feu à supprimer un paquet de Mise à jour entrant d'un homologue eBGP qui ne répertorie pas le numéro AS de l'homologue eBGP comme premier numéro AS dans l'attribut AS_PATH. Cela empêche BGP de traiter ultérieurement un paquet de Mise à jour usurpé ou erroné qui provient d'un AS autre qu'un AS voisin. La valeur par défaut est activée.

© 2020 Palo Alto Networks, Inc.

Paramètres avancés BGP	Configuré dans	Description
Redémarrage sans échec		Activez l'option de redémarrage en douceur. • **Stale Route Time (Délai pour itinéraire obsolète)** - Indiquez la durée, en secondes, pendant laquelle un itinéraire peut rester dans l'état Obsolète (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120). • **Local Restart Time (Délai de redémarrage local (s))** - Spécifiez le délai d'attente, en secondes, du pare-feu local pour redémarrer. Cette valeur est publiée chez les homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120). • **Max Peer Restart Time (Durée maximale de redémarrage des homologues)** - Indiquez la durée maximale, en secondes, qu'un pare-feu local accepte comme délai de redémarrage en période de grâce pour des périphériques homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120).
ID du groupe de réflecteurs		Indiquez un identifiant IPv4 pour représenter un groupe de réflecteurs. Un réflecteur d'itinéraire (routeur) dans une AS effectue un rôle visant à republier des itinéraires qu'il a appris à ses homologues (plutôt que d'exiger une connectivité en maillage complet et que tous les homologues s'envoient des itinéraires les uns aux autres). Le réflecteur d'itinéraire simplifie la configuration.
AS membre de la confédération		Indiquez le numéro d'identification du système autonome (AS) qui n'est visible qu'au sein de la confédération BGP (également nommé numéro de système sous-autonome). Utilisez une confédération BGP pour diviser les systèmes autonomes en systèmes sous-autonomes et réduire l'appairage de maillage complet.
Profils d'atténuation	**BGP** > **Advanced (avancé)** (suite)	Le blocage de l'itinéraire est une méthode qui détermine si un itinéraire est supprimé de la publication parce qu'il est instable. Le blocage de l'itinéraire peut réduire le nombre de fois que les routeurs sont forcés à la conversion en raison de l'instabilité des itinéraires. Les paramètres sont les suivants'A0;: • **Profile Name (Nom du profil)** - Saisissez un nom pour identifier le profil. • **Enable (Activer)** - Activez le profil. • **Cutoff (Limite)** - Indiquez le seuil de retrait d'itinéraires au-delà duquel une publication d'itinéraire est supprimée (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 1,25). • **Reuse (Réutiliser)** - Indiquez le seuil de retrait d'itinéraires au-dessous duquel un itinéraire supprimé est réutilisé (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 5). • **Max. Max. Hold Time (Durée d'attente maximale)** - Indiquez la durée maximale, en secondes, au bout de laquelle un itinéraire peut être supprimé, quelle que soit son instabilité (intervalle compris entre 0 et 3 600 ; valeur par défaut : 900). • **Réduction de moitié pendant l'état accessible** – Indiquez la durée, en secondes, après laquelle la mesure de stabilité d'un

© 2020 Palo Alto Networks, Inc.

Paramètres avancés BGP	Configuré dans	Description
		itinéraire est réduite de moitié si le pare-feu est accessible (plage de 0 à 3 600 ; par défaut 300). • **Réduction de moitié pendant l'état inaccessible** – Indiquez la durée, en secondes, après laquelle la mesure de stabilité d'un itinéraire est réduite de moitié si le pare-feu est inaccessible (plage de 0 à 3 600 ; par défaut 300). Supprimez ( ) les profils vous n'en avez plus besoin.

Onglet Groupe d'homologues BGP

- Réseau > Routeur virtuel > BGP > Groupe d'homologues

Un groupe d'homologues BGP est un ensemble d'homologues BGP qui partagent des paramètres comme le type de groupe d'homologues (EBGP, par exemple) ou le paramètre servant à supprimer des numéros AS privés de la liste AS_PATH que le routeur virtuel envoie dans les paquets de Mise à jour. Les groupes d'homologues BGP vous évitent de devoir configurer plusieurs homologues avec les mêmes paramètres. Vous devez configurer au moins un groupe d'homologues BGP afin de configurer les homologues BGP appartenant au groupe.

Paramètres du groupe d'homologues BG	Configuré dans	Description
Name (Nom)	**BGP** > **Peer Group (Groupe d'homologues)**	Saisissez un nom pour identifier le groupe d'homologues.
Activer		Sélectionnez cette option pour activer un groupe d'homologues.
Chemin AS de confédération agrégé		Sélectionnez pour inclure un chemin vers l'AS de confédération agrégé configuré.
Réinitialisation logicielle avec les informations stockées		Sélectionnez pour procéder à une réinitialisation logicielle du pare-feu après avoir mis à jour les paramètres des homologues.
Type		Indiquez le type d'homologue ou de groupe et configurez les paramètres associés (pour plus de détails sur les options **Import Next Hop (Importer le saut suivant)** et **Export Next Hop (Exporter le saut suivant)**, consultez le tableau ci-dessous). • **IBGP** - Spécifiez les options suivantes : • **Exporter le saut suivant** • **EBGP Confed (Conféd. EBGP)** - Spécifiez les options suivantes : • **Exporter le saut suivant** • **IBGP Confed (Conféd. IBGP)** - Spécifiez les options suivantes : • **Exporter le saut suivant**

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe d'homologues BG	Configuré dans	Description
		• **EBGP** - Indiquez les options suivantes : • **Importer le saut suivant** • **Exporter le saut suivant** • **Remove Private AS (Supprimer l'AS privé)** (sélectionnez cette option si vous voulez forcer le protocole BGP à supprimer des numéros d'AS privés provenant de l'attribut AS_PATH).
Importer le saut suivant		Sélectionnez une option pour importer le saut suivant'A0;: • **Original** – Utilisez l'adresse du Saut suivant fournie dans la publication de l'itinéraire d'origine. • **Use Peer (Utiliser homologue)** – Utilisez l'adresse IP de l'homologue en tant qu'adresse du Saut suivant.
Exporter le saut suivant		Sélectionnez une option pour exporter le saut suivant'A0;: • **Resolve (Résoudre)** – Résolvez l'adresse Saut suivant à l'aide de la base d'informations de transfert (FIB). • **Original** – Utilisez l'adresse du Saut suivant fournie dans la publication de l'itinéraire d'origine. • **Use Self (Utiliser auto)** – Remplacez l'adresse du Saut suivant par l'adresse IP du routeur virtuel afin de s'assurer qu'elle apparaîtra dans le chemin de transfert.
Supprimer l'AS privé		Sélectionnez cette option pour supprimer les systèmes autonomes privés de la liste AS_PATH.
Name (Nom)	**BGP** > **Peer Group (Groupe d'homologues)** > **Peer (Homologue)**	Ajouter un **New (Nouvel)** homologue BGP et saisissez un nom pour l'identifier.
Activer		Sélectionnez cette option pour activer un homologue.
AS Homologue		Indiquez le système autonome (AS) de l'homologue.
Activer les extensions MP-BGP	**BGP** > **Peer Group (Groupe d'homologues)** > **Peer (Homologue)** > **Addressing (Adressage)**	Permet au pare-feu de prendre en charge l'Identifiant de la famille d'adresses de BGP multi-protocoles pour IPv4 et IPv6 et les options d'Identifiant de la famille d'adresses subséquentes conformément au protocole RFC 4760.
Type de famille d'adresses		Sélectionnez soit la famille d'adresses **IPv4** ou **IPv6** que les sessions BGP avec cet homologue prennent en charge.
Famille d'adresses subséquentes		Sélectionnez le protocole de la famille d'adresses subséquentes **Unicast** ou **Multicast** que les sessions BGP avec cet homologue transmettent.
Adresse locale – Interface		Choisissez une interface de pare-feu.

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe d'homologues BG	Configuré dans	Description
Adresse locale – IP		Choisissez une adresse IP locale.
Adresse de l'homologue — Type et adresse		Sélectionnez le type d'adresse qui identifie l'homologue : • **IP** —Sélectionnez l'adresse IP et sélectionnez un objet d'adresse qui utilise une adresse IP (ou créez un nouvel objet d'adresse qui utilise une adresse IP). • **FQDN** —Sélectionnez FQDN et sélectionnez un objet d'adresse qui utilise un FQDN (ou créez un nouvel objet d'adresse qui utilise un FQDN).
Profil d'authentification	**BGP** > **Peer Group (Groupe d'homologues)** > **Peer (Homologue)** > **Connection Options (Options de connexion)**	Sélectionnez un profil ou sélectionnez **New Auth Profile (Nouveau profil d'authentification)** dans le menu déroulant. Saisissez un **Name (Nom)** de profil et l'élément **Secret**, et **(Confirmer l'élément secret)**.
Intervalle KeepAlive		Indiquez un intervalle après lequel les itinéraires d'un homologue sont supprimés conformément au paramètre de durée d'attente (plage comprise entre 0 et 1 200 secondes ; valeur par défaut : 30 secondes).
Plusieurs sauts		Définissez la valeur TTL (Time-To-Live) dans l'en-tête IP. Plage comprise entre 0 et 255. La valeur par défaut de 0 signifie 1 pour eBGP et 255 pour iBGP.
Délai avant ouverture		Indiquez le délai écoulé entre l'ouverture de la connexion TCP de l'homologue et l'envoi du premier message d'ouverture BGP (plage comprise entre 0 et 240 secondes ; par défaut : 0 seconde).
temps d'attente		Indiquez la durée pouvant s'écouler entre des messages KEEPALIVE ou UPDATE successifs émis par un homologue avant la fermeture de la connexion d'un homologue (plage comprise entre 3 et 3 600 secondes ; par défaut : 90 secondes).
Temps d'attente d'inactivité		Indiquez la durée d'attente en état inactif avant de retenter une connexion à un homologue (plage comprise entre 1 et 3 600 secondes ; par défaut : 15 secondes).
Connexions entrantes – Port distant		Indiquez le numéro de port entrant et veillez à **Allow (Autoriser)** le trafic vers ce port.
Connexions sortantes – Port local		Indiquez le numéro de port sortant et veillez à **Allow (Autoriser)** le trafic provenant de ce port
Client réflecteur	**BGP** > **Peer Group (Groupe d'homologues)** > **Peer**	Sélectionnez le type de client réflecteur (**Non-Client**, **Client** ou **Meshed Client (Client avec maillage)**). Les itinéraires qui sont envoyés par les clients réflecteurs sont partagés avec l'ensemble des homologues BGP internes et externes.

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe d'homologues BG	Configuré dans	Description
Type d'homologie	**(Homologue) > Advanced (Avancé)**	Indiquez un homologue Bilatéral ou laissez ce champ Non spécifié.
Nombre max. de préfixes		Indiquez le nombre maximum de préfixes IP pris en charge (1 à 100 000 ou illimité).
Activer la détection des boucles côté expéditeur		Permet de faire en sorte que le pare-feu vérifie l'attribut AS_PATH d'un itinéraire dans sa FIB avant d'envoyer l'itinéraire dans une mise à jour afin de s'assurer que le numéro AS de l'homologue n'est pas sur la liste AS_PATH. Si c'est le cas, le pare-feu le supprime pour éviter une boucle. Généralement, le récepteur effectue la détection des boucles, mais cette fonctionnalité d'optimisation comporte la détection des boucles par l'expéditeur.
BFD		Pour activer la BFD (Bidirectional Forwarding Detection) pour un homologue BGP (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour BGP, du moment que la **BFD** n'est pas désactivée pour BGP au niveau du routeur virtuel), sélectionnez le profil par défaut (paramètres BFD par défaut), un profil BFD existant, **Inherit-vr-global-setting** (pour hériter du profil BFD BGP global), ou **New BFD Profile (Nouveau profil BFD)** (pour créer un nouveau profil BFD). **Disable BFD (Désactiver la BFD)** - désactive la BFD pour l'homologue BGP. *Si vous activez ou désactivez la BFG globalement, toutes les interfaces qui exécutent BGP seront désactivées et réactivées avec la fonctionnalité BFD, ce qui pourrait interrompre le trafic BGP. Lorsque vous activez la BFD sur l'interface, le pare-feu arrête la connexion BGP vers l'homologue pour programmer la BFD sur l'interface. La connexion BGP sera abandonnée sur le périphérique homologue, ce qui pourrait entraîner une reconvergence qui influera sur le trafic de production. vous devez activer la BFD sur les interfaces BGP lors des périodes creuses où une reconvergence n'influera pas sur le trafic de production.*

Onglets d'Importation et d'Exportation BGP

- Réseau > Routeur virtuel > BGP > Importation
- Réseau > Routeur virtuel > BGP > Exportation

Ajouter une nouvelle règle d'Importation ou d'Exportation pour importer ou exporter des itinéraires BGP.

© 2020 Palo Alto Networks, Inc.

Paramètres d'Importation et d'Exportation BG	Configuré dans	Description
Règles	**BGP** > **Import or Export (Importation ou exportation)** > **General (Général)**	Indiquez un nom permettant d'identifier la règle.
Activer		Sélectionnez pour activer la règle.
Utilisé par		Sélectionnez les groupes d'homologues qui vont utiliser cette règle.
Expression régulière du chemin AS	**BGP** > **Import or Export (Importation ou exportation)** > **Match (Correspondance)**	Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.
Moyen		Indiquez une valeur de Discriminateur de sorties multiples pour le filtrage d'itinéraire dans la plage de 0 à 4 294 967 295.
Table d'itinéraires		Pour une **Règle d'importation**, indiquez dans quelle table de routage les itinéraires correspondants seront importés : **unicast**, **multicast** ou **les deux**. Pour une **Règle d'importation**, indiquez à partir de quelle table de routage les itinéraires correspondants seront importés : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Indiquez des adresses IP ou des préfixes pour le filtrage des itinéraires.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour le filtrage des itinéraires
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires
Action (Action)	**BGP** > **Import or Export (Importation ou exportation)** > **Action**	Indiquez une action (**Allow (Autoriser)** ou **Deny (Refuser)**) à prendre lorsque des conditions de correspondance sont respectées.
Atténuation		Indiquez un paramètre d'atténuation, uniquement si l'action est **Allow (Autoriser)**.
Préférence locale		Indiquez une mesure de préférence locale, uniquement si l'action est **Allow (Autoriser)**.

© 2020 Palo Alto Networks, Inc.

Paramètres d'Importation et d'Exportation BG	Configuré dans	Description
Moyen		Indiquez une valeur MED, uniquement si l'action est **Allow (Autoriser)** (0 à 65 535).
Poids		Indiquez une valeur de pondération, uniquement si l'action est **Allow (Autoriser)** (0 à 65 535).
Saut suivant		Indiquez un routeur de saut suivant, uniquement si l'action est **Allow (Autoriser)**.
Origine		Indiquez le type de chemin de l'itinéraire d'origine : IGP, EGP ou incomplet, uniquement si l'action affiche **Allow (Autoriser)**.
Limite du chemin AS		Indiquez une limite du chemin AS uniquement si l'action est **Allow (Autoriser)**.
Chemin AS		Indiquez un chemin AS : **None (Aucun)**, **Remove (Supprimer)**, **Prepend (Ajouter)**, **Remove and Prepend (Supprimer et ajouter)**, uniquement si l'action affiche **Allow (Autoriser)**.
Communauté		Indiquez une option de communauté : **None (Aucun)**, **Remove All (Supprimer tout)**, **Remove Regex (Supprimer Regex)**, **Append (Ajouter)** ou **Overwrite (Écraser)**, uniquement si l'action affiche **Allow (Autoriser)**.
Communauté étendue		Indiquez une option de communauté : **None (Aucun)**, **Remove All (Supprimer tout)**, **Remove Regex (Supprimer Regex)**, **Append (Ajouter)** ou **Overwrite (Écraser)**, uniquement si l'action affiche **Allow (Autoriser)**.
		Vous devez **Delete (Supprimer)** les règles lorsque vous n'en avez plus besoin ou **Clone (Cloner)** une règle, le cas échéant. Vous pouvez également sélectionner des règles et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier leur ordre.

Onglet Avancé Publication conditionnelle BGP

- Réseau > Routeur virtuel > BGP > Publication conditionnelle

Une publication conditionnelle BGP vous permet de contrôler l'itinéraire à publier au cas où un itinéraire préféré ne serait pas disponible dans la table de routage BGP local (LocRIB) et indiquerait un échec de partage de réseau ou d'accessibilité. Ceci est utile dans les cas où vous souhaitez forcer des itinéraires vers un AS en direction d'un autre. Par exemple, lorsque vous disposez de liaisons vers Internet passant par plusieurs ISP et que vous voulez que le trafic soit acheminé vers un fournisseur à la place d'un autre, sauf s'il y a une perte de connectivité avec le fournisseur préféré.

Pour la publication conditionnelle, vous configurez un filtre Inexistant qui indique les itinéraires préférés (**Address Prefix (Préfixe d'adresse)**) plus tous les autres attributs qui identifient l'itinéraire préféré (comme l'Expression régulière du chemin AS). Si n'importe quel itinéraire correspondant à un filtre Inexistant est introuvable dans la table de routage BGP local, alors ce n'est qu'à ce moment-là que le pare-feu autorisera la

© 2020 Palo Alto Networks, Inc.

publication de l'itinéraire alternatif (l'itinéraire vers l'autre fournisseur non préféré) comme indiqué dans son filtre de Publication.

Pour configurer la publication conditionnelle, sélectionnez l'onglet **Conditional Adv (Publication conditionnelle)**, **Add (Ajouter)** une publication conditionnelle et configurez les valeurs décrites dans le tableau suivant.

Paramètres de publication conditionnelle BC	Configuré dans	Description
Politique	**BGP** > **Conditional Adv (Publication condit.)**	Indiquez un nom pour cette règle de politique de publication conditionnelle.
Activer		Sélectionnez cette option pour activer cette règle de politique de publication conditionnelle.
Utilisé par		Cliquez sur **Add (Ajouter)** les groupes d'homologues qui vont utiliser cette règle de politique de publication conditionnelle.
Filtre inexistant	**BGP** > **Conditional Adv (Publication conditionnelle)** > **Non Exist Filters (Filtres inexistants)**	Cet onglet permet de définir le(s) préfixe(s) de l'itinéraire préféré. Ceci indique l'itinéraire que vous voulez publier, s'il est disponible dans la table de routage BGP local. (Si la publication d'un préfixe est prévue et qu'il correspond à un filtre Inexistant, la publication sera supprimée.) Vous devez **Add (Ajouter)** un Filtre inexistant et indiquer un nom pour identifier celui-ci.
Activer		Sélectionnez cette option pour activer le filtre Inexistant.
Expression régulière du chemin AS		Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.
Moyen		Indiquez une valeur MED pour le filtrage des itinéraires (la plage est de 0 à 4 294 967 295).
Table d'itinéraires		Indiquez la table de routage (**unicast**, **multicast**, ou **both (les deux)**) que le pare-feu recherche pour voir s'il existe un itinéraire correspondant. C'est seulement si l'itinéraire correspondant n'existe pas dans cette table de routage que le pare-feu autorise la publication d'un autre itinéraire.

© 2020 Palo Alto Networks, Inc.

Paramètres de publication conditionnelle BG	Configuré dans	Description
Préfixe d'adresse		Il vous faut **Add (Ajouter)** le préfixe Network Layer Reachability Information (NLRI, informations d'accessibilité à la couche réseau) exact pour le ou les itinéraires préférés.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour filtrer l'itinéraire.
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires.
Filtre de publication	**BGP** > **Conditional Adv (Publication conditionnelle)** > **Advertise Filters (Filtres de publication)**	Utilisez cet onglet pour définir le(s) préfixe(s) de l'itinéraire dans la table de routage RIB locale à publier au cas où l'itinéraire du filtre Inexistant serait indisponible dans la table de routage local. Si la publication d'un préfixe doit être effectuée et qu'il ne correspond pas à un filtre Inexistant, la publication aura lieu. Vous devez **Add (Ajouter)** un filtre de publication et indiquer un nom pour identifier celui-ci.
Activer		Sélectionnez pour activer le filtre.
Expression régulière du chemin AS		Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.
Moyen		Indiquez une valeur MED pour le filtrage des itinéraires (la plage est de 0 à 4 294 967 295).
Table d'itinéraires		Indiquez la table de routage utilisée par le pare-feu lorsqu'un itinéraire correspondant doit être publié de façon conditionnelle : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Cliquez sur **Add (Ajouter)** le préfixe Network Layer Reachability Information (NLRI, informations d'accessibilité à la couche réseau) exact de l'itinéraire à publier si l'itinéraire préféré est indisponible.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour le filtrage des itinéraires.

© 2020 Palo Alto Networks, Inc.

Paramètres de publication conditionnelle BG	Configuré dans	Description
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires.

Onglet Agrégation BGP

- Réseau > Routeur virtuel > BGP > Agrégation

L'agrégation d'itinéraires consiste à combiner des itinéraires spécifiques (ceux avec une longueur de préfixe plus longue) en un seul itinéraire (avec une longueur de préfixe plus courte) pour réduire les publications d'itinéraires que le pare-feu doit envoyer et avoir moins d'itinéraires dans la table de routage.

Paramètres d'agrégation BGP	Configuré dans	Description
Name (Nom)	**BGP > Aggregate (Agréger)**	Saisissez un nom pour la règle d'agrégation.
Préfixe		Saisissez un préfixe récapitulatif (adresse IP / longueur de préfixe) qui sera utilisé pour agréger les préfixes plus longs.
Activer		Sélectionnez cette option pour activer cette agrégation d'itinéraires.
Résumé		Sélectionnez cette option pour récapituler les itinéraires.
Définition AS		Sélectionnez cette option pour que le pare-feu, pour cette règle d'agrégation, inclue l'ensemble des numéros AS (ensemble AS) dans le chemin AS de l'itinéraire agrégé. L'ensemble AS est la liste non triée des numéros AS d'origine provenant des itinéraires individuels qui sont agrégés.
Name (Nom)	**BGP > Aggregate (Agrégation) > Suppress Filters (Filtres de suppression)**	Définissez les attributs qui entraîneront la suppression des itinéraires correspondants. Cliquez sur **Add (Ajouter)** et saisissez un nom pour un Filtre de suppression.
Activer		Sélectionnez cette option pour activer les Filtres de suppression.
Expression régulière du chemin AS		Indiquez une expression régulière pour que l'attribut AS_PATH filtre les itinéraires qui seront agrégés, par exemple, ^5000 suppose les itinéraires tirés de l'AS 5000.
Expression régulière de la communauté		Indiquez une expression régulière pour que les communautés filtrent les itinéraires qui seront agrégés, par exemple, 500:.* correspond aux communautés avec 500:x.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour les communautés étendues afin de filtrer les itinéraires qui seront agrégés.

© 2020 Palo Alto Networks, Inc.

Paramètres d'agrégation BGP	Configuré dans	Description
Moyen		Indiquez le MED qui filtre les itinéraires qui seront agrégés.
Table d'itinéraires		Indiquez la table de routage à utiliser pour les itinéraires agrégés qui doivent être supprimés (non publiés) : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Saisissez l'adresse IP que vous souhaitez supprimer de la publication.
Saut suivant		Saisissez l'adresse du saut suivant du préfixe BGP que vous souhaitez supprimer.
De l'homologue		Saisissez l'adresse IP de l'homologue duquel le préfixe BGP (que vous souhaitez supprimer) a été reçu.
Name (Nom)	**BGP** > **Aggregate (Agrégation)** > **Advertise Filters (Filtres de publication)**	Définissez les attributs d'un Filtre de publication qui amène le pare-feu à annoncer aux homologues tout itinéraire qui correspond au filtre. Cliquez sur **Add (Ajouter)** et saisissez un nom pour le Filtre de publication.
Activer		Sélectionnez cette option pour activer ce Filtre de publication.
Expression régulière du chemin AS		Indiquez une expression régulière pour que AS_PATH filtre les itinéraires qui seront publiés.
Expression régulière de la communauté		Indiquez une expression régulière pour que la Communauté filtre les itinéraires qui seront publiés.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour que la Communauté étendue filtre les itinéraires qui seront publiés.
Moyen		Indiquez une valeur MED pour filtrer les itinéraires qui seront publiés.
Table d'itinéraires		Indiquez la table de routage à utiliser pour un Filtre de publication des itinéraires agrégés : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Saisissez une adresse IP que vous souhaitez que BGP publie.
Saut suivant		Saisissez l'adresse du Saut suivant de l'adresse IP que vous souhaitez que BGP publie.
De l'homologue		Saisissez l'adresse IP de l'homologue duquel le préfixe a été reçu et que vous souhaitez que BGP publie.
	BGP > **Aggregate**	Définissez les attributs de l'itinéraire agrégé.

© 2020 Palo Alto Networks, Inc.

Paramètres d'agrégation BGP	Configuré dans	Description
Préférence locale	**(Agrégation) > Aggregate Route Attributes (Attributs des itinéraires agrégés)**	Préférence locale dans la plage 0 à 4 294 967 295.
Moyen		Discriminateur de sorties multiples dans la plage 0 à 4 294 967 295.
Poids		Poids dans la plage 0 à 65 535.
Saut suivant		Adresse IP du saut suivant.
Origine		Origine de l'itinéraire : **igp**, **egp** ou **incomplete (incomplet)**.
Limite du chemin AS		Limite du chemin AS dans la plage 1 à 255.
Chemin AS		Sélectionnez le type : **Aucun** ou **Ajouter**.
Communauté		Sélectionnez le type : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**.
Communauté étendue		Sélectionnez le type : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**.

Onglet Règles de redistribution BGP

- Réseau > Routeur virtuel > BGP > Règles de redistribution

Configuration des paramètres décrits dans le tableau suivant pour créer des règles pour la redistribution des itinéraires BGP.

Paramètres des règles de redistribution BG	Configuré dans	Description
Autoriser la redistribution des itinéraires par défaut	**BGP > Redist Rules (Règles de redistribution)**	Autorise le pare-feu à redistribuer son itinéraire par défaut vers des homologues BGP.
Name (Nom)		Vous devez **Ajouter** un sous-réseau IP ou d'abord créer une règle de redistribution.
Activer		Sélectionnez cette option pour activer cette règle de redistribution.
Table d'itinéraires		Indiquez la table de routage sur laquelle l'itinéraire sera redistribué : **unicast**, **multicast** ou **les deux**.
Mesure		Saisissez une mesure dans la plage comprise entre 1 et 65 535.

© 2020 Palo Alto Networks, Inc.

Paramètres des règles de redistribution BG	Configuré dans	Description
Définir l'origine		Sélectionnez l'origine de l'itinéraire redistribué (**igp**, **egp** ou **incomplet**). La valeur « **incomplet** » indique un itinéraire connecté.
Définir MED		Saisissez un MED pour l'itinéraire redistribué dans la plage comprise entre 0 et 4 294 967 295.
Définir les préférences locales		Saisissez une préférence locale pour l'itinéraire redistribué dans la plage comprise entre 0 et 4 294 967 295.
Définir la limite de chemin de l'AS		Saisissez une limite du chemin AS pour l'itinéraire redistribué dans la plage comprise entre 1 et 255.
Définir la community		Sélectionnez ou saisissez une valeur 32 bits au format décimal, hexadécimal ou AS:VAL ; où AS et VAL sont tous deux dans la plage de 0 à 65 535. Saisissez un maximum de 10 communautés.
Définir une community élargie		Saisissez une valeur de 64 bits au format hexadécimal ou au format TYPE:AS:VAL ou au format TYPE:IP:VAL. TYPE est de 16 bits, AS ou IP sont de 16 bits et VAL est de 32 bits. Saisissez un maximum de cinq communautés étendues.

Multidiffusion IP

- Réseau > Routeur virtuel > Multicast

La définition des protocoles multicast nécessite la configuration du paramètre standard suivant :

Paramètre multicast	Description
Activer	Sélectionnez pour activer le routage multicast.

Les paramètres des onglets suivants doivent également être configurés'A0;:

- **Rendezvous Point (Point de rendez-vous)** : Voir l'Onglet Point de rendez-vous de Multicast.
- **Interfaces** : Voir Onglet Interfaces multicast.
- **SPT Threshold (Seuil SPT)** : Voir l'Onglet Seuil SPT de Multicast.
- **Source Specific Address Space (Espace d'adresses spécifique à la source)** : Voir l'Onglet Espace d'adresses spécifiques à la source de Multicast.
- **Advanced (Avancé)** : Voir Onglet avancé multicast.

Onglet Point de rendez-vous multicast

- Réseau > Routeur virtuel > Multicast > Point de rendez-vous

Utilisez les champs suivants pour configurer un point de rendez-vous IP multicast :

© 2020 Palo Alto Networks, Inc.

Paramètres multicast – Point de rendez-vous	Description
Type RP	Sélectionnez le type de point de rendez-vous (RP) qui va s'exécuter sur ce routeur virtuel. Un RP statique doit être explicitement configuré sur d'autres routeurs PIM, alors qu'un RP candidat est automatiquement élu. • **None (Aucun)** - Indiquez si aucun RP n'est en cours d'exécution sur ce routeur virtuel. • **Static (Statique)** - Indiquez une adresse IP statique pour le RP et sélectionnez des options pour **RP Interface (Interface du RP)** et **RP Address (Adresse du RP)** dans la liste déroulante. Sélectionnez **Override learned RP for the same group (Appliquer un contrôle prioritaire RP appris pour le même groupe)** si vous voulez utiliser le RP défini au lieu du RP élu pour ce groupe. • **Candidate (Candidat)** - Indiquez les informations suivantes pour le RP candidat en cours d'exécution sur ce routeur virtuel : • **RP Interface (Interface du RP)** - Sélectionnez une interface pour le RP. Les types d'interfaces valides incluent une interface en boucle, C3, VLAN, Ethernet agrégée et de tunnel. • **RP Address (Adresse du RP)** - Sélectionnez une adresse IP pour le RP. • **Priority (Priorité)** - Indiquez une priorité pour les messages RP candidats (valeur par défaut : 192). • **Advertisement interval (Intervalle de publication)** - Indiquez un intervalle entre les publications de messages RP candidats. • **Group list (Liste de groupes)** - Si vous sélectionnez **Static (Statique)** ou **Candidate (Candidat)**, cliquez sur **Add (Ajouter)** pour spécifier une liste de groupes pour lesquels ce RP candidat propose d'être le RP.
Rendezvous Point distant	Cliquez sur **Add (Ajouter)** et indiquez les éléments suivants : • **IP address (Adresse IP)** - Indiquez une adresse IP pour le RP. • **Override learned RP for the same group (Écraser le RP appris pour le même groupe)** - Sélectionnez pour utiliser le RP défini au lieu du RP élu pour ce groupe. • **Group (Groupe)** - Indiquez une liste de groupes pour lesquels l'adresse spécifiée va servir de RP.

Onglet Interfaces multicast

- Réseau > Routeur virtuel > Multicast > Interfaces

Utilisez les champs suivants pour configurer les interfaces multicas qui partagent les paramètres IGMP, PIM et d'autorisation du groupe :

Paramètres multicast – Interfaces	Description
Name (Nom)	Saisissez un nom pour identifier un groupe d'interfaces.
Description	Saisissez une description (facultatif).

© 2020 Palo Alto Networks, Inc.

Paramètres multicast – Interfaces	Description
Interface	**Add (Ajoutez)** une ou plusieurs interfaces de pare-feu qui appartiennent au groupe d'interfaces et, par conséquence, qui partagent les paramètres d'autorisation du groupe, les paramètres IGMP et les paramètres PIM.
Autorisations du groupe	Précisez les groupes multicast qui participent à PIM Any-Source Multicast (n'importe quelle source multicast ; ASM) ou à PIM Source-Specific Multicast (multicast spécifique à la source ; SSM) : • **Any Source (N'importe quelle source)** : **Add (Ajoutez)** un **Name (Nom)** pour identifier un **Group (Groupe)** multicast autorisé à recevoir du trafic multicast de n'importe quelle source qui se trouve sur les interfaces faisant partie du groupe d'interfaces. Le groupe est **Included (Inclus)** par défaut dans la liste **Any Source (N'importe quelle source)**. Désélectionnez **Included (Inclus)** pour facilement exclure un groupe sans en supprimer la configuration. • **Source Specific (Spécifique à la source)** : **Add (Ajoutez)** un **Name (Nom)** pour un **Group (Groupe)** multicast et une paire d'adresses IP **Source** pour laquelle le trafic multicast est autorisé sur les interfaces faisant partie du groupe d'interfaces. Le Groupe et la Paire source sont **Included (Inclus)** par défaut dans la liste Source Specific (Spécifique à la source). Désélectionnez **Included(Inclus)** pour facilement exclure un groupe et une paire Source sans en supprimer la configuration.
IGMP	Indiquez les paramètres du trafic IGMP. IGMP doit être activé pour les interfaces orientées vers le récepteur multicast. • **Enable (Activer)** - Sélectionnez pour activer la configuration IGMP. • **IGMP Version (Version IGMP)** - Sélectionnez la version 1, 2 ou 3 à exécuter sur l'interface. • **Enforce Router-Alert IP Option (Appliquer l'option IP d'alerte du routeur)** - Sélectionnez pour exiger l'utilisation de l'option IP d'alerte du routeur avec IGMPv2 ou IGMPv3. Cette option doit être désactivée pour être compatible avec IGMPv1. • **Robustness (Robustesse)** - Sélectionnez un entier pour indiquer la perte de paquets sur un réseau (intervalle compris entre 1 et 7, valeur par défaut : 2). Si la perte de paquets est chose courante, sélectionnez une valeur supérieure. • **Max Sources (Sources max.)** - Indiquez le nombre maximum d'appartenances propres à la source autorisées sur ce groupe d'interfaces (intervalle compris entre 1 et 65 535 ou **unlimited (illimitées)**). • **Max Groups (Groupes max.)** - Indiquez le nombre maximum de groupes multicast autorisées sur ce groupe d'interfaces (intervalle compris entre 1 et 65 535 ou **unlimited (illimités)**). • **Query Configuration (Configuration d'une requête)** - Spécifiez les options suivantes : • **Query Interval (Intervalle de requête)** - Indiquez l'intervalle au cours duquel des requêtes générales sont envoyées à tous les récepteurs. • **Max Query Response Time (Délai max. de réponse aux requêtes)** - Indiquez le délai maximum écoulé entre une requête générale et la réponse d'un récepteur.

© 2020 Palo Alto Networks, Inc.

Paramètres multicast – Interfaces	Description
	• **Last Member Query Interval (Dernier intervalle de requête d'un membre)** - Indiquez l'intervalle entre les messages de requête d'un groupe ou spécifiques à la source (y compris ceux envoyés en réponse à des messages d'abandon de groupe). • **Immediate Leave (Quitter immédiatement)** - Sélectionnez pour quitter le groupe immédiatement lors de la réception d'un message d'abandon.
Configuration PIM	Définissez les paramètres Protocol Independent Multicast (protocole de routage multicast ; PIM) : • **Enable (Activer)** - Sélectionnez pour autoriser cette interface à recevoir et/ou à transférer des messages PIM. Vous devez procéder à l'activation pour qu'une interface transfère le trafic multicast. • **Assert Interval (Intervalle d'affirmation)** - Indiquez l'intervalle entre les messages d'affirmation PIM pour choisir un transmetteur PIM. • **Hello Interval (Intervalle Hello)** - Indiquez l'intervalle entre les messages Hello PIM. • **Join Prune Interval (Intervalle Join/Prune)** - Indiquez le nombre de secondes entre les messages de jointure (Join) PIM (et entre les messages d'élagage (Prune) PIM). La valeur par défaut est 60. • **DR Priority (Priorité du DR)** - Indiquez la priorité du routeur désigné pour cette interface. • **BSR Border (Bordure BSR)** - Sélectionnez pour utiliser l'interface en tant que bordure bootstrap. • **PIM Neighbors (Voisins PIM)** - **Add (Ajoutez)** la liste de voisins qui vont communiquer entre eux à l'aide de PIM.

Onglet Seuil SPT multicast

- Réseau > Routeur virtuel > Multicast > Seuil'A0;SPT

Le seuil Shortest Path Tree (arbre du chemin le plus court ; SPT) définit le moment où le routeur virtuel fait basculer le routage multicast d'un préfixe ou d'un groupe multicast d'une distribution en arborescence partagée (issue du point de rendez-vous) à une distribution en arborescence source également connue sous le nom de Shortest Path Tree (arbre du chemin le plus court ; SPT). **Add (Ajoutez)** un seuil SPT à un préfixe ou un groupe multicast.

Seuil SPT	Description
Préfixe/groupe multicast	Indiquez le préfixe ou le groupe multicast pour lequel le routage multicast bascule à une distribution SPT lorsque le débit vers le groupe ou le préfixe atteint le seuil défini.
Seuil (en Kbit/s)	Sélectionnez un paramètre pour définir le moment où le routage multicast bascule à une distribution SPT pour le préfixe ou le groupe multicast correspondant : • **0 (commuter au premier paquet de données)** : (par défaut) Lorsqu'un paquet multicast destiné au groupe ou au préfixe arrive, le routeur virtuel fait basculer le routage à une distribution SPT.

© 2020 Palo Alto Networks, Inc.

Seuil SPT	Description
	• **jamais (ne pas basculer vers SPT)** : le routeur virtuel continue de transférer le trafic multicast à ce groupe ou à ce préfixe via l'arbre partagé. • Saisissez le nombre total de kilobits provenant des paquets multicast qui peuvent arriver pour le préfixe ou le groupe multicast correspondant à toute interface sur une période de temps déterminée (plage comprise entre 1 et 4 294 967 295). Lorsque le débit atteint ce chiffre, le routeur virtuel passe à la distribution SPT.

Onglet Espace d'adresses spécifique à la source multicast

- Réseau > Routeur virtuel > Multicast > Espace d'adresses spécifique à la source

Add (Ajoutez) les groupes multicast qui peuvent recevoir des paquets multicast d'une source donnée uniquement. Il s'agit des mêmes noms et groupes multicast que vous avez indiqués comme Spécifique à la source à l'onglet **Multicast** > **Interfaces** > **Group Permissions (Permissions du groupe)**.

Paramètres multicast – Espace d'adresses spécifique à la source	Description
Name (Nom)	Identifiez un groupe multicast auquel le pare-feu va fournir des services Source-Specific Multicast (multicast spécifique à la source ; SSM).
Group (Groupe)	Définissez une adresse de groupe multicast qui peut accepter les paquets multicast d'une source donnée uniquement.
inclus(e)	Sélectionnez cette option pour inclure les groupes multicast dans l'espace d'adresses SSM.

Onglet Avancé multicast

- Réseau > Routeur virtuel > Multicast > Avancé

Configurez la durée pendant laquelle un itinéraire de multidiffusion reste dans la table de routage après la fin de la session.

Paramètres avancés multicast	Description
Paramètres d'expiration de l'itinéraire (sec)	Vous permet d'ajuster le délai, en secondes, pendant lequel une route multidiffusion demeure dans la table de routage sur le pare-feu à la fin de la session (intervalle compris entre 210 et 2 700 ; valeur par défaut : 210).

ECMP

- Réseau > Routeur virtuel > Paramètres de routeur > ECMP

Le traitement ECMP (Equal Cost Multiple Path/chemin multiple à coût égal) est une fonction réseau qui permet au pare-feu d'utiliser jusqu'à quatre itinéraires de coût égal vers la même destination. Sans cette

© 2020 Palo Alto Networks, Inc.

fonction, s'il existe plusieurs itinéraires de coût égal vers la même destination, le routeur virtuel choisit l'un de ces itinéraires dans la table de routage et l'ajoute à sa table de transfert ; il n'utilise aucun autre itinéraire à moins qu'il n'y ait une interruption dans l'itinéraire choisi. L'activation de la fonctionnalité ECMP sur un routeur virtuel permet au pare-feu d'avoir jusqu'à quatre chemins de coût égal vers une destination dans sa table de transfert, grâce auxquels il peut :

- Équilibrer la charge des flux (sessions) vers la même destination sur plusieurs liaisons de coût égal.
- Utiliser la bande passante disponible sur toutes les liaisons vers la même destination plutôt que de laisser certains liens inutilisés.
- Déplacer le trafic de façon dynamique d'un autre membre ECMP vers la même destination en cas de défaillance d'une liaison, au lieu d'attendre que le protocole de routage ou la table RIB choisisse un autre chemin, ce qui peut aider à réduire le délai d'inactivité en cas de défaillance de la liaison.

L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu choisit ainsi un chemin de coût égal au début d'une nouvelle session et non à chaque fois que le pare-feu reçoit un paquet.

L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le pare-feu, ce qui peut mettre fin aux sessions existantes.

Afin de configurer ECMP pour un routeur virtuel, sélectionnez un routeur virtuel et, dans **Paramètres de routeur**, cliquez sur l'onglet **ECMP** et configurez les Paramètres ECMP suivants :

Que voulez-vous faire ?	Reportez-vous à la section :
Quels sont les champs disponibles pour configurer ECMP ?	Paramètres ECMP
Vous souhaitez en savoir plus ?	ECMP

Paramètres ECMP

- Réseau > Routeur virtuel > Paramètres de routeur > ECMP

Utilisez les champs suivants pour configurer les paramètres de Chemin multiple à coût égal.

Paramètres ECMP	Description
Activer	**Activez** ECMP. *L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le pare-feu, ce qui peut mettre fin aux sessions existantes.*
Retour symétrique	(Facultatif) Sélectionnez l'option **Symmetric Return (Retour symétrique)** pour que les paquets de retour sortent de la même interface que celle sur laquelle les paquets d'entrée associés sont arrivés. Autrement dit, le pare-feu utilisera l'interface d'entrée sur laquelle envoyer des paquets de retour, au lieu de l'interface ECMP. Ainsi, le paramètre **Symmetric Return (Retour symétrique)** applique un contrôle prioritaire sur l'équilibrage de la charge. Ce

© 2020 Palo Alto Networks, Inc.

Paramètres ECMP	Description
	comportement se produit uniquement pour les flux de trafic du serveur au client.
Nombre max. de chemins	Sélectionnez le nombre maximum de chemins de coût égal : (2, 3 ou 4) vers un réseau de destination qui peut être copié de la RIB à la FIB. La valeur par défaut est 2.
Méthode	Choisissez l'un des algorithmes d'équilibrage de la charge ECMP suivants à utiliser sur le routeur virtuel. L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu (ECMP) choisit ainsi un chemin de coût égal au début d'une nouvelle session et non à chaque fois qu'un paquet est reçu. • **IP Modulo (Modulo IP)**- Par défaut, le routeur virtuel équilibre la charge des sessions à l'aide de cette option, qui utilise un hachage des adresses IP source et de destination dans l'en-tête des paquets pour déterminer l'itinéraire ECMP à utiliser. • **IP Hash (Hachage IP)** : il existe deux méthodes de hachage IP qui déterminent quel itinéraire ECMP il convient d'utiliser : • Si vous sélectionnez **IP Hash (Hachage IP)**, par défaut, le pare-feu utilise un hachage des adresses IP source et de destination. • Vous pouvez également sélectionner **Use Source Address Only (Utiliser l'adresse source uniquement)** (disponible dans PAN-OS 8.0.3 et dans les versions ultérieures). Cette méthode de hachage IP garantit que toutes les sessions appartenant à la même adresse IP source prennent toujours le même chemin. • Vous pouvez éventuellement sélectionner **Use Source/Destination Ports (Utiliser les ports source/de destination)** pour inclure les ports dans l'un ou l'autre des calculs du hachage. Vous pouvez également saisir une **Hash Seed (Valeur initiale de hachage)** (un nombre entier) pour randomiser l'équilibrage de la charge. • **Weighted Round Robin (Pondération comparative)** - Cet algorithme peut être utilisé pour prendre en compte les différentes capacités et vitesses de liaison. Lorsque vous choisissez cet algorithme, la fenêtre Interface s'ouvre. Cliquez sur **Add (Ajouter)** et sélectionnez une **Interface** à inclure dans le groupe Pondération comparative. Saisissez la valeur **Weight (Pondération)** à utiliser pour cette interface. La valeur de **Weight (Pondération)** est de 100 par défaut et l'intervalle est de 1-255. Plus la valeur de pondération d'un chemin de coût égal spécifique est élevée, plus ce chemin sera sélectionné pour une nouvelle session. Une liaison plus rapide doit avoir une pondération supérieure à une liaison plus lente, de manière à ce que le trafic ECMP passe par la liaison plus rapide. Cliquez à nouveau sur **Add (Ajouter)** pour ajouter une autre interface et une autre pondération. • **Balanced Round Robin (Équilibrage comparatif)** - Distribue les sessions ECMP entrantes de manière égale entre les liaisons.

Statistiques d'exécution supplémentaires d'un routeur virtuel

Après avoir configuré des itinéraires statiques ou des protocoles de routage pour un routeur virtuel, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez **More Runtime**

© 2020 Palo Alto Networks, Inc.

Stats (Statistiques d'exécution supplémentaires) dans la dernière colonne pour afficher des informations détaillées sur le routeur virtuel, comme la table de routage, la table de transfert et les protocoles de routage et les itinéraires statiques que vous avez configurés. Ces fenêtres fournissent plus d'informations que ne peut en contenir un écran unique pour le routeur virtuel. La fenêtre affiche les onglets suivants :

- **Routing (Routage)** : voir Onglet Routage.
- **RIP** : voir Onglet RIP.
- **BGP** : voir Onglet BGP.
- **Multicast** : voir Onglet Multicast.
- **BFD Summary Information (Informations récapitulatives de BFP)** : voir Onglet Informations récapitulatives de BFD.

Onglet Routage

Le tableau suivant décrit les statistiques d'exécution du routeur virtuel pour la Table de routage, la Table de transfert, et la table de Surveillance des itinéraires statiques.

Statistiques d'exécution	Description
Table d'itinéraires	
Table d'itinéraires	Sélectionnez **Unicast** ou **Multicast** pour afficher la table de routage unicast ou multicast.
Afficher la famille d'adresses	Sélectionnez **IPv4 uniquement**, **IPv6 uniquement**, ou **IPv4 et IPv6** (par défaut) pour contrôler quel groupe d'adresses afficher dans le tableau.
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur virtuel peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
Mesure	Mesure de l'itinéraire. Lorsqu'un protocole de routage comporte plus d'une route vers le même réseau de destination, il privilégie l'itinéraire avec la valeur métrique la plus basse. Chaque protocole de routage utilise un autre type de métrique, par exemple, RIP utilise le nombre de sauts.
Poids	Poids de l'itinéraire. Par exemple, lorsque BGP comporte plus d'un itinéraire vers la même destination, il préfèrera l'itinéraire avec le poids le plus élevé.
flags	• **A?B** – Actif et appris via BGP. • **A C** – Actif et résultat d'une interface interne (connectée) – Destination = réseau • **A H** – Actif et résultat d'une interface interne (connectée) – Destination = Hôte uniquement • **A R** – Actif et appris via RIP. • **A S** – Actif et statique. • **S** – Inactif (car cet itinéraire a une mesure supérieure) et statique • **O1**–OSPF externe de type 1 • **O2**–OSPF externe de type 2 • **Oi**–OSPF intra-zone

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution	Description
	• **Oo**–OSPF inter-zone
Age	Antériorité de l'entrée d'itinéraire dans la table de routage. Les itinéraires statiques n'ont aucune antériorité.
Interface	L'interface de sortie du routeur virtuel qui sera utilisée pour atteindre le saut suivant.
Actualiser	Cliquez pour actualiser les statistiques d'exécution dans le tableau.
Table de transfert	
 *Le pare-feu choisit le meilleur itinéraire (de la table de routage (RIB) vers un réseau de destination) à placer dans la FIB.*	
Afficher la famille d'adresses	Sélectionnez **IPv4 uniquement**, **IPv6 uniquement**, ou **IPv4 et IPv6** (par défaut) pour contrôler la table de routage à afficher.
Destination	Meilleure adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur virtuel peut atteindre, sélectionné depuis la Table de routage.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
flags	• **u** – L'itinéraire se dirige vers le haut. • **h** – L'itinéraire dirige vers un hôte. • **g** – L'itinéraire dirige vers une passerelle. • **e** – Le pare-feu a sélectionné cet itinéraire en utilisant le Chemin multiple à coût égal (ECMP). • * – L'itinéraire est le chemin privilégié vers un réseau de destination.
Interface	Interface de sortie du routeur virtuel qui sera utilisé pour atteindre le saut suivant.
MTU	Unité de transmission maximale (MTU) ; le nombre maximum d'octets que le pare-feu transmettra dans un seul paquet TCP vers cette destination.
Actualiser	Cliquez pour actualiser les statistiques d'exécution dans le tableau.
Surveillance des itinéraires statiques	
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe d'un réseau que le routeur virtuel peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution	Description
Mesure	Mesure de l'itinéraire. Lorsqu'il y a plus d'un itinéraire statique sur le même réseau de destination, le pare-feu favorise l'itinéraire avec la valeur métrique la plus basse.
Poids	Poids de l'itinéraire.
flags	• **A?B** – Actif et appris via BGP. • **A C** – Actif et résultat d'une interface interne (connectée) – Destination = réseau • **A H** – Actif et résultat d'une interface interne (connectée) – Destination = Hôte uniquement • **A R** – Actif et appris via RIP. • **A S** – Actif et statique. • **S** – Inactif (car cet itinéraire a une mesure supérieure) et statique • **O1**–OSPF externe de type 1 • **O2**–OSPF externe de type 2 • **Oi**–OSPF intra-zone • **Oo**–OSPF inter-zone
Interface	L'interface de sortie du routeur virtuel qui sera utilisée pour atteindre le saut suivant.
Surveillance des chemins (échec)	Si la surveillance des chemins est activée pour cet itinéraire statique, l'Échec indique : • **Tout** – Le pare-feu considère l'itinéraire statique vers le bas et échoue si toutes les destinations surveillées pour l'itinéraire statique sont en panne. • **Un** – Le pare-feu considère l'itinéraire statique vers le bas et échoue si l'une des destinations surveillées pour l'itinéraire statique est en panne. Si la surveillance des chemins d'itinéraires statiques est désactivée, l'Échec indique **Désactivé**.
Status (État)	Le statut de l'itinéraire statique basé sur les requêtes pings ICMP vers les destinations surveillées : **Haut**, **Bas**, ou la surveillance des chemins pour l'itinéraire statique est **Désactivé**.
Actualiser	Actualise les statistiques d'exécution dans le tableau.

Onglet RIP

Le tableau suivant décrit les statistiques d'exécution RIP du routeur virtuel.

Statistiques d'exécution RIP	Description
Onglet Récapitulation	

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution RIP	Description
Intervalle (en secondes)	Nombre de secondes dans un intervalle. RIP utilise cette valeur (une période de temps) pour contrôler ses intervalles de Mise à jour, d'Expiration et de Suppression.
Intervalles de mise à jour	Nombre d'intervalles entre les mises à jour de publication des itinéraires RIP que le routeur virtuel envoie aux homologues.
Intervalles d'expiration	Nombre d'intervalles depuis la dernière mise à jour du routeur virtuel reçue d'un homologue, après lequel le routeur virtuel marque les itinéraires de l'homologue comme inutilisables.
Intervalles de suppression	Nombre d'intervalles depuis le marquage d'un itinéraire comme inutilisable après lequel, si aucune mise à jour n'est reçue, le pare-feu supprime l'itinéraire de la table de routage.
Onglet Interface	
Adresse	Adresse IP d'une interface sur le routeur virtuel où RIP est activé.
Type d'authentification	Type d'authentification : mot de passe simple, MD5 ou aucun.
Envoi autorisé	Une coche indique que cette interface est autorisée à envoyer des paquets RIP.
Réception autorisée	Une coche indique que cette interface est autorisée à recevoir des paquets RIP.
Publier la route par défaut	Une coche indique que RIP publiera son itinéraire par défaut sur ses homologues.
Mesure d'itinéraire par défaut	Mesure (nombre de sauts) affectée à l'itinéraire par défaut. Plus la valeur de mesure est faible, plus l'itinéraire a de chance dans la table de routage d'être sélectionné comme chemin préféré.
ID de la clé	Clé d'authentification utilisée par les homologues.
Préféré	Clé préférée pour l'authentification.
Onglet Homologue	
Adresse de l'homologue	Adresse IP d'un homologue sur l'interface RIP du routeur virtuel.
Dernière mise à jour	Date et heure auxquelles la dernière mise à jour a été reçue de cet homologue.
Version RIP	Version RIP exécutée par l'homologue.
Paquets non valides	Nombre de paquets non valides reçus de cet homologue. Raisons possibles pour lesquelles le pare-feu ne peut pas analyser le paquet RIP : x octets au-delà de la limite d'itinéraire, trop d'itinéraires dans un paquets, sous-réseau incorrect, adresse non conforme, échec de l'authentification ou mémoire insuffisante.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution RIP	Description
Itinéraires non valides	Nombre d'itinéraires non valides reçus de cet homologue. Causes possibles : itinéraire non valide, échec de l'importation ou mémoire insuffisante.

Onglet BGP

Le tableau suivant décrit les statistiques d'exécution BGP du routeur virtuel.

Statistiques d'exécution BGP	Description
Onglet Récapitulation	
ID de routeur	ID de routeur affecté à l'instance BGP.
Rejeter les itinéraires par défaut	Indique si l'option Rejeter l'itinéraire par défaut est configurée, qui permet au routeur virtuel d'ignorer les itinéraires par défaut publiés par les homologues BGP.
Redistribuer l'itinéraire par défaut	Indique si l'option Autoriser la redistribution de l'itinéraire par défaut est configurée.
Installer un itinéraire	Indique si l'option Installer l'itinéraire est configurée, qui permet au routeur virtuel d'installer des itinéraires BGP dans la table de routage générale.
Redémarrage sans échec	Indique si l'option Redémarrage en douceur est activée (prise en charge).
Taille AS	Indique si le format AS sélectionné est de 2 ou 4 octets.
AS local	Numéro de l'AS auquel le routeur virtuel appartient.
AS membre local	Numéro de l'AS membre local (valide uniquement si le routeur virtuel se trouve dans une confédération). La valeur du champ est de 0 si le routeur virtuel n'est pas dans une confédération.
ID du cluster	Affiche l'ID du cluster de réflecteurs configuré.
Préférence locale par défaut	Affiche la préférence locale par défaut configurée pour le routeur virtuel.
Toujours comparer MED	Indique si l'option Toujours comparer MED est configurée, qui permet une comparaison afin de sélectionner un itinéraire parmi ceux des voisins dans différents systèmes autonomes.
Agréger sans tenir compte de MED	Indique si l'option Agréger MED est configurée, qui permet l'agrégation des itinéraires même lorsqu'ils ont différentes valeurs MED.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution BGP	Description
Traitement MED déterministe	Indique si l'option Comparaison MED déterministe est configurée, qui permet une comparaison afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues IBGP (homologues BGP figurant dans le même AS).
Entrées RIB actives	Nombre d'entrées de la table RIB Out.
Pic des entrées RIB Out	Nombre maximal d'itinéraires Adj-RIB-Out qui ont été affectés à un moment donné.
Onglet Homologue	
Name (Nom)	Nom de l'homologue.
Group (Groupe)	Nom du groupe d'homologues auquel cet homologue appartient.
IP locale	Adresse IP de l'interface BGP sur le routeur virtuel.
Adresse IP de l'homologue	Adresse IP de l'homologue.
AS Homologue	Système autonome auquel l'homologue appartient.
Mot de passe défini	Oui ou Non indique si l'authentification est définie.
Status (État)	État de l'homologue (par exemple, Actif, Connexion, Établie, Inactif, OpenConfirm ou OpenSent).
Durée de l'état (sec)	Durée de l'état de l'homologue.
Onglet Groupe d'homologues	
Nom du groupe	Nom du groupe d'homologues.
Type	Type de groupe d'homologues configuré, tel que EBGP ou IBGP.
Agréger AS conféd. AS	Oui ou Non indique si l'option Agréger l'AS de la confédération est configurée.
Prise en charge de la réinitialisation logicielle	Oui ou Non indique si le groupe d'homologues prend en charge la réinitialisation logicielle. Lorsque les politiques de routage vers un homologue BGP sont modifiées, les mises à jour des tables de routage peuvent être affectées. Une réinitialisation logicielle est préférée plutôt qu'une réinitialisation matérielle, car elle permet la mise à jour des tables de routage sans effacer les sessions BGP.
Saut auto. suivant	Oui ou Non indique si cette option est configurée.
Tiers du saut suivant	Oui ou Non indique si cette option est configurée.
Supprimer l'AS privé	Indique si les numéros des AS privés seront supprimés de l'attribut AS_PATH dans les mises à jour avant leur envoi.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution BGP	Description
Onglet RIB locale	
Préfixe	Préfixe réseau et masque de sous-réseau dans la RIB locale.
Indicateur	* indique l'itinéraire choisi comme meilleur itinéraire BGP.
Saut suivant	Adresse IP du saut suivant vers le préfixe.
Homologue	Nom de l'homologue.
Poids	Attribut de pondération affecté au préfixe. Si le pare-feu dispose de plusieurs itinéraires vers le même préfixe, l'itinéraire dont la valeur de pondération est la plus élevée est installé dans la table de routage IP.
Préf. locale	Attribut de préférence locale de l'itinéraire, qui est utilisé pour choisir le point de sortie vers le préfixe s'il existe plusieurs points de sortie. Une préférence locale élevée est préférée à une préférence locale faible.
Chemin AS	Liste des systèmes autonomes dans le chemin vers le réseau du préfixe ; la liste est publiée dans les mises à jour BGP.
Origine	Attribut d'origine du préfixe ; comment BGP a appris l'itinéraire.
Moyen	Attribut MED (Multi-Exit Discriminator/discriminateur de sorties multiples) de l'itinéraire. Le MED est un attribut de mesure d'un itinéraire, que l'AS publiant l'itinéraire suggère à un AS externe. Un MED faible est préféré à un MED élevé.
Nombre de battements	Nombre de battements de l'itinéraire.
Onglet RIB Out	
Préfixe	Entrée de routage réseau dans la RIB.
Saut suivant	Adresse IP du saut suivant vers le préfixe.
Homologue	Homologue sur lequel le routeur virtuel publiera cet itinéraire.
Préf. locale	Attribut de préférence locale pour accéder au préfixe, qui est utilisé pour choisir le point de sortie vers le préfixe s'il existe plusieurs points de sortie. Une préférence locale élevée est préférée à une préférence locale faible.
Chemin AS	Liste des systèmes autonomes dans le chemin vers le réseau du préfixe ; la liste est publiée dans les mises à jour BGP.
Origine	Attribut d'origine du préfixe ; comment BGP a appris l'itinéraire.
Moyen	Attribut MED (Multi-Exit Discriminator/discriminateur de sorties multiples) vers le préfixe. Le MED est un attribut de mesure d'un itinéraire que l'AS publiant l'itinéraire suggère à un AS externe. Un MED faible est préféré à un MED élevé.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution BGP	Description
État Status (État)	État de publication de l'itinéraire.
État Status (État)	Indique si cet itinéraire est agrégé avec d'autres itinéraires.

Onglet Multicast

Le tableau suivant décrit les statistiques d'exécution multicast IP du routeur virtuel.

Statistiques d'exécution multicast	Description
Onglet FIB	
Group (Groupe)	Entrée d'itinéraire dans la Forwarding Information Base (base d'informations de transfert ; FIB) ; adresse du groupe multicast à laquelle le routeur virtuel transfèrera les paquets.
Source	Adresse source des paquets multicast du groupe.
Interfaces trafic entrant	Interfaces où les paquets multicast du groupe arrivent.
Interfaces en cours	Interfaces desquelles le routeur virtuel transfère les paquets multicast du groupe.
Onglet Interface IGMP	
Interface	Interface sur laquelle IGMP est activé.
Version	Version 1, 2 ou 3 du protocole Internet Group Management Protocol (protocole de gestion de groupe Internet ; IGMP) exécutée sur le routeur virtuel.
Requérant	Adresse IP du requérant IGMP sur le segment multi-accès connecté à l'interface.
Délai d'activation du requérant	Nombre de secondes pendant lesquelles le requérant IGMP a été actif.
Délai d'expiration du requérant	Nombre de secondes restant avant l'expiration du minuteur Autre requérant présent.
Robustesse	Variable de robustesse de l'interface IGMP.
Limite de groupes	Nombre maximum de groupes par interface qu'IGMP peut traiter simultanément.
Limite de sources	Nombre maximum de sources par interface qu'IGMP peut traiter simultanément.
Quitter immédiatement	Oui ou Non indique si l'option Quitter immédiatement est configurée. Celle-ci permet au routeur virtuel de supprimer une interface de la table de transfert sans envoyer de requêtes spécifiques au groupe IGMP de l'interface.

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution multicast	Description
Onglet Membres IGMP	
Interface	Nom de l'interface qui appartient au groupe.
Group (Groupe)	Adresse du groupe multicast auquel l'interface appartient.
Source	Adresse IP de la source qui envoie les paquets multicast au groupe.
Délai d'activation	Nombre de secondes pendant lesquelles cette appartenance est active.
Délai d'expiration	Nombre de secondes avant l'expiration de l'appartenance.
Mode de filtrage	Inclusion ou exclusion de la source. Le routeur virtuel est configuré pour inclure l'ensemble du trafic ou uniquement le trafic de cette source (inclusion), ou bien le trafic de n'importe quelle source excepté celle-ci (exclusion).
Expiration de l'exclusion	Nombre de secondes avant l'expiration de l'état Exclure de l'interface.
Minuteur d'hôte V1	Temps restant avant que le routeur local suppose qu'il n'y a plus aucun membre IGMP Version 1 sur le sous-réseau IP associé à l'interface.
Minuteur d'hôte V2	Temps restant avant que le routeur local suppose qu'il n'y a plus aucun membre IGMP Version 2 sur le sous-réseau IP associé à l'interface.
Onglet Mappage de groupe PIM	
Group (Groupe)	Adresse IP du groupe mappé à un point de rendez-vous.
RP	Adresse IP du point de rendez-vous du groupe.
Origine	Indique si le routeur virtuel a appris le RP.
Mode PIM	ASM ou SSM.
Inactif	Indique si le mappage du groupe au RP est inactif.
Onglet Interface PIM	
Interface	Nom de l'interface participant à PIM.
Adresse	Adresse IP de l'interface.
DR	Adresse IP du routeur désigné sur le segment multi-accès connecté à l'interface.
Intervalle Hello	Intervalle Hello configurée (en secondes).
Intervalle Join/ Prune	Intervalle configuré pour les messages Join et Prune (en secondes).

© 2020 Palo Alto Networks, Inc.

Statistiques d'exécution multicast	Description
Intervalle d'affirmation	Intervalle configuré entre les messages d'affirmation PIM (en secondes) pour que le routeur virtuel envoie les messages d'affirmation. PIM utilise le mécanisme d'affirmation pour initier la sélection du transmetteur PIM pour le réseau multi-accès.
Dr priorité	Priorité configurée pour le routeur désigné sur le segment multi-accès connecté à l'interface.
Limite BSR	Oui ou Non indique si l'interface se trouve sur un routeur virtuel qui est Bootstrap Router (routeur d'amorçage ; BSR) situé à la limite du réseau local d'une entreprise.
Onglet Voisin PIM	
Interface	Nom de l'interface sur le routeur virtuel.
Adresse	Adresse IP du voisin PIM accessible sur l'interface.
Adresse secondaire	Adresse IP secondaire du voisin PIM accessible sur l'interface.
Délai d'activation	Durée pendant laquelle le voisin a été actif.
Délai d'expiration	Durée restante avant expiration du voisin, car le routeur virtuel ne reçoit pas de paquets Hello du voisin.
ID de génération	Valeur de 32-bit aléatoirement générée qui est régénérée chaque fois que la transmission PIM commence ou recommence sur l'interface (y compris lorsque le routeur lui-même est redémarré).
Dr priorité	Priorité du routeur désigné reçue par le routeur virtuel dans le dernier message Hello PIM de ce voisin.

Onglet Informations récapitulatives de BFD

Les informations récapitulatives de BFD comprennent les données suivantes.

Informations récapitulatives de BFD concernant les Statistiques d'exécution	Description
Interface	Interface qui exécute BFD.
Protocole	Itinéraire statique (famille d'adresses IP d'itinéraire statique) ou protocole de routage dynamique qui exécute BFD sur l'interface.
Adresse IP locale	Adresse IP de l'interface sur laquelle vous avez configuré BFD.

© 2020 Palo Alto Networks, Inc.

Informations récapitulatives de BFD concernant les Statistiques d'exécution	Description
Adresse IP du voisin	Adresse IP du voisin BFD.
État	Les états BFD des homologues BFD locaux et distants : **administrateur inactif**, **inactif**, **initialisation** ou **actif**.
Temps de fonctionnement	Délai pendant lequel BFD a été activé (heures, minutes, secondes et millisecondes).
Discriminateur (local)	Discriminateur pour les homologues BFD locaux. Un discriminateur est une valeur unique et non nulle que les homologues utilisent pour distinguer plusieurs sessions BFD entre eux.
Discriminateur (distant)	Discriminateur pour les homologues BFD distants.
Erreurs	Nombre d'erreurs BFD.
Détails de la session	Cliquez sur **Détails** pour voir les informations BFD pour une session comme les adresses IP des voisins locaux et distants, le dernier code de diagnostic distant reçu, le nombre de paquets de contrôle transmis et reçus, le nombre d'erreurs, des informations sur le dernier paquet engendrant un changement d'état, etc.

© 2020 Palo Alto Networks, Inc.

Réseau > Tunnels'A0;IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour établir et gérer des tunnels VPN IPSec entre les pare-feu. Il s'agit de la phase 2 de la configuration de VPN IKE/IPSec.

Que voulez-vous faire ?	Reportez-vous à la section :
Gestion des tunnels VPN IPSec.	Gestion d’un tunnel VPN IPSec
Configuration d’un tunnel IPSec.	Onglet Général Tunnel IPSec
	Onglet ID de proxy Tunnel IPSec
Affichage du statut du tunnel IPSec.	Statut du tunnel IPSec sur le pare-feu
Redémarrer ou actualiser un tunnel IPSec.	Redémarrage ou actualisation d'un tunnel IPSec
Vous souhaitez en savoir plus ?	Configuration d’un tunnel IPSec.

Gestion d’un tunnel VPN IPSec

- Réseau > Tunnels'A0;IPSec

Le tableau suivant explique comment gérer les tunnels VPN IPSec.

Champs pour gérer les tunnels VPN IPSec	
Ajouter	Cliquez pour **Ajouter** un nouveau tunnel VPN IPSec. Voir l’onglet Tunnel IPSec - Onglet Général pour des instructions sur la configuration du nouveau tunnel.
Supprimer	Cliquez pour **Supprimer** un tunnel dont vous n’avez plus besoin.
Activer	Cliquez pour **Activer** un tunnel qui a été désactivé (les tunnels sont activés par défaut).
Désactivation	Cliquez pour **Désactiver** un tunnel que vous ne voulez pas utiliser, mais qui n’est pas encore prêt à être supprimé.
PDF/CSV	Exportez la configuration des tunnels au format **PDF/CSV**. Vous pouvez appliquer des filtres pour personnaliser le tableau et n’inclure que les colonnes dont vous avez besoin. Seules les colonnes visibles dans le dialogue d’exportation sont exportées. Consultez la section Exportation des données du tableau de configuration.

© 2020 Palo Alto Networks, Inc.

Onglet Général Tunnel IPSec

- Réseau > Tunnels IPSec > Général

Utilisez les champs suivants pour configurer un tunnel IPSec.

Paramètres généraux d'un tunnel IPSec	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier le tunnel (63 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. La limite de 63 caractères de ce champ inclut le nom du tunnel, en plus de l'ID de proxy, séparé par deux-points.
en texte clair	Sélectionnez une interface de tunnel existante ou cliquez sur **New Tunnel Interface (Nouvelle interface de tunnel)**. Pour des informations sur la création d'une interface de tunnel, reportez-vous à Réseau > Interfaces > Tunnel.
IPv4 ou IPv6	Sélectionnez **IPv4** ou **IPv6** pour configurer le tunnel de manière à avoir des points d'extrémité avec ce type d'adresse IP.
Type	Indiquez si une clé de sécurité générée automatiquement ou saisie manuellement doit être utilisée. L'option **Auto key (Clé automatique)** est recommandée.
Clé automatique	Si vous choisissez **Auto key (Clé automatique)**, indiquez les options suivantes : • **IKE Gateway (Passerelle IKE)** – Reportez-vous à Réseau > Profils réseau > Passerelles IKE pour des descriptions des paramètres de passerelle IKE. • **IPSec Crypto Profile (Profil crypto IPSec)** - Sélectionnez un profil existant ou conservez le profil par défaut. Pour définir un nouveau profil, cliquez sur **New (Nouveau)** et suivez les instructions dans Réseau > Profils réseau > Crypto IPSec. • Cliquez sur **Show Advanced Options (Afficher les options avancées)** pour accéder aux champs restants. • **Enable Replay Protection (Activer la protection contre les attaques par relecture)** – Sélectionnez pour vous protéger des attaques par relecture. • **Copy TOS Header (Copier l'en-tête TOS)** - Permet de copier le champ Type de service (TOS) à partir de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés afin de conserver les informations TOS d'origine. Cette option copie également le champ Notification explicite de congestion (ECN). • **Add GRE Encapsulation (Ajouter l'encapsulation GRE)** : sélectionnez cette option pour ajouter un en-tête GRE encapsulé dans le tunnel IPSec. Le pare-feu génère un en-tête GRE après l'en-tête IPSec pour l'interopérabilité avec les points de terminaison du tunnel d'un autre fournisseur, partageant ainsi un tunnel GRE avec le tunnel IPSec. • **Tunnel Monitor (Surveillance des tunnels)** – Sélectionnez pour informer l'administrateur de périphérique de la défaillance d'un tunnel et basculer automatiquement vers une autre interface.  *Vous devez affecter une adresse'A0;IP à l'interface de tunnel à surveiller.*

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'un tunnel IPSec	Description
	• **Destination IP (Adresse IP de destination)** : indiquez une adresse IP de l'autre côté du tunnel que le moniteur de tunnels va utiliser pour déterminer si le tunnel fonctionne correctement. • **Profile (Profil)** - Sélectionnez un profil existant qui déterminera les actions prises en cas de défaillance d'un tunnel. Si l'action spécifiée dans le profil de surveillance est en attente de récupération, le pare-feu attend que le tunnel devienne fonctionnel et ne cherche PAS d'autre chemin dans la table de routage. Si l'action de basculement est sélectionnée, le pare-feu recherche dans la table de routage si un autre itinéraire peut être utilisé pour atteindre la destination. Pour plus d'informations, voir Réseau > Profils réseau > Surveillance.
Clé manuelle	Si vous choisissez **Manual Key (Clé manuelle)**, indiquez les options suivantes : • **Local SPI (SPI local)** - Indiquez l'index de paramètres de sécurité (SPI) local pour le parcours du paquet entre le pare-feu local et l'homologue. SPI est un index hexadécimal ajouté à l'en-tête du tunnel IPSec permettant de différencier les flux de trafic IPSec. • **Interface** - Sélectionnez l'interface correspondant au point d'extrémité du tunnel. • **Local Address (Adresse locale)** - Sélectionnez l'adresse IP de l'interface locale correspondant au point d'extrémité du tunnel. • **Remote SPI (SPI distant)** - Indiquez l'index de paramètres de sécurité (SPI) distant pour le parcours du paquet entre le pare-feu distant et l'homologue. • **Protocol (Protocole)** - Sélectionnez le protocole utilisé pour le trafic passant par le tunnel (**ESP** ou **AH**). • **Authentication (Authentification)** - Sélectionnez le type d'authentification pour accéder au tunnel (**SHA1**, **SHA256**, **SHA384**, **SHA512**, **MD5** ou **None (Aucun)**). • **Key/Confirm Key (Clé/Confirmer la clé)** - Saisissez et confirmez une clé d'authentification. • **Encryption (Chiffrement)** - Sélectionnez une option de chiffrement pour le trafic du tunnel (**3des**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **des** ou **null (aucun)** [aucun chiffrement]). • **Key/Confirm Key (Clé/Confirmer la clé)** - Saisissez et confirmez une clé de chiffrement.
Satellite GlobalProtect	Si vous choisissez **GlobalProtect Satellite (Satellite GlobalProtect)**, indiquez les options suivantes : • **Name (Nom)** - Saisissez un nom pour identifier le tunnel (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. • **Tunnel Interface (Interface de tunnel)** – Sélectionnez une interface de tunnel existante ou cliquez sur Nouvelle interface de tunnel. • **Portal Address (Adresse du portail)** – Saisissez l'adresse IP du portail GlobalProtect™. • **Interface** – Sélectionnez l'interface dans la liste déroulante correspondant à l'interface de sortie permettant d'atteindre le Portail GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'un tunnel IPSec	Description
	• **Local IP Address (Adresse IP locale)** – Saisissez l'adresse IP de l'interface de sortie qui se connecte au Portail GlobalProtect. • **Options avancées** • **Publish all static and connected routes to Gateway (Publier tous les itinéraires statiques et connectés à la Passerelle)** – Sélectionnez cette option afin de publier tous les itinéraires du satellite vers la Passerelle GlobalProtect à laquelle ce satellite est connecté. • **Subnet (Sous-réseau)** - Cliquez sur **Add (Ajouter)** pour ajouter manuellement des sous-réseaux locaux à l'emplacement d'un satellite. Si d'autres satellites utilisent les mêmes informations de sous-réseau, vous devez traduire l'adresse réseau (NAT) de l'ensemble du trafic vers l'adresse IP de l'interface de tunnel. De plus, le satellite ne doit partager aucun itinéraire dans ce cas de figure, le routage entier sera alors réalisé via l'IP de tunnel. • **External Certificate Authority (Autorité de certification externe)** – Sélectionnez si vous prévoyez d'utiliser une autorité de certification (CA) externe pour gérer les certificats. Une fois vos certificats générés, vous devrez les importer dans le satellite et sélectionner le **Local Certificate (Certificat local)** et le **Certificate Profile (Profil du certificat)**.

Onglet ID de proxy Tunnel IPSec

- Réseau > Tunnels IPSec > ID Proxy

L'onglet **IPSec Tunnel Proxy IDs (ID de proxy du tunnel IPSec)** est séparé en deux sous-onglets : **IPv4** et **IPv6**. L'aide est similaire pour les deux types ; les différences entre IPv4 et IPv6 sont décrites dans les champs **Local** et **Remote (Distant)** du tableau suivant.

L'onglet **IPSec Tunnel Proxy IDs (ID de proxy du tunnel IPSec)** permet également de spécifier les sélecteurs de trafic pour IKEv2.

Paramètres d'ID de proxy IPv4 et IPv6	Description
ID de proxy	Cliquez sur **Add (Ajouter)** et saisissez un nom pour identifier le proxy. Ce champ est utilisé comme nom pour un sélecteur de trafic IKEv2.
Local	Pour IPv4 : saisissez une adresse IP ou un sous-réseau au format x.x.x.x/masque (par exemple : 10.1.2.0/24). Pour IPv6 : Saisissez une adresse IP et une longueur de préfixe au format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longueur-préfixe (ou par connexion IPv6, par exemple : 2001:DB8:0::/48). L'adressage IPv6 ne nécessite pas la saisie de tous les zéros ; les zéros non significatifs peuvent être omis et un groupe de zéros consécutifs peut être remplacé par deux-points adjacents (::). Ce champ est converti en adresse IP source pour un sélecteur de trafic IKEv2.
Distant	Si l'homologue l'exige :

© 2020 Palo Alto Networks, Inc.

Paramètres d'ID de proxy IPv4 et IPv6	Description
	Pour IPv4, saisissez une adresse IP ou un sous-réseau au format x.x.x.x/masque (par exemple : 10.1.1.0/24). Pour IPv6, saisissez une adresse IP et une longueur de préfixe au format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longueur-préfixe (ou par connexion IPv6, par exemple : 2001:DB8:55::/48). Ce champ est converti en adresse IP de destination pour un sélecteur de trafic IKEv2.
Protocole	Indiquez le protocole et les numéros de port pour les ports locaux et distants'A0;: **Number (Numéro)** - Indiquez le numéro de protocole (pour assurer l'interopérabilité avec des périphériques tiers). • **Any (Indifférent)** - Autorisez le trafic TCP et/ou UDP. • **TCP** - Indiquez les numéros de port TCP locaux et distants. • **UDP** - Indiquez les numéros de port UDP locaux et distants. chaque ID de proxy configuré va être inclus dans la capacité du tunnel VPN IPSec du pare-feu. Ce champ est également utilisé comme sélecteur de trafic IKEv2.

Statut du tunnel IPSec sur le pare-feu

- Réseau > Tunnels'A0;IPSec

Pour afficher le statut des tunnels VPN IPSec actuellement définis, ouvrez la page **IPSec Tunnels (Tunnels IPSec)**. Les informations suivantes concernant le statut sont signalées sur la page'A0;:

- Statut du tunnel (première colonne du statut) – La couleur verte indique un tunnel SA de phase 2 IPSec. La couleur rouge indique qu'une SA IPSec de phase 2 n'est pas disponible ou a expiré.
- Statut de la passerelle IKE – La couleur verte indique une SA de phase 1 IKE ou IKEv2 valide. La couleur rouge indique qu'une association de sécurité'A0;IKE de phase'A0;1 n'est pas disponible ou a expiré.
- Statut de l'interface de tunnel – La couleur verte indique que l'interface du tunnel est active (car la surveillance de tunnels est désactivée ou car le statut de la surveillance de tunnels affiche ACTIF et l'adresse IP de la surveillance est accessible). La couleur rouge indique que l'interface de tunnel est inactive, car la surveillance des tunnels est activée et l'adresse IP de surveillance des tunnels ne peut pas être atteinte.

Redémarrage ou actualisation d'un tunnel IPSec

- Réseau > Tunnels'A0;IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour afficher l'état des tunnels. Dans la première colonne Statut se trouve un lien vers les informations du tunel. Cliquez sur le tunnel que vous souhaitez redémarrer ou actualiser pour ouvrir la page **Tunnel Info (Informations du tunnel)** qui correspond à ce tunnel. Cliquez sur l'une des entrées de la liste, puis sur :

- **Restart (Redémarrer)** – Redémarre le tunnel sélectionné. Un redémarrage interrompt le trafic passant à travers le tunnel.
- **Refresh (Rafraichir)** – Affiche le statut actuel de la SA IPSec.

© 2020 Palo Alto Networks, Inc.

Réseau > Tunnels GRE

Le protocole de tunnel de Generic Routing Encapsulation (encapsulation générique de routage ; GRE) est un protocole de transport qui encapsule un protocole de charge utile. Le paquet GRE lui-même est encapsulé dans un protocole de transport (IPv4 ou IPv6). Le tunnel GRE connecte deux points de terminaison en une liaison logique de point à point entre le pare-feu et un routeur (ou un autre pare-feu). Les pare-feu Palo Alto Networks prennent en charge l'interruption du tunnel GRE.

Que voulez-vous faire ?	Reportez-vous à la section :
Blocs de construction d'un tunnel GRE	Tunnels GRE
Comment fournir l'interopérabilité avec le point de terminaison du tunnel d'un autre fournisseur	Sélectionnez **Add GRE Encapsulation (Ajouter l'encapsulation GRE)** lors de la création d'un tunnel IPSec.
Vous souhaitez en savoir plus ?	Tunnels GRE

Tunnels GRE

- Réseau > Tunnels GRE

Commencez par configurer une interface de tunnel (Réseau > Interfaces > Tunnel). Ajoutez ensuite un tunnel de generic routing encapsulation (encapsulation générique de routage ; GRE) et fournissez les renseignements suivants, en faisant référence à l'interface de tunnel que vous avez créée :

Champs du tunnel GRE	Description
Name (Nom)	Nom du tunnel GRE.
Interface	Sélectionnez l'interface à utiliser en tant que point de terminaison du tunnel GRE local (interface source), soit une interface ou une sous-interface Ethernet, une interface Aggregate Ethernet (AE), une interface de bouclage ou une interface VLAN.
Adresse locale	Sélectionnez l'adresse IP locale de l'interface à utiliser en tant qu'adresse de l'interface du tunnel.
Adresse de l'homologue	Saisissez l'adresse IP à l'extrémité opposée du tunnel GRE.
en texte clair	Sélectionnez l'interface de tunnel que vous avez configurée. (Cette interface identifie le tunnel lorsqu'il correspond au saut suivant du routage.)
TTL	Saisissez la TTL du paquet IP encapsulé dans le paquet GRE (plage comprise entre 1 et 255 ; la valeur par défaut est 64).

© 2020 Palo Alto Networks, Inc.

Champs du tunnel GRE	Description
Copier l'en-tête ToS	Sélectionnez cette option pour copier le champ ToS (Type of Service) de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés pour préserver les informations ToS d'origine.
Keep Alive	Sélectionnez cette option pour activer la fonction Keep Alive du tunnel GRE (désactivée par défaut). Si vous activez la fonction Keep Alive, il faut trois paquets keep alive non retournés (retentatives) à des intervalles de dix secondes pour que le tunnel GRE échoue, et il faut cinq intervalles Délai de maintien à des intervalles de dix secondes pour que le tunnel GRE redevienne actif.
Intervalle (s)	Définissez l'intervalle entre des paquets keepalive que l'extrémité locale du tunnel GRE envoie au tunnel homologue et l'intervalle que chaque Minuterie d'attente attend des paquets keepalive réussis avant que le pare-feu rétablit la communication avec le tunnel homologue (la plage est comprise entre 1 et 50 ; la valeur par défaut est 10).
Relance	Définissez les intervalles pendant lesquels aucun paquet keepalive n'est retourné avant que le tunnel homologue considère que le tunnel homologue est inactif (la plage est comprise entre 1 et 255 ; la valeur par défaut est 3).
Minuterie d'attente	Définissez les intervalles pendant lesquels les paquets keepalive réussissent avant que le pare-feu rétablit la communication avec le tunnel homologue (la plage est comprise entre 1 et 64 ; la valeur par défaut est 5).

© 2020 Palo Alto Networks, Inc.

Réseau > DHCP

DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) est un protocole normalisé qui fournit des paramètres de configuration de la couche de liaison et TCP/IP, ainsi que des adresses IP, aux hôtes configurés de façon dynamique sur un réseau TCP/IP. Une interface sur un pare-feu Palo Alto Networks peut avoir comme un serveur, un client ou un agent de relais DHCP. L'affectation de ces rôles à différentes interfaces permet au pare-feu de remplir plusieurs rôles.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est-ce que DHCP ?	Présentation de DHCP
Comment un serveur DHCP alloue-t-il des adresses ?	Adressage DHCP
Configuration d'une interface sur le pare-feu pour agir en tant que :	
	Serveur DHCP
	Relais DHCP
	Réseau > Proxy'A0;DNS
Vous souhaitez en savoir plus ?	DHCP

Présentation de DHCP

- Réseau > DHCP

DHCP utilise un modèle de communication client/serveur. Ce modèle est composé de trois rôles que le pare-feu peut remplir : client DHCP, serveur DHCP et agent de relais DHCP.

- Un pare-feu agissant comme un client (hôte) DHCP peut demander une adresse IP et d'autres paramètres de configuration auprès d'un serveur DHCP. Les utilisateurs sur les pare-feu clients gagnent ainsi du temps lors de la configuration et n'ont pas besoin de connaître le plan d'adressage du réseau ou d'autres ressources et options héritées du serveur DHCP.
- Un pare-feu agissant comme un serveur DHCP peut servir des clients. L'utilisation de l'un des trois mécanismes d'adressage DHCP permet à l'administrateur de gagner du temps lors de la configuration et de réutiliser un nombre limité d'adresses IP lorsque les clients n'ont plus besoin de connexion réseau. Le serveur peut également fournir l'adressage IP et les options DCHP à plusieurs clients.
- Un pare-feu agissant comme un agent de relais DHCP écoute les messages DHCP de diffusion et de monodiffusion, et les relais entre les clients et les serveurs DHCP.

DHCP utilise User Datagram Protocol (Protocole de datagramme utilisateur, UDP), à savoir RFC 768 comme protocole de transport. Un client envoie des messages DHCP à un serveur sur le port 67 bien connu (port UDP utilisé par BOOTP et DHCP). Un serveur envoie des messages DHCP à un client sur le port 68.

Adressage DHCP

Un serveur DHCP affecte ou envoie une adresse IP à un client de trois manières différentes :

© 2020 Palo Alto Networks, Inc.

- **Automatic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP permanente de ses **IP Pools (pools d'adresses IP)** à un client. Sur le pare-feu, un **Lease (Bail)** spécifié comme **Unlimited (Illimité)** signifie que l'allocation est permanente.
- **Dynamic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP réutilisable de ses **IP Pools (pools d'adresses IP)** à un client, pour une durée maximale, appelée *bail*. Cette méthode d'allocation d'adresse est utile lorsque le client dispose d'un nombre limité d'adresses IP ; celles-ci peuvent être affectées aux clients qui ont besoin d'un accès temporaire au réseau.
- **Static allocation (Allocation statique)** : l'administrateur réseau choisit l'adresse IP à affecter au client et le serveur DHCP l'envoie au client. Une allocation DHCP statique est permanente ; elle est effectuée en configurant un serveur DHCP et en choisissant une **Reserved Address (Adresse réservée)** correspondant à la **MAC Address (Adresse MAC)** du pare-feu client. L'allocation DHCP reste en place même si le client se déconnecte, (ferme sa session, redémarre, subit une coupure de courant, etc.).

  L'allocation statique d'une adresse IP est utile, par exemple, si vous disposez d'une imprimante sur un réseau local et que vous ne souhaitez pas que cette adresse IP change, car elle est associée à un nom d'imprimante via DNS. Un autre exemple est si un pare-feu client est utilisé pour des tâches essentielles et doit conserver la même adresse IP, même si le pare-feu est désactivé, déconnecté, redémarré ou subit une coupure de courant.

  Souvenez-vous des points suivants lors de la configuration d'une **Reserved Address (Adresse réservée)** :

  - Il s'agit d'une adresse des **IP Pools (Pools d'adresses IP)**. Vous pouvez configurer plusieurs adresses IP réservées.
  - Si vous ne configurez aucune **Reserved Address (Adresse réservée)**, les clients du serveur recevront de nouvelles allocations DHCP du pool lorsque leur bail expirera ou quand ils redémarreront, etc. (à moins que vous n'indiquiez un **Lease (Bail) Unlimited (Illimité)**).
  - Si vous affectez chaque adresse des **IP Pools (Pools d'adresses IP)** comme **Reserved Address (Adresse réservée)**, il ne reste aucune adresse dynamique à affecter au prochain client DHCP demandant une adresse.
  - Vous pouvez configurer une **Reserved Address (Adresse réservée)** sans configurer de **MAC Address (Adresse MAC)**. Dans ce cas, le serveur DHCP n'affecte la **Reserved Address (Adresse réservée)** à aucun pare-feu. Vous pouvez réserver plusieurs adresses du pool et les affecter de manière statique à une imprimante et un fax, par exemple, sans utiliser DHCP.

Serveur DHCP

- Réseau > DHCP > Serveur DHCP

La section suivante décrit chaque composant du serveur DHCP. Avant de configurer un serveur DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de couche 3 et de l'avoir affectée à un routeur virtuel et une zone. Vous devez également connaître un pool valide d'adresses IP de votre plan réseau qui peut être désigné pour être affecté par votre serveur DHCP aux clients.

Lors de l'ajout d'un serveur DHCP, vous devez configurer les paramètres décrits dans le tableau ci-dessous :

Paramètres d'un serveur DHCP	Configuré dans	Description
Interface	**Serveur DHCP**	Nommez l'interface qui servira de serveur DHCP.
Mode		Sélectionnez **enabled (activé)** ou le mode **auto (automatique)**. Le mode **Auto (Automatique)** active le serveur et le désactive si un autre serveur DHCP est détecté sur le réseau. Le paramètre **disabled (désactivé)** désactive le serveur.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un serveur DHCP	Configuré dans	Description
Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP	**DHCP Server (Serveur DHCP)** > **Lease (Bail)**	Si vous cliquez sur **Ping IP when allocating new IP (Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP)**, le serveur envoie un message ping à l'adresse IP avant d'affecter cette adresse à son client. Si le message ping reçoit une réponse, cela signifie qu'un autre pare-feu dispose déjà de cette adresse ; celle-ci n'est donc pas disponible pour l'affectation. Le serveur affecte alors l'adresse suivante du pool. Si vous choisissez cette option, la colonne Sonder l'adresse IP sera cochée.
Crédit-bail		Indiquez un type de bail. • **Unlimited (Illimité)** : le pare-feu choisit de manière dynamique les adresses IP de ses pools d'adresses IP et les affecte définitivement aux clients. • **Timeout (Délai d'expiration)** : cette option détermine la durée du bail. Saisissez le nombre de **Days (Jours)**, **Hours (Heures)** et éventuellement **Minutes**.
Pools d'adresses IP		Indiquez le pool d'adresses IP dynamiques dans lequel le serveur DHCP choisit une adresse et l'affecte à un client DHCP. Vous pouvez saisir une adresse unique, une adresse/<longueur de masque>, telle que 192.168.1.0/24, ou une plage d'adresses, telle que 192.168.1.10-192.168.1.20.
Adresse réservée		Vous pouvez indiquer une adresse IP (format x.x.x.x) des pools d'adresses IP que vous ne souhaitez pas voir affectée de façon dynamique par le serveur DHCP. Si vous spécifiez une **MAC Address (Adresse MAC)** (format xx:xx:xx:xx:xx:xx), la **Reserved Address (Adresse réservée)** est affectée au pare-feu associé à cette adresse MAC lorsqu'il demande une adresse IP via DHCP.
Source de l'héritage	**DHCP Server (Serveur DHCP)** > **Options**	Laissez **None (Aucune)** (par défaut) ou sélectionnez une interface client PPPoE ou DHCP source pour propager les divers paramètres du serveur sur le serveur DHCP. Si vous indiquez la **Inheritance Source (Source de l'héritage)**, sélectionnez une ou plusieurs options **inherited (héritées)** de cette source ci-dessous. L'un des avantages de la spécification de la source d'héritage est le transfert rapide des options DHCP du serveur qui se trouve en amont du client DHCP source. Celle-ci permet également de maintenir les options du client à jour en cas de modification sur la source

© 2020 Palo Alto Networks, Inc.

Paramètres d'un serveur DHCP	Configuré dans	Description
		de l'héritage. Par exemple, si le pare-feu source de l'héritage remplace son serveur NTP (qui a été identifié comme serveur **Primary NTP (NTP principal)**), le client héritera automatiquement de la nouvelle adresse en tant que son serveur **Primary NTP (NTP principal)**.
Vérifier l'état de la source de l'héritage		Si vous sélectionnez une **Inheritance Source (Source de l'héritage)**, cliquez sur **Check inheritance source status (Vérifier l'état de la source de l'héritage)** pour ouvrir la fenêtre Statut de l'interface IP dynamique, qui affiche les options héritées du client DHCP.
Passerelle	**DHCP Server (Serveur DHCP)** > **Options (suite)**	Adresse IP de la passerelle réseau (une interface sur le pare-feu) permettant d'accéder à chaque périphérique situé sur un autre réseau local que ce serveur DHCP.
Masque de sous-réseau		Indiquez le masque réseau qui s'applique aux adresses figurant dans le champ **IP Pools (Pools d'adresses IP)**.
Options (Options)		Pour les champs suivants, cliquez sur la liste déroulante et sélectionnez **None (Aucun)** ou **inherited (hérité)** ou saisissez l'adresse IP du serveur distant que votre serveur DHCP enverra aux clients pour accéder à ce service. Si vous sélectionnez **inherited (hérité)**, le serveur DHCP hérite des valeurs du client DHCP source indiqué comme **Inheritance Source (Source de l'héritage)**. Le serveur DHCP envoie ces paramètres à ses clients. • **Primary DNS (DNS principal)**, **Secondary DNS (DNS secondaire)** : adresse IP des serveurs Domain Name System (système de noms de domaine ; DNS) préféré et alternatif. • **Primary WINS (WINS principal)**, **Secondary WINS (WINS secondaire)** – Adresse IP des serveurs WINS (Windows Internet Name Service) préférés et alternatifs. • **Primary NIS (NIS principal)**, **Secondary NIS (NIS secondaire)** : adresse IP des serveurs Network Information Service (service d'informations réseau ; NIS) préférés et alternatifs. • **Primary NTP (NTP principal)**, **Secondary NTP (NTP secondaire)** – Adresse IP des serveurs NTP (Serveur du protocole de temps du réseau) préférés et alternatifs. • **POP3 Server (Serveur POP3)** : adresse IP du serveur POP3 (Post Office Protocol version 3). • **SMTP Server (Serveur SMTP)** : adresse IP du serveur Simple Mail Transfer Protocol (protocole simple de transfert de courrier ; SMTP).

© 2020 Palo Alto Networks, Inc.

Paramètres d'un serveur DHCP	Configuré dans	Description
		• **DNS Suffix (Suffixe DNS)** : suffixe que le client pourra utiliser localement lors de la saisie d'un nom d'hôte non qualifié irrésoluble.
Options DHCP personnalisées		Cliquez sur **Add (Ajouter)** et saisissez le **Name (Nom)** de l'option personnalisée que vous souhaitez que le serveur DHCP envoie aux clients. Saisissez un **Option Code (Code d'option)** (intervalle compris entre 1 et 254). Si un **Option Code 43 (Code d'option 43)** est saisi, le champ Identificateur de classe du fournisseur (VCI) s'affiche. Saisissez un critère de correspondance qui sera comparé au VCI provenant de l'option 60 du client. Le pare-feu examine le VCI provenant de l'option 60 du client, trouve le VCI correspondant dans la table du serveur DHCP et renvoie la valeur correspondante au client dans l'option 43. Le critère de correspondance du VCI est une chaîne ou une valeur hexadécimale. Une valeur hexadécimale doit avoir un préfixe « 0x ». Sélectionnez **Inherited from DCHP server inheritance source (Hérité de la source de l'héritage du serveur DHCP)** pour que le serveur hérite de la valeur de ce code d'option de la source de l'héritage au lieu de saisir une **Option Value (Valeur d'option)**. Vous pouvez également procéder comme suit : **Option Type (Type d'option)** : sélectionnez **IP Address (Adresse IP)**, **ASCII** ou **Hexadecimal (Hexadécimal)** pour indiquer le type de données utilisé pour la Valeur de l'option. Pour **Option Value (Valeur de l'option)**, cliquez sur **Add (Ajouter)** et saisissez la valeur de l'option personnalisée.

Relais DHCP

- Réseau > DHCP > Relais DHCP

Avant de configurer une interface de pare-feu en tant que relais DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de Niveau 3 et de l'avoir affectée à un routeur virtuel et à une zone. Vous souhaitez que cette interface puisse transmettre des messages DHCP entre les clients et les serveurs. Chaque interface peut transmettre des messages à un maximum de huit serveurs DHCP IPv4 externes et de huit serveurs DHCP IPv6 externes. Un client envoie un message DHCPDISCOVER à tous les serveurs configurés, et le pare-feu relaye le message DHCPOFFER du premier serveur qui répond au client qui a effectué la demande.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un relais DHCP	Description
Interface	Nommez l'interface qui servira d'agent de relais DHCP.
IPv4/IPv6	Sélectionnez le type de serveur DHCP et d'adresse IP que vous indiquerez.
Adresse IP du serveur DHCP	Saisissez l'adresse IP du serveur DHCP duquel et auquel vous relayerez les messages DHCP.
Interface	Si vous avez sélectionné IPv6 comme protocole d'adresse IP pour le serveur DHCP et spécifié une adresse multicast, vous devez également indiquer une interface sortante.

Client DHCP

- Réseau > Interfaces > Ethernet > IPv4
- Réseau > Interfaces > VLAN > IPv4

Avant de configurer une interface de pare-feu en tant que client DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de Niveau 3 et de l'avoir affectée à un routeur virtuel et à une zone. Effectuez cette tâche si vous devez utiliser DHCP pour demander une adresse IPv4 pour une interface sur votre pare-feu.

Paramètres d'un client DHCP	Description
Type	Sélectionnez l'option **DHCP Client (Client DHCP)**, puis **Enable (Activer)** pour configurer cette interface en tant que client DHCP.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur	Le pare-feu crée un itinéraire statique vers la passerelle par défaut qui sera utile lorsque les clients tenteront d'accéder à de nombreuses destinations qui n'ont pas besoin de conserver des itinéraires dans une table de routage sur le pare-feu.
Mesure d'itinéraire par défaut	Saisissez éventuellement une **Default Route Metric (Mesure d'itinéraire par défaut)** (niveau de priorité) pour l'itinéraire entre le pare-feu et le serveur DHCP. Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur métrique de 10 est utilisé avant un itinéraire avec une valeur métrique de 100 (intervalle compris entre 1 et 65 535 ; aucune valeur définie par défaut).
Afficher les informations d'exécution du client DHCP	Affiche tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).

© 2020 Palo Alto Networks, Inc.

Réseau > Proxy'A0;DNS

Les serveurs DNS fournissent le service de résolution d'un nom de domaine en adresse IP et vice-versa. Lorsque vous configurez le pare-feu en tant que proxy DNS, il agit comme un intermédiaire entre les clients et les serveurs, et comme un serveur DNS en résolvant les requêtes du cache DNS ou en transférant les requêtes à d'autres serveurs DNS. Cette page vous permet de configurer les paramètres qui déterminent comment le pare-feu sert de proxy DNS.

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment le pare-feu sert de proxy pour les requêtes DNS?	Présentation du proxy DNS
Comment puis-je configurer un proxy DNS ?	Paramètres du proxy DNS
Comment puis-je configurer les mappages d'adresse FQDN vers les IP statiques ?	
Comment puis-je gérer les proxys DNS ?	Actions de proxy DNS supplémentaires
Vous souhaitez en savoir plus ?	DNS

Présentation du proxy DNS

Vous pouvez configurer le pare-feu pour qu'il agisse en tant que serveur DNS. Tout d'abord, créez un proxy DNS et sélectionnez les interfaces auxquelles s'applique le proxy. Ensuite, spécifiez les serveurs primaires et secondaires DNS par défaut auxquels le pare-feu envoie les requêtes DNS lorsqu'il ne trouve pas le nom de domaine dans le cache du proxy DNS (et lorsque le nom de domaine ne correspond pas à une règle de proxy).

Pour diriger les requêtes DNS vers différents serveurs DNS en fonction des noms de domaine, créez des règles de proxy DNS. L'indication de plusieurs serveurs DNS peut assurer la localisation des requêtes DNS et améliorer l'efficacité. Par exemple, vous pouvez transférer toutes les requêtes DNS vers un serveur DNS d'entreprise et transférer toutes les autres requêtes vers des serveurs DNS fournisseurs de services Internet.

Utilisez les onglets suivants pour définir un proxy DNS (au-delà des serveurs DNS primaires et secondaires par défaut) :

- **Entrées statiques** – Vous permet de configurer les mappages d'adresse FQDN vers les IP statiques que le pare-feu met en cache et envoie aux hôtes en réponse aux requêtes DNS.
- **Règles de proxy DNS** – Vous permet de spécifier les noms de domaine et les serveurs DNS principaux et secondaires correspondants pour résoudre les requêtes qui correspondent à la règle. Si le nom de domaine est introuvable dans le cache du proxy DNS, le pare-feu recherche une correspondance dans le proxy DNS (sur l'interface sur laquelle la requête est parvenue) et la transmet la requête à un serveur DNS en fonction des résultats de correspondance. Si aucun résultat ne correspond, le pare-feu envoie la requête aux serveurs DNS primaires et secondaires par défaut. Vous pouvez activer la mise en cache des domaines qui correspondent à la règle.

© 2020 Palo Alto Networks, Inc.

- **Avancé** - Vous devez activer la mise en cache (sélectionnez **Cache**) et **Cache EDNS Responses (Réponse EDNS Cache)** si l'objet proxy DNS sera utilisé pour résoudre les requêtes DNS/FQDN que le pare-feu génère. L'onglet Avancé vous permet aussi de contrôler les requêtes TCP et les nouvelles tentatives de requêtes UDP. Le pare-feu envoie des requêtes UDP DNS ou TCP par l'intermédiaire de l'interface configurée. Les requêtes UDP basculent vers TCP lorsque la réponse d'une requête DNS est trop longue pour un seul paquet UDP.

Paramètres du proxy DNS

Cliquez sur **Add (Ajouter)** et configurez le pare-feu pour qu'il agisse en tant que proxy DNS. Vous pouvez configurer jusqu'à un maximum de 256 proxys DNS sur un pare-feu.

Paramètres du proxy DNS	Configuré dans	Description
Activer	**Proxy DNS**	Sélectionnez cette option pour activer ce proxy DNS.
Name (Nom)		Saisissez un nom pour identifier un objet de proxy DNS (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)		Indiquez le système virtuel auquel l'objet de proxy DNS s'applique : • **Shared (Partagé)** : le proxy s'applique à tous les systèmes virtuels. Si vous choisissez **Shared (Partagé)**, le champ **Server Profile (Profil de serveur)** n'est pas disponible. Saisissez plutôt les objets d'adresse ou adresses IP des serveurs DNS **Primary (Principal)** et **Secondary (Secondaire)**. • Sélectionnez un système virtuel qui utilisera ce proxy DNS ; vous devez d'abord configurer un système virtuel. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**, sélectionnez un système virtuel, puis sélectionnez un **DNS Proxy (Proxy DNS)**.
Source de l'héritage (Emplacement partagé uniquement)		Sélectionnez une source de laquelle hériter des paramètres du serveur DNS par défaut. Cette méthode est couramment utilisée dans les déploiements de bureaux de filiales dans lesquels l'interface WAN du pare-feu est prise en charge par DHCP ou PPPoE.
Vérifier l'état de la source de l'héritage (Emplacement partagé uniquement)		Sélectionnez cette option pour afficher les paramètres des serveurs qui sont actuellement affectés aux interfaces client DHCP et client PPPoE. Ces paramètres peuvent inclure DNS, WINS, NTP, POP3, SMTP ou un suffixe DNS.
Principal/Secondaire (Emplacement partagé uniquement)		Spécifiez les adresses IP des serveurs DNS primaires et secondaires par défaut auxquels ce pare-feu (en tant que proxy DNS) envoie des requêtes DNS. Si le serveur DNS principal est introuvable, le pare-feu utilise le serveur DNS secondaire.

© 2020 Palo Alto Networks, Inc.

Paramètres du proxy DNS	Configuré dans	Description
Profil de serveur (Emplacement du système virtuel uniquement)		Sélectionnez ou créez un nouveau profil de serveur DNS. Ce champ ne s'affiche pas si l'emplacement des systèmes virtuels a été indiqué comme Partagé.
Interface		Vous devez **Add (Ajouter)** une interface pour qu'elle fonctionne en tant que proxy DNS. Vous pouvez ajouter plusieurs interfaces. Pour supprimer le proxy DNS de l'interface, sélectionnez-le et cliquez sur **Delete (Supprimer)**. Une interface n'est pas requise si le proxy DNS est utilisé uniquement pour la fonctionnalité d'itinéraire de service. Utilisez un itinéraire de service de destination avec un proxy DNS sans interface si vous souhaitez que l'itinéraire de service de destination définisse l'adresse IP source. Sinon, le proxy DNS sélectionne une adresse IP d'interface à utiliser comme source (lorsqu'aucun itinéraire de service DNS n'est défini).
Name (Nom)	**DNS Proxy (Proxy DNS) > DNS Proxy Rules (Règles de proxy DNS)**	Un nom est requis pour qu'une entrée puisse être référencée et modifiée via la CLI.
Activer la mise en cache des domaines résolus par ce mappage		Sélectionnez cette option pour activer la mise en cache des domaines non résolus par ce mappage.
nom de domaine		Vous devez **Ajouter** un ou plusieurs noms de domaine auxquels le pare-feu compare les FQDN entrants. Si le FQDN correspond à l'un des domaines de la règle, le pare-feu transmet la requête au serveur DNS primaire / secondaire spécifié pour ce proxy. Pour supprimer un nom de domaine, sélectionnez-le, puis cliquez sur **Supprimer**.
DNS Server Profile (profil de serveur DNS) (Emplacement partagé uniquement)		Sélectionnez ou ajoutez un profil de serveur DNS pour définir les paramètres DNS pour le système virtuel, y compris les serveurs DNS principaux et secondaires auquel le pare-feu transmet des requêtes de noms de domaine.
Principal/Secondaire (Emplacement du système virtuel uniquement)		Saisissez le nom d'hôte ou l'adresse IP des serveurs DNS principaux et secondaires auxquels le pare-feu envoie les requêtes de noms de domaine compatibles.
Name (Nom)	**DNS Proxy (Proxy DNS) > Static Entries**	Saisissez un nom pour l'entrée statique.
Nom de domaine complet		Saisissez le nom de domaine complet (FQDN) à mapper aux adresses IP statiques définies dans le champ Adresse.

© 2020 Palo Alto Networks, Inc.

Paramètres du proxy DNS	Configuré dans	Description
Adresse	**(Entrées statiques)**	Cliquez sur **Ajouter** pour ajouter une ou plusieurs adresses IP à mapper à ce domaine. Le pare-feu inclut toutes ces adresses dans sa réponse DNS et le client choisit l'adresse IP à utiliser. Pour supprimer une adresse, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Requêtes TCP	**DNS Proxy (Proxy DNS)** > **Advanced (Avancé)**	Sélectionnez cette option pour activer des requêtes DNS à l'aide de TCP. Indiquez le nombre maximum de requêtes DNS TCP en attente simultanées (**Max Pending Requests (Nombre max. de requêtes en attente)**) que le pare-feu prend en charge (plage comprise entre 64 et 256 ; par défaut 64).
Nouvelles tentatives de requêtes UDP	**DNS Proxy (Proxy DNS)** > **Advanced (Avancé)**	Spécifiez des paramètres pour les nouvelles tentatives de requête UDP : • **Interval (Intervalle)** – Temps, en secondes, après lequel le proxy DNS envoie une autre requête s'il n'a pas reçu de réponse (la plage est comprise entre 1 et 30, la valeur par défaut est 2). • **Attempts (Tentatives)** – Le nombre maximum de tentatives (hormis la première) après lesquelles le proxy DNS essaie le serveur DNS suivant (plage comprise entre 1 et 30 ; par défaut 5).
Cache	**DNS Proxy (Proxy DNS)** > **Advanced (Avancé)**	Vous devez activer la fonction **Cache** (activé par défaut) si cet objet proxy DNS est utilisé pour des requêtes que le pare-feu génère (dans la section **Device [Périphérique]** > **Setup [Configuration]** > **Services** > **DNS**, ou dans la section **Device [Périphérique]** > **Virtual Systems [Systèmes virtuels]**, vous sélectionnez un système virtuel et ensuite **General [Général]** > **DNS Proxy [Proxy DNS]**). Indiquez ensuite les options suivantes : • **Enable TTL (Activer TTL)** – Limitez la durée pendant laquelle le pare-feu met en cache les entrées DNS pour l'objet proxy. TTL est désactivé par défaut. Ensuite, saisissez la **Time to Live (sec) (Durée de vie (sec))** – le nombre de secondes après lesquelles toutes les entrées mises en cache pour l'objet proxy sont supprimées et les nouvelles requêtes DNS doivent être résolues et remises en cache. La plage est comprise entre 60 et 86 400. Il n'y a pas de TTL par défaut ; les entrées restent jusqu'à ce que le pare-feu n'ait plus de mémoire cache. • **Cache EDNS Responses (Réponses EDNS Cache)** - Vous devez activer les mécanismes d'extension de cache pour les réponses DNS (EDNS) si cet objet proxy DNS est utilisé pour les requêtes que le pare-feu génère. Le pare-feu doit pouvoir mettre en cache les réponses

© 2020 Palo Alto Networks, Inc.

Paramètres du proxy DNS	Configuré dans	Description
		DNS pour que les requêtes d'objets d'adresse FQDN réussissent.

Actions de proxy DNS supplémentaires

Après configuration du pare-feu en tant que proxy DNS, vous pouvez effectuer les actions suivantes sur la page **Network (Réseau)** > **DNS Proxy (Proxy DNS)** pour gérer les configurations du proxy DNS :

- **Modify (Modifier)** - Pour modifier un proxy DNS, cliquez sur le nom de la configuration de proxy DNS.
- **Delete (Supprimer)** - Sélectionnez une entrée de proxy DNS, cliquez sur **Delete (Supprimer)** pour supprimer la configuration de proxy DNS.
- **Disable (Désactiver)** - Pour désactiver un proxy DNS, cliquez sur le nom de l'entrée de proxy DNS et désélectionnez l'option **Activer**. Pour activer un proxy DNS qui a été désactivé, cliquez sur le nom de l'entrée de proxy DNS et sélectionnez **Enable (Activer)**.

© 2020 Palo Alto Networks, Inc.

Réseau > QoS

Les rubriques suivantes décrivent la Qualité de service (QoS).

Que voulez-vous faire ?	Reportez-vous à la section :
Définissez les limites de bande passante pour une interface et mettez en œuvre la QoS pour le trafic sortant d'une interface.	Paramètres d'une interface de QoS
Surveiller le trafic existant sur une interface sur laquelle la QoS est activée.	Statistique de l'interface QoS
Vous souhaitez en savoir plus ?	Voir Qualité de service pour avoir accès à un flux de travail QoS complet, des concepts et des cas pratiques.
	Sélectionnez Politiques > QoS pour affecter une classe QoS au trafic mis en correspondance ou sélectionnez Réseau > Profils réseau > QoS pour définir des limites de bande passante et une priorité pour un maximum de huit classes QoS.

Paramètres d'une interface de QoS

Activez la QoS sur une interface pour définir les limites de bande passante de l'interface et/ou de permettre à l'interface de mettre en œuvre la QoS pour le trafic sortant. L'activation d'une interface de QoS inclut l'association d'un profil de QoS à l'interface. La QoS est prise en charge sur les interfaces physiques et, selon le modèle de pare-feu, également sur les sous-interfaces et les interfaces Ethernet agrégées (AE). Pour savoir si la fonction QoS est prise en charge par votre modèle de pare-feu, utilisez l'outil de comparaison de produits Palo Alto Networks.

Pour commencer, vous devez **Ajouter** ou modifier une interface de QoS, puis configurer les paramètres comme décrits dans le tableau suivant.

Paramètres d'une interface de QoS	Configuré dans	Description
Nom de l'interface	**QoS Interface (Interface de QoS)** > **Physical Interface (Interface physique)**	Sélectionnez l'interface de pare-feu sur laquelle activer la QoS.
Sortie max. (Mbits/s)		Entrez le débit maximum (en Mbits/s) pour le trafic sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures).

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de QoS	Configuré dans	Description
		Bien qu'il ne s'agisse pas d'un champ obligatoire, nous recommandons de toujours définir la valeur de Egress Max (Sortie max.) d'une interface de QoS.
Activer la fonction QoS sur cette interface		Sélectionnez pour activer la QoS sur l'interface sélectionnée.
Interface de tunnel en texte clair	**QoS Interface (Interface de QoS)** > **Physical Interface (Interface Physique)** > **Default Profile (Profil par défaut)**	Sélectionnez les profils de QoS par défaut pour le trafic en texte clair et par tunnel. Vous devez définir un profil par défaut pour chacun. Pour le trafic en texte clair, le profil par défaut s'applique à l'ensemble du trafic en texte clair en tant que profil agrégé. Pour le trafic par tunnel, le profil par défaut s'applique individuellement à chaque tunnel ne disposant d'aucune attribution de profil spécifique dans la section de configuration détaillée. Pour obtenir des instructions sur la définition des profils QoS, reportez-vous à Réseau > Profils réseau > QoS.
en texte clair		
Sortie garantie (Mbits/s)	**QoS Interface (Interface de QoS)** > **Clear Text Traffic/ Tunneled Traffic (Trafic en texte clair / par tunnel)**	Saisissez la bande passante garantie pour le trafic en texte clair ou par tunnel depuis cette interface.
Sortie max. (Mbits/s)		Entrez le débit maximum (en Mbits/s) pour le trafic en texte clair ou par tunnel sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). La valeur de **Egress Max (Sortie max.)** du trafic en texte clair ou par tunnel ne doit pas dépasser la valeur de **Egress Max (Sortie max.)** de l'interface physique.
Ajouter		• Dans l'onglet **Clear Text Traffic (Trafic en texte clair)**, cliquez sur **Add (Ajouter)** pour définir la granularité supplémentaire au traitement du trafic en texte clair. Cliquez sur chaque entrée pour configurer les paramètres suivants : • **Name (Nom)** - Donnez un nom à ces paramètres afin de les identifier. • **QoS Profile (Profil de QoS)** - Sélectionnez le profil de QoS à appliquer à l'interface et au sous-réseau spécifiés. Pour obtenir des instructions sur la définition des profils QoS, reportez-vous à Réseau > Profils réseau > QoS. • **Source Interface (Interface source)** - Sélectionnez l'interface de pare-feu. • **Source Subnet (Sous-réseau source)** - Sélectionnez un sous-réseau pour limiter les paramètres au trafic provenant de cette source ou conservez la valeur **Indifférent** par défaut pour appliquer les paramètres à n'importe quel trafic de l'interface spécifiée.

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de QoS	Configuré dans	Description
		• Dans l'onglet **Tunneled Traffic (Trafic par tunnel)**, cliquez sur **Add (Ajouter)** pour appliquer un contrôle prioritaire sur l'affectation du profil par défaut de tunnels spécifiques, puis configurez les paramètres suivants : • **Tunnel Interface (Interface de tunnel)** - Sélectionnez l'interface de tunnel sur le pare-feu. • **QoS Profile (Profil de QoS)** - Sélectionnez le profil de QoS à appliquer à l'interface de tunnel spécifiée. Prenons comme exemple la configuration de deux sites, dont l'un dispose d'une connexion à 45 Mbits/s et l'autre d'une connexion T1 au pare-feu. Vous pouvez appliquer des paramètres de QoS restrictifs au site T1 afin que la connexion ne soit pas saturée, tout en autorisant des paramètres plus flexibles pour le site disposant d'une connexion à 45 Mbits/s. Pour supprimer une entrée de trafic en texte clair ou par tunnel, supprimez l'entrée et cliquez sur **Delete (Supprimer)**. Si les sections Trafic en texte clair et Trafic par tunnel ne sont pas renseignées, les valeurs définies dans la section Profil par défaut de l'onglet Interface physique sont utilisées.

Statistique de l'interface QoS

- Réseau > QoS > Statistiques

Pour une interface de QoS, sélectionnez **Statistics (Statistiques)** pour afficher les informations de bande passante, de session et d'application relatives aux interfaces de QoS.

Statistiques QoS	Description
Bande passante	Affiche les diagrammes de bande passante en temps réel pour le nœud et les classes sélectionnés. Ces informations sont mises à jour toutes les deux secondes. *les limitations Sortie max. et Sortie garantie de QoS configurées pour les classes QoS peuvent avoir une valeur légèrement différente dans l'écran Statistiques de QoS. Il s'agit d'un comportement normal qui est causé par la manière dont le moteur matériel résume les compteurs et les limites de bande passante. Il n'y a aucun problème opérationnel, car les graphiques d'utilisation de bande passante affichent les valeurs et les quantités en temps réel.*
Applications	Affiche toutes les applications actives du nœud et/ou de la classe de QoS sélectionné(e)(s).
Utilisateurs sources	Affiche tous les utilisateurs sources actifs du nœud et/ou de la classe de QoS sélectionné(e)(s).

© 2020 Palo Alto Networks, Inc.

Statistiques QoS	Description
Utilisateurs de destination	Affiche tous les utilisateurs de destination actifs du nœud et/ou de la classe de QoS sélectionné(e)(s).
Règles de sécurité	Affiche les règles de sécurité mises en correspondance et mettant en œuvre le nœud et/ou la classe de QoS.
Règles de QoS	Affiche les règles de QoS mises en correspondance et mettant en œuvre le nœud et/ou la classe de QoS.

© 2020 Palo Alto Networks, Inc.

Réseau > LLDP

LLD (Link Layer Discovery Protocol/protocole de découverte de couche liaison) fournit une méthode automatique de détection de périphériques voisins et de leurs fonctionnalités au niveau de la couche de liaison.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est-ce que LLDP ?	Présentation de LLDP
Configuration de LLDP.	Étapes de configuration de LLDP
Configuration d'un profil LLDP.	Réseau > Profils réseau > Profil LLDP
Vous souhaitez en savoir plus ?	LLDP

Présentation de LLDP

LLDP permet au pare-feu d'envoyer et de recevoir des trames Ethernet contenant des unités de données LLDP (LLDPDU) depuis et vers les voisins. Le périphérique de réception stocke les informations dans une MIB, accessible par le protocole SNMP (Simple Network Management Protocol/protocole de gestion de réseau simple). LLDP permet aux périphériques réseau de mapper leur topologie de réseau et d'apprendre les fonctionnalités des périphériques connectés. Cela facilite la résolution des problèmes, en particulier pour les déploiements de câble virtuel où le pare-feu n'est généralement pas détecté dans une topologie de réseau.

Étapes de configuration de LLDP

Pour activer LLDP sur le pare-feu, cliquez sur Modifier, puis sur **Enable (Activer)**. Vous pouvez configurer les quatre paramètres affichés dans le tableau ci-dessous, si les paramètres par défaut ne sont pas adaptés à votre environnement. Les entrées restantes du tableau décrivent l'état et les statistiques de l'homologue.

Paramètres LLDP	Configuré dans	Description
Intervalle de transmission (s)	**LLDP Général**	Précisez l'intervalle, en secondes, auquel les LLDPDU sont transmis (intervalle compris entre 1 et 3 600 ; valeur par défaut : 30).
Délai de transmission (s)		Indiquez le délai, en secondes, entre les transmissions LLDP envoyées après une modification apportée à un élément TLV (Type-Longueur-Valeur). Ce délai permet d'éviter la saturation du segment avec les LLDPDU si de nombreuses modifications réseau dépassent le nombre de modifications LLDP ou en cas de battement de l'interface. Le **Transmit Delay (délai de transmission)** doit être inférieur à **Transmit Interval (intervalle de transmission)** (intervalle compris entre 1 et 600 ; valeur par défaut : 2).

© 2020 Palo Alto Networks, Inc.

Paramètres LLDP	Configuré dans	Description
Temps d'attente multiple		Spécifiez une valeur qui est multipliée par **Transmit Interval (intervalle de transmission)** pour déterminer le temps d'attente TTL total (intervalle compris entre 1 et 100 ; valeur par défaut : 4). Le temps d'attente TTL est la durée de validité des informations de l'homologue conservées par le pare-feu. Le temps d'attente TTL maximum est de 65 535 secondes, quelle que soit la valeur du multiplicateur.
Intervalle de notification		Indiquez l'intervalle, en secondes, auquel les notifications de piège SNMP et Syslog sont transmises lorsque des modifications sont apportées à la MIB (intervalle compris entre 1 et 3 600 ; valeur par défaut : 5).
Filtre loupe	**LLDP** > **Status (État)**	Vous pouvez saisir une valeur de données dans la ligne de filtre et cliquer sur la flèche grise, pour afficher uniquement les lignes qui incluent cette valeur de données. Cliquez sur le X rouge pour effacer le filtre.
Interface		Nommez les interfaces auxquelles des profils LLDP seront affectés.
LLDP		État de LLDP : activé ou désactivé.
Mode		Mode LLDP de l'interface : Transmission/Réception, Transmission uniquement ou Réception uniquement.
Profil		Nom du profil affecté à l'interface.
Total transmis		Nombre de LLDPDU transmises de l'interface.
Transmission abandonnée		Nombre de LLDPDU non transmises de l'interface en raison d'une erreur. Par exemple, une erreur de longueur lorsque le système construit une LLDPDU pour la transmission.
Total reçu		Nombre de trames LLDP reçues sur l'interface.
TLV abandonné		Nombre de trames LLDP supprimées à la réception.
Erreurs		Nombre d'éléments TLV (Type-Longueur-Valeur) reçus sur l'interface qui contiennent des erreurs. Les types d'erreurs TLV sont les suivants : un ou plusieurs éléments TLV obligatoires sont manquants, hors service, contiennent des informations en dehors de la plage admise, ou erreur de longueur.
Non reconnu		Nombre d'éléments TLV reçus sur l'interface qui ne sont pas reconnus par l'agent LLDP local, par exemple, car le type TLV se trouve dans l'intervalle TLV réservé.

© 2020 Palo Alto Networks, Inc.

Paramètres LLDP	Configuré dans	Description
Expiré		Nombre d'éléments supprimés de la MIB de réception en raison de l'expiration du TTL.
Effacement des statistiques LLDP		Sélectionnez pour effacer toutes les statistiques LLDP.
Filtre loupe	**LLDP** > **Peers (Homologues)**	Vous pouvez saisir une valeur de données dans la ligne de filtre et cliquer sur la flèche grise, pour afficher uniquement les lignes qui incluent cette valeur de données. Cliquez sur le X rouge pour effacer le filtre.
Interface locale		Interface sur le pare-feu qui a détecté le périphérique voisin.
ID du châssis distant		ID de châssis de l'homologue ; l'adresse MAC est utilisée.
ID du port	**LLDP** > **Peers (Homologues) (suite)**	ID de port de l'homologue.
Name (Nom)		Nom de l'homologue.
En savoir plus		Cliquez sur **More Info (Plus d'informations)** pour afficher les détails de l'homologue distant, basés sur les éléments TLV obligatoires et facultatifs.
Type de châssis		Le type de châssis est l'adresse MAC.
Adresse MAC		Adresse MAC de l'homologue.
Nom du système		Nom de l'homologue.
Description du système		Description de l'homologue.
Description du port		Description du port de l'homologue.
Type de port		Nom de l'interface.
ID du port		Le pare-feu utilise l'attribut ifName de l'interface.
Fonctionnalités du système		Fonctionnalités du système. O=Other (autre), P=Repeater (répéteur), B=Bridge (pont), W=Wireless-LAN (réseau local sans fil), R=Router (routeur), T=Telephone (téléphone)
Fonctions activées		Fonctionnalités activées sur l'homologue.
Adresse de gestion		Adresse de gestion de l'homologue.

© 2020 Palo Alto Networks, Inc.

Réseau > Profils réseau

Les rubriques suivantes décrivent les profils réseau :

- Réseau > Profils réseau > Crypto IPSec GlobalProtect
- Réseau > Profils réseau > Passerelles'A0;IKE
- Réseau > Profils réseau > Crypto'A0;IPSec
- Réseau > Profils réseau > Crypto IKE
- Réseau > Profils réseau > Surveillance
- Réseau > Profils réseau > Gestion de l'interface
- Réseau > Profils réseau > Protection de zone
- Réseau > Profils réseau > QoS
- Réseau > Profils réseau > Profil LLDP
- Réseau > Profils réseau > Profil BFD
- Réseau > Profils réseau > Profil d'interface SD-WAN

Réseau > Profils réseau > Crypto IPSec GlobalProtect

La page **GlobalProtect IPSec Crypto Profiles (Profils crypto IPSec GlobalProtect)** vous permet de spécifier les algorithmes d'authentification et de chiffrement dans les tunnels VPN entre des clients et une passerelle GlobalProtect. L'ordre d'ajout des algorithmes est leur ordre d'application par le pare-feu, et peut affecter la sécurité et les performances du tunnel. Pour changer l'ordre, sélectionnez un algorithme et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**.

Pour les tunnels VPN entre les passerelles GlobalProtect et les satellites (pare-feu), voir Réseau > Profils réseau > Crypto IPSec.

Paramètres d'un profil crypto IPSec GlobalProtect	
Name (Nom)	Saisissez un nom pour identifier le profil. Le nom est sensible à la casse, doit être unique et peut comporter **31** caractères maximum. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Chiffrement	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes de chiffrement de votre choix. Pour une sécurité maximale, changez l'ordre (de haut en bas) en : **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.
Authentification	Cliquez sur **Add (Ajouter)** et sélectionnez l'algorithme d'authentification. Actuellement, la seule option est **sha1**.

Réseau > Profils réseau > Passerelles'A0;IKE

Utilisez cette pour gérer ou définir une passerelle contenant les informations de configuration nécessaires à la négociation du protocole IKE (Internet Key Exchange / échange de clés Internet) avec une passerelle homologue. Il s'agit de la phase 1 de la configuration de VPN IKE/IPSec.

Pour gérer, configurer, redémarrer ou actualiser une passerelle IKE, reportez-vous aux sections suivantes :

- Gestion de la passerelle IKE
- Passerelle IKE - Onglet Général
- Passerelle IKE - Onglet Options avancées

© 2020 Palo Alto Networks, Inc.

- Redémarrage ou actualisation d'une passerelle IKE

Gestion de la passerelle IKE

- Réseau > Profils réseau > Passerelles'A0;IKE

Le tableau suivant explique comment gérer les passerelles IKE.

Gestion des passerelles IKE	Description
Ajouter	Pour créer une nouvelle passerelle IKE, cliquez sur **Add (Ajouter)**. Voir Passerelle IKE – Onglet Général et Passerelle IKE – Onglet Options avancées pour obtenir des instructions sur la configuration de la nouvelle passerelle.
Supprimer	Pour supprimer une passerelle, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Activer	Pour activer une passerelle qui a été désactivée, sélectionnez-la et cliquez sur **Enable (Activer)**, qui est le paramètre par défaut.
Désactivation	Pour désactiver une passerelle, sélectionnez-la et cliquez sur **Disable (Désactiver)**.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau de configuration de l'objet au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Passerelle IKE - Onglet Général

- Réseau > Profils réseau > Passerelles IKE > Général

Le tableau suivant décrit les premiers paramètres de configuration d'une passerelle IKE. IKE est la phase 1 du processus de configuration de VPN IKE/IPSec. Après avoir configuré ces paramètres, reportez-vous à la section Onglet Options avancées de passerelle IKE.

Paramètres généraux d'une passerelle IKE	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier la passerelle (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Version	Sélectionnez la version IKE que la passerelle prend en charge et doit accepter d'utiliser avec la passerelle homologue : **IKEv1 only mode (Mode IKEv1 uniquement)**, **IKEv2 only mode (Mode IKEv2 uniquement)** ou **IKEv2 preferred mode (Mode IKEv2 préféré)**. Le mode IKEv2 préféré entraîne la négociation IKEv2 par la passerelle, et c'est ce mode qu'elles

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'une passerelle IKE	Description
	utiliseront si la passerelle homologue prend également en charge IKEv2 ; sinon, la passerelle revient à IKEv1.
Type d'adresse	Sélectionnez le type d'adresse IP que la passerelle utilise. **IPv4** ou **IPv6**.
Interface	Spécifiez l'interface de tunnel VPN sortante sur le pare-feu.
Adresse IP locale	Sélectionnez ou saisissez l'adresse IP de l'interface locale correspondant au point d'extrémité du tunnel.
Adresse IP de l'homologue Type	Sélectionnez l'un des paramètres suivants et saisissez les informations correspondantes de l'homologue : • **Dynamic (Dynamique)** : sélectionnez cette option si l'adresse IP ou la valeur FQDN de l'homologue est inconnue. Lorsque le type d'adresse IP de l'homologue est défini sur Dynamique, il revient à l'homologue de lancer la négociation de la passerelle IKE. • **IP** : saisissez la **Peer Address (Adresse de l'homologue)** en tant qu'adresse IPv4 ou IPv6 ou qu'objet d'adresse correspondant à une adresse IPv4 ou IPv6. • **FQDN** : saisissez la **Peer Address (Adresse de l'homologue)** sous forme de FQDN ou d'objet d'adresse utilisant un FQDN. Si vous saisissez un FQDN ou un objet d'adresse FQDN qui se résout en plus d'une adresse IP, le pare-feu choisit l'adresse préférée dans l'ensemble d'adresses qui correspondent au Type d'adresse (IPv4 ou IPv6) de la passerelle IKE, comme suit : • Si aucune Security Association (association de sécurité ; SA) IKA n'a été négotiée, l'adresse préférée correspond à l'adresse IP qui possède la plus faible valeur. • Si une adresse est utilisée par la passerelle IKE et qu'elle figure dans l'ensemble d'adresses renvoyées, celle-ci est utilisée (qu'elle possède la plus faible valeur ou non). • Si une adresse est utilisée par la passerelle IKE, mais qu'elle ne figure pas dans l'ensemble d'adresses renvoyées, une nouvelle adresse est sélectionnée : celle qui possède la plus faible valeur.  *L'utilisation d'un FQDN ou d'un objet d'adresse FQDN réduit les problèmes d'environnements où l'homologue est soumis aux changements des adresses IP dynamiques (ce qui autrement vous obligerez à reconfigurer l'adresse de cette passerelle IKE homologue).*
Authentification	Sélectionnez le type d'authentification : **Pre-Shared Key (Clé prépartagée)** ou **Certificate (Certificat)**) qui se produira sur la passerelle homologue. En fonction de la sélection, voir Champs de Clé prépartagée ou Champs de certificat.
Champs de l'option Clé prépartagée	

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'une passerelle IKE	Description
Clé prépartagée / Confirmer la clé prépartagée	Si vous sélectionnez **Pre-Shared Key (Clé prépartagée)**, saisissez une clé de sécurité unique à utiliser pour l'authentification symétrique via le tunnel. La valeur de la **Pre-Shared Key (Clé prépartagée)** est une chaîne créée par l'administrateur à l'aide d'un maximum de 255 caractères ASCII ou autres. Générez une clé difficile à décoder par des attaques par dictionnaire ; utilisez un générateur de clés prépartagées, si nécessaire.
Identification locale	Définit le format et l'identification de la passerelle locale, qui sont utilisés avec la clé prépartagée pour l'établissement d'une SA IKEv1 de phase 1 et d'une SA IKEv2. Sélectionnez l'un des types suivants et saisissez une valeur : **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)**, **KEYID** (chaîne d'ID au format binaire hexadécimal), **FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail). Si vous n'indiquez aucune valeur, la passerelle utilisera l'adresse IP locale comme valeur de **Local Identification (Identification locale)**.
Identification de l'homologue	Définit le type et l'identification de la passerelle homologue, qui sont utilisés avec la clé prépartagée lors de l'établissement d'une SA IKEv1 de phase 1 et d'une SA IKEv2. Sélectionnez l'un des types suivants et saisissez une valeur : **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)**, **KEYID** (chaîne d'ID au format binaire hexadécimal), **FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail). Si vous n'indiquez aucune valeur, la passerelle utilisera l'adresse IP de l'homologue comme valeur de **Peer Identification (Identification de l'homologue)**.
Champs de l'option Certificat	
Certificat local	Si l'option **Certificate (Certificat)** est sélectionnée comme type d'**Authentication (Authentification)**, choisissez un certificat qui est déjà sur le pare-feu dans la liste déroulante. Sinon, vous pouvez **Import (Importer)** un certificat ou **Generate (Générer)** un nouveau certificat, comme suit : **Import (Importer)** : • **Certificate Name (Nom du certificat)** - Saisissez un nom pour le certificat que vous importez. • **Shared (Partagé)** - Sélectionnez cette option si le certificat sera partagé par plusieurs systèmes virtuels. • **Certificate File (Fichier de certificat)** - Cliquez sur **Browse (Parcourir)** pour accéder à l'emplacement où se trouve le fichier de certificat. Cliquez sur le fichier et sélectionnez **Open (Ouvrir)**. • **File Format (Format de fichier)** - Sélectionnez l'un des formats suivants : • **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))** - Contient le certificat mais pas la clé. Texte en clair.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'une passerelle IKE	Description
	• **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** - Contient le certificat et la clé. • **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)** - Sélectionnez cette option si le pare-feu est un client d'un serveur de module de sécurité matériel où la clé réside. • **Import private key (Importer la clé privée)** - Sélectionnez cette option si une clé privée sera importée car celle-ci se trouve dans un autre fichier que le fichier de certificat. • **Key File (Fichier de clé)** - Cliquez sur Parcourir et accédez au fichier de clé à importer. Cette entrée est disponible si vous avez choisi PEM comme format de fichier. • **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmer la phrase secrète)** - Saisissez-la pour accéder à la clé.
Certificat local (suite)	**Generate (Générer)** : • **Certificate Name (Nom du certificat)** - Saisissez un nom pour le certificat que vous créez. • **Common Name (Nom commun)** - Saisissez le nom commun, qui est l'adresse IP ou le nom de domaine complet à apparaître sur le certificat. • **Shared (Partagé)** - Sélectionnez cette option si le certificat sera partagé par plusieurs systèmes virtuels. • **Signed By (Signé par)** - Sélectionnez Autorité externe (demande de signature de certificat) ou saisissez l'adresse IP du pare-feu. Cette entrée doit être une autorité de certification. • **Certificate Authority (Autorité de certification)** - Sélectionnez cette option si le pare-feu est l'autorité de certification racine. • **OCSP Responder (Répondeur OCSP)** – Saisissez le répondeur OSCP qui suit si le certificat est valide ou révoqué. • **Algorithm (Algorithme)** - Sélectionnez RSA ou ECDSA pour générer la clé du certificat. • **Number of Bits (Nombre de bits)** - Sélectionnez 512, 1024, 2048 ou 3072 comme nombre de bits de la clé. • **Digest (Résumé)** - Sélectionnez md5, sha1, sha256, sha384, ou sha512 comme méthode pour rétablir la chaîne à partir du hachage. • **Expiration (days) (Expiration (jours))** - Saisissez le nombre de jours pendant lequel le certificat est valide. • **Certificate Attributes (Attributs du certificat)** : **Type** - Vous pouvez éventuellement sélectionner des types d'attributs de certificat supplémentaires dans la liste déroulante. • **Value (Valeur)** - Saisissez une valeur pour l'attribut.
Échange des certificats HTTP	Cliquez sur **HTTP Certificate Exchange (Échange des certificats HTTP)** et saisissez le **Certificate URL (URL du certificat)** afin d'utiliser la méthode Hachage et URL pour informer l'homologue de l'emplacement du certificat. L'URL du certificat est l'URL du serveur distant où vous stockez votre certificat.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'une passerelle IKE	Description
	Si l'homologue indique qu'il prend également en charge la méthode Hachage et URL, les certificats sont alors échangés via le hachage SHA1 et l'échange d'URL. Lorsque l'homologue reçoit les données utiles du certificat IKE, il voit l'URL HTTP et récupère le certificat sur ce serveur. L'homologue utilise ensuite le hachage spécifié dans les données utiles du certificat pour vérifier les certificats téléchargés sur le serveur HTTP.
Identification locale	Identifie comment l'homologue local est identifié dans le certificat. Sélectionnez l'un des types suivants et saisissez une valeur : **Distinguished Name (Nom unique)** (objet), **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)** ou **User FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail).
Identification de l'homologue	Identifie comment l'homologue distant est identifié dans le certificat. Sélectionnez l'un des types suivants et saisissez une valeur : **Distinguished Name (Nom unique)** (objet), **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)** ou **User FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail).
Vérification de l'ID de l'homologue	Sélectionnez **Exact** ou **Wildcard (Caractère générique)**. Ce paramètre s'applique à l'identification de l'homologue qui est examinée pour valider le certificat. Par exemple, si l'Identification de l'homologue est un nom égal à domain.com, vous sélectionnez l'option **Exact**, et si le nom qui figure dans les données utiles du certificat IKE est .domain2.com, la négociation IKE échouera. Mais si vous avez sélectionnez l'option **Wildcard (Caractère générique)**, alors seuls les caractères qui figurent dans la chaîne Nom avant l'astérisque (*) doivent correspondre et tout caractère après l'astérisque peut différer.
Autoriser la non-correspondance de l'identification d'homologue et de l'identification des données utiles du certificat	Sélectionnez si vous souhaitez avoir la possibilité d'une SA IKE réussie même si l'identification de l'homologue ne correspond pas aux données utiles du certificat.
Profil du certificat	Sélectionnez ou créer un nouveau **Certificate Profile (Profil de certificat)** qui configure les options de certificat s'appliquant au certificat que la passerelle locale envoie à la passerelle homologue. Voir Périphérique > Gestion des certificats > Profil de certificat.
Activer la validation stricte de l'utilisation de la clé étendue de l'homologue	Sélectionnez si vous souhaitez contrôler strictement l'utilisation de la clé.

© 2020 Palo Alto Networks, Inc.

Passerelle IKE - Onglet Options avancées

- Réseau > Profils réseau > Passerelles IKE > Options avancées

Configurez les paramètres avancés de la passerelle IKE tels que le mode passif, le parcours NAT et les réglages IKEv1 comme la détection des homologues qui ne répondent pas.

Options avancées d'une passerelle IKE	Description
Activer le mode passif	Sélectionnez cette option pour que le pare-feu réponde uniquement aux connexions IKE sans jamais les initier.
Activer le parcours NAT	Sélectionnez cette option pour utiliser l'encapsulation UDP sur les protocoles IKE et UDP, en les autorisant à passer par des périphériques NAT intermédiaires. Activez le parcours NAT si la traduction d'adresses réseau (NAT) est configurée sur un périphérique entre les points de terminaison VPN IPSec.
Onglet'A0;IKEv1	
Mode d'échange	Sélectionnez **auto (automatique)**, **aggressive (agressif)** ou **main (principal)**. En mode **auto (automatique)** (le mode par défaut), le périphérique peut accepter des demandes de négociation en mode **main (principal)** et en mode **aggressive (agressif**. Toutefois, chaque fois que cela est possible, il initie une négociation et autorise des échanges en mode **main (principal)**. Vous devez configurer le périphérique homologue avec le même mode d'échange afin qu'il puisse accepter des demandes de négociation initiées à partir du premier périphérique.
Profil crypto IKE	Sélectionnez un profil existant, conservez le profil par défaut ou créez un nouveau profil. Les profils sélectionnés pour IKEv1et IKEv2 peuvent différer. Pour plus d'informations sur les profils Crypto IKE, voir Réseau > Profils réseau > Crypto IKE.
Activer la fragmentation	Sélectionnez cette option pour autoriser la passerelle locale à recevoir des paquets IKE fragmentés. La taille maximale des paquets fragmentés est de 576 octets.
Détection des homologues arrêtés	Cochez cette case pour activer cette option, puis saisissez un intervalle (2-100 secondes) et un délai avant toute nouvelle tentative (2-100 secondes). La détection des homologues arrêtés identifie les homologues IKE inactifs ou indisponibles et permet de restaurer des ressources perdues en cas d'indisponibilité d'un homologue.
Onglet IKEv2	
Profil crypto IKE	Sélectionnez un profil existant, conservez le profil par défaut ou créez un nouveau profil. Les profils sélectionnés pour IKEv1et IKEv2 peuvent différer.

© 2020 Palo Alto Networks, Inc.

Options avancées d'une passerelle IKE	Description
	Pour plus d'informations sur les profils Crypto IKE, voir Réseau > Profils réseau > Crypto IKE.
Validation stricte du cookie	Cochez cette case pour activer l'option **Strict Cookie Validation (Validation stricte du cookie)** sur la passerelle IKE. • Lorsque vous activez l'option **Strict Cookie Validation (Validation stricte du cookie)**, la validation du cookie IKEv2 est toujours mise en œuvre ; l'initiateur doit envoyer un message IKE_SA_INIT contenant un cookie. • Lorsque vous désactivez l'option **Strict Cookie Validation (Validation stricte du cookie)** (le paramètre par défaut), le système compare le nombre de SA à moitié ouvertes au **Cookie Activation Threshold (Seuil d'activation du cookie)**, qui est un paramètre des sessions VPN. Si le nombre de SA à moitié ouvertes dépasse le **Cookie Activation Threshold (Seuil d'activation du cookie)**, l'initiateur doit envoyer un message IKE_SA_INIT contenant un cookie.
Vérification de l'activité	L'option **Liveness Check (Vérification de l'activité)** IKEv2 est toujours activée ; tous les paquets IKEv2 permettent d'effectuer une vérification de l'activité. Cochez cette case pour que le système envoie des paquets d'information vides après que l'homologue a été inactif pendant un nombre de secondes spécifié. Plage entre 2 et 100. Par défaut : 5. Si nécessaire, le côté qui essaie d'envoyer des paquets IKEv2 effectue la vérification d'activité 10 fois maximum (tous les paquets IKEv2 sont pris en compte dans le paramètre de retransmission). S'il ne reçoit aucune réponse, l'expéditeur ferme et supprime les IKE_SA et CHILD_SA. L'expéditeur envoie un autre message IKE_SA_INIT.

Redémarrage ou actualisation d'une passerelle IKE

- Réseau > Tunnels'A0;IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour afficher l'état des tunnels. Dans la deuxième colonne Statut se trouve un lien vers les Informations IKE. Cliquez sur la passerelle que vous souhaitez redémarrer ou actualiser. La page Informations IKE s'ouvre. Cliquez sur l'une des entrées de la liste, puis sur :

- **Restart (Redémarrer)** – Redémarre la passerelle sélectionnée. Un redémarrage interrompt le trafic passant à travers le tunnel. Les comportements de redémarrage sont différents pour IKEv1 et IKEv2, comme suit :
  - **IKEv1** - Vous pouvez redémarrer (effacer) une SA de phase 1 ou de phase 2 de façon indépendante. Seule cette SA est affectée.
  - **IKEv2** - Entraîne l'effacement de toutes les SA enfants (tunnels IPSec) lorsque la SA IKEv2 est redémarrée.

    Si vous redémarrez la SA IKEv2, tous les tunnels IPSec sous-jacents sont également effacés.

    Si vous redémarrez le tunnel IPSec (SA enfant) associé à une SA IKEv2, le redémarrage n'affecte pas la SA IKEv2.
- **Refresh (Rafraichir)** – Affiche le statut actuel de la SA IKE.

© 2020 Palo Alto Networks, Inc.

Réseau > Profils réseau > Crypto'A0;IPSec

Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)** pour définir des protocoles Crypto IPSec qui indiquent les protocoles et les algorithmes pour l'identification, l'authentification et le cryptage dans les tunnels VPN en fonction de la négociation SA IPSec (Phase 2).

Pour les tunnels VPN entre les passerelles GlobalProtect et les clients, voir Réseau > Profils réseau > Crypto IPSec GlobalProtect.

Paramètres d'un profil crypto IPSec	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier le profil (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Protocole IPSec	Sélectionnez un protocole pour sécuriser les données qui traversent le tunnel VPN : • **ESP** - Le protocole ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile) crypte les données, authentifie la source et vérifie l'intégrité des données. • **AH** - Le protocole AH (Authentication Header/En-tête d'authentification) authentifie la source et vérifie l'intégrité des données. *Utilisez le protocole ESP, car il assure la confidentialité de la connexion (chiffrement) et procure l'authentification.*
Chiffrement (protocole ESP uniquement)	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes de chiffrement de votre choix. Pour une sécurité optimale, utilisez **Move Up (Déplacer vers le haut)** et **Move Down (Déplacer vers le bas)** pour modifier l'ordre (du haut vers le bas) comme suit : **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (le pare-feu VM-Series ne prend pas en charge cette option), **aes-128-cbc**, **3des** et **des**. Vous pouvez également sélectionner **null (aucun)** (aucun chiffrement). *Utilisez une forme de chiffrement AES. (Les algorithmes DES et 3DES sont faibles et vulnérables.)*
Authentification	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes d'authentification de votre choix. Pour une sécurité maximale, utilisez **Move Up (Monter)** ou **Move Down (Descendre)** afin d'obtenir l'ordre (de haut en bas) suivant : **sha512**, **sha384**, **sha256**, **sha1**, **md5**. Si le **protocole IPSec** est **ESP**, vous pouvez également sélectionner **none (aucune)** (aucune authentification). *Utilisez sha256 ou une authentification plus forte, car md5 et sha1 ne sont pas sûrs. Utilisez sha256 pour les sessions de courte durée et sha384 ou plus pour le trafic qui exige l'authentification la plus sécuritaire, comme les transactions financières.*

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil crypto IPSec	Description
Groupe DH	Sélectionnez le groupe DH Diffie-Hellman pour IKE (Internet Key Exchange/échange de clés Internet) : **group1 (groupe1)**, **group2 (groupe2)**, **group5 (groupe5)**, **group14 (groupe14)**, **group19 (groupe19)** ou **group20 (groupe20)**. Pour une sécurité maximale, choisissez le groupe dont le nombre est le plus élevé. Si vous ne souhaitez pas renouveler la clé créée par le pare-feu lors de la négociation IKE de phase 1, sélectionnez **no-pfs (Mode PFS (Perfect Forward Secrecy) désactivé)** ; le pare-feu réutilise la clé actuelle pour les négociations SA IPSec.
Durée de vie	Sélectionnez les unités et saisissez la durée (le paramètre par défaut est une heure) pendant laquelle la clé négociée restera active.
Taille réelle	Sélectionnez des unités facultatives et saisissez la quantité de données qu'une clé peut utiliser pour le chiffrement.

Réseau > Profils réseau > Crypto IKE

Utilisez la page **IKE Crypto Profiles (Profils crypto IKE)** pour définir des protocoles et des algorithmes pour l'identification, l'authentification et le cryptage (IKEv1 ou IKEv2, Phase 1).

Pour modifier l'ordre d'affichage d'un algorithme ou d'un groupe, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**. L'ordre détermine le premier choix lors de la négociation des paramètres avec un homologue distant. Un essai du paramètre situé en tête de liste est réalisé en premier, puis en descendant dans la liste jusqu'à ce qu'un essai soit réussi.

Paramètres d'un profil crypto IKE	Description
Name (Nom)	Saisissez un Name (Nom) pour le profil.
Groupe DH	Indiquez la priorité des groupes Diffie-Hellman (DH). Cliquez sur **Add (Ajouter)** et sélectionnez des groupes : **group1 (groupe1)**, **group2 (groupe2)**, **group5 (groupe5)**, **group14 (groupe14)**, **group19 (groupe19)** ou **group20 (groupe20)**. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)** pour déplacer les groupes dont les identifiants numériques sont les plus élevés en tête de liste. Par exemple, déplacez **group14 (groupe14)** au-dessus de **group2 (groupe2)**.
Authentification	Indiquez la priorité des algorithmes de hachage. Cliquez sur **Add (Ajouter)** et sélectionnez des algorithmes. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)** afin d'obtenir l'ordre (de haut en bas) suivant : **sha512**, **sha384**, **sha256**, **sha1**, **md5**.
Chiffrement	Sélectionnez les options appropriées d'authentification ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile). Cliquez sur **Add (Ajouter)** et sélectionnez des algorithmes. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move**

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil crypto IKE	Description
	Down (Descendre) afin d'obtenir l'ordre (de haut en bas) suivant : **aes-256-cbc**, **aes-192-cbc**, **aes-128-cbc**, **3des**, **des**.
Durée de vie de la clé	Sélectionnez l'unité de temps et saisissez la durée pendant laquelle la clé IKE de phase 1 négociée sera effective. • IKEv2 - Avant que la durée de vie de la clé expire, la SA doit être renouvelée ou sinon, lors de l'expiration, la SA doit démarrer une nouvelle négociation de clé de phase 1. • IKEv1 - Le renouvellement de clé de phase 1 n'est pas effectué de manière active avant l'expiration. Le renouvellement de clé de phase 1 IKEv1 est déclenché uniquement lors de l'expiration de la SA IPSec IKEv1.
Authentification à facteurs multiples IKEv2	Spécifiez une valeur (intervalle : 0-50, valeur par défaut : 0) qui est multipliée par la durée de vie de la clé pour déterminer le nombre d'authentifications. Le nombre d'authentifications est le nombre de fois que la passerelle peut effectuer un renouvellement de clé SA IKE IKEv2 avant la réauthentification IKEv2. Une valeur de 0 désactive la fonction de réauthentification.

Réseau > Profils réseau > Surveillance

Un profil de surveillance permet de surveiller des tunnels IPSec et le périphérique du saut suivant dans le cadre de règles de transfert basé sur une politique (PBF). Dans les deux cas, le profil de surveillance permet de définir une action à appliquer lorsqu'une ressource (tunnel IPSec ou périphérique d'un saut suivant) devient indisponible. Les profils de surveillance sont facultatifs, mais peuvent être très utiles pour maintenir la connectivité entre des sites et s'assurer que les règles'A0;PBF sont également maintenues. Les paramètres suivants permettent de configurer un profil de surveillance.

Champ	Description
Name (Nom)	Saisissez un nom pour identifier le profil de surveillance (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Action (Action)	Indiquez une action à appliquer en cas d'indisponibilité du tunnel. Si le seuil du nombre de pulsations est perdu, le pare-feu applique l'action définie. • **wait-recover (en attente de récupération)** - Attendez que le tunnel récupère ; n'appliquez aucune action supplémentaire. Les paquets vont continuer à être envoyés conformément à la règle PBF. • **fail-over (basculement)** - Le trafic va basculer vers un chemin de secours, à condition qu'il soit disponible. Le pare-feu utilise la recherche de tables de routage afin de déterminer le routage à appliquer pendant toute la durée de cette session. Dans les deux cas, le pare-feu essaie de négocier de nouvelles clés IPSec afin d'accélérer la récupération.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Intervalle	Indiquez un délai entre les pulsations (intervalle compris entre 2 et 10, valeur par défaut : 3).
Seuil	Indiquez le nombre de pulsations devant être perdues avant que le pare-feu n'applique l'action définie (intervalle est compris entre 2 et 10 ; la valeur par défaut est 5).

Réseau > Profils réseau > Gestion de l'interface

Un profil de gestion de l'interface protège le pare-feu contre un accès non autorisé en définissant les services et les adresses IP qu'une interface du pare-feu autorise. Vous pouvez assigner un profil de gestion aux interfaces Ethernet de couche 3 (y compris les sous-interfaces) et aux interfaces logiques (groupe d'interfaces agrégées, interfaces VLAN, interfaces en boucle et interfaces de tunnel). Pour assigner un profil de gestion de l'interface, reportez-vous à la section Réseau > Interfaces.

N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface qui autorise l'accès aux zones sécurisées de votre entreprise depuis l'Internet ou d'autres zones non sécurisées. Il s'agit entre autres de l'interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect ; GlobalProtect n'a pas besoin d'un profil de gestion de l'interface pour autoriser l'accès au portail ou à la passerelle. Reportez-vous à la section Pratiques exemplaires pour sécuriser l'accès administratif *pour obtenir des précisions sur la manière de protéger l'accès à vos pare-feu et à Panorama.*

N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l'interface de gestion à l'Internet.

Champ	Description
Name (Nom)	Saisissez un nom pour le profil (**31** caractères maximum). Ce nom apparaît dans la liste des profils des Interface de gestion lors de la configuration d'interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Services de gestion administrative	• **Telnet** - Utilisez cette fonction pour accéder à la CLI du pare-feu. Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. *Activez le protocole SSH plutôt que le protocole de Telnet pour le trafic de gestion sur l'interface.* • **SSH** - Utilisez ce protocole pour obtenir un accès sécurisé à la CLI du pare-feu. • **HTTP** - Utilisez ce protocole pour accéder à l'interface Web du pare-feu. HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS. *Activez le protocole HTTPS plutôt que le protocole HTTP pour le trafic de gestion sur l'interface.*

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• **HTTPS** - Utilisez ce protocole pour obtenir un accès sécurisé à l'interface Web du pare-feu.
Services du réseau	• **Ping** - Utilisez cette fonction pour tester la connectivité avec des services externes. Par exemple, vous pouvez envoyer un ping à l'interface pour vérifier qu'elle reçoit les mises à jour logicielles et de contenu de PAN-OS du serveur de mises à jour Palo Alto Networks. • **HTTP OCSP** - Utilisez ce protocole pour configurer le pare-feu en tant que répondeur du protocole OCSP (Online Certificate Status Protocol). Pour plus d'informations, voir Périphérique > Gestion des certificats > Répondeur OCSP. • **SNMP** - Utilisez ce protocole pour traiter les requêtes de statistiques du pare-feu à partir d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **Response Pages (Pages de réponse)** - Utilisez cette fonction pour activer des pages de réponse du portail captif. • **Captive Portal (Portail captif)** - Les ports utilisés pour fournir les pages de réponses du portail captif sont laissées ouverts sur les interfaces de couche 3 : le port 6080 pour NTLM, 6081 pour le portail captif sans profil de serveur SSL/TLS et 6082 pour le portail captif avec un profil de serveur SSL/TLS. Pour plus d'informations, reportez-vous à la section Périphérique > Identification des utilisateurs > Paramètres du portail captif. • **URL Admin Override (Contrôle prioritaire de l'URL par l'administrateur)** – Pour plus d'informations, voir Périphérique > Configuration > Content-ID. • **User-ID** – Utilisez pour activer la redistribution des mappages d'utilisateurs sur les pare-feu. • **User-ID Syslog Listener-SSL (Écouteur Syslog User-ID-SSL)** - Est utilisé pour permettre à l'agent User-ID intégré à PAN-OS de recueillir les messages Syslog via SSL. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés. • **User-ID Syslog Listener-UDP (Écouteur Syslog User-ID-UDP)** - Est utilisé pour permettre à l'agent User-ID intégré à PAN-OS de recueillir les messages Syslog via UDP. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés.
Adresses IP autorisées	Saisissez la liste d'adresses IPv4 ou IPv6 à partir desquelles le pare-feu autorise l'accès.

Réseau > Profils réseau > Protection de zone

Un Profil de protection de zone appliqué à une zone offre une protection contre les attaques par saturation et les attaques de reconnaissance les plus fréquentes, les autres attaques basées sur les paquets et l'utilisation de protocoles non IP. Celui-ci est conçu pour fournir une protection renforcée de la zone d'entrée (la zone où le trafic entre sur le pare-feu) ; il ne permet pas de protéger un hôte spécifique ou du trafic vers une zone de destination particulière. Vous pouvez attacher un profil de protection de zone à une zone.

© 2020 Palo Alto Networks, Inc.

Appliquez un profil de protection de zone à chaque zone pour ajouter des couches de protection supplémentaire contre les attaques par saturation, les attaques de reconnaissance, les attaques basées sur les paquets et les attaques par utilisation de protocoles non IP. La protection de zone sur le pare-feu doit être une deuxième couche de protection après un périphérique DDoS dédié au périmètre Internet.

Pour améliorer les fonctions de protection de zone sur le pare-feu, configurez une politique de protection DoS (Politiques > Protection DoS) pour la mise en correspondance avec une zone, une interface, une adresse IP ou un utilisateur spécifique.

La protection de zone est uniquement mise en œuvre lorsque le paquet ne correspond à aucune session existante, car la protection de zone est basée sur de nouvelles connexions par seconde (cps) et non sur des paquets par seconde (pps). Dans le cas contraire, le paramètre de protection de zone est ignoré.

Que voulez-vous faire ?	Reportez-vous à la section :
Comment puis-je créer un profil de Protection de zone ?	Blocs de construction des profils de protection de zone Protection contre la saturation Protection contre la reconnaissance Protection contre les attaques basées sur les paquets Protection du protocole

Blocs de construction des profils de protection de zone

Pour créer un profil de Protection de zone, il faut **Ajouter** un profil et lui donner un nom.

Paramètres d'un profil de protection de zone	Configuré dans	Description
Name (Nom)	**Network (Réseau) > Network Profiles (Profils réseaux) > Zone Protection (Protection de zone)**	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste des profils de Protection de Zone lors de la configuration des zones. Celui-ci est sensible à la casse et doit être unique. Vous pouvez uniquement utiliser des lettres, des nombres, des espaces et des caractères de soulignement.
Description		Saisissez une description facultative du profil de Protection de Zone.

Continuez la création d'un profil de Protection de zone en configurant toutes les combinaisons de paramètres qui correspondent aux types de protections dont votre zone a besoin :

- Protection contre la saturation
- Protection contre la reconnaissance
- Protection contre les attaques basées sur les paquets
- Protection du protocole

© 2020 Palo Alto Networks, Inc.

Si vous disposez d'un environnement de systèmes virtuels multiples et que vous avez activé'A0;:

- *Les zones externes pour permettre la communication entre les systèmes virtuels'A0;;*
- *Les passerelles partagées pour permettre aux systèmes virtuels de partager une interface commune et une adresse IP unique pour les communications externes'A0;;*

Les mécanismes de protection de Zone et DoS suivants seront désactivés dans la zone externe :

- *Cookies SYN*
- *Fragmentation IP*
- *ICMPv6*

Pour activer la fragmentation IP et la protection ICMPv6 pour la passerelle partagée, vous devez créer un profil de Protection de zone distinct pour la passerelle partagée.

Pour protéger la passerelle partagée contre la saturation SYN, vous pouvez appliquer un profil de protection contre la saturation SYN avec l'abandon anticipé aléatoire ou les cookies SYN ; dans une zone externe, seule l'abandon anticipé aléatoire est disponible pour la protection contre la saturation SYN.

Protection contre la saturation

- Réseau > Profils réseau > Protection de zone > Protection contre la saturation

Configurez un profil qui fournit une protection contre la saturation relative aux paquets SYN, ICMP, ICMPv6, SCTP INIT et UDP, ainsi qu'une protection contre la saturation provenant d'autres types de paquets IP. Les taux correspondent à des connexions par seconde ; par exemple, un paquet SYN entrant qui ne correspond par à une session existante est considéré comme une nouvelle connexion.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
SYN	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)**	Sélectionnez cette option pour activer la protection contre les saturations SYN.
Action (Action)		Sélectionnez l'action à appliquer en réponse à une attaque par saturation SYN. • **Random Early Drop (RED)** - Supprime des paquets SYN afin d'atténuer une attaque par saturation : • Lorsque le flux dépasse le seuil du taux **Alert (Alerte)**, une alarme est générée. • Lorsque le flux dépasse le seuil du taux **Activate (Activation)**, le pare-feu supprime des paquets SYN individuels de façon aléatoire afin de restreindre le flux. • Lorsque le flux dépasse le seuil du taux **Maximum**, 100 % des paquets SYN entrants sont supprimés.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		• **SYN Cookies (Cookies SYN)** – Ils permettent au pare-feu d'agir comme un proxy, interceptent le SYN, génèrent un cookie au nom du serveur vers lequel le SYN a été dirigé et envoient un SYN-ACK avec le cookie à la source d'origine. C'est uniquement lorsque la source renvoie un ACK avec le cookie au pare-feu que ce dernier considère la source valide et renvoie le SYN au serveur. Cette Action est recommandée. *Le trafic légitime traite les cookies SYN équitablement, mais consomme plus de ressources du pare-feu que RED. Si les syncookies consomment trop de ressources, basculez sur RED. Si vous ne disposez pas d'un périphérique de prévention DDoS devant le pare-feu (au périmètre Internet), utilisez toujours RED.*
Taux d'alarmes (connexions/s)	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Saisissez le nombre de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme. Vous pouvez consulter ces alarmes sur le Tableau de bord et dans le journal des menaces (Surveillance > Capture de paquets). Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. La meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.
Activer (connexions/s)		Saisissez le nombre de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche l'Action spécifiée dans ce Profil de protection de zone. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets SYN si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. Il est recommandé de définir le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
Maximum (connexions/s)		Saisissez le nombre maximum de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. Franchir le seuil bloque de nouvelles connexions jusqu'à ce que le taux de CPS repasse sous le seuil. Il est recommandé de définir le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.
ICMP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations ICMP.
Taux d'alarmes (connexions/s)		Saisissez le nombre de demandes d'écho ICMP (pings ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. La meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.
Activer (connexions/s)		Saisissez le nombre de paquets ICMP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets ICMP subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets ICMP si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. Il est recommandé de définir le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum de paquets ICMP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		Il est recommandé de définir le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.
SCTP INIT	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre la saturation des paquets de Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) qui contiennent un bloc d'initiation (INIT). Un bloc INIT ne peut être groupé avec d'autres blocs ; le paquet est alors appelé paquet SCTP INIT.
Taux d'alarmes (connexions/s)		Saisissez le nombre de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent une alarme contre les attaques. La plage est comprise entre 0 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est la suivante : • **PA-5280** : 10 000 • **PA-5260** : 7 000 • **PA-5250** : 5 000 • **PA-5220** : 3 000 • **VM-700** : 1 000 • **VM-500** : 500 • **VM-300** : 250 • **VM-100** : 200 • **VM-50** : 100
Activer (connexions/s)		Saisissez le nombre de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets SCTP INIT subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets SCTP INIT si le taux entrant descend sous le seuil d'Activation. La valeur doit être comprise entre 1 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est identique à la valeur par défaut du taux d'alarmes.
Maximum (connexions/s)	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection**	Saisissez le nombre maximum de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La valeur doit être comprise

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
	de zone) > **Flood Protection (Protection contre la saturation)** (suite)	entre 1 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est la suivante : • **PA-5280** : 20 000 • **PA-5260** : 14 000 • **PA-5250** : 10 000 • **PA-5220** : 6 000 • **VM-700** : 2 000 • **VM-500** : 1 000 • **VM-300** : 500 • **VM-100** : 400 • **VM-50** : 200
UDP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations UDP.
Taux d'alarmes (connexions/s)		Saisissez le nombre de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. La meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.
Activer (connexions/s)		Saisissez le nombre de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent la suppression aléatoire de paquets UDP. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets UDP si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. Il est recommandé de définir le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		Il est recommandé de définir le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.
ICMPv6	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations ICMPv6.
Taux d'alarmes (connexions/s)		Saisissez le nombre de demandes d'écho ICMPv6 (pings ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. La meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.
Activer (connexions/s)		Saisissez le nombre de paquets ICMPv6 (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets ICMPv6 subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets ICMPv6 si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. Il est recommandé de définir le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum de paquets ICMPv6 (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. Il est recommandé de définir le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.
Autre IP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone**	Sélectionnez pour activer la protection contre d'autres attaques par saturation d'IP (non TCP, non ICMP, non ICMPv6, non SCTP et non UDP).

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
Taux d'alarmes (connexions/s)	**Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Saisissez le nombre d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6, non SCTP et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. La meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.
Activer (connexions/s)		Saisissez le nombre d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6 et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde et qui déclenche la suppression aléatoire de paquets d'autres IP. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets d'autres IP si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. Il est recommandé de définir le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6 et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde avant que les paquets qui dépassent le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. Il est recommandé de définir le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.

Protection contre la reconnaissance

- Réseau > Profils réseau > Protection de zone > Protection contre la reconnaissance

Les paramètres suivants définissent la protection de reconnaissance :

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection de la reconnaissance	Configuré dans	Description
Balayage des ports TCP	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** > **Reconnaissance Protection (Protection contre la reconnaissance)**	**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage des ports TCP.
Balayage de port UDP		**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage des ports UDP.
Balayage de l'hôte		**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage de l'hôte.
Action (Action)		Action que le système va appliquer en réponse à la tentative de reconnaissance correspondante : • **Allow (Autoriser)** - Autorise la reconnaissance par l'analyse de ports ou le balayage d'hôtes. • **Alert (Alerter)**- Génère une alerte pour chaque analyse de ports ou balayage d'hôtes correspondant au seuil et dans l'intervalle de temps spécifié (l'action par défaut). • **Block (Bloquer)** - Supprime tous les paquets suivants entre la source et la destination pendant l'intervalle de temps restant spécifié. • **Block IP (Blocage IP)** - Supprime tous les paquets suivants pour la **Duration (Durée)** indiquée, en secondes (plage comprise entre 1 et 3 600). **Track By (Suivre en fonction de)** détermine s'il faut bloquer le trafic source ou le trafic source et de destination. Par exemple, bloque les tentatives qui dépassent le seuil établi par intervalle provenant d'une seule source (plus stricte) ou les tentatives qui disposent d'une paire source et de destination (moins stricte). *Bloquez tous les balayages de reconnaissance, sauf vos balayages de vulnérabilité interne.*
Intervalle (s)		Intervalle de temps, en secondes, pour la détection du balayage des ports TCP ou UDP (plage comprise entre 2 et 65 535 ; par défaut 2). Intervalle de temps, en secondes, pour la détection du balayage de l'hôte (plage comprise entre 2 et 65 535 ; par défaut 10).
Seuil (événements)		Nombres d'événements relatifs à un balayage de ports ou à un balayage d'hôtes survenus au cours de l'intervalle de temps précisé qui ont déclenché l'Action (intervalle compris entre 2 et 65 535 ; valeur par défaut : 100). *Utilisez le seuil d'événement par défaut pour journaliser quelques paquets à des fins d'analyse avant de bloquer les tentatives de reconnaissance.*

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil de protection de zone – Protection de la reconnaissance	Configuré dans	Description
Exclusion de l'adresse source		Les adresses IP listées sur la liste de protection de la reconnaissance. La liste prend en charge un maximum de 20 adresses IP ou objets d'adresse Netmask. • Nom : Saisissez un nom descriptif pour l'adresse à exclure. • Type d'adresse : Sélectionnez IPv4 ou IPv6 dans la liste déroulante. • Address (Adresse) : Sélectionnez une adresse ou un objet d'adresse dans la liste déroulante ou saisissez-en un manuellement.  *Excluez uniquement les adresses IP des groupes internes de confiance qui effectuent des tests de vulnérabilité de « chapeau blanc ».*

Protection contre les attaques basées sur les paquets

- Réseau > Profils réseau > Protection de zone > Protection contre les attaques basées sur les paquets

Vous pouvez configurer la protection contre les attaques basées sur les paquets pour supprimer les types de paquets suivants :

- Abandon de l'IP
- Abandon de TCP
- Drop de ICMP
- Abandon d'IPv6
- Abandon d'ICMPv6

Abandon de l'IP

Pour indiquer au pare-feu ce qu'il doit faire de certains paquets IP qu'il reçoit dans la zone, précisez les paramètres suivants :

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Adresse IP usurpée	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone**	Vérifiez que l'adresse IP source du paquet d'entrée est routable et que l'interface de routage est dans la même zone que l'interface d'entrée. Si l'une de ces conditions n'est pas vraie, supprimez le paquet.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
	Protection (Protection de zone) > **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **ICMP Drop (Abandon ICMP)**	*Suru les zones internes uniquement, abandonnez les paquets d'adresses IP usurpées pour veiller à ce qu'à l'entrée l'adresse source correspond à la table de routage du pare-feu.*
Stricte vérification de l'adresse IP		Vérifiez que les deux conditions sont vraies : • L'adresse IP source n'est pas l'adresse IP de diffusion de sous-réseau de l'interface d'entrée. • L'adresse IP source est routable sur l'interface d'entrée exacte. Si l'une de ces conditions n'est pas vraie, supprimez le paquet. Si le pare-feu est en mode CC (Common Criteria/critères communs), vous pouvez activer la journalisation des paquets supprimés. Sur l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres du journal)**. À la section Gestion des journaux, sélectionnez **Selective Audit (Audit sélectif)**, puis activez la **Packet Drop Logging (Consignation dans les journaux des paquets abandonnés)**.
Trafic fragmenté		Supprime des paquets IP fragmentés.
Abandon de l'option IP		Sélectionnez les paramètres dans ce groupe pour permettre au pare-feu de supprimer les paquets contenant ces Options IP.
Routage source strict		Supprime des paquets dans lesquels l'option IP de routage source strict est définie. Le Routage de source strict est une option qui permet à une source d'un datagramme de fournir les informations de routage par l'intermédiaire desquelles une passerelle ou un hôte doit envoyer le datagramme. *Abandonnez les paquets dotés d'un routage de source strict, car le routage de source permet aux adversaires de contourner les règles de politique de sécurité qui utilisent l'adresse IP de destination en tant que critère de correspondance.*
Routage source vague		Supprime des paquets dans lesquels l'option IP de routage source vague est définie. Le routage de source souple est une option qui permet à une source d'un datagramme de fournir des informations de routage, et une passerelle ou un hôte est autorisé à choisir n'importe quelle route composée d'un certain nombre de passerelles intermédiaires pour router le datagramme vers l'adresse suivante dans l'itinéraire.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
		Abandonnez les paquets dotés d'un routage de source vague, car le routage de source permet aux adversaires de contourner les règles de politique de sécurité qui utilisent l'adresse IP de destination en tant que critère de correspondance.
Horodatage		Supprime des paquets dans lesquels l'option IP Horodatage est définie.
Itinéraire d'enregistrement		Supprime des paquets dans lesquels l'option IP de l'itinéraire d'enregistrement est définie. Lorsqu'un datagramme comporte cette option, chaque routeur qui route le datagramme ajoute sa propre adresse IP à l'en-tête, fournissant ainsi le chemin d'accès au destinataire.
Sécurité		Supprime des paquets, à condition que l'option de sécurité soit définie.
ID du flux		Supprime des paquets, à condition que l'option ID du flux soit définie.
inconnue		Supprime des paquets, à condition que la classe et le numéro soient inconnus. *Supprime les paquets inconnus.*
Incorrect		Supprime des paquets, à condition que leurs combinaisons de classes, de nombres et de longueurs basés sur RFC 791, 1108, 1393 et 2113 soient incorrectes. *Supprimer les paquets mal formés.*

Abandon de TCP

Pour indiquer au pare-feu ce qu'il doit faire de certains paquets TCP qu'il reçoit dans la zone, précisez les paramètres suivants.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Segments TCP superposés différents	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** > **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**	Les pirates peuvent établir des connexions avec des données qui se recoupent, mais différentes, pour essayer d'induire une interprétation erronée de la connexion. Les pirates peuvent utiliser l'usurpation d'IP et la prédiction du numéro de séquence pour intercepter la connexion d'un utilisateur et y injecter leurs propres données. Utilisez ce paramètre pour signaler une non-concordance de superposition et abandonner le paquet lorsque les données du segment ne correspondent pas dans ces cas : • Le segment est dans un autre segment. • Le segment et une partie d'un autre segment sont superposés. • Le segment couvre un autre segment. Ce mécanisme de protection utilise des numéros de séquence pour déterminer l'emplacement des paquets dans le flux de données'A0;TCP.  *Abandonne des paquets dont les segments TCP superposés sont différents.*
Établissement de liaison de segmentation		Empêche l'établissement d'une session TCP si la procédure d'établissement de session n'utilise pas l'établissement de la connexion en trois étapes bien connues. Une procédure d'établissement de liaison de segmentation en quatre ou cinq étapes ou une procédure d'ouverture de sessions simultanées sont des exemples de variations qui ne seraient pas autorisées. Le pare-feu Palo Alto Networks de dernière génération gère correctement les sessions et tous les processus de couche 7 pour l'établissement de liaison de segmentation et d'ouverture de sessions simultanées sans configurer l'**Établissement de liaison de segmentation**. Lorsque cette option est configurée pour un profil de protection de zone et que celui-ci est appliqué à une zone, les sessions TCP des interfaces de cette zone doivent être établies à l'aide de l'établissement de la connexion en trois étapes ; les variations ne sont pas autorisées.  *Abandonne des paquets avec établissement de liaison de segmentation.*
Paquet TCP SYN avec les données		Empêche qu'une session TCP soit ouverte si le paquet TCP SYN contient des données lors d'une connexion en trois étapes. Cette option est activée par défaut.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Paquet TCP SYN/ACK avec les données		Empêche qu'une session TCP soit ouverte si le paquet TCP SYN-ACK contient des données lors d'une connexion en trois étapes. Cette option est activée par défaut.
Rejeter le protocole TCP non-SYN		Détermine si un paquet doit être rejeté ou pas, à condition que le premier paquet pour la configuration d'une session TCP ne soit pas un paquet SYN : • **global** - Utilisez un paramètre système qui est attribué via l'interface CLI. • **yes (oui)** - Rejetez le protocole TCP non-SYN. • **no (non)** - Acceptez le protocole TCP non-SYN. *L'autorisation du trafic TCP non-SYN peut empêcher le fonctionnement normal des politiques de blocage des fichiers, lorsque la connexion client et/ou serveur n'est pas définie après l'occurrence du blocage.* *Si vous configurez l'inspection du contenu du tunnel sur une zone et activez l'option Rematch Sessions (Revérifier les sessions), puis, pour cette zone uniquement, désactivez Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN) pour que l'activation ou la modification d'une politique d'inspection du contenu du tunnel n'entraîne pas l'abandon des sessions de tunnel existantes de la part du tunnel.*
Chemin asymétrique		Détermine si des paquets contenant des ACK désynchronisés ou des numéros de séquence hors de la fenêtre doivent être supprimés ou ignorés : • **global** - Utilisez un paramètre système qui est attribué via l'interface CLI. • **drop (supprimer)** - Supprimez des paquets contenant un chemin asymétrique. • **bypass (ignorer)** - Ignorez l'analyse de paquets contenant un chemin asymétrique.
Extraire les options TCP		Détermine s'il faut supprimer l'option Horodatage TCP ou l'option TCP Fast Open des paquets TCP.
Horodatage TCP	**Network (Réseau)** >	Détermine si l'en-tête du paquet contient un horodatage TCP et, le cas échéant, le supprime.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
	Network Profiles (Profils réseau) > **Zone Protection (Protection de zone)** > **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**	*Supprime l'horodatage TCP des paquets qui le contiennent pour empêcher une attaque DoS par horodatage.*
TCP Fast Open		Supprime l'option TCP Fast Open (et la charge utile de données, le cas échéant) du paquet TCP SYN ou du paquet SYN-ACK lors d'une connexion TCP en trois étapes. Lorsque cette option est décochée (désactivée), l'option TCP Fast Open est autorisée, ce qui préserve la vitesse d'une configuration de connexion en incluant la livraison des données. Cela fonctionne indépendamment du paquet TCP SYN avec les données et du paquet TCP SYN-ACK avec les données. Cette option est désactivée par défaut.
Options MPTCP (Multipath TCP)		MPTCP est une extension de TCP qui permet à un client de maintenir une connexion en utilisant simultanément plusieurs chemins pour se connecter à l'hôte de destination. Par défaut, la prise en charge de MPTCP est désactivée, en fonction du paramètre MPTCP global. Vérifiez ou ajustez les paramètres MPTCP pour les zones de sécurité associées à ce profil : • **Non** – Active la prise en charge MPTCP (ne supprime pas l'option MPTCP). • **Oui** – Désactive la prise en charge MPTCP (supprime l'option MPTCP). Avec cette configuration, les connexions MPTCP sont converties en connexions TCP standards, car MPTCP est rétrocompatible avec TCP. • **(Par défaut) global** – Prise en charge MPTCP basée sur le paramètre MPTCP global. Par défaut, le paramètre MPTCP global est défini sur oui pour que l'option MPTCP soit désactivée (l'option MPTCP est supprimée du paquet). Vous pouvez vérifier

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
		ou ajuster le paramètre MPTCP global en utilisant la commande de la CLI suivante : `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

Drop de ICMP

Pour indiquer au pare-feu qu'il doit supprimer certains paquets ICMP qu'il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
ID ping ICMP 0	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** > **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **ICMP Drop (Abandon ICMP)**	Supprime des paquets, à condition que le paquet de pings ICMP affiche une valeur d'identifiant égale à 0.
Fragment ICMP		Supprime des paquets composés de fragments ICMP.
Paquet volumineux ICMP (>1024)		Supprime des paquets ICMP supérieurs à 1 024 octets.
Supprimer ICMP incorporé dans un message d'erreur		Supprime des paquets ICMP incorporés dans un message d'erreur.
Supprimer l'erreur d'expiration ICMP TTL		Arrête l'envoi de messages ICMP TTL arrivés à expiration.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Supprimer la fragmentation ICMP requise		Arrête l'envoi de messages de fragmentation ICMP requis en réponse à des paquets qui dépassent la valeur MTU de l'interface et dont l'octet DF (Do not Fragment/ne pas fragmenter) est défini. Ce paramètre va interférer avec le processus PMTUD exécuté par les hôtes situés derrière le pare-feu.

Abandon d'IPv6

Pour indiquer au pare-feu qu'il doit supprimer certains paquets IPv6 qu'il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
En-tête de routage de type 0	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** > **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **IPv6 Drop (Abandon IPv6)**	Supprime les paquets IPv6 contenant un en-tête de routage de type 0. Voir RFC 5095 pour des informations d'en-tête de routage de type 0.
Adresse compatible IPv4		Supprime les paquets IPv6 définis comme adresse IPv6 compatible IPv4 selon le document RFC 4291.
Adresse source anycast		Supprime les paquets IPv6 qui contiennent une adresse source anycast.
En-tête de fragment inutile		Supprime les paquets IPv6 qui disposent de l'indicateur de dernier fragment (M=0) et d'un décalage de zéro.
MTU dans ICMP (paquet trop volumineux) inférieure à 1 280 octets		Supprime les paquets IPv6 qui contiennent un message Paquet ICMPv6 trop volumineux lorsque l'unité de transmission maximale (MTU) est inférieure à 1 280 octets.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Extension saut par saut		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Options saut par saut.
Extension de routage		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Routage, qui dirige les paquets vers un ou plusieurs nœuds intermédiaires en chemin vers sa destination.
Extension de destination		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Options de destination incluant des options destinées uniquement à la destination du paquet.
Options IPv6 non valides dans l'en-tête d'extension		Supprime les paquets IPv6 qui contiennent des options IPv6 non valides dans un en-tête d'extension.
Valeur de champ réservé non nulle		Supprime les paquets IPv6 qui contiennent un en-tête dont la valeur de champ réservé n'est pas définie sur zéro.

Abandon d'ICMPv6

Pour indiquer au pare-feu ce qu'il doit faire de certains paquets ICMPv6 qu'il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Erreur ICMPv6 - Destination inaccessible - Exiger la correspondance explicite de la règle de sécurité	**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)** > **Packet Based Attack**	Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de destination inaccessibles, même lorsque le message est associé à une session existante.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
ICMPv6 de paquet trop volumineux - Exiger la correspondance explicite de la règle de sécurité	**Protection (Protection contre les attaques basées sur les paquets) > ICMPv6 Drop (Abandon IPv6)**	Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de paquet trop volumineux, même lorsque le message est associé à une session existante.
ICMPv6 de délai dépassé - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de délai dépassé, même lorsque le message est associé à une session existante.
ICMPv6 de problème de paramètre - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de problème de paramètre, même lorsque le message est associé à une session existante.
ICMPv6 de redirection - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de redirection, même lorsque le message est associé à une session existante.

Protection du protocole

- Réseau > Profils réseau > Protection de zone > Protection de protocole

Le pare-feu autorise normalement des protocoles non-IP entre les zones de couche 2 et entre les zones à câble virtuel. La protection du protocole vous permet de contrôler les protocoles non-IP qui sont autorisés (inclure) ou refusés (exclure) entre ou au sein des zones de sécurité sur un VLAN de couche 2 ou un câble virtuel. Parmi les exemples de protocoles non-IP se trouvent des systèmes AppleTalk, Banyan VINES, Novell, NetBEUI et Contrôle de supervision et Acquisition de données (SCADA), tels qu'un Evénement de Sous-poste Orienté objet Générique (GOOSE).

© 2020 Palo Alto Networks, Inc.

Après avoir configuré la protection du protocole dans un profil de Protection de zone, appliquez le profil à une zone de sécurité d'entrée sur un VLAN de niveau 2 ou un câble virtuel.

Activez la protection du protocole sur les zones Internet pour empêcher le trafic de couche 2 des protocoles que vous n'utilisez pas à accéder au réseau.

Paramètres d'un profil de protection de zone – Protection du protocole	Configuré dans	Description
Rule Type (Type de règle)	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Protocol Protection (Protection de protocole)**	Spécifiez le type de liste que vous créez pour la protection du protocole : • **Inclure la liste** – Seuls les protocoles de la liste sont autorisés, en plus des trames étiquettées IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) et VLAN (0x8100). Tous les autres protocoles sont implicitement refusés (bloqués). • **Exclure la liste** – Seuls les protocoles de la liste sont refusés. Tous les autres protocoles sont implicitement autorisés. Vous ne pouvez pas exclure les trames étiquettées IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) ou VLAN (0x8100). *Utilisez la liste d'inclusion pour autoriser uniquement les protocoles de couche 2 que vous utilisez et pour refuser tous les autres protocoles. Cela réduit la surface d'attaque en refusant les protocoles que vous n'utilisez pas sur le réseau. La liste d'exclusion est une liste noire qui autorise tous les protocoles que vous n'incluez pas sur la liste et, si vous ne configurez pas la protection de couche 2, tous les protocoles de couche 2 sont autorisés.*
Nom du protocole		Saisissez le nom du protocole qui correspond au code Ethertype que vous ajoutez à la liste. Le pare-feu ne vérifie pas que le nom du protocole correspond au code Ethertype, mais le code Ethertype détermine le filtre de protocole.
Activer		Vous pouvez **Activer** le code Ethertype sur la liste. Si vous souhaitez désactiver un protocole à des fins de test, mais pas le supprimer, désactivez-le plutôt.
EtherType (format hexadécimal)		Saisissez un code Ethertype (protocole) précédé de 0x pour indiquer l'hexadécimal (la plage est de 0x0000 à 0xFFFF). Une liste peut avoir un maximum de 64 Ethertypes. Certaines sources de codes Ethertype sont : • IEEE hexadécimal Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

© 2020 Palo Alto Networks, Inc.

Réseau > Profils réseau > QoS

Vous devez **Ajouter** un profil QoS pour définir les limites de bande passante et les priorités d'un maximum de huit classes de services. Il est possible de définir des limites de bande passante garanties et maximales pour chacune des classes ou pour l'ensemble des classes. Ces priorités déterminent la méthode de traitement du trafic en cas de contention.

Pour permettre au pare-feu de fournir une QoS, effectuez également les actions suivantes :

- Définissez le trafic qui doit recevoir le traitement QoS (sélectionnez Politiques > QoS pour ajouter ou modifier une politique QoS).
- Activez la QoS sur une interface (sélectionnez Réseau > QoS).

Voir Qualité de service pour avoir accès à un flux de travail QoS complet, des concepts et des cas pratiques.

Paramètres d'un profil QoS	
Nom du profil	Saisissez un nom pour identifier le profil (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Trafic sortant max.	Entrez le débit maximum (en Mbits/s) pour le trafic sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). La valeur de **Egress Max (Sortie max.)** d'un profil de QoS ne doit pas dépasser la valeur de **Egress Max (Sortie max.)** définie pour l'interface physique sur laquelle la QoS est activée. Voir Réseau > QoS. *Bien qu'il ne s'agisse pas d'un champ obligatoire, il est recommandé de toujours définir la valeur de Egress Max (Sortie max.) d'un profil QoS.*
Trafic sortant garanti	Saisissez la bande passante garantie pour ce profil (Mbits/s). Dans l'éventualité où le trafic dépasse la bande passante de sortie garantie, le pare-feu achemine le trafic dans la mesure du possible.
Classes	Cliquez pour **Ajouter** et indiquer la méthode de traitement des classes de QoS individuelles. Vous pouvez sélectionner une ou plusieurs classes pour configurer'A0;: • **Class (Classe)** - Si vous ne configurez aucune classe, vous pouvez toujours l'inclure dans une politique de QoS. Dans ce cas, le trafic est soumis à des limites de QoS globales. Le trafic qui ne correspond pas à une politique de QoS sera assigné à la classe 4. • **Priority (Priorité)** - Cliquez et sélectionnez une priorité à assigner à une classe : • **real-time (temps réel)** • **élevée** • **Médium** • **faible**

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil QoS	
	En cas de contention, le trafic assigné à une priorité inférieure est supprimé. La priorité en temps réel utilise sa propre file d'attente distincte. • **Egress Max (Sortie max.)** - Cliquez et saisissez le débit maximum (Mbits/s) pour cette classe. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). La valeur de **Egress Max (Sortie max.)** d'une classe QoS ne doit pas dépasser la valeur de **Egress Max (Sortie max.)** du profil QoS. *Bien qu'il ne s'agisse pas d'un champ obligatoire, nous recommandons de toujours définir la valeur de Egress Max (Sortie max.) d'un profil QoS.* • **Egress Guaranteed (Sortie garantie)** - Cliquez et saisissez la bande passante garantie (Mbits/s) pour cette classe. La bande passante garantie attribuée à une classe n'est pas réservée à cette classe ; la bande passante qui n'est pas utilisée demeure disponible pour l'acheminement de tout trafic. Toutefois, lorsque le trafic dépasse la bande passante de sortie garantie attribuée à une classe de trafic, le pare-feu achemine le trafic dans la mesure du possible.

Réseau > Profils réseau > Profil LLDP

Un profil LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) vous permet de configurer le mode LLDP du pare-feu, d'activer les notifications SNMP et Syslog, ainsi que de configurer les éléments TLV (Type-Longueur-Valeur) que vous souhaitez transmettre aux homologues LLDP. Une fois le profil LLDP configuré, affectez-le à une ou plusieurs interfaces.

En savoir plus sur LLDP, y compris la façon de configurer et de surveiller LLDP.

Paramètres d'un profil LLDP	Description
Name (Nom)	Donnez un nom au profil LLDP.
Mode	Sélectionnez le mode dans lequel LLDP fonctionnera : **transmit-receive (transmission/réception)**, **transmit-only (transmission uniquement)** ou **receive-only (réception uniquement)**.
Notifications SNMP et Syslog	Active les notifications de piège SNMP et Syslog, qui se produiront au **Notification Interval (Intervalle de notification)** global. Si cette option est activée, le pare-feu envoie des événements de piège SNMP et Syslog, tel que configuré dans **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** > **System (Système)** > **SNMP Trap Profile (Profil de déroutement SNMP)** et **Syslog Profile (Profil Syslog)**.
Description du port	Permet l'envoi de l'objet ifAlias du pare-feu dans l'élément TLV Description du port.

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil LLDP	Description
Nom du système	Permet l'envoi de l'objet sysName du pare-feu dans l'élément TLV Nom du système.
Description du système	Permet l'envoi de l'objet sysDescr du pare-feu dans l'élément TLV Description du système.
Fonctionnalités du système	Permet l'envoi du mode de déploiement (C3, C2 ou câble virtuel) de l'interface, via le mappage suivant, dans l'élément TLV Fonctionnalités du système. • Si celui-ci est C3, le pare-feu publie la fonctionnalité de routeur (bit 6) et l'autre bit (bit 1). • Si celui-ci est C2, le pare-feu publie la fonctionnalité de pont MAC (bit 3) et l'autre bit (bit 1). • Si celui-ci est C3, le pare-feu publie la fonctionnalité de répéteur (bit 2) et l'autre bit (bit 1). La MIB SNMP combinera les fonctionnalités configurées sur les interfaces en une entrée unique.
Adresse de gestion	Permet l'envoi de la **Management Address (Adresse de gestion)** dans l'élément TLV Adresse de gestion. Vous pouvez saisir jusqu'à quatre adresses de gestion, qui sont envoyées dans l'ordre spécifié. Pour modifier l'ordre, cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**.
Name (Nom)	Donnez un nom à l'adresse de gestion.
Interface	Sélectionnez une interface dont l'adresse IP sera l'adresse de gestion. Si vous sélectionnez **None (Aucune)**, vous pouvez saisir une adresse IP dans le champ en regard de la sélection IPv4 ou IPv6.
Choix IP	Sélectionnez **IPv4** ou **IPv6**, puis, dans le champ adjacent, choisissez ou saisissez l'adresse IP à transmettre comme adresse de gestion. Au moins une adresse est requise si l'élément TLV **Management Address (Adresse de gestion)** est activé. Si aucune adresse IP de gestion n'est configurée, le système utilise l'adresse MAC de l'interface de transmission comme adresse de gestion transmise.

Réseau > Profils réseau > Profil BFD

La BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) contribue à une détection extrêmement rapide d'un échec de la liaison, ce qui accélère le basculement vers un itinéraire différent.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est ce que la BFD?	Présentation de la BFD
Quels champs sont disponibles pour la création d'un profil BFD?	Blocs de construction d'un profil BFD

© 2020 Palo Alto Networks, Inc.

Que voulez-vous faire ?	Reportez-vous à la section :
Affichage du statut BFD pour un routeur virtuel.	Affichage du récapitulatif et des détails BFD
Vous souhaitez en savoir plus ?	En savoir plus sur la BFD et la configurer. Configurez la BFD pour : Itinéraires statiques BGP OSPF OSPFv3 RIP

Présentation de la BFD

La BFD est un protocole qui reconnaît un échec d'un chemin bidirectionnel entre deux moteurs d'acheminement, comme des interfaces, des liaisons de données ou les moteurs d'acheminement en tant que tel. Dans l'implémentation PAN-OS, l'un des moteurs d'acheminement est une interface sur le pare-feu et l'autre est un homologue BFD adjacent qui a été configuré. La détection de l'échec BFG entre deux moteurs est extrêmement rapide, ce qui assure un basculement plus rapide que ce que l'on pourrait atteindre en surveillant les liaisons ou en effectuant fréquemment des vérifications de l'état santé du routage dynamique, comme des pulsations ou des paquets Hello.

Une fois que la BDF a détecté un échec, elle avise le protocole de routage d'utiliser un autre chemin vers l'homologue. Si la BFD est configurée pour l'utilisation d'un itinéraire statique, le pare-feu supprime les itinéraires attribués dans les tables RIB et FIB.

La BFD est prise en charge sur les types d'interface suivants : ethernet physique, ethernet agrégé, VLAN, de tunnel (VPN de site à site et LSVPN) ainsi que sur les sous-interfaces des interfaces de couche 3. Pour chaque itinéraire statique ou protocole de routage dynamique, vous pouvez activer ou désactiver la BFD, sélectionner le profil BFD par défaut ou configurer un profil BFD.

Blocs de construction d’un profil BFD

- Réseau > Profils réseau > Profil BFD

Vous pouvez activer la BFD pour un itinéraire statique ou un protocole de routage dynamique en appliquant le profil BFD par défaut ou un profil BFD que vous avez créé. Le profil par défaut se sert des paramètres BFD par défaut et ne peut être modifié. Vous pouvez cliquer sur **Add (Ajouter)** pour ajouter un nouveau profil BFD et précisez les informations suivantes.

Paramètres d'un profil BFD	Description
Name (Nom)	Nom du profil BFD (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique sur le pare-feu. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Mode	Mode sous lequel la BFD fonctionne :

© 2020 Palo Alto Networks, Inc.

Paramètres d'un profil BFD	Description
	• **Active (Actif)** - La BFD initie l'envoi de paquets de contrôle (par défaut). Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux. • **Passive (Passif)** - La BFD attend que l'homologue envoie des paquets de contrôles et répond comme il se doit.
Intervalle Tx minimum souhaité (ms)	Intervalle minimum (en millisecondes) auquel vous souhaitez que le protocole BFD envoie des paquets de contrôles BFD. La valeur minimum par défaut est 50 sur les pare-feu PA-7000 ; 100 sur les pare-feu PA-3200 ; 200 sur les pare-feu VM-Series (valeur maximale : 2000 ; valeur par défaut : 1000).  *Si vous disposez de plusieurs protocoles qui utilisent des profils BFD différents sur la même interface, configurez les profils BFD avec le même Desired Minimum Tx Interval (Intervalle Tx minimum souhaité).*
Intervalle Rx minimum souhaité (ms)	Intervalle minimum (en millisecondes) auquel la BFD peut recevoir les paquets de contrôles BFD. La valeur minimum par défaut est 50 sur les pare-feu PA-7000 ; 100 sur les pare-feu PA-3200 ; 200 sur les pare-feu VM-Series (valeur maximale : 2000 ; valeur par défaut : 1000).
Multiplicateur de délai de détection	Le système local calcule le délai de détection en tant que **Detection Time Multiplier (Multiplicateur de délai de détection)** reçu du système distant multiplié par l'intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Required Minimum Rx Interval (Intervalle de réception minimum requis)** et le dernier **Desired Minimum Tx Interval (Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu (intervalle compris entre 2 et 50 ; valeur par défaut : 3).
Temps d'attente (ms)	Délai (en millisecondes) entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par le pare-feu. Le **Hold Time (Temps d'attente)** ne s'applique qu'au mode Actif de la BFD. Si le pare-feu reçoit des paquets de contrôles BFD pendant le **Hold Time (Temps d'attente)**, il les ignore (intervalle compris entre 0 et 120 000 ; valeur par défaut : 0). Le paramètre défini par défaut de 0 signifie qu'aucun **Hold Time (Temps d'attente)** n'est utilisé ; le pare-feu envoie et reçoit les paquets de contrôles BFD immédiatement après l'établissement de la liaison.
Activer les sauts multiples	Active la BFD à sauts multiples. Ne s'applique que dans le cas d'une implémentation BGP.
TTL Rx minimum	Valeur TTL minimale (nombre de sauts) la BFD acceptera (recevra) lorsqu'elle prend en charge la BFD à sauts multiples. Ne s'applique que dans le cas d'une implémentation BGP (intervalle compris entre 1 et 254 ; aucune valeur par défaut).

Affichage du récapitulatif et des détails BFD

- Réseau > Routeurs virtuels

Le tableau suivant décrit les informations récapitulatives de BFD.

© 2020 Palo Alto Networks, Inc.

Voir des informations sur la BFD	
Voir le récapitulatif de la BFD.	Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la rangée du routeur virtuel qui vous intéresse, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**. Sélectionnez l'onglet **BFD Summary Information (Informations récapitulatives de BFP)** sur la BFD.
Voir des informations sur la BFD	Sélectionnez **details (détails)** dans la rangée de l'interface qui vous intéresse pour afficher les Détails de la BFD.

Réseau > Profils réseau > Profil d'interface SD-WAN

Créez un profil d'interface SD-WAN pour regrouper les liens physiques par Link Tag (étiquette de liens) et pour contrôler la vitesse des liens et la fréquence à laquelle le pare-feu surveille ces liens.

	Profil d'interface SD-WAN
Name (Nom)	Saisissez un **Name (Nom)** pour le profil d'interface SD-WAN en utilisant un maximum de 31 caractères alphanumériques. Le nom doit commencer par un caractère alphanumérique et peut contenir des lettres, des nombres, des traits de soulignement (_), des traits-d'union (-), des points (.) et des espaces.
Étiquette de liens	Sélectionnez la **Link Tag (Étiquette de liens** que ce profil attribuera à l'interface ou **Add (Ajoutez)** une nouvelle étiquette. Une étiquette de liens regroupe les liens physiques (de différents ISP) pour que le pare-feu puisse sélectionner parmi ceux-ci lors de la sélection du chemin d'accès et du basculement.
Description	Saisissez une description conviviale pour le profil.
Type de lien	Sélectionnez le type de lien physique dans la liste prédéfinie (**ADSL/DSL**, **Cable Modem [Modem câble]**, **Ethernet**, **Fiber [Fibre]**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio [micro-onde/radio]**, **Satellite**, **WiFi**, ou **Other [Autre]**). Le pare-feu est compatible avec n'importe quel périphérique CPE qui se termine par et offre une connexion Ethernet au pare-feu. Par exemple, les points d'accès Wi-Fi, les modems LTE (Long-Term Evolution) et les customer-premises equipment (appareils terminaux des clients, CPE) laser/micro-onde peuvent tous se terminer par un raccord Ethernet.
Assistance du tunnel de données VPN	(PAN-OS 9.1.2 et versions 9.1 ultérieures) Détermine si le trafic de la branche vers le hub et le trafic de retour passent par un tunnel VPN pour plus de sécurité (option activée par défaut) ou passe en dehors du tunnel VPN afin d'éviter la surcharge du cryptage. • Laissez **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) activé pour les types de liens publics qui ont des connexions internet directes ou une capacité d'interruption d'internet, comme le modem câble, l'ADSL et les autres connexions internet. • Vous pouvez désactiver **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) pour les types de liens privés comme MPLS, satellite, ou micro-onde qui n'ont pas de capacité de sortie internet. Cependant, vous devez

© 2020 Palo Alto Networks, Inc.

	Profil d'interface SD-WAN
	d'abord vous assurer que le trafic ne peut pas être intercepté parce qu'il sera envoyé en dehors du tunnel VPN. • La branche peut avoir un trafic DIA qui nécessite de basculer sur le lien MPLS privé se connectant au hub et atteindre internet depuis le hub. Le réglage de **VPN Data Tunnel Support (Assistance du tunnel de données VPN)** détermine si les données privées passent par le tunnel VPN ou en dehors du tunnel et le trafic qui a basculé utilise l'autre connexion (que le flux de données privées n'utilise pas). Le pare-feu utilise des zones pour segmenter le trafic qui a basculé en DIA depuis le trafic MPLS privé.
Téléchargement maximum (Mbps)	Spécifiez la vitesse de téléchargement maximum de l'ISP en mégabits par seconde (Mbps) (la plage est comprise entre 1 et 100 000 ; il n'y a pas de valeur par défaut). Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l'aide d'un outil comme speedtest.net et prenez la moyenne des vitesses maximales pendant une durée appropriée.
Upload maximum (Mbps)	Spécifiez la vitesse d'upload maximum de l'ISP en mégabits par seconde (Mbps) (la plage est comprise entre 1 et 100 000 ; il n'y a pas de valeur par défaut). Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l'aide d'un outil comme speedtest.net et prenez la moyenne des vitesses maximales pendant une durée appropriée.
Surveillance des chemins	Sélectionnez le mode de surveillance des chemins dans lequel le pare-feu surveille les interfaces auxquelles vous appliquez le profil d'interface SD-WAN. • **Aggressive (mode agressif)** — (Par défaut pour tous les types sauf LTE et Satellite) - Le pare-feu sonde les paquets à l'extrémité opposée du lien SD-WAN à une fréquence constante.  *Utilisez le mode Agressif si vous avez besoin d'une détection rapide et d'un basculement dans des conditions de dégradation et de panne générale.* • **Relaxed (Mode souple)** (par défaut pour les types de liens LTE et Satellite) Le pare-feu patiente quelques secondes (selon le**Probe Idle Time [délai d'attente de la sonde]**) entre l'envoi d'ensemble de paquets de sondage, ce qui rend la surveillance des chemins moins fréquente. Lorsque le délai d'attente de la sonde expire, le pare-feu envoie des sondes pendant sept secondes selon la **Probe Frequency (Fréquence de sondage)** configurée.  *Utilisez le mode Souple lorsque vous avez des liens de bande passante faibles, des liens qui chargent en fonction de l'usage (comme LTE) ou lorsque la détection rapide n'est pas aussi importante que la préservation du coût et de la bande passante.*
Fréquence de sondage (par seconde)	Réglez la fréquence de sondage, qui correspond au nombre de fois par seconde où le pare-feu envoie un paquet de sondage à l'extrémité opposée du lien SD-WAN (la plage est comprise entre 1 et 5 ; la valeur par défaut est de 5).
Délai d'attente de la sonde (secondes)	Si vous sélectionnez le mode de surveillance des chemins **Relaxed (Souple)**, vous pouvez régler le délai d'attente de la sonde (en secondes) pendant lequel le pare-

© 2020 Palo Alto Networks, Inc.

	Profil d'interface SD-WAN
	feu attend entre des ensembles de paquets de sondage (la plage est comprise entre 1 et 60 ; la valeur par défaut est 60).
Délai d'attente avant basculement (secondes)	Saisissez le délai d'attente avant basculement (en secondes) pendant lequel le pare-feu attend qu'un lien récupéré soit qualifié avant que le pare-feu réaffecte ce lien en tant que lien préféré après le basculement (la plage est comprise entre 20 et 120 ; la valeur par défaut est 120). Le délai d'attente avant basculement empêche un lien récupéré d'être rétabli comme lien préféré trop rapidement et d'échouer de nouveau immédiatement.

Périphérique

Les sections suivantes servent de référence lors de la réalisation de tâches de maintenance et de configuration du système de base sur le pare-feu'A0;:

- Périphérique > Configuration
- Périphérique > Haute disponibilité
- Périphérique > Carte de transfert des journaux
- Périphérique > Audit de configuration
- Périphérique > Profils de mot de passe
- Périphérique > Administrateurs
- Périphérique > Rôles admin
- Périphérique > Domaine d'accès
- Périphérique > Profil d'authentification
- Périphérique > Séquence d'authentification
- Identification utilisateur
- Périphérique > Sources d'informations de machine virtuelle
- Périphérique > Résolution des problèmes
- Périphérique > Systèmes virtuels
- Périphérique > Passerelles partagées
- Périphérique > Gestion des certificats
- Périphérique > Pages de réponse
- Périphérique > Paramètres des journaux
- Périphérique > Profils de serveur
- Périphérique > Base de données d'utilisateurs locale > Utilisateurs
- Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs
- Périphérique > Exportation programmée des journaux
- Périphérique > Logiciel
- Périphérique > Client GlobalProtect
- Périphérique > Mises à jour dynamiques
- Périphérique > Licences
- Périphérique > Support
- Périphérique > Clé principale et diagnostics

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration

- Périphérique > Configuration > Gestion
- Périphérique > Configuration > Opérations
- Périphérique > Configuration > Module de sécurité matériel
- Périphérique > Configuration > Services
- Périphérique > Configuration > Interfaces
- Périphérique > Configuration > Télémesure
- Périphérique > Configuration > Content-ID
- Périphérique > Configuration > WildFire
- Périphérique > Configuration > Session

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Gestion

- **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**
- **Panorama** > **Setup (Configuration)** > **Management (Gestion)**

Sur un pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** pour configurer les paramètres de gestion.

Sur Panorama™, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** pour configurer les pare-feu que vous gérez à l'aide des modèles Panorama. Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)** pour configurer les paramètres de gestion de Panorama.

Sauf mention contraire, les paramètres de gestion suivants s'appliquent à la fois au pare-feu et à Panorama.

- Paramètres généraux
- Paramètres d'authentification
- Paramètres de la base de règles de politique
- Paramètres de Panorama : Périphérique > Configuration > Gestion (paramètres configurés sur le pare-feu pour se connecter à Panorama)
- Paramètres de Panorama : Panorama > Configuration > Gestion (paramètres configurés sur Panorama pour les connexions aux pare-feu)
- Paramètres de journalisation et de génération de rapports
- Bannières et messages
- Complexité minimale des mots de passe
- AutoFocus™
- Logging Service

Élément	Description
Paramètres généraux	
Nom d'hôte	Saisissez un nom d'hôte (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. Si vous ne saisissez rien, PAN-OS® utilise le modèle de pare-feu (par exemple, PA-5220_2) comme valeur par défaut. Vous pouvez éventuellement configurer le pare-feu afin d'utiliser un nom d'hôte fourni par un serveur DHCP. Reportez-vous à la section Accepter le Nom d'hôte fourni par le serveur DHCP (pare-feu uniquement). *Configurez un nom d'hôte unique pour facilement identifier le périphérique que vous gérez.*
Domain (Domaine)	Saisissez le nom de domaine du réseau pour le pare-feu (31 caractères maximum). Vous pouvez éventuellement configurer les pare-feu et Panorama afin d'utiliser un domaine fourni par un serveur DHCP. Reportez-

© 2020 Palo Alto Networks, Inc.

Élément	Description
	vous à la section Accepter le Domaine fourni par le serveur DHCP (pare-feu uniquement).
Accepter le Nom d'hôte fourni par le serveur DHCP (Pare-feu uniquement)	(S'applique uniquement lorsque le Type d'adresse IP de l'interface de gestion est Client DHCP.)Sélectionnez cette option pour que l'interface de gestion accepte le nom d'hôte qu'elle reçoit du serveur DHCP. Le nom d'hôte obtenu du serveur (s'il est valide) remplace toute valeur spécifiée dans le champ Nom d'hôte.
Accepter le Domaine fourni par le serveur DHCP (Pare-feu uniquement)	(S'applique uniquement lorsque le Type d'adresse IP de l'interface de gestion est Client DHCP.)Sélectionnez cette option pour que l'interface de gestion accepte le domaine (suffixe DNS) qu'elle reçoit du serveur DHCP. Le domaine obtenu du serveur remplace toute valeur spécifiée dans le champ **Domain (Domaine)**.
Bannière de connexion	Saisissez le texte (jusqu'à 3 200 caractères) que vous souhaitez afficher sur la page de connexion de l'interface Web en dessous des champs **Name (Nom)** et **Password (Mot de passe)**.
Forcer les administrateurs à accuser réception de la bannière de connexion	Sélectionnez cette option pour afficher et forcer les administrateurs à sélectionner **I Accept and Acknowledge the Statement Below (J'accepte et accuse réception de l'énoncé ci-dessous)** au-dessus de la bannière de connexion figurant sur la page de connexion, ce qui force les administrateurs à reconnaître qu'ils comprennent et acceptent le contenu du message avant de pouvoir **Login (Se connecter)**.
Profil de service SSL/TLS	Affectez un profil de service SSL/TLS existant ou créez-en un nouveau pour indiquer un certificat et les paramètres de protocole SSL/TLS autorisés sur l'interface de gestion (voir Périphérique > Gestion des certificats > Profil de service SSL/TLS). Le pare-feu ou Panorama utilise ce certificat pour authentifier les administrateurs qui accèdent à l'interface Web via l'interface de gestion (MGT) ou toute autre interface prenant en charge le trafic de gestion HTTP/HTTPS (voir Réseau > Profils réseau> Gestion de l'interface). Si vous sélectionnez **none (aucun)** (par défaut), le pare-feu ou Panorama utilise le certificat prédéfini. *Le certificat prédéfini est fourni pour plus de commodité. Pour une meilleure sécurité, affectez un profil de service SSL/TLS. Pour garantir la fiabilité, le certificat doit être signé par un certificat d'autorité de certification (AC) qui se trouve dans le magasin de certificats racines approuvés des systèmes clients.*
Fuseau horaire	Sélectionnez le fuseau horaire du pare-feu.
Lieu	Sélectionnez la langue des rapports PDF dans la liste déroulante. Voir Surveillance > Rapports PDF > Gérer le récapitulatif PDF.

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Même si une préférence de langue spécifique est définie pour l'interface Web, les rapports PDF utiliseront tout de même la langue indiquée dans ces **Locale (Paramètres régionaux)**.
Date	Définissez la date sur le pare-feu ; saisissez la date du jour (au format AAAA/MM/JJ) ou sélectionnez la date dans le menu déroulant. *Vous pouvez également définir un serveur NTP (Device (Périphérique) > Setup (Configuration) > Services).*
Période	Définissez l'heure sur le pare-feu ; saisissez l'heure actuelle (en format 24 heures) ou sélectionnez l'heure dans le menu déroulant. *Vous pouvez également définir un serveur NTP (Device (Périphérique) > Setup (Configuration) > Services).*
Numéro de série (Appareils virtuels Panorama uniquement)	Saisissez le numéro de série de Panorama. Vous pouvez trouver le numéro de série dans l'e-mail de confirmation de commande qui vous a été envoyé par Palo Alto Networks®.
Latitude	Saisissez la latitude (de -90,0 à 90,0) du pare-feu.
Longitude	Saisissez la longitude (de -180,0 à 180,0) du pare-feu.
Appliquer automatiquement un verrou de validation	Sélectionnez cette option pour appliquer automatiquement un verrou de validation lors de la modification de la configuration candidate. Pour plus d'informations, reportez-vous à la section Verrouillage des configurations. *Activez Automatically Acquire Commit Lock (Appliquer automatiquement un verrou de validation) afin d'éviter que d'autres administrateurs puissent apporter des changements de configuration avant que le premier administrateur ait valider ses changements.*
Vérification de la date d'expiration du certificat	Configurez le pare-feu pour qu'il renvoie des messages d'avertissement lorsque des certificats inclus approchent de leur date d'expiration. *Activez la Certificate Expiration Check (Vérification de la date d'expiration du certificat) pour générer un message d'avertissement lorsque des certificats inclus approchent de leur date d'expiration.*

© 2020 Palo Alto Networks, Inc.

Élément	Description
Fonction de systèmes virtuels multiples	Permet d'utiliser plusieurs systèmes virtuels sur les pare-feu prenant en charge cette fonctionnalité (voir Périphérique > Systèmes virtuels). *Pour activer plusieurs systèmes virtuels sur un pare-feu, les politiques du pare-feu doivent faire référence à un maximum de 640 groupes d'utilisateurs distincts. Si nécessaire, réduisez le nombre de groupes d'utilisateurs référencés. Puis, après avoir activé et ajouté plusieurs systèmes virtuels, les politiques peuvent ensuite référencer à nouveau 640 groupes d'utilisateurs pour chaque système virtuel supplémentaire.*
Base de données de filtrage des URL (Panorama uniquement)	Sélectionnez un fournisseur de filtrage des URL à utiliser avec Panorama : **brightcloud** ou **paloaltonetworks** (PAN-DB).
Utiliser les adresses MAC attribuées par l'hyperviseur (Pare-feu VM-Series uniquement)	Sélectionnez cette option pour que le pare-feu VM-Series utilise l'adresse MAC affectée par l'hyperviseur au lieu de générer une adresse MAC à l'aide du schéma personnalisé de PAN-OS. Si vous activez cette option et que vous utilisez une adresse IPv6 pour l'interface, l'ID d'interface ne doit pas être au format EUI-64 qui dérive l'adresse IPv6 de l'adresse MAC de l'interface. Dans une configuration High Availability (haute disponibilité ; HD) active/passive, une erreur de validation se produit si vous utilisez le format EUI-64.
Sécurité GTP	Sélectionnez cette option pour permettre l'inspection des messages du plan de contrôle et du plan de données utilisateur dans le trafic du GPRS Tunneling Protocol (protocole tunnel GPRS ; GTP). Voir Objets > Profils de sécurité > Protection GTP pour configurer un profil de protection GTP afin que vous puissiez appliquer la politique sur le trafic GTP.
Sécurité SCTP	Sélectionnez cette option pour permettre l'inspection et le filtrage des paquets et des blocs Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) et pour appliquer la protection contre la saturation initiation (INIT) SCTP. Reportez-vous à la section Objets > Profils de sécurité > Protection SCTP. Pour la protection contre la saturation SCTP INIT flood protection, reportez-vous à la section Configuration de la protection contre la saturation SCTP INIT.
Certificat de périphérique (PAN-OS 9.1.3 et les versions ultérieures uniquement)	
Obtenir un certificat	Cliquez afin de saisir le mot de passe à usage unique généré par le Customer Support Portal (Portail Support Client). Le certificat de périphérique est requis pour réussir l'identification de Panorama avec le portail support Client et pour optimiser les fonctions

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Zero Touch Provisioning (ZTP). Après avoir réussi l'installation du certificat de périphérique, les éléments suivants s'affichent : • **Current Device Certificate Status (État du certificat de périphérique actuel)** - L'état actuel du certificat de périphérique (`Valid [Valide]`, `Invalid [Invalide]` ou `Expired [Expiré]`) • **Not Valid Before (Valide à partir de)** - L'horodotage indiquant le moment où la validité du certificat de périphérique commence. • **Not Valid After (Valide jusqu'à)** - L'horodotage indiquant le moment où la validité du certificat de périphérique expire et le certificat de périphérique devient donc `Invalid (invalide)` ou `Expired (expiré)`. • **Last Fetched Message (Dernier message extrait)** - Message indiquant si le certificat de périphérique est correctement installé ou si l'installation du certificat de périphérique a échoué. • **Last Fetched Status (Dernier état extrait)** - L'état de l'extraction du certificat de périphérique (`success [réussite]` ou `failed [échec]`). • **Last Fetched Timestamp (Dernier horodatage extrait)** - L'horodatage de la dernière tentative d'installation du certificat de périphérique.
Paramètres d'authentification	
Profil d'authentification	Sélectionnez le profil d'authentification (ou la séquence) utilisé par le pare-feu pour authentifier les comptes administratifs que vous définissez sur un serveur externe plutôt que localement sur le pare-feu (voir Périphérique > Profil d'authentification). Lorsque des administrateurs externes se connectent, le pare-feu requiert l'authentification et demande des informations relatives aux autorisations (notamment le rôle administratif) au serveur externe. L'activation de l'authentification pour les administrateurs externes requiert des étapes supplémentaires en fonction du type de serveur indiqué par le profil d'authentification, qui doit être l'un des éléments suivants : • RADIUS • TACACS+ • SAML *Les administrateurs peuvent utiliser SAML pour s'authentifier sur l'interface Web, mais pas sur la CLI.* Sélectionnez **None (Aucun)** pour désactiver l'authentification pour les administrateurs externes. Pour les comptes administratifs que vous définissez localement (sur le pare-feu), le pare-feu s'authentifie à l'aide du profil

© 2020 Palo Alto Networks, Inc.

Élément	Description
	d'authentification attribué à ces comptes (voir Périphérique > Administrateurs).
Profil du certificat	Sélectionnez un profil de certificat pour vérifier les certificats clients des administrateurs qui sont configurés pour pouvoir accéder à l'interface Web du pare-feu grâce à un certificat. Pour obtenir des instructions sur la configuration des profils de certificat, voir Périphérique > Gestion des certificats > Profil du certificat. *Configurez un profil de certificat pour vous assurer que la machine qui héberge l'administrateur possède les bons certificats pour authentifier le certificat CA racine défini dans le profil de certificat.*
Délai d'inactivité	Saisissez, pour l'interface Web ou la CLI, le délai d'inactivité maximum (en minutes) avant qu'un administrateur ne soit automatiquement déconnecté (la plage est comprise entre 0 et 1 440, la valeur par défaut est 60). Une valeur égale à 0 signifie que l'inactivité n'entraîne pas une déconnexion automatique. *L'actualisation manuelle et automatique des pages de l'interface Web (telles que l'onglet Dashboard (Tableau de bord) et la boîte de dialogue Alarmes système) réinitialise le compteur Idle Timeout (Délai d'inactivité). Pour permettre au pare-feu d'appliquer le délai d'inactivité lorsque vous êtes sur une page qui prend en charge l'actualisation automatique, définissez l'intervalle d'actualisation sur Manual (Manuel) ou sur une valeur supérieure au Idle Timeout (Délai d'inactivité). Vous pouvez également désactiver l'Auto Refresh (Actualisation automatique) dans l'onglet ACC.* *Définissez un Idle Timeout (Délai d'inactivité) de 10 minutes pour empêcher les utilisateurs non autorisés d'accéder au pare-feu si un administrateur laisse une session du pare-feu ouverte.*
Délai de vie de la clé API	Saisissez la durée, en minutes, pendant lesquelles la clé API est valide (plage comprise entre 0 et 525 600 ; par défaut 0). Une valeur de 0 signifie que la clé API n'expire jamais. Sélectionnez **Expire All API Keys (Expirer toutes les clés API)** pour invalider toutes les clés API précédemment générées. Utilisez cette option avec parcimonie, car toutes les clés existantes deviennent inutiles et les opérations pour lesquelles vous utilisez ces clés API cessent de fonctionner.

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Effectuez cette opération lors d'une maintenance pour que vous puissiez remplacer les clés sans perturber les applications actuelles où les clés API sont référencées.
Les dernières clés API arrivées à expiration	Affiche l'horodatage de la dernière expiration de clés API Ce champ ne comporte aucune valeur si vous n'avez jamais réinitialisé vos clés.
Tentatives échouées	Saisissez le nombre d'échecs de tentatives de connexion (de 0 à 10) autorisées par le pare-feu pour l'interface Web et la CLI avant le verrouillage du compte administrateur. Une valeur de 0 indique un nombre illimité de tentatives de connexion. La valeur par défaut est de 0 pour les pare-feu en mode opérationnel normal et de 10 pour les pare-feu enmode FIPS-CC. Limiter les tentatives de connexion peut vous permettre de protéger le pare-feu contre les attaques en force. *Si vous définissez les Failed Attempts (Tentatives échouées) sur une valeur autre que 0 mais que vous conservez la valeur DLockout Time (Durée de verrouillage) de 0, les Failed Attempts (Tentatives échouées) sont ignorées et l'utilisateur n'est jamais verrouillé.* *Définissez le nombre de Failed Attempts (Tentatives échouées) sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d'attaque par force pour se connecter au pare-feu.*
Durée de verrouillage	Saisissez le nombre de minutes (plage de 0 à 60) pendant lesquelles l'accès d'un administrateur à l'interface Web et la CLI est verrouillé par le pare-feu si la limite de **Failed Attempts (Tentatives échouées)** est atteinte. Une valeur de 0 (par défaut) signifie que le verrouillage s'applique jusqu'à ce qu'un autre administrateur déverrouille manuellement le compte. *Si vous définissez le champ Failed Attempts (Tentatives échouées) sur une valeur non nulle, mais que vous laissez le champ Lockout Time (Durée de verrouillage) sur 0, l'utilisateur est verrouillé une fois le nombre défini de tentatives de connexion atteint et jusqu'à ce qu'un autre administrateur déverrouille manuellement le compte.* *Définissez la Lockout Time (Durée de verrouillage) sur au moins 30 minutes pour*

© 2020 Palo Alto Networks, Inc.

Élément	Description
	empêcher les tentatives de connexion continues d'un acteur malveillant.
Paramètres de la base de règles de politique	
Étiquette exigée dans les politiques	Exige la présence d'au moins une étiquette lors de la création d'une nouvelle règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, vous devez ajouter au moins une étiquette lors de votre prochaine modification de la règle.
Description exigée dans les politiques	Vous devez ajouter une **Description** lors de la création d'une nouvelle règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, vous devez ajouter une **Description** lors de votre prochaine modification de la règle.
Échec de validation si les politiques ne possèdent aucune étiquette ou description	Force l'échec de votre validation si vous n'ajoutez aucune étiquette ou description à la règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, la validation échouera si vous n'ajoutez aucune étiquette ou description lors de votre prochaine modification de la règle. Pour que la validation échoue, vous devez sélectionner les options **Require tag on policies (Étiquette exigée dans les politiques)** ou **Require description on policies (Description exigée dans les politiques)**.
Commentaire d'audit exigé dans les politiques	Exige la présence d'un **Audit Comment (Commentaire d'audit)** lors de la création d'une nouvelle règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, vous devez ajouter un **Audit Comment (Commentaire d'audit)** lors de votre prochaine modification de la règle.
Expression régulière de commentaire d'audit	Précisez les exigences de paramètres pour le format des commentaires dans les commentaires d'audit.
Nombre de correspondance à la règle de politique	Suivez la fréquence à laquelle le trafic est mis en correspondance avec des règles de politique que vous avez configurées sur le pare-feu. Lorsque cette option est activée, vous pouvez afficher le Nombre de correspondances total entre le trafic et chacune des règles, ainsi que la date et l'heure de création et de modification de la règle, et de la première correspondance et de la dernière correspondance.
Utilisation de l'application de la politique	
Paramètres de Panorama : Périphérique > Configuration > Gestion	
Configurez les paramètres suivants sur le pare-feu ou dans un modèle sur Panorama. Ces paramètres permettent d'établir une connexion entre le pare-feu et Panorama.	

© 2020 Palo Alto Networks, Inc.

Élément	Description
Vous devez également configurer les paramètres de connexion et de partage d'objet sur Panorama (voir Paramètres de Panorama : Panorama > Configuration > Gestion). *Le pare-feu utilise une connexion SSL avec cryptage AES256 pour s'enregistrer sur Panorama. Par défaut, Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits prédéfinis et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux. Pour sécuriser davantage les connexions SSL entre Panorama, les pare-feu et les collecteurs de journaux, veuillez vous référer à la section Sécurisation des communications avec le client pour configurer des certificats personnalisés entre le pare-feu et Panorama ou un collecteur de journaux.*	
Serveurs de Panorama	Saisissez l'adresse IP ou le nom de domaine complet du serveur Panorama Si Panorama est dans une configuration haute disponibilité (HD), saisissez l'adresse IP ou le nom de domaine complet du serveur Panorama secondaire dans le second champ **Panorama Servers (Serveurs Panorama)**.
Délai d'attente en réception pour la connexion à Panorama	Saisissez le délai (en secondes) de réception des messages TCP de Panorama (plage de 1 à 240 ; par défaut 240).
Délai d'attente à l'envoi pour la connexion à Panorama	Saisissez le délai (en secondes) d'envoi des messages TCP à Panorama (plage de 1 à 240 ; par défaut 240).
Nombre de relances pour les envois SSL à Panorama	Saisissez le nombre de tentatives autorisées lors de l'envoi de messages SSL (Secure Socket Layer) à Panorama (plage de 1 à 64 ; par défaut 25).
Activation de la récupération automatique de la validation	Activez pour permettre au pare-feu de vérifier automatiquement sa connexion au serveur de gestion Panorama lorsqu'une configuration est validée et transmise au pare-feu et à des intervalles configurés après qu'une configuration a été transmise avec succès. Lorsque cette option est activée et que le pare-feu ne réussit pas à vérifier sa connexion avec le serveur de gestion Panorama, le pare-feu et la gestion Panorama reviennent à leur dernière configuration fonctionnelle afin de restaurer la connectivité.
Nombre de tentatives de vérification de la connectivité Panorama	Lorsque l'option **Enabled Automated Commit Recovery (Activation de la récupération automatique de la validation)** est activée, configurez le nombre de fois que le pare-feu teste sa connexion avec le serveur de gestion Panorama.
Intervalle entre les tentatives (sec)	Lorsque l'option **Enabled Automated Commit Recovery (Activation de la récupération automatique de la validation)** est activée, configurez la durée en secondes entre les tentatives de connexion du pare-feu au serveur de gestion Panorama.
Communication sécurisée avec le client	Activez la **Secure Client Communication (Sécurisation des communications avec le client)** pour vous assurer que le pare-feu utilise des certificats personnalisés configurés (plutôt que le

© 2020 Palo Alto Networks, Inc.

Élément	Description
	certificat par défaut) pour authentifier les connexions SSL avec Panorama ou les collecteurs de journaux. • **None (Aucun)** (par défaut) – Si aucun certificat de périphérique n'est configuré et que le certificat prédéfini par défaut est utilisé. • **Local** – Le pare-feu utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d'un serveur PKI d'entreprise existant. • **Certificate (Certificat)** – Sélectionnez le certificat de périphérique local que vous avez généré ou importé. Ce certificat peut être unique au pare-feu (en fonction d'un hachage du numéro de série du pare-feu) ou il peut s'agir d'un certificat de périphérique commun utilisé par tous les pare-feu qui se connectent à Panorama. • **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. Le Profil de certificat définit le certificat CA à utiliser pour vérifier les certificats clients et comment vérifier l'état de révocation des certificats. • **SCEP** – Le pare-feu utilise un certificat de périphérique et une clé privée générée par un serveur SCEP (Protocole d'inscription de certificats simple). • **SCEP Profile (Profil SCEP)** – Sélectionnez un Profil SCEP dans le menu déroulant. Le Profil SCEP fournit à Panorama les informations nécessaires pour authentifier les périphériques clients auprès d'un serveur SCEP de votre PKI d'entreprise. • **Certificate Profile (Profil de certificat)** – Sélectionnez le Profil de certificat dans le menu déroulant. Le Profil de certificat définit le certificat CA à utiliser pour vérifier les certificats clients et comment vérifier l'état de révocation des certificats.
	• **Customize Communication (Personnaliser la communication)** – Le pare-feu utilise son certificat personnalisé configuré pour s'authentifier auprès des périphériques sélectionnés. • **Panorama Communication (Communication avec Panorama)** – Le pare-feu utilise le certificat client configuré pour communiquer avec Panorama. • **PAN-DB Communication (Communication avec PAN-DB)** – Le pare-feu utilise le certificat client configuré pour communiquer avec un appareil PAN-DB. • **WildFire Communication (Communication avec WildFire)** – Le pare-feu utilise le certificat client configuré pour communiquer avec un appareil WildFire®. • **Log Collector Communication (Communication avec le Collecteur de journaux)** – Le pare-feu utilise le certificat client configuré pour communiquer avec le Collecteur de journaux. • **Check Server Identity (Vérification de l'identité du serveur)** – (Communication avec Panorama et avec le Collecteur

© 2020 Palo Alto Networks, Inc.

Élément	Description
	de journaux) Le pare-feu confirme l'identité du serveur en faisant correspondre le Common Name (nom commun ; CN) avec l'adresse IP ou le FQDN du serveur.
Activer/Désactiver les politiques et objets'A0;Panorama	Cette option s'affiche uniquement lorsque vous modifiez les **Panorama Settings (Paramètres de Panorama)** sur un pare-feu (et non dans un modèle sur Panorama). **Disable Panorama Policy and Objects (Désactiver les politiques et objets Panorama)** désactive la propagation des politiques et objets de groupe de périphériques sur le pare-feu. Par défaut, cette action supprime également ces politiques et objets du pare-feu. Pour conserver une copie locale des politiques et objets sur le pare-feu, cochez **Import Panorama Policy and Objects before disabling (Importer les politiques et objets Panorama avant la désactivation)** dans la boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option. Une fois validés, ces politiques et objets font partie de la configuration du pare-feu et Panorama ne les gère plus. Dans des conditions d'exploitation normales, la désactivation de la gestion Panorama est inutile et peut compliquer la configuration et la maintenance des pare-feu. Cette option s'applique généralement à des situations dans lesquelles les pare-feu nécessitent des règles et des valeurs d'objet différentes de celles définies dans le groupe de périphériques. Un exemple type est lorsque vous déplacez un pare-feu hors de la production dans un environnement de laboratoire afin de le tester. Pour rétablir la gestion des politiques et des objets Panorama, cliquez sur le lien **Enable Panorama Policy and Objects (Activer les politiques et objets Panorama)**.
Activer/Désactiver le modèle de réseau et de périphérique	Cette option s'affiche uniquement lorsque vous modifiez les **Panorama Settings (Paramètres de Panorama)** sur un pare-feu (et non dans un modèle sur Panorama). **Disable Device and Network Template (Désactiver le modèle de réseau et de périphérique)** désactive la propagation des informations relatives au modèle (configuration de périphérique et réseau) sur le pare-feu. Par défaut, cette action supprime également les informations de modèle du pare-feu. Pour conserver une copie locale des informations de modèle sur le pare-feu, cochez **Import Device and Network Templates before disabling (Importer les modèles de réseau et de périphérique avant la désactivation)** dans la boîte de dialogue qui s'affiche lorsque vous sélectionnez cette option. Une fois validés, les informations de modèle font partie de la configuration du pare-feu et Panorama ne les gère plus. *Dans des conditions d'exploitation normales, la désactivation de la gestion Panorama est inutile et peut compliquer la configuration et la maintenance des pare-feu. Cette option s'applique généralement à des situations dans*

© 2020 Palo Alto Networks, Inc.

Élément	Description
	lesquelles les pare-feu nécessitent des valeurs de configuration de périphérique et réseau différentes de celles définies dans le modèle. Un exemple type est lorsque vous déplacez un pare-feu hors de la production dans un environnement de laboratoire afin de le tester. Pour configurer le pare-feu afin qu'il recommence à accepter les modèles, cliquez sur **Enable Device and Network Templates (Activer/Désactiver les modèles de réseau et de périphérique)**.

Paramètres de Panorama : Panorama > Configuration > Gestion

Si vous utilisez Panorama pour gérer les pare-feu, configurez les paramètres suivants sur Panorama. Ces paramètres déterminent les délais d'expiration et les tentatives de message SSL des connexions entre Panorama et les pare-feu gérés, ainsi que les paramètres de partage d'objet.

Vous devez également configurer les paramètres de connexion Panorama sur le pare-feu ou dans un modèle sur Panorama voir Paramètres de Panorama : Périphérique > Configuration > Gestion.

Le pare-feu utilise une connexion SSL avec cryptage AES256 pour s'enregistrer sur Panorama. Par défaut, Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits prédéfinis et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux. Pour sécuriser davantage ces connexions SSL, veuillez vous référer à la section Personnaliser la communication sécurisée avec le serveur *pour configurer des certificats personnalisés entre Panorama et ses clients.*

Délai d'attente en réception pour connexion au périphérique	Saisissez le délai (en secondes) de réception des messages TCP provenant de tous les pare-feu gérés (plage de 1 à 240 ; par défaut 240).
Délai d'attente à l'envoi pour la connexion au périphérique	Saisissez le délai (en secondes) d'envoi des messages TCP à tous les pare-feu gérés (plage de 1 à 240 ; par défaut 240).
Nombre de relances pour le périphérique SSL destinataire	Saisissez le nombre de tentatives autorisées lors de l'envoi de messages SSL (Secure Socket Layer) aux pare-feu gérés (plage de 1 à 64 ; par défaut 25).
Partager les objets de service et d'adresse inutilisés avec les périphériques	Sélectionnez cette option (activée par défaut) pour partager tous les objets partagés et les objets spécifiques à un groupe de périphériques Panorama avec les pare-feu gérés. Si vous désactivez cette option, l'appareil recherche des objets d'adresse, de groupe d'adresses, de services ou de groupes de services dans les politiques Panorama et ne partage aucun objet non référencé. Cette option permet de réduire le nombre total d'objets en s'assurant que l'appareil envoie uniquement les objets nécessaires aux pare-feu gérés. Si vous avez une règle de politique qui cible des appareils spécifiques dans un groupe d'appareils, alors les objets utilisés dans cette politique sont considérés comme utilisés dans ce groupe d'appareils.

© 2020 Palo Alto Networks, Inc.

Élément	Description
Les objets définis dans la section ancienne ont une priorité supérieure.	Sélectionnez cette option (désactivée par défaut) pour indiquer que les valeurs d'objet dans les anciens groupes ont priorité sur celles des groupes descendants lorsque les groupes de périphériques à différents niveaux dans la hiérarchie ont des objets du même type et du même nom, mais avec des valeurs différentes. Cela signifie que lorsque vous validez un groupe de périphériques, les anciennes valeurs appliquent un contrôle prioritaire sur toutes les valeurs de contrôle prioritaire. De même, cette option entraîne le fait que la valeur d'un objet partagé remplace les valeurs d'objets du même type et du même nom dans les groupes de périphériques. Si vous sélectionnez cette option, le lien Recherche d'objets remplacés s'affiche.
Recherche d'objets remplacés	Sélectionnez cette option (en bas de la boîte de dialogue Paramètres de Panorama) pour énumérer tous les objets *grisés*. Un objet ombré est un objet dans l'Emplacement partagé qui a le même nom, mais une valeur différente dans un groupe de périphériques. Le lien ne s'affiche que si vous indiquez que les objets définis dans les anciens emplacements auront préséance.
Activation des rapports et du filtrage sur les groupes	Sélectionnez cette option (désactivée par défaut) pour permettre à Panorama de stocker localement les noms d'utilisateur, les noms des groupes d'utilisateurs et les informations de mappage de nom d'utilisateur / groupe qu'il reçoit des pare-feu. Cette option est universelle pour tous les groupes de périphériques de Panorama. Cependant, vous devez également activer le stockage local au niveau de chaque groupe de périphériques en indiquant un Périphérique principal et en configurant la pare-feu pour le Stockage des utilisateurs et des groupes à partir du périphérique principal.
Paramètres de communication sécurisée : Panorama > Configuration > Gestion	
Personnaliser la communication sécurisée avec le serveur	• **Custom Certificate Only (Certificat personnalisé uniquement)** – Lorsque cette option est activée, Panorama accepte uniquement des certificats personnalisés pour l'authentification avec des pare-feu et des Collecteurs de journaux gérés. • **SSL/TLS Service Profile (Profil de service SSL/TLS)** – Sélectionnez un profil de service SSL/TLS à partir du menu déroulant. Ce profil définit le certificat et les versions SSL/TLS compatibles que le pare-feu peut utiliser pour communiquer avec Panorama. • **Certificate Profile (Profil de certificat)** – Sélectionnez un profil de certificat dans le menu déroulant. Ce profil de certificat définit le comportement de la vérification de la révocation du certificat et le certificat CA racine utilisé pour authentifier la chaîne de certificats présentée par le client. • **Authorization List (Liste d'autorisations)** – **Add (Ajoutez)** et configurez un nouveau profil d'autorisation en utilisant les

© 2020 Palo Alto Networks, Inc.

Élément	Description
	champs suivants pour définir les critères d'autorisation des périphériques cliens qui peuvent se connecter à Panorama. La Liste d'autorisations prend en charge un maximum de 16 entrées de profil. • **Identifier (Identifiant)** – Sélectionnez **Subject (Objet)** ou **Subject Alt. (Autre nom d'objet)** en tant qu'identifiant d'autorisation. • **Type** – Si vous avez choisi **Subject Alt. (Autre objet).** en tant qu'identifiant, puis sélectionnez **IP**, **hostname (nom d'hôte)** ou **e-mail** comme type de l'identifiant. Si vous avez sélectionné **Subject (Objet)**, vous devez utiliser le **common name (nom commun)** comme type d'identifiant. • **Value (Valeur)** – Saisissez la valeur d'identifiant. • **Authorize Clients Based on Serial Number (Autorisation des clients en fonction du numéro de série)** – Panorama autorise les périphériques clients en fonction du hachage du numéro de série du périphérique. • **Check Authorization List (Vérifier la liste d'autorisations)** – Panorama vérifie l'identité des périphériques clients par rapport à la liste d'autorisations. Un appareil ne doit correspondre qu'à un seul critère de la liste à autoriser. Si aucune correspondance n'est trouvée, le périphérique n'est pas autorisé. • **Disconnect Wait Time (min) (Délai d'attente de déconnexion (min))** – Période (en minutes) pendant laquelle Panorama attend avant de mettre fin à la connexion actuelle avec ses périphériques gérés. Panorama rétablit alors les connexions avec ses périphériques gérés en utilisant les paramètres de communication du serveur sécurisé et configuré. Le délai d'attente commence après que vous avez validé la configuration des communications sécurisées avec le serveur.
Communications sécurisées avec le client	L'utilisation de la **Secure Client Communication (Communication sécurisée avec le client)** permet de s'assurer que le client Panorama utilise des certificats personnalisés configurés (plutôt que le certificat prédéfini par défaut) pour authentifier les connexions SSL avec un autre appareil Panorama dans une paire HA ou avec un autre appareil WildFire. • **Predefined (Prédéfini)** (par défaut) – Aucun certificat de périphérique n'est configuré est Panorama utilise le certificat prédéfini par défaut. • **Local** – Panorama utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d'un serveur PKI d'entreprise existant. • **Certificat** – Sélectionnez le certificat de périphérique local. • **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. • **SCEP** – Panorama utilise un certificat de périphérique et une clé privée générée par un serveur Simple Certificate

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Enrollment Protocol (Protocole d'inscription de certificats simple ; SCEP). • **Profil SCEP** – Sélectionnez le Profil SCEP dans le menu déroulant. • **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. • **Personnaliser la communication** • **HA Communication (Communication HA)** – Panorama utilise le certificat client configuré pour assurer la communication HA avec son homologue HA. • **WildFire Communication (Communication avec WildFire)** – Panorama utilise le certificat client configuré pour communiquer avec un appareil WildFire.
Paramètres de journalisation et de génération de rapports Utilisez cette section pour modifier : • Les périodes d'expiration et les quotas de stockage des rapports et des types de journaux suivants. Les paramètres sont synchronisés entre les paires haute disponibilité. • Journaux de tous types qui sont générés par le pare-feu et qui sont stockés localement (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**. Les paramètres s'appliquent à tous les systèmes virtuels sur le pare-feu. • Journaux qui sont générés par un appareil M-Series ou un appareil virtuel Panorama en mode Panorama et qui sont stockés localement : journaux système, journaux de configuration, journaux de statistiques d'application et journaux User-ID™ (**Panorama** > **Setup (Configuration)** > **Management (Gestion)**). • Journaux de tous types qui sont générés localement par l'appareil virtuel Panorama en Mode hérité ou qui sont rassemblés à partir des pare-feu (**Panorama** > **Setup (Configuration)** > **Management (Gestion)**). *Pour les journaux qui sont envoyés aux collecteurs de journaux Panorama par les pare-feu, vous pouvez définir des quotas de stockage et des périodes d'expiration pour chaque groupe de collecteurs (voir Panorama > Groupes de collecteurs).* • Attributs permettant le calcul et l'exportation de rapports d'activité des utilisateurs. • Rapports prédéfinis créés sur le pare-feu ou sur Panorama.	
Onglet Stockage des journaux (Le serveur de gestion de Panorama et tous les modèles de pare-feu, à l'exception des pare-feu de la série PA-5200 et de la série PA-7000) *Panorama affiche cet onglet si vous modifiez les paramètres de journalisation et de génération de rapports*	Pour chaque type de journal, indiquez : • **Quota** – Le **Quota**, en pourcentage, attribué sur le disque dur pour le stockage des journaux. Lorsque vous modifiez une valeur de **Quota**, l'allocation du disque associée change automatiquement. Si le total de toutes les valeurs est supérieur à 100 %, un message s'affiche en rouge et un message d'erreur s'affiche lorsque vous tentez d'enregistrer les paramètres. Dans ce cas, ajustez les pourcentages afin que le total soit inférieur ou égal à 100 %. *Par défaut, les pare-feu VM-Series dispose d'un quota de 0 % alloué au stockage du journalSCTP, au SCTP Summary (Récapitulatif SCTP), au Hourly SCTP*

© 2020 Palo Alto Networks, Inc.

Élément	Description
(Panorama > Setup (Configuration) > Management (Gestion)). Si vous utilisez un modèle Panorama pour configurer les paramètres des pare-feu (Device (Périphérique) > Setup (Configuration) > Management (Gestion)), veuillez vous référer aux onglets Stockage à disque unique et Stockage à disque multiple*.*	*Summary (Récapitulatif SCTP horaire), au Daily SCTP Summary (Récapitulatif SCTP quotidien) et au Weekly SCTP Summary (Récapitulatif SCTP hebdomadaire). Vous devez donc allouer un certain pourcentage à la journalisation de ces informations SCTP par ces pare-feu.* • **Max Days (Jours max)** – La durée (en jours) de la période d'expiration du journal (plage comprise entre 1 et 2 000). Le pare-feu ou l'appareil Panorama supprime automatiquement les journaux qui ont atteint la période spécifiée. Par défaut, il n'existe aucune période d'expiration, ce qui signifie que les journaux n'expirent jamais. Le pare-feu ou l'appareil Panorama évalue les journaux lors de leur création, puis supprime les journaux ayant atteint la période d'expiration ou la taille du quota. *Les journaux récapitulatifs hebdomadaires peuvent dépasser le seuil avant la suppression suivante s'ils atteignent le seuil d'expiration entre les intervalles de suppression des journaux par le pare-feu. Lorsqu'un quota de journal atteint la taille maximale, les nouvelles entrées du journal commencent à remplacer les entrées du journal les plus anciennes. Si vous réduisez la taille d'un quota de journal, le pare-feu ou Panorama supprime les journaux les plus anciens lorsque vous validez les modifications. Dans une configuration haute disponibilité, l'homologue passif ne reçoit pas les journaux et ne les supprime donc pas, sauf en cas de basculement et si l'homologue passif devient de fait actif.*
	• **Core Files (Fichiers noyau)** – Si votre pare-feu connaît une défaillance du système fonctionnel, il générera un fichier noyau qui contient des détails sur le processus et sur la raison de l'échec. Si un fichier noyau est trop lourd pour l'emplacement de stockage du fichier noyau par défaut (`/var/cores` partition), vous pouvez activer l'option de fichier **`large-core`** pour attribuer un emplacement de stockage alternatif et plus grand (`/opt/panlogs/cores`). Un ingénieur d'assistance de Palo Alto Networks peut augmenter le stockage attribué si nécessaire. Pour activer ou désactiver l'option de fichier **`large-core`**, saisissez la commande de la CLI suivante à partir du mode de configuration et **`commit`** ensuite la configuration : **`# set deviceconfig setting management large-core [yes|no]`**

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Le fichier noyau est supprimé si vous désactivez cette option. Vous devez utiliser le protocole SCP du mode opérationnel pour exporter le fichier noyau : `> scp export core-file large-corefile` *Seul un ingénieur d'assistance de Palo Alto Networks peut interpréter le contenu des fichiers noyaux.* • **Restore Defaults (Rétablir les valeurs par défaut)** – Sélectionnez cette option pour revenir aux valeurs par défaut.
Onglets **Session Log Storage (Stockage du journal de session)** et **Management Log Storage (Stockage du journal de gestion)** (Uniquement les pare-feu des séries PA-5200 et PA-7000)	Les pare-feu de la série PA-5200 et de la série PA-7000 enregistrent les journaux de gestion et les journaux de sessions sur des disques séparés. Sélectionnez l'onglet pour chaque ensemble de journaux et configurez les paramètres décrits dans l'Onglet Stockage des journaux : • **Session Log Storage (Stockage des journaux de sessions)** – Sélectionnez **Session Log Quota (Quota de journal de sessions)** et définissez des quotas et des périodes d'expiration pour les journaux de trafic, de menaces, de filtrage des URL, de correspondance HIP, d'User-ID, de GTP / Tunnel, de SCTP, d'authentification et de GlobalProtect, ainsi que les PCAPs de menaces étendues. • **Management Log Storage (Stockage des journaux de gestion)** – Définissez des quotas et des périodes d'expiration pour les journaux système, les journaux de configuration et les journaux de statistiques de l'application, ainsi que pour les rapports HIP, les captures de filtrage de données, les PCAP d'application et les PCAP de filtrage de débogage.
Onglets **Single Disk Storage (Stockage à disque unique)** et **Multi Disk Storage (Stockage à disque multiple)** (Modèle Panorama uniquement)	Si vous utilisez un modèle Panorama pour configurer les quotas de journal et les périodes d'expiration, configurez les paramètres dans l'un ou dans les deux onglets suivants en fonction des pare-feu affectés au modèle : • **Pare-feu de la série PA-5200 et de la série PA-7000** – Sélectionnez **Multi Disk Storage (Stockage à disque multiple)** et configurez les paramètres dans les onglets Stockage des journaux de session et Stockage des journaux de gestion. *Par défaut, les pare-feu de la série PA-5200 dispose d'un quota de 0 % alloué au stockage du journalSCTP, au SCTP Summary (Récapitulatif SCTP), au Hourly SCTP Summary (Récapitulatif SCTP horaire), au Daily SCTP Summary (Récapitulatif SCTP quotidien) et au Weekly SCTP Summary (Récapitulatif SCTP hebdomadaire). Vous*

© 2020 Palo Alto Networks, Inc.

Élément	Description
	devez donc allouer un certain pourcentage à la journalisation de ces informations SCTP par ces pare-feu. • **Tous les autres modèles de pare-feu** – Sélectionnez **Single Disk Storage (Stockage à disque unique)**, sélectionnez **Session Log Quota (Quota de journal de session)** et configurez les paramètres sur l'onglet Stockage des journaux.
Onglet Exportation des journaux et génération de rapports	Configurez les paramètres d'exportation et de rapport des journaux suivants au besoin : • **Number of Versions for Config Audit (Nombre de versions d'audit de configuration)** : saisissez le nombre de versions de configuration à enregistrer avant de supprimer les plus anciennes (par défaut 100). Vous pouvez utiliser ces versions enregistrées pour contrôler et comparer les modifications apportées à la configuration. • **Number of Versions for Config Backups (Nombre de versions de sauvegarde de configuration)** – (Panorama uniquement) Saisissez le nombre de sauvegardes de configuration à enregistrer avant de supprimer les plus anciennes (la valeur par défaut est 100). • **Max Rows in CSV Export (Nombre max. de lignes exportées au format CSV)** – Saisissez le nombre maximum de lignes qui s'affichent dans les rapports CSV générés en cliquant sur **Export to CSV (Exporter vers un fichier CSV)** dans la vue des journaux du trafic (plage de 1 à 1 048 576 ; par défaut 65 535). • **Max Rows in User Activity Report (Nombre max. de lignes dans le rapport d'activité des utilisateurs)** – Saisissez le nombre maximum de lignes pris en charge pour les rapports d'activité des utilisateurs détaillés (plage de 1 à 1 048 576 ; par défaut 5 000).
Onglet Exportation des journaux et génération de rapports (suite)	• **Average Browse Time (sec) (Durée de navigation moyenne (secondes))** – Configurez cette variable pour ajuster la manière dont la durée de navigation est calculée en secondes pour Surveillance > Rapports au format PDF > Rapport d'activité des utilisateurs (plage de 0 à 300 secondes ; par défaut 60). Le calcul ignore les sites classés comme des publicités Web et des réseaux de distribution de contenu. Le calcul de la durée de navigation est basé sur les pages de conteneur consignées dans les journaux de filtrage des URL. Les pages de conteneur servent de base au calcul car de nombreux sites chargent du contenu de sites externes qui ne doit pas être pris en compte. Pour plus d'informations sur la page de conteneur, reportez-vous à la section Container Pages (Pages de conteneur). Le paramètre de durée de navigation moyenne correspond à la durée moyenne jugée nécessaire par l'administrateur à la navigation d'une page Web par un utilisateur. Toute requête formulée une fois la durée de navigation moyenne écoulée sera considérée comme une nouvelle activité de navigation. Le calcul ignore les nouvelles pages Web chargées entre la

© 2020 Palo Alto Networks, Inc.

Élément	Description
	première requête (heure de début) et la durée de navigation moyenne. Ce comportement a été conçu afin d'exclure des sites externes et chargés depuis la page Web consultée. Exemple : si la durée de navigation moyenne est définie sur 2 minutes et qu'un utilisateur ouvre une page Web et la consulte pendant 5 minutes, la durée de navigation de cette page sera toujours de 2 minutes. Ceci est dû au fait qu'il est impossible de déterminer la durée de consultation d'une page donnée par un utilisateur • **Page Load Threshold (sec) (Seuil de chargement de page [secondes])** – Vous permet de régler la durée supposée (en secondes) de chargement des éléments sur la page (plage de 0 à 60 ; par défaut 20). Toute requête formulée entre le premier chargement de page et le seuil de chargement de page est considérée comme des éléments de la page. Toute requête formulée en dehors du seuil de chargement de page est supposée correspondre à un clic de l'utilisateur sur un lien dans la page. Le seuil de chargement de page est également utilisé dans les calculs pour Surveillance > Rapports PDF > Rapport d'activité des utilisateurs. • **Syslog HOSTNAME Format (Format NOM D'HÔTE Syslog)** – Choisissez le FQDN, le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) à utiliser dans l'en-tête du message Syslog. Cet en-tête identifie le serveur de gestion du pare-feu ou de Panorama d'où le message est originaire. • **Report Runtime (Temps d'exécution du rapport)** – Sélectionnez l'heure (la valeur par défaut est 2 heures) à laquelle le pare-feu ou l'appareil Panorama commence à générer des rapports quotidiens programmés. • **Report Expiration Period (Période d'expiration du rapport)** – Définissez la période d'expiration (en jours) des rapports (plage de 1 à 2 000). Par défaut, il n'existe aucune période d'expiration, ce qui signifie que les rapports n'expirent jamais. Le pare-feu ou l'appareil Panorama supprime les rapports expirés chaque nuit à 2 h, en fonction de l'heure du système.
	• **Stop Traffic when LogDb full (Arrêter le trafic lorsque la base de données des journaux est saturée)** (pare-feu uniquement ; désactivée par défaut) – Sélectionnez cette option si vous souhaitez que le trafic via le pare-feu soit arrêté lorsque la base de données des journaux est saturée. • **Enable Threat Vault Access (Activer l'accès à l'archivage sécurisé des menaces)** (activé par défaut) – Permet au pare-feu d'accéder à l'Archivage sécurisé des menaces pour recueillir les dernières informations sur les menaces détectées. Cette information est disponible pour les journaux de menaces et pour les principales activités de menaces inscrites sur l'ACC. • **Enable Log on High DP Load (Activer la journalisation de la charge DP)** (pare-feu uniquement ; désactivée par défaut) – Sélectionnez cette option pour indiquer qu'une entrée du journal système est générée lorsque la charge de traitement des paquets sur le pare-feu utilise le processeur à 100 %.

© 2020 Palo Alto Networks, Inc.

Élément	Description
	L'option Enable Log on High DP Load(Activer la journalisation de la charge DP) permet aux administrateurs d'enquêter et d'identifier la cause de la forte utilisation du processeur. *Une charge processeur élevée peut altérer le fonctionnement du système, car le nombre de cycles du processeur n'est pas suffisant pour traiter tous les paquets. Le journal système vous informe de ce problème (une entrée est générée dans le journal à chaque minute) et vous permet d'en déterminer la cause.* • **Enable High Speed Log Forwarding (Activer le transfert de données à grande vitesse)** (pare-feu de la série PA-5200 et de la série PA-7000 uniquement ; désactivé par défaut) – En tant que meilleure pratique, sélectionnez cette option pour transférer des journaux vers Panorama avec un débit maximal de 120 000 journaux/seconde. Lorsque cette option est désactivée, le pare-feu transmet des journaux à Panorama avec un débit maximal de seulement 80 000 journaux par seconde. Si vous activez cette option, le pare-feu ne stocke pas les journaux localement ou ne les affiche pas dans les onglets **Dashboard (Tableau de bord)**, **ACC**, ou **Monitor (Surveillance)**. De plus, vous devez configurer le transfert de journal vers Panorama pour utiliser cette option. • **Log Collector Status (État du collecteur de journaux)** : affiche l'état du pare-feu, à savoir s'il a établi avec succès une connexion à l'architecture de Collecte de journaux distribuée et s'il lui envoie des journaux. Si le pare-feu est également configuré pour envoyer des journaux au service de journalisation, vérifiez le **Logging Service Status (État du service de journalisation)**.De la section du Service de journalisation.
(Panorama uniquement)	• **Buffered Log Forwarding from Device (Transfert des journaux mis en mémoire tampon depuis le périphérique)** (activé par défaut) – Permet au pare-feu de mettre en mémoire tampon les entrées de journal sur son disque dur (stockage local) lorsqu'il perd la connectivité à Panorama. Lorsque la connexion à Panorama est rétablie, le pare-feu transfère les entrées de journal à Panorama ; l'espace disque disponible pour la mise en mémoire tampon dépend du quota de stockage des journaux sur le modèle du pare-feu et du volume des journaux en attente de transfert. Si l'espace disque disponible est utilisé, les entrées les plus anciennes sont supprimées pour permettre la journalisation des nouveaux événements. *Activez l'option Buffered Log Forwarding from Device (Transfert des journaux mis en mémoire tampon depuis le périphérique)*

© 2020 Palo Alto Networks, Inc.

Élément	Description
	pour empêcher la perte des journaux en cas d'échec de la connexion à Panorama. • **Get Only New Logs on Convert to Primary (Obtenir uniquement les nouveaux journaux lors de la conversion vers le périphérique principal)** (désactivé par défaut) – Cette option s'applique uniquement à un appareil virtuel Panorama en mode hérité qui écrit des journaux dans un système de fichiers réseau (NFS). Avec la journalisation NFS, seul le serveur Panorama principal est monté sur le NFS. Par conséquent, les pare-feu envoient des journaux uniquement à l'appareil Panorama principal actif. Cette option vous permet de configurer les pare-feu de manière à ce qu'ils envoient les nouveaux journaux générés uniquement à Panorama, lorsqu'un basculement HD se produit et que le serveur Panorama secondaire reprend la journalisation sur le NFS (après avoir été promu serveur principal). Cette option est généralement activée pour éviter aux pare-feu d'envoyer de gros volumes de journaux placés en mémoire tampon une fois la connectivité vers Panorama restaurée après une période significative. • **Only Active Primary Logs to Local Disk (Seulement les journaux actifs sur le disque local)** (désactivé par défaut) – Cette option s'applique uniquement à un appareil virtuel Panorama en mode hérité. Cette option vous permet de configurer uniquement le Panorama actif pour enregistrer les journaux sur le disque local.
	Pre-Defined Reports (Rapports prédéfinis) (activé par défaut) – Des rapports prédéfinis relatifs aux applications, au trafic, aux menaces, au filtrage des URL et au Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) sont disponibles sur le pare-feu et sur Panorama. Les rapports prédéfinis relatifs à SCTP sont disponibles sur le pare-feu et sur Panorama une fois que la Sécurité SCTP est activée sous **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**. Comme les pare-feu consomment des ressources mémoires lors de la génération des résultats toutes les heures (et de leur transfert à Panorama où ils sont agrégés et compilés pour affichage), pour réduire l'utilisation de la mémoire, vous pouvez désactiver les rapports qui ne vous sont pas utiles. Pour désactiver un rapport, désactivez cette option en regard du rapport. Cliquez sur **Select All (Sélectionner tout)** ou **Deselect All (Désélectionner tout)** pour activer ou de désactiver la génération de rapports prédéfinis. *Avant de désactiver un rapport, assurez-vous qu'aucun Rapport de groupe ou Rapport au format PDF ne l'utilise. Si vous désactivez un rapport prédéfini attribué à un ensemble de*

© 2020 Palo Alto Networks, Inc.

Élément	Description
	rapports, l'ensemble des rapports ne contiendra plus aucune donnée.
Bannières et messages Pour afficher tous les messages dans une boîte de dialogue Message du jour, reportez-vous à la section Message du jour. *Une fois que vous avez configuré le Message du jour et cliqué sur OK, les administrateurs qui se connectent ensuite ainsi que les administrateurs actifs qui actualisent leur navigateur verront immédiatement le nouveau message ou le message mis à jour ; une validation n'est pas requise. Cela vous permet d'avertir les autres administrateurs qu'une validation est imminente juste avant que vous l'effectuiez.*	
Message du jour (case à cocher)	Sélectionnez cette option pour afficher la boîte de dialogue Message du jour lorsqu'un administrateur se connecte à l'interface Web.
Message du jour (champ de saisie de texte)	Saisissez le texte (jusqu'à 3 200 caractères) de la boîte de dialogue Message du jour.
Autoriser l'option Ne plus afficher	Sélectionnez cette option (désactivée par défaut) pour inclure la case à cocher **Do not show again (Ne plus afficher)** dans la boîte de dialogue Message du jour. Cette option offre aux administrateurs la possibilité de ne pas revoir ce même message lors de leurs prochaines connexions. *Si vous modifiez le texte du Message of the Day (Message du jour), le message s'affichera même pour les administrateurs qui ont sélectionné Do not show again (Ne plus afficher). Les administrateurs doivent resélectionner cette option pour éviter de voir le message modifié lors de sessions ultérieures, à moins que le message soit modifié de nouveau.*
Title	Saisissez le texte de l'en-tête du Message du jour (par défaut `Message du jour`).
Couleur d'arrière-plan	Sélectionnez une couleur de fond pour la boîte de dialogue Message du jour. Par défaut (**None (Aucune)**), la couleur de fond est un gris clair.
Icône	Sélectionnez une icône prédéfinie qui apparaîtra au-dessus du texte dans la boîte de dialogue Message du jour : • **None (Aucune)** (par défaut) • **Error (Erreur)** • **Help (Aide)** • **Information (Informations)**

© 2020 Palo Alto Networks, Inc.

Élément	Description
	• **Warning (Avertissement)** 
Bannière de l'en-tête	Saisissez le texte qu'affiche la bannière de l'en-tête (jusqu'à 3 200 caractères).
Couleur de l'en-tête	Sélectionnez une couleur de fond pour l'en-tête. Par défaut (**None (Aucune)**), il n'y a aucune couleur de fond (transparent).
Couleur de texte de l'en-tête	Sélectionnez une couleur pour le texte de l'en-tête. Par défaut (**None (Aucune)**), la couleur de fond est noire.
Même bannière pour l'en-tête et le pied de page	Sélectionnez cette option (activée par défaut) si vous voulez que la bannière du pied de page possède le même texte et les mêmes couleurs que la bannière de l'en-tête. Lorsque cette option est activée, les champs pour le texte et les couleurs de la bannière du pied de page sont grisés.
Bannière du pied de page	Saisissez le texte qu'affiche la bannière du pied de page (jusqu'à 3 200 caractères).
Couleur du pied de page	Sélectionnez une couleur de fond pour le pied de page. Par défaut (**None (Aucune)**), il n'y a aucune couleur de fond (transparent).
Couleur de texte du pied de page	Sélectionnez une couleur pour le texte du pied de page. Par défaut (**None (Aucune)**), la couleur de fond est noire.
Complexité minimale des mots de passe	
Activé	Activez les exigences minimales des mots de passe pour les comptes locaux. Cette fonction garantit que les comptes administrateur locaux sur le pare-feu sont conformes à un ensemble d'exigences des mots de passe. Vous pouvez également créer un profil de mot de passe contenant un sous-ensemble de ces options qui appliqueront un contrôle prioritaire sur ces paramètres et qui peut être appliqué à des comptes spécifiques. Pour plus d'informations, voir Périphérique > Profils de mot de passe et reportez-vous à la section Exigences relatives au nom d'utilisateur et au mot de passe pour obtenir des informations sur les caractères valides qui peuvent être utilisés pour les comptes.  *La longueur maximale du mot de passe est de 31 caractères. Évitez de définir les exigences que n'accepte pas PAN-OS. Par exemple, ne définissez pas une exigence constituée de 10 majuscules, 10 minuscules, 10 chiffres et de 10 caractères spéciaux, parce qu'elle serait supérieure à la longueur maximale de 31 caractères.* Si la haute disponibilité (HD) est configurée, utilisez toujours l'homologue principal lors de la configuration des options de

© 2020 Palo Alto Networks, Inc.

Élément	Description
	complexité des mots de passe et validez immédiatement après l'apport de modifications. Les paramètres de complexité minimale du mot de passe ne s'appliquent pas aux comptes de bases de données locales pour lesquelles vous avez indiqué un **Hachage du mot de passe** (voir Périphérique > Base de données locale des utilisateurs > Utilisateurs).  *Exigez des mots de passe forts pour aider à prévenir les attaques par force brute d'accès au réseau. Exigez une longueur minimale et l'utilisation d'au moins un de chacun des éléments suivants : lettre majuscule, lettre minuscule, valeur numérique et caractère spécial. De plus, évitez les répétitions excessives de caractères et de noms d'utilisateur dans les mots de passe, définissez les limites sur la fréquences de réutilisation des mots de passe et définissez les périodes régulières de modification des mots de passe, afin d'éviter que les mots de passe soient utilisés trop longtemps. Plus les exigences en matière de mot de passe sont élevées, plus il est difficile pour les pirates de pirater un mot de passe. Veillez à respecter les pratiques exemplaires en matière de robustesse des mots de passe pour vous assurer de créer un mot de passe fort.*
Longueur minimale	Une longueur minimale de mot de passe est requise (plage de 1 à 15 caractères).
Nombre minimum de lettres en majuscules	Un nombre minimum de lettres en majuscules est requis (plage de 0 à 15 caractères).
Nombre minimum de lettres en minuscule	Un nombre minimum de lettres en minuscules est requis (plage de 0 à 15 caractères).
Nombre minimum de chiffres	Un nombre minimum de chiffres est requis (plage de 0 à 15 chiffres).
Nombre minimum de caractères spéciaux	Un nombre minimum de caractères spéciaux (non alphanumériques) est requis (plage de 0 à 15 caractères).
Bloquer les caractères récurrents	Indiquez le nombre de caractères en double séquentiels qui sont autorisés dans un mot de passe (plage de 2 à 15). Si vous définissez la valeur 2, le mot de passe peut comporter le même caractère séquentiel deux fois, mais si le même caractère est utilisé trois fois ou plus dans une séquence, le mot de passe n'est pas autorisé.

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Par exemple, si la valeur est définie sur 2, le système acceptera le mot de passe test11 ou 11test11, mais pas test111, car le chiffre 1 apparaît trois fois dans la séquence.
Bloquer l'intégration du nom d'utilisateur (inversé inclus)	Sélectionnez cette option pour empêcher l'utilisation du nom d'utilisateur du compte (ou une version inversée du nom) dans le mot de passe.
Les caractères du nouveau mot de passe sont différents	Lorsque les administrateurs changent leurs mots de passe, les caractères doivent être différents de la valeur définie.
Changement de mot de passe exigé à la première ouverture de session	Sélectionnez cette option pour demander aux administrateurs de changer leurs mots de passe à la prochaine connexion au pare-feu.
Empêcher la limite de réutilisation du mot de passe	Demandez à ce qu'un mot de passe précédent ne soit pas réutilisé en fonction du nombre défini. Par exemple, si la valeur est définie sur 4, vous ne pouvez pas réutiliser l'un de vos 4 derniers mots de passe (plage de 0 à 50).
Blocage de la période de modification du mot de passe (jours)	L'utilisateur ne peut pas changer son mot de passe avant le nombre de jours défini (plage de 0 à 365 jours).
Période de modification du mot de passe requise (jours)	Requiert que les administrateurs modifient régulièrement leur mot de passe (plage de 0 à 365 jours). Par exemple, si la valeur est définie sur 90, les administrateurs sont invités à modifier leur mot de passe tous les 90 jours. Vous pouvez également définir un message d'avertissement d'expiration de 0 à 30 jours et indiquer un délai supplémentaire.
Avertissement avant la date d'expiration (jours)	Si une **Required Password Change Period (Période de modification du mot de passe requise)** est définie, vous pouvez utiliser cet **Expiration Warning Period (Avertissement avant expiration)** pour demander à l'utilisateur de modifier son mot de passe lorsqu'il reste moins qu'un certain nombre de jours indiqués avant la date de modification du mot de passe requise (plage de 0 à 30).
Nombre d'ouvertures de session Administrateur après expiration (nombre)	Autorise l'administrateur à se connecter un certain nombre de fois après la date de modification requise (plage de 0 à 3). Par exemple, si vous définissez cette valeur sur 3 et que le compte est arrivé à expiration, l'administrateur peut se connecter encore trois fois sans modifier son mot de passe avant que le compte ne soit verrouillé.
Période de grâce après expiration (jours)	Autorise l'administrateur à se connecter un certain nombre de jours une fois le compte arrivé à expiration (plage de 0 à 30).
AutoFocus™	

© 2020 Palo Alto Networks, Inc.

Élément	Description
Activé	Activez le pare-feu pour qu'il se connecte à un portail AutoFocus afin de récupérer des données de renseignement sur la menace et de permettre des recherches intégrées entre le pare-feu et AutoFocus. Lorsque le pare-feu est connecté à AutoFocus, il affiche les données AutoFocus associées aux entrées de journal en ce qui concerne le Trafic, la Menace, le Filtrage des URL, les Envois WildFire et le Filtrage des données (**Monitor (Surveillance)** > **Logs (Journaux)**). Vous pouvez cliquer sur un artefact dans ces types d'entrées de journal (comme une adresse IP ou une URL) pour afficher un récapitulatif des résultats et des statistiques AutoFocus pour cet artefact. Vous pouvez ensuite lancer une recherche AutoFocus élargie pour l'artefact directement à partir du pare-feu.  *Vérifiez que votre licence AutoFocus est active sur le pare-feu (Device (Périphérique) > Licenses (Licences)). Si la licence AutoFocus n'est pas affichée, utilisez l'une des options de License Management (Gestion des licences) pour activer la licence.*
URL AutoFocus	Saisissez l'URL AutoFocus : **`https://autofocus.paloaltonetworks.com:10443`**
Délai d'expiration de la requête (secondes)	Réglez la durée (en secondes) pendant laquelle le pare-feu peut tenter d'effectuer une requête auprès d'AutoFocus pour obtenir les données de renseignement sur la menace. Si le portail AutoFocus ne répond pas avant la fin de la période spécifiée, le pare-feu met fin à la connexion.
Logging Service Utilisez cette section pour configurer les pare-feu VM-Series et matériels pour le transfert des journaux au Cortex Data Lake. Voici le flux de travail complet pour configurer les options décrites ci-dessous : • Start Logging to Cortex Data Lake (without Panorama) (Commencer la journalisation dans Cortex Data Lake [sans Panorama]) • Start Logging to Cortex Data Lake (for Panorama-managed firewalls) (Commencer la journalisation dans Cortex Data Lake [pour les pare-feux gérés par Panorama])  *Le service de journalisation se nomme désormais Cortex Data Lake. Cependant, certaines fonctionnalités et certains boutons du pare-feu continuent d'afficher le nom Logging Service (service de journalisation).*	
Activer le Service de journalisation	Sélectionnez cette option pour activer le pare-feu (ou, si vous utiliser Panorama, les pare-feux qui appartiennent au **Template [Modèle]**sélectionné) pour le transfert des journaux au Cortex Data Lake (Cortex Data Lake était auparavant nommé Logging Service [Service de journalisation]).

© 2020 Palo Alto Networks, Inc.

Élément	Description
	Après avoir configuré le transfert des journaux (Objects [Objets] > Log Forwarding [Transfert des journaux]), le pare-feu transfère les journaux directement au Cortex Data Lake ; c'est aussi le cas pour les pare-feux gérés par Panorama.
Activer la journalisation double (pour les pare-feux gérés par Panorama uniquement)	**Enable Duplicate Logging (Activer la journalisation double)** pour continuer d'envoyer les journaux à Panorama et aux collecteurs de journaux distribués, en plus d'envoyer les journaux au Cortex Data Lake. Cette option est très utile lorsque vous évaluez Cortex Data Lake ; lorsque cette option est activée, les pare-feux qui appartiennent au modèle sélectionné enregistrent une copie des journaux auprès du Cortex Data Lake et de votre Panorama ou de l'architecture de collecte de journaux distribuée.
Activer la journalisation améliorée des applications	**Enable Enhanced Application Logging (Activez la journalisation améliorée des applications)** si vous voulez que le pare-feu recueille des données qui accroissent la visibilité des applications de Palo Alto Networks. Par exemple, cette visibilité accrue permet aux applications Cortex XDR de Palo Alto Networks de mieux catégoriser les activités normales sur le réseau et d'établir une base de référence pour celles-ci de sorte que le pare-feu puisse détecter les comportements inhabituels qui pourraient indiquer la présence d'une attaque. La journalisation améliorée des applications exige une licence à un service de journalisation (Cortex Data Lake). Vous ne pouvez afficher ces journaux ; ils sont conçus pour n'être utilisés que par les applications de Palo Alto Networks.
Région	Sélectionnez la région géographique de l'instance Cortex Data Lake (service de journalisation) à laquelle le pare-feu transférera les journaux. Connectez-vous au Cortex hub (concentrateur Cortex) pour confirmer la région dans laquelle l'instance Cortex Data Lake est déployée (dans le concentrateur, sélectionnez l'engrenage des paramètres dans la barre de menu supérieure et cliquez sur **Manage Apps (gérer les applications)**.
Nombre de connexions au service de journalisation pour les pare-feu PA-7000 et PA-5200.	(Pare-feux PA-7000 Series et PA-5200 Series) Spécifiez le nombre de connexions pour envoyer des journaux depuis les pare-feux vers Cortex Data Lake (la plage est comprise entre 1 et 20 ; la valeur par défaut est 5). Vous pouvez utiliser la commande de la CLI **`request logging-service-forwarding status`** sur le pare-feu pour vérifier le nombre de connexions actives entre le pare-feu et Cortex Data Lake.
Intégrer sans Panorama (pour les pare-feux qui ne sont pas gérés par Panorama)	Vous pouvez permettre aux pare-feux qui ne sont pas gérés par Panorama de se connecter à Cortex Data Lake. Pour ce faire, vous devez d'abord générer une clé dans l'application Cortex Data Lake. Cette clé permet au pare-feu de s'authentifier et de se connecter en toute sécurité à Cortex Data Lake. Après avoir généré la clé, saisissez-la ici. Ensuite, passez à la section permettre

© 2020 Palo Alto Networks, Inc.

Élément	Description
	au pare-feu de commencer à transférer les journaux à Cortex Data Lake.
État du service de journalisation	Affichez l'état de la connexion à Cortex Data Lake. **Show Status (Montrer l'état)** pour afficher les détails des contrôles suivants : • **Licence** : `OK` ou `Error (Erreur)` pour indiquer si le pare-feu dispose d'une licence valide pour transférer les journaux au Cortex Data Lake. • **Certificat** : `OK` ou `Error (Erreur)` pour indiquer si le pare-feu a bien récupéré le certificat nécessaire pour s'authentifier auprès de Cortex Data Lake.. • **Info client** : `OK` ou `Error (Erreur)` pour indiquer si le pare-feu dispose du numéro d'identification du client nécessaire pour utiliser Cortex Data Lake. Lorsque l'état correspond à `OK`, vous pouvez également voir le numéro d'identification du client. • **Connectivité du périphérique** : indique si le pare-feu s'est bien connecté au Cortex Data Lake.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Opérations

Vous pouvez exécuter les tâches suivantes pour gérer les configurations candidate et active du pare-feu et de Panorama™. Si vous utilisez un appareil virtuel Panorama, vous pouvez également utiliser les paramètres de cette page pour configurer les Partitions de stockage de journaux pour un appareil virtuel Panorama en mode hérité.

Vous devez Valider les modifications que vous apportez dans la configuration candidate pour activer ces changements, afin qu'ils fassent partie de la configuration en cours d'exécution. Comme pratique exemplaire, nous vous recommandons d'Enregistrer les configurations candidates, et ce, régulièrement.

Vous pouvez utiliser les commandes SCP (Secure Copy) à partir de la CLI pour exporter des fichiers de configuration, des journaux, des rapports ainsi que d'autres fichiers vers un serveur SCP et importer les fichiers vers un autre pare-feu ou vers un appareil Panorama M-Series ou vers un appareil virtuel. Cependant, parce que la base de données des journaux est trop grande pour l'exporter ou l'importer afin qu'elle puisse être utilisée, les modèles suivants ne prennent pas en charge l'exportation ou l'importation de la base de données des journaux en entier : Pare-feu PA-7000 Series (toutes les versions de PAN-OS®), appareils virtuels Panorama exécutant Panorama 6.0 ou versions ultérieures, et appareils Panorama M-Series (toutes les versions de Panorama).

*** Untranslated ***	Description
Gestion de la configuration	
Rétablir la dernière configuration enregistrée	Restaure l'instantané par défaut (.snapshot.xml) de la configuration candidate (l'instantané que vous créez ou que vous remplacez lorsque vous sélectionnez **Config (Configuration)** > **Save Changes (Enregistrer les modifications)** dans le coin supérieur droit de l'interface Web). (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à annuler. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Revenir à la configuration en cours d'exécution	Restaure la configuration active actuelle. Cette opération annule toutes les modifications apportées par chaque administrateur à la configuration candidate depuis la dernière validation. Pour annuler uniquement les changements d'administrateurs spécifiques, voir Annuler les changements. (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à annuler. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
Sauvegarder le cliché de la configuration nommée	Crée un instantané de la configuration candidate qui ne remplace pas l'instantané par défaut (.snapshot.xml). Saisissez un **Nom** pour l'instantané ou sélectionnez un instantané nommé existant à remplacer. (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à enregistrer. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Sauvegarder la configuration candidate	Crée ou remplace l'instantané par défaut de la configuration candidate (.snapshot.xml) par la configuration candidate actuelle. Il s'agit de la même action que lorsque vous sélectionnez **Config (Configuration)** > **Save Changes (Enregistrer les modifications)** dans le coin supérieur droit de l'interface Web. Pour sauvegarder uniquement les modifications d'administrateurs spécifiques, voir Enregistrer les configurations candidates. (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à enregistrer. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Charger l'instantané de la configuration (pare-feu) OU Charger l'instantané de la configuration nommé Panorama	Remplace la configuration candidate actuelle par l'une des options suivantes : • Instantané au nom personnalisé de la configuration candidate (plutôt que l'instantané par défaut). • Configuration active au nom personnalisé que vous avez importé. • Configuration active actuelle. La configuration doit demeurer sur le pare-feu ou sur le Panorama sur lequel vous le chargez. Sélectionnez le **Name (Nom)** de la configuration et saisissez la **Decryption Key (Clé de décryptage)** qui est la clé principale du pare-feu ou de Panorama (voir Périphérique > Clé principale et diagnostics). La clé principale est requise pour décrypter tous les mots de passe et les clés privées de la configuration. Si vous chargez une configuration importée, vous devez saisir la clé principale du pare-feu ou de Panorama à partir duquel vous réalisez l'importation. Une fois l'opération de chargement terminée, la clé principale du pare-feu ou de Panorama sur laquelle vous avez chargé la configuration recrypte les mots de passe et les clés privées. Pour générer de nouveaux UUID pour toutes les règles de la configuration (par exemple, si vous chargez une configuration d'un autre pare-feu tout en souhaitant préserver les règles uniques lors du chargement de cette configuration), le super utilisateur doit **Regenerate Rule UUIDs for selected named configuration (Régénérer les UUID de la règle pour la configuration nommée qui est sélectionnée)** afin de générer de nouveaux UUID pour toutes les règles.

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	(Panorama uniquement) Précisez les configurations d'objet, de politique, de groupe de périphériques ou de modèles pour charger partiellement les configurations à partir des configurations nommées en faisant votre sélection à partir de ce qui suit : • **Load Shared Objects (Charger les objets partagés)** : Chargez uniquement les objets partagés ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Load Shared Policies (Charger les politiques partagées)** : Chargez uniquement les politiques partagées ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** : Sélectionnez les configurations de groupes de périphériques, de modèles ou de piles de modèles à charger. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté. • **Retain Rule UUIDs (Préserver les UUID de la règle)** : Conservez les UUID de la configuration active.
Charger la version de la configuration (pare-feu) OU Charger la version de la configuration Panorama	Remplace la configuration candidate actuelle par une version précédente de la configuration en cours d'exécution qui est stockée sur le pare-feu ou sur Panorama. Sélectionnez le **Name (Nom)** de la configuration et saisissez la **Decryption Key (Clé de décryptage)** qui est la clé principale du pare-feu ou de Panorama (voir Périphérique > Clé principale et diagnostics). La clé principale est requise pour décrypter tous les mots de passe et les clés privées de la configuration. Une fois l'opération de chargement terminée, la clé principale recrypte les mots de passe et les clés privées. (Panorama uniquement) Précisez les configurations d'objet, de politique, de groupe de périphériques ou de modèles pour charger partiellement les configurations à partir des configurations nommées en faisant votre sélection : • **Load Shared Objects (Charger les objets partagés)** : Chargez uniquement les objets partagés ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Load Shared Policies (Charger les politiques partagées)** : Chargez uniquement les politiques partagées ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** : Sélectionnez les configurations de groupes de périphériques, de modèles ou de piles de modèles à charger. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter l'instantané de la configuration	Exporte la configuration active actuelle, un instantané de la configuration candidate ou une configuration précédemment importée (candidate ou active). Le pare-feu exporte la configuration sous la forme d'un fichier XML

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	avec le nom spécifié. Vous pouvez enregistrer l'instantané dans n'importe quel emplacement réseau. (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à exporter. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter la version de la configuration	Exporte une **Version** de la configuration active sous la forme d'un fichier XML. (Panorama uniquement) **Select Device Groups & Templates (Sélectionnez les groupes de périphériques et les modèles)** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à exporter. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter la solution de configuration des périphériques et de Panorama (Panorama uniquement)	Génère et exporte les dernières versions de la configuration de secours en cours d'exécution de Panorama et de chaque pare-feu géré. Pour automatiser le processus de création et exporter la solution de configuration quotidienne vers un serveur SCP ou FTP, voir Panorama > Déploiement du périphérique.
Exporter ou appliquer la solution de configuration des périphériques (Panorama uniquement)	Vous invite à sélectionner un pare-feu et à effectuer l'une des actions suivantes sur la configuration de pare-feu stockée sur Panorama : • **Appliquez et validez** la configuration sur le pare-feu. Cette action nettoie le pare-feu (supprime toute configuration locale de celui-ci) et applique la configuration de pare-feu stockée sur Panorama. Après l'importation d'une configuration de pare-feu, utilisez cette option pour nettoyer le pare-feu pour pouvoir le gérer à l'aide de Panorama. • **Export (Exportez)** la configuration vers le pare-feu sans la charger. Pour charger la configuration, vous devez accéder à la CLI du pare-feu et exécuter la commande de mode de configuration **load device-state**. Cette commande nettoie le pare-feu comme l'option **Push & Commit (Appliquer & valider)**. *Ces options ne sont disponibles que pour les pare-feu exécutant PAN-OS 6.0.4 et ses versions ultérieures.*
Exporter l'état du périphérique (Pare-feu uniquement)	Exporte les informations relatives à l'état du pare-feu sous la forme d'un module. En plus de la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect™, le module comprend également des informations relatives au certificat, une liste des satellites que le portail gère et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	restaurer les informations exportées relatives au remplacement en important le module d'état. *Vous pouvez exécuter manuellement l'exportation de l'état du pare-feu ou créer un script d'API XML planifié afin d'exporter le fichier sur un serveur distant. Cette tâche doit être régulièrement exécutée puisque les certificats des satellites font fréquemment l'objet de modifications.* Pour créer le fichier d'état du pare-feu à partir de la CLI, en mode de configuration, exécutez la commande **`save device state`**. Le nom du fichier sera `device_state_cfg.tgz` et il sera stocké dans `/opt/pancfg/mgmt/device-state`. La commande opérationnelle pour exporter le fichier d'état du pare-feu est **`scp export device-state`** (vous pouvez aussi utiliser **`tftp export device-state`**). Pour plus d'informations sur l'utilisation de l'API XML ou REST, consultez la section Guide de l'API de Panorama et de PAN-OS.
Importer l'instantané de la configuration	Importe une configuration active ou candidate à partir d'un emplacement réseau. Cliquez sur **Browse (Parcourir)** et sélectionnez le fichier de configuration à importer.
Importer l'état du périphérique (Pare-feu uniquement)	Permet d'importer le module d'informations relatives à l'état que vous avez exporté d'un pare-feu lorsque vous avez décidé de **Export device state (Exporter l'état du périphérique)**. Outre la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect, le module comprend également des informations relatives au certificat, une liste des satellites et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez restaurer les informations relatives au remplacement en important le module d'état.
Importer la configuration de périphérique vers Panorama (Panorama uniquement)	Permet d'importer une configuration de pare-feu vers Panorama. Panorama crée automatiquement un modèle contenant les configurations réseau et de périphérique. Pour chaque système virtuel (vsys) sur le pare-feu, Panorama crée automatiquement un groupe de périphériques qui contiendra les configurations de politique et d'objet. Les groupes de périphériques se situeront un niveau en dessous de l'emplacement Partagé dans la hiérarchie, même si vous pouvez les réaffecter à un autre groupe de périphériques parent une fois l'importation terminée (voir Panorama > VMware NSX). *Les versions de contenu sur Panorama (la base de données d'applications et de menaces par exemple) doivent être supérieures ou égales aux versions sur le pare-feu duquel vous importerez une configuration.* Configurez les options d'importation suivantes : • **Device (Périphérique)** : sélectionnez le pare-feu duquel Panorama importera les configurations. Le menu déroulant comprend uniquement les pare-feu connectés à Panorama et non affectés à un autre groupe de

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	périphériques ou modèle. Vous pouvez ne sélectionner qu'un pare-feu dans son ensemble, et non un système virtuel individuel. • **Template Name (Nom du modèle)** : donnez un nom au modèle qui contiendra les paramètres de périphérique et réseau importés. Pour un pare-feu à plusieurs systèmes virtuels, ce champ est vide. Pour les autres pare-feu, la valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser le nom d'un modèle existant. • **Device Group Name Prefix (Préfixe de nom du groupe de périphériques)** (pare-feu à plusieurs systèmes virtuels uniquement) : facultativement, ajoutez une chaîne de caractères comme préfixe pour chaque nom de groupe de périphériques. • **Device Group Name (Nom du groupe de périphériques)** : pour un pare-feu à plusieurs systèmes virtuels, chaque groupe de périphérique comporte un nom de système virtuel par défaut. Pour les autres pare-feu, la valeur par défaut est le nom du pare-feu. Vous pouvez modifier les noms par défaut, mais vous ne pouvez pas utiliser le nom d'un groupe de périphériques existant. • **Import devices' shared objects into Panorama's shared context (Importer les objets partagés des périphériques vers le contexte partagé de Panorama)** (activé par défaut) – Panorama importe des objets appartenant à Partagé sur le pare-feu vers Partagé sur Panorama. *Panorama prend en considération tous les objets partagés sur un pare-feu sans avoir besoin de plusieurs systèmes virtuels. Si vous désactivez cette option, Panorama copie les objets de pare-feu partagés dans des groupes de périphériques au lieu de Partagé. Ce paramètre inclut les exceptions suivantes :* • Si un objet de pare-feu partagé a le même nom et la même valeur qu'un objet Panorama partagé existant, l'importation exclut cet objet pare-feu. • Si le nom ou la valeur de l'objet de pare-feu partagé est différent de l'objet Panorama partagé, Panorama importe l'objet de pare-feu dans chaque groupe de périphériques. • Si une configuration importée dans un modèle fait référence à un objet de pare-feu partagé, Panorama importe cet objet dans Partagé que vous sélectionniez l'option ou non. • Si un objet de pare-feu partagé fait référence à une configuration importée dans un modèle, Panorama importe l'objet dans un groupe de périphériques que vous sélectionniez l'option ou non. • **Rule Import Location (Emplacement d'importation de règle)** : sélectionnez si Panorama importera les politiques en tant que pré ou post-règles. Quel que soit votre choix, Panorama importe les règles de sécurité par défaut (défaut intrazone et interzone) dans la post-règle de base. *Si Panorama comporte une règle portant le même nom qu'une règle de pare-feu que vous importez, Panorama affiche les deux règles. Les noms de règles doivent*

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	toutefois être uniques : supprimez une des règles avant de valider sur Panorama, sinon la validation échouera.
Opérations périphérique	
Redémarrer	Pour redémarrer le pare-feu ou Panorama, **Reboot Device (Redémarrez le périphérique)**. Le pare-feu ou Panorama vous déconnecte, recharge le logiciel (PAN-OS ou Panorama) et la configuration active, ferme et consigne les sessions existantes, et crée une entrée de journal système pour noter le nom de l'administrateur à l'origine de l'arrêt. Toutes les modifications apportées à la configuration et non enregistrées ou validées sont perdues (voir Périphérique > Configuration > Opérations). *Si l'interface Web n'est pas disponible, utilisez la commande opérationnelle de la CLI suivante :* `request restart system`
Arrêter	Pour procéder à un arrêt progressif du pare-feu ou de Panorama, **Shutdown Device (Arrêtez le périphérique)** ou **Shutdown Panorama (Arrêtez Panorama)**, puis cliquez sur **Yes (Oui)** lorsque vous êtes invité à le faire. Toutes les modifications apportées à la configuration et non enregistrées ou validées sont perdues. Tous les administrateurs sont déconnectés et le processus suivant se produit'A0;: • Toutes les sessions de connexion sont fermées. • Les interfaces sont désactivées. • Tous les processus du système sont arrêtés. • Les sessions en cours sont fermées et consignées. • Des journaux système indiquant le nom de l'administrateur à l'origine de l'arrêt sont créés. Si cette entrée du journal ne peut pas être écrite, un avertissement s'affiche et le système n'est pas arrêté. • Les lecteurs de disques sont démontés de manière appropriée et le pare-feu ou Panorama est mis hors tension. Vous devez débrancher la source d'alimentation puis la rebrancher avant de remettre le pare-feu ou Panorama sous tension. *Si l'interface Web n'est pas disponible, utilisez la commande de la CLI :* `request shutdown system`
Redémarrer le panneau de données	**Restart Dataplane (Redémarrez le panneau de données)** pour relancer les fonctions de données du pare-feu sans redémarrer. Cette option n'est pas disponible sur les pare-feu Panorama ou de la série PA-220, PA-800 ou VM-Series. *Si l'interface Web n'est pas disponible, utilisez la commande de la CLI :* `request restart dataplane`

© 2020 Palo Alto Networks, Inc.

*** Untranslated ***	Description
	Sur les pare-feu de la série PA-7000, chaque NPC possède un data plane afin que vous puissiez redémarrer le NPC pour effectuer cette opération en exécutant la commande **`request chassis restart slot`**.
Divers	
Personnaliser les logos	Utilisez **Custom Logos (Personnaliser les logos)** pour personnaliser les éléments suivants : • Image de l'arrière-plan du **Login Screen (Écran de connexion)** • Image de l'en-tête de la **Main UI (interface utilisateur principale)** (interface Web) • Image de la **PDF Report Title Page (Page de titre du rapport PDF)**. Voir Surveillance > Rapports PDF > Gérer le récapitulatif PDF. • Image du **PDF Report Footer (Pied de page du rapport PDF)**. Chargez (<image>) un fichier image pour la prévisualiser ou pour supprimer ( ) une image précédemment chargée. Pour rétablir le logo par défaut, supprimez votre entrée et **Commit (Validez)**. Pour le **Login Screen (Écran de connexion)** et la **Main UI (Interface utilisateur principale)**, vous pouvez afficher ( ) l'image comme elle apparaîtra ; au besoin, le pare-feu recadre l'image aux dimensions de la page. Pour les rapports PDF, le pare-feu redimensionne automatiquement les images pour qu'elles correspondent aux dimensions de la page sans rognage. Dans tous les cas de figure, l'aperçu présente les dimensions recommandées pour l'image. La taille maximale d'image d'un logo est de 128 Ko. Les types de fichier pris en charge sont .png, .gif et .jpg. Le pare-feu ne prend pas en charge les fichiers d'image qui sont entrelacés ou qui contiennent des canaux alpha, car ces fichiers interfèrent avec la génération de rapports PDF. Il se peut que vous deviez contacter l'illustrateur qui a créé l'image pour en supprimer les canaux alpha, ou vous assurer que le grapheur utilisé n'enregistre pas les fichiers avec la fonction de canal alpha. Pour plus d'informations sur la génération de rapports PDF, voir Surveillance > Rapports PDF > Gérer le résumé PDF.
Réglage SNMP	Activation de la surveillance SNMP.
Configuration de la partition de stockage (uniquement sur Panorama)	Partitions de stockage des journaux pour un appareil virtuel Panorama en mode hérité.

Activation de la surveillance SNMP

- Périphérique > Configuration > Opérations

© 2020 Palo Alto Networks, Inc.

SNMP (Simple Network Management Protocol) est un protocole standard permettant la surveillance des périphériques sur votre réseau. Sélectionnez **Operations (Opérations)** pour configurer le pare-feu afin qu'il utilise la version SNMP prise en charge par votre gestionnaire SNMP (SNMPv2c ou SNMPv3). Pour obtenir la liste des MIB que vous devez charger dans le gestionnaire SNMP afin qu'il puisse interpréter les statistiques qu'il collecte sur le pare-feu, reportez-vous à MIB prises en charge. Pour configurer le profil de serveur permettant au pare-feu de communiquer avec les destinations de pièges SNMP sur votre réseau, reportez-vous à la section Périphérique > Profils de serveur > Piège SNMP. Les MIB SNMP définissent tous les objets SNMP et événements générés par le pare-feu. Un piège SNMP identifie un événement par un ID d'objet (OID) unique et chaque champ est défini comme liste de liaisons de variables. Cliquez sur **Configuration SNMP** et définissez les paramètres suivants pour autoriser les requêtes SNMP GET de votre gestionnaire SNMP :

Champ	Description
Emplacement physique	Indiquez l'emplacement physique du pare-feu. Lorsqu'un journal ou un piège est généré, ces informations vous permettent d'identifier (dans un gestionnaire SNMP) le pare-feu qui a généré la notification.
Contact	Saisissez le nom ou l'adresse de courrier électronique de la personne en charge de la gestion du pare-feu. Ce paramètre est rapporté dans le MIB d'informations du système standard.
Utiliser les définitions des pièges spécifiques	Cette option est sélectionnée par défaut, ce qui signifie que le pare-feu utilise un OID unique pour chaque piège SNMP en fonction du type d'événement. Si vous désélectionnez cette option, tous les pièges porteront le même OID.
Version	Sélectionnez la version de SNMP : **V2c** (par défaut) ou **V3**. Votre sélection détermine les autres champs affichés dans la boîte de dialogue.
Pour SNMP V2c	
Chaîne de communauté SNMP	Saisissez la chaîne de communauté qui identifie une *communauté* SNMP de gestionnaires SNMP et de périphériques surveillés, et qui sert également de mot de passe pour authentifier les membres de la communauté entre eux lorsqu'ils échangent des messages SNMP get (requêtes de statistiques) et de pièges. La chaîne peut comporter 127 caractères maximum, accepte tous les caractères et est sensible à la casse. *Il convient de ne pas utiliser la chaîne de communauté publique définie par défaut. Les messages SNMP contenant des chaînes de communautés en clair, tenez compte des exigences de sécurité de votre réseau lors de la définition de l'appartenance à la communauté (accès administrateur).*
Pour SNMP V3	
Nom / Vue	Vous pouvez affecter un groupe d'une ou plusieurs vues à l'utilisateur d'un gestionnaire SNMP afin de contrôler les objets MIB (statistiques) que l'utilisateur peut obtenir du pare-feu. Chaque vue est constituée d'une paire OID/masque de niveau bit : l'OID définit un MIB et le masque (au format hexadécimal) définit les objets qui sont accessibles à l'intérieur (inclure correspondance) ou à l'extérieur (exclure correspondance) de ce MIB.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Par exemple, si l'**OID** est 1.3.6.1, que l'**Option** de correspondance est définie sur **inclure** et le **Masque** est 0xf0, les OID des objets demandés par l'utilisateur doivent correspondre aux quatre premiers nœuds (f = 1111) de 1.3.6.1. Les objets ne doivent pas nécessairement correspondre aux nœuds restants. Dans cet exemple, 1.3.6.1.2 correspond au masque et 1.4.6.1.2 n'y correspond pas. Pour chaque groupe de vues, cliquez sur **Add (Ajouter)**, donnez un **Name (Nom)** au groupe, puis configurez les paramètres suivants pour chaque vue que vous **Add (Ajouter)** au groupe : • **View (Vue)** : donnez un nom à la vue. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union. • **OID** : indiquez l'OID du MIB. • **Option** : sélectionnez la logique de correspondance à appliquer au MIB. • **Mask (Masque)** : indiquez le masque au format hexadécimal.  *Pour pouvoir accéder à toutes les informations de gestion, utilisez l'OID de niveau supérieur 1.3.6.1, et définissez le Mask (Masque) sur 0xf0 et l'Option de correspondance sur include (inclure).*
Users (Utilisateurs)	Les comptes utilisateur SNMP fournissent l'authentification, la confidentialité et le contrôle d'accès lorsque des pare-feu transfèrent des pièges et que des gestionnaires SNMP obtiennent des statistiques de pare-feu. Pour chaque utilisateur, cliquez sur **Add (Ajouter)** et configurez les paramètres suivants : • **Users (Utilisateurs)** : indiquez un nom d'utilisateur pour identifier le compte utilisateur SNMP. Le nom d'utilisateur que vous configurez sur le pare-feu doit correspondre au nom d'utilisateur configuré sur le gestionnaire SNMP. Le nom d'utilisateur peut comporter 31 caractères maximum. • **View (Vue)** : affectez un groupe de vues à l'utilisateur. • **Auth Password (Mot de passe d'authentification)** : indiquez le mot de passe d'authentification de l'utilisateur. Le pare-feu utilise le mot de passe pour s'authentifier auprès du gestionnaire SNMP lors du transfert de pièges et de la réponse à des requêtes de statistiques. Le pare-feu utilise l'algorithme Secure Hash Algorithm (SHA-1 160) pour chiffrer le mot de passe. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés. • **Priv Password (Mot de passe privé)** : indiquez le mot de passe privé de l'utilisateur. Le pare-feu utilise le mot de passe et la norme Advanced Encryption Standard (AES-128) pour crypter les pièges SNMP et les réponses aux requêtes de statistiques. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Module de sécurité matériel

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM** pour configurer un Hardware Security Module (module de sécurité matériel ; HSM), pour effectuer des opérations et pour afficher le statut du HSM.

Que voulez-vous faire ?	Reportez-vous à la section :
Quel est le but d'un module de sécurité matériel (HSM) et où puis-je trouver des procédures de configuration détaillées ?	Sécurisation des clés avec un module de sécurité matériel (HSM)
Configurer :	Paramètres du fournisseur du module matériel de sécurité
	Authentication HSM
Effectuer des opérations matérielles de sécurité	Opérations matérielles de sécurité
Comment puis-je afficher le statut du HSM ?	Configuration et état du fournisseur du module matériel de sécurité matériel
	Statut du module matériel de sécurité

Paramètres du fournisseur du module matériel de sécurité

Pour configurer un module de sécurité matériel sur le pare-feu, modifiez les paramètres du module de sécurité matériel.

Paramètres du fournisseur du module matériel de sécurité	Description
Fournisseur configuré	Sélectionnez le fournisseur HSM : • **None (Aucun)** (par défaut) : le pare-feu ne se connecte à aucun module de sécurité matériel. • **HSM Réseau SafeNet** • **nCipher nShield Connect** *La version du serveur HSM doit être compatible avec la version du client HSM installée sur le pare-feu.*
Nom du module	Ajoutez un nom au module de sécurité matériel. Il peut s'agir de n'importe quelle chaîne'A0;ASCII de 31'A0;caractères maximum. Ajoutez un maximum de 16 noms de module si vous configurez des modules de sécurité matériels SafeNet haute disponibilité ou indépendants.

© 2020 Palo Alto Networks, Inc.

Paramètres du fournisseur du module matériel de sécurité	Description
Adresse du serveur	Indiquez une adresse IPv4 pour chaque module de sécurité matériel configuré.
Haute disponibilité (Réseau SafeNet uniquement)	(Facultatif) Sélectionnez cette option si vous définissez des modules de sécurité matériels SafeNet dans une configuration haute disponibilité. Vous devez configurer le nom du module et l'adresse du serveur de chaque module de sécurité matériel.
Tentative de rétablissement automatique (Réseau SafeNet uniquement)	Indiquez le nombre de fois que le pare-feu tente de rétablir la connexion à un module de sécurité matériel avant de basculer vers un autre dans une configuration de module de sécurité matériel haute disponibilité (plage de 0 à 500 ; valeur par défaut de 0).
Nom du groupe de haute disponibilité (Réseau SafeNet uniquement)	Donnez un nom au groupe de modules de sécurité matériels haute disponibilité. Ce nom est utilisé en interne par le pare-feu. Il peut s'agir de n'importe quelle chaîne'A0;ASCII de 31'A0;caractères maximum.
Supprimer l'adresse du système de fichiers nCipher nShield Connect uniquement	Configurez l'adresse IPv4 du système de fichiers distant utilisé dans la configuration du module de sécurité matériel nCipher nShield Connect.

Authentication HSM

Sélectionnez **Setup Hardware Security Module (Paramétrer le module de sécurité matériel)** et configurez les paramètres suivants pour authentifier le pare-feu sur le module de sécurité matériel.

Authentification du module HSM	
Nom du serveur	Sélectionnez le nom du serveur du module de sécurité matériel dans le menu déroulant.
Mot de passe de l'administrateur	Saisissez le mot de passe administrateur du module de sécurité matériel pour authentifier le pare-feu sur le module de sécurité matériel.

Opérations matérielles de sécurité

Pour effectuer une opération sur le module de sécurité matériel (HSM) ou le pare-feu connecté au HSM, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM (Module de sécurité matériel)**, puis sélectionnez l'une des opérations de matérielles de sécurité suivantes :

© 2020 Palo Alto Networks, Inc.

Opérations matérielles de sécurité	
Configurer le module matériel de sécurité	Configure le pare-feu pour qu'il s'authentifie auprès d'un HSM.
Afficher les informations détaillées	Affiche des informations sur les serveurs HSM, sur l'état de la haute disponibilité HSM et sur le matériel HSM.
Synchroniser avec le système de fichiers distants (HSM nCipher nShield Connect uniquement)	Synchronise les données de clés provenant du système de fichiers distants de HSM nShield Connect avec le pare-feu.
Réinitialiser la configuration	Supprime toutes les connexions HSM au pare-feu. Vous devez répéter toutes la procédures d'authentification avant de réinitialiser la configuration HSM.
Sélectionner la version du client HSM (HSM Réseau SafeNet uniquement))	Vous permet de choisir la version du logiciel qui s'exécute sur le client HSM (le pare-feu). La version du client HSM doit être compatible avec la version du serveur HSM. Reportez-vous à la documentation du fournisseur HSM pour une matrice de compatibilité de la version client/serveur.

Configuration et état du fournisseur du module matériel de sécurité matériel

La section Fournisseur du module de matériel de sécurité vous permet de visualiser les paramètres de configuration HSM et l'état de connectivité du HSM.

Statut du fournisseur du module matériel de sécurité	
Fournisseur configuré	Sélectionnez le fournisseur HSM configuré sur le pare-feu : • **None** • **HSM Réseau SafeNet** • **nCipher nShield Connect**
Haute disponibilité	(Réseau SafeNet uniquement) La haute disponibilité du module de sécurité matériel est configurée.
Nom du groupe de haute disponibilité	(Réseau SafeNet uniquement) Nom du groupe configuré sur le pare-feu pour la haute disponibilité du module de sécurité matériel.
Adresse source du pare-feu	Adresse du port utilisé pour le module de sécurité matériel. Il s'agit par défaut de l'adresse du port de gestion. Toutefois, une autre adresse de port peut être spécifiée dans la fenêtre Services Route Configuration (Configuration de l'itinéraire de service) en sélectionnant **Device (Périphérique)** > **Setup (Configuration)** > **Services**.
Clé principale sécurisée par HSM	Cochez cette case pour sécuriser la clé principale par le module de sécurité matériel.

© 2020 Palo Alto Networks, Inc.

Statut du fournisseur du module matériel de sécurité	
Status (État)	S'affiche en vert si le pare-feu est connecté et authentifié au HSM et s'affiche en rouge si le pare-feu n'est pas authentifié ou si la connectivité réseau vers le HSM est désactivée. Vous pouvez également voir l'État du module du matériel de sécurité pour plus de détails sur la connexion HSM.

Statut du module matériel de sécurité

L'État du module de sécurité matériel comprend les informations suivantes sur les modules de sécurité matériels qui ont été authentifiés avec succès. L'affichage diffère en fonction du fournisseur de modules de sécurité matériels configuré (SafeNet ou nCipher).

Statut du module matériel de sécurité	
HSM Réseau SafeNet	• **Numéro de série** – Le numéro de série de la partition du module de sécurité matériel s'affiche si celle-ci a été authentifiée avec succès. • **Partition** – Le nom de la partition du module de sécurité matériel qui a été affectée sur le pare-feu. • **État du module** – L'état de fonctionnement actuel du module de sécurité matériel. Le champ affiche **Authentifié** si le HSM s'affiche dans ce tableau.
nCipher nShield Connect	• **Nom** – Le nom du Serveur du module de sécurité matériel. • **Adresse IP** – L'adresse IP du HSM qui a été affecté sur le pare-feu. • **État du module** – L'état de fonctionnement actuel du module de sécurité matériel. Ce paramètre affiche **Authentifié** si le pare-feu a été authentifié avec succès au HSM et affiche **Non authentifié** si l'authentification a échoué.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Services

Les rubriques suivantes décrivent les paramètres des services de système globaux et virtuels sur le pare-feu :

- configuration des services pour les systèmes globaux et virtuels ;
- Paramètres des services globaux
- Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l'itinéraire de service
- Route pour le service de destination

configuration des services pour les systèmes globaux et virtuels ;

Sur un pare-feu sur lequel plusieurs systèmes virtuels sont activés, sélectionnez **Services** pour afficher les onglets **Global** et **Systèmes virtuels** sur lesquels vous définissez des services utilisés respectivement par le pare-feu ou ses systèmes virtuels pour fonctionner efficacement. (Si le pare-feu comporte un seul système virtuel ou si plusieurs systèmes virtuels sont désactivés, l'onglet **Systèmes virtuels** ne s'affiche pas.)

Sélectionnez **Global** pour définir des services pour l'ensemble du pare-feu. Ces paramètres sont également utilisés comme valeurs par défaut pour les systèmes virtuels pour lesquels aucun paramètre personnalisé n'est défini pour un service.

- Modifiez **Services** pour définir les adresses IP de destination des serveurs DNS, du Serveur de mises à jour et du Serveur proxy. L'onglet **NTP** vous permet de configurer les paramètres NTP (Network Time Protocol). Pour obtenir une description des options Services disponibles, reportez-vous à la section Table 12.
- Dans **Service Features (Fonctions de service)**, cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)** pour définir comment le pare-feu communiquera avec les autres serveurs/périphériques pour des services tels que DNS, messagerie, LDAP, RADIUS, Syslog, et bien d'autres encore. Deux méthodes de configuration des itinéraires de service sont possibles :
  - L'option **Use Management Interface for all (Utiliser l'interface de gestion pour tous)** force toutes les communications de services du pare-feu avec des serveurs externes via l'interface de gestion (MGT). Si vous sélectionnez cette option, vous devez configurer l'interface MGT pour qu'elle autorise les communications entre le pare-feu et les serveurs/périphériques qui proposent des services. Pour configurer l'interface MGT, sélectionnez Périphérique > Configuration > Gestion et modifiez les paramètres.
  - L'option **Customize (Personnaliser)** vous permet de contrôler de manière granulaire la communication du service en configurant une interface source spécifique et une adresse IP utilisées par le service comme interface de destination et adresse IP de destination dans sa réponse. (Par exemple, vous pouvez configurer une adresse IP / interface source spécifique pour la messagerie entre le pare-feu et un serveur de messagerie et utiliser une autre adresse IP / interface source pour les Services Palo Alto.) Sélectionnez le ou les services que vous souhaitez personnaliser sur les mêmes paramètres, puis cliquez sur **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)**. Les services sont répertoriés dans la Table 13, qui indique si un service peut être configuré pour le pare-feu **Global** ou des **Systèmes virtuels** et si le service prend en charge une adresse source IPv4 et/ou IPv6.

L'onglet **Destination** est une autre fonction d'itinéraire de service Global que vous pouvez personnaliser. Cet onglet s'affiche dans la fenêtre Configuration de l'itinéraire de service et est décrit dans la section Itinéraire de service de destination.

Utilisez l'onglet **Virtual Systems (Systèmes virtuels)** pour définir les itinéraires de service d'un système virtuel unique. Sélectionnez un Emplacement (système virtuel), puis cliquez sur **ervice Route Configuration (Configuration de l'itinéraire de service)**. Sélectionnez **Hériter de la configuration d'itinéraire de service global** ou **Personnaliser** des itinéraires de service pour un système virtuel. Si vous choisissez de

© 2020 Palo Alto Networks, Inc.

personnaliser des paramètres, sélectionnez **IPv4** ou **IPv6**. Sélectionnez le ou les services que vous souhaitez personnaliser sur les mêmes paramètres, puis cliquez sur **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)**. Reportez-vous à la Table 13 pour les services pouvant être personnalisés.

Pour contrôler et rediriger des requêtes DNS entre des systèmes virtuels partagés et spécifiques, vous pouvez utiliser un proxy DNS et un profil de Serveur DNS.

Paramètres des services globaux

- Périphérique > Configuration > Services

Pour contrôler et rediriger des requêtes DNS entre des systèmes virtuels partagés et spécifiques, vous pouvez utiliser un proxy DNS et un profil de Serveur DNS.

Paramètres des services globaux	Description
Services	
Serveur de mises à jour	Correspond à l'adresse IP ou au nom d'hôte du serveur à partir duquel télécharger les mises à jour de Palo Alto Networks. La valeur actuelle est **updates.paloaltonetworks.com**. Ne modifiez ce paramètre que si le support technique vous demande de le faire.
Vérifier l'identité du serveur de mises à jour	Si vous activez cette option, le pare-feu ou Panorama vérifie que le serveur sur lequel est téléchargé le module logiciel ou de contenu dispose d'un certificat SSL signé par une autorité de confiance. Cette option ajoute un niveau de sécurité supplémentaire à la communication entre les pare-feu ou les serveurs Panorama et le serveur de mises à jour. *Vérifiez l'identité du serveur de mise à jour afin de valider que le serveur dispose d'un certificat SSL signé par une autorité de confiance.*
Paramètres DNS	Choisissez le type de service DNS (**Servers (Serveurs)** ou **DNS Proxy Object (Objet de proxy DNS)**) pour toutes les requêtes DNS provenant du pare-feu afin de prendre en charge des objets d'adresse FQDN, la journalisation et la gestion du pare-feu. Les options disponibles sont les suivantes'A0;: • Serveurs DNS principal et secondaire pour permettre la résolution du nom de domaine. • Un proxy DNS configuré sur le pare-feu constitue une autre méthode de configuration des serveurs DNS. Si vous activez un proxy DNS, vous devez activer **Cache** et **EDNS Cache Responses (Réponses EDNS Cache)** (**Network (Réseau)** > **DNS Proxy (Proxy DNS)** > **Advanced (Avancé)**).
Serveur DNS principal	Saisissez l'adresse IP du serveur DNS principal à utiliser pour la résolution des requêtes DNS provenant du pare-feu. Par exemple, pour trouver le serveur de mise à jour, pour résoudre des entrées DNS dans des journaux ou pour résoudre des objets d'adresse FQDN.
Serveur DNS secondaire	(Facultatif) Saisissez l'adresse IP d'un serveur DNS secondaire à utiliser si le serveur principal n'est pas disponible.

© 2020 Palo Alto Networks, Inc.

Paramètres des services globaux	Description
Fréquence d'actualisation minimale du FQDN (sec)	Définissez une limite quant à la vitesse d'actualisation par le pare-feu des FQDN qu'il reçoit d'un DNS. Le pare-feu actualise un FQDN en fonction de la TTL du FQDN tant que la TTL est supérieure ou égale à ce **Minimum FQDN Refresh Time (Fréquence d'actualisation minimale du FQDN)** (en secondes). Si la TTL est inférieure à cette fréquence d'actualisation minimale du FQDN, le pare-feu actualise le FQDN en fonction de la fréquence d'actualisation minimale du FQDN (c'est-à-dire que le pare-feu ne respecte pas les TTL qui sont plus rapides que ce paramètre). La minuterie commence lorsque le pare-feu reçoit une réponse DNS d'un serveur DNS ou d'un objet de proxy DNS pour résoudre le FQDN (plage comprise entre 0 et 14 400 ; la valeur par défaut est 30). Si le paramètre est défini sur 0, le pare-feu actualisera le FQDN en fonction de la valeur TTL du DNS et n'applique pas une fréquence d'applications minimale du FQDN.  *Si la TTL du FQDN du DNS est courte, mais que les résolutions FQDN ne changent pas aussi souvent que le délai TTL, une fréquence d'actualisation plus rapide n'est pas nécessaire. Vous devriez donc définir une fréquence d'actualisation minimale du FQDN pour éviter des tentatives d'actualisation du FQDN non nécessaires.*
Délai de temporisation des entrées obsolètes du FQDN (min.)	Précisez la durée de temps (en minutes) pendant laquelle le pare-feu continue à utiliser des résolutions FQDN obsolètes en cas d'échec du réseau ou d'un serveur DNS inaccessible — lorsqu'un FQDN n'est pas actualisé (la plage est comprise entre 0 et 10 080 ; la valeur par défaut est 1 440). Une valeur nulle indique que le pare-feu ne continue pas d'utiliser une entrée obsolète. Si le serveur DNS demeure inaccessible à la fin du délai de temporisation de l'état, l'entrée FQDN devient non résolue (les résolutions d'état sont supprimées).  *Assurez-vous que la valeur de FQDN Stale Entry Timeout (Délai de temporisation des entrées obsolètes du FQDN) est suffisamment courte pour ne pas autoriser le transfert incorrect de trafic (qui présente un risque à la sécurité), mais suffisamment longue pour permettre la continuité du trafic sans causer de panne réseau non planifiée.*
Section Serveur proxy	
Serveur	Si le pare-feu doit utiliser un serveur proxy pour accéder aux services de mises à jour Palo Alto Networks, saisissez l'adresse IP ou le nom d'hôte du serveur proxy.
Port	Saisissez le port du serveur proxy
Utilisateur	Saisissez le nom d'utilisateur que l'administrateur doit entrer lorsqu'il accède au serveur proxy.
Mot de passe/ Confirmer le mot de passe	Saisissez et confirmez le mot de passe que l'administrateur doit entrer pour accéder au serveur proxy.

© 2020 Palo Alto Networks, Inc.

Paramètres des services globaux	Description
NTP	
Adresse du serveur NTP	Saisissez l'adresse IP ou le nom d'hôte d'un serveur NTP que vous utiliserez pour synchroniser l'horloge du pare-feu. Vous pouvez éventuellement saisir l'adresse IP ou le nom d'hôte d'un second serveur NTP à utiliser pour synchroniser l'horloge du pare-feu, si le serveur principal devient indisponible. *Lorsqu'un serveur NTP conserve la synchronisation de toutes les horloges du pare-feu réseau, les travaux planifiés sont exécutés comme prévu et les horodatages peuvent permettre d'identifier les causes profondes des problèmes touchant plusieurs pare-feu. Configurez un serveur NTP principal et un serveur NTP secondaire, au cas où le serveur NTP principal devienne inaccessible.*
Authentication Type (Type d'authentification)	Vous pouvez permettre au pare-feu d'authentifier les mises à jour de l'heure provenant d'un serveur'A0;NTP. Pour chaque serveur'A0;NTP, sélectionnez le type d'authentification à utiliser'A0;: • **None (Aucune)** (par défaut) : sélectionnez cette option pour désactiver l'authentification NTP. • **Symmetric Key (Clé symétrique)** : sélectionnez cette option pour que le pare-feu utilise un échange de clés symétriques (secrets partagés) pour authentifier les mises à jour de l'heure du serveur NTP. Si vous sélectionnez l"option Clé symétrique, poursuivez en indiquant les valeurs suivantes : • **Key ID (ID de clé)**– Saisissez l'ID de la clé (1 à -65534). • **Algorithm (Algorithme)** : sélectionnez l'algorithme MD5 ou SHA1 à utiliser pour l'authentification NTP. • **Authentication Key/Confirm Authentication Key (Clé d'authentification/ Confirmer la clé)** : saisissez et confirmez la clé d'authentification de l'algorithme d'authentification. • **Autokey (Clé automatique)** : sélectionnez cette option pour que le pare-feu utilise une clé automatique (chiffrement à clé publique) pour authentifier les mises à jour de l'heure du serveur NTP. *Activez l'authentification du serveur NTP pour que le serveur NTP approuve le client et fournisse des mises à jour synchronisées.*

Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l'itinéraire de service

Le tableau suivant présente la prise en charge IPv4 et IPv6 pour les configurations de l'itinéraire de service sur les systèmes globaux et virtuels.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
AutoFocus : serveur AutoFocus™	✓	—	—	—
État CRL : serveur Certificate Revocation List (liste de révocation du certificat ; CRL).	✓	✓	—	—
DDNS : Service DNS dynamique.	✓	✓	✓	✓
Mises à jour transmises à Panorama : mises à jour de contenu et logiciels déployées depuis Panorama™.	✓	✓	—	—
DNS : serveur Domain Name System. * Pour les systèmes virtuels, le DNS est inclus dans le profil de serveur DNS.	✓	✓	✓ *	✓ *
Listes dynamiques externes : mises à jour pour les listes dynamiques externes.	✓	✓	—	—
Messagerie : serveur de messagerie électronique.	✓	✓	✓	✓
HSM : serveur Hardware Security Module.	✓	—	—	✓
HTTP - Transfert HTTP.	✓	✓	✓	✓
Kerberos : serveur d'authentification Kerberos.	✓	—	✓	✓
LDAP : serveur Lightweight Directory Access Protocol.	✓	✓	✓	✓
MDM : serveur Mobile Device Management.	✓	✓	—	—
Authentification multifacteur : serveur d'authentification multifacteur (MFA).	✓	✓	✓	✓
NetFlow : le collecteur Netflow pour la collecte des statistiques de trafic réseau.	✓	✓	✓	✓
NTP : serveur Network Time Protocol.	✓	✓	—	—
Services Palo Alto Networks : mises à jour depuis Palo Alto Networks® et le serveur public WildFire®. Il s'agit également de l'itinéraire de	✓	—	—	—

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
service pour la transmission des données de télémétrie vers Palo Alto Networks.				
Panorama : serveur de gestion de Panorama.	✓	✓	–	–
Transfert des journaux de Panorama (Les pare-feu de la Série PA-5200 uniquement) : transfert des journaux depuis le pare-feu vers les collecteurs de journaux.	✓	✓	–	–
Proxy : serveur agissant en tant que proxy sur le pare-feu.	✓	✓	–	–
RADIUS : serveur Remote Authentication Dial-in User Service.	✓	✓	✓	✓
SCEP : protocole Simple Certificate Enrollment Protocol pour la demande et la distribution de certificats clients.	✓	✓	✓	–
Piège SNMP : serveur de pièges Simple Network Management Protocol.	✓	–	✓	–
Syslog : serveur de journalisation des messages système.	✓	✓	✓	✓
TACACS+ : Serveur Terminal Access Controller Access-Control System Plus (TACACS+) pour les services d'authentification, d'autorisation et de comptabilité (AAA).	✓	✓	✓	✓
Agent UID : serveur d'agent User-ID.	✓	✓	–	✓
Mises à jour d'URL : serveur de mises à jour Uniform Resource Locator (localisateur uniforme de ressource ; URL).	✓	✓	–	–
Surveillance des machines virtuelles : surveillance des informations des machines virtuelles, lorsque vous avez activé Périphérique > Sources d'informations de machine virtuelle. *Les pare-feu VM-Series dans des déploiements de cloud public qui surveillent des machines virtuelles doivent*	✓	✓	✓	✓

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
utiliser l'interface MGT. Vous ne pouvez pas utiliser une interface de plan de données comme itinéraire de service.				
Wildfire privé : serveur WildFire privé de Palo Alto Networks.	✓	—	—	—

Lors de la personnalisation d'un itinéraire de service **Global**, sélectionnez **Service Route Configuration (Configuration de l'itinéraire de service)** et, à l'onglet **IPv4** ou **IPv6**, sélectionnez un service dans la liste des services disponibles ; vous pouvez également sélectionner plusieurs services et **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)** pour configurer plusieurs itinéraires de service en même temps. Pour restreindre les choix qui apparaissent dans la liste déroulante **Source Address (Adresse source)**, sélectionnez une **Source Interface (Interface source)** puis une **Source Address (Adresse source)** (correspondant à cette interface). Une interface source définie sur **Any (Tout)** vous permet de sélectionner une Adresse source parmi toutes les interfaces disponibles. Le champ Adresse source affiche l'adresse IPv4 ou IPv6 affectée à l'interface sélectionnée ; l'adresse IP sélectionnée est la source du trafic du service. Vous pouvez sélectionner **Use Default (Utiliser les paramètres par défaut)** si vous voulez que le pare-feu utilise l'interface de gestion pour l'itinéraire de service. Cependant, si l'adresse IP de destination du paquet correspond à l'adresse IP de destination configurée, l'adresse IP source est définie par l'Adresse Source configurée pour la Destination. Vous n'avez pas besoin de définir une adresse de destination car la destination est configurée lorsque vous configurez chaque service. Par exemple, lorsque vous définissez vos serveurs DNS (**Device (Périphérique)** > **Setup (Configuration)** > **Services**), vous définissez la destination des requêtes DNS. Vous pouvez spécifier une adresse IPv4 et une adresse IPv6 pour un service.

Une autre façon de personnaliser un itinéraire de service **Global** consiste à sélectionner **Service Route Configuration (Configuration de l'itinéraire de service)**, puis à sélectionner **Destination**. Définissez une adresse IP de **Destination** à laquelle un paquet entrant est comparé. Si l'adresse de destination du paquet correspond à l'Adresse IP de destination configurée, l'adresse IP source est définie sur l'Adresse source configurée pour la Destination. Pour restreindre les choix qui apparaissent dans la liste déroulante **Source Address (Adresse source)**, sélectionnez une **Source Interface (Interface source)** puis une **Source Address (Adresse source)** (correspondant à cette interface). Une interface source définie sur **Any (Tout)** vous permet de sélectionner une adresse source parmi toutes les interfaces disponibles. L'interface **MGT** source entraîne l'utilisation par le pare-feu de l'interface de gestion pour l'itinéraire de service.

Lorsque vous configurez des itinéraires de service pour un **Virtual System (Système virtuel)**, le choix de l'option **Inherit Global Service Route Configuration (Hériter de la configuration d'itinéraire de service globale)** implique que tous les services du système virtuel hériteront des paramètres de l'itinéraire de service global. Vous pouvez plutôt choisir **Customize (Personnaliser)**, sélectionner **IPv4** ou **IPv6**, puis sélectionner un service ; vous pouvez également sélectionner plusieurs services et **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)**. La **Source Interface (Interface source)** propose les trois choix suivants :

- **Inherit Global Setting (Hériter du paramètre global)** : les services sélectionnés héritent des paramètres globaux de ces services.
- **Any (Tout)** : vous permet de sélectionner une adresse source parmi toutes les interfaces disponibles (interfaces du système virtuel spécifique).

© 2020 Palo Alto Networks, Inc.

- **Une interface qui figure dans la liste déroulante** : restreind les choix de la liste déroulante **Source Address (Adresse source)** aux adresses IP de cette interface.

Pour la **Source Address (Adresse source)**, sélectionnez une adresse dans la liste déroulante. Pour les services sélectionnés, les réponses du serveur sont envoyées à cette adresse source.

Route pour le service de destination

- Périphérique > Configuration > Services > Global

À l'onglet **Global**, lorsque vous cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)**, puis sur **Customize (Personnaliser)**, l'onglet **Destination** s'affiche. Les routes de service de destination sont disponibles dans l'onglet **Global** uniquement (et non dans l'onglet **Virtual Systems (Systèmes virtuels)**), de sorte que le service de route d'un système virtuel ne peut pas appliquer un contrôle prioritaire sur les entrées de table de routage non associées à ce système virtuel.

Vous pouvez utiliser un itinéraire de service de destination pour ajouter une redirection personnalisée d'un service non pris en charge dans la liste de services **Customize (Personnaliser)**. Un itinéraire de service de destination constitue une méthode de configuration du routage pour appliquer un contrôle prioritaire sur la table d'itinéraire de base d'informations de transfert (FIB). Tous les paramètres des itinéraires de service de destination appliqueront un contrôle prioritaire sur les entrées de la table d'itinéraire. Ils peuvent être liés ou non à n'importe quel service.

L'onglet **Destination** s'applique aux cas pratiques suivants :

- Lorsqu'un service ne comporte pas d'itinéraire de service d'application.
- Dans un système virtuel, lorsque vous souhaitez utiliser plusieurs routeurs virtuels ou une combinaison routeur virtuel/port de gestion.

Paramètres d'itinéraire de service de destination	Description
Destination	Saisissez l'adresse IP de **Destination**. Un paquet entrant dont l'adresse de destination correspond à cette adresse utilisera comme source l'adresse source que vous avez spécifié pour cette route de service.
Interface source	Pour restreindre la liste déroulante Souce Address (Adresse source), sélectionnez une **Source Interface (Interface source)**. Si vous sélectionnez **Any (Indifférent)**, toutes les adresses IP de toutes les interfaces seront disponibles dans la liste déroulante Souce Address (Adresse source). Le fait de sélectionner **MGT** entraîne l'utilisation par le pare-feu de l'interface MGT pour l'itinéraire de service.
Source Address (Adresse source)	Sélectionnez la **Source Address (Adresse source)** de la route de service ; cette adresse servira aux paquets qui reviennent de la destination. Vous n'avez pas besoin de saisir le sous-réseau de l'adresse de destination.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Interfaces

Utilisez cette page pour configurer les paramètres de connexion, les services autorisés et l'accès administratif pour l'interface de gestion (MGT) sur tous les modèles de pare-feu et pour les interfaces auxiliaires (AUX-1 et AUX-2) sur les pare-feu de la série PA-5200.

Palo Alto Networks vous recommande de toujours indiquer l'adresse IP et le masque de réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut pour chaque interface. Si vous omettez l'un de ces paramètres pour l'interface MGT (comme la passerelle par défaut), vous pouvez uniquement accéder au pare-feu via le port de la console pour les modifications de configuration futures.

Pour configurer l'interface MGT sur l'appareil M-500 ou sur l'appareil virtuel Panorama, voir Panorama > Configuration > Interfaces*.*

*Vous pouvez utiliser une interface en boucle en tant qu'alternative à l'interface MGT pour la gestion des pare-feu (*Réseau > Interfaces > En boucle*).*

Élément	Description
Type (Interface MGT uniquement)	Sélectionnez parmi les choix suivants : • **Static (Statique)** : Vous oblige à saisir manuellement l'**IP Address (Adresse IP)** (IPv4), le **Netmask (Masque réseau)** (IPv4) et la **Default Gateway (Passerelle par défaut)**. • **DHCP Client (Client DHCP)** : Configure l'interface MGT en tant que client DHCP afin que le pare-feu puisse envoyer des messages de Découverte ou de Demande de serveur DHCP pour trouver un serveur DHCP. Le serveur répond en fournissant une adresse IP (IPv4), un masque réseau (IPv4) et une passerelle par défaut pour l'interface MGT. Le serveur DHCP sur l'interface MGT est désactivé par défaut pour le pare-feu VM-Series (sauf pour le pare-feu VM-Series à AWS et Azure). Si vous sélectionnez **DHCP Client (Client DHCP)**, vous pouvez sélectionnez une ou les deux Options clientes suivantes : • **Send Hostname (Envoyer le nom d'hôte)** – Permet à l'interface MGT d'envoyer son nom d'hôte au serveur DHCP dans le cadre de l'Option DHCP 12. • **Send Client ID (Envoyer l'ID du client)** – Permet à l'interface MGT d'envoyer son identifiant client dans le cadre de l'Option DHCP 61. Si vous sélectionnez **DHCP Client (Client DHCP)**, vous pouvez cliquer sur **Show DHCP Client Runtime Info (Afficher l'information concernant l'exécution du client DHCP)** pour afficher l'état dynamique de l'interface IP : • Interface – Indique l'interface MGT. • Adresse IP : Adresse IP de l'interface MGT. • Masque réseau – Masque du sous-réseau pour l'adresse IP qui indique quels bits représentent le réseau ou le sous-réseau et lesquels représentent l'hôte. • Passerelle : Passerelle par défaut pour le trafic sortant de l'interface MGT. • NTP primaire/secondaire : L'adresse IP d'un maximum de deux serveurs NTP desservant l'interface de gestion. Si le serveur DHCP renvoie les adresses du serveur NTP, le pare-feu les considère seulement si vous n'avez pas configuré manuellement les adresses du serveur NTP. Si vous

© 2020 Palo Alto Networks, Inc.

Élément	Description
	avez configuré manuellement les adresses du serveur NTP, le pare-feu ne les remplace pas par celles du serveur DHCP. • Durée d'attribution : Nombre de jours, d'heures, de minutes et de secondes pendant lesquels l'adresse IP du serveur DHCP est attribuée. • Moment d'expiration : La date (année/mois/jour), l'heure (heures/minutes/secondes) et le fuseau horaire indiquant le moment où expirera l'attribution du serveur DHCP. • Serveur DHCP – Adresse IP du serveur DHCP répondant au Client DHCP de l'interface MGT. • Domaine : Nom de domaine auquel appartient l'interface MGT. • Serveur DNS : Adresse IP d'un maximum de deux serveurs DNS desservant l'interface de gestion. Si le serveur DHCP renvoie les adresses du serveur DNS, le pare-feu les considère seulement si vous n'avez pas configuré manuellement les adresses du serveur DNS. Si vous avez configuré manuellement les adresses du serveur DNS, le pare-feu ne les remplace pas par celles du serveur DHCP. Vous pouvez éventuellement **Renew (Renouveler)** le bail DHCP pour l'adresse IP affectée à l'interface MGT. Sinon, cliquez sur **Close (Fermer)** pour fermer la fenêtre.
Aux 1 / Aux 2 (Pare-feu de la série PA-5200 uniquement)	Sélectionnez l'une des options suivantes pour activer une interface auxiliaire. Ces interfaces assurent un débit de 10 Gbit/s (SFP+) pour : • Trafic de gestion du pare-feu – Vous devez activer les Services réseau (protocoles) qui seront utilisés par les administrateurs lorsqu'ils accéderont à l'interface Web et à la CLI pour gérer le pare-feu.  *Activez HTTPS au lieu de HTTP pour l'interface Web et activez SSH au lieu de Telnet pour la CLI.* • Synchronisation de la haute disponibilité (HD) entre les pare-feu homologues – Après avoir configuré l'interface, vous devez la sélectionner en tant que Liaison de contrôle HD (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**). • Transfert des journaux vers Panorama – Vous devez configurer un itinéraire de service avec le service activé **Panorama Log Forwarding (Transfert des journaux Panorama)** (Périphérique > Configuration > Services).
Adresse'A0;IP (IPv4)	Si votre réseau utilise IPv4, affectez une adresse IPv4 à l'interface. Vous pouvez éventuellement affecter l'adresse IP d'une interface en boucle pour la gestion du pare-feu (voir Réseau > Interfaces > En boucle). Par défaut, l'adresse IP que vous saisissez correspond à l'adresse source pour le transfert des journaux.
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).

© 2020 Palo Alto Networks, Inc.

Élément	Description
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:400:f00::1/64).
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
Vitesse	Configurez un débit de données et une option de duplex pour l'interface. Les choix possibles sont : 10 Mbits/s, 100 Mbits/s et 1 Gbit/s en duplex intégral ou semi-duplex. Utilisez le paramètre de négociation automatique par défaut pour que le pare-feu détermine la vitesse de l'interface. *Ce paramètre doit correspondre aux paramètres de port de l'équipement réseau voisin. Pour assurer les paramètres de mappage, sélectionnez la négociation automatique si l'équipement voisin prend en charge cette option.*
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Services de gestion administrative	• **HTTP** – Utilisez ce service pour accéder à l'interface Web du pare-feu. *HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS. Par conséquent, Palo Alto Networks vous recommande d'activer le protocole HTTPS au lieu du protocole HTTP pour le trafic de gestion sur l'interface.* • **Telnet** – Utilisez ce service pour accéder au mode CLI du pare-feu. *Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. Par conséquent, Palo Alto Networks vous recommande d'activer le protocole SSH au lieu du protocole Telnet pour le trafic de gestion sur l'interface.* • **HTTPS** – Utilisez ce service pour obtenir un accès sécurisé à l'interface Web du pare-feu. • **SSH** – Utilisez ce service pour obtenir un accès sécurisé à la CLI du pare-feu.
Services du réseau	Sélectionnez les services que vous souhaitez activer sur l'interface : • **HTTP OCSP** – Utilisez ce service pour configurer le pare-feu en tant que répondeur du protocole OCSP (Online Certificate Status Protocol). Pour plus d'informations, voir Périphérique > Gestion des certificats > Répondeur OCSP. • **Ping** – Utilisez ce service pour tester la connectivité avec des services externes. Par exemple, vous pouvez envoyer un ping à l'interface pour vérifier qu'elle reçoit les mises à jour logicielles et de contenu de PAN-OS du serveur de mises à jour Palo Alto Networks. Dans un déploiement

© 2020 Palo Alto Networks, Inc.

Élément	Description
	haute disponibilité (HD), les pairs HA utilisent l'envoi de ping pour échanger de l'information sur la sauvegarde de pulsation. • **SNMP** – Utilisez ce service pour traiter les requêtes de statistiques du pare-feu à partir d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – Utilisez ce service pour Activer la redistribution des associations d'utilisateurs sur les pare-feu. • **User-ID Syslog Listener-SSL (SSL de l'écouteur Syslog de User-ID)** – Utilisez ce service pour permettre à l'agent User-ID™ intégré à PAN-OS de collecter les messages Syslog sur SSL. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés. • **User-ID Syslog Listener-UDP (UDP de l'écouteur Syslog de User-ID)** – Utilisez ce service pour permettre à l'agent User-ID intégré à PAN-OS de collecter les messages Syslog sur UDP. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés.
Adresses IP autorisées	Saisissez les adresses IP à partir desquelles les administrateurs peuvent accéder au pare-feu via l'interface. Une liste vide (par défaut) indique que l'accès est possible à partir de n'importe quelle adresse IP. *Ne laissez pas la liste vide. Indiquez uniquement les adresses IP des administrateurs de pare-feu pour empêcher tout accès non autorisé.*

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Télémesure

La télémétrie est le processus de collecte et de transmission des données à analyser. Lorsque vous activez la télémétrie sur le pare-feu, le pare-feu collecte et transmet les données qui contiennent des informations sur les applications, les menaces, l'état des périphériques et la DNS passive vers Palo Alto Networks. Tous les utilisateurs de Palo Alto Networks bénéficient des données que chaque participant à la télémétrie partage, ce qui fait de la télémétrie une approche communautaire pour la prévention des menaces. En savoir plus sur la télémétrie et ses avantages.

La télémétrie est une fonctionnalité d'adhésion et, pour la plupart des données de télémétrie, vous pouvez prévisualiser les informations collectées par le pare-feu. Palo Alto Networks ne partage pas vos données de télémétrie avec d'autres clients ou d'autres organisations tierces.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)** pour choisir des données de télémétrie à partager avec Palo Alto Networks. Les rapports de Données de prévention des menaces et les rapports Captures de paquets de menaces fournissent à Palo Alto Networks une plus grande visibilité sur le trafic de votre réseau que les autres rapports de télémétrie.

Paramètres de télémétrie	Description
Exemple de rapport	Cliquez sur un exemple de rapport ( ) pour visualiser un rapport au format XML dans un onglet distinct. Les données indiquées dans l'exemple de rapport sont basées sur l'activité du pare-feu dans les quatre heures suivant votre visualisation d'un exemple de rapport. Le pare-feu fournit un exemple de rapport uniquement pour les rapports d'application, de prévention des menaces, des URL et d'identification de type de fichier. Un rapport peut consister en plusieurs rapports : • **Type** – Décrit le nom du rapport. • **Aggregate (Agrégat)** – Liste les champs de journal que le pare-feu collecte pour le rapport (voir Description des champs Syslog pour déterminer le nom des champs tel qu'ils apparaissent dans les journaux du pare-feu). • **Values (Valeurs)** – Indique les unités de mesure utilisées dans le rapport (par exemple, la valeur **count (nombre)** pour le rapport des Pays à l'origine des attaques se réfère au nombre de fois où le pare-feu a détecté une menace associée à un pays particulier). Un exemple de rapport n'affiche aucune entrée si le pare-feu n'a trouvé aucun trafic correspondant pour le rapport. Vous pouvez uniquement générer un nouvel exemple de rapport lorsque vous redémarrez le pare-feu.
Rapports de l'application (Désactivés par défaut)	Partage le nombre et la taille des applications connues regroupées par port de destination, les applications inconnues regroupées par port de destination et les applications inconnues regroupées par adresse IP de destination. Le pare-feu génère ces rapports à partir des Journaux de trafic. Lorsqu'il est activé, le pare-feu transfère les rapports d'application toutes les 4 heures.
Rapports de prévention des menaces (Désactivés par défaut)	Partage le nombre de menaces pour chaque pays source et port de destination, les informations du pirate et les objets de corrélation qui menacent les événements déclenchés lorsque le pare-feu collectait des données pour ces rapports.

© 2020 Palo Alto Networks, Inc.

Paramètres de télémétrie	Description
	Lorsqu'il est activé, le pare-feu transfère les rapports de prévention des menaces toutes les 4 heures.
Rapports des URL (Désactivés par défaut)	Partage les rapports générés à partir des journaux de filtrage des URL avec les catégories d'URL de PAN-DB suivantes : logiciels malveillants, hameçonnage, DNS dynamique, évitement de proxy, URL douteuse, URL parquée et inconnue (URL que PAN-DB n'a pas encore catégorisées). Le pare-feu envoie également des statistiques PAN-DB au moment où les données pour les rapports des URL ont été collectées. Ces statistiques incluent la version de la base de données de filtrage des URL sur le pare-feu et sur le Cloud PAN-DB, le nombre d'URL dans ces bases de données et le nombre d'URL que le pare-feu a catégorisées. Ces statistiques sont fondées sur le moment où le pare-feu a transmis les rapports des URL. Lorsqu'il est activé, le pare-feu transfère les rapports des URL toutes les 4 heures.
Rapports d'identification des types de fichiers (Désactivés par défaut)	Partagez des rapports sur les fichiers que le pare-feu a autorisés ou bloqués en fonction des paramètres de filtrage de données et des paramètres de blocage des fichiers. Lorsqu'il est activé, le pare-feu transfère les rapports d'identification des types de fichiers toutes les 4 heures.
Données de prévention des menaces (Désactivés par défaut)	Partage les journaux provenant des menaces qui ont déclenché les signatures que Palo Alto Networks évalue. Les informations collectées peuvent inclure les adresses IP source ou de la victime. L'activation de cette option permet également aux signatures inédites, que Palo Alto Networks teste actuellement, d'être exécutées en arrière-plan. Ces signatures n'affectent pas vos règles de politique de sécurité et les journaux de pare-feu et n'ont aucune incidence sur les performances de votre pare-feu. Lorsqu'il est activé, le pare-feu transfère les Données de prévention des menaces toutes les 5 minutes. Cliquez sur **Download Threat Prevention Data (Télécharger les données sur la prévention des menaces)** () pour télécharger un fichier tarball (.tar.gz) avec les 100 dossiers les plus récents de **Threat Prevention Data (Données de prévention des menaces)** et de **Threat Prevention Packet Captures (Captures de paquets de prévention de menace)** que le pare-feu a transmis à Palo Alto Networks. Si vous n'avez jamais activé ces paramètres ou si vous les avez activés, mais qu'aucune menace n'a été associée aux conditions de ces paramètres de télémétrie, le pare-feu ne génère pas de fichier et renvoie, à la place, un message d'erreur.
Captures de paquets de prévention des menaces (Désactivés par défaut)	Partage des captures de paquets (si vous avez activé votre pare-feu pour prendre des captures de paquets des menaces) des menaces qui donnent lieu à des signatures qui sont évaluées par Palo Alto Networks. Les informations collectées peuvent inclure les adresses IP source ou de la victime. Lorsqu'il est activé, le pare-feu transfère les Captures de paquets de prévention des menaces toutes les 5 minutes.

© 2020 Palo Alto Networks, Inc.

Paramètres de télémétrie	Description
	Pour activer les Captures de paquets de prévention des menaces, vous devez également activer les Données de prévention des menaces.
Statistiques d'utilisation du produit (Désactivés par défaut)	Partage les traces des processus de pare-feu qui ont échoué, ainsi que des informations sur l'état du pare-feu. Les traces exposent l'historique d'exécution des processus qui ont échoué. Les statistiques d'utilisation du produit comprennent également des détails sur le modèle de pare-feu et les versions de PAN-OS et du contenu installés sur votre pare-feu. Pour afficher les informations que le pare-feu envoie en tant que Statistiques d'utilisation du produit, saisissez la commande opérationnelle de la CLI suivante : `show system info` Lorsqu'il est activé, le pare-feu transfère les Statistiques d'utilisation du produit toutes les 5 minutes.
Surveillance DNS passive (Désactivés par défaut)	Permet au pare-feu d'agir comme un détecteur DNS passif et d'envoyer des informations DNS à Palo Alto Networks pour qu'elles fassent l'objet d'une analyse. Les données que vous partagez par surveillance DNS passive se composent uniquement des associations d'adresse IP à un domaine. L'équipe spécialisée dans la recherche des menaces de Palo Alto Networks utilise ces informations pour améliorer la catégorie d'URL PAN-DB, la précision de la signature C2 basée sur DNS ainsi que la détection des logiciels malveillants WildFire. La surveillance DNS passive est un paramètre global qui s'applique à l'ensemble du trafic du pare-feu. Une fois activé, le pare-feu transmet les données de surveillance DNS passive par lots de 1 Mo.
Sélectionner tout	Active tous les paramètres de télémétrie.
Désélectionner tout	Désactive tous les paramètres de télémétrie.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Content-ID

Utilisez l'onglet **Content-ID™** pour définir des paramètres de filtrage des URL, de protection des données et de pages de conteneur.

Paramètres Content-ID	Description
Filtrage des URL	
Délai de mise en cache de l'URL dynamique	Cliquez sur **Edit (Modifier)** et saisissez le délai en heures. Cette valeur est utilisée dans le filtrage des URL dynamiques afin de déterminer la durée de conservation d'une entrée dans le cache avant d'être renvoyée du service de filtrage des URL. Cette option s'applique au filtrage des URL via la base de données BrightCloud uniquement. Pour obtenir plus d'informations sur le filtrage des URL, sélectionnez Objets > Profils de sécurité > Filtrage des URL.
Délai de maintien des URL	Indiquez l'intervalle suivant une action **Continue (Continuer)** d'un utilisateur avant que celui-ci ne doive de nouveau appuyer sur continuer pour des URL de même catégorie (plage de 1 à 86 400 minutes, par défaut 15).
Délai de contrôle prioritaire sur l'URL par l'administrateur	Indiquez l'intervalle suivant la saisie du mot de passe de **Admin Override (Contrôle prioritaire administratif)** par l'utilisateur avant que celui-ci ne doive de nouveau saisir le mot de passe pour des URL de même catégorie (plage de 1 à 86 400 minutes ; par défaut 15).
Garder en mémoire la demande du client pour la recherche de catégorie	Activez cette option pour indiquer que lorsque le pare-feu ne peut trouver les informations sur les catégories pour un URL dans son cache local, il garde en mémoire la requête Web pendant la requête PAN-DB. *Cette option est désactivée par défaut. Activez-la pour respecter les*bonnes pratiques du profil de filtrage des URL .
Délai d'expiration pour le recherche de catégorie (secondes)	Précisez la période de temps, en secondes, pendant laquelle le pare-feu essaiera de trouver la catégorie d'un URL avant de déterminer que la catégorie est `not-resolved (non résolue)` (plage comprise entre 1 et 60 secondes ; par défaut : 2).
Délai de verrouillage de l'URL par l'administrateur	Indiquez l'intervalle pendant lequel un utilisateur ne peut pas utiliser le mot de passe de Contrôle prioritaire administratif des URL après trois échecs (plage de 1 à 86 400 minutes ; par défaut 30).
Serveur PAN-DB (Obligatoire pour la connexion à un serveur PAN-DB privé)	Indiquez l'adresse IPv4, l'adresse IPv6 ou le nom de domaine complet des serveurs PAN-DB privés sur votre réseau. Vous pouvez ajouter jusqu'à 20 entrées. Le pare-feu se connecte par défaut au cloud PAN-DB public. La solution PAN-DB privé est conçue pour les entreprises qui interdisent aux pare-feux d'accéder directement aux serveurs PAN-DB du cloud public. Les pare-feu accèdent aux serveurs figurant dans cette liste de serveurs PAN-DB pour

© 2020 Palo Alto Networks, Inc.

Paramètres Content-ID	Description
	la base de données d'URL, les mises à jour des URL et les recherches d'URL afin de classer les pages Web.
Contrôle prioritaire sur l'URL par l'administrateur	
Paramètres de contrôle prioritaire de l'URL par l'administrateur	Pour chaque système virtuel que vous souhaitez configurer pour le contrôle prioritaire de l'URL par l'administrateur, cliquez sur **Add (Ajouter)** et indiquez les paramètres qui s'appliquent lorsqu'un profil de filtrage des URL bloque une page et que l'action **Override (Contrôle prioritaire)** est spécifiée. Pour plus d'informations, voir Objets > Profils de sécurité > Filtrage des URL. • **Location (Emplacement)** - (multi-vsys firewalls only [pare-feu comportant plusieurs systèmes virtuels uniquement]) Sélectionnez le système virtuel dans le menu déroulant. • **Password/Confirm Password (Mot de passe/Confirmer le mot de passe)** - Saisissez le mot de passe que l'utilisateur doit entrer pour appliquer un contrôle prioritaire sur la page de blocage. • **SSL/TLS Service Profile (Profil de service SSL/TLS)** - Pour préciser un certificat et les versions du protocole TLS autorisées pour sécuriser les communications lors d'une redirection via le serveur indiqué, sélectionnez un profil de service SSL/TLS. Pour plus d'informations, reportez-vous à la section Périphérique > Gestion des certificats > Profil de service SSL/TLS. • **Mode** - Déterminez si la page de blocage est distribuée de manière transparente (elle semble provenir du site Web bloqué) ou si elle est redirige l'utilisateur vers le serveur défini. Si vous choisissez **Redirect (Rediriger)**, saisissez ensuite l'adresse IP de redirection. Vous pouvez aussi **Delete (Supprimer)** une entrée.
Paramètres Content-ID	
Autoriser le transfert du contenu déchiffré	Activez cette option pour configurer le pare-feu pour qu'il transfère du contenu déchiffré à un service externe lors de la mise en miroir du port ou de l'envoi de fichiers WildFire® pour analyse.  *Activez cette option et envoyez tous les fichiers inconnus du trafic déchiffré à WildFire à des fins d'analyse.* Pour un pare-feu doté de la fonctionnalité de systèmes virtuels multiples (plusieurs systèmes virtuels), vous activez cette option individuellement pour chaque système virtuel. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)** et sélectionnez le système virtuel sur lequel vous souhaitez activer le transfert du contenu décrypté. Cette option est disponible dans la boîte de dialogue Système virtuel.
Longueur de capture étendue des paquets	Définissez le nombre de paquets à capturer lorsque l'option de capture étendue est activée dans les profils antispyware et de Protection contre les vulnérabilités (plage de 1 à 50 ; par défaut 5).
Transférer les segments excédant le nombre	Activez cette option pour transférer les segments et enregistrer l'application comme `tcp-inconnu` lorsque la file d'attente de l'App-ID

© 2020 Palo Alto Networks, Inc.

Paramètres Content-ID	Description
permis par la file d'attente d'inspection de l'App-ID™ TCP	dépasse la limite de 64 segments. Utilisez le compteur global suivant pour afficher le nombre de segments excédant le nombre permis par cette file d'attente indépendamment du fait que vous ayez activé ou désactivé cette option : `appid_exceed_queue_limit` Désactivez cette option pour empêcher le pare-feu de transférer les segments TCP et de sauter l'inspection de l'App-ID lorsque la file d'attente d'inspection de l'App-ID est pleine. *Cette option est désactivée par défaut et vous devez la laisser désactivée pour garantir une sécurité maximale.* *Lorsque vous désactivez cette option, il est possible de constater une augmentation de la latence sur les flux où plus de 64 segments ont été mis en attente du traitement de l'App-ID.*
Transférer les segments excédant le nombre permis par la file d'attente d'inspection du contenu TCP	Activez cette option pour transférer des segments TCP et sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu TCP est pleine. Le pare-feu peut mettre en file d'attente jusqu'à 64 segments lorsqu'il attend une réponse du moteur de contenu. Lorsque le pare-feu transmet un segment et ignore l'inspection du contenu en raison de la file d'attente d'inspection de l'ensemble du contenu, il incrémente le compteur global suivant : `ctd_exceed_queue_limit` Désactivez cette option pour empêcher le pare-feu de transférer les segments TCP et de sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu est pleine. Lorsque vous désactivez cette option, le pare-feu supprime tous les segments qui dépassent la limite de la file d'attente et incrémente le compteur global suivant : `ctd_exceed_queue_limit_drop` Cette paire de compteurs globaux s'applique à la fois aux paquets TCP et UDP. Si, après avoir affiché les compteurs généraux, vous décidez de modifier les paramètres, vous pouvez les modifier au sein de la CLI à l'aide de la commande CLI suivante : **`set deviceconfig setting ctd tcp-bypass-exceed-queue`** *Cette option est activée par défaut, mais Palo Alto Networks vous recommande de désactiver cette option. Cependant, en raison des retransmissions TCP du trafic abandonné, la désactivation de cette option peut*

© 2020 Palo Alto Networks, Inc.

Paramètres Content-ID	Description
	entraîner une dégradation des performances et certaines applications peuvent engendrer une perte de fonctionnalité, en particulier dans les environnements de trafic à fort volume.
Transférer les datagrammes excédant le nombre permis par la file d'attente d'inspection du contenu UDP	Activez cette option pour transférer des datagrammes UDP et sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu UDP est pleine. Le pare-feu peut mettre en file d'attente jusqu'à 64 datagrammes lorsqu'il attend une réponse du moteur de contenu. Lorsque le pare-feu transmet un datagramme et ignore l'inspection du contenu en raison d'un débordement de la file d'attente d'inspection du contenu UDP, il incrémente le compteur global suivant : `ctd_exceed_queue_limit` Désactivez cette option pour empêcher le pare-feu de transférer les datagrammes et de sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu UDP est pleine. Lorsque cette option est désactivée, le pare-feu supprime tous les datagrammes qui dépassent la limite de la file d'attente et incrémente le compteur global suivant : `ctd_exceed_queue_limit_drop` Cette paire de compteurs globaux s'applique à la fois aux paquets TCP et UDP. Si, après avoir affiché les compteurs généraux, vous décidez de modifier les paramètres, vous pouvez les modifier au sein de la CLI à l'aide de la commande suivante : **`set deviceconfig setting ctd udp-bypass-exceed-queue`** *Cette option est activée par défaut, mais Palo Alto Networks vous recommande de désactiver cette option. Cependant, en raison des paquets abandonnés, la désactivation de cette option peut entraîner une dégradation des performances et certaines applications peuvent engendrer une perte de fonctionnalité, en particulier dans les environnements de trafic à fort volume.*
Autoriser les réponses HTTP partielles	Activez cette option de réponse partielle HTTP pour permettre à un client d'extraire seulement une partie d'un fichier. Lorsqu'un pare-feu de nouvelle génération identifie et supprime un fichier malveillant dans le chemin d'accès d'un transfert, il met fin à la session TCP à l'aide d'un paquet RST. Si le navigateur Web implémente l'option de plage HTTP, il peut commencer une nouvelle session pour extraire uniquement la partie restante du fichier. Cela empêche le pare-feu de déclencher à nouveau la même signature en raison de l'absence de contexte dans la session initiale, tout en permettant au navigateur Web de réassembler le fichier et de livrer le contenu malveillant ; pour éviter cette situation, assurez vous de désactiver cette option.

© 2020 Palo Alto Networks, Inc.

Paramètres Content-ID	Description
	Par défaut, l'option Allow HTTP partial response (Autoriser les réponses HTTP partielles) est activée, mais pour garantir une sécurité maximale, Palo Alto Networks vous recommande de désactiver cette option. La désactivation de cette option ne devrait pas affecter les performances du périphérique ; cependant, la reprise du transfert interrompu de fichiers HTTP peut être altérée. En outre, la désactivation de cette option peut influer sur les services de diffusion en continu tels que les mises à jour de contenu de Netflix, Microsoft Updates et Palo Alto Networks.
Recherche de signatures en temps réel	
DNS Signature Lookup Timeout (ms)	Précisez la durée de temps, en millisecondes, avant que le pare-feu interroge le service de Sécurité DNS. Si le nuage ne répond pas avant la fin de la période précisée, le pare-feu communique la réponse DNS associée au client effectuant la demande (la plage est comprise entre 0 et 60 000 ; la valeur par défaut est 80).
En-têtes X-Forwarded-For	
Utiliser l'en-tête X-Forwarded-For dans User-ID	Activez cette option pour indiquer que User-ID lit les adresses IP de l'en-tête X-Forwarded-For (XFF) dans les demandes client de services Web lorsque le pare-feu est déployé entre internet et un serveur proxy qui masquerait autrement les adresses IP des clients. User-ID met en correspondance les adresses IP qu'il lit avec les noms d'utilisateur référencés dans vos politiques afin que ces politiques puissent contrôler et consigner l'accès des utilisateurs et groupes associés. Si l'en-tête comporte plusieurs adresses IP, User-ID utilise la première entrée à gauche. Dans certains cas, la valeur d'en-tête est une chaîne de caractères au lieu d'être une adresse IP. Si la chaîne correspond à un nom d'utilisateur que l'User-ID a mappé à une adresse IP, le pare-feu utilise ce nom d'utilisateur pour les références de mappage de groupe dans les politiques. Si aucun mappage d'adresse IP n'existe pour la chaîne, le pare-feu invoque les règles de politique dans lesquelles l'utilisateur source est configuré sur **any (indifférent)** ou **unknown (inconnu)**. Les journaux de filtrage des URL affichent les noms d'utilisateur correspondants dans le champ Utilisateur source. Si User-ID ne parvient pas à effectuer la correspondance ou s'il n'est pas activé pour la zone associée à l'adresse IP, le champ Utilisateur source indique l'adresse IP XFF avec le préfixe **`x-fwd-for`**. *Activez l'utilisation de l'en-tête XFF dans User-ID pour que l'adresse IP du client d'origine apparaisse dans les journaux pour vous aider quand vous devez enquêter sur un problème.*
En-tête Strip-X-Forwarded-For	Activez cette option pour supprimer l'en-tête X-Forwarded-For (XFF), qui contient l'adresse IP d'un client demandant un service Web lorsque le pare-feu est déployé entre internet et un serveur proxy. Le pare-feu réinitialise la

© 2020 Palo Alto Networks, Inc.

Paramètres Content-ID	Description
	valeur de l'en-tête avant de transférer la requête : les paquets transférés ne contiennent aucune information sur l'adresse IP source interne.  *L'activation de cette option ne désactive pas l'utilisation d'en-têtes XFF pour l'attribution d'utilisateur dans des politiques ; le pare-feu réinitialise la valeur XFF uniquement après l'avoir utilisée pour l'attribution d'utilisateur.*  *Lorsque vous activez l'utilisation d'en-têtes XFF dans User-ID, activez également la suppression de l'en-tête XFF avant le transfert du paquet pour protéger la confidentialité des utilisateurs sans perdre la capacité de les suivre. L'activation des deux options vous permet de journaliser et de faire le suivi des adresses IP des utilisateurs initiaux tout en protégeant leur confidentialité en évitant de transférer leur adresse IP d'origine.*
ID de contenu - Caractéristiques	
Gérer la protection des données	Ajoutez une protection supplémentaire à l'accès aux journaux pouvant contenir des informations sensibles, des numéros de carte de crédit ou de sécurité sociale par exemple. Cliquez sur **Manage Data Protection (Gérer la protection des données)** pour effectuer les tâches suivantes : • **Set Password (Définir le mot de passe)** - Si aucun mot de passe n'a déjà été configuré, saisissez et confirmez-en un nouveau. • **Change Password (Modifier le mot de passe)** - Saisissez l'ancien mot de passe, puis saisissez et confirmez-en un nouveau. • **Delete Password (Supprimer le mot de passe)** - Supprime le mot de passe et les données protégées.
Pages de conteneur	Utilisez ces paramètres pour préciser les types d'URL qui seront suivis ou consignés par le pare-feu en fonction du type de contenu, application/pdf, application/soap+xml, application/xhtml+, texte/html, texte/brut et texte/xml par exemple. Les pages de conteneur sont définies par système virtuel que vous sélectionnez dans le menu déroulant **Location (Emplacement)**. Si une page de conteneur n'est pas explicitement définie pour un système virtuel, le pare-feu utilise les types de contenu par défaut. **Add (Ajoutez)** et saisissez un type de contenu ou sélectionnez un type de contenu existant. L'ajout de nouveaux types de contenu pour un système virtuel applique un contrôle prioritaire sur la liste des types de contenu par défaut. Si aucun type de contenu n'est associé à un système virtuel, la liste des types de contenu par défaut est utilisée.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > WildFire

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire** pour configurer les paramètres WildFire sur le pare-feu et sur Panorama. Vous pouvez activer le cloud WildFire et un appareil WildFire pour les utiliser afin d'analyser des fichiers. Vous pouvez également définir des limites de taille de fichier et des informations de session à signaler. Après avoir renseigné des paramètres WildFire, vous pouvez indiquer les fichiers à transférer au cloud WildFire ou à l'appareil WildFire en créant un profil d'**WildFire Analysis (Analyse WildFire)** (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**).

Pour transférer le contenu déchiffré à WildFire, reportez-vous à la section Transfert du trafic déchiffré pour analyse WildFire.

Paramètres WildFire	Description
Paramètres généraux	
Cloud public WildFire	Saisissez **`wildfire.paloaltonetworks.com`** pour envoyer des fichiers sur le Cloud mondial WildFire, hébergé aux États-Unis, pour qu'ils fassent l'objet d'une analyse. Par ailleurs, vous pouvez, à la place, envoyer des fichiers à un Cloud régional WildFire pour qu'ils fassent l'objet d'une analyse. Les Cloud régionaux sont conçus pour adhérer à vos attentes en matière de confidentialité des données en fonction de votre emplacement. *Transmettez les échantillons à un cloud régional WildFire pour veiller au respect des normes en matière de conformité et de confidentialité des données propres à votre région. Les clouds régionaux sont les suivants :* • *Europe :* **`eu.wildfire.paloaltonetworks.com`** • *Japon :* **`jp.wildfire.paloaltonetworks.com`** • *Singapour :* **`sg.wildfire.paloaltonetworks.com`**
Cloud WildFire privé	Indiquez l'adresse IP ou le nom de domaine complet de l'appareil WildFire. Le pare-feu envoie des fichiers pour analyse à l'appareil WildFire spécifié. Panorama collecte des ID de menace depuis l'appareil WildFire pour permettre l'ajout d'exceptions de menace dans les profils antispyware (uniquement pour les signatures DNS) et les profils antivirus que vous configurez dans les groupes de périphériques. Panorama collecte également des informations provenant de l'appareil WildFire pour remplir les champs manquants dans les journaux des envois WildFire reçus de la part des pare-feu exécutant des versions de logiciels antérieures à PAN-OS 7.0.
Limites de taille de fichier	Indiquez la taille de fichier maximale à transférer au serveur'A0;WildFire. Pour toutes les recommandations relatives aux tailles de fichiers, si la limite est trop grande et empêche le pare-feu de transférer en même temps plusieurs fichiers du jour zéro de grande taille, réduisez et affinez la limite maximale à la taille d'espace tampon disponible sur le pare-feu. Si de l'espace tampon supplémentaire est disponible, vous pouvez accroître la limite de taille du fichier au-dessus de la recommandation. Les recommandations sont un bon

© 2020 Palo Alto Networks, Inc.

Paramètres WildFire	Description
	point de départ pour définir des limites efficaces qui ne surchargent pas les ressources du pare-feu. Les intervalles disponibles sont'A0;: • **pe** (Portable Executable) – La plage est comprise entre 1 et 50 Mo ; 16 Mo par défaut.  *Définissez la taille des fichiers PE sur 16 Mo.* • **apk** (Android Application) – La plage est comprise entre 1 et 50 Mo ; 10 Mo par défaut.  *Définissez la taille des fichiers APK sur 10 Mo.* • **pdf** (Portable Document Format) – La plage est comprise entre 100 Ko et 51 200 Ko ; 3 072 Ko par défaut.  *Définissez la taille des fichiers PDF sur 3 072 Ko.* • **ms-office** (Microsoft Office) – La plage est comprise entre 200 Ko et 51 200 Ko ; 16 384 Ko par défaut.  *Définissez la taille des fichiers ms-office sur 16 384 Ko.* • **jar** (Packaged Java class file) – La plage est comprise entre 1 et 20 Mo ; 5 Mo par défaut.  *Définissez la taille des fichiers jar sur 5 Mo.* • **Flash** (Adobe Flash) – La plage est comprise entre 1 et 10 Mo ; 5 Mo par défaut.  *Définissez la taille des fichiers flash sur 5 Mo.* • **Mac OS X** (Fichiers DMG / MAC-APP / MACH-O PKG) – Plage comprise entre 1 et 50 Mo ; la valeur par défaut est de 10 Mo.  *Définissez la taille des fichiers MacOSX sur 1 Mo.* • **archive** (Fichiers RAR et 7z) – La plage est comprise entre 1 et 50 Mo ; 50 Mo par défaut.  *Définissez la taille des fichiers d'archive sur 50 Mo.* • **linux** (Fichiers ELF) – La plage est comprise entre 1 et 50 Mo ; 50 Mo par défaut.  *Définissez la taille des fichiers linux sur 50 Mo.*

© 2020 Palo Alto Networks, Inc.

Paramètres WildFire	Description
	• **script** (fichiers JScript, VBScript, PowerShell et Shell Script) – La plage est comprise entre 10 et 4 096 Ko; 20 Ko par défaut.  *Définissez la taille des fichiers script sur 20 Ko.*  *Les valeurs précédentes peuvent varier en fonction de la version actuelle de PAN-OS ou de la version du contenu. Pour afficher les plages valides, cliquez sur le champ Size Limit (Taille maximale). Une fenêtre contextuelle indiquant la plage disponible et la valeur par défaut s'affiche.*
Signaler des fichiers bénins	Lorsque cette option (désactivée par défaut) est activée, les fichiers analysés par WildFire déterminés comme bénins s'affichent dans le journal des envois WildFire dans **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)**. même si cette option est activée sur le pare-feu, les liens contenus dans les e-mails que WildFire considère comme bénins ne sont pas consignés en raison de la quantité possible de liens traités.
Signaler des fichiers Grayware	Lorsque cette option (désactivée par défaut) est activée, les fichiers analysés par WildFire déterminés comme indésirables s'affichent dans le journal des envois WildFire dans **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)**.  *même si cette option est activée sur le pare-feu, les liens contenus dans les e-mails que WildFire considère comme « grayware » ne sont pas consignés en raison de la quantité possible de liens traités.*  *Activez le signalement des fichiers bénins pour journaliser les informations de session, l'activité réseau, l'activité des hôtes et les autres informations qui aident les analyses.*
Paramètres des informations de session	
Settings (Paramètres)	Indiquez les informations à transférer au serveur'A0;WildFire. Par défaut, toutes les options sont sélectionnées. Il est recommandé de transférer toutes les informations de session pour fournir des statistiques et d'autres mesures qui vous permettent de prendre des mesures pour empêcher les événements des menaces : • **Source IP (Adresse IP source)** : adresse IP source ayant envoyé le fichier suspect. • **Source Port (Port source)** : port source ayant envoyé le fichier suspect. • **Destination IP (Adresse IP de destination)** : adresse IP de destination ayant envoyé le fichier suspect. • **Destination Port (Port de destination)** : port de destination ayant envoyé le fichier suspect. • **Vsys** : système virtuel de pare-feu ayant identifié le logiciel malveillant possible.

© 2020 Palo Alto Networks, Inc.

Paramètres WildFire	Description
	• **Application** : application utilisateur utilisée pour transmettre le fichier. • **User (Utilisateur)** : utilisateur ciblé. • **URL** : URL associée au fichier suspect. • **Filename (Nom du fichier)** : nom du fichier envoyé. • **Email sender (Expéditeur de l'e-mail)** : indique le nom de l'expéditeur dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3. • **Email recipient (Destinataire de l'e-mail)** : indique le nom du destinataire dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3. • **Email subject (Objet de l'e-mail)** : indique l'objet de l'e-mail dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3.

© 2020 Palo Alto Networks, Inc.

Périphérique > Configuration > Session

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session** pour configurer les paramètres d'expiration de session, les paramètres de certificat de déchiffrement et les paramètres généraux relatifs à la session, comme la protection par pare-feu du trafic IPv6 et la revérification de la politique de Sécurité sur les sessions existantes en cas de modification de la politique. Cet onglet contient les sections suivantes'A0;:

- Paramètres de session
- Délais d'expiration de session
- Paramètres TCP
- Paramètres de décryptage : Vérification de la révocation du certificat
- Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert
- Paramètres de session VPN

Paramètres de session

Le tableau suivant décrit les paramètres de session.

Paramètres de session	Description
Revérifier les sessions	Cliquez sur **Edit (Modifier)** et sélectionnez **Rematch Sessions (Revérifier les sessions)** pour que le pare-feu applique les nouvelles politiques de sécurité configurées aux sessions en cours. Cette option est activée par défaut. Si ce paramètre est désactivé, une fois validée, toute modification de politique s'applique uniquement aux sessions initiées. Par exemple, si une session'A0;Telnet commence alors qu'une politique associée a été configurée pour autoriser Telnet et que vous validez par la suite une modification de politique pour refuser Telnet, le pare-feu applique la politique révisée à la session en cours et la bloque. *Activez Rematch Sessions (Revérifier les sessions) pour appliquer votre dernière politique de sécurité aux sessions actuellement actives.*
ICMPv6, jeton - Taille du compartiment	Saisissez la taille du jeton pour la limitation des messages d'erreur ICMPv6. La taille du jeton est un paramètre de l'algorithme du jeton qui contrôle la distribution en paquets des erreurs ICMPv6 (plage de 10 à 65 535 paquets ; par défaut 100).
Erreur ICMPv6 - Débit du paquet	Saisissez le nombre moyen de paquets d'erreur ICMPv6 par seconde autorisés globalement sur le pare-feu (plage de 10 à 65 535 paquets/seconde ; par défaut 100). Cette valeur s'applique à toutes les interfaces. Si le pare-feu atteint le nombre moyen de paquets d'erreur ICMPv6, le sceau à jetons permet la limitation des messages d'erreur ICMPv6.
Activer le pare-feu IPv6	Pour activer les fonctions du pare-feu pour IPv6, cliquez sur **Edit (Modifier)** et sélectionnez **IPv6 Firewalling (Activer le pare-feu IPv6)**. Toutes les configurations basées sur IPv6 sont ignorées si l'option IPv6 est désactivée. Même si IPv6 est activé pour une interface, l'option **IPv6**

© 2020 Palo Alto Networks, Inc.

Paramètres de session	Description
	Firewalling (Activer le pare-feu IPv6) doit également être sélectionnée pour qu'IPv6 fonctionne.
Activer la trame Jumbo Global MTU	Sélectionnez cette option pour activer la prise en charge de trames'A0;Jumbo sur les interfaces'A0;Ethernet. Les trames Jumbo disposent d'une unité de transmission maximale (MTU) de 9 192 octets et sont disponibles sur certains modèles uniquement. • Si vous ne cochez pas la case **Enable Jumbo Frame (Activer la trame Jumbo)**, la **Global MTU (MTU globale)** est de 1 500 octets par défaut (plage de 576 à 1 500). • Si vous cochez la case **Enable Jumbo Frame (Activer la trame Jumbo)** Jumbo, la **Global MTU (MTU globale)** est de 9 192 octets par défaut (plage de 9 192 à 9 216 octets). *Les trames Jumbo peuvent utiliser jusqu'à cinq fois plus de mémoire que les paquets normaux et peuvent réduire le nombre de mémoires tampons des paquets disponibles de 20 %. Ceci réduit la taille de la file d'attente dédiée aux tâches hors service et d'identification des applications, ainsi qu'aux autres tâches similaires de traitement des paquets. Depuis PAN-OS 8.1, si vous activez la configuration MTU globale de trames jumbo et redémarrez votre pare-feu, les mémoires tampons des paquets sont alors redistribuées pour traiter les trames jumbo plus efficacement.* Si vous activez les trames'A0;Jumbo et qu'une MTU spécifique n'est pas configurée sur certaines interfaces, ces dernières héritent automatiquement de la taille de trame'A0;Jumbo. Par conséquent, avant d'activer les trames Jumbo, si vous ne souhaitez pas qu'une interface ait des trames Jumbo, vous devez définir la MTU de cette interface sur 1 500 octets ou une autre valeur. Pour configurer le MTU pour l'interface (**Network [Réseau]** > **Interfaces** > **Ethernet**), reportez-vous à la section Interface de niveau 3 de la série PA-7000.
MTU IPv6 min. pour le réseau NAT64	Saisissez la MTU globale du trafic traduit en IPv6. La valeur par défaut de 1'A0;280'A0;octets est basée sur la MTU minimum standard du trafic'A0;IPv6. Plage comprise entre 1 280 et 9 216.
Taux de sursouscription NAT	Sélectionnez le taux de sursouscription'A0;NAT'A0;DIPP, qui est le nombre de fois qu'une adresse'A0;IP traduite et une paire de ports identiques peuvent être utilisées simultanément. La réduction du taux de sursouscription diminue le nombre de traductions de périphérique source, mais étend les fonctionnalités des règles'A0;NAT. • **Platform Default (Valeur par défaut de la plate-forme)** – La configuration explicite du taux de sursouscription est désactivée ; le taux de sursouscription par défaut du modèle s'applique. Voir les taux par défaut des modèles de pare-feu à l'adresse https://www.paloaltonetworks.com/products/product-selection.html. • **1x** – 1 fois. Aucune sursouscription n'est effectuée'A0;; chaque adresse'A0;IP traduite et paire de ports ne peuvent être utilisées qu'une à la fois.

© 2020 Palo Alto Networks, Inc.

Paramètres de session	Description
	• **2x** – 2 fois. • **4x** – 4 fois. • **8x** – 8 fois.
Taux de paquets ICMP inaccessibles (par sec)	Définissez le nombre maximum de réponses ICMP inaccessibles que le pare-feu peut envoyer par seconde. Cette limite est partagée par les paquets IPv4 et IPv6. La valeur par défaut est de 200 messages par seconde (plage de 1 à 65 535).
Vieillissement accéléré	Permet d'accélérer le vieillissement des sessions inactives. Sélectionnez cette option pour activer le vieillissement accéléré et préciser le seuil (en %) et le facteur d'échelle. Lorsque la table de la session atteint **Accelerated Aging Threshold (Seuil du vieillissement accéléré)** (% saturé), PAN-OS applique **Accelerated Aging Scaling Factor (Facteur d'échelle du vieillissement accéléré)** est appliqué aux calculs de vieillissement de toutes les sessions. Le facteur d'échelle par défaut est de 2, ce qui signifie que le vieillissement accéléré se produit à un taux deux fois plus élevé que la durée d'inactivité configurée. La durée d'inactivité configurée divisée par 2 a pour conséquence un délai plus court réduit de 50 %. Pour calculer le vieillissement accéléré de la session, PAN-OS divise la durée d'inactivité configurée (pour ce type de session) par le facteur d'échelle afin de déterminer un délai plus court. Par exemple, si le facteur d'échelle est de 10, une session qui expirerait normalement au bout de 3'A0;600'A0;secondes expirerait 10'A0;fois plus vite (en 1/10e du temps), c'est-à-dire au bout de 360'A0;secondes. *Activez un seuil de vieillissement accéléré et définissez un facteur d'échelle acceptable pour libérer plus rapidement l'espace de la table des sessions lorsque celle-ci commence à se remplir.*
Protection de la mémoire tampon des paquets	Il est recommandé d'activer la protection de la mémoire tampon des paquets globalement et à chaque zone pour protéger les mémoires tampons des pare-feux des attaques DoS et des sessions et sources agressives. Cette option protège les mémoires tampons de réception du pare-feu contre les attaques ou le trafic abusif qui provoque la sauvegarde des ressources du système et la suppression du trafic légitime. La protection de la mémoire tampon des paquets identifie les sessions incriminées, utilise Random Early Detection (RED, Détection anticipée aléatoire) en tant que première ligne de défense et abandonne la session ou bloque l'adresse IP offensante si l'abus se poursuit. Si le pare-feu détecte de nombreuses petites sessions ou la création rapide de sessions (ou les deux) à partir d'une adresse IP spécifique, il bloque cette adresse IP. Prenez les mesures de base de l'utilisation des mémoires tampons des paquets du pare-feu pour comprendre la capacité du pare-feu et veiller à ce qu'il soit bien dimensionné de sorte que seule une attaque puisse entraîner une forte hausse de l'utilisation de la mémoire tampon. • **Alert (%) (Alerte (%))** : lorsque l'utilisation de la mémoire tampon des paquets dépasse ce seuil pendant plus de 10 secondes, le pare-feu crée

© 2020 Palo Alto Networks, Inc.

Paramètres de session	Description
	un journal d'événements toutes les minutes. Le pare-feu génère des événements de journal lorsque la protection de la mémoire tampon des paquets est activée globalement (la plage est comprise entre 0 et 99 % ; par défaut : 50 %). Si la valeur est de 0 %, le pare-feu ne crée pas de journaux d'événements. Commencez par la valeur de seuil par défaut et ajustez-la, au besoin. • **Activate (%) (Activer [%])** – Lorsque ce seuil est atteint, le pare-feu commence à limiter les sessions les plus abusives (la plage est comprise entre 0 et 99 % ; par défaut : 50 %). Si la valeur est de 0 %, le pare-feu n'applique pas la RED. Commencez par la valeur de seuil par défaut et ajustez-la, au besoin. • **Block Hold Time (sec) (Délai de maintien du blocage (sec))** – La période, en secondes, pendant laquelle la session est autorisée à se poursuivre avant qu'elle ne soit abandonnée ou l'adresse IP source est bloquée (la plage est comprise entre 0 et 65 535 ; par défaut : 60). Ce minuteur surveille les sessions limitées par RED pour voir si elles continuent de s'obstiner à utiliser la mémoire tampon au-dessus du seuil configuré. Si le comportement abusif se poursuit après le délai de maintien du blocage, la session est abandonnée. Si la valeur est 0, le pare-feu n'abandonne pas les sessions en fonction de la protection de la mémoire tampon des paquets. Commencez par la valeur par défaut, surveillez l'utilisation de la mémoire tampon des paquets et ajustez la valeur de la durée, au besoin. • **Block Duration (sec) (Durée de blocage [secondes])** – La période, en secondes, pendant laquelle une session abandonnée reste abandonnée ou pendant laquelle une adresse IP bloquée reste bloquée (la plage est comprise entre 1 et 15 999 999 ; par défaut : 3 600). Utiliser la valeur par défaut, à moins que le blocage d'une adresse IP pendant une heure serait trop sévère pour vos conditions d'affaires, dans ce cas, vous pouvez réduire la durée. Surveillez l'utilisation de la mémoire tampon des paquets et ajustez la durée, au besoin. *La traduction de l'adresse réseau peut accroître l'utilisation de la mémoire tampon des paquets. Si une telle traduction affecte l'utilisation de la mémoire tampon, réduisez le délai de maintien du blocage pour bloquer les sessions individuelles plus rapidement et réduirez la durée du blocage pour que les autres sessions provenant de l'adresse IP sous-jacente ne soient pas indûment pénalisées.*
Mise en tampon de configuration de route multidiffusion	Sélectionnez cette option (désactivée par défaut) pour activer la mise en tampon de configuration de route multidiffusion, qui permet au pare-feu de préserver le premier paquet dans une session multidiffusion lorsque l'entrée de la route multidiffusion ou la base d'informations de transfert (FIB) n'existe pas encore pour le groupe multidiffusion correspondant. Par défaut, le pare-feu ne procède pas à la mise en tampon du premier paquet multidiffusion dans une nouvelle session ; il utilise plutôt le premier paquet pour paramétrer la route multidiffusion. Ce comportement est normal pour le trafic multicast. Si vos serveurs de contenu sont directement connectés au pare-feu et que votre application personnalisée ne peut pas prendre en charge le premier paquet dans la session en cours de suppression, vous n'avez qu'à activer la mise en tampon de configuration de route multidiffusion.

© 2020 Palo Alto Networks, Inc.

Paramètres de session	Description
Taille de tampon de configuration de route multidiffusion	Si vous activez la Mise en tampon de configuration de route multidiffusion, vous pouvez régler la taille du tampon, qui spécifie la taille du tampon par flux (plage de 1 à 2 000 ; par défaut 1 000.) Le pare-feu peut mettre en tampon un maximum de 5 000 paquets.

Délais d'expiration de session

Certains délais d'expiration de session définissent la durée pendant laquelle PAN-OS maintient une session sur le pare-feu après son inactivité. Par défaut, lorsque le délai du protocole expire, PAN-OS ferme la session. Le délai d'expiration des sessions en état de rejet définit la durée maximale pendant laquelle une session demeure ouverte après que PAN-OS l'a refusée en fonction des règles de politique de Sécurité.

Vous pouvez définir plus particulièrement un délai d'expiration pour les sessions TCP, UDP, ICMP et SCTP sur le pare-feu. Le délai d'expiration **Default (Par défaut)** s'applique à tout autre type de session. Tous ces délais d'expiration sont globaux, ce qui signifie qu'ils s'appliquent à toutes les sessions de ce type sur le pare-feu.

Outre les paramètres généraux, vous pouvez définir des délais d'expiration pour une application particulière dans l'onglet **Objects (Objets)** > **Applications**. Les délais d'expiration disponibles pour cette application s'affichent dans la fenêtre'A0;Options. Le pare-feu applique les délais d'expiration d'application à une application qui se trouve dans un état établi. Une fois configurés, les délais d'expiration d'une application remplacent les délais d'expiration de session TCP, UDP ou SCTP généraux.

Les options de cette section vous permettent de configurer les paramètres d'expiration de session généraux (spécifiquement pour les sessions TCP, UDP, ICMP, SCTP ainsi que pour tous les autres types de sessions).

Les valeurs par défaut sont des valeurs optimales et il est recommandé d'utiliser les valeurs par défaut. Toutefois, vous pouvez les modifier selon vos besoins en matière de réseau. La définition d'une valeur trop faible peut engendrer une certaine sensibilité aux retards mineurs sur le réseau et une impossibilité d'établir une connexion avec le pare-feu, tandis qu'une valeur trop élevée peut entraîner un retard dans la détection des échecs.

Paramètres de délais d'expiration de session	Description
Default (Par défaut)	Durée maximale, en secondes, pendant laquelle une session non TCP/UDP, non SCTP ou non ICMP peut être ouverte sans aucune réponse (plage de 1 à 15 999 999 ; par défaut 30).
Supprimer les valeurs par défaut	Durée maximale (en secondes) pendant laquelle une session non TCP/UDP/SCTP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 60).
Supprimer TCP	Durée maximale(en secondes) pendant laquelle une session TCP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 90).
Supprimer UDP	Durée maximale (en secondes) pendant laquelle une session UDP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques

© 2020 Palo Alto Networks, Inc.

Paramètres de délais d'expiration de session	Description
	de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 60).
ICMP	Durée maximale pendant laquelle une session ICMP peut être ouverte sans aucune réponse ICMP (plage de 1 à 15 999 999 ; par défaut 6).
Balayage	Durée maximal, en secondes, pendant laquelle une session peut rester inactive avant que le pare-feu arrête la session et récupère les ressources de la mémoire tampon que la session utilisait. Le temps d'inactivité est le temps qui a passé depuis que la session a été actualisée pour la dernière fois par un paquet ou un événement. La plage est comprise entre 5 et 30 ; la valeur par défaut est 10.
TCP	Durée maximale pendant laquelle une session TCP reste ouverte sans aucune réponse TCP, une fois qu'une session TCP se trouve dans un état Établi (après que la liaison a été établie et/ou que les données ont été transmises) ; (plage de 1 à 15 999 999 ; par défaut 3 600).
Établissement de liaison TCP	Durée maximale, en secondes, entre la réception du paquet SYN-ACK et le paquet ACK suivant pour complètement établir la session (plages de 1 à 60 ; par défaut 10).
Initialisation TCP	Durée maximale, en secondes, entre la réception du paquet SYN et le paquet SYN-ACK avant de démarrer le minuteur d'établissement de liaison TCP (plages de 1 à 60 ; par défaut 5).
Délai d'attente des sessions TCP à moitié fermées	Durée maximale, en secondes, entre la réception du premier paquet FIN et celle du second paquet FIN ou RST (plage de 1 à 604 800 ; par défaut 120).
Délai d'attente des sessions TCP en état time_wait	Durée maximale, en secondes, après la réception du second paquet FIN ou RST (plages de 1 à 600 ; par défaut 15).
RST non vérifié	Durée maximale, en secondes, après la réception d'un paquet RST qui ne peut pas être vérifié (le paquet RST se trouve dans la fenêtre TCP, mais dispose d'un numéro de séquence inattendu ou provient d'un chemin asymétrique) ; (plages de 1 à 600 ; par défaut 30).
UDP	Durée maximale, en secondes, pendant laquelle une session UDP reste ouverte sans aucune réponse UDP (plage de 1 à 1 599 999 ; par défaut 30).
portail captif	Le délai d'expiration de session d'authentification, en secondes, du formulaire Web du Portail captif (par défaut 30, plage de 1 à 1 599 999). Pour accéder au contenu demandé, l'utilisateur doit saisir les informations d'identification d'authentification dans ce formulaire et être authentifié avec succès. Le délai d'expiration de session d'authentification, en secondes, du formulaire Web du Portail captif (par défaut 30, plage de 1 à 1 599 999). Pour accéder au contenu demandé, l'utilisateur doit saisir les informations

© 2020 Palo Alto Networks, Inc.

Paramètres de délais d'expiration de session	Description
	d'identification d'authentification dans ce formulaire et être authentifié avec succès.
SCTP INIT	Durée de temps maximale, en secondes, après la réception d'un bloc SCTP INIT au cours de laquelle le pare-feu doit recevoir le bloc INIT ACK avant que le pare-feu n'arrête l'initiation de l'association SCTP (plage comprise entre 1 et 60 ; par défaut 5).
SCTP COOKIE	Durée de temps maximale, en secondes, après la réception d'un bloc SCTP INIT ACK avec paramètre d'état COOKIE, au cours de laquelle le pare-feu doit recevoir le bloc COOKIE ECHO avant que le pare-feu n'arrête l'initiation de l'association SCTP (plage comprise entre 1 et 600 ; par défaut 60).
Supprimer SCTP	Durée maximale, en secondes, pendant laquelle une association SCTP reste ouverte après que PAN-OS a refusé la session en fonction des règles de politique de Sécurité configurées sur le pare-feu (plage entre 1 et 604 800 ; par défaut 30).
SCTP	Durée de temps maximale, en secondes, qui peut s'écouler sans qu'aucun trafic SCTP pour association ne se présente avant que toutes les sessions de l'association n'expirent (plage comprise entre 1 et 604 800 ; par défaut 3 600).
Arrêt SCTP	Durée de temps maximale, en secondes, que le pare-feu attend qu'un bloc SHUTDOWN SCTP reçoive un bloc SHUTDOWN ACK avant que le pare-feu n'ignore le bloc SHUTDOWN (plage comprise entre 1 et 600 ; par défaut 30).

Paramètres TCP

Le tableau suivant décrit les paramètres TCP.

Paramètres TCP	Description
Transférer les segments excédant le nombre permis par la file d'attente TCP hors service	Sélectionnez cette option si vous souhaitez que le pare-feu transfère les segments qui dépassent la limite de 64 par session permise par la file d'attente TCP hors service. Si vous désactivez cette option, le pare-feu supprime les segments qui dépassent la limite de la file d'attente hors service. Pour afficher un décompte du nombre de segments que le pare-feu a supprimé en raison de l'activation cette option, exécutez la commande CLI suivante : `show counter global tcp_exceed_flow_seg_limit` *Cette option est désactivée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. La désactivation de cette option peut entraîner une augmentation de la latence sur le flux spécifique ayant reçu plus de 64 segments hors*

© 2020 Palo Alto Networks, Inc.

Paramètres TCP	Description
	service. Il ne devrait pas y avoir de perte de connectivité étant donné que la pile TCP doit gérer la retransmission des segments manquants.
Supprimer les segments dont l'option d'horodatage est invalide	L'horodatage TCP enregistre le moment où le segment a été envoyé et autorise le pare-feu à vérifier que l'horodatage est valide pour cette session, ce qui empêche le numéro de séquence TCP d'être englobé. L'horodatage TCP est également utilisé pour calculer le temps d'aller-retour. Si cette option est activée, le pare-feu supprime les paquets dont l'horodatage est invalide. Pour afficher un décompte du nombre de segments que le pare-feu a supprimé en raison de l'activation cette option, exécutez la commande CLI suivante : `show counter global tcp_invalid_ts_option` *Cette option est activée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. L'activation de cette option ne doit pas entraîner une dégradation des performances. Toutefois, si une pile de réseau génère incorrectement des segments dont la valeur de l'option d'horodatage TCP est invalide, le fait d'activer cette option peut entraîner des problèmes de connectivité.*
Indicateur de données urgentes	Utilisez cette option pour configurer si le pare-feu permet ou non l'utilisation du pointeur urgent (indicateur bit URG) dans l'en-tête TCP. Le pointeur urgent figurant dans l'en-tête TCP permet de promouvoir un paquet pour un traitement immédiat ; le pare-feu le supprime de la file d'attente de traitement et l'envoie vers la pile TCP/IP de l'hôte. Ce processus est appelé 'AB; traitement hors bande 'BB;. Étant donné que l'implémentation du pointeur urgent varie selon l'hôte, sélectionnez cette option pour **Effacer** (le paramètre par défaut et recommandé) afin d'éviter toute ambiguïté, en interdisant le traitement hors bande pour que le bit hors bande de la charge utile soit intégré à la charge utile et que le paquet ne soit pas traité en urgence. En outre, le paramètre **Effacer** garantit que le pare-feu identifie le flux exact dans la pile du protocole en tant qu'hôte à qui le paquet est destiné. Pour afficher un décompte du nombre de segments dans lesquels le pare-feu a effacé l'indicateur URG lorsque cette option est définie sur **Effacer**, exécutez la commande CLI suivante : `show counter global tcp_clear_urg` *Par défaut, cet indicateur est défini sur Effacer et devrait le rester pour garantir un déploiement plus sécurisé. Cela ne devrait pas entraîner une dégradation des performances ; dans les rares cas où les applications, telles que telnet, utilisent la fonction données urgentes, le protocole TCP peut être affecté. Si vous définissez cet indicateur sur Ne pas*

© 2020 Palo Alto Networks, Inc.

Paramètres TCP	Description
	modifier, le pare-feu autorise les paquets portant l'indicateur bit URG dans l'en-tête TCP et permet le traitement hors-bande (non recommandé).
Supprimer les segments sans indicateur	Les segments TCP illégaux qui ne disposent d'aucun indicateur peuvent être utilisés pour échapper à l'inspection du contenu. Si cette option est activée (par défaut), le pare-feu supprime les paquets qui ne disposent d'aucun indicateur dans l'en-tête TCP. Pour afficher un décompte du nombre de segments que le pare-feu a supprimés en raison de la définition de cette option, exécutez la commande CLI suivante : `show counter global tcp_flag_zero` *Cette option est activée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. L'activation de cette option ne doit pas entraîner une dégradation des performances. Toutefois, si une pile de réseau génère incorrectement des segments sans indicateur TCP, le fait d'activer cette option peut entraîner des problèmes de connectivité.*

Paramètres de décryptage : Vérification de la révocation du certificat

Sélectionnez **Session**, puis dans les Paramètres de déchiffrement, sélectionnez **Certificate Revocation Checking (Vérification de la révocation du certificat)** pour définir les paramètres décrits dans le tableau suivant.

Caractéristiques de la session'A0;: paramètres de vérification de la révocation du certificat	Description
Activer : CRL	Sélectionnez cette option pour utiliser la méthode de liste de révocation du certificat (CRL) afin de vérifier l'état de révocation des certificats. Si vous activez également le protocole OCSP (Online Certificate Status Protocol), le pare-feu essaie d'abord OCSP ; si le serveur OCSP est indisponible, le pare-feu essaie alors la méthode CRL. Pour plus d'informations sur les certificats de déchiffrement, voir Clés et certificats de déchiffrement </37.
Délai de réception'A0;: CRL	Si vous avez activé la méthode CRL pour vérifier l'état de révocation des certificats, indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse du service CRL.

© 2020 Palo Alto Networks, Inc.

Caractéristiques de la session'A0;: paramètres de vérification de la révocation du certificat	Description
Activer : OCSP	Sélectionnez cette option pour utiliser OCSP afin de vérifier l'état de révocation des certificats.
Délai de réception'A0;: OCSP	Si vous avez activé la méthode OCSP pour vérifier l'état de révocation des certificats, indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse du répondeur OCSP.
Bloquer une session dont l'état du certificat est inconnu	Sélectionnez cette option pour bloquer les sessions SSL/TLS lorsque le service OCSP ou CRL renvoie un état de révocation de certificat inconnu. Sinon, le pare-feu poursuit la session.
Bloquer une session dont le délai d'attente de vérification de l'état du certificat a expiré	Sélectionnez cette option pour bloquer les sessions SSL/TLS une fois que le pare-feu a enregistré un délai d'expiration de la demande OCSP ou CRL. Sinon, le pare-feu poursuit la session.
Délai d'expiration du statut du certificat	Indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse d'aucun service d'état de certificat et applique la logique de blocage de la session que vous avez éventuellement définie. Le **Certificate Status Timeout (Délai d'expiration du statut du certificat)** correspond au **Receive Timeout (Délai de réception)** des méthodes OCSP/CRL de la manière suivante : • Si vous activez les deux méthodes, OCSP et CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou l'agrégation des deux valeurs **Receive Timeout (Délai de réception)**. • Si vous activez uniquement la méthode OCSP : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode OCSP. • Si vous activez uniquement la méthode CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode CRL.

Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert

Dans les paramètres de décryptage (onglet **Session**), sélectionnez **SSL Forward Proxy Settings (Paramètres du proxy de transfert SSL)** pour configurer la **RSA Key Size (Taille de la clé RSA)** ou **ECDSA Key Size (Taille de la clé ECDSA)** et l'algorithme de hachage des certificats que le pare-feu présente aux clients lors de l'établissement de sessions pour le déchiffrement du proxy de transfert SSL/TLS. Le tableau suivant décrit ces paramètres.

© 2020 Palo Alto Networks, Inc.

Caractéristiques de la session'A0;: Paramètres de certificat du serveur proxy de transfert	
Taille de la clé RSA	Sélectionnez l'une des options suivantes : • **Defined by destination host (Définie par l'hôte de destination)** (par défaut) : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats en fonction de la clé utilisée par le serveur de destination : • Si le serveur utilise une clé RSA de 1 024 bits, le pare-feu génère un certificat avec cette taille de clé et un algorithme de hachage SHA1. • Si le serveur de destination utilise une taille de clé supérieure à 1 024 bits (par exemple, 2 048 ou 4 096 bits), le pare-feu générera un certificat qui utilisera une clé de 2 048 bits et un algorithme de hachage SHA-256. • **1024-bit RSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé RSA de 1 024 bits et l'algorithme de hachage SHA1, quelle que soit la taille de clé utilisée par le serveur de destination. Depuis le 31 décembre 2013, les Certificate Authorities (autorités de certification - CA) publiques et les navigateurs les plus courants ont limité la prise en charge des certificats X.509 qui utilisent des clés de moins de 2 048 bits. À l'avenir, selon les paramètres de sécurité définis, un navigateur peut avertir l'utilisateur ou bloquer entièrement la session SSL/TLS lorsque de telles clés lui sont présentées. • **2048-bit RSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé RSA de 2 048 bits et l'algorithme de hachage SHA-256, quelle que soit la taille de clé utilisée par le serveur de destination. Les CA publiques et les navigateurs les plus courants prennent en charge les clés de 2 048 bits qui offrent une meilleure sécurité que les clés de 1 024 bits.
Taille de la clé ECDSA	Sélectionnez l'une des options suivantes : • **Defined by destination host (Définie par l'hôte de destination)** (par défaut) : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats en fonction de la clé utilisée par le serveur de destination : • Si le serveur utilise une clé ECDSA de 256 bits ou de 384 bits, le pare-feu génère un certificat avec cette taille de clé. • Si le serveur de destination utilise une taille de clé supérieure à 384 bits, le pare-feu générera un certificat qui utilisera une clé de 521 bits. • **256-bit ECDSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé ECDSA de 256 bits, quelle que soit la taille de clé utilisée par le serveur de destination. • **384-bit ECDSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé ECDSA de 384 bits, quelle que soit la taille de clé utilisée par le serveur de destination.

Paramètres de session VPN

Sélectionnez **Session**, puis dans Paramètres de session VPN, configurez les paramètres généraux liés au pare-feu établissant une session VPN. Le tableau suivant décrit ces paramètres.

© 2020 Palo Alto Networks, Inc.

Paramètres de session VPN	Description
Seuil d'activation du cookie	Indiquez un nombre maximum de SA IKE demi-ouvertes IKEv2 autorisés par pare-feu, au-dessus duquel une validation du cookie est effectuée. Lorsque le nombre de SA IKE demi-ouvertes est supérieur au Seuil d'activation du cookie, le répondeur demande un cookie, et l'initiateur doit répondre par un IKE_SA_INIT contenant un cookie. Si la validation du cookie réussit, une autre session SA peut être ouverte. Une valeur de 0 signifie que la validation du cookie est toujours activée. Le Seuil d'activation du cookie est un paramètre de pare-feu global et il doit être inférieur au paramètre Nombre max de SA demi-ouvertes, qui est également global (plage comprise entre 0 et 65 535 ; par défaut 500).
Nombre max de SA demi-ouvertes	Indiquez le nombre maximum de SA IKE demi-ouvertes IKEv2 que les initiateurs peuvent envoyer au pare-feu sans obtenir de réponse. Une fois le nombre maximum atteint, le pare-feu ne répondra pas aux nouveaux paquets IKE_SA_INIT (plage comprise entre 1 et 65 535 ; par défaut 65 535).
Certificats mis en mémoire cache max	Indiquez le nombre maximum de certificats d'autorité de certification (AC) homologues récupérés via HTTP que le pare-feu peut mettre en mémoire cache. Cette valeur est utilisée uniquement par le Hachage IKEv2 et la fonction d'URL (plage comprise entre 1 et 4 000 ; par défaut 500).

© 2020 Palo Alto Networks, Inc.

Périphérique > Haute disponibilité

- Périphérique > Haute disponibilité

Pour la redondance, déployez vos pare-feu Palo Alto Networks de nouvelle génération selon une configuration haute disponibilité. Il existe deux déploiements HD :

- Actif / passif – Pour ce déploiement, l'homologue actif synchronise en permanence sa configuration et ses informations de session avec l'homologue passif sur deux interfaces dédiées. Dans l'éventualité où survient une interruption matérielle ou logicielle sur le pare-feu actif, le pare-feu passif devient automatiquement actif sans qu'il y ait perte de service. Les déploiements HD actifs/passifs sont pris en charge par tous les modes de l'interface : câble virtuel, couche 2 ou couche 3.
- Actif / actif – Pour ce déploiement, les deux homologues HD sont actifs et traitent le trafic. Ces déploiements sont les plus adaptés pour les scénarios impliquant un routage asymétrique ou dans les cas où vous souhaitez autoriser des protocoles de routage dynamique (OSPF, BGP) pour maintenir le statut actif entre les deux pairs. La HD Active/active est uniquement prise en charge dans les modes d'interface à câble virtuel et de couche 3. En plus des liens HD1 et HD2, des déploiements actifs/actifs exigent une liaison HD3 dédié. La liaison HD3 est utilisée en tant que liaison de transfert des paquets pour la configuration de session et la gestion du trafic asymétrique.



Dans une paire HD, les deux homologues doivent être du même modèle, exécuter la même version PAN-OS et la même version du Contenu, et disposer du même ensemble de licences.

De plus, pour les pare-feu VM-Series, les deux homologues doivent se trouver sur le même hyperviseur, et le même nombre de cœurs de processeur doit être alloué sur chaque homologue.

- Considérations importantes pour la configuration HD
- Configuration des paramètres HD

Considérations importantes pour la configuration HD

- Le sous-réseau utilisé pour l'adresse'A0;IP locale et d'homologue ne doit pas être réutilisé sur le routeur virtuel.
- Les versions OS et du Contenu doivent être identiques sur les deux pare-feu. Une disparité peut empêcher les pare-feu de l'homologue de se synchroniser.
- Les voyants sont verts sur les ports HD du pare-feu actif et orange sur le pare-feu passif.
- Pour comparer les configurations des pare-feu local et homologue à l'aide l'outil **Config Audit (Audit de configuration)** de l'onglet **Device (Périphérique)**, sélectionnez la configuration locale souhaitée dans la zone de sélection de gauche et la configuration de l'homologue dans la zone de sélection de droite.
- Synchronisez les pare-feu via l'interface Web en cliquant sur **Push Configuration (Diffuser la configuration)** dans le widget HD du **Dashboard (Tableau de bord)**. La configuration du pare-feu duquel vous diffusez la configuration remplace celle présente sur le pare-feu homologue. Pour synchroniser les pare-feu à partir de la CLI du pare-feu actif, utilisez la commande request high-availability sync-to-remote running-config.



Dans une configuration HD active/passive comportant des pare-feu qui utilisent des ports 10 gigabits SFP+, lorsqu'un basculement a lieu et que le pare-feu actif passe à l'état passif, le port 10 gigabits Ethernet est désactivé puis réactivé afin d'être actualisé, mais il ne permet pas la transmission jusqu'à ce que le pare-feu soit de nouveau actif. Si vous disposez d'un logiciel de surveillance sur le périphérique voisin, il indique le bagottement du port, car ce dernier devient inactif, puis de nouveau actif. Ce qui n'est pas le cas avec les autres ports, notamment le port 1 gigabit Ethernet, qui est désactivé, mais qui

© 2020 Palo Alto Networks, Inc.

permet encore la transmission ; par conséquent, le bagottement n'est pas détecté par le périphérique voisin.

Configuration des paramètres HD

Pour configurer les paramètres HD, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)**, puis, pour chaque groupe de paramètres, indiquez les informations correspondantes décrites dans le tableau suivant.

Paramètres HA	Description
Onglet Général	
setup	Définissez les paramètres suivants : • **Enable HA (Activer HD)** : activez la fonction HD. • **Group ID (ID du groupe)** : saisissez un numéro pour identifier la paire HD (1 à 63). Ce champ est requis (et doit être unique) si plusieurs paires HD résident sur le même domaine de diffusion. • **Description** – (Facultatif) Saisissez une description de la paire HD. • **Mode** : définissez le type de déploiement HD : **Active Passive (Actif passif)** ou **Active Active (Actif actif)**. • **Device ID (ID de périphérique)** : dans la configuration active/active, définissez l'ID de périphérique pour déterminer quel homologue sera actif principal (définissez l'**Device ID (ID de périphérique)** à **0**) et lequel sera actif secondaire (définissez l'**Device ID (ID de périphérique)** à **1**). • **Enable Config Sync (Activer la synchronisation de la configuration)** : sélectionnez cette option pour activer la synchronisation des paramètres de configuration entre les homologues. *Activez toujours la synchronisation de la configuration pour que les deux périphériques disposent toujours de la même configuration et qu'ils traitent le trafic de la même façon.* • **Peer HA1 IP Address (Adresse IP de l'homologue HD1)** : saisissez l'adresse IP de l'interface HD1 du pare-feu de l'homologue. • **Adresse IP de l'homologue HD1 de secours** – Saisissez l'adresse IP de la liaison de contrôle de secours de l'homologue. *Configurez une adresse IP de l'homologue HD1 de secours pour permettre à la liaison de secours de préserver la synchronisation et la mise à jour des périphériques en cas d'échec de la liaison principale.*
Paramètres Actifs/ Passifs	• **Passive Link State (État passif de la liaison)** : sélectionnez l'une des options suivantes pour spécifier si les liaisons de données sur le pare-feu passif devraient demeurer comme elles sont. Cette option n'est pas disponible sur le pare-feu VM-Series dans AWS. • **Auto** : les liaisons qui possèdent une connectivité physique demeurent les mêmes physiquement, mais dans un état désactivé ; elles ne participent pas à l'apprentissage ARP ou au transfert des paquets. Cette option est utile pour le traitement des temps de convergence lors du basculement puisque le pare-feu gagne du temps pour effectuer

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	la récupération des liaisons. Afin d'éviter des boucles de réseau, ne sélectionnez pas cette option si des interfaces de couche 2 sont configurées sur le pare-feu. • **Shutdown (Arrêter)** : force l'arrêt de la liaison de l'interface. Il s'agit de l'option par défaut qui empêche la création de boucles dans le réseau. *Si aucune interface de couche 2 n'est configurée pour le pare-feu, réglez le Passive Link State (État passif de la liaison) sur auto.* • **Monitor Fail Hold Down Time (min) (Temps d'attente actif après l'échec de la surveillance (min))** : cette valeur comprise entre 1 et 60 minutes détermine l'intervalle pendant lequel un pare-feu sera dans un état non fonctionnez avant de devenir passif. Ce minuteur est utilisé en cas de pulsations ou de messages hello manqués en raison d'un échec de surveillance des liaisons ou des chemins.
Paramètres de sélection	Définissez ou activez les paramètres suivants'A0;: • **Device Priority (Priorité du périphérique)** : saisissez une valeur de priorité pour identifier le pare-feu actif. Le pare-feu ayant la valeur la plus faible (priorité la plus élevée) devient le pare-feu actif (plage de 0 et 255) lorsque la fonction de préemption est activée sur les deux pare-feu de la paire. • **Heartbeat Backup (Sauvegarde de pulsation)** : utilise les ports de gestion des pare-feu HD afin d'indiquer un chemin de sauvegarde des messages de pulsations et Hello. L'adresse'A0;IP du port de gestion est partagée avec l'homologue HD via la liaison de contrôle HA1. Aucune configuration supplémentaire n'est requise. *Activez la Heartbeat Backup (Sauvegarde des pulsations) si vous utilisez un port sur bande pour les liaisons HD1 et HD1 de secours. N'activez pas la Heartbeat Backup (Sauvegarde des pulsations) si vous utilisez un port de gestion sur bande pour les liaisons HD1 et HD1 de secours.* • **Preemptive (Préemptif)** : active le pare-feu prioritaire pour qu'il reprenne l'opération active (active/passive) ou active principale (active/active) après la récupération d'un échec. L'option de préemption doit être activée sur les deux pare-feu pour que le pare-feu prioritaire puisse reprendre l'opération active ou active principale après la récupération d'un échec. Si ce paramètre est désactivé, le pare-feu de priorité inférieure reste actif ou actif principal même si le pare-feu prioritaire est en cours de récupération suite à un échec. *La décision d'activer la Preemptive (préemption) dépend de vos exigences d'affaires. Si vous exigez que le périphérique principal soit le périphérique actif, activez la Preemptive (préemption) de sorte qu'après la récupération d'un échec, le périphérique principal remplace le périphérique secondaire. Si vous exigez le moins d'événements de basculement possible, désactivez les options Preemptive (Préemption) pour qu'après un basculement, la paire HA ne bascule de nouveau pour faire du pare-feu prioritaire le pare-feu principal.*

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	• **HA Timer Settings (Paramètres du minuteur HD)** : sélectionnez l'un des profils prédéfinis : • **Recommended (Recommandé)** : utilisez les paramètres types du minuteur de basculement. À moins que vous soyez certain d'avoir besoin de paramètres différents, il est recommandé d'utiliser les paramètres **Recommended (Recommandés)**. • **Aggressive (Agressif)** : paramètres plus rapides du minuteur de basculement.  *Pour afficher la valeur prédéfinie d'un minuteur inclus dans un profil, sélectionnez Advanced (Avancé) et cliquez sur Load Recommended (Charger le profil recommandé) ou Load Aggressive (Charger le profil agressif). Les valeurs prédéfinies de votre modèle matériel s'affichent alors à l'écran.* • **Advanced (Avancé)** : vous permet de personnaliser les valeurs de manière à ce qu'elles répondent à vos besoins en matière de réseau pour chacun des minuteurs suivants'A0;: • **Promotion Hold Time (Délai de maintien de promotion)** : saisissez la durée d'attente de l'homologue passif (en mode active/passive) ou de l'homologue actif secondaire (en mode active/active) avant de prendre l'état de l'homologue actif ou actif principal après la perte de la communication avec l'homologue HD. Ce délai de maintien démarre après la déclaration de l'échec de l'homologue uniquement. • **Hello Interval (Intervalle Hello)** : saisissez le nombre de millisecondes entre l'envoi des paquets hello et la vérification que le programme HD sur l'autre pare-feu est opérationnel (plage de 8 000 à 60 000 ; par défaut 8 000). • **Heartbeat Interval (Intervalle de pulsation)** : précisez la fréquence de l'échange de messages de pulsations entre les homologues HD sous la forme d'une commande ping ICMP (plage de 1 000 à 60 000 ms ; par défaut 1 000 ms). • **Maximum No. of Flaps (Nombre maximum de battements)** : un battement est comptabilisé lorsque le pare-feu n'est plus à l'état actif pendant 15 minutes après son dernier état actif. Vous pouvez préciser le nombre maximum de battements autorisés avant que le pare-feu ne soit considéré comme suspendu et que le pare-feu passif ne prenne le relais (plage de 0 à 16 ; par défaut 3). La valeur 0 signifie qu'il n'y a pas de valeur maximum (nombre infini de battements avant que le pare-feu ne devienne actif). • **Preemption Hold Time (Délai de maintien de préemption)** : saisissez la durée d'attente (en minutes) que prend un homologue passif ou actif secondaire avant de prendre l'état de l'homologue actif ou actif principal (plage de 1 à 60 ; par défaut 1).
	• **Monitor Fail Hold Up Time (ms) (Temps d'attente actif après l'échec de la surveillance (ms))** : précisez la durée pendant laquelle le pare-feu reste actif après un échec de surveillance des chemins ou des liaisons. Ce paramètre est recommandé pour empêcher un basculement HD dû à l'instabilité occasionnelle de périphériques à proximité (plage de 0 à 60 000 ms ; valeur par défaut 0 ms).

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	• **Additional Master Hold Up Time (min) (Temps d'attente actif principal supplémentaire (min))** – Cet intervalle s'applique aux mêmes événements que le Temps d'attente actif après l'échec de la surveillance (plage de 0 à 60 000 ms, valeur par défaut 500 ms). Cette durée supplémentaire s'applique uniquement à l'homologue actif en mode active/passive et à l'homologue actif principal en mode active/active. Ce délai est recommandé pour empêcher un basculement lorsque les deux homologues rencontrent le même échec de surveillance des liaisons/chemins simultanément.
Liaison de contrôle HD1 / Liaison de contrôle (sauvegarde HD1)	Les pare-feu d'une paire HD utilisent des liaisons HD pour synchroniser des données et gérer des informations d'état. Certains modèles de pare-feu disposent d'une liaison de contrôle dédiée et d'une liaison de contrôle de secours dédiée ; par exemple, les pare-feu PA-5200 Series ont HA1-A et HA1-B. Dans ce cas, vous devriez activer l'option de sauvegarde des pulsations à la page Elections Settings (Paramètres de sélection). Si vous utilisez un port HA1 dédié pour la liaison Liaison de contrôle HA et un port de données comme Liaison de contrôle (HA de secours), il est recommandé d'activer l'option Sauvegarde de pulsation. Pour les pare-feu ne disposant pas d'un port HD dédié, le pare-feu PA-220 par exemple, vous devez configurer le port de gestion pour la connexion Liaison de contrôle HD et une interface de port de données doit être définie sur le type HD pour la connexion Liaison de contrôle HA1 de secours. Le port de gestion étant alors utilisé, vous n'avez pas besoin d'activer l'option Sauvegarde de pulsation, car les sauvegardes des pulsations sont déjà exécutées via la connexion de l'interface de gestion. Sur le pare-feu VM-Series dans AWS, le port de gestion sert de liaison HA1. *Lorsque vous utilisez un port de données pour la liaison de contrôle HD, gardez en tête que les messages de contrôle doivent être transférés entre le panneau de données et le panneau de gestion. Ainsi, en cas d'échec dans le panneau de données, les homologues ne peuvent communiquer les informations relatives à la liaison de contrôle HD et un basculement se produit. Il convient d'utiliser les ports HD dédiés ou, sur les pare-feu ne disposant pas d'un port HD dédié, d'utiliser le port de gestion.* Indiquez les paramètres suivants pour les liaisons de contrôle HD principale et de secours'A0;: • **Port** : sélectionnez le port HD des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. • **IPv4/IPv6 Address (Adresse IPv4/6)** : saisissez l'adresse IPv4 ou IPv6 des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. *Les pare-feu PA-3200 Series ne prennent pas en charge l'adresse IPv6 pour les interfaces HA1 de secours ; utilisez une adresse IPv4.* • **Netmask (Masque réseau)** – Saisissez le masque réseau de l'adresse IP (255.255.255.0 par exemple) des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif.

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	• **Gateway (Passerelle)** : saisissez l'adresse IP de la passerelle par défaut des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. • **Link Speed (Vitesse de liaison)** (modèles dotés de ports HD dédiés uniquement) : sélectionnez la vitesse de la liaison de contrôle entre les pare-feu pour le port HA1 dédié. • **Link Duplex (Mode duplex de la liaison)** (modèles dotés de ports HD dédiés uniquement) : sélectionnez une option de duplex pour la liaison de contrôle entre les pare-feu pour le port HA1 dédié. • **Encryption Enabled (Cryptage activé)** : activez le cryptage après l'exportation de la clé HD de l'homologue HD et son importation sur ce pare-feu. La clé HD de ce pare-feu doit également être exportée depuis ce pare-feu et importée sur l'homologue HD. Configurez ce paramètre pour l'interface HA1 principale. Importez / exportez des clés sur la page Certificats (voir Périphérique > Gestion des certificats > Profil du certificat).  *Activez le chiffrement lorsque les pare-feu ne sont pas directement connectés (les connexions HA1 passent par les périphériques réseau qui peuvent inspecter, traiter et/ou capturer le trafic).* • **Monitor Hold Time (ms) (Temps d'attente pour la surveillance (ms))** – Saisissez la durée d'attente (en millisecondes) du pare-feu avant de déclarer un échec d'homologue dû à l'échec d'une liaison de contrôle (1 000 à 60 000 ms, par défaut, 3 000 ms). Cette option surveille l'état de la liaison physique du ou des ports HA1.
Liaison de données (HA2)  *lorsqu'une liaison de secours HA2 est configurée, un basculement vers la liaison de secours se produit en cas d'échec d'une liaison physique. Lorsque l'option HA2*	Indiquez les paramètres suivants pour les liaisons de données principale et de secours'A0;: • **Port** : sélectionnez le port HD. Configurez ce paramètre pour les interfaces HA2 principale et de secours. Le paramètre de secours est facultatif. • **IP Address (Adresse IP)** : précisez l'adresse IPv4 ou IPv6 des interfaces HD2 principale et de secours. Le paramètre de secours est facultatif. • **Netmask (Masque réseau)** : précisez le masque réseau des interfaces HD2 principale et de secours. Le paramètre de secours est facultatif. • **Gateway (Passerelle)** : précisez la passerelle par défaut des interfaces HD2 principale et de secours. Le paramètre de secours est facultatif. Si les adresses IP HD2 des pare-feu se trouvent dans le même sous-réseau, le champ Passerelle ne doit pas être renseigné. • **Enable Session Synchronization (Activer la synchronisation de la session)** : activez la synchronisation des informations relatives à la session avec le pare-feu passif, puis choisissez une option de transport.  *Activez la synchronisation de la session pour que le périphérique secondaire dispose de la session dans son panneau de données, qui autorise le pare-feu à mettre en correspondance les paquets à la session synchronisée et à transférer rapidement les paquets. Si vous n'activez pas la synchronisation de la session, le pare-feu doit créer la session de nouveau, ce qui introduit la latence et pourrait entraîner l'abandon des connexions.* • **Transport** : choisissez l'une des options de transport suivantes :

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
persistante est activée, le basculement se produit également en cas d'échec des messages de persistance HD dû au seuil défini.	• **Ethernet** : utilisez cette option lorsque les pare-feu sont connectés dos-à-dos ou via un commutateur (Ethertype 0x7261). • **IP** : utilisez cette option lorsque le transport de couche 3 est nécessaire (protocole IP n°99). • **UDP** : utilisez cette option pour que la somme de contrôle soit calculée sur l'ensemble du paquet et non sur l'en-tête comme avec l'option IP (port UDP n°29281). L'avantage d'utiliser le mode UDP est la présence de la somme de contrôle UDP pour vérifier l'intégrité d'un message de synchronisation de la session. • **Link Speed (Vitesse de liaison)** (modèles dotés de ports HD dédiés uniquement) : sélectionnez la vitesse de la liaison de contrôle entre les homologues pour le port HD2 dédié. • **Link Duplex (Mode duplex de la liaison)** (modèles dotés de ports HD dédiés uniquement) : sélectionnez une option de duplex pour la liaison de contrôle entre les homologues pour le port HD2 dédié. • **HA2 keep-alive (HD2 persistante)** : il est recommandé de sélectionner cette option pour surveiller la qualité de la liaison de données HD2 entre les homologues HD. Cette option est désactivée par défaut et vous pouvez l'activer sur un ou les deux homologues. Si cette option est activée, les homologues utiliseront des messages persistants pour surveiller la connexion HD2 afin de détecter une défaillance en fonction du **Threshold (Seuil)** que vous avez défini (par défaut 10 000 ms). Si vous activez la HD2 persistante, l'Action de récupération HD2 persistante sera entreprise. Sélectionnez une **Action** : • **Log Only (Journalisation seulement)** : consigne les défaillances de l'interface HD2 dans le journal système en tant qu'événements critiques. Sélectionnez cette option pour les déploiements actifs/passifs parce que l'homologue actif est le seul pare-feu effectuant le transfert du trafic. L'homologue passif est dans un état de sauvegarde et ne transfère pas le trafic ; ainsi, un chemin de données divisé n'est pas nécessaire. Si vous n'avez pas configuré de liaisons de secours HD2, la synchronisation de l'état sera éteinte. Un journal d'informations est généré en cas de récupération du chemin HA2. • **Split Datapath (Chemin de données divisé)** : sélectionnez cette option dans les déploiements HD actifs/actifs pour indiquer à chaque homologue de prendre possession de leurs tables d'état et de session locaux lorsqu'il détecte une défaillance de l'interface HD2. Aucune synchronisation de l'état et de la session ne peut se produire sans connectivité HD2 ; cette action permet une gestion séparée des tables de session pour assurer le transfert réussi du trafic par chaque homologue HD. Pour éviter cette situation, configurez une liaison de secours HD2. • **Threshold (ms) (Seuil (ms))** – La durée pendant laquelle les messages de persistance ont échoué avant le déclenchement de l'une des actions ci-dessus (plage de 5 000 à 60 000 ms, par défaut 10 000 ms).
Onglet Surveillance des liaisons et des chemins (non disponible pour le pare-feu VM-Series dans AWS)	
Surveillance des chemins	Indiquez les options suivantes'A0;:

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	• **Enabled (Activé)** : activez la surveillance des chemins. La surveillance des chemins permet au pare-feu de surveiller les adresses'A0;IP de destination définies en envoyant des messages ping ICMP afin de vérifier qu'elles répondent. Utilisez la surveillance des chemins pour les configurations à câble virtuel, couche 2 ou couche 3 dans lesquelles la surveillance des autres périphériques du réseau est requise pour le basculement, mais où la surveillance des liaisons seule ne suffit pas. • **Failure Condition (Condition d'échec)** : sélectionnez cette option en cas de basculement lorsqu'un ou tous les groupes de chemins surveillés ne répondent pas.  *Activez et configurez la surveillance des chemins ou la surveillance des liaisons pour déclencher un basculement en cas d'échec d'un chemin ou d'une liaison. Configurez au moins un Path Group (Groupe de chemins) pour la surveillance des chemins et configurez au moins un Link Group (Groupe de liaisons) pour la surveillance des liaisons.*
Groupe de chemins	Définissez un ou plusieurs groupes de chemins afin de surveiller des adresses de destination spécifiques. Pour ajouter un groupe de chemins, cliquez sur **Add (Ajouter)** pour le type d'interface (**Virtual Wire (Câble virtuel)**, **VLAN** ou **Virtual Router (Routeur virtuel)**) et précisez les paramètres suivants : • **Name (Nom)** : sélectionnez un câble virtuel, un VLAN ou un routeur virtuel dans le menu déroulant (qui est renseigné selon l'ajout d'un chemin d'accès au câble virtuel, au VLAN ou au routeur virtuel). • **Enabled (Activé)** : activez le groupe de chemins. • **Condition d'échec** – Sélectionnez cette option en cas d'échec lorsqu'une ou toutes les adresses de destination précisées ne répondent pas. • **Source IP (IP source)** : pour les interfaces câble virtuel et VLAN, saisissez l'adresse IP source utilisée dans les paquets à analyser envoyés au routeur du saut suivant (adresse IP de destination). Le routeur local doit être en mesure de transmettre l'adresse au pare-feu. L'adresse'A0;IP source de groupes de chemins associés aux routeurs virtuels est automatiquement configurée en tant qu'adresse'A0;IP de l'interface indiquée dans la table de routage comme interface d'entrée de l'adresse'A0;IP de destination définie. • **Destination IPs (IP de destination)** : saisissez une ou plusieurs adresses de destination (séparées par des virgules) à surveiller. • **Intervalle des requêtes ping** – Indiquez l'intervalle entre les requêtes ping envoyées à l'adresse de destination (plage de 200 à 60 000 ms ; par défaut 200 ms). • **Ping Count (Nombre de requêtes ping)** – Indiquez le nombre d'échecs de requêtes ping avant de déclarer un échec (plage de 3 à 10 requêtes ping ; par défaut 10 requêtes ping).
Surveillance des liaisons	Indiquez les options suivantes'A0;: • **Enabled (Activé)** : activez la surveillance des liaisons. Elle permet de déclencher un basculement en cas d'échec d'une liaison physique ou d'un groupe de liaisons physiques.

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	• **Failure Condition (Condition d'échec)** : sélectionnez cette option en cas de basculement lorsqu'un ou tous les groupes de liaisons surveillés ne répondent pas.  *Activez et configurez la surveillance des chemins ou la surveillance des liaisons pour déclencher un basculement en cas d'échec d'un chemin ou d'une liaison. Configurez au moins un Path Group (Groupe de chemins) pour la surveillance des chemins et configurez au moins un Link Group (Groupe de liaisons) pour la surveillance des liaisons.*
Groupes de liaisons	Définissez un ou plusieurs groupes de liaisons afin de surveiller des liaisons Ethernet spécifiques. Pour ajouter un groupe de liaisons, précisez les informations suivantes, puis cliquez sur **Add (Ajouter)** : • **Name (Nom)** : donnez un nom au groupe de liaisons. • **Enabled (Activé)** : activez le groupe de liaisons. • **Failure Condition (Condition d'échec)** – Sélectionnez en cas d'échec lorsqu'une ou toutes les liaisons sélectionnées sont défaillantes. • **Interfaces** : sélectionnez une ou plusieurs interfaces Ethernet à surveiller.
Onglet Configuration Active/Active	
Transfert des paquets	Cliquez sur **Enable (Activer)** pour activer les homologues afin qu'ils transfèrent les paquets vers la liaison HD3 pour la configuration de session et pour l'inspection de la couche 7 (inspection de l'App-ID, du Content-ID et des menaces) des sessions asymétriquement acheminées.
Interface HA3	Sélectionnez l'interface de données que vous prévoyez utiliser pour transférer des paquets entre les homologues HD actifs/actifs. L'interface que vous utilisez doit être une interface dédiée de couche 2 dont le type d'interface est défini à **HD**.  *Si la liaison HD3 échoue, l'homologue actif secondaire passera à l'état non fonctionnel. Pour éviter cette situation, configurez une interface de groupe d'agrégation de liaison (LAG) avec deux ou plusieurs interfaces physiques en tant que liaison HD3. Le pare-feu ne prend pas en charge une liaison de secours HD3. Une interface globale comprenant de multiples interfaces fournira une capacité supplémentaire et une redondance des liaisons pour prendre en charge le transfert des paquets entre les homologues HD.* lorsque vous utilisez l'interface HD3, vous devez activer les trames Jumbo sur le pare-feu et tous les périphériques réseau intermédiaires. Pour activer les trames Jumbo, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session**, puis l'option **Enable Jumbo Frame (Activer les trames Jumbo)** dans la section Paramètres de session.
Sync VR	Forcez la synchronisation de tous les routeurs virtuels configurés sur les homologues HD.

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	Utilisez cette option lorsque le routeur virtuel n'est pas configuré pour fonctionner avec des protocoles de routage dynamique. Les deux homologues doivent être connectés au même routeur de saut suivant via un réseau commuté et utiliser uniquement un routage statique.
Synchronisation QoS	Synchronisez la sélection du profil de qualité de service (QoS) sur toutes les interfaces physiques. Utilisez cette option lorsque les homologues disposent de vitesses de liaison similaires et que les mêmes profils QoS sont requis sur toutes les interfaces physiques. Ce paramètre s'applique à la synchronisation des paramètres de QoS de l'onglet **Network (Réseau)**. La politique de QoS est synchronisée, quel que soit ce paramètre.
Temps d'attente provisoire (s)	En cas d'échec d'un pare-feu en configuration HD active/active échoue, celui-ci passe à l'état provisoire. La transition de l'état provisoire à l'état actif secondaire déclenche le Temps d'attente provisoire, au cours duquel le pare-feu tente de créer des contiguïtés de routage et de remplir sa table de routage avant de traiter les paquets. Sans ce minuteur, le pare-feu de récupération passe immédiatement à l'état actif/secondaire et rejette les paquets, car il ne dispose pas des itinéraires nécessaires (60 secondes par défaut).
Sélection du propriétaire de la session	Le propriétaire de la session est responsable de toutes les inspections de couche 7 (App-ID et Content-ID) de la session et de générer tous les journaux de trafic de la session. Sélectionnez l'une des options suivantes pour spécifier la façon de déterminer le propriétaire de la session pour un paquet : • **First packet (Premier paquet)** : sélectionnez cette option pour désigner le pare-feu qui reçoit le premier paquet dans une session en tant que propriétaire de la session. Il s'agit de la configuration recommandée pour minimiser le trafic sur HD3 et répartir la charge du panneau de données entre les homologues. • **Primary Device (Périphérique principal)** : sélectionnez cette option si vous souhaitez que le pare-feu actif principal accueille toutes les sessions. Dans ce cas, si le pare-feu actif secondaire reçoit le premier paquet, il transfère tous les paquets nécessitant une inspection de couche 7 du pare-feu actif principal sur la liaison HD3.
Configuration de la session	Le pare-feu responsable de la configuration de la session exécute le traitement de couche 2 à couche 4 (notamment la traduction d'adresse) et crée l'entrée de table de la session. Puisque la configuration de la session consomme des ressources provenant du panneau de gestion, vous pouvez sélectionner l'une des options suivantes pour aider à distribuer la charge : • **Primary Device (Périphérique principal)** : le pare-feu actif principal configure toutes les sessions. • **IP Modulo (Modulo IP)** : distribue une configuration de session en fonction de la parité de l'adresse IP source. • **IP Hash (Hachage IP)** : distribue une configuration de session en fonction d'un hachage de l'adresse IP source ou de l'adresse IP source et de destination, ainsi qu'une valeur de départ pour le hachage si vous avez besoin d'une opération plus aléatoire. • **First Packet (Premier paquet)** : le pare-feu qui reçoit le premier paquet exécute la configuration de la session, même dans les cas où l'homologue est propriétaire de la session. Cette option réduit le trafic sur la liaison HD3

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
	et veille à ce que le travail intensif du panneau de gestion visant à configurer la session ait toujours lieu sur le pare-feu qui reçoit le premier paquet.
Adresse virtuelle	Cliquez sur **Add (Ajouter)**, sélectionnez l'onglet **IPv4** ou **IPv6**, puis cliquez à nouveau sur **Add (Ajouter)** pour saisir des options afin de spécifier le type d'adresse virtuelle HD à utiliser : Partage de charge ARP ou flottante Vous pouvez également mélanger le type de types d'adresse virtuelle dans l'homologue. Par exemple, vous pourriez utiliser le partage de charge ARP sur l'interface LAN et une adresse IP flottante sur l'interface WAN. • **Floating (Adresse IP flottante)** : saisissez une adresse IP qui se déplacera entre les homologues HD en cas d'échec d'une liaison ou d'un système. Configurez deux adresses IP flottantes sur l'interface de sorte que chaque pare-feu dispose d'une adresse propre, puis définir la priorité. En cas d'échec de l'un des pare-feu, l'adresse IP flottante est transmise à l'homologue HD. • **Device 0 Priority (Priorité périphérique 0)** : définissez la priorité du pare-feu à ID de périphérique 1 afin de déterminer quel pare-feu dispose de l'adresse IP flottante. Le pare-feu avec la valeur la plus faible dispose de la priorité la plus élevée. • **Device 1 Priority (Priorité périphérique 1)** : définissez la priorité du pare-feu à ID de périphérique 1 afin de déterminer quel pare-feu dispose de l'adresse IP flottante. Le pare-feu avec la valeur la plus faible dispose de la priorité la plus élevée. • **Failover address if link state is down (Adresse de basculement si l'état de liaison est inactif)** : utilisez l'adresse de basculement lorsque l'état de liaison est inactif sur l'interface. • **Floating IP bound to the Active-Primary HA device (Adresse IP flottante liée au périphérique HD actif principal)** : sélectionnez cette option pour lier l'adresse IP flottante à l'homologue actif principal. Dans le cas où un homologue ne fonctionne pas, le trafic est envoyé en continu à l'homologue actif principal, même après le rétablissement du pare-feu défaillant et devient l'homologue actif secondaire. • **ARP Load Sharing (Partage de charge ARP)** : saisissez une adresse IP qui sera partagée par la paire HD et qui fournira des services de passerelle aux hôtes. Cette option est uniquement nécessaire si le pare-feu est situé sur le même domaine de diffusion que les hôtes. Sélectionnez le **Device Selection Algorithm (Algorithme de sélection du périphérique)** : • **IP Modulo (Modulo IP)** : sélectionnez le pare-feu qui répondra aux requêtes ARP en fonction de la parité de l'adresse IP des demandeurs ARP. • **IP Hash (Hachage IP)** : sélectionnez le pare-feu qui répondra aux requêtes ARP en fonction d'un hachage de l'adresse IP des demandeurs ARP.
Commandes opérationnelles	
Suspendre le périphérique local	La commande suivante de la CLI en mode opérationnel fait passer l'homologue HA local à l'état suspendu et désactive temporairement la fonction HA sur le pare-feu. Si vous suspendez le pare-feu actif, le pare-feu secondaire prend le relais.

© 2020 Palo Alto Networks, Inc.

Paramètres HA	Description
(ou Rendre fonctionnel le périphérique local)	`request high-availability state suspend` Pour remettre un pare-feu suspendu à l'état fonctionnel, utilisez la commande suivante de la CLI en mode opérationnel : **`request high-availability state functional`** Pour tester le basculement, vous pouvez déconnecter le pare-feu actif (ou actif/principal) ou cliquez sur ce lien pour suspendre le pare-feu actif.

© 2020 Palo Alto Networks, Inc.

Périphérique > Carte de transfert des journaux

- Périphérique > Carte de transfert des journaux

La Log Forwarding Card (Carte de transfert des journaux ; LFC) est une carte de journal haute performance qui transfère tous les journaux des panneaux de données (trafic et menace, par exemple) depuis le pare-feu vers un ou plusieurs systèmes de journalisation externes, comme Panorama ou un serveur syslog. Comme les journaux des panneaux de données ne sont plus disponibles sur le pare-feu local, l'onglet ACC est supprimé de l'interface Web de gestion et Surveillance > Journaux ne contient que les journaux de gestion (Configuration, Système et Alarmes).

Vous devez configurer les ports de la LFC. Le port 1 opère à 10 Go et le port 9 opère à 40 Go. Configurez les ports sous **Device (Périphérique) > Log Forwarding Card (Carte de transfert des journaux)**. Le pare-feu utilise ces ports pour transférer les journaux des panneaux de données à un système externe, comme Panorama ou un serveur syslog.

Reportez-vous au Guide de référence matérielle du pare-feu PA-7000 Series pour obtenir des informations sur les exigences et les composants de la LFC.

Pour une interface LFC, configurez les paramètres décrits dans le tableau suivant.

Paramètres d'une interface LFC	Description
Name (Nom)	Saisissez un nom d'interface. Pour une LFC, vous devez sélectionner **lfc1/1** ou **lfc1/9**.
Commentaire	Saisissez une description de l'interface (facultatif).
IPv4	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6	Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10000** ou **40000**) ou sélectionnez **auto** (par défaut) pour que le pare-feu détermine automatiquement la vitesse en fonction de la connexion. La vitesse d'interface disponible dépend du port utilisé (lfc1/1 ou lfc1/9). **Auto** est la seule option possible pour les interfaces dont la vitesse ne peut être configurée.
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé en fonction de la connexion (**auto**). La valeur par défaut est **auto**.
Priorité du port LACP	Le pare-feu utilise ce champ uniquement si vous avez activé LACP (Link Aggregation Control Protocol/protocole d'agrégation de liens) pour le groupe agrégé. Si le nombre d'interfaces que vous affectez au groupe dépasse le nombre

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface LFC	Description
	d'interfaces actives (le champ Max Ports [Nombre maximum de ports]), le pare-feu utilise les priorités de port LACP des interfaces pour déterminer celles qui sont en mode veille. Plus le nombre est petit, plus la priorité est grande (intervalle compris entre 1 et 65 535 ; valeur par défaut : 32 768).

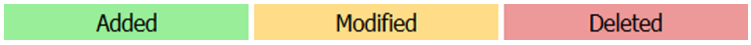
Les sous-interfaces sont disponibles si vous avez activé la fonctionnalité de systèmes virtuels multiples. Pour configurer une sous-interface LFC, ajoutez une sous-interface et utilisez les paramètres décrits dans le tableau suivant.

Paramètres d'une sous-interface LFC	Description
Nom de l'interface	**Interface Name (Nom de l'interface)** (en lecture seule) affiche le nom de l'interface de carte de journal sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de l'interface (facultatif).
Étiquette	Saisissez le **Tag (Étiquette)** VLAN (0-4 094) de la sous-interface.  *Donnez à l'étiquette le même numéro que la sous-interface pour simplifier son utilisation.*
Virtual System (système virtuel - vsys)	Sélectionnez le système virtuel auquel la sous-interface Log Forwarding Card (Carte de transfert des journaux ; LFC) est affectée. Sinon, vous pouvez cliquer sur **Virtual Systems (Systèmes virtuels)** pour ajouter un nouveau système virtuel. Une fois qu'une sous-interface LFC est affectée à un système virtuel, cette interface est utilisée comme interface source pour tous les services qui transfèrent les journaux (Syslog, messagerie, SNMP) depuis la carte de journal.
IPv4	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6	Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.

© 2020 Palo Alto Networks, Inc.

Périphérique > Audit de configuration

Sélectionnez **Device (Périphérique)** > **Config Audit (Audit de configuration)** pour afficher les différences entre les fichiers de configuration. La page affiche les configurations côte à côte dans des volets distincts et met en évidence les différences ligne par ligne en utilisant des codes de couleurs pour indiquer les ajouts (vert), les modifications (jaune) ou les suppressions (rouge) :



Paramètres d'audit de configuration	Description
Menus déroulants de noms de configuration (sans référence)	Sélectionnez deux configurations à comparer dans les menus déroulants de noms de configuration (sans référence) (les valeurs par défaut sont **Running config (Configuration active)** et **Candidate config (Configuration candidate)**). *Vous pouvez filtrer un menu déroulant en saisissant une chaîne de texte dérivée de la valeur Description de l'opération de validation associée à la configuration souhaitée (reportez-vous à la section Validation des modifications).*
Menu déroulant Contexte	Utilisez le menu déroulant **Context (Contexte)** pour spécifier le nombre de lignes à afficher avant et après que les différences aient été mises en évidence dans chaque fichier. Le fait de spécifier plus de lignes peut vous aider à corréler les résultats de l'audit des paramètres dans l'interface Web. Si vous définissez le **Context (Contexte)** à **All (Tous)**, les résultats incluent l'ensemble des fichiers de configuration.
accéder	Cliquez sur **Go (Lancer)** pour débuter l'audit.
Précédent ( ) et Suivant ( )	Ces flèches de navigation sont activées lorsque des versions de configuration consécutives sont sélectionnées dans les menus déroulants de noms de configuration. Cliquez sur pour comparer la paire précédente de configurations dans les menus déroulants ou cliquez sur pour comparer la prochaine paire de configurations.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de mot de passe

- Périphérique > Profils de mot de passe
- Panorama > Profils de mot de passe

Sélectionnez **Device (Périphérique)** > **Password Profiles (Profils de mot de passe)** ou **Panorama** > **Password Profiles (Profils de mot de passe)** pour définir les exigences relatives au mot de passe de base pour les comptes locaux individuels. Les profils de mot de passe remplacent tous les paramètres Complexité minimale du mot de passe que vous avez définis pour tous les comptes locaux (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**).

Pour appliquer un profil de mot de passe à un compte, sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)** (pare-feu) ou à **Panorama** > **Administrators (Administrateurs)** (Panorama), sélectionnez un compte et ensuite choisissez le **Password Profile (Profil de mot de passe)**.

Vous ne pouvez pas attribuer des profils de mot de passe à des comptes administratifs qui utilisent l'authentification de la base de données locale (voir Périphérique > Base de données d'utilisateurs locale > Utilisateurs).

Pour créer un profil de mot de passe, cliquez sur **Add (Ajouter)** et spécifiez les informations répertoriées dans le tableau suivant.

Paramètres du profil de mot de passe	Description
Name (Nom)	Saisissez un nom pour identifier le profil de mot de passe (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Période de modification du mot de passe requise (jours)	Requiert que les administrateurs modifient régulièrement leurs mots de passe en fonction du nombre de jours défini (plage de 0 à 365 jours). Exemple'A0;: si la valeur est définie sur 90, les administrateurs sont invités à modifier leurs mots de passe tous les 90'A0;jours. Vous pouvez également définir un message d'avertissement d'expiration de 0 à 30 jours et indiquer un délai supplémentaire.
Avertissement avant la date d'expiration (jours)	Si une période de modification du mot de passe requise est définie, ce paramètre peut être utilisé pour demander à l'utilisateur de modifier son mot de passe à chaque connexion à mesure que la date de modification du mot de passe requise approche (plage de 0 à 30).
Nombre d'ouvertures de session Administrateur après expiration	Autorisez l'administrateur à se connecter pour un certain nombre de fois une fois son compte arrivé à expiration. Par exemple, si la valeur est définie sur 3 et que le compte a expiré, il peut se connecter 3 autres fois avant que le compte ne soit verrouillé (plage de 0 à 3).
Période de grâce après expiration (jours)	Autorise l'administrateur à se connecter le nombre de jours indiqué une fois son compte arrivé à expiration (plage de 0 à 30).

© 2020 Palo Alto Networks, Inc.

Exigences relatives au nom d'utilisateur et au mot de passe

Le tableau suivant répertorie les caractères valides pouvant être utilisés dans les noms d'utilisateurs et les mots de passe des comptes PAN-OS et Panorama.

Account Type (Type de compte)	Restrictions de nom d'utilisateur et de mot de passe
Jeu de caractères du mot de passe	Aucune restriction ne s'applique aux jeux de caractères des mots de passe.
Admin distant, VPN SSL ou portail captif	Les caractères suivants ne sont pas autorisés dans le nom d'utilisateur'A0;: • Apostrophe inversée (`) • Symbole inférieur et supérieur (< et >) • Perluète (&) • Astérisque (*) • A commercial (@) • Point d'interrogation (?) • Barre verticale (|) • Guillemet simple (') • Point-virgule (;) • Guillemet double (") • Dollar ($) • Parenthèses ('(' et ')') • Deux-points (':')
Comptes administrateur locaux	Les caractères suivants sont autorisés dans les noms d'utilisateurs locaux'A0;: • Minuscules (a-z) • Majuscules (A-Z) • Chiffres (0-9) • Trait de soulignement (_) • Point (.) • Trait d'union (-) *les noms d'utilisateurs ne peuvent pas commencer par un tiret (-).*

© 2020 Palo Alto Networks, Inc.

Périphérique > Administrateurs

Les comptes administrateur contrôlent l'accès aux pare-feu et à Panorama. Un administrateur de pare-feu peut disposer d'un accès complet ou en lecture seule à un pare-feu ou à un système virtuel d'un pare-feu. Les pare-feu ont un compte **admin** prédéfini qui dispose d'un accès complet.

Pour définir les administrateurs Panorama, voir Panorama > Périphériques gérés > Récapitulatif.

Les options d'authentification suivantes sont prises en charge'A0;:

- Authentification par mot de passe : l'administrateur saisit un nom d'utilisateur et un mot de passe pour se connecter. Aucun certificat n'est requis pour cette authentification. Vous pouvez l'utiliser conjointement avec d'autres profils d'authentification, ou pour l'authentification de base de données locale.
- Authentification du certificat du client (Web) : aucun nom d'utilisateur ni mot de passe n'est requis pour cette authentification ; le certificat suffit pour authentifier l'accès au pare-feu.
- Authentification des clés publiques (SSH) : l'administrateur génère une paire de clés publique/privée sur la machine qui doit accéder au pare-feu, puis charge la clé publique sur le pare-feu pour permettre un accès sécurisé sans devoir saisir un nom d'utilisateur ni un mot de passe.

Pour ajouter un administrateur, cliquez sur **Add (Ajouter)** et renseignez les informations suivantes :

Paramètres du compte administrateur	Description
Name (Nom)	Donnez un nom de connexion à l'administrateur (31'A0;caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des tirets, des points et des caractères de soulignement. les noms d'utilisateurs ne peuvent pas commencer par un tiret (-).
Profil d'authentification	Sélectionnez un profil d'authentification pour l'authentification de l'administrateur Vous pouvez utiliser ce paramètre pour l'authentification RADIUS, TACACS+, LDAP, Kerberos, SAML ou de base de données locale. Pour plus de détails, voir Périphérique > Profil d'authentification.
Utiliser uniquement l'authentification du certificat client (Web)	Sélectionnez cette option pour utiliser l'authentification du certificat du client pour l'accès au Web. Si vous sélectionnez cette option, un nom d'utilisateur et un mot de passe ne sont pas requis ; le certificat suffit pour authentifier l'accès au pare-feu.
Nouveau mot de passe Confirmer le nouveau mot de passe	Saisissez et confirmez un mot de passe sensible à la casse pour l'administrateur (31 caractères maximum). Vous pouvez également sélectionner **Setup (Configuration)** > **Management (Gestion)** pour imposer un nombre minimal de caractères requis pour le mot de passe. *Pour garantir la sécurité de l'interface de gestion des pare-feu, nous recommandons que vous changiez les mots de passe administrateur régulièrement en utilisant des lettres en minuscules, en majuscules et des chiffres. Vous pouvez également configurer les paramètres*

© 2020 Palo Alto Networks, Inc.

Paramètres du compte administrateur	Description
	de Complexité minimale des mots de passe pour tous les administrateurs du pare-feu.
Utiliser l'authentification à clef publique (SSH)	Sélectionnez cette option pour utiliser l'authentification de clé publique SSH. Cliquez sur **Import Key (Importer la clé)** et recherchez le fichier de clé publique à sélectionner. La clé chargée s'affiche dans la zone de texte en lecture seule. Les formats de fichier de clé pris en charge sont IETF SECSH et OpenSSH. Les algorithmes de clé pris en charge sont DSA (1 024 bits) et RSA (768 à 4 096 bits). *Si l'authentification des clés publiques échoue, le pare-feu demande à l'administrateur son nom d'utilisateur et mot de passe.*
Type d'administrateur	Affectez un rôle à cet administrateur. Le rôle détermine les éléments que l'administrateur peut consulter et modifier. Si vous sélectionnez **Role Based (Basé sur les rôles)**, sélectionnez un profil de rôle personnalisé dans la liste déroulante. Pour plus de détails, voir Périphérique > Rôles admin. Si vous sélectionnez **Dynamic (Dynamique)**, vous pouvez choisir l'un des rôles prédéfinis suivants : • **Superuser (Super utilisateur)** – Dispose d'un accès complet au pare-feu et peut définir de nouveaux comptes administrateur et de nouveaux systèmes virtuels. Vous devez posséder des privilèges de super utilisateur pour créer un utilisateur administratif avec privilèges de super utilisateur. • **Superuser (Super utilisateur)** (lecture seule) – Dispose d'un accès en lecture seule au pare-feu. • **Device administrator (Administrateur du périphérique)** – Dispose d'un accès complet à tous les paramètres du pare-feu, sauf pour la définition de nouveaux comptes ou de nouveaux systèmes virtuels. • **Device administrator (Administrateur du périphérique)** (lecture seule) – Dispose d'un accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et aux comptes administrateur (seul le compte connecté est visible). • **Virtual system administrator (Administrateur du système virtuel)** - A accès à des systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particulier des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un administrateur du système virtuel n'a pas accès aux interfaces de réseau, aux routeurs virtuels, aux tunnels IPSec, aux VLAN, aux câbles virtuels, aux tunnels GRE, à DHCP, au proxy DNS, à QoS, à LLDP ou aux profils réseaux. • **Virtual system administrator (Administrateur du système virtuel)** (lecture seule) - A accès en lecture seule à des

© 2020 Palo Alto Networks, Inc.

Paramètres du compte administrateur	Description
	systèmes virtuels spécifiques du pare-feu pour visualiser des aspects particuliers des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un administrateur du système virtuel ayant un accès en lecture seule n'a pas accès aux interfaces de réseau, aux routeurs virtuels, aux tunnels IPSec, aux VLAN, aux câbles virtuels, aux tunnels GRE, à DHCP, au proxy DNS, à QoS, à LLDP ou aux profils réseaux.
Virtual System (système virtuel - vsys) (Rôle administrateur du système virtuel uniquement)	Cliquez sur **Add (Ajouter)** pour sélectionner les systèmes virtuels que peut gérer l'administrateur.
Profil de mot de passe	Sélectionnez le profil de mot de passe, le cas échéant. Pour créer un nouveau profil de mot de passe, voir Périphérique > Profils de mot de passe. *Créez un profil de mot de passe pour les administrateurs pour veiller à ce que les mots de passe des administrateurs expirent après une période de temps configurée. La modification fréquente des mots de passe des administrateurs permet aux pirates d'utiliser les identifiants enregistrés ou volés.*

© 2020 Palo Alto Networks, Inc.

Périphérique > Rôles admin

Sélectionnez **Device (Périphérique)** > **Admin Roles (Rôles administrateur)** pour définir les profils de Rôles administrateur, qui sont des rôles personnalisés déterminant les privilèges d'accès et les responsabilités des utilisateurs administratifs. Vous affectez des profils de Rôle administrateur ou des rôles dynamiques lorsque vous créez des comptes administratifs (Périphérique > Administrateurs).

Pour définir des profils de Rôle administrateur pour les administrateurs Panorama, voir Panorama > Périphériques gérés > Récapitulatif.

Le pare-feu possède trois rôles prédéfinis que vous pouvez utiliser pour établir des critères communs. Vous utilisez tout d'abord le rôle super utilisateur pour la configuration initiale du pare-feu et pour créer les comptes administrateur de l'administrateur de sécurité, de l'administrateur d'audit et de l'administrateur cryptographique. Après avoir créé ces comptes et appliqué les Rôles admin aux critères communs appropriés, vous devez ensuite vous connecter en utilisant ces comptes. Le compte super utilisateur par défaut en mode FIPS-CC (FIPS [Federal Information Processing Standard] / CC [Common Criteria]) est **admin** et le mot de passe par défaut est **paloalto**. En mode d'utilisation standard, le compte par défaut est **admin** et le mot de passe **admin**. Les rôles administrateur prédéfinis sont créés sans fonction de chevauchement, à l'exception près qu'ils disposent tous d'un accès en lecture seule à la piste de vérification (sauf l'administrateur d'audit qui dispose d'un accès en lecture/suppression complet). Ces rôles administrateur ne peuvent pas être modifiés et sont définis comme suit'A0;:

- auditadmin : l'administrateur d'audit est responsable de la révision régulière des données d'audit du pare-feu.
- cryptoadmin : l'administrateur cryptographique est responsable de la configuration et de la maintenance des éléments cryptographiques liés à l'établissement de connexions sécurisées avec le pare-feu.
- Securityadmin – L'Administrateur de la sécurité est responsable de toutes les autres tâches administratives (la création de la politique de Sécurité par exemple) non exécutées par les deux autres rôles administrateur.

Pour ajouter un profil de Rôle administrateur, cliquez sur **Add (Ajouter)** et spécifiez les paramètres décrits dans le tableau suivant.

Créez des règles personnalisées pour restreindre l'accès des administrateurs à ce que chaque type d'administrateur a besoin. Pour chaque type d'administrateur, activez, désactivez ou configurez l'accès en lecture seule pour l'accès Web UI (UI Web), XML/REST API (API REST/XML) et Command Line (Ligne de commande).

Paramètres du rôle administrateur	
Name (Nom)	Saisissez un nom pour identifier ce rôle administrateur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	(Facultatif) Saisissez une description pour le rôle (255 caractères maximum).
Rôle	Sélectionnez la portée des responsabilités administratives : • **Device (Périphérique)** – Le rôle s'applique à l'ensemble du pare-feu, peu importe s'il possède plus d'un système virtuel (vsys). • **Virtual System (Système virtuel)** - Le role (rôle) s'applique à des systèmes virtuels spécifiques du pare-feu et à des aspects spécifiques

© 2020 Palo Alto Networks, Inc.

Paramètres du rôle administrateur	
	des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un profil du rôle admin basé sur un **Virtual system (système virtuel)** n'a pas accès à l'onglet **Web UI (UI Web)** des interfaces de réseau, des VLAN, des câbles virtuels, des tunnels IPSec, des tunnels GRE, du DHCP, du proxy DNS, du QoS ou des profils réseaux. Vous sélectionnez les systèmes virtuels lorsque vous créez des comptes administratifs (Périphérique > Administrateurs).
Interface Utilisateur Web	Cliquez sur les icônes pour que les fonctions spécifiques à l'interface Web définissent les privilèges d'accès autorisé : • **Enable (Activer)** – Accès en lecture/écriture à la fonction sélectionnée. • **Read Only (Lecture seule)** – Accès en lecture seule à la fonction sélectionnée. • **Disable (Désactiver)** – Aucun accès à la fonction sélectionnée.
Interface API REST/XML	Cliquez sur les icônes pour que les fonctions spécifiques de l'API XML/ REST définissent les privilèges d'accès autorisé (**Enable (Activer)**, ou **Disable (Désactiver)**).
Ligne de commande	Sélectionnez le type de rôle d'accès à la CLI. La valeur par défaut est **Aucun**, ce qui signifie que l'accès à la CLI n'est pas autorisé. Les autres options varient selon la portée du Rôle : • **Périphérique** • **superuser (super utilisateur)** – Dispose d'un accès complet au pare-feu et peut définir de nouveaux comptes administrateur et de nouveaux systèmes virtuels. Vous devez posséder des privilèges de super utilisateur pour créer un utilisateur administratif avec privilèges de super utilisateur. • **superreader (super lecteur)** – Dispose de l'accès en lecture seule au pare-feu. • **deviceadmin (administrateur de périphérique)** – Dispose d'un accès complet à tous les paramètres du pare-feu, sauf pour la définition de nouveaux comptes ou de nouveaux systèmes virtuels. • **devicereader (lecteur de périphérique)** – Dispose d'un accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et aux comptes administrateur (seul le compte connecté est visible). • **Virtual System (système virtuel - vsys)** • **vsysadmin** : a accès aux systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particuliers des systèmes virtuels. Le paramètre **vsysadmin (vsysadmin)** ne contrôle pas les fonctions du pare-feu et du réseau (comme le routage statique ou dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP ou les profils de réseaux). • **vsysreader** : a un accès en lecture seule aux systèmes virtuels spécifiques du pare-feu et aux aspects particuliers d'un système virtuel. Le paramètre **vsysreader (vsysreader)** ne n'a pas accès aux fonctions du pare-feu et du réseau (comme le routage statique ou

© 2020 Palo Alto Networks, Inc.

Paramètres du rôle administrateur	
	dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP ou les profils de réseaux).

© 2020 Palo Alto Networks, Inc.

Périphérique > Domaine d'accès

- Périphérique > Domaine d'accès

Configurez les domaines d'accès pour restreindre l'accès administrateur aux systèmes virtuels spécifiques sur le pare-feu. Le pare-feu prend uniquement en charge les domaines d'accès si vous utilisez un serveur RADIUS, TACACS+ ou SAML (IDP) pour gérer l'authentification et l'autorisation de l'administrateur. Pour activer les domaines d'accès, vous devez définir :

- Un profil de serveur pour le serveur d'authentification externe – Voir Périphérique > Profils de serveur > RADIUS, Périphérique > Profils de serveur > TACACS+ et Périphérique > Profils de serveur > Fournisseur d'identité SAML.
- Les attributs spécifiques aux fournisseurs (VSA) RADIUS, les VSA TACACS+, ou les attributs SAML.

Lorsqu'un administrateur tente de se connecter au pare-feu, ce dernier interroge le serveur externe pour connaître le domaine d'accès de l'administrateur. Le serveur externe renvoie le domaine associé et le pare-feu restreint alors l'administrateur aux systèmes virtuels que vous avez spécifiés dans le domaine d'accès. Si le pare-feu n'utilise pas un serveur externe pour authentifier et autoriser les administrateurs, les paramètres **Device (Périphérique)** > **Access Domain (Domaine d'accès)** sont ignorés.

Sur Panorama, vous pouvez gérer les domaines d'accès localement ou en utilisant les VSA RADIUS, les VSA TACACS+ ou les attributs SAML (voir Panorama > Domaines d'accès*).*

Paramètres du domaine d'accès	Description
Name (Nom)	Donnez un nom au domaine d'accès (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union, traits de soulignement et points.
Systèmes virtuels	Sélectionnez des systèmes virtuels dans la colonne Disponible et cliquez sur **Add (Ajouter)** pour les ajouter. Les domaines d'accès ne sont pris en charge que sur les pare-feu prenant en charge des systèmes virtuels.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profil d'authentification

Utilisez cette page pour configurer les paramètres d'authentification des administrateurs et des utilisateurs finaux. Les pare-feu et Panorama prennent en charge les services d'authentification locaux, RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0 et multifacteur (MFA).

Créez au moins un profil pour fournir l'authentification externe, qui permet de conserver toutes les demandes d'authentification en un seul endroit, ce qui facilite la gestion, et utilise un processus d'authentification standard qui comprend des services comme le suivi. Il est recommandé de créer et de prioritiser (Device (Périphérique) > Authentication Sequence (Séquence d'authentification)) plusieurs profils d'authentification à l'aide de méthodes diverses pour faire face aux échecs d'authentification et de créer au moins un compte de connexion auquel revenir si toutes les méthodes externes échouent.

Vous pouvez également utiliser cette page pour enregistrer un pare-feu ou un service Panorama (tel qu'un accès administratif à l'interface Web) avec un fournisseur d'identité SAML (IDP). L'enregistrement du service permet au pare-feu ou à Panorama d'utiliser l'IDP pour authentifier les utilisateurs qui demandent le service. Vous enregistrez un service en saisissant ses métadonnées SAML sur l'IDP. Le pare-feu et Panorama facilitent l'enregistrement en générant automatiquement un fichier de métadonnées SAML en fonction du profil d'authentification que vous avez attribué au service. Vous pouvez d'ailleurs exporter ce fichier de métadonnées vers l'IDP.

- Profil d'authentification
- Exportation des métadonnées SAML à partir d'un Profil d'authentification

Profil d'authentification

- Périphérique > Profil d'authentification

Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** ou **Panorama** > **Authentication Profile (Profil d'authentification)** pour gérer les profils d'authentification. Pour créer un nouveau profil, vous devez en **Ajouter** un et remplir les champs suivants.

Après la configuration d'un profil d'authentification, utilisez la commande de la CLI ***`test authentication`*** *d'authentification test pour déterminer si le pare-feu ou le serveur de gestion Panorama peut communiquer avec le serveur d'authentification dorsal et si la demande d'authentification est fructueuse. Vous pouvez effectuer des tests d'authentification sur la configuration candidate pour déterminer si la configuration est correcte avant de la valider.*

Paramètres de profil d'authentification	Description
Name (Nom)	Saisissez un nom pour identifier le profil. Celui-ci est sensible à la casse, peut comporter 31 caractères maximum, et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, traits de soulignement et des points. Le nom doit être unique au **Location (Emplacement)** actuel (pare-feu ou système virtuel) par rapport aux autres profils d'authentification et séquences d'authentification. *Dans un pare-feu en mode plusieurs systèmes virtuels, si le Location (Emplacement) du profil d'authentification est un système virtuel, ne saisissez pas le même nom qu'une séquence d'authentification dans l'emplacement Partagé. De*

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
	même, si le profil Location (Emplacement) est Partagé, ne saisissez pas le même nom qu'une séquence dans un système virtuel. Même si vous pouvez valider un profil et une séquence d'authentification avec les mêmes noms dans ces cas de figure, des erreurs de référence sont possibles.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Onglet Authentification Le pare-feu appelle le service d'authentification que vous configurez dans cet onglet avant de faire appel aux services d'authentification multifacteur (MFA) que vous ajoutez dans l'Onglet Facteurs. *Si le pare-feu s'intègre avec un fournisseur MFA par l'intermédiaire de RADIUS au lieu de l'API fournisseur, vous devez configurer un profil de serveur RADIUS pour ce fournisseur et non un profil de serveur MFA.*	
Type	Sélectionnez le type de service qui fournit la première (et éventuellement la seule) demande d'authentification que les utilisateurs voient. En fonction de votre sélection, la boîte de dialogue affiche d'autres paramètres que vous définissez pour le service. Les options à votre disposition sont les suivantes : • **None (Aucun)** – N'utilisez aucune authentification. • **Local Database (Base de données locale)** – Utilisez la base de données d'authentification sur le pare-feu. Cette option n'est pas disponible sur Panorama. • **RADIUS** – Utilisez un serveur Remote Authentication Dial-in User Service (RADIUS). • **TACACS+** – Utilisez un serveur Terminal Access Controller Access-Control System Plus (TACACS+). • **LDAP** – Utilisez un serveur Lightweight Directory Access Protocol (LDAP). • **Kerberos** – Utilisez un serveur Kerberos. • **SAML** – Utilisez un fournisseur d'identité Security Assertion Markup Language 2.0 (SAML 2.0) (IDP). *Les administrateurs peuvent utiliser SAML pour s'authentifier sur le pare-feu ou l'interface Web Panorama, mais pas sur le CLI.*
Profil de serveur (RADIUS, TACACS+, LDAP ou Kerberos uniquement)	Sélectionnez le profil de serveur d'authentification dans la liste déroulante. Reportez-vous à la section Périphérique > Profils de serveur > RADIUS, Périphérique > Profils de serveur > TACACS+, Périphérique > Profils de serveur > LDAP ou Périphérique > Profils de serveur > Kerberos.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
Profil du serveur IDP (SAML uniquement)	Sélectionnez le profil de serveur du fournisseur d'identité SAML dans la liste déroulante. Reportez-vous à la section Périphérique > Profils de serveur > Fournisseur d'identité SAML.
Récupérer le groupe d'utilisateurs auprès de RADIUS (RADIUS uniquement)	Sélectionnez cette option pour collecter des informations sur les groupes d'utilisateurs à partir des Attributs spécifiques aux fournisseurs (VSA) définis sur le serveur RADIUS. Le pare-feu utilise les informations pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations, pas pour appliquer les politiques ou générer des rapports.
Récupérer le groupe d'utilisateurs auprès de TACACS+ (TACACS+ uniquement)	Sélectionnez cette option pour collecter des informations sur les groupes d'utilisateurs à partir des Attributs spécifiques aux fournisseurs (VSA) définis sur le serveur TACACS+. Le pare-feu utilise les informations pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations, pas pour appliquer les politiques ou générer des rapports.
Attributs connexion (LDAP uniquement)	Saisissez un attribut d'annuaire LDAP qui identifie de manière unique l'utilisateur et qui sert d'identifiant de connexion pour cet utilisateur.
Avertissement pour l'expiration du mot de passe (LDAP uniquement)	Si le profil d'authentification s'applique aux utilisateurs GlobalProtect, saisissez le nombre de jours avant expiration du mot de passe pour démarrer l'affichage de messages de notification aux utilisateurs afin de les avertir que leurs mots de passe expirent dans x jours. Par défaut, les messages de notification s'affichent sept jours avant l'expiration du mot de passe (plage de 1 à 255). Les utilisateurs ne pourront pas accéder au VPN si leur mot de passe expire. *Envisagez l'option de configurer les agents GlobalProtect de manière à utiliser la méthode de pré-ouverture de session. Cela permettra aux utilisateurs de se connecter au domaine pour changer leur mot de passe même après expiration du mot de passe.* Si les utilisateurs autorisent l'expiration de leur mot de passe, l'administrateur peut affecter un mot de passe LDAP temporaire afin de permettre aux utilisateurs de se connecter au VPN. Dans ce flux de travail, nous recommandons de définir le **Authentication Modifier (modificateur d'authentification)** dans la configuration du portail sur **Cookie authentication for config refresh (Authentification par cookie pour actualiser la configuration)** (sinon, le mot de passe temporaire sera utilisé pour l'authentification sur le portail, mais la connexion à la passerelle échouera, empêchant l'accès au VPN).
Certificat de signature des demandes (SAML uniquement)	Sélectionnez le certificat que le pare-feu utilisera pour signer les messages SAML qu'il envoie au fournisseur d'identité (IDP). Ce champ est requis si vous activez l'option **Sign SAML Message to IdP (Signer le message SAML vers IDP)** dans le **IdP Server Profile (Profil de serveur IDP)** (voir Périphérique > Profils de serveur > Fournisseur d'identité SAML). Sinon, sélectionner un certificat pour signer des messages SAML est facultatif.

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
	Lors de la génération ou de l'importation d'un certificat et de sa clé privée associée, les attributs d'utilisation des clés spécifiés dans le certificat contrôlent la manière dont vous pouvez utiliser la clé : • Si le certificat énumère explicitement les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur le pare-feu. Dans ce cas, vous devez Importer le certificat et la clé à partir de l'autorité de certification (CA) de votre entreprise ou d'une autorité de certification tierce. • Si le certificat ne spécifie pas les attributs d'utilisation des clés, vous pouvez utiliser la clé à toutes fins utiles, y compris la signature de messages. Dans ce cas, vous pouvez utiliser n'importe quelle méthode pour obtenir le certificat et la clé pour signer des messages SAML. *Palo Alto Networks recommande d'utiliser un certificat de signature pour assurer l'intégrité des messages SAML envoyés à IDP.*
Activer la déconnexion unique (SAML uniquement)	Sélectionnez cette option pour permettre aux utilisateurs de vous déconnecter de tous les services authentifiés en vous déconnectant de n'importe quel service unique. La fermeture de session unique (SLO) s'applique uniquement aux services auxquels les utilisateurs ont accès via l'authentification SAML. Les services peuvent être externes ou internes à votre organisation (par exemple, l'interface Web du pare-feu). Cette option ne s'applique que si vous avez saisi une **Identity Provider SLO URL (URL de fermeture de session unique du fournisseur d'identité)** dans le Profil du serveur IDP. Vous ne pouvez pas activer la SLO pour les utilisateurs du Portail captif. *Après la fermeture de session des utilisateurs, le pare-feu supprime automatiquement leurs* mappages d'adresse IP / nom d'utilisateur.
Profil du certificat (SAML uniquement)	Sélectionnez le Profil de certificat que le pare-feu utilise pour valider : • L'**Identity Provider Certificate (Certificat du fournisseur d'identité)** spécifié dans le Profil de serveur IDP. L'IDP utilise ce certificat pour s'authentifier sur le pare-feu. Le pare-feu valide le certificat lorsque vous effectuez l'action visant à **Valider** la configuration du profil d'authentification. • Les messages SAML que l'IDP envoie au pare-feu pour l'authentification d'ouverture de session unique (SSO) et l'authentification de fermeture de session unique (SLO). L'IDP utilise l'**Identity Provider Certificate (Certificat du fournisseur d'identité)** spécifié dans le Profil de serveur IDP pour signer les messages. Voir Périphérique > Gestion des certificats > Profil de certificat.
Domaine d'utilisateur ET Modificateur du nom d'utilisateur	Le pare-feu utilise le **User Domain (Domaine utilisateur)** pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations et pour le mappage de groupe User-ID. Vous pouvez indiquer un **Username Modifier (Modificateur du nom d'utilisateur)** pour modifier la chaîne domaine / nom d'utilisateur qu'un

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
(Tous les types d'authentification à l'exception de SAML)	utilisateur saisit lors de la connexion. Le pare-feu utilise la chaîne modifiée pour l'authentification. Choisissez l'une des options suivantes : • Pour envoyer uniquement l'entrée non modifiée de l'utilisateur, laissez le **User Domain (Domaine utilisateur)** vide (par défaut) et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** à la variable **%USERINPUT%** (par défaut). • Pour ajouter un domaine à la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERDOMAIN%\%USERINPUT%**. • Pour ajouter un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERINPUT%@%USERDOMAIN% (%SAISIEUTILISATEUR%@%DOMAINEUTILISATEUR%)**. *Si Username Modifier (Modificateur du nom d'utilisateur) inclut la variable %USERDOMAIN%, la valeur User Domain (Domaine utilisateur) remplace toute chaîne de domaine saisie par l'utilisateur. Si vous précisez la valeur %USERDOMAIN% et que vous ne renseignez pas User Domain (Domaine utilisateur), le pare-feu supprime toute chaîne de domaine saisie par l'utilisateur. Le pare-feu résout les noms de domaine en nom NetBIOS approprié pour le mappage de groupe User-ID. Ceci s'applique aux domaines parent et enfant. Les modificateurs de User Domain (Domaine utilisateur) sont prioritaires sur les noms NetBIOS dérivés automatiquement.* • Pour permettre au pare-feu d'utiliser le type de profil de serveur pour déterminer comment et à quel moment dans la séquence d'authentification modifier le format de la saisie utilisateur, saisissez manuellement **`None (Aucune)`** en tant que **Username Modifier (Modificateur du nom d'utilisateur)**. Pour obtenir plus d'informations sur cette option, reportez-vous à la section Configure an Authentication Profile and Sequence (Configurer un profil et une séquence d'authentification) dans le Guide de l'administrateur PAN-OS.
Partition Kerberos (Tous les types d'authentification à l'exception de SAML)	Si votre réseau prend en charge l'ouverture de session unique (SSO) Kerberos, saisissez la **Kerberos Realm (Partition Kerberos)** (127 caractères maximum). Il s'agit de la partie du nom d'hôte dans le nom de connexion utilisateur. Par exemple, le nom de compte utilisateur utilisateur@EXEMPLE.LOCAL comporte la partition EXEMPLE.LOCAL.
Keytab Kerberos (Tous les types d'authentification à l'exception de SAML)	Si votre réseau prend en charge l'ouverture de session unique Kerberos (SSO), cliquez sur **Import (Importer)**, puis sur **Browse (Parcourir)** pour localiser le fichier de keytab, puis cliquez sur **OK**. Un keytab contient les informations de compte Kerberos (nom principal et mot de passe haché) du pare-feu, qui sont nécessaires pour l'authentification SSO. Chaque profil d'authentification peut comporter un keytab. Pendant l'authentification, le pare-feu tente tout d'abord d'utiliser le keytab pour établir une SSO. S'il réussit et que l'utilisateur tentant l'accès figure dans la Liste d'autorisations, l'authentification réussit immédiatement. Sinon, le processus d'authentification

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
	revient à l'authentification manuelle (nom d'utilisateur / mot de passe) du **Type** spécifié, qui ne doit pas nécessairement être Kerberos. *Si le pare-feu est en mode FIPS/CC, l'algorithme doit être aes128-cts-hmac-sha1-96 ou aes256-cts-hmac-sha1-96. Sinon, vous pouvez également utiliser des3-cbc-sha1 ou arcfour-hmac. Cependant, si l'algorithme contenu dans le keytab ne correspond pas à l'algorithme contenu dans le ticket de service généré par le Service d'émission de tickets pour que les clients puissent activer la SSO, le processus de SSO échoue. Le rôle de votre administrateur Kerberos est de déterminer les algorithmes utilisés par les tickets de service.*
Attribut du nom d'utilisateur (SAML uniquement)	Saisissez l'attribut SAML qui identifie le nom d'utilisateur d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **nom d'utilisateur**). Si le **IdP Server Profile (Profil de serveur IDP)** contient des métadonnées qui spécifient un attribut de nom d'utilisateur, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu correspond aux noms d'utilisateur récupérés à partir des messages SAML avec les utilisateurs et les groupes d'utilisateurs dans **Allow List (Liste d'autorisations)** du profil d'authentification. Puisque vous ne pouvez pas configurer le pare-feu pour modifier la chaîne domaine / nom d'utilisateur qu'un utilisateur saisit pendant les connexions SAML, le nom d'utilisateur de connexion doit correspondre exactement à une entrée de **Allow List (Liste d'autorisations)**. C'est le seul attribut SAML qui est obligatoire. *Les messages SAML peuvent afficher le nom d'utilisateur dans le champ objet. Le pare-feu vérifie automatiquement le champ objet si l'attribut du nom d'utilisateur n'affiche pas le nom d'utilisateur.*
Attribut du groupe d'utilisateurs (SAML uniquement)	Saisissez l'attribut SAML qui identifie le groupe d'utilisateurs d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **groupe d'utilisateurs**). Si le **IdP Server Profile (Profil de serveur IDP)** contient des métadonnées qui spécifient un attribut de groupe d'utilisateurs, le champ utilise automatiquement cet attribut. Le pare-feu utilise les informations de groupe pour faire correspondre les utilisateurs s'authentifiant aux entrées de **Allow List (Liste d'autorisations)** et non aux politiques ou aux rapports.
Attribut du rôle admin (SAML uniquement)	Saisissez l'attribut SAML qui identifie le rôle administrateur d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **rôle administrateur**). Cet attribut s'applique uniquement aux administrateurs de pare-feu et non aux utilisateurs finaux. Si le **IdP Server Profile (Profil de serveur IDP)** contient des métadonnées qui spécifient un attribut de rôle administrateur, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu correspond à ses rôles (dynamiques) prédéfinis ou à des profils des profils de Rôle administrateur avec les rôles extraits des messages SAML pour renforcer le contrôle d'accès basé sur les rôles. Si un message SAML a plusieurs valeurs de rôle administrateur pour un administrateur avec un seul rôle, la mise en correspondance s'applique uniquement à la première valeur (la plus à gauche) dans l'attribut du rôle

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
	administrateur. Pour un administrateur avec plus d'un rôle, la mise en correspondance peut s'appliquer à plusieurs valeurs dans l'attribut.
Attribut du domaine d'accès (SAML uniquement)	Saisissez l'attribut SAML qui identifie le domaine d'accès d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **access-domain (domaine d'accès)**). Cet attribut s'applique uniquement aux administrateurs de pare-feu et non aux utilisateurs finaux. Si le **IdP Server Profile (Profil de serveur IDP)** contient des métadonnées qui spécifient un attribut de domaine d'accès, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu fait correspondre ses domaines d'accès configurés localement avec ceux récupérés à partir des messages SAML pour appliquer le contrôle d'accès. Si un message SAML a plusieurs valeurs du domaine d'accès pour un administrateur avec un seul domaine d'accès, la mise en correspondance s'applique uniquement à la première valeur (la plus à gauche) dans l'attribut du domaine d'accès. Pour un administrateur avec plus d'un domaine d'accès, la mise en correspondance peut s'appliquer à plusieurs valeurs dans l'attribut.
Onglet Facteurs	
Activer les facteurs d'authentification supplémentaires	Sélectionnez cette option si vous souhaitez que le pare-feu appelle des facteurs d'authentification supplémentaires (demandes) après la réponse fructueuse des utilisateurs au premier facteur (spécifié dans le champ **Type** dans l'onglet **Authentification**). *Des facteurs d'authentification supplémentaires sont pris en charge pour l'authentification des utilisateurs finaux via la Politique d'authentification uniquement. Des facteurs supplémentaires ne sont pas pris en charge pour l'authentification des utilisateurs distants aux portails et passerelles GlobalProtect ou pour l'authentification des administrateurs à l'interface Web de Panorama ou PAN-OS. Bien que vous puissiez configurer des facteurs supplémentaires, ceux-ci ne seront pas appliqués dans le cadre de ces cas pratiques. Vous pouvez toutefois procéder à l'intégration aux fournisseurs MFA au moyen de RADIUS ou de SAML pour tous les cas pratiques d'authentification.* Après avoir configuré un profil d'authentification utilisant une authentification multifacteur (MFA), vous devez l'affecter à un objet d'application d'authentification (Objets > Authentification) et affecter l'objet aux règles de la politique d'Authentification (Politiques > Authentification) qui contrôlent l'accès à vos ressources réseau.
Facteurs	Ajoutez un profil de serveur MFA (Périphérique > Profils de serveur > Authentification multifacteur) pour chaque facteur d'authentification que le pare-feu appelle après que les utilisateurs répondent avec succès au premier facteur (spécifié dans le champ **Type** dans l'onglet **Authentification**). Le pare-feu appelle chaque facteur dans l'ordre du haut vers le bas dans lequel vous répertoriez les services MFA qui fournissent les facteurs. Pour changer l'ordre, sélectionnez un profil de serveur et **Déplacer en haut** ou **Déplacer en bas**. Vous pouvez indiquer jusqu'à trois facteurs supplémentaires. Chaque service MFA

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
	fournit un facteur. Certains services MFA permettent aux utilisateurs de choisir un facteur à partir d'une liste composée de plusieurs facteurs. Le pare-feu s'intègre avec ces services MFA au moyen des API des fournisseurs. Des intégrations des API des fournisseurs MFA sont ajoutées périodiquement via les mises à jour de contenu Applications ou Applications et menaces.
Onglet Avancé	
Liste d'autorisations	Cliquez sur **Add (Ajouter)** et sélectionnez **all (tous)** ou sélectionnez les utilisateurs et groupes spécifiques autorisés à s'authentifier avec ce profil. Lorsqu'un utilisateur s'authentifie, le pare-feu fait correspondre le nom d'utilisateur ou le groupe associé aux entrées de cette liste. Si vous n'ajoutez pas d'entrées, aucun utilisateur ne peut s'authentifier. *Pour restreindre l'authentification uniquement aux utilisateurs qui ont besoin d'un accès pour des raisons professionnelles légitimes et pour réduire la surface d'attaque, précisez des utilisateurs ou des groupes d'utilisateurs et évitez d'utiliser l'option all (tous).* *Si vous avez saisi une valeur User Domain (Domaine utilisateur), vous ne devez pas nécessairement préciser de domaines dans Allow List (Liste d'autorisation). Par exemple, si le ser Domain (Domaine utilisateur) est **businessinc** et que vous souhaitez ajouter l'utilisateur **admin1** à Allow List (Liste d'autorisations), la saisie de `admin1` a le même effet que la saisie de `businessinc\admin1`. Vous pouvez préciser des groupes existant déjà dans votre service d'annuaires ou préciser des groupes personnalisés sur la base de filtres LDAP.*
Tentatives échouées (Tous les types d'authentification à l'exception de SAML)	Saisissez le nombre d'échecs de tentatives de connexion successives (0 à 10) autorisés par le pare-feu avant de verrouiller le compte utilisateur. Une valeur de 0 indique un nombre illimité de tentatives de connexion. La valeur par défaut est de 0 pour les pare-feu en mode opérationnel normal et de 10 pour les pare-feu enmode FIPS-CC. *Définissez le nombre de Failed Attempts (Tentatives échouées) sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d'attaque par force pour se connecter au pare-feu.* *Si vous définissez les Failed Attempts (Tentatives échouées) sur une valeur autre que 0 mais que vous conservez la valeur DLockout Time (Durée de verrouillage) de 0, les Failed Attempts (Tentatives échouées) sont ignorées et l'utilisateur n'est jamais verrouillé.*
Durée de verrouillage	Saisissez le nombre de minutes (plage comprise entre 0 et 60 ; par défaut 0) pendant lesquelles le pare-feu verrouille un compte utilisateur après que l'utilisateur a atteint le nombre de **Failed Attempts (Tentatives échouées)**. Une

© 2020 Palo Alto Networks, Inc.

Paramètres de profil d'authentification	Description
(Tous les types d'authentification à l'exception de SAML)	valeur de 0 signifie que le verrouillage s'applique jusqu'à ce qu'un administrateur déverrouille manuellement le compte utilisateur. *Définissez la Lockout Time (Durée de verrouillage) sur au moins 30 minutes pour empêcher les tentatives de connexion continues d'un acteur malveillant.* *Si vous définissez Lockout Time (Durée de verrouillage) sur une valeur autre que 0 mais que vous conservez la valeur Failed Attempts (Tentatives échouées) de 0, Lockout Time (Durée de verrouillage) est ignorée et l'utilisateur n'est jamais verrouillé.*

Exportation des métadonnées SAML à partir d'un Profil d'authentification

- Périphérique > Profil d'authentification

Le pare-feu et Panorama peuvent utiliser un fournisseur d'identité SAML (IDP) pour authentifier les utilisateurs qui demandent des services. Pour les administrateurs, le service est accessible depuis l'interface Web. Pour les utilisateurs finaux, le service peut être Portail captif ou GlobalProtect, ce qui permet d'accéder aux ressources de votre réseau. Pour activer l'authentification SAML pour un service, vous devez enregistrer ce service en saisissant des informations spécifiques le concernant sur l'IDP, sous la forme de métadonnées SAML. Le pare-feu et Panorama simplifient l'enregistrement en générant automatiquement un fichier de métadonnées SAML en fonction du profil d'authentification que vous avez attribué au service, et vous pouvez exporter ce fichier de métadonnées vers l'IDP. L'exportation des métadonnées est une alternative plus simple à la saisie des valeurs pour chaque champ de métadonnées dans l'IDP.

Certaines des métadonnées du fichier exporté proviennent du profil de serveur SAML IDP affecté au profil d'authentification (Périphérique > Profils de serveur> Fournisseur d'identité SAML). Toutefois, le fichier exporté spécifie toujours POST comme méthode de liaison HTTP, quelle que soit la méthode spécifiée dans le profil de serveur SAML IDP. IDP utilisera la méthode POST pour transmettre des messages SAML au pare-feu ou à Panorama.

Pour exporter des métadonnées SAML à partir d'un profil d'authentification, cliquez sur les **Metadata (Métadonnées)** SAML dans la colonne Authentification et complétez les champs suivants. Pour importer le fichier de métadonnées dans un IDP, reportez-vous à votre documentation IDP.

Paramètres d'exportation de métadonnées SAML	Description
Commandes	Sélectionnez le service pour lequel vous voulez exporter les métadonnées SAML. • **management (gestion)** (par défaut) – Fournit un accès administrateur à l'interface Web. • **captive-portal (portail captif)** – Fournit à l'utilisateur final un accès aux ressources du réseau via le Portail captif.

© 2020 Palo Alto Networks, Inc.

Paramètres d'exportation de métadonnées SAML	Description
	• **global-protect (protection globale)** – Fournit à l'utilisateur final un accès aux ressources du réseau via GlobalProtect. Votre sélection détermine les autres champs affichés par la boîte de dialogue.
[Gestion | Portail captif | GlobalProtect] Profil d'authentification	Saisissez le nom du profil d'authentification à partir duquel vous exportez des métadonnées. La valeur par défaut représente le profil à partir duquel vous avez ouvert la boîte de dialogue en cliquant sur le lien **Metadata (Métadonnées)**.
Choix de gestion (Gestion uniquement)	Sélectionnez une option pour spécifier une interface activée pour le trafic de gestion (comme l'interface MGT) : • **Interface** – Sélectionnez l'interface à partir de la liste des interfaces du pare-feu. • **IP Hostname (Nom d'hôte IP)** – Saisissez l'adresse IP ou le nom d'hôte de l'interface. Si vous saisissez un nom d'hôte, le serveur DNS doit avoir un enregistrement d'adresse (A) qui correspond à l'adresse IP.
[Portail captif | GlobalProtect] Système virtuel (Portail captif ou GlobalProtect uniquement)	Sélectionne le système virtuel pour lequel les paramètres du Portail captif ou du portail GlobalProtect sont définis.
Nom d'hôte IP (Portail captif ou GlobalProtect uniquement)	Saisissez l'adresse IP ou le nom d'hôte du service. • **Portail captif** – Saisissez l'adresse IP ou le nom d'hôte pour **Redirect Host (Rediriger l'hôte)** (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Captive Portal Settings (Paramètres du Portail captif)**). • **GlobalProtect** – Saisissez le **Hostname (nom d'hôte)** ou l'**IP Address (adresse IP)** du portail GlobalProtect. Si vous saisissez un nom d'hôte, le serveur DNS doit avoir un enregistrement d'adresse (A) qui correspond à l'adresse IP.

© 2020 Palo Alto Networks, Inc.

Périphérique > Séquence d'authentification

- Périphérique > Séquence d'authentification
- Panorama > Séquence d'authentification

Dans certains environnements, les comptes utilisateur se trouvent dans plusieurs répertoires (par exemple LDAP et RADIUS). Une séquence d'authentification est un ensemble de profils d'authentification que le pare-feu tente d'utiliser pour authentifier des utilisateurs lorsqu'ils se connectent. Le pare-feu essaie les profils de manière séquentielle en partant du haut de la liste vers le bas, en appliquant les valeurs d'authentification, de SSO Kerberos, de liste d'autorisation et de verrouillage de compte pour chacun d'entre eux jusqu'à ce qu'un profil authentifie avec succès l'utilisateur. Le pare-feu ne refuse l'accès que si l'authentification de tous les profils de la séquence échoue. Pour plus d'informations sur les profils d'authentification, voir Périphérique > Profil d'authentification.

Configurez une séquence d'authentification détenant plusieurs profils d'authentification qui utilisent des méthodes d'authentification différentes. Configurez au moins deux méthodes d'authentification externes et une méthode d'authentification locale (interne), pour que les problèmes de connectivité n'empêchent pas l'authentification. Faites du profil d'authentification locale le dernier profil de la séquence, pour qu'il ne soit utilisé que si toutes les méthodes d'authentification externes échouent. (L'authentification externe fournit des services d'authentification dédiés, fiables et centralisés, y compris des fonctions de journalisation et de dépannage.)

Paramètres de séquence d'authentification	Description
Name (Nom)	Saisissez un nom pour identifier la séquence. Celui-ci est sensible à la casse, peut comporter 31 caractères maximum, et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, traits de soulignement et des points. Le nom doit être unique au **Location (Emplacement)** actuel (pare-feu ou système virtuel) par rapport aux autres séquences d'authentification et profils d'authentification. *Si un pare-feu comporte plusieurs systèmes virtuels (mode multi-vsys), si le Location (Emplacement) de la séquence d'authentification est un système virtuel (vsys), ne saisissez pas le même nom de profil d'authentification dans l'emplacement Partagé. De même, si la séquence Location (Emplacement) est Shared (Partagée), ne saisissez pas le même nom qu'un profil dans un système virtuel. Même si vous pouvez valider une séquence et un profil d'authentification avec les mêmes noms dans ces cas de figure, des erreurs de référence sont possibles.*
Location (Emplacement)	Sélectionnez la portée dans laquelle la séquence est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré la séquence, vous ne pouvez plus changer son **Location (Emplacement)**.

© 2020 Palo Alto Networks, Inc.

Paramètres de séquence d'authentification	Description
Utiliser le domaine pour déterminer le profil d'authentification	Sélectionnez cette option (cochée par défaut) si vous souhaitez que le pare-feu mette en correspondance le nom de domaine saisi par un utilisateur lors de la connexion avec le **User Domain (Domaine utilisateur)** ou la **Kerberos Realm (Partition Kerberos)** d'un profil d'authentification associé à la séquence, puis utilise ce profil pour authentifier l'utilisateur. La saisie utilisateur utilisée par le pare-feu pour la mise en correspondance peut être le texte situé avant le nom d'utilisateur (avec le séparateur barre oblique inverse) ou le texte situé après le nom d'utilisateur (avec le séparateur @). Si le pare-feu ne trouve pas de correspondance, il essaie les profils d'authentification de la séquence dans l'ordre du haut vers le bas.
Profiles d'authentification	Cliquez sur **Add (Ajouter)** et choisissez dans la liste déroulante pour chaque profil d'authentification que vous souhaitez ajouter à la séquence. Pour changer l'ordre de la liste, sélectionnez un profil, puis cliquez sur **Move Up (Déplacer en haut)** ou sur **Move Down (Déplacer en bas)**. Pour supprimer un profil, sélectionnez-le, puis cliquez sur **Delete (Supprimer)**. *Vous ne pouvez pas ajouter un profil d'authentification qui spécifie un profil de serveur d'authentification multifacteur (MFA) ou un profil de serveur de fournisseur d'identité de langage de balisage d'assertion de sécurité (SAML).*

© 2020 Palo Alto Networks, Inc.

Périphérique > Sources d'informations de machine virtuelle

Cet onglet suit de façon proactive les modifications sur les machines virtuelles installées sur l'une de ces sources : serveur VMware ESXi, serveur VMware vCenter, Amazon Web Services, Virtual Private Cloud (AWS-VPC) ou Google Compute Engine (GCE).

Lors de la surveillance des serveurs ESXi qui font partie de la solution VM-Series édition NSX, utilisez des Groupes d'adresses dynamiques plutôt que d'utiliser des Sources d'informations de machine virtuelle pour en apprendre davantage sur les changements dans l'environnement virtuel. Pour la solution VM-Series édition NSX, le Gestionnaire NSX fournit à Panorama des informations sur le groupe de sécurité NSX auquel appartient une adresse IP. Les informations du Gestionnaire NSX fournit le contexte global permettant la définition des critères de correspondance dans un Groupe d'adresses dynamiques, car il utilise l'ID du profil de service en tant qu'attribut distinctif et vous permet de mettre en œuvre correctement la politique lorsque vous avez des adresses IP qui se chevauchent entre les différents groupes de sécurité NSX.

Vous pouvez enregistrer jusqu'à 32 étiquettes pour une adresse IP.

Vous pouvez surveiller les sources d'informations de deux manières différentes'A0;:

- Le pare-feu peut surveiller votre serveur VMware ESXi, le serveur VMware vCenter, les instances GCE ou les VPC, et récupérer les modifications apportées aux invités configurés sur les sources surveillées. Pour chaque pare-feu ou pour chaque système virtuel sur un pare-feu dont la configuration prévoit des systèmes virtuels multiples, vous pouvez configurer jusqu'à 10 sources.

  Les conditions suivantes s'appliquent lorsque vos pare-feu sont configurés dans une configuration High Availability (Haute disponibilité ; HA).

  - **Configuration HA active/passive** : seul le pare-feu actif surveille les sources d'informations de machine virtuelle.
  - **Configuration HA active/active** : seul le pare-feu possédant la valeur de priorité `primary` surveille les sources d'informations de machine virtuelle.

  Pour savoir comment les sources d'informations de machine virtuelle et les groupes d'adresses dynamiques fonctionnent de manière synchrone et vous permettent de surveiller les modifications dans l'environnement virtuel, reportez-vous au Guide de déploiement VM-Series.
- Pour le mappage des adresses IP aux noms d'utilisateurs, vous pouvez configurer les sources d'informations de machine virtuelle sur l'agent User-ID Windows ou sur le pare-feu pour surveiller les serveurs VMware ESXi et vCenter, et récupérer les modifications des invités configurés sur le serveur. L'agent User-ID Windows prend en charge un maximum de 100 sources. La prise en charge de AWS et de Google Compute Engine n'est pas disponible pour l'agent User-ID.

  VMware'A0;Tools doit être installé et exécuté sur chaque machine virtuelle se trouvant sur un serveur'A0;ESXi ou vCenter surveillé. VMware Tools permet de les adresses IP et d'autres valeurs affectées à chaque machine virtuelle.

Pour collecter les valeurs affectées aux machines virtuelles surveillées, le pare-feu surveille les attributs énumérés dans les tableaux suivants.

© 2020 Palo Alto Networks, Inc.

Attributs surveillés sur une source'A0;VMware

- UUID
- Name (Nom)
- Système d'exploitation invité
- Annotation
- État de la machine virtuelle : l'état d'alimentation peut être `poweredOff` (Mis hors tension), `poweredOn` (Mis sous tension), `standBy` (En veille) ou `unknown` (Inconnu).
- Version
- Réseau : Nom du commutateur virtuel, Nom du groupe de ports et ID de VLAN
- Nom du conteneur : Nom vCenter, Nom de l'objet de centre de données, Nom du pool de ressources, Nom du cluster, Hôte et Adresse IP de l'hôte.

Attributs surveillés sur AWS-VPC

- Architecture
- Système d'exploitation invité
- ID d'image
- ID de l'instance
- État de l'instance
- Type d'instance
- Nom de la clé
- Emplacement : Location, Nom du groupe et Zone de disponibilité
- Nom DNS privé
- Nom DNS public
- ID de sous-réseau
- Étiquette (clé, valeur) ; jusqu'à 18 étiquettes prises en charge par instance
- ID VPC

Attributs surveillés pour Google Compute Engine (CGE)

- Nom d'hôte de la machine virtuelle
- Type de machine
- Numéro du projet
- Source (Type de système d'exploitation)
- Status (État)
- Sous-réseau
- Réseau VPC
- Employé

Add (Ajouter) : cliquez sur **Add (Ajouter)** pour ajouter une nouvelle source pour la surveillance des machines virtuelles, puis renseignez les informations en fonction de la source que vous surveillez :

- Pour les serveurs VMware ESXi ou vCenter, reportez-vous aux Paramètres pour activer les sources d'informations de machine virtuelle pour les serveurs VMware ESXi et vCenter.
- Pour AWS-VPC, reportez-vous aux Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC.

© 2020 Palo Alto Networks, Inc.

- Pour Google Compute Engine (GCE), reportez-vous à la section Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine.

Refresh Connected (Actualiser les éléments connectés) : actualise l'état de la connexion qui s'affiche à l'écran ; cette option n'actualise pas la connexion entre le pare-feu et les sources surveillées.

Delete (Supprimer) : supprime la source d'informations de machine virtuelle que vous sélectionnez.

PDF/CSV : exporte le tableau de configuration des sources d'informations de machine virtuelle au format PDF ou dans un fichier Comma-Separated Values (valeur séparée par une virgule ; CSV). Reportez-vous à la section Exportation du tableau de configuration.

Paramètres pour activer les sources d'informations de machine virtuelle pour les Serveurs VMware ESXi et vCenter

Le tableau suivant décrit les paramètres que vous pouvez configurer pour activer les sources d'informations de machine virtuelle pour les serveurs VMware ESXi et vCenter.

Pour récupérer les étiquettes des machines virtuelles, le pare-feu exige un compte avec accès en lecture seule sur les serveurs VMware ESXi et vCenter.

Paramètres pour activer les sources d'informations de machine virtuelle pour VMware ESXi ou les serveurs vCenter	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Type	Indiquez si l'hôte/la source surveillé(e) est un **ESXi server (Serveur ESXi)** ou un **vCenter server (Serveur vCenter)**.
Description	(Facultatif) Ajoutez une étiquette permettant d'identifier l'emplacement ou la fonction de la source.
Port	Indiquez le port d'écoute de l'hôte/la source (port par défaut : 443).
Activé	Par défaut, la communication entre le pare-feu et la source configurée est activée. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit'A0;: • Connecté • Déconnecté • En attente ; l'état de la connexion s'affiche également en jaune lorsque la source surveillée est désactivée. Désélectionnez l'option **Enabled (Activé)** pour désactiver la communication entre l'hôte et le pare-feu.
délai d'expiration	Saisissez l'intervalle en heures après lequel la connexion à la source surveillée est fermée, si l'hôte ne répond pas (plage de 2 à 10 ; par défaut 2).

© 2020 Palo Alto Networks, Inc.

Paramètres pour activer les sources d'informations de machine virtuelle pour VMware ESXi ou les serveurs vCenter	
	(Facultatif) Pour modifier la valeur par défaut, vous devez **Activer le délai d'expiration lorsque la source est déconnectée** et indiquer une valeur. Lorsque la limite définie est atteinte, si l'hôte n'est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source.
Source	Saisissez le nom de domaine complet (FQDN) ou l'adresse'A0;IP de l'hôte/la source surveillé(e).
Username (Nom d'utilisateur)	Indiquez le nom d'utilisateur requis pour l'authentification auprès de la source.
Mot de passe	Saisissez et confirmez le mot de passe.
Intervalle de mise à jour	Indiquez l'intervalle (en secondes) auquel le pare-feu récupère les informations de la source (plage de 5 à 600 ; par défaut 5).

Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC

Le tableau suivant décrit le paramètre que vous configurez pour activer les sources d'informations de machine virtuelle pour un AWS VPC.

Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Type	Sélectionnez **AWS VPC**.
Description	(Facultatif) Ajoutez une étiquette permettant d'identifier l'emplacement ou la fonction de la source.
Activé	Par défaut, la communication entre le pare-feu et la source configurée est activée. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit'A0;: • Connecté • Déconnecté • En attente ; l'état de la connexion s'affiche également en jaune lorsque la source surveillée est désactivée. Désélectionnez l'option **Enabled (Activé)** pour désactiver la communication entre l'hôte et le pare-feu.
Source	Ajoutez l'URI dans lequel Virtual Private Cloud (VPC) réside. Par exemple, ec2.us-west-1.amazonaws.com

© 2020 Palo Alto Networks, Inc.

Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC	
	La syntaxe est ec2.<*your_AWS_region*>.amazonaws.com ; pour AWS China, la syntaxe est : ec2.<AWS_region>.amazonaws.com.cn
ID de clé d'accès	Saisissez la chaîne de texte alphanumérique qui identifie de manière unique l'utilisateur qui possède ou est autorisé à accéder au compte AWS. Ces informations font partie des informations d'identification de sécurité'A0;AWS. Le pare-feu nécessite les informations d'identification (l'ID de clé d'accès et la clé d'accès secrète) pour pouvoir signer numériquement les appels de l'API aux services AWS.
Clé d'accès secrète	Saisissez et confirmez le mot de passe.
Intervalle de mise à jour	Indiquez l'intervalle, en secondes, auquel le pare-feu récupère les informations de la source (plage de 60 à 1 200 ; par défaut 60).
délai d'expiration	Intervalle en heures après lequel la connexion à la source surveillée est fermée, si l'hôte ne répond pas (par défaut 2) (Facultatif) **Activer le délai d'expiration lorsque la source est déconnectée**. Lorsque la limite définie est atteinte, si la source n'est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source.
ID VPC	Saisissez l'ID du AWS-VPC à surveiller, par exemple, vpc-1a2b3c4d. Seules les instances'A0;EC2 déployées dans ce VPC sont surveillées. Si votre compte est configuré pour utiliser un VPC par défaut, l'ID du VPC par défaut est répertoriée sous Attributs du compte'A0;AWS.

Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine

Device (Périphérique) > VM Information Sources (Sources d'informations de machine virtuelle) > Add (Ajouter)

Le tableau suivant décrit les paramètres que vous devez configurer pour activer les sources d'informations de machine virtuelle pour les instances de Google Compute Engine sur Google Cloud Platform. Activez la surveillance des instances de Google Compute Engine (GCE) pour permettre au pare-feu (physique ou virtuel sur site, ou fonctionnant dans Google Cloud) de récupérer une balise, une étiquette ou toute autre métadonné sur les instances s'exécutant dans une zone particulière de Google Cloud du projet. Pour obtenir de plus amples renseignements sur l'utilisation du pare-feu VM-Series dans Google Cloud Platform, consultez le Guide de déploiement VM-Series.

Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Type	Sélectionnez **Google Compute Engine**.

© 2020 Palo Alto Networks, Inc.

Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine	
Description	(Facultatif) Ajoutez une étiquette permettant d'identifier l'emplacement ou la fonction de la source.
Activé	La communication entre le pare-feu et la source configurée est activée par défaut. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit'A0;: • - Connecté • - Déconnecté • - En attente ou la source surveillée est désactivée. Désélectionnez l'option **Enabled (Activé)** pour désactiver la communication entre la source configurée et le pare-feu. Lorsque vous désactivez la communication, toutes les adresses IP et les étiquettes enregistrées sont supprimées du groupe d'adresses dynamiques qui y est associé. C'est-à-dire que les règles de politique ne s'appliqueront pas aux instances GCE de ce projet Google Cloud.
Type d'authentification de service	Sélectionnez le pare-feu VM-Series qui fonctionne sur GCE ou sur un compte de service. • **VM-Series running on GCE (Pare-feu VM-Series fonctionnant sur GCE)** : sélectionnez cette option sur le pare-feu matériel ou VM-Series sur lequel vous activez la Surveillance VM n'est pas déployé dans Google Cloud Platform. • **Service Account (Compte de service)** : sélectionnez cette option si vous surveillez les instances de Google Cloud Engine sur un pare-feu qui n'est pas déployé dans Google Cloud Platform. Cette option vous permet d'utiliser un compte Google spéciale qui appartient à la machine virtuelle ou à l'application plutôt que d'utiliser un compte d'utilisateur final. Le compte de service doit disposer des politiques IAM (privilège **Compute Engine** > **Compute Viewer**) qui autorisent l'accès à l'API Google API et qui l'autorisent à interroger les machines virtuelles dans le projet Google Cloud Project afin d'obtenir les métadonnées des machines virtuelles.
Informations d'identification pour le compte de service	(Uniquement pour le compte de service) Téléchargez le fichier JSON qui contient les informations d'identification pour le compte de service. Ce fichier permet au pare-feu de s'authentifier auprès de l'instance et autorise l'accès aux métadonnées. Vous pouvez créer un compte sur la console Google Cloud (**IAM & admin (IAM & administrateur)** > **Service Accounts (Comptes de service)**). Reportez-vous à la documentation de Google pour obtenir des informations sur la création d'un compte, sur l'ajout d'une clé et sur le téléchargement du fichier JSON que vous devez charger sur le pare-feu.

© 2020 Palo Alto Networks, Inc.

Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine	
Numéro du projet	Entrez la chaîne de texte alphanumérique qui identifie de manière unique le projet Google Cloud que vous souhaitez surveiller.
Nom de la zone	Saisissez les informations sur la zone sous forme d'une chaîne contenant un maximum de 63 caractères de longueur. Par exemple : **`us-west1-a`**.
Intervalle de mise à jour	Indiquez l'intervalle (en secondes) auquel le pare-feu récupère les informations de la source (plage de 60 à 1 200 ; par défaut 60).
délai d'expiration	Intervalle (en heures) après lequel la connexion à la source surveillée est fermée si l'hôte ne répond pas (par défaut 2) (Facultatif) **Activer le délai d'expiration lorsque la source est déconnectée**. Lorsque la limite définie est atteinte, si la source n'est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source. Lorsque la source est déconnectée, toutes les étiquettes et adresses IP qui ont été enregistrées depuis ce projet sont supprimées du groupe d'adresses dynamiques.

© 2020 Palo Alto Networks, Inc.

Périphérique > Résolution des problèmes

- **Périphérique** > **Résolution des problèmes**
- **Panorama** > **Managed Devices (Périphériques gérés)** > **Troubleshooting (Résolution des problèmes)**

Avant de valider des changements de configuration apportés à un groupe de périphériques ou à un modèle, testez la fonctionnalité à partir de l'interface Web pour vérifier que les changements n'ont pas introduit de problèmes de connectivité dans la configuration active et que vos politiques autorisent ou refusent correctement le trafic.

- **Tests de correspondance de la politique**
  - Correspondance de la politique de sécurité
  - Correspondance de la politique QoS
  - Correspondance de la politique d'authentification
  - Correspondance politique SSL/déchiffrement
  - Correspondance de la politique NAT
  - Correspondance à la politique PBF (transfert basé sur une politique)
  - Correspondance de la politique DoS
- **Tests de connectivité**
  - Routage
  - Test WildFire
  - Archivage sécurisé des menaces
  - Ping
  - Trace Route
  - Connectivité du collecteur de journaux
  - Liste dynamique externe
  - Serveur de mises à jour
  - État du service de journalisation du cloud de test GP
  - État du service du cloud de test GP

Correspondance de la politique de sécurité

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.

© 2020 Palo Alto Networks, Inc.

Champ	Description
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Affichez toutes les règles de correspondance potentielles jusqu'à la première règle d'autorisation.	Activez cette option pour afficher toutes les correspondances de règles potentielles jusqu'au résultat de la première règle mise en correspondance. Désélectionnez (décochez) cette option pour obtenir uniquement la première règle mise en correspondance dans les résultats des tests.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
(Pare-feu uniquement) Vérifiez le masque HIP.	Cochez cette option pour vérifier l'état de sécurité du périphérique final qui accède à votre réseau.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

© 2020 Palo Alto Networks, Inc.

Correspondance de la politique QoS

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Sélectionnez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Type de point de code	Sélectionnez le type de codage par point de code que vous voulez tester.
Valeur de point de code	Spécifiez la valeur du codage par point de code : • **DSCP** : de 0 à 63 • **ToS** : de 0 à 7
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé :

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance de la politique d'authentification

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé :

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance politique SSL/déchiffrement

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	(Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Correspondance de la politique NAT

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port source	Saisissez le port spécifique d'où le trafic tire son origine.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Vers l'interface	Saisissez l'interface de destination du périphérique vers laquelle le trafic doit se rendre.
ID du périphérique HA	Saisissez l'ID du périphérique HA : • **0** : homologue HA principal • **1** : homologue HA secondaire
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance à la politique PBF (transfert basé sur une politique)

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Interface d'origine	Saisissez l'interface du périphérique de laquelle le trafic tire son origine.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
ID du périphérique HA	ID du périphérique HA : • **0** : homologue HA principal • **1** : homologue HA secondaire
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance de la politique DoS

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.

© 2020 Palo Alto Networks, Inc.

Champ	Description
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Interface d'origine	Saisissez l'interface du périphérique de laquelle le trafic tire son origine.
Vers l'interface	Saisissez l'interface de destination du périphérique vers laquelle le trafic doit se rendre.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

© 2020 Palo Alto Networks, Inc.

Routage

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Recherche FiB, Recherche Mfib	Sélectionnez l'une des recherches suivantes : • **FiB** : Effectuez la recherche d'itinéraires au sein de la table de routage active. • **Mfib** : Effectuez la recherche d'itinéraires multicast au sein de la table de routage active.
IP de destination	Saisissez l'adresse IP vers laquelle le trafic doit se rendre.
Virtual Router (routeur virtuel - VR)	Routeur virtuel spécifique au sein duquel le test de routage est effectué. Sélectionnez le routeur virtuel dans le menu déroulant.
ECMP	
IP source	Saisissez l'adresse IP spécifique de laquelle provient le trafic.
Port source	Saisissez le port spécifique duquel provient le trafic.
IP de destination	Saisissez l'adresse IP spécifique vers laquelle le trafic doit se rendre.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche :

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Test WildFire

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
contrôle	Sélectionnez le canal WildFire : **`Public`** ou **`Private`**.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Archivage sécurisé des menaces

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.

© 2020 Palo Alto Networks, Inc.

Champ	Description
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Ping

Le test de résolution de problèmes ping n'est pris en charge que sur les pare-feu exécutant les versions 9.0 ou ultérieures de PAN-OS.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Contourne la table de routage, utilise l'interface spécifiée	Activez cette option pour contourner la table de routage et utiliser une interface spécifiée. Désélectionnez (décochez) cette option pour tester la table de routage configurée.
Nombre	Saisissez le nombre de requêtes à envoyer. Le nombre par défaut est 5.
Don't fragment echo request packets (IPv4)	Activez cette option pour éviter de fragmenter les paquets de requêtes écho du test. Désactivation
Force to IPv6 destination	Activez cette option effectuer le test de force vers la destination IPv6.
Intervalle	Précisez un délai, en secondes, entre les requêtes (plage comprise entre 1 et 2 000 000 000).
Source	Saisissez l'adresse source de la requête écho.
Ne tentez pas d'imprimer les adresses symboliquement.	Activez cette option pour afficher les adresses IP dans les résultats des tests et pour ne pas résoudre l'adresse IP/nom d'hôte. Désactivez (décochez) cette option pour résoudre les adresses IP/noms d'hôte.
Pattern	Spécifiez le modèle de remplissage hexadécimal.
Taille	Saisissez la taille, en octets, des paquets de requêtes (la plage est comprise entre 0 et 65 468).
Tos	Saisissez la valeur adresse IP type de service (plage comprise entre 1 et 255).
TTL	Saisissez la valeur de durée de vie IP en sauts - valeur de la limite de sauts IPv6 (plage comprise entre 1 et 255).
Afficher les résultats détaillés	Activez cette option pour afficher les résultats détaillés du test.
Hôte	Saisissez le nom d'hôte ou l'adresse IP de l'hôte distant.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	• `Device not connected` : la connexion au périphérique a été abandonnée.

Trace Route

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Utilisez IPv4	Activez cette option pour utiliser l'adresse IPv4 des périphériques sélectionnés.
Utilisez IPv6	Activez cette option pour utiliser l'adresse IPv6 des périphériques sélectionnés.
Premier TTL	Saisissez la durée de vie utilisée dans le premier paquet à analyser sortant (plage comprise entre 1 et 255).
Max TTL	Saisissez les sauts de durée de vie maximaux (plage comprise entre 1 et 255).
Port	Saisissez le numéro de port de base utilisé dans le sondage.
Tos	Saisissez la valeur adresse IP type de service (plage comprise entre 1 et 255).
Attente	Indiquez le nombre de secondes pendant lesquelles attendre une réponse (plage comprise entre 1 et 99 999).
Suspendu	Saisissez le temps, en millisecondes, pendant lesquelles faire un arrêt entre les sondages (la valeur est comprise entre 1 et 2 000 000 000).
Définir le bit « Ne pas fragment »	Activez cette option pour ne pas fragmenter le paquet ICMP en plusieurs paquets si le chemin ne peut prendre en charge l'unité de transmission maximale (MTU).
Activer le débogage au niveau du socket	Activez cette option pour vous permettre de déboguer au niveau du socket.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Passerelle	Indiquez un maximum de huit passerelles de routage de source souple.
Ne tentez pas d'imprimer les adresses symboliquement.	Activez cette option pour afficher les adresses IP dans les résultats des tests et pour ne pas résoudre l'adresse IP/nom d'hôte. Désactivez (décochez) cette option pour résoudre les adresses IP/noms d'hôte.
Contourner les tables de routage et envoyer directement à un hôte	Activez cette option pour contourner les tables de routage et effectuez le test directement auprès de l'hôte.
Source	Saisissez une adresse source dans les paquets à analyser sortants.
Hôte	Saisissez le nom d'hôte ou l'adresse IP de l'hôte distant.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Connectivité du collecteur de journaux

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels qui ont été sélectionnés à des fins de test.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	(Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Liste dynamique externe

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Test URL	Spécifiez l'URL à utiliser pour tester la connexion.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

© 2020 Palo Alto Networks, Inc.

Serveur de mises à jour

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

État du service de journalisation du cloud de test GP

Testez l'état de connectivité au service de journalisation du cloud. Ce test n'est disponible que sur un serveur de gestion Panorama exécutant la version 1.3 ou ultérieure du plug-in des services de cloud.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche :

État du service du cloud de test GP

Testez l'état de connectivité à GlobalProtection en tant que Service. Ce test n'est disponible que sur un serveur de gestion Panorama exécutant la version 1.3 ou ultérieure du plug-in des services de cloud.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche :

© 2020 Palo Alto Networks, Inc.

Périphérique > Systèmes virtuels

Un système virtuel (vsys) est une instance de pare-feu indépendante (virtuelle) que vous pouvez gérer séparément dans un pare-feu physique. Chaque système virtuel peut être un pare-feu indépendant ayant sa politique de Sécurité, ses interfaces et administrateurs propres. Un système virtuel vous permet de segmenter l'administration de toutes les politiques, de la génération de rapports et des fonctions de visibilité proposées par le pare-feu.

Par exemple, si vous souhaitez personnaliser les fonctions de sécurité du trafic associé à votre service financier, vous pouvez définir un système virtuel Finance et définir des politiques de sécurité spécifiques à ce service. Pour optimiser l'administration des politiques, vous pouvez séparer la gestion des comptes administrateur pour les fonctions réseau et de pare-feu générales, tout en créant des comptes administrateur de système virtuel qui permettent d'accéder à chaque système virtuel. Cela permet à l'administrateur de système virtuel du service Finance de gérer la politique de sécurité de ce service uniquement.

Les fonctions de réseautage (tels que le routage statique et dynamique, les adresses IP des interfaces et les tunnels IPSec) appartiennent à un pare-feu complet et à ses systèmes virtuels. Une configuration de système virtuel (**Device [appareil]** > **Virtual Systems [système virtuels]**) ne contrôle pas les fonctions du pare-feu et du réseau (comme le routage statique ou dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP et les profils de réseaux). Pour chaque système virtuel, vous pouvez spécifier un ensemble d'interfaces de pare-feu physiques et logiques (notamment des VLAN et des câbles virtuels) et des zones de sécurité. Si vous avez besoin d'une segmentation de routage pour chaque système virtuel, vous devez créer et affecter des routeurs virtuels supplémentaires et affecter des interfaces, des VLAN et des câbles virtuels, le cas échéant.

Si vous utilisez un modèle Panorama pour définir vos systèmes virtuels, vous pouvez définir un système virtuel par défaut. Le système virtuel par défaut et la fonction de systèmes virtuels multiples déterminent si un pare-feu accepte des configurations spécifiques au système virtuel lors de la validation d'un modèle :

- Les pare-feux qui ont la fonction de systèmes virtuels multiples activée acceptent des configurations spécifiques au système virtuel pour tous les systèmes virtuels définis dans le modèle.
- Les pare-feux qui n'ont pas la fonction de systèmes virtuels multiples activée acceptent des configurations spécifiques uniquement au système virtuel par défaut. Si vous ne configurez pas de système virtuel par défaut, ces pare-feu n'accepteront pas de configurations propres au système virtuel.



Les pare-feux PA-3200, PA-5200, ainsi que les pare-feux PA-7000 Series prennent en charge plusieurs systèmes virtuels. Cependant, les pare-feux PA-3200 Series exigent une licence pour l'activation de plusieurs systèmes virtuels. Les pare-feu PA-220 et PA-800 Series ne prennent pas en charge plusieurs systèmes virtuels.

Avant d'activer plusieurs systèmes virtuels, notez les points suivants :

- Un administrateur de système virtuel crée et gère tous les éléments nécessaires à la politique de sécurité par système virtuel attribué.
- Les zones sont des objets au sein d'un système virtuel. Avant de définir une politique ou un objet de politique, sélectionnez le **Virtual System (Système virtuel)** approprié dans la liste déroulante de l'onglet **Policies (Politiques)** ou **Objects (Objets)**.
- Vous pouvez définir des destinations de journalisation à distance (SNMP, Syslog et messages), des applications, des services et des profils applicables à tous les systèmes virtuels (partagés) ou à un seul système virtuel.
- Si vous disposez de plusieurs systèmes virtuels, vous pouvez sélectionner un système virtuel en tant que pôle User-ID afin de partager les informations de mappage adresse IP/nom d'utilisateur entre les systèmes virtuels.

© 2020 Palo Alto Networks, Inc.

- Vous pouvez configurer des itinéraires de service globaux (pour tous les systèmes virtuels d'un pare-feu) ou spécifiques aux systèmes virtuels (Périphérique > Configuration > Services).
- Vous pouvez renommer un système virtuel uniquement sur le pare-feu local. La modification du nom d'un système virtuel n'est pas prise en charge sur Panorama. Si vous renommez un système virtuel sur Panorama, il en résulte un tout nouveau système virtuel, ou le nom du système virtuel est associé au mauvais système virtuel sur le pare-feu.

Avant de définir un système virtuel, vous devez d'abord activer la fonctionnalité de systèmes virtuels multiples sur le pare-feu. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les **General Settings (Paramètres généraux)**, sélectionnez **Multi Virtual System Capability (Fonction de systèmes virtuels multiples)**, puis cliquez sur **OK**. Ceci ajoute une page **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**. Sélectionnez la page, **Add (Ajoutez)** un système virtuel et indiquez les informations suivantes.

Paramètres d'un système virtuel	Description
ID	Saisissez l'identifiant (entier) du système virtuel. Pour plus d'informations sur le nombre de systèmes virtuels pris en charge, reportez-vous à la fiche technique de votre modèle de pare-feu. *si vous utilisez un modèle Panorama pour configurer le système virtuel, ce champ ne s'affiche pas.*
Name (Nom)	Saisissez un nom pour identifier le système virtuel (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. *si vous utilisez un modèle Panorama pour appliquer des configurations de système virtuel, le nom du système virtuel dans le modèle doit correspondre au nom du système virtuel sur le pare-feu.*
Autoriser le transfert du contenu déchiffré	Sélectionnez cette option pour autoriser le système virtuel à transférer du contenu déchiffré à un service externe lors de la mise en miroir du port ou de l'envoi de fichiers WildFire pour analyse. Reportez-vous également à la section Mise en miroir du port de déchiffrement.
Onglet Général	Sélectionnez un objet de **DNS Proxy (Proxy DNS)** dans la liste déroulante si vous souhaitez appliquer des règles de proxy DNS à ce système virtuel. (Réseau > Proxy DNS). Pour inclure des objets d'un type donné, sélectionnez ce type (interface, VLAN, câble virtuel, routeur virtuel ou système virtuel visible), **Add (Ajoutez)** un objet, puis sélectionnez l'objet dans la liste déroulante. Vous pouvez ajouter un ou plusieurs objets d'un quelconque type. Pour supprimer un objet, sélectionnez-le et **Delete (Supprimez)**-le.
Onglet Ressource	Indiquez les limites de ressources suivantes autorisées pour ce système virtuel : Chaque champ affiche la plage de valeurs valide; qui varie selon le modèle de pare-feu. Le paramètres par défaut est fixé sur 0, ce qui signifie que la limite du système virtuel est la limite du modèle de pare-feu. Cependant, la limite d'un paramètre spécifique n'est pas reproduite

© 2020 Palo Alto Networks, Inc.

Paramètres d'un système virtuel	Description
	pour chaque système virtuel. Par exemple, si un pare-feu dispose de quatre systèmes virtuels, chaque système virtuel ne peut disposer du nombre total de règles de décryptage autorisées par pare-feu. Une fois que le nombre total de règles de décryptage pour tous les systèmes virtuels atteint la limite du pare-feu, vous ne pouvez en ajouter plus. • **Sessions Limit (Limite de sessions)** : nombre maximum de sessions.  *Si vous utilisez la commande `show session meter` de la CLI, le pare-feu affiche le nombre maximal de sessions autorisé par plan de données, le nombre de sessions actuelles qui sont utilisées par le système virtuel et le nombre limité de sessions par système virtuel. Sur les pare-feu PA-5200 Series ou PA-7000 Series, le nombre de sessions actuelles qui sont utilisées peut être supérieur au nombre maximal de sessions configuré, puisque chaque système virtuel comporte plusieurs plans de données. La limite des sessions que vous avez configurée sur un pare-feu PA-5200 Series ou PA-7000 Series s'applique à chaque plan de données ; le nombre maximal par système virtuel est donc supérieur.* • **Security Rules (Règles de sécurité)** : nombre maximum de règles de sécurité. • **NAT Rules (Règles NAT)** : nombre maximum de règles NAT. • **Decryption Rules (Règles de décryptage)** : nombre maximum de règles de déchiffrement. • **QoS Rules (Règles QoS)** : nombre maximum de règles QoS. • **Application Override Rules (Règles de contrôle prioritaire sur l'application)** : nombre maximum de règles de contrôle prioritaire sur l'application. • **Policy Based Forwarding Rules (Règles de transfert basé sur une politique)** : nombre maximum de règles de transfert basé sur une politique (PBF). • **Captive Portal Rules (Règles de portail captif)** : nombre maximum de règles de portail captif (CP). • **DoS Protection Rules (Règles de protection DoS)** : nombre maximum de règles de déni de service (DoS). • **Site to Site VPN Tunnels (Tunnels VPN de site à site)** : nombre maximum de tunnels VPN de site à site. • **Concurrent GlobalProtect Tunnels (Tunnels GlobalProtect simultanés)** : nombre maximum d'utilisateurs GlobalProtect à distance simultanés. • **Inter-Vsys User-ID Data Sharing (Partage des données User-ID entre les systèmes virtuels)—Make this vsys a User-ID data hub (Faites de ce système virtuel un centre de données User-ID)** pour permettre à tous les autres systèmes virtuels du pare-feu d'accéder aux informations de mappage utilisateur partagées ou **Change hub (Modifiez le centre)** et sélectionnez un nouveau système virtuel à réaffecter en tant que centre de données User-ID. Des privilèges de super-utilisateur ou d'administrateur sont requis.

© 2020 Palo Alto Networks, Inc.

Périphérique > Passerelles partagées

Les passerelles partagées permettent à plusieurs systèmes virtuels de partager une seule interface pour la communication externe (généralement connectée à un réseau en amont commun, tel qu'un Fournisseur de services Internet). Tous les systèmes virtuels communiquent avec le monde extérieur via l'interface physique à l'aide d'une adresse'A0;IP unique. Un routeur virtuel est utilisé pour acheminer le trafic de tous les systèmes virtuels via la passerelle partagée.

Les passerelles partagées utilisent des interfaces de Niveau 3 et au moins une interface de Niveau3 doit être configurée en tant que passerelle partagée. Les communications provenant d'un système virtuel et quittant le pare-feu via une passerelle partagée nécessitent des politiques similaires aux communications entre deux systèmes virtuels. Vous pouvez configurer une zone « vsys externe » pour définir les règles de sécurité du système virtuel.

Paramètres de passerelle partagée	Description
ID	Identifiant de la passerelle (non utilisé par le pare-feu).
Name (Nom)	Saisissez un nom pour la passerelle partagée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. Seul le nom est requis.
Proxy DNS	(Facultatif) Si un proxy DSN est configuré, sélectionnez le(s) serveur(s) DNS à utiliser pour les requêtes de nom de domaine.
Interfaces	Sélectionnez les interfaces que la passerelle partagée utilisera.

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats

- Périphérique > Gestion des certificats > Certificats
- Périphérique > Gestion des certificats > Profil de certificat
- Périphérique > Gestion des certificats > Répondeur'A0;OCSP
- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Périphérique > Gestion des certificats > SCEP
- Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > Certificats

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)** pour gérer (générer, importer, renouveler, supprimer et révoquer) les certificats, qui sont utilisés pour sécuriser la communication à travers un réseau. Vous pouvez également exporter et importer la clé haute disponibilité (HD) utilisée pour sécuriser la connexion entre les homologues HD sur le réseau. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Default Trusted Certificate Authorities (Autorités de certification de confiance par défaut)** pour afficher, activer et désactiver les autorités de certification (AC) approuvées par le pare-feu.

Pour plus d'informations sur la façon de mettre en œuvre des certificats sur le pare-feu et Panorama, reportez-vous à la section Gestion des certificats.

- Gestion des certificats du pare-feu et de Panorama
- Gestion des autorités de certification de confiance par défaut
- Périphérique > Gestion des certificats > Profil de certificat
- Périphérique > Gestion des certificats > Répondeur'A0;OCSP
- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Périphérique > Gestion des certificats > SCEP
- Périphérique > Clé principale et diagnostics

Gestion des certificats du pare-feu et de Panorama

- Périphérique > Gestion des certificats > Certificats > Certificats de périphérique
- Panorama > Gestion des certificats > Certificats

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des Certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats du périphérique)** ou **Panorama** > **Certificate Management (Gestion des Certificats)** > **Certificats** > **Device Certificates (Certificats du périphérique)** pour afficher les certificats que le pare-feu ou Panorama utilise pour certaines tâches telles que la sécurisation de l'accès à l'interface Web, le déchiffrement SSL ou le LSVPN.

Voici quelques utilisations possibles des certificats. Définissez l'utilisation du certificat après que vous l'avez généré (voir Gestion des autorités de certification de confiance par défaut).

- **Forward Trus (Approbation de transfert)** – Le pare-feu utilise ce certificat pour signer une copie du certificat du serveur que le pare-feu présente aux clients lors du Décryptage du proxy de transfert SSL lorsque l'autorité de certification (AC) qui a signé le certificat du serveur se trouve dans la liste des AC de confiance du pare-feu.
- **Forward Untrust (Non-approbation de transfert)** – Le pare-feu utilise ce certificat pour signer une copie du certificat du serveur que le pare-feu présente aux clients lors du Déchiffrement du proxy de transfert SSL lorsque l'autorité de certification (AC) qui a signé le certificat du serveur ne se trouve pas dans la liste des AC de confiance du pare-feu.
- **Trusted Root CA (AC racine approuvée)** – Le pare-feu utilise ce certificat en tant qu'AC de confiance pour le Déchiffrement du proxy de transfert SSL, GlobalProtect, le Contrôle prioritaire de l'URL par l'administrateur et le Portail captif. Le pare-feu dispose d'une liste importante d'AC de confiance. Le certificat AC racine de confiance s'applique aux autres AC de confiance pour votre organisation, mais qui ne figurent pas dans la liste prédéfinie d'AC de confiance.

© 2020 Palo Alto Networks, Inc.

- **SSL Exclude (Certificat d'exclusion SSL)** – Le pare-feu utilise ce certificat si vous définissez la configuration des exceptions au Déchiffrement afin d'exclure certains serveurs du Déchiffrement SSL/TLS.
- **Certificate for Secure Syslog (Certificat pour Secure Syslog)** – Le pare-feu utilise ce certificat pour sécuriser la transmission de journaux sous forme de messages Syslog vers un serveur Syslog.

Pour générer un certificat, cliquez sur Générer et renseignez les champs suivants :

Une fois qu'un certificat a été généré, la page affichera Autres actions prises en charge pour gérer les certificats.

Paramètres de génération d'un certificat	Description
Type de certificat	Sélectionnez l'entité qui génère le certificat. **Local** – Le pare-feu ou Panorama génère le certificat. **SCEP** – Un serveur SCEP (Simple Certificate Enrollment Protocol, Protocole d'inscription de certificats simple) génère le certificat et l'envoie au pare-feu ou à Panorama.
Nom du certificat	Required (Requis) Saisissez un nom (maximum de 63 caractères sur le pare-feu ou de 31 caractères sur Panorama) pour identifier le certificat. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Profil SCEP	(Certificats SCEP uniquement) Sélectionnez un **SCEP Profile (Profil SCEP)** pour définir comment le pare-feu ou Panorama communique avec un serveur SCEP et pour définir les paramètres du certificat SCEP. Pour plus de détails, voir Périphérique > Gestion des certificats > SCEP. Vous pouvez configurer un pare-feu servant de portail GlobalProtect pour solliciter des certificats SCEP sur demande et déployer automatiquement les certificats aux terminaux. Les autres champs de la boîte de dialogue Générer un certificat ne s'appliquent pas aux certificats SCEP. Après avoir spécifié le **Certificate Name (Nom du certificat)** et le **SCEP Profile (Profil SCEP)**, cliquez sur **Generate (Générer)**.
Common Name (nom commun - CN)	(Requis) Saisissez l'adresse IP ou le FQDN qui apparaîtra sur le certificat.
Partagé	Sur un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez **Shared (Partagé)** si vous souhaitez que le certificat s'applique à chaque système virtuel.
Signés par	Pour signer le certificat, vous pouvez utiliser un certificat d'autorité de certification (AC) que vous avez importé dans le pare-feu. Le certificat peut également être auto-signé, auquel cas le pare-feu constitue l'autorité de certification. Si vous utilisez Panorama, vous pouvez également générer un certificat auto-signé pour Panorama. Si vous avez importé des certificats d'autorité de certification ou que vous en avez émis sur le pare-feu (auto-signé), la liste déroulante inclut

© 2020 Palo Alto Networks, Inc.

Paramètres de génération d'un certificat	Description
	les autorités de certification disponibles pour signer le certificat que vous créez. Pour générer une demande de signature de certificat (CSR), sélectionnez **External Authority (CSR) (Autorité externe (demande de signature de certificat))**. Vous pouvez exporter la CSR et l'envoyer à l'AC pour signature après que le pare-feu a généré le certificat et la paire de clés.
Autorité de certification	Sélectionnez cette option si vous souhaitez que le pare-feu génère le certificat. Désignez ce certificat comme une AC afin de pouvoir l'utiliser pour signer d'autres certificats sur le pare-feu.
Répondeur OCSP	Sélectionnez un profil de répondeur OCSP dans le menu déroulant (voir Périphérique > Gestion des certificats > Répondeur OCSP). Le nom d'hôte correspondant apparaît dans le certificat.
Algorithme	Sélectionnez un algorithme de génération de clé pour le certificat : **RSA** ou **Elliptic Curve DSA** (ECDSA). ECDSA utilise des clés de plus petite taille que l'algorithme RSA, et offre donc une meilleure performance de traitement des connexions SSL/TLS. ECDSA offre également une sécurité supérieure ou égale à celle de RSA. ECDSA est recommandé pour les navigateurs et systèmes d'exploitation clients qui le prennent en charge, mais vous devrez peut-être sélectionner RSA pour la compatibilité avec les navigateurs et systèmes d'exploitation existants. *Les pare-feu exécutant PAN-OS 6.1 ou versions antérieures supprimeront tous les certificats ECDSA que vous appliquez à partir de Panorama et aucun certificat RSA signé par une autorité de certification de certificat ECDSA ne sera valide sur ces pare-feu.* Vous ne pouvez pas utiliser un Module de sécurité matériel (HSM) pour stocker les clés ECDSA privées utilisées pour le décryptage du Proxy de transfert SSL ou l'Inspection SSL entrante.
Nombre de bits	Sélectionnez la longueur de la clé du certificat. Si le pare-feu est en mode FIPS-CC et que l'**Algorithm (Algorithme)** de génération de clé est **RSA**, les clés RSA générées doivent comporter **2 048** ou **3 027** bits. Si l'**Algorithm (Algorithme)** est **Elliptic Curve DSA**, les deux options de longueur de clé (**256** et **384**) s'appliquent.
Résumer	Sélectionnez l'algorithme **Digest (Résumer)** du certificat. Les options disponibles dépendent de l'**Algorithm (Algorithme)** de génération de clé : • **RSA** : **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512** • **Elliptic Curve DSA** : **SHA256** ou **SHA384** Si le pare-feu est en mode FIPS-CC et que l'**Algorithm (Algorithme)** de génération de clé est **RSA**, vous devez sélectionner **SHA256**, **SHA384** ou

© 2020 Palo Alto Networks, Inc.

Paramètres de génération d'un certificat	Description
	SHA512 comme algorithme **Digest (Résumer)**. Si l'**Algorithm (Algorithme)** est **Elliptic Curve DSA**, les deux algorithmes **Digest (Résumer)** (**SHA256** et **SHA384**) s'appliquent. *Les certificats clients utilisés lors de la demande de services de pare-feu basés sur TLSv1.2 (comme l'accès administrateur à l'interface Web) ne peuvent avoir SHA512 (sha512) comme algorithme Résumer. Les certificats clients doivent utiliser un algorithme Résumer inférieur (tel que SHA384) ou vous devez limiter la Max Version (Version max) à TLSv1.1 lorsque vous configurez les profils de service SSL/TLS pour les services de pare-feu (voir Périphérique > Gestion des certificats > Profil de service SSL/TLS).*
Expiration (jours)	Indiquez le nombre de jours de validité du certificat (la valeur par défaut est 365). *Si vous indiquez une Validity Period (Période de validité) dans une configuration satellite GlobalProtect, cette valeur appliquera un contrôle prioritaire sur la valeur saisie dans ce champ.*
Attributs du certificat	Cliquez sur **Add (Ajouter)** pour ajouter des **Certificate Attributes (Attributs de certificat)** supplémentaires permettant d'identifier l'entité pour laquelle vous émettez le certificat. Vous pouvez ajouter les attributs suivants'A0;: **Country (Pays)**, **State (État)**, **Locality (Région)**, **Organization (Organisation)**, **Department (Service)** et **Email (Adresse e-mail)**. De plus, vous pouvez définir l'un des champs Autre nom de l'objet suivants'A0;: **Host Name (Nom d'hôte)** (SubjectAltName:DNS), **IP (Adresse IP)** (SubjectAltName:IP) et **Alt Email (Autre adresse e-mail)** (SubjectAltName:email). *Pour ajouter un pays comme attribut de certificat, sélectionnezCountry (Pays) dans la colonne Type, puis cliquez sur Value (Valeur) pour voir les indicatifs de pays ISO 6366.*

Si vous avez configuré un module de sécurité matériel (HSM), les clés privées sont stockées sur le stockage de module de sécurité matériel externe, et non sur le pare-feu.

Autres actions prises en charge pour gérer les certificats

Après avoir généré le certificat, ses détails s'affichent sur la page et les actions suivantes sont disponibles :

© 2020 Palo Alto Networks, Inc.

Autres actions prises en charge pour gérer les certificats	Description
Supprimer	Sélectionnez le certificat et **Supprimez**-le. *Si le pare-feu possède une politique de déchiffrement, vous ne pouvez pas supprimer un certificat pour lequel l'utilisation est réglée comme Certificat d'approbation de transfert or Certificat de non-approbation de transfert. Pour modifier l'utilisation du certificat, voir* Gestion des autorités de certification de confiance par défaut.
Révoquer	Sélectionnez le certificat que vous souhaitez révoquer et cliquez sur **Revoke (Révoquer)**. Le certificat passe immédiatement à l'état révoqué. Aucune validation n'est requise.
Renouveler	Lorsqu'un certificat expire ou est sur le point d'expirer, sélectionnez le certificat correspondant et cliquez sur **Renew (Renouveler)**. Définissez la période de validité (en jours) du certificat et cliquez sur **OK**. Si le pare-feu est la CA ayant généré le certificat, le pare-feu le remplacera par un nouveau certificat doté d'un numéro de série différent mais des mêmes attributs que l'ancien. Si une autorité de certification externe (AC) a signé le certificat et que le pare-feu utilise la méthode OCSP (Online Certificate Status Protocol) pour vérifier le statut de révocation du certificat, le pare-feu utilise les informations du répondeur OCSP pour mettre à jour le statut du certificat.
Importer	Cliquez pour **Importer** un certificat et configurez-le comme suit : • Saisissez un nom de certificat pour identifier le certificat. • Recherchez le fichier de certificat. Si vous importez un certificat **PKCS12** et une clé privée, un seul fichier contient ces deux éléments. Si vous importez un certificat **PEM**, le fichier ne contient que le certificat. *Importez chaque certificat individuellement. Si vous sélectionnez une chaîne de certificats, le pare-feu importe le premier certificat dans la chaîne.* • Sélectionnez le **File Format (Format de fichier)** du certificat. • Sélectionnez **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)** si un module de sécurité matériel stocke la clé privée de ce certificat. Pour plus de détails sur les modules de sécurité matériels, voir Périphérique > Configuration > Module de sécurité matériel (HSM). • **Importer une clé privée** comme requise (format PEM uniquement). Si vous avez sélectionné **PKCS12** comme **Format de fichier** du certificat, le **Fichier du certificat** sélectionné comprend la clé. Si vous avez sélectionné le format **PEM**, recherchez le fichier de clé privée chiffré (généralement *.key). Pour les deux formats, saisissez la **Phrase secrète** et **Confirmez la phrase secrète**.

© 2020 Palo Alto Networks, Inc.

Autres actions prises en charge pour gérer les certificats	Description
	Lorsque vous importez un certificat sur un pare-feu de Palo Alto Networks ou un serveur Panorama qui est en mode FIPS-CC, vous devez importer le certificat en tant que Certificat codé en base-64 (PEM) et vous devez crypter la clé privée avec AES. En outre, vous devez utiliser SHA1 comme méthode de dérivation de clé basée sur la phrase secrète. Pour importer un certificat PKCS12, convertissez le certificat au format PEM (en utilisant un outil tel que OpenSSL) ; assurez-vous que la phrase secrète que vous utilisez pendant la conversion comporte au moins de six caractères.
Export (Exporter)	Sélectionnez le certificat que vous souhaitez exporter, cliquez sur **Exporter**, puis sélectionnez un **Format de fichier** : • Certificat et clé privée cryptés (PKCS12) - Le fichier exporté contiendra à la fois le certificat et la clé privée. • Certificat codé en base-64 (PEM) - Si vous souhaitez exporter également la clé privée, sélectionnez Exporter la clé privée, saisissez une Phrase secrète puis Confirmez la phrase secrète. • Certificat codé binaire (DER) - Vous pouvez exporter uniquement le certificat, et non la clé : ignorez les champs Exporter la clé privée et Phrase secrète.
Importer la clé HD Exporter la clé HD	Les clés HD doivent être échangées entre les homologues de pare-feu'A0;; la clé du pare-feu'A0;1 doit être exportée, puis importée sur le pare-feu'A0;2 et vice-versa. Pour importer des clés pour la haute disponibilité (HD), cliquez sur **Import HA Key (Importer la clé HD)** et cliquez sur **Browse (Parcourir)** pour rechercher le fichier de clé à importer. Pour exporter des clés pour HD, cliquez sur **Export HA Key (Exporter la clé HD)** et indiquez l'emplacement où enregistrer le fichier.
Définissez l'utilisation du certificat.	Dans la colonne Nom, cliquez sur le certificat, puis sélectionnez les options appropriées selon l'utilisation prévue du certificat.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau de configuration des certificats gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Gestion des autorités de certification de confiance par défaut

- Périphérique > Gestion des certificats > Certificats > Autorités de certification de confiance par défaut

© 2020 Palo Alto Networks, Inc.

Cette page vous permet d'afficher, de désactiver ou d'exporter les autorités de certification (AC) pré-incluses approuvées par le pare-feu. La liste prédéfinie des AC comprend les fournisseurs de certificats de confiance et les plus courants qui sont responsables de la génération des certificats dont le pare-feu a besoin pour sécuriser les connexions à l'Internet. Pour chaque AC racine de confiance, le nom, l'objet, l'émetteur, la date d'expiration et l'état de validité s'affichent.

Par défaut, le pare-feu n'approuve pas les AC intermédiaires, puisque ceux-ci ne font pas partie de la chaîne de confiance entre le pare-feu et l'AC racine de confiance. Vous devez ajouter manuellement les AC intermédiaires que vous voulez que le pare-feu approuve de même que les autres AC d'entreprises de confiance dont votre organisation a besoin (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**).

Paramètres des autorités de certification de confiance	Description
Activer	Si vous avez désactivé une autorité de certification, vous pouvez la **Enable (Réactiver)**.
Désactivation	Sélectionnez l'autorité de certification et **Disable (Désactivez)**-la. Vous pouvez utiliser cette option si vous souhaitez seulement faire confiance à certains AC ou si vous souhaitez tous les désactiver et faire confiance uniquement à votre AC locale.
Export (Exporter)	Sélectionnez le certificat AC et cliquez sur **Export (Exporter)** pour l'exporter. Cette action vous permet de l'importer dans un autre système ou de consulter le certificat hors ligne.

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > Profil de certificat

- **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**
- **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**

Les profils de certificat indiquent les certificats de l'autorité de certification (AC) qui doivent être utilisés pour vérifier les certificats clients, comment vérifier l'état de révocation des certificats et de quelle façon cet état permet de restreindre l'accès. Vous sélectionnez les profils quand vous configurez l'authentification du certificat pour Portail captif, GlobalProtect, VPN de site à site IPsec, Dynamic DNS (DNS dynamique ; DDNS) et accès de l'interface Web aux pare-feu et à Panorama. Vous pouvez configurer un profil de certificat distinct pour chacun de ces services.

Paramètres d'un profil de certificat	Description
Name (Nom)	(Required [Requis]) Saisissez un nom pour identifier le profil (maximum de 63 caractères sur le pare-feu ou de 31 caractères sur Panorama). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Champ Username	Si GlobalProtect utilise les certificats uniquement pour l'authentification auprès du portail et de la passerelle, le logiciel PAN-OS utilise le champ de certificat sélectionné dans la liste déroulante **Username Field (Champ Nom d'utilisateur)** comme nom d'utilisateur et le fait correspondre à l'adresse IP pour le service User-ID : • **Subject (Sujet)** : le nom commun. • **Subject Alt (Autre objet)** : le Nom principal ou le nom de messagerie. • **None (Aucun)** : Généralement utilisée pour l'authentification avant ouverture de session ou de périphériques GlobalProtect.
Domain (Domaine)	Saisissez le domaine NetBIOS de manière à ce que le logiciel PAN-OS puisse mapper les utilisateurs via la fonctionnalité User-ID.
Certificats de l'autorité de certification	(Requis) **Add (Ajoutez)** un **CA Certificate (Certificat AC)** à affecter au profil. Éventuellement, si le pare-feu utilise la méthode OCSP (Online Certificate Status Protocol) pour vérifier le statut de révocation du certificat, vous pouvez configurer les champs suivants pour appliquer

© 2020 Palo Alto Networks, Inc.

Paramètres d’un profil de certificat	Description
	un contrôle prioritaire sur le comportement par défaut. Pour la plupart des déploiements, ces champs ne s'appliquent pas. • Par défaut, le pare-feu utilise les informations du Authority Information Access (accès aux informations de l'autorité ; AIA) du certificat pour extraire les informations sur le répondeur OCSP. Pour appliquer un contrôle prioritaire sur les informations d’AIA, saisissez une **Default OCSP URL (URL OCSP par défaut)** (commençant par `http://` ou par `https://`). • Par défaut, le pare-feu utilise le certificat sélectionné dans le champ **CA Certificate (Certificat AC)** pour valider les réponses OCSP. Pour utiliser un certificat différent pour la validation, sélectionnez-le dans le champ **OCSP Verify CA Certificate (Certificat AC pour la vérification OCSP)**. De plus, saisissez un **Template Name (Nom de modèle)** pour identifier le modèle qui a été utilisé pour signer le certificat.
Utiliser CRL	Sélectionnez cette option pour utiliser une liste de révocation de certificat (CRL) afin de vérifier l'état de révocation des certificats.
Utiliser OCSP	Sélectionnez cette option pour utiliser OCSP afin de vérifier l'état de révocation des certificats. *si vous sélectionnez OCSP et CRL, le pare-feu essaie d'abord le protocole'A0;OCSP et ne fait appel à la méthode'A0;CRL en secours que si le répondeur'A0;OCSP est indisponible.*
Délai d'expiration de la réception CRL	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse du service CRL.
Délai d'attente en réception OCSP	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse du répondeur OCSP.
Délai d'expiration du statut du certificat	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse d’aucun service d’état du certificat et applique la logique de blocage de la session que vous avez définie.
Bloquer une session si le statut du certificat est inconnu	Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions lorsque le service OCSP ou CRL renvoie un état de révocation de certificat *inconnu*. Sinon, le pare-feu poursuit les sessions.
Bloquer une session si le statut du certificat ne peut pas être récupéré avant le délai d'expiration	Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions une fois qu'il a enregistré un délai d'expiration de la demande OCSP ou CRL. Sinon, le pare-feu poursuit les sessions.
Bloquer les sessions si le certificat n'a pas été	(GlobalProtect uniquement) Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions lorsque l'attribut numéro de série qui figure dans le champ sujet du certificat client

© 2020 Palo Alto Networks, Inc.

Paramètres d’un profil de certificat	Description
généré pour le périphérique s'authentifiant	ne correspond pas à l'ID de l'hôte que l'application GlobalProtect signale pour le point de terminaison. Sinon, le pare-feu autorise la session. Cette option ne s’applique qu’à l’authentification du certificat GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > Répondeur'A0;OCSP

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **OCSP Responder (Répondeur OCSP)** pour définir un répondeur (serveur) OCSP (Online Certificate Status Protocol) pour vérifier l'état de révocation des certificats.

Outre l'ajout d'un répondeur OCSP, pour activer OCSP, vous devez effectuer les tâches suivantes :

- Activez la communication entre le pare-feu et le serveur OCSP : sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, puis sélectionnez **HTTP OCSP** dans les Management Interface Settings (Paramètres de l'interface de gestion), et cliquez sur **OK**.
- Si le pare-feu déchiffre le trafic SSL/TLS sortant, vous pouvez le configurer pour vérifier l'état de révocation des certificats du serveur de destination : sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Sessions**, puis cliquez sur **Decryption Certificate Revocation Settings (Paramètres de révocation du certificat de décryptage)**, sélectionnez **Enable (Activer)** dans les paramètres OCSP, ensuite saisissez le **Receive Timeout (Délai de réception)** (l'intervalle après lequel le pare-feu n'attend plus de réponse OCSP), puis cliquez sur **OK**.
- Pour configurer le pare-feu lui-même comme un répondeur OCSP, vous pouvez éventuellement ajouter un profil de gestion d'interface à l'interface utilisée pour les services OCSP. D'abord, sélectionnez **Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Interface Mgmt (Gestion de l'interface)**, cliquez sur **Add (Ajouter)**, sélectionnez **HTTP OCSP**, puis cliquez sur **OK**. Ensuite, sélectionnez **Network (Réseau)** > **Interfaces**, cliquez sur le nom de l'interface que le pare-feu utilisera pour les services OCSP, sélectionnez **Advanced (Avancé)** > **Other info (Autres informations)**, choisissez le profil de Gestion d'interface configuré, enfin cliquez sur **OK** et sur **Commit (Valider)**.



Activez un répondeur OCSP de sorte que vous soyez avisé de la révocation éventuelle d'un certificat afin de pouvoir prendre les mesures appropriées pour établir une connexion sécurisée au portail et aux passerelles.

Paramètres du répondeur OCSP	Description
Name (Nom)	Saisissez un nom pour identifier le répondeur (31 caractères maximum). Ce nom est sensible à la casse. Il doit être unique et utiliser uniquement des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le répondeur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans les autres contextes, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé. Après avoir enregistré le répondeur, vous ne pouvez plus changer son **Location (Emplacement)**.
Nom de l'hôte	Saisissez le nom d'hôte (recommandé) ou l'adresse'A0;IP du répondeur'A0;OCSP. À partir de cette valeur, PAN-OS déduit automatiquement une URL et l'ajoute au certificat en cours de vérification. Si vous configurez le pare-feu comme un répondeur OCSP, le nom d'hôte doit se résoudre en une adresse IP dans l'interface que le pare-feu utilise pour les services OCSP.

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > Profil de service SSL/TLS

- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Panorama > Gestion des certificats > Profil de service SSL/TLS

Les profils de service SSL/TLS définissent un certificat du serveur et une version de protocole ou une plage de versions pour les services de pare-feu ou Panorama utilisant SSL/TLS (comme l'accès administrateur à l'interface Web). En définissant les versions de protocole, les profils vous permettent de limiter les suites de chiffrements disponibles pour sécuriser les communications avec les systèmes client demandant les services.

En ce qui concerne les systèmes clients qui requièrent un pare-feu ou les services Panorama, la liste d'approbation de certificats (CTL) doit inclure le certificat de l'autorité de certification (CA) qui a délivré le certificat spécifié dans le profil de service SSL/TLS. Dans le cas contraire, les utilisateurs constateront une erreur de certificat lorsqu'ils solliciteront les services. La plupart des certificats d'une tierce CA sont présents par défaut sur les navigateurs des clients. Si une entreprise ou une CA de certificat généré par un pare-feu est l'émetteur, vous devez déployer ce certificat CA à la liste CTL dans les navigateurs des clients.

Pour ajouter un profil, cliquez sur **Ajouter** et renseignez les champs dans le tableau suivant.

Paramètres de profil de service SSL/TLS	Description
Name (Nom)	Saisissez un nom pour identifier le profil (31 caractères maximum). Ce nom est sensible à la casse. Il doit être unique et utiliser uniquement des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Partagé	Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionner cette option rend le profil disponible sur tous les systèmes virtuels. Cette option est sélectionnée par défaut et le profil s'applique uniquement au système virtuel sélectionné dans l'onglet **Périphérique**, dans la liste déroulante **Emplacement**.
certificate	Sélectionner, importer ou générer un certificat de serveur à associer au profil (voir Gérer les certificats du pare-feu et de Panorama). *n'utilisez pas de certificats d'autorité de certification (AC) pour les services ; utilisez des certificats signés uniquement.*
Version min	Sélectionnez la première (**Version min**) et la dernière (**Version max**) version de TLS que les services peuvent utiliser : **TLSv1.0**, **TLSv1.1**, **TLSv1.2** ou **Max** (la dernière version disponible).
Version max	

© 2020 Palo Alto Networks, Inc.

Paramètres de profil de service SSL/TLS	Description
	TLSv1.1 (TLSv1.1) est la version de TLS la plus ancienne qui est prise en charge sur les pare-feu en mode FIPS-CC sur lesquels PAN-OS 8.0 ou une version ultérieure de PAN-OS est installé ; ne sélectionnez pas TLSv1.0 (TLSv1.0). *Les certificats clients qui sont utilisés lors de la demande de services de pare-feu reposant sur TLSv1.2 ne peuvent pas avoir SHA512 en tant qu'algorithme de cryptage. Les certificats clients doivent utiliser un algorithme de cryptage inférieur (tel que SHA384) ou vous devez limiter la Version max à TLSv1.1 pour les services.*  *Utilisez la version la plus forte possible du protocole de sorte à fournir la sécurité la plus forte au réseau. Si vous le pouvez, définissez la Min Version (Version min) sur TLSv1.2 ert la Max Version (Version max) sur Max.*

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > SCEP

Le protocole de recrutement de certificat simple (SCEP) fournit un mécanisme pour générer un certificat unique aux terminaux, aux passerelles et aux périphériques satellites. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP** pour créer une configuration SCEP.

Pour plus d'informations sur la création d'un profil SCEP, reportez-vous à la section Déploiement de certificats au moyen de SCEP

.

Pour démarrer une nouvelle configuration SCEP, cliquez sur **Ajouter** et renseignez les champs suivants.

Paramètres SCEP	Description
Name (Nom)	Indiquez un Nom descriptif pour identifier cette configuration SCEP, comme SCEP_*Example*. Ce nom distingue un profil SCEP des autres instances que vous pourriez trouver parmi les profils de configuration.
Location (Emplacement)	Si le système dispose de plusieurs systèmes virtuels, sélectionnez l'Emplacement du profil. L'emplacement précise où la configuration SCEP est disponible.
Mot de passe à usage unique (demande d'authentification)	
Demande d'authentification SCEP	(Facultatif) Pour rendre la génération de certificats basée sur SCEP plus sécurisée, vous pouvez configurer un mécanisme de réponse au défi SCEP (un mot de passe à usage unique [OTP]) entre l'infrastructure à clé publique (PKI) et le portail pour chaque demande de certificat. *Après avoir configuré ce mécanisme, son fonctionnement est invisible et aucune autre intervention de votre part n'est nécessaire.* Le mécanisme de contestation que vous sélectionnez détermine la source de l'OTP. Si vous sélectionnez **Fixed (Fixe)**, copiez le mot de passe d'authentification à partir du serveur SCEP pour le PKI et saisissez la chaîne dans la boîte de dialogue **Password (Mot de passe)** qui s'affiche sur le portail lorsqu'il est configuré comme **Fixed (Fixe)**. Chaque fois que le portail demande un certificat, il utilise ce mot de passe pour s'authentifier avec le PKI. Si vous sélectionnez **Dynamic (Dynamique)**, vous saisissez le nom d'utilisateur et le mot de passe de votre choix (ceux-ci peuvent être les informations d'identification de l'administrateur PKI) et **Server URL (URL du serveur)** SCEP où le client portail saisit ces informations d'identification. Ce nom d'utilisateur et ce mot de passe demeurent les mêmes lorsque le serveur SCEP génère de manière transparente un mot de passe OTP pour le portail lors de chaque demande de certificat. (Lors de chaque demande de certificat, vous pouvez afficher ce changement d'OTP après un rafraîchissement de l'écran dans le champ « Le mot de passe d'authentification est ».) L'ICP transmet au portail de manière transparente chaque nouveau mot de passe. Le portail utilise ensuite le mot de passe pour sa demande de certificat.

© 2020 Palo Alto Networks, Inc.

Paramètres SCEP	Description
	Pour vous conformer à la norme américaine du traitement de l'information (FIPS), sélectionnez Dynamic (Dynamique), indiquez ensuite une Server URL (URL du serveur) qui utilise le protocole HTTPS, puis activez SCEP Server SSL Authentication (Authentification SSL du serveur SCEP). (L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.)
Configuration	
URL du serveur	Saisissez l'URL à laquelle le portail demande et qui reçoit des certificats clients de la part du serveur SCEP. Exemple : `http://<hostname or IP>/certsrv/mscep/.`
Nom CA-IDENT	Saisissez une chaîne pour identifier le serveur SCEP. Longueur maximale de 255 caractères.
Objet	Configurez le sujet pour inclure des informations d'identification sur le périphérique et, éventuellement, sur l'utilisateur et pour inclure ces informations dans la demande de signature de certificat (CSR) sur le serveur SCEP. Lorsqu'il est utilisé pour demander des certificats clients pour les terminaux, le terminal envoie des informations d'identification relatives au périphérique qui incluent sa valeur d'ID d'hôte. La valeur d'ID d'hôte varie selon le type de périphérique, soit GUID (Windows), adresse MAC de l'interface (Mac), Android ID (appareils Android), UDID (périphériques iOS), ou un nom unique qui GlobalProtect assigne (Chrome). Lorsqu'il est utilisé pour demander des certificats pour les périphériques satellites, la valeur d'ID de l'hôte est le numéro de série du périphérique. Pour indiquer des informations supplémentaires dans la CSR, saisissez le nom du Sujet. Le sujet doit être un nom différent au format <*attribute*>=<*value*> et doit inclure la clé du nom commun (CN). Par exemple : `O=acme,CN=acmescep` Il existe deux façons d'indiquer le CN : • (Recommandé) **CN par jeton d'authentification** – Saisissez l'un des jetons supportés **`$USERNAME`**, **`$EMAILADDRESS`**, ou **`$HOSTID`**. Utilisez la variable nom d'utilisateur ou adresse de messagerie pour vous assurer que le portail demande des certificats pour un utilisateur spécifique. Pour demander des certificats pour le périphérique uniquement, indiquez la variable ID d'hôte. Lorsque le portail GlobalProtect insère les paramètres SCEP dans l'agent, la portion NC du nom du sujet est remplacée par la valeur réelle (nom d'utilisateur, ID d'hôte ou adresse e-mail) du propriétaire du certificat. Par exemple : `O=acme,CN=$HOSTID`

© 2020 Palo Alto Networks, Inc.

Paramètres SCEP	Description
	• **CN statique** : Le CN que vous indiquez sera utilisé comme sujet pour tous les certificats générés par le serveur SCEP. Par exemple : `O=acme,CN=acmescep`
Autre type de nom de l'objet	*Utilisez des entrées statiques pour l'autre type de nom de l'objet. Le pare-feu ne prend pas en charge les jetons dynamiques tels que* ***$USERNAME****.* Après avoir sélectionné un type autre qu'**Aucun**, une boîte de dialogue s'affiche pour que vous y saisissiez la valeur appropriée : • **RFC 822 Name (Nom RFC 822)** : saisissez le nom de la messagerie dans l'objet du certificat ou l'extension alternative du nom de l'objet. • **DNS Name (Nom DNS)** : saisissez le nom DNS utilisé pour évaluer les certificats. • **Uniform Resource Identifier (URI) (Identifiant URI)** – Saisissez le nom de la ressource URI à partir de laquelle le client obtient le certificat.
Paramètres cryptographiques	• **Number of Bits (Nombre de bits)** – Sélectionnez le **Number of Bits (Nombre de bits)** de la clé pour le certificat. Si le pare-feu est en mode FIPS-CC, les clés générées doivent être d'au moins 2 048 bits. (L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.) • **Digest (Résumer)** - Sélectionnez l'algorithme **Digest (Résumer)** du certificat : **SHA1**, **SHA256**, **SHA384** ou **SHA512**. Si le pare-feu est en mode FIPS-CC, vous devez sélectionner **SHA256**, **SHA384** ou **SHA512** comme algorithme **Digest (Résumer)**.
Utiliser en tant que signature numérique	Sélectionnez cette option pour configurer le terminal afin d'utiliser la clé privée dans le certificat dans le but de valider une signature numérique.
Utiliser pour le chiffrement de la clé	Sélectionnez cette option pour configurer le terminal client afin d'utiliser la clé privée dans le certificat dans le but de crypter les données échangées par le biais de la connexion HTTPS établie avec les certificats générés par le serveur SCEP.
Empreinte du certificat de l'autorité de certification	(Facultatif) Pour garantir que le portail se connecte au bon serveur SCEP, saisissez la **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**. Vous pouvez obtenir cette empreinte auprès de l'interface du serveur SCEP dans le champ **Thumbprint (Empreinte numérique)**. Connectez-vous à l'interface utilisateur administrative du serveur SCEP (par exemple, à l'adresse http://<nom d'hôte ou adresse IP>/CertSrv/mscep_admin/). Copiez l'empreinte numérique et saisissez-la dans **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**.
Authentification SSL du serveur SCEP	Pour activer le protocole SSL, sélectionnez la racine **CA Certificate (Certificat AC)** pour le serveur SCEP. Vous pouvez activer l'authentification

© 2020 Palo Alto Networks, Inc.

Paramètres SCEP	Description
	SSL mutuelle entre le serveur SCEP et le portail GlobalProtect en sélectionnant **Client Certificate (Certificat client)**.

© 2020 Palo Alto Networks, Inc.

Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL

Visualiser et gérer les exclusions de déchiffrement SSL. Il existe deux types d'exclusions de déchiffrement, les exclusions prédéfinies et les exclusions personnalisées :

- Les exclusions de décodage prédéfinies permettent aux applications et aux services qui peuvent être interrompus de rester chiffré lorsque le pare-feu les déchiffre. Palo Alto Networks définit les exclusions de déchiffrement prédéfinies et fournit des mises à jour et des ajouts à la liste des exclusions prédéfinies à intervalles réguliers dans le cadre de la mise à jour des contenus des applications et des menaces. Les exclusions prédéfinies sont activées par défaut, mais vous pouvez choisir de désactiver l'exclusion si nécessaire.
- Vous pouvez créer des exclusions de déchiffrement personnalisées pour exclure le trafic du serveur du déchiffrement. Tout le trafic provenant ou destiné au serveur ciblé reste chiffré.



Vous pouvez également exclure le trafic du déchiffrement en fonction de l'application, de la source, de la destination, de la catégorie d'URL et du service.

Utilisez les paramètres de cette page pour Modifier ou ajouter une exclusion de déchiffrement et pour Gérer les exclusions de déchiffrement.

Paramètres des exclusions de déchiffrement SSL	Description
Modifier ou **Ajouter** une exclusion de déchiffrement	
Nom d'hôte	Saisissez un **Nom d'hôte** pour définir une exclusion de déchiffrement personnalisée. Le pare-feu compare le nom d'hôte à la SNI demandée par le client ou le CN présenté dans le certificat du serveur. Le pare-feu exclut du déchiffrement les sessions où le serveur présente un CN qui contient le domaine défini. Vous pouvez utiliser des astérisques (*) en tant que caractères génériques pour créer des exclusions de déchiffrement pour plusieurs noms d'hôte associés à un domaine. Les astérisques se comportent de la même façon que les carets (^) se comportent avec les exceptions de catégories URL : chaque astérisque indique un sous-domaine variable (étiquette) dans le nom d'hôte. Ceci vous permet de créer des exclusions aussi bien très spécifiques que très générales. Par exemple : • mail.*.com correspond à mail.company.com, mais ne correspond pas à mail.company.sso.com. • *.company.com correspond à tools.company.com, mais ne correspond pas à eng.tools.company.com. • *.*.company.com correspond à eng.tools.company.com, mais ne correspond pas à eng.company.com. • *.*.*.company.com correspond à corp.exec.mail.company.com, mais ne correspond pas à corp.mail.company.com. • mail.google.* correspond à mail.google.com, mais ne correspond pas à mail.google.uk.com.

© 2020 Palo Alto Networks, Inc.

Paramètres des exclusions de déchiffrement SSL	Description
	• mail.google.*.* correspond à mail.google.co.uk, mais ne correspond pas à mail.google.com. Par exemple, pour utiliser des caractères génériques pour exclure video-stats.video.google.com du décryptage, mais sans exclure video.google.com du décryptage, excluez *.*.google.com *Peu importe le nombre d'astérisques qui précèdent le nom d'hôte (sans une étiquette de caractère non générique qui précède le nom d'hôte), le nom d'hôte correspond à l'entrée. Par exemple, *.google.com, *.*.google.com et *.*.*.google.com correspondent tous à google.com. Cependant, *.dev.*.google.com ne correspond par à google.com, car une étiquette (dev) n'est pas un caractère générique.* Les noms d'hôtes doivent être uniques pour chaque saisie. Si une saisie prédéfinie fournie au pare-feu correspond à une saisie personnalisée existante, la saisie personnalisée est prioritaire. Vous ne pouvez pas modifier le Nom d'hôte pour une exclusion de déchiffrement prédéfinie.
Partagé	Sélectionnez **Partager** pour partager une exclusion de déchiffrement sur tous les systèmes virtuels dans un pare-feu à plusieurs systèmes virtuels. Alors que les exclusions de déchiffrement prédéfinies sont partagées par défaut, vous pouvez activer et désactiver les saisies prédéfinies et personnalisées pour un système virtuel spécifique.
Description	(Optionnel) Décrivez l'application que vous excluez du déchiffrement, y compris la raison pour laquelle l'application s'interrompt lors du déchiffrement.
Exclure	Exclure l'application du déchiffrement. Désactivez cette option pour commencer à déchiffrer une application précédemment exclue du déchiffrement.
Gestion des exclusions de déchiffrement	
Activer	Cliquez sur **Activer** une ou plusieurs saisies pour les exclure du déchiffrement.
Désactivation	Cliquez sur **Désactiver** une ou plusieurs exclusions de déchiffrement prédéfinies. Étant donné que les exclusions de déchiffrement identifient les applications qui s'interrompent lors du déchiffrement, la désactivation de l'une de ces saisies entraînera la non-prise en charge de l'application. Le pare-feu tentera de déchiffrer l'application et l'application s'interrompra. Vous pouvez utiliser cette option si vous souhaitez vous assurer que certaines applications chiffrées ne pénètrent pas sur votre réseau.

© 2020 Palo Alto Networks, Inc.

Paramètres des exclusions de déchiffrement SSL	Description
Afficher les données obsolètes	Cliquez sur **Afficher les données obsolètes** pour afficher les entrées prédéfinies que Palo Alto Networks ne définit plus comme des exclusions de déchiffrement. **En savoir plus sur les saisies obsolètes :** Les mises à jour des exclusions de décodage prédéfinies (y compris la suppression d'une saisie prédéfinie) sont envoyées au pare-feu dans le cadre des mises à jour du contenu des Applications et des Menaces. Les saisies prédéfinies et disposant de l'option **Exclure du déchiffrement** activée sont automatiquement supprimées de la liste des exclusions de déchiffrement SSL lorsque le pare-feu reçoit une mise à jour de contenu qui ne comporte plus cette saisie. Toutefois, les saisies prédéfinies avec l'option **Exclure du déchiffrement** désactivée restent dans la liste de déchiffrement SSL même si le pare-feu reçoit une mise à jour de contenu qui ne comporte plus cette saisie. Lorsque vous cliquez sur **Afficher les données obsolètes**, vous verrez que ces saisies prédéfinies désactivées ne sont pas appliquées à l'heure actuelle. Vous pouvez supprimer manuellement ces saisies si nécessaire.

© 2020 Palo Alto Networks, Inc.

Périphérique > Pages de réponse

Les pages de réponse personnalisées correspondent aux pages Web qui s'affichent lorsqu'un utilisateur tente d'accéder à une URL. Vous pouvez définir un message HTML personnalisé qui est téléchargé et affiché à la place de la page Web ou du fichier demandé.

Chaque système virtuel peut disposer de pages de réponse personnalisées propres. Le tableau suivant décrit les types de page de réponse personnalisée prenant en charge des messages personnalisés.

Types de page de réponse personnalisée	Description
Page de blocage de l'antivirus	Accès bloqué en raison d'une infection par un virus.
Page de blocage des applications	Accès bloqué, car l'application est bloquée par une règle de politique de Sécurité.
Page Confort du portail captif	Le pare-feu affiche cette page afin que les utilisateurs puissent saisir leurs informations d'identification de connexion pour accéder aux services qui sont soumis aux règles de politique d'authentification (voir Politiques > Authentification). Saisissez un message qui indique aux utilisateurs comment relever ce défi d'authentification. Le pare-feu authentifie les utilisateurs en fonction du **Profil d'authentification** indiqué dans l'objet d'application de l'authentification attribué à une règle d'authentification (voir Objets > Authentification). *Vous pouvez afficher des instructions d'authentification uniques pour chaque règle d'authentification en saisissant un Message dans l'objet d'application de l'authentification associé. Le message défini dans l'objet remplace le message défini sur la Page Confort du portail captif.*
Page de blocage du filtrage des données	Le contenu a été mis en correspondance avec un profil de filtrage des données et bloqué, parce que de l'information sensible a été détectée.
Page de poursuite du blocage des fichiers	Page destinée aux utilisateurs pour confirmer que le téléchargement doit se poursuivre. Cette option est disponible uniquement si la fonction de poursuite est activée dans le profil de sécurité. Sélectionnez Objets > Profils de sécurité > Blocage des fichiers.
Page de blocage des fichiers	Accès bloqué car l'accès au fichier est bloqué.
Page d'aide de l'application GlobalProtect	Page d'aide personnalisée destinée aux utilisateurs de GlobalProtect (accessible à partir du menu des paramètres de panneau d'état GlobalProtect).
Page de connexion du portail GlobalProtect	Page de connexion destinée aux utilisateurs tentant de s'authentifier à la page Web du portail GlobalProtect.
Page d'accueil du portail GlobalProtect	Page d'accueil destinée aux utilisateurs qui réussissent à s'authentifier à la page Web du portail GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Types de page de réponse personnalisée	Description
Page de bienvenue de l'application GlobalProtect	Page de bienvenue destinée aux utilisateurs qui réussissent à se connecter à GlobalProtect.
Page de connexion MFA	Le pare-feu affiche cette page afin que les utilisateurs puissent relever les défis d'authentification multifacteur (MFA) lorsqu'ils accèdent à des services qui sont soumis aux règles de politique d'authentification (voir Politiques > Authentification). Saisissez un message qui indique aux utilisateurs comment relever ce défi MFA.
Page d'erreur interne de l'authentification SAML	Page destinée à informer les utilisateurs que l'authentification SAML a échouée. La page contient un lien permettant à l'utilisateur de tenter une nouvelle authentification.
Page de notification des erreurs de certificat SSL	Notification indiquant qu'un certificat SSL a été révoqué.
Page d'exclusion de décryptage SSL	Page d'avertissement de l'utilisateur indiquant que le pare-feu décryptera les sessions SSL pour procéder à leur inspection.
Page de blocage du filtrage et des correspondances de catégories des URL	Accès bloqué par un profil de filtrage des URL ou parce que la catégorie d'URL est bloquée par une règle de politique de Sécurité.
Page de maintien et de contrôle prioritaire du filtrage des URL	Page incluant la politique de blocage initiale permettant aux utilisateurs d'ignorer le blocage. Par exemple, un utilisateur qui pense que la page a été bloquée de manière inappropriée peut cliquer sur **Continue (Continuer)** pour accéder à la page. Avec la page de contrôle prioritaire, un mot de passe est requis pour que l'utilisateur puisse avoir le contrôle prioritaire sur la politique bloquant cette URL. Reportez-vous à la section Contrôle prioritaire de l'URL par l'administrateur pour obtenir des instructions sur la définition du mot de passe de contrôle prioritaire.
Page de blocage de la mise en œuvre de la recherche sécurisée du filtrage des URL	Accès bloqué par une règle de politique de Sécurité dotée d'un profil de filtrage des URL pour lequel l'option **Mise en œuvre de la recherche sécurisée** est activée. Cette page est présentée à l'utilisateur si une recherche est effectuée à l'aide de Google, Bing, Yahoo, Yandex ou YouTube et que le paramètre de recherche sécurisée de son compte de moteur de recherche ou de navigateur n'est pas défini sur strict. La page de blocage invite l'utilisateur à définir les paramètres de recherche sécurisée sur Strict.
Page de blocage anti-hameçonnage	S'affiche aux utilisateurs lorsqu'ils tentent de saisir des informations d'identification d'entreprise valides (noms d'utilisateur ou mots de passe) sur une page Web sur laquelle l'envoi des informations d'identification est bloqué. L'utilisateur peut accéder au site, mais il ne peut toujours pas saisir des informations d'identification d'entreprise valides pour tous les formulaires Web associés.

© 2020 Palo Alto Networks, Inc.

Types de page de réponse personnalisée	Description
	Sélectionnez Objets > Profils de sécurité > Filtrage des URL pour activer la détection des informations d'identification et contrôler l'envoi des informations d'identification sur les pages Web en fonction de la catégorie d'URL.
Page de poursuite anti-hameçonnage	Cette page met en garde les utilisateurs contre la transmission des informations d'identification de l'entreprise (noms d'utilisateur et mots de passe) vers un site Web. La mise en garde des utilisateurs contre la transmission des informations d'identification peut les décourager de réutiliser les informations d'identification de l'entreprise et les informer sur les éventuelles tentatives d'hameçonnage. Les utilisateurs visualisent cette page lorsqu'ils tentent de saisir des informations d'identification sur un site pour lequel les autorisations d'**Envoi des informations d'identification de l'utilisateur** sont définies sur **continuer** (voir Objets > Profils de sécurité > Filtrage des URL). Ils doivent sélectionner **Continuer** pour saisir les informations d'identification sur le site.

Vous pouvez exécuter l'une des fonctions suivantes pour les **Response Pages (Pages de réponse)**.

- Pour importer une page de réponse HTML personnalisée, cliquez sur le lien du type de page que vous souhaitez modifier, puis cliquez sur Importer/Exporter. Recherchez la page. Un message indiquant si l'importation a abouti s'affiche. Pour que l'importation aboutisse, le fichier doit être au format HTML.
- Pour exporter une page de réponse HTML personnalisée, cliquez sur **Export (Exporter)** pour le type de page. Indiquez si le fichier doit être ouvert ou enregistré sur le disque, puis sélectionnez **lways use the same option (Toujours utiliser la même option)**, le cas échéant.
- Pour activer ou désactiver la page **Application Block (Blocage des applications)** ou les pages **SSL Decryption Opt-out (Exclusion de décryptage SSL)**, cliquez sur **Enable (Activer)** pour le type de page. Sélectionnez ou désélectionnez **Enable (Activer)**, le cas échéant.
- Pour utiliser la page de réponse par défaut au lieu de la page personnalisée précédemment chargée, supprimez la page de blocage personnalisée et validez. La page de blocage par défaut devient la nouvelle page active.

© 2020 Palo Alto Networks, Inc.

Périphérique > Paramètres des journaux

Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** pour configurer des alarmes, effacer des journaux ou activer le transfert des journaux à Panorama, au service de journalisation et aux services externes.

- Sélection des destinations du transfert des journaux
- Définition des paramètres d'alarme
- Effacer les journaux

Sélection des destinations du transfert des journaux

Device (Périphérique) > **Log Settings (Paramètres des journaux)**

La page Log Settings (Paramètres des journaux) vous permet de configurer le transfert des journaux vers :

- **Panorama, récepteurs de pièges SNMP, serveurs e-mail, serveurs Syslog et serveurs HTTP** : vous pouvez également ajouter ou supprimer des étiquettes à partir d'une adresse IP source ou de destination dans une entrée de journal ; tous les types de journaux, sauf les journaux Système et les journaux de Configuration prennent en charge l'étiquetage.
- **Service de journalisation** : si vous disposez d'un abonnement à un Service de journalisation et que vous avez activé le Service de journalisation (Périphérique > Configuration > Gestion), le pare-feu enverra alors les journaux au Service de journalisation lorsque vous configurez le transfert des journaux vers Panorama/le Service de journalisation. Panorama interrogera le Service de journalisation pour accéder aux journaux, pour afficher les journaux et pour générer des rapports.
- **Centre de sécurité Azure** : l'intégration au Centre de sécurité Azure est disponible pour les pare-feu VM-Series dans Azure.
  - Si vous avez lancé le pare-feu depuis le Centre de sécurité Azure, une règle de politique de sécurité contenant les profils de transfert des journaux est automatiquement activée pour vous.
  - Si vous avez lancé le pare-feu VM-Series à partir de la Place de marché Azure ou au moyen de modèles Azure personnalisés, vous devez sélectionnez manuellement **Azure-Security-Center-Integration (Intégration au Centre de sécurité Azure)** pour transférer les journaux système, les journaux User-ID et les journaux de correspondance HIP au Centre de sécurité Azure et utiliser le profil de transfert des journaux pour les autres types de journaux (voir Objets > Transfert des journaux).

    Le niveau gratuit du Centre de sécurité est automatiquement activé avec votre abonnement à Azure.

Vous pouvez transférer les types de journaux suivants : journaux Système, de Configuration, User-ID, de Correspondance HIP et journaux de Corrélation. Pour indiquer les destinations pour chaque type de journal, vous devez **Ajouter** un ou plusieurs profils de liste de correspondance (jusqu'à 64) et renseigner les champs décrits dans le tableau suivant.

Pour transférer les journaux de Trafic, de Menaces, d'envois WildFire, de Filtrage des URL, de Filtrage des données, d'Inspection des tunnels, de journaux GTP et de journaux d'Authentification, vous devez configurer un profil de Transfert des journaux (voir Objets > Transfert des journaux).

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de la liste de correspondance	Description
Name (Nom)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance. Un nom valide doit commencer par un caractère alphanumérique et peut contenir des zéros, des caractères alphanumériques, des traits de soulignement, des traits d'union, des points ou des espaces.
Filtre	Par défaut, le pare-feu transfère **All Logs (Tous les journaux)** du type pour lequel vous ajoutez le profil de liste de correspondance. Pour transférer un sous-ensemble de journaux, ouvrez le menu déroulant et sélectionnez un filtre existant ou sélectionnez **Filter Builder (Générateur de filtre)** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez le connecteur logique (ET/OU) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les attributs disponibles varient selon le type de journal. • **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les critères disponibles varient selon le type de journal. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. Pour afficher ou exporter les journaux auxquels correspond le filtre, sélectionnez **View Filtered Logs (Afficher les journaux filtrés)**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).  *Définissez le filtre pour le transfert des journaux pour tous les niveaux de gravité d'événement (le filtre par défaut est fixé sur All Logs [Tous les journaux]). Pour créer des méthodes de transfert des journaux distinctes pour différents niveaux de gravité, spécifiez un ou plusieurs niveaux de gravité dans le Filter (Filtre), configurez une Forward Method (Méthode de transfert), puis répétez le processus pour les autres niveaux de gravité.*
Description	Saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but de ce profil de liste de correspondance.
Panorama/Service de journalisation	Sélectionnez **Panorama/Logging Service (Panorama/Service de journalisation)** si vous souhaitez transmettre des journaux au Service de journalisation, aux collecteurs de journaux ou au serveur de gestion Panorama. Si vous activez cette option, vous devez configurer le transfert des journaux vers Panorama.

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de la liste de correspondance	Description
	Vous ne pouvez pas transférer les Journaux de corrélation du pare-feu à Panorama. Panorama génère des Journaux de corrélation en fonction des journaux provenant du pare-feu.
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).
Actions intégrées	Il existe deux types d'actions intégrées : • **Étiquetage** : vous pouvez ajouter une action pour tous les types de journaux qui incluent une adresse IP source ou de destination dans l'entrée de journal en configurant les paramètres suivants en fonction de vos besoins. *Vous pouvez identifier uniquement l'adresse IP source dans les journaux de Corrélation et les journaux de Correspondance HIP. Vous ne pouvez configurer aucune action pour les journaux Système et les journaux de Configuration parce que le type de journal n'inclut pas une adresse IP dans l'entrée de journal.* • Cliquez pour **Add (Ajouter)** une action et saisissez un nom pour la décrire. • Sélectionnez l'adresse IP que vous souhaitez étiqueter automatiquement (**Source Address (Adresse source)** ou **Destination Address (Adresse de destination)**). • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez enregistrer l'adresse IP et étiqueter le mappage sur l'agent **Local User-ID (User-ID local)** sur ce pare-feu ou Panorama, ou sur un agent **Remote User-ID (User-ID à distance)**. • Pour enregistrer l'adresse IP et étiqueter le mappage sur un agent **User-ID à distance**, sélectionnez le profil de serveur HTTP (Périphérique > Profils de serveur > HTTP) qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/étiquette est maintenu. Si vous définissez le délai sur 0,

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de la liste de correspondance	Description
	le mappage de l'indicateur d'adresse IP n'expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l'action Add Tag (Ajouter une étiquette).* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination. • **Intégration** : disponible uniquement pour les pare-feu VM-Series dans Azure. **Add (Ajoutez)** un nom et utilisez cette action pour transférer les journaux sélectionnés au Centre de sécurité Azure. Si cette option ne s'affiche pas, il se peut que votre abonnement à Azure ne vous autorise pas à utiliser le Centre de sécurité Azure.

Définition des paramètres d'alarme

- Périphérique > Paramètres des journaux

Utilisez les Paramètres d'alarme pour configurer Alarmes pour la CLI et l'interface Web. Vous pouvez configurer les notifications pour les événements suivants :

- Une règle de sécurité (ou un groupe de règles) correspondait à un seuil spécifié et était comprise dans un intervalle de temps spécifié.
- Le seuil d'échecs de cryptage/décryptage est atteint.
- La base de données de journaux pour chaque type de journal est quasiment pleine ; le quota par défaut est défini pour envoyer une notification lorsque 90 % de l'espace disque disponible est utilisé. La configuration d'alarmes vous permet d'entreprendre une action lorsque le disque est plein, et les journaux sont supprimés.

Lorsque vous activez des alarmes, vous pouvez afficher la liste actuelle en cliquant sur **Alarmes** ( ) en bas de l'interface Web.

Pour ajouter une alarme, modifiez les Paramètres d'alarme qui sont décrits dans le tableau suivant.

Paramètres du journal des alarmes	Description
Activer les alarmes	Les alarmes ne sont visibles que si vous cliquez sur **Activer les alarmes**. *Si vous désactivez les alarmes, le pare-feu ne vous informe pas des événements critiques qui nécessitent une action. Par exemple, une alarme vous indique quand la clé principale est sur le point d'expirer. Si la clé expire avant que vous ne la modifiiez, le pare-feu redémarre en mode Maintenance et requiert une réinitialisation d'usine.*
Activer les notifications d'alarme CLI	Activez les notifications d'alarme CLI lorsque des alarmes se produisent.

© 2020 Palo Alto Networks, Inc.

Paramètres du journal des alarmes	Description
Activer les notifications d'alarme Web	Ouvrez une fenêtre pour afficher les alarmes de sessions utilisateur, notamment lorsqu'elles se produisent et lorsqu'elles sont reçues.
Activer les alarmes sonores	Une tonalité d'alarme sonore retentira toutes les 15 secondes sur l'ordinateur de l'administrateur lorsque l'administrateur est connecté à l'interface Web et que des alarmes ne sont pas acquittées. La tonalité d'alarme retentira jusqu'à ce que l'administrateur acquitte toutes les alarmes. Pour afficher et acquitter les alarmes, cliquez sur **Alarms (Alarmes)**. Cette fonction est disponible uniquement lorsque le pare-feu est en mode FIPS-CC.
Seuil d'échec du cryptage/décryptage	Indiquez le nombre d'échecs de cryptage/décryptage après lequel une alarme est déclenchée.
<*Type de journal* > Base de données du journal	Générez une alarme lorsqu'une base de données de journaux atteint le pourcentage de taille maximale indiqué.
Seuil des violations de sécurité / Intervalle temporel des violations de sécurité	Une alarme est générée si une adresse IP ou un port spécifique correspond à une règle de refus le nombre de fois défini dans le paramètre **Seuil des violations de sécurité** sur la période (en secondes) indiquée dans le paramètre **Intervalle temporel des violations de sécurité**.
Seuil des violations / Intervalle temporel des violations / Etiquettes de stratégies de sécurité	Une alarme est générée si l'ensemble de règles atteint le nombre de limites de violations de règle spécifié dans le champ **Violations Threshold (Seuil des violations de sécurité)** sur la période indiquée dans le champ **Violations Time Period (Intervalle temporel des violations de sécurité)**. Les violations sont comptabilisées lorsqu'une session correspond à une politique de refus. Utilisez des **Security Policy Tags (Étiquettes de politique de sécurité)** pour préciser les tags pour lesquelles les seuils de violations généreront des alarmes. Ces étiquettes peuvent être définies lors de la définition des politiques de sécurité.
Audit sélectif	Les options d'audit sélectif sont disponibles uniquement lorsque le pare-feu est en mode FIPS-CC. Définissez les paramètres suivants : • **FIPS-CC Specific Logging (Journalisation spécifique FIPS-CC)** : active la journalisation verbose requise pour la conformité aux Critères communs (CC). • **Packet Drop Logging (Journalisation des paquets supprimés)** : consigne les paquets supprimés par le pare-feu. • **Suppress Login Success Logging (Interdiction de la journalisation des réussites d'ouverture de session)** : cesse de consigner les connexions administrateur réussies au pare-feu. • **Suppress Login Failure Logging (Interdiction de la journalisation des échecs d'ouverture de session)** : cesse de consigner les connexions administrateur échouées au pare-feu.

© 2020 Palo Alto Networks, Inc.

Paramètres du journal des alarmes	Description
	• **TLS Session Logging (Journalisation des sessions TLS)** : consigne les ouvertures de sessions TLS. • **CA (OCSP/CRL) Session Establishment Logging (Journalisation des ouvertures de session AC (OCSP/CRL))** : consigne les ouvertures de session entre le pare-feu et une autorité de certification lorsque le pare-feu envoie une requête de vérification de l'état de révocation de certificat en utilisant le protocole OCSP (Online Certificate Status Protocol) ou une demande de serveur CRL (liste de révocation du certificat). (Cette option est désactivée par défaut.) • **IKE Session Establishment Logging (Journalisation d'ouvertures de session IKE)** : consigne les ouvertures de session IKE IPSec lorsque la passerelle VPN du pare-feu s'authentifie auprès d'un homologue. L'homologue peut être un pare-feu Palo Alto Networks ou un autre périphérique de sécurité utilisé pour initier et mettre fin à des connexions VPN. Le nom de l'interface qui est spécifié dans le journal est l'interface qui est liée à la passerelle IKE. Le nom de la passerelle IKE est également affiché, le cas échéant. La désactivation de cette option arrête la journalisation de tous les événements de journalisation IKE. (Cette option est activée par défaut.) • **Suppressed Administrators (Administrateurs interdits)** : cesse la journalisation des modifications apportées à la configuration du pare-feu par les administrateurs répertoriés.

Effacer les journaux

- Périphérique > Paramètres des journaux

Vous pouvez effacer les journaux sur le pare-feu lorsque vous cliquez sur Gérer les journaux à la page Paramètres des journaux. Cliquez sur le type de journal que vous souhaitez effacer et cliquez sur **Oui** pour confirmer la demande.

Pour supprimer automatiquement les journaux et les rapports, vous pouvez configurer les périodes d'expiration. Pour plus d'informations, reportez-vous à la section Paramètres de journalisation et de génération de rapports.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur

Les rubriques suivantes décrivent les paramètres du profil de serveur que vous pouvez configurer sur le pare-feu :

- Périphérique > Profils de serveur > Piège'A0;SNMP
- Périphérique > Profils de serveur > Syslog
- Périphérique > Profils de serveur > Messagerie
- Périphérique > Profils de serveur > HTTP
- Périphérique > Profils de serveur > NetFlow
- Périphérique > Profils de serveur > RADIUS
- Périphérique > Profils de serveur > TACACS+
- Périphérique > Profils de serveur > LDAP
- Périphérique > Profils de serveur > Kerberos
- Périphérique > Profils de serveur > Fournisseur d'identité SAML
- Périphérique > Profils de serveur > DNS
- Périphérique > Profils de serveur > Authentification multifacteur

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Piège'A0;SNMP

SNMP (Simple Network Management Protocol) est un protocole standard permettant la surveillance des périphériques sur votre réseau. Pour vous informer d'événements système ou de menaces sur votre réseau, les périphériques surveillés envoient des pièges SNMP aux gestionnaires SNMP (serveurs de pièges). Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SNMP Trap (Piège SNMP)** ou **Panorama** > **Server Profiles (Profils de serveur)** > **SNMP Trap (Piège SNMP)** pour configurer le profil de serveur autorisant le pare-feu ou Panorama à envoyer des pièges aux gestionnaires SNMP. Pour activer les messages SNMP GET (requêtes de statistiques d'un gestionnaire SNMP), reportez-vous à la section Activation de la surveillance SNMP.

Après avoir créé le profil de serveur, vous devez préciser les types de journaux pour lesquels le pare-feu enverra des pièges SNMP (voir Périphérique > Paramètres des journaux). Pour obtenir la liste des MIB que vous devez charger dans le gestionnaire SNMP afin qu'il puisse interpréter les pièges, reportez-vous à MIB pris en charge.

ne supprimez pas un profil de serveur utilisé par un quelconque paramètre de journal système ou profil de journalisation.

Paramètres du profil de serveur de pièges SNMP	Description
Name (Nom)	Saisissez un nom pour le profil SNMP (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Version	Sélectionnez la version de SNMP : **V2c** (par défaut) ou **V3**. Votre sélection détermine les autres champs affichés dans la boîte de dialogue. Pour ces deux versions, vous pouvez ajouter jusqu'à quatre gestionnaires SNMP. *Utilisez SNMPv3, qui fournit l'authentification et d'autres fonctions pour garantir la sécurité des connexions réseau.*
Pour SNMP V2c	
Name (Nom)	Donnez un nom au gestionnaire SNMP. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union.
Gestionnaire SNMP	Indiquez le nom de domaine complet ou l'adresse IP du gestionnaire SNMP.

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de serveur de pièges SNMP	Description
Communauté	Saisissez la chaîne de communauté qui identifie une *communauté* SNMP composée de gestionnaires SNMP et de périphériques surveillés, et qui sert également de mot de passe pour authentifier les membres de la communauté entre eux lors du transfert de pièges. La chaîne peut comporter 127 caractères maximum, accepte tous les caractères et est sensible à la casse.  *N'utilisez pas la chaîne de communauté publique définie par défaut (ne définissez pas la chaîne de communauté sur public [publique] ou private [privée]). Utilisez des chaînes de communauté uniques, qui évitent les conflits si vous utilisez plusieurs services SNMP. Les messages SNMP contenant des chaînes de communautés en clair, tenez compte des exigences de sécurité de votre réseau lors de la définition de l'appartenance à la communauté (accès administrateur).*
Pour SNMP V3	
Name (Nom)	Donnez un nom au gestionnaire SNMP. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union.
Gestionnaire SNMP	Indiquez le nom de domaine complet ou l'adresse IP du gestionnaire SNMP.
Utilisateur	Saisissez un nom d'utilisateur pour identifier le compte utilisateur SNMP (31 caractères maximum). Le nom d'utilisateur que vous configurez sur le pare-feu doit correspondre au nom d'utilisateur configuré sur le gestionnaire SNMP.
IdMoteur	Précisez l'ID du moteur du pare-feu. Lorsqu'un gestionnaire SNMP et le pare-feu s'authentifient entre eux, les messages de pièges utilisent cette valeur pour identifier le pare-feu de manière unique. Si vous ne renseignez pas ce champ, les messages utilisent le numéro de série du pare-feu pour l'**EngineID (ID du moteur)**. Si vous saisissez une valeur, elle doit être au format hexadécimal, préfixée par 0x et comporter entre 10 et 128 caractères supplémentaires pour représenter n'importe quel nombre de 5 à 64 octets (2 caractères par octet). Pour les pare-feu d'une configuration haute disponibilité (HD), ne renseignez pas le champ pour que le gestionnaire SNMP puisse identifier l'homologue HD qui a envoyé les pièges ; sinon, la valeur est synchronisée et les deux homologues utiliseront le même **EngineID (ID du moteur)**.
Mot de passe d'authentification	Indiquez le mot de passe d'authentification de l'utilisateur SNMP. Le pare-feu utilise le mot de passe pour s'authentifier sur le gestionnaire SNMP. Le pare-feu utilise l'algorithme Secure Hash Algorithm (SHA-1 160) pour chiffrer le mot de passe. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de serveur de pièges SNMP	Description
Mot de passe privé	Indiquez le mot de passe privé de l'utilisateur SNMP. Le pare-feu utilise le mot de passe et la norme Advanced Encryption Standard (AES-128) pour crypter les pièges SNMP. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Syslog

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveurs)** > **Syslog** ou **Panorama** > **Server Profiles (Profils de serveurs)** > **Syslog** pour configurer un profil de serveur pour transmettre les journaux de pare-feu, les journaux Panorama et les journaux de Collecteur de journaux en tant que messages Syslog vers un serveur Syslog. Pour définir un profil de serveur Syslog, cliquez sur **Add (Ajouter)** et remplissez les champs Nouveau serveur Syslog.

- *Pour sélectionner le profil du serveur Syslog pour les journaux Système, de Configuration, de User-ID, de Correspondance HIP et de Corrélation, voir* Périphérique > Paramètres des journaux.
- *Pour sélectionner le profil de serveur Syslog pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage de données, d'inspection des tunnels, d'authentification et de GTP, voir* Objets > Transfert des journaux.
- *Vous ne pouvez pas supprimer un profil de serveur utilisé par le pare-feu dans des paramètres du journal système ou de configuration, ou des profils de journalisation.*

Paramètres du serveur Syslog	Description
Name (Nom)	Saisissez un nom pour le profil Syslog (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Onglet Serveurs	
Name (Nom)	Cliquez sur **Add (Ajouter)** et saisissez un nom pour le serveur Syslog (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Serveur	Saisissez l'adresse IP ou le nom de domaine complet du serveur syslog.
Transport	Indiquez si les messages'A0;Syslog doivent être transportés sur UDP, TCP ou SSL. *Utilisez SSL pour chiffrer et sécuriser les données envoyées à un serveur syslog. Les données sont envoyées via UDP ou TCP en texte en clair et sont lisibles dans le transit.*

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur Syslog	Description
Port	Saisissez le numéro de port du serveur Syslog (le port standard pour UDP est 514 ; le port standard pour SSL est 6514 ; pour TCP, vous devez indiquer un numéro de port).
Format	Indiquez le format'A0;Syslog à utiliser'A0;: BSD (par défaut) ou IETF.
Installation	Sélectionnez l'une des valeurs Syslog standard. Sélectionnez la valeur correspondant à la manière selon laquelle votre serveur Syslog utilise le champ de la fonctionnalité pour gérer les messages. Pour plus d'informations sur le champ de la fonctionnalité, reportez-vous à RFC 3164 (format BSD) ou RFC 5424 (format IETF).
Onglet Format de journal personnalisé	
Type de journal	Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé. Dans la boîte de dialogue, cliquez sur un champ pour l'ajouter à la zone du format de journal. D'autres chaînes de texte peuvent être modifiées directement dans la zone du format de journal. Cliquez sur **OK** pour enregistrer les paramètres. Consultez une description de chaque champ pouvant être utilisé pour les journaux personnalisés. Pour plus d'informations sur les champs pouvant être utilisés pour les journaux personnalisés, voir Périphérique > Profils de serveur > E-mail.
Échappement	Indiquez des séquences d'échappement. **Escaped characters (Caractères d'échappement)** est une liste de tous les caractères d'échappement sans espaces.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Messagerie

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveurs)** > **Email (Messagerie)** ou **Panorama** > **Server Profiles (Profils de serveurs)** > **Email (Messagerie)** pour configurer un profil de serveur pour transmettre des journaux en tant que notifications par courrier électronique. Pour définir un profil de serveur de messagerie, cliquez sur **Add (Ajouter)** un profil et indiquez les paramètres de notification par courrier électronique.

- *Pour sélectionner le profil du serveur Syslog pour les journaux Système, de Configuration, de User-ID, de Correspondance HIP et de Corrélation, voir* Périphérique > Paramètres des journaux.
- *Pour sélectionner le profil de serveur Syslog pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage de données, d'inspection des tunnels, d'authentification et de GTP, voir* Objets > Transfert des journaux.
- *Vous pouvez également consulter* Surveillance > Rapports au format PDF > Planificateur de messagerie.
- *Vous ne pouvez pas supprimer un profil de serveur utilisé par le pare-feu dans des paramètres du journal système ou de configuration, ou des profils de journalisation.*

Paramètres de notification par courrier électronique	Description
Name (Nom)	Saisissez un nom pour le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Onglet Serveurs	
Serveur	Saisissez un nom pour identifier le serveur (31 caractères maximum). Ce champ est un simple intitulé et ne doit pas comporter le nom d'hôte d'un serveur'A0;SMTP existant.
Nom affichage	Saisissez le nom indiqué dans le champ **From (De)** du courrier électronique.
De	Saisissez l'adresse électronique Source, par exemple alerte_securite@societe.com.
A	Saisissez l'adresse électronique du destinataire.
Destinataires supplémentaires	Facultativement, saisissez l'adresse électronique d'un autre destinataire. Vous ne pouvez ajouter qu'un seul destinataire supplémentaire. Pour

© 2020 Palo Alto Networks, Inc.

Paramètres de notification par courrier électronique	Description
	ajouter plusieurs destinataires, saisissez l'adresse e-mail d'une liste de distribution.
Passerelle	Saisissez l'adresse'A0;IP ou le nom d'hôte du serveur SMTP (Simple Mail Transport Protocol) utilisé pour envoyer le courrier électronique.
Onglet Format de journal personnalisé	
Type de journal	Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé. Dans la boîte de dialogue, cliquez sur un champ pour l'ajouter à la zone du format de journal. Cliquez sur **OK** pour enregistrer les paramètres.
Échappement	Autorisez les caractères d'échappement et indiquez le ou les caractères d'échappement.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > HTTP

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveurs)** > **HTTP** ou **Panorama** > **Server Profiles (Profils de serveurs)** > **HTTP** pour configurer un profil de serveur pour transmettre des journaux. Vous pouvez configurer le pare-feu pour transférer des journaux vers une destination HTTP(S) ou pour l'intégrer à un service HTTP qui expose une API et vous pouvez modifier l'URL, l'en-tête HTTP, les paramètres et la charge utile dans la requête HTTP pour répondre à vos besoins. Vous pouvez également utiliser le profil de serveur HTTP pour accéder aux pare-feu exécutant l'agent User-ID intégré à PAN-OS et enregistrer une ou plusieurs étiquettes sur une adresse IP source ou de destination sur les journaux générés par un pare-feu.



Pour utiliser le profil de serveur HTTP pour transférer les journaux :

- *Voir Périphérique > Paramètres du journal pour les journaux du système, de configuration, d'User-ID, de correspondance HIP et de corrélation.*
- *Voir Objets > Transfert de journaux pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage des données, d'inspection des tunnels, d'authentification et de GTP.*

Vous ne pouvez pas supprimer un profil de serveur HTTP s'il est utilisé pour transférer des journaux. Pour supprimer un profil de serveur sur le pare-feu ou Panorama, vous devez supprimer toutes les références au profil à partir du profil Device (Périphérique) > Log settings (Paramètres du journal) ou Objects (Objets) > Log Forwarding (Transfert des journaux).

Pour définir un profil de serveur HTTP, cliquez sur **Add (Ajouter)** un nouveau profil et configurez les paramètres dans le tableau suivant.

Paramètres du serveur HTTP	Description
Name (Nom)	Saisissez un nom pour le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Un nom valide doit commencer par un caractère alphanumérique et peut contenir des zéros, des caractères alphanumériques, des traits de soulignement, des traits d'union, des points ou des espaces.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil de serveur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer le **Location (Emplacement)**.
Enregistrement des balises	L'enregistrement des étiquettes vous permet d'ajouter ou de supprimer une étiquette sur une adresse IP source ou de destination dans une entrée de journal et d'enregistrer l'adresse IP et le mappage des étiquettes sur l'agent User-ID sur un pare-feu utilisant une adresse HTTP(S). Vous pouvez ensuite définir des groupes d'adresses dynamiques qui utilisent ces étiquettes comme critères de filtrage pour déterminer leurs membres et appliquer les règles de politique à une adresse IP en fonction des étiquettes.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur HTTP	Description
	Cliquez pour **Ajouter** les détails de connexion pour activer l'accès HTTP(S) à l'agent User-ID sur un pare-feu. Pour enregistrer des étiquettes sur l'agent User-ID de Panorama, vous n'avez pas besoin d'un profil de serveur. En outre, vous ne pouvez pas utiliser le profil de serveur HTTP pour enregistrer des étiquettes dans un agent User-ID exécuté sur un serveur Windows.
Onglet Serveurs	
Name (Nom)	Cliquez pour **Ajouter** un serveur HTTP(s) et saisissez un nom (jusqu'à 31 caractères) ou un agent User-ID distant. Un nom valide doit être unique et doit commencer par un caractère alphanumérique. Le nom peut contenir des zéros, des caractères alphanumériques, des tirets bas, des traits d'union, des points ou des espaces. Un profil de serveur peut inclure jusqu'à quatre serveurs.
Adresse	Saisissez l'adresse IP du ou des serveurs HTTP. En ce qui concerne l'enregistrement des étiquettes, indiquez l'adresse IP sur le pare-feu configuré en tant qu'agent User-ID.
Protocole	Sélectionnez le protocole : HTTP ou HTTPS.
Port	Saisissez le numéro de port sur lequel il est possible d'accéder au serveur ou au pare-feu. Le port 80 est le port par défaut utilisé pour HTTP, tandis que pour HTTPS il s'agit du port 443. Pour l'enregistrement des étiquettes, le pare-feu utilise HTTP ou HTTPS pour se connecter au serveur Web sur les pare-feu qui sont configurés en tant qu'agents User-ID.
TLS Version (Version TLS)	Sélectionnez la TLS Version (Version TLS) prise en charge par le protocole SSL sur le serveur : La valeur par défaut est de **1.2**.
Profil du certificat	Sélectionnez le profil de certificat à utiliser pour la connexion TLS avec le serveur. Le pare-feu utilisera le profil de certificat spécifié pour valider le certificat du serveur lors de l'établissement d'une connexion sécurisée au serveur.
Méthode HTTP	Sélectionnez la méthode HTTP que le serveur prend en charge. Les options sont GET, PUT, POST (par défaut) et DELETE. Pour l'agent User-ID, utilisez la méthode GET.
Username (Nom d'utilisateur)	Saisissez le nom d'utilisateur qui a des autorisations d'accès pour réaliser la méthode HTTP que vous avez sélectionnée. Si vous enregistrez des étiquettes de l'agent User-ID sur un pare-feu, le nom d'utilisateur doit être celui d'un administrateur ayant un rôle de super utilisateur.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur HTTP	Description
Mot de passe	Saisissez le mot de passe pour vous authentifier sur le serveur ou sur le pare-feu.
Tester la connexion au serveur	Sélectionnez un serveur et cliquez sur **Test Server Connection (Tester la connexion au serveur)** pour tester la connectivité réseau au serveur. Ce test ne teste pas la connectivité d'un serveur qui exécute l'agent User-ID.
Onglet Format de la charge utile	
Type de journal	Le type de journal disponible pour le transfert HTTP s'affiche. Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé.
Format	S'affiche si le type de journal utilise le format par défaut, un format prédéfini ou un format de charge utile personnalisé que vous avez défini.
Formats prédéfinis	Sélectionnez le format qui sera utilisé pour le transfert de journaux pour votre service ou votre fournisseur. Les formats prédéfinis sont affichés à l'aide de mises à jour de contenu et peuvent être modifiés chaque fois que vous installez une nouvelle mise à jour de contenu sur le pare-feu ou sur Panorama.
Name (Nom)	Saisissez un nom pour le format de journal personnalisé.
Format de l'URI	Indiquez la ressource à laquelle vous souhaitez envoyer des journaux en utilisant HTTP(S). Si vous créez un format personnalisé, l'**URI (URI)** est le terminal de ressource pour le service HTTP. Le pare-feu ajoute l'URI à l'adresse IP que vous avez définie précédemment pour construire l'URL de la requête HTTP. Assurez-vous que le format de l'URI et de la charge utile correspond à la syntaxe requise par votre fournisseur tiers. Vous pouvez utiliser n'importe quel attribut pris en charge sur le type de journal sélectionné dans l'en-tête HTTP, les paramètres, les paires de valeurs et la charge utile requise.
En-têtes HTTP	Ajoutez un en-tête et sa valeur correspondante.
par le fournisseur	Indiquez les paramètres optionnels et les valeurs.
Charge utile	Sélectionnez les attributs de journal que vous souhaitez inclure en tant que charge utile dans le message HTTP pour le serveur Web externe.
Envoyer le journal de test	Cliquez sur ce bouton pour valider le fait que le serveur Web externe reçoit la demande et la charge utile au bon format.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > NetFlow

Les pare-feu de Palo Alto Networks peuvent exporter des statistiques sur le trafic IP sur leurs interfaces sous forme de champs NetFlow vers un collecteur NetFlow. Le collecteur NetFlow est un serveur que vous utilisez pour analyser le trafic réseau pour la sécurité, l'administration, la comptabilité et le dépannage. Tous les pare-feu de Palo Alto Networks prennent en charge la version 9 de NetFlow. Les pare-feu ne prennent en charge que le protocole NetFlow unidirectionnel, et non bidirectionnel. Les pare-feu effectuent le traitement de NetFlow sur tous les paquets IP des interfaces et ne prennent pas en charge le NetFlow échantillonné. Vous pouvez exporter des enregistrements NetFlow pour les interfaces Niveau3, Niveau 2, câble virtuel, tap, VLAN, loopback et tunnel. Pour les interfaces Ethernet agrégées, vous pouvez exporter des enregistrements pour le groupe agrégé, mais pas pour les interfaces individuelles dans le groupe. Les pare-feu prennent en charge les modèles NetFlow standards et d'entreprise (propres à PAN-OS), qui sont utilisés par les collecteurs NetFlow pour déchiffrer les champs NetFlow. Les pare-feu choisissent un modèle en fonction du type de données exportées : trafic IPv4 ou IPv6, avec ou sans NAT, et avec des champs standard ou entreprise.

Pour configurer les exportations NetFlow, vous devez **Ajouter** un profil de serveur NetFlow pour indiquer les serveurs NetFlow qui recevront les données exportées et pour spécifier les paramètres d'exportation. Après avoir affecté le profil à une interface (voir Réseau > Interfaces), le pare-feu exporte les données NetFlow pour l'ensemble du trafic passant par cette interface vers les serveurs spécifiés.

Paramètres de Netflow	Description
Name (Nom)	Saisissez un nom pour le profil Netflow (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Taux de rafraîchissement du modèle	Le pare-feu actualise régulièrement les modèles NetFlow pour réévaluer le modèle à utiliser (en cas de changement du type de données exportées) et pour appliquer les modifications nécessaires aux champs du modèle sélectionné. Indiquez la fréquence à laquelle le pare-feu actualise les modèles NetFlow en **Minutes** (la plage est comprise entre 1 et 3 600, la valeur par défaut est de 30) et en **Paquets** (pour les enregistrements exportés, la plage est comprise entre 1 et 600, la valeur par défaut est 20), selon les exigences de votre collecteur NetFlow. Le pare-feu actualise le modèle après que le seuil soit dépassé. Le taux de rafraîchissement requis dépend du collecteur NetFlow. Si vous ajoutez plusieurs collecteurs'A0;NetFlow au profil de serveur, utilisez la valeur du collecteur dont le taux de rafraîchissement est le plus élevé.
Délai d'activation	Indiquez la fréquence (en minutes) à laquelle le pare-feu exporte les enregistrements de données pour chaque session (plage de 1 à 60 ; par défaut 5). Définissez cette fréquence en fonction de la fréquence à laquelle vous souhaitez que le collecteur'A0;NetFlow mette à jour les statistiques du trafic.
Types de champs PAN-OS	Exportez des champs spécifiques à PAN-OS pour l'App-ID et le service User-ID dans des enregistrements Netflow.
Serveurs	

© 2020 Palo Alto Networks, Inc.

Paramètres de Netflow	Description
Name (Nom)	Indiquez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Serveur	Saisissez le nom d'hôte ou l'adresse IP du serveur. Vous pouvez ajouter deux serveurs maximum par profil.
Port	Indiquez le numéro de port d'accès au serveur (par défaut 2 055).

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > RADIUS

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveurs)** > **RADIUS** ou **Panorama** > **Server Profiles (Profils de serveurs)** > **RADIUS** pour configurer les paramètres des serveurs Remote Authentication Dial-In User Service (Service d'authentification d'usager distant ; RADIUS) auxquels les profils d'authentification font référence (voir Périphérique > Profil d'authentification). Vous pouvez utiliser RADIUS pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail captif), pour authentifier les administrateurs définis localement sur le pare-feu ou sur Panorama et pour authentifier et autoriser les administrateurs définis en externe sur le serveur RADIUS.

Paramètres du serveur RADIUS	Description
Nom du profil	Saisissez un nom pour identifier le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Location (Emplacement)** est **Shared (Partagé)**.
délai d'expiration	Saisissez un intervalle, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 30 ; par défaut 3). *Si vous utilisez le profil du serveur RADIUS pour intégrer le pare-feu avec un service MFA, indiquez un intervalle qui donne aux utilisateurs suffisamment de temps pour répondre à la demande d'authentification. Par exemple, si le service MFA demande un One-Time Password (Mot de passe à usage unique ; OTP), les utilisateurs ont besoin de temps pour visualiser l'OTP sur leur périphérique final, puis pour saisir l'OTP sur la page de connexion MFA.*
Protocole d'authentification	Sélectionnez le **Authentication Protocol (Protocole d'authentification)** que le pare-feu utilise pour sécuriser une connexion au serveur RADIUS : • **PEAP-MSCHAPv2** : (Par défaut) Protected EAP et protocole MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol) offre une sécurité accrue par rapport au protocole PAP ou CHAP en transmettant le nom d'utilisateur et le mot de passe dans un tunnel crypté.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur RADIUS	Description
	• **PEAP with GTC (PEAP-GTC)** : sélectionnez Protected EAP (PEAP) avec la Generic Token Card (carte à jeton générique ; GTC) pour utiliser des jetons à usage unique dans un tunnel crypté. • **EAP-TTLS with PAP (EAP-TTLS avec PAP)** : sélectionnez EAP avec TTLS (Tunneled Transport Layer Security) et le protocole PAP pour transporter des identifiants en texte claire pour l'autorisation PAP dans un tunnel crypté. • **Chap** : sélectionnez le protocole CHAP (Challenge-Handshake Authentication Protocol) si le serveur RADIUS ne prend pas en charge le protocole EAP ou PAP ou s'il n'est pas configuré pour celui-ci. • **PAP** : sélectionnez le protocole PAP (Password Authentication Protocol) si le serveur RADIUS ne prend pas en charge le protocole EAP ou CHAP ou s'il n'est pas configuré pour celui-ci.
Autorisez les utilisateurs à modifier les mots de passe après leur expiration.	(PEAP-MSCHAPv2 et GlobalProtect 4.1 ou version ultérieure) : sélectionnez cette option pour autoriser les utilisateurs de GlobalProtect à modifier leurs mots de passe expirés.
Rendre l'identité externe anonyme	(PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP) Cette option est activée par défaut pour assurer l'anonymat de l'identité de l'utilisateur dans le tunnel externe que le pare-feu crée après s'être authentifié auprès du serveur. *Certaines configurations du serveur Radius pourraient ne pas prendre en charge les ID externes anonymes, vous pourriez donc devoir décocher cette option. Lorsqu'elle est décochée, les noms d'utilisateur sont transmis en texte clair.*
Profil du certificat	(PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP) Sélectionnez ou configurez un Profil de certificat à associer à un profil de serveur RADIUS. Le pare-feu utilise le Profil du certificat pour s'authentifier auprès du serveur RADIUS.
Relances	Précisez le nombre de nouvelles tentatives après l'expiration du délai d'attente (plage de 1 à 5 ; valeur par défaut de 3).
Serveurs	Configurez les informations de chaque serveur dans l'ordre indiqué. • **Name (Nom)** - Saisissez un nom pour identifier le serveur. • **RADIUS Server (Serveur RADIUS)** - Saisissez l'adresse IP ou le nom de domaine complet du serveur. • **Secret/Confirm Secret (Secret/Confirmer le secret)** - Saisissez et confirmez une clé pour vérifier et chiffer la connexion entre le pare-feu et le serveur RADIUS. • **Port** - Saisissez le port du serveur (la plage est comprise entre 1 et 65 535 ; par défaut 1812) pour les requêtes d'authentification.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > TACACS+

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveurs)** > **TACACS+** ou **Panorama** > **Server Profiles (Profils de serveurs)** > **TACACS+** pour configurer les paramètres qui définissent la façon dont le pare-feu ou Panorama se connecte aux serveurs Terminal Access Controller Access-Control System Plus (TACACS+) (Voir Périphérique > Profil d'authentification). Vous pouvez utiliser TACACS+ pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail captif), pour authentifier les administrateurs définis localement sur le pare-feu ou sur Panorama et pour authentifier et autoriser les administrateurs définis en externe sur le serveur TACACS+.

Paramètres du serveur TACACS+	Description
Nom du profil	Saisissez un nom pour identifier le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu à plusieurs systèmes virtuels, cette option n'apparaît que si le **Location (Emplacement)** est **Shared (Partagé)**.
délai d'expiration	Saisissez un intervalle, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 30 ; par défaut 3).
Protocole d'authentification	Sélectionnez le **Authentication Protocol (Protocole d'authentification)** que le pare-feu utilise pour sécuriser une connexion au serveur TACACS+ : • **CHAP** – Le protocole CHAP (Challenge-Handshake Authentication Protocol) est le protocole qui est utilisé par défaut et qui est privilégié, car il est plus sécurisé que le protocole PAP. • **PAP** – Sélectionnez le protocole PAP (Password Authentication Protocol) si le serveur TACACS+ ne prend pas en charge le protocole CHAP ou s'il n'est pas configuré pour celui-ci. • **Auto** – Le pare-feu tente d'abord de s'authentifier à l'aide du protocole CHAP. Si le serveur TACACS+ ne répond pas, le pare-feu fait appel au protocole PAP.
Utiliser une simple connexion pour toutes les authentifications	Sélectionnez cette option pour utiliser la même session TCP pour toutes les authentifications. Cette option améliore la performance en empêchant le traitement requis d'ouvrir et de fermer une session TCP distincte pour chaque événement d'authentification.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur TACACS+	Description
Serveurs	Cliquez sur **Add (Ajouter)** et indiquez les paramètres suivants pour chaque serveur TACACS+ : • **Name (Nom)** - Saisissez un nom pour identifier le serveur. • **TACACS+ Server (Serveur TACACS+)** - Saisissez l'adresse IP ou le nom de domaine complet du serveur TACACS+. • **Secret/Confirm Secret (Secret/Confirmer le secret)** - Saisissez et confirmez une clé pour vérifier et crypter la connexion entre le pare-feu et le serveur TACACS+. • **Port** - Saisissez le port du serveur (par défaut 49) pour les requêtes d'authentification.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > LDAP

- **Device (Périphérique)** > **Server Profiles (Profil de serveur)** > **LDAP**
- **Panorama** > **Server Profiles (Profils de serveur)** > **LDAP**

Add (Ajoutez) ou sélectionnez un profil de serveur LDAP pour configurer les paramètres pour les serveurs Lightweight Directory Access Protocol (protocole allégé d'accès annuaire ; LDAP) auxquels les profils d'authentification font référence (voir Périphérique > Profil d'authentification). Vous pouvez utiliser LDAP pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail actif) et les administrateurs définis localement sur le pare-feu ou sur Panorama.

Paramètres du serveur LDAP	Description
Nom du profil	Saisissez un nom pour identifier le profil (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Location (Emplacement)** est **Shared (Partagé)**.
Utilisez ce profil pour effectuer la vérification du numéro de série	Sélectionnez cette option pour permettre à ce profil de serveur LDAP pour recueillir les numéros de série auprès des points de terminaison gérés. Ces informations sont utilisées par la passerelle et le portail GlobalProtect pour vérifier si le point de terminaison est géré (le numéro de série existe dans Active Directory) ou non.
Liste du serveur	Pour chaque serveur LDAP, **Add (Ajoutez)** un **Name (Nom)** d'hôte, l'adresse IP ou le nom de domaine complet (**LDAP Server (Serveur LDAP)**), ainsi que le **Port** (par défaut 389). *Configurez au moins deux serveurs LDAP pour fournir la redondance.*
Type	Choisissez le type de serveur dans le menu déroulant.
Base DN (ND de base)	Indiquez le contexte racine dans le serveur d'annuaires afin d'affiner la recherche d'informations d'utilisateur ou de groupe.
ND Bind	Indiquez le nom de connexion (nom distinctif) du serveur d'annuaires.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur LDAP	Description
	Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.
Mot de passe/ Confirmer le mot de passe	Indiquez le mot de passe du compte Bind. L'agent enregistre le mot de passe crypté dans le fichier de configuration.
Lier le délai d'attente	Indiquez l'heure limite (en secondes) imposée lors de la connexion au serveur d'annuaire (la plage est comprise entre 1 et 30 ; par défaut 30).
Délai d'attente de la recherche	Indiquez l'heure limite (en secondes) imposée lors de recherches d'annuaires (la plage est comprise entre 1 et 30 ; par défaut 30).
Intervalle de relance	Indiquez l'intervalle (en secondes) après lequel le système tente de se connecter au serveur LDAP après une tentative infructueuse précédente (plage de 1 à 3 600 secondes ; par défaut 60).
Exiger une connexion sécurisée SSL/TLS	Sélectionnez cette option si vous souhaitez que le pare-feu utilise SSL ou TLS pour les communications avec le serveur d'annuaires. Le protocole dépend du port du serveur : • 389 (par défaut) – TLS (le pare-feu utilise plus précisément la fonction Démarrer l'opération TLS, qui met à niveau la connexion en texte brut initiale en TLS.) • 636 : SSL. • Tout autre port : le pare-feu tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le pare-feu fera appel à SSL. *Cette option est recommandée, car elle accroît la sécurité et qu'elle est sélectionnée par défaut.*
Vérifier le certificat du serveur pour les sessions SSL	Sélectionnez cette option (décochée par défaut) si vous souhaitez que le pare-feu vérifie le certificat présenté par le serveur d'annuaires pour les connexions SSL/TLS. Le pare-feu vérifie deux aspects du certificat : • Le certificat est approuvé et valide. Pour que le pare-feu approuve le certificat, son autorité de certification (AC) racine et tous les certificats intermédiaires doivent se trouver dans le magasin de certificats sous **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**. • Le nom du certificat doit correspondre au **Name (Nom)** d'hôte du serveur LDAP. Le pare-feu vérifie tout d'abord la correspondance de l'attribut de certificat Autre nom de l'objet, puis l'attribut DN de l'objet. Si le certificat utilise le nom de domaine complet du serveur d'annuaires, vous devez utiliser le nom de domaine complet dans le champ **LDAP Server (Serveur LDAP)** pour que la correspondance du nom réussisse. Si la vérification échoue, la connexion échouera également. Pour activer cette vérification, vous devez également sélectionner **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur LDAP	Description
	 *Activez la vérification par le pare-feu du certificat du serveur pour les sessions SSL pour accroître la sécurité.*

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Kerberos

Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Kerberos** ou **Panorama** > **Server Profiles (Profils de serveur)** > **Kerberos** pour configurer un profil de serveur permettant aux utilisateurs de s'authentifier de manière native auprès d'un contrôleur de domaine Active Directory ou d'un serveur d'authentification compatible avec Kerberos V5. Après avoir configuré un profil de serveur Kerberos, vous pouvez l'affecter à un profil d'authentification (voir Périphérique > Profil d'authentification). Vous pouvez utiliser Kerberos pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail actif) et les administrateurs définis localement sur le pare-feu ou sur Panorama.

pour utiliser l'authentification Kerberos, votre serveur Kerberos dorsal doit être accessible via une adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.

Paramètres du serveur Kerberos	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Location (Emplacement)** est **Shared (Partagé)**.
Serveurs	Pour chaque serveur Kerberos, cliquez sur **Add (Ajouter)** et précisez les paramètres suivants : • **Name (Nom)** - Donnez un nom au serveur. • **Kerberos Server (Serveur Kerberos)** - Saisissez l'adresse IPv4 ou le nom de domaine complet du serveur. • **Port** - Saisissez un port facultatif (la plage est comprise entre 1 et 65 535 ; par défaut 88) pour les communications avec le serveur.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Fournisseur d'identité SAML

Utilisez cette page pour enregistrer un fournisseur d'identité (IDP) SAML 2.0 (Security Assertion Markup Language) avec le pare-feu ou Panorama. L'enregistrement est une étape nécessaire pour que le pare-feu ou Panorama fonctionnent en tant que fournisseur de services SAML, qui contrôle l'accès à vos ressources réseau. Lorsque les administrateurs et les utilisateurs finaux demandent des ressources, le fournisseur de services redirige les utilisateurs vers l'IDP pour l'authentification. Les utilisateurs finaux peuvent être des utilisateurs de GlobalProtect ou du portail captif. Les administrateurs peuvent être gérés localement sur le pare-feu et sur Panorama ou gérés en externe dans le magasin d'identité de l'IDP. Vous pouvez configurer une ouverture de session unique (SSO) en SAML afin que chaque utilisateur puisse accéder automatiquement à plusieurs ressources après avoir ouvert une session. Vous pouvez également configurer une ouverture de session unique (SSO) en SAML afin que chaque utilisateur puisse se connecter simultanément à tous les services SSO en se déconnectant de tout service unique.

Les séquences d'authentification ne prennent pas en charge les profils d'authentification qui spécifient les profils de serveur d'IDP en SAML.

Dans la plupart des cas, vous ne pouvez pas utiliser une SSO pour accéder à plusieurs applications sur le même appareil mobile.

Vous ne pouvez pas activer la SLO pour les utilisateurs du Portail captif.

La manière la plus simple de créer un profil de serveur d'IDP en SAML est d'**Importer** un fichier de métadonnées contenant les informations d'enregistrement de l'IDP. Après avoir enregistré un profil de serveur avec des valeurs importées, vous pouvez éditer le profil pour modifier les valeurs. Si l'IDP ne fournit pas de fichier de métadonnées, vous pouvez **Ajouter** le profil de serveur et saisir manuellement les renseignements. Après avoir créé un profil de serveur, affectez-le à un profil d'authentification (voir Périphérique > Profil d'authentification) pour un pare-feu ou des services Panorama spécifiques.

Paramètres du serveur du fournisseur d'identité SAML	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels, sélectionnez un système virtuel ou sélectionnez **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Location (Emplacement)**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Location (Emplacement)** est **Shared (Partagé)**.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur du fournisseur d'identité SAML	Description
ID de fournisseur d'identité	Saisissez un identifiant pour l'IDP. Votre IDP vous donne cette information.
Certificat du fournisseur d'identité	Sélectionnez le certificat que l'IDP utilise pour signer les messages SAML qu'il envoie au pare-feu. Vous devez sélectionner un certificat de l'IDP pour assurer l'intégrité des messages que l'IDP envoie au pare-feu. Pour valider le certificat de l'IDP auprès d'une autorité de certification (CA), vous devez indiquer un **Profil de certificat** pour tout profil d'authentification qui fait référence au profil de serveur de l'IDP (voir Périphérique > Profil d'authentification). Lors de la génération ou de l'importation d'un certificat et de sa clé privée associée, n'oubliez pas que les attributs d'utilisation des clés spécifiés dans le certificat contrôlent ce que vous pouvez utiliser avec la clé. Si le certificat énumère explicitement les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur le pare-feu. Dans ce cas, vous devez Importer le certificat et la clé à partir de l'autorité de certification (CA) de votre entreprise ou d'une autorité de certification tierce. Si le certificat ne spécifie pas les attributs d'utilisation des clés, vous pouvez utiliser la clé à toutes fins utiles, y compris la signature de messages. Dans ce cas, vous pouvez utiliser n'importe quelle méthode pour obtenir le certificat et la clé pour signer des messages SAML. Les certificats IDP prennent en charge les algorithmes suivants : • **Algorithmes à clé publique** : RSA (1 024 bits ou plus) et ECDSA (toutes les tailles). Un pare-feu en mode FIPS/CC prend en charge RSA (2 048 bits ou plus) et ECDSA (toutes les tailles). • **Algorithmes de signature** – SHA1, SHA256, SHA384 et SHA512. Un pare-feu en mode FIPS/CC prend en charge SHA256, SHA384 et SHA512.
URL d'authentification unique du fournisseur d'identité	Saisissez l'URL que l'IDP promeut pour son service d'authentification unique (SSO). Si vous créez le profil de serveur en important un fichier de métadonnées et que le fichier indique plusieurs URL SSO, le pare-feu utilise la première URL qui indique une méthode de liaison POST ou une méthode de redirection. *Palo Alto Networks recommande fortement d'utiliser une URL qui est fondée sur HTTPS, même si SAML prend également en charge le HTTP.*
URL de déconnexion unique du fournisseur d'identité	Saisissez l'URL que l'IDP promeut pour son service de déconnexion unique (SLO). Si vous créez le profil de serveur en important un fichier de métadonnées et que le fichier indique plusieurs URL SLO, le pare-feu utilise la première URL qui indique une méthode de liaison POST ou une méthode de redirection.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur du fournisseur d'identité SAML	Description
	Palo Alto Networks recommande fortement d'utiliser une URL qui est fondée sur HTTPS, même si SAML prend également en charge le HTTP.
Liaison HTTP SAML d'authentification unique	Sélectionnez la liaison HTTP associée à l'**URL d'authentification unique du fournisseur d'identité**. Le pare-feu utilise la liaison pour envoyer des messages SAML à l'IDP. Les options à votre disposition sont les suivantes : • **POST** – Le pare-feu envoie des messages utilisant des formulaires HTML codés en base64. • **Redirection** – Le pare-feu envoie des messages d'authentification encodés en base64 et codés en URL dans les paramètres d'URL. *Si vous importez un fichier de métadonnées de l'IDP qui possède plusieurs URL d'authentification unique, le pare-feu utilise la liaison de la première URL qui utilise la méthode POST ou la méthode de redirection. Le pare-feu ignore les URL qui utilisent d'autres liaisons.*
Liaison HTTP SAML de déconnexion unique	Sélectionnez la liaison HTTP associée à l'**URL de déconnexion unique du fournisseur d'identité**. Le pare-feu utilise la liaison pour envoyer des messages SAML à l'IDP. Les options à votre disposition sont les suivantes : • **POST** – Le pare-feu envoie des messages utilisant des formulaires HTML codés en base64. • **Redirection** – Le pare-feu envoie des messages d'authentification encodés en base64 et codés en URL dans les paramètres d'URL. *Si vous importez un fichier de métadonnées de l'IDP qui possède plusieurs URL de déconnexion unique, le pare-feu utilise la liaison de la première URL qui utilise la méthode POST ou la méthode de redirection. Le pare-feu ignore les URL qui utilisent d'autres liaisons.*
Métadonnées du fournisseur d'identité	Ce champ s'affiche uniquement si vous cliquez pour **Importer** un fichier de métadonnées de l'IDP que vous avez téléchargé sur le pare-feu depuis l'IDP. Le fichier indique les valeurs et le certificat de signature pour un nouveau profil de serveur de l'IDP en SAML. Vous devez **Naviguer** sur le fichier, indiquer le Nom de profil et le Déréglage d'horloge maximum, puis cliquer sur **OK** pour créer le profil. Vous pouvez également si vous le souhaitez éditer le profil pour modifier les valeurs importées.
Confirmer le certificat du fournisseur d'identité	Sélectionnez cette option pour valider la chaîne de confiance et éventuellement l'état de révocation du certificat de signature de l'IDP. Pour activez cette option, une autorité de certificat (CA) doit émettre votre certificat de signature de l'IDP. Vous devez créer un profil de certificat qui a l'autorité de certificat (CA) qui a émis le certificat de signature de l'IDP. Dans le profil d'authentification, sélectionnez le profil du serveur SAML et le

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur du fournisseur d'identité SAML	Description
	profil de certificat pour valider le certificat de l'IDP (voir Périphérique > Profil d'authentification). Si le certificat de signature de l'IDP est un certificat auto-signé, il n'y pas de chaîne de confiance, par conséquent, vous ne pouvez pas activer cette option. Le pare-feu valide toujours la signature des réponses et des assertions SAML auprès du certificat de fournisseur d'identité que vous activiez ou non l'option **Confirmer le certificat du fournisseur d'identité**. Si votre IDP fournit un certificat auto-signé, assurez-vous d'utiliser PAN-OS 9.1.3 ou une version ultérieure pour éviter l'exposition au CVE-2020-2021.
Signer le message SAML vers IdP	Sélectionnez cette option pour indiquer que le pare-feu signe les messages qu'il envoie à l'IDP. Le pare-feu utilise le **Certificat de signature des demandes** que vous indiquez dans un profil d'authentification (voir Périphérique > Profil d'authentification). *L'utilisation d'un certificat de signature garantit l'intégrité des messages envoyés à l'IDP.*
Déréglage d'horloge maximum	Saisissez l'intervalle de temps maximal acceptable en secondes entre le moment où l'IDP envoie le message et le moment où le système de pare-feu valide le message qu'il reçoit de la part de l'IDP (la plage est de 1 à 900, la valeur par défaut est de 60). Si l'intervalle de temps dépasse cette valeur, la validation (et donc l'authentification) échoue.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > DNS

Pour simplifier la configuration d'un système virtuel, un profil de serveur DNS vous permet de préciser le système virtuel configuré, une source d'héritage ou les adresses DNS principale et secondaire des serveurs DNS, ainsi que l'interface source et l'adresse source (itinéraire de service) qui seront utilisées dans les paquets envoyés au serveur DNS. L'interface source et l'adresse source sont utilisées comme interface de destination et adresse de destination dans la réponse du serveur DNS.

Un profil de serveur DNS s'applique à un système virtuel uniquement, et non à l'emplacement Partagé global.

Paramètres de profil de serveur DNS	Description
Name (Nom)	Nom du profil de serveur DNS.
Location (Emplacement)	Sélectionnez le système virtuel auquel le profil s'applique.
Source de l'héritage	Sélectionnez **None (Aucun)** si les adresses du serveur DNS ne sont pas héritées. Sinon, précisez le serveur DNS duquel le profil doit hériter des paramètres.
Vérifier l'état de la source de l'héritage	Cliquez pour afficher des informations sur la source de l'héritage.
DNS principal	Indiquez l'adresse IP du serveur DNS principal.
DNS secondaire	Indiquez l'adresse IP du serveur DNS secondaire.
Itinéraire de service IPv4	Sélectionnez cette option si vous souhaitez préciser que les paquets destinés au serveur DNS proviennent d'une adresse IPv4.
Interface source	Indiquez l'interface source utilisée par les paquets destinés au serveur DNS.
Source Address (Adresse source)	Indiquez l'adresse source IPv4 de laquelle les paquets destinés au serveur DNS proviennent.
Itinéraire de service IPv6	Sélectionnez cette option si vous souhaitez préciser que les paquets destinés au serveur DNS proviennent d'une adresse IPv6.
Interface source	Indiquez l'interface source utilisée par les paquets destinés au serveur DNS.
Source Address (Adresse source)	Indiquez l'adresse source IPv6 de laquelle les paquets destinés au serveur DNS proviennent.

© 2020 Palo Alto Networks, Inc.

Périphérique > Profils de serveur > Authentification multifacteur

Utilisez cette page pour configurer un profil de serveur d'authentification multifacteur (MFA) qui définit comment le pare-feu se connecte à un serveur MFA. MFA peut protéger vos ressources les plus importantes en veillant à ce que les pirates ne puissent pas accéder à votre réseau et ne puissent pas le contourner en compromettant un seul facteur d'identification (par exemple, en volant les informations d'identification de connexion). Après avoir configuré le profil du serveur, affectez-le aux profils d'authentification pour les services nécessitant une authentification (voir Périphérique > Profil d'authentification).

Pour les cas pratiques d'authentification suivants, le pare-feu s'intègre aux fournisseurs Multi-Factor Authentication (authentification multifacteur ; MFA) au moyen de RADIUS et de SAML :

- Authentification des utilisateurs distants via les portails et les passerelles GlobalProtect™.
- Authentification des administrateurs dans l'interface Web de PAN-OS et de Panorama™.
- Authentification via la politique d'authentification.

De plus, le pare-feu peut également s'intégrer aux fournisseurs MFA en utilisant l'API pour appliquer la MFA via la politique d'authentification applicable aux utilisateurs finaux uniquement (ne s'applique pas à l'authentification GlobalProtect ni à l'authentification des administrateurs).

La procédure complète utilisée pour configurer le MFA requiert des tâches supplémentaires autres que la création d'un profil de serveur.

Les séquences d'authentification ne prennent pas en charge les profils d'authentification qui spécifient les profils de serveur MFA.

Si le pare-feu s'intègre avec votre fournisseur MFA via RADIUS, configurez un profil de serveur RADIUS (voir Périphérique > Profils de serveur > RADIUS). Le pare-feu prend en charge tous les fournisseurs MFA via RADIUS.

Paramètres du serveur MFA	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sur un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou l'emplacement **Partagé**. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Profil du certificat	Sélectionnez le **Profil du certificat** qui indique le certificat de l'autorité de certification (AC) que le pare-feu utilisera pour valider le certificat du serveur MFA lors de la configuration d'une connexion sécurisée au serveur. Pour plus d'informations, voir Périphérique > Gestion des certificats > Profil de certificat.
Fournisseur MFA / Valeur	Sélectionnez un **MFA Vendor (fournisseur MFA)** et saisissez une **Value (Valeur)** pour chaque attribut de fournisseur. Les attributs varient selon le fournisseur. Reportez-vous à la documentation de votre fournisseur pour connaître les valeurs correctes.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur MFA	Description
	• **Duo v2** : • **Hôte API** – Le nom d'hôte du serveur Duo v2. • **Clé d'intégration** et **clé secrète –** Le pare-feu utilise ces clés pour s'authentifier sur le serveur Duo v2 et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser ces clés, la clé principale sur le pare-feu les crypte automatiquement afin que leurs valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur Duo v2 pour obtenir les clés. • **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec l'**hôte API** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre l'hôte API et le périphérique final de l'utilisateur. • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur Duo v2, saisissez l'URI du serveur proxy (par défaut / auth / v2). • **Okta Adaptive** : • **Hôte API –** Le nom d'hôte du serveur Okta. • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur Okta, saisissez l'URI du serveur proxy (par défaut / API / v1). • **Jeton** – Le pare-feu utilise ce jeton pour s'authentifier sur le serveur Okta et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser ce jeton, la clé principale sur le pare-feu le crypte automatiquement afin que ses valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur Okta pour obtenir le jeton. • **Organisation** – Le sous-domaine de votre organisation pour l'**Hôte API**. • **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec l'**hôte API** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre l'hôte API et le périphérique final de l'utilisateur. • **PingID** : • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur PingID, saisissez l'URI du serveur proxy (par défaut / PingID / 4). • **Nom d'hôte** – Saisissez le nom d'hôte du serveur PingID (par défaut idpxnyl3m.pingidentity.com). • **Utilisation de la clé en base64** et du **jeton –** Le pare-feu utilise la clé et le jeton pour s'authentifier sur le serveur PingID et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser la clé et le jeton, la clé principale sur le pare-feu les crypte automatiquement afin que leurs valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur PingID pour obtenir les valeurs. • **ID de l'organisation client PingID** – L'identifiant PingID pour votre organisation.

© 2020 Palo Alto Networks, Inc.

Paramètres du serveur MFA	Description
	• **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec le serveur PingID spécifié dans le champ **Nom de l'hôte** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre le serveur PingID et le périphérique final de l'utilisateur.

© 2020 Palo Alto Networks, Inc.

Périphérique > Base de données d'utilisateurs locale > Utilisateurs

Vous pouvez configurer une base de données locale sur le pare-feu pour stocker les informations d'authentification pour les administrateurs du pare-feu, les utilisateurs finaux du Portail captif et les utilisateurs finaux qui s'authentifient sur un Portail GlobalProtect et une passerelle GlobalProtect. L'authentification de la base de données locale ne nécessite aucun service d'authentification externe, vous pouvez effectuer toute la gestion du compte sur le pare-feu. Après avoir créé la base de données locale et (éventuellement) assigné les utilisateurs aux groupes (voir Périphérique > Base de données locale des utilisateurs > Groupes d'utilisateurs), vous pouvez cliquer sur Périphérique > Profil d'authentification en fonction de la base de données locale.

Vous ne pouvez pas configurer la section Périphérique > Profils de mots de passe pour les comptes administratifs qui utilisent l'authentification de la base de données locale.

Pour **Ajouter** un utilisateur local à la base de données, configurez les paramètres décrits dans le tableau suivant.

Paramètres d'utilisateur local	Description
Name (Nom)	Saisissez un nom pour identifier l'utilisateur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le compte utilisateur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le compte utilisateur, vous ne pouvez plus changer son **Location (Emplacement)**.
Mode	Utilisez ce champ pour préciser l'option d'authentification'A0;: • **Password (Mot de passe)** - Saisissez et confirmez un mot de passe pour l'utilisateur. • **Password Hash (Hachage du mot de passe)** – Saisissez une chaîne de mot de passe haché. Cela peut être utile si, par exemple, vous souhaitez réutiliser les informations d'identification pour un compte Unix existant, mais que vous ne connaissez pas le mot de passe en clair, seulement le mot de passe haché. Le pare-feu accepte n'importe quelle chaîne de 63 caractères indépendamment de l'algorithme utilisé pour générer la valeur de hachage. La commande CLI opérationnelle **`request password-hash password`** utilise l'algorithme MD5 lorsque le pare-feu est en mode normal et l'algorithme SHA256 lorsque le pare-feu est en mode CC/FIPS. *Tous les paramètres de Complexité minimale du mot de passe que vous avez définis pour le pare-feu (Device*

© 2020 Palo Alto Networks, Inc.

Paramètres d’utilisateur local	Description
	(Périphérique) > Setup (Configuration) > Management (Gestion)) ne s’appliquent pas aux comptes qui utilisent un Password Hash (Mot de passe haché).
Activer	Sélectionnez cette option pour activer le compte utilisateur.

© 2020 Palo Alto Networks, Inc.

Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs

Sélectionnez **Device (Périphérique)** > **Local User Database (Base de données d'utilisateurs locale)** > **User Groups (Groupes d'utilisateurs)** pour ajouter des informations de groupes d'utilisateurs à la base de données locale.

Paramètres de groupe d'utilisateurs locaux	Description
Name (Nom)	Saisissez un nom pour identifier le groupe (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Sélectionnez la portée dans laquelle le groupe d'utilisateurs est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Shared (Partagé)** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner le **Location (Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le groupe d'utilisateurs, vous ne pouvez plus changer son **Location (Emplacement)**.
Tous les utilisateurs locaux	Cliquez sur **Add (Ajouter)** pour sélectionner les utilisateurs que vous souhaitez ajouter au groupe.

© 2020 Palo Alto Networks, Inc.

Périphérique > Exportation programmée des journaux

Vous pouvez planifier des exportations des journaux et les enregistrer sur un serveur FTP (File Transfer Protocol) au format CSV ou utilisez la fonction SCP (Secure Copy) pour transférer des données en toute sécurité entre le pare-feu et un hôte distant. Les profils des journaux contiennent les informations relatives à la planification et au serveur FTP. Par exemple, un profil peut déterminer que les journaux du jour précédent sont collectés chaque jour à 15 heures et stockés sur un serveur FTP spécifique.

Cliquez sur **Add (Ajouter)** et renseignez les informations suivantes :

Paramètres d'exportation programmée des journaux	Description
Name (Nom)	Saisissez un nom pour identifier le profil (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. Une fois le profil créé, vous ne pouvez pas en modifier le nom.
Description	Saisissez une description (facultatif) (jusqu'à 255 caractères).
Activer	Sélectionnez cette option pour activer la planification des exportations des journaux.
Type de journal	Sélectionnez le type de journal (**traffic (trafic)**, **threat (menace)**, **gtp**, **sctp**, **tunnel (tunnel)**, **userid (id utilisateur)**, **auth (autorisation)**, **url**, **data (données)**, **hipmatch (correspondance HIP)** ou **wildfire**). La valeur par défaut est trafic.
Heure (quotidienne) de début de l'exportation programmée	Saisissez l'heure (hh:mm) à laquelle le démarrage de l'exportation doit débuter en utilisant le format d'horloge 24 heures (00:00 - 23:59).
Protocole	Sélectionnez le protocole à utiliser pour l'exportation des journaux entre le pare-feu et un hôte distant : • **FTP** – Ce protocole n'est pas sécurisé. • **SCP** – Ce protocole est sécurisé. Après avoir renseigné les champs restants, vous devez cliquer sur **Tester la connexion au serveur SCP** pour tester la connectivité entre le pare-feu et le serveur SCP et vous devez vérifier et accepter la clé d'hôte du serveur SCP.
Nom d'hôte	Saisissez l'adresse'A0;IP ou le nom d'hôte du serveur FTP utilisé pour l'exportation.
Port	Saisissez le numéro de port utilisé par le serveur FTP. La valeur par défaut est 21.
Chemin d'accès	Précisez le chemin d'accès sur le serveur FTP qui sera utilisé pour stocker les informations exportées.

© 2020 Palo Alto Networks, Inc.

Paramètres d’exportation programmée des journaux	Description
Activer le mode passif FTP	Sélectionnez cette option pour utiliser le mode passif pour l'exportation. Cette option est cochée par défaut.
Username (Nom d’utilisateur)	Saisissez le nom d'utilisateur d'accès au serveur FTP. La valeur par défaut est anonyme.
Mot de passe/ Confirmer le mot de passe	Saisissez le mot de passe d'accès au serveur FTP. Le mot de passe n’est pas nécessaire si l’utilisateur est anonyme.
Tester la connexion au serveur SCP (Protocole SCP uniquement)	Si vous définissez le **Protocole** sur **SCP**, vous devez cliquer sur ce bouton pour tester la connectivité entre le pare-feu et le serveur SCP, puis vérifier et accepter la clé d’hôte du serveur SCP. *Si vous utilisez un modèle Panorama pour configurer la planification de l’exportation de journal, vous devez réaliser cette étape après avoir validé la configuration du modèle sur les pare-feu. Une fois le modèle validé, connectez-vous à chaque pare-feu, ouvrez la planification de l’exportation des journaux et cliquez sur Test SCP server connection (Testez la connexion au serveur SCP).*

© 2020 Palo Alto Networks, Inc.

Périphérique > Logiciel

Sélectionnez **Device (Périphérique)** > **Software (Logiciel)** pour afficher les versions logicielles disponibles, télécharger ou charger une version, installer une version (une licence de support est requise), supprimer une image logicielle du pare-feu ou consulter les notes de version.

Avant d'effectuer une mise à niveau vers une version antérieure ou ultérieure de votre logiciel :

- Passez en revue les Notes de version en vigueur pour consulter les descriptions des nouvelles caractéristiques et des modifications apportées aux comportements par défaut dans une version et pour connaître le chemin de migration pour la mise à niveau du logiciel.
- Examinez les éléments à considérer pour la mise à niveau vers une version antérieure ou ultérieure ainsi que les instructions de mises à niveau dans le Guide des nouvelles caractéristiques de Pan-OS® version 9.1.
- Assurez-vous que les paramètres de date et d'heure du pare-feu sont à jour. Le logiciel PAN-OS est signé numériquement et le pare-feu vérifie la signature avant l'installation d'une nouvelle version. Si les paramètres de date et d'heure du pare-feu ne sont pas à jour et que le pare-feu interprète que la signature du logiciel est par la suite incorrecte, il affichera le message suivant :

```
Decrypt failed: GnuPG edit non-zero, with code 171072 Failed to load into
 PAN software manager.
```

Le tableau suivant vous aide à utiliser la page **Software (Logiciel)**.

Champs optionnels du logiciel	Description
Version	Répertorie les versions logicielles actuellement disponibles sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel est disponible auprès de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**. Le pare-feu utilise l'itinéraire de service pour se connecter au serveur de mises à jour, y rechercher de nouvelles versions et, si des mises à jour sont disponibles, les afficher en tête de liste.
Taille	Indique la taille de l'image logicielle.
Date de version	Indique la date et l'heure de disponibilité de la version auprès de Palo Alto Networks.
Disponible	Indique que la version correspondante de l'image logicielle est chargée ou téléchargée sur le pare-feu.
Actuellement installé	Indique si la version correspondante de l'image logicielle est activée et en cours d'exécution sur le pare-feu.
Action (Action)	Indique l'action que vous pouvez entreprendre pour l'image logicielle correspondante comme suit'A0;: • **Download (Télécharger)** : la version correspondante du logiciel est disponible sur le serveur de mises à jour Palo Alto Networks ; cliquez sur **Download (Télécharger)** pour télécharger une version disponible du logiciel.

© 2020 Palo Alto Networks, Inc.

Champs optionnels du logiciel	Description
	• **Install (Installer)** : la version correspondante du logiciel a été téléchargée ou chargée sur le pare-feu ; cliquez sur **Install (Installer)** pour installer le logiciel. Un redémarrage est requis pour terminer le processus de mise à niveau. • **Reinstall (Réinstaller)** : la version correspondante du logiciel a été précédemment installée ; cliquez sur **Reinstall (Réinstaller)** pour réinstaller la même version.
Notes de version	Cette option fournit un lien vers les notes de version relatives à la mise à jour logicielle correspondante. Ce lien est disponible uniquement pour les mises à jour que vous avez téléchargées depuis le serveur de mises à jour Palo Alto Networks : il ne s'applique pas aux mises à jour chargées.
	Il supprime l'image logicielle précédemment téléchargée ou chargée à partir du pare-feu. Vous ne souhaiterez peut-être supprimer que l'image de base de versions antérieures pour lesquelles une mise à niveau ne sera pas nécessaire. Par exemple, si vous exécutez la version 7.0, vous pouvez supprimer l'image de base de 6.1 si vous pensez avoir besoin d'une version antérieure.
Vérifier maintenant	Permet de vérifier si une nouvelle mise à jour logicielle est disponible auprès de Palo Alto Networks.
Télécharger	Permet d'importer une image de mise à jour logicielle d'un ordinateur auquel le pare-feu a accès. Vous effectuez généralement cette action si le pare-feu n'a pas accès à Internet, ce qui est nécessaire pour télécharger des mises à jour du serveur de mises à jour Palo Alto Networks. Pour effectuer des chargements, utilisez un ordinateur connecté à Internet pour vous rendre sur le site Web de Palo Alto Networks, téléchargez l'image logicielle à partir du Site de support (Mises à jour logicielles), téléchargez la mise à jour sur votre ordinateur, puis sélectionnez **Device (Périphérique)** > **Software (Logiciel)** sur le pare-feu et cliquez sur **Upload (Télécharger)** l'image logicielle. Dans une configuration haute disponibilité (HD), vous pouvez sélectionner l'option **Sync To Peer (Synchroniser sur homologue)** pour appliquer l'image logicielle importée à l'homologue HD. Après le chargement, la page **Software (Logiciel)** affiche les mêmes informations (version et taille par exemple), ainsi que les options **Install (Installer)** / **Reinstall (Réinstaller)** pour les logiciels chargés et téléchargés. L'option **Release Notes (Notes de version)** n'est pas active pour les logiciels chargés.

© 2020 Palo Alto Networks, Inc.

Périphérique > Mises à jour dynamiques

- Périphérique > Mises à jour dynamiques
- Panorama > Mises à jour dynamiques

Palo Alto Networks publie régulièrement des mises à jour qui incluent les applications nouvelles et modifiées et la protection contre les menaces, ainsi que des fichiers de données GlobalProtect via des mises à jour dynamiques. Le pare-feu peut extraire ces mises à jour et les utiliser pour appliquer la politique, sans exiger de modifications de configuration. Les mises à jour d'application et certaines mises à jour antivirus sont disponibles sans abonnement ; d'autres sont liées à vos abonnements.

Vous pouvez consulter les dernières mises à jour, lire les notes de version de chaque mise à jour, puis sélectionner la mise à jour que vous souhaitez télécharger et installer. Vous pouvez également rétablir la version précédemment installée d'une mise à jour.

L'établissement d'un calendrier de mises à jour dynamiques vous permet de définir la fréquence à laquelle le pare-feu vérifie la présence de nouvelles mises à jour et, le cas échéant, les télécharge ou les installe. Dans le cas particulier des mises à jour de contenu des applications et des menaces, vous pourriez souhaiter définir un calendrier qui échelonne les mises à jour d'applications nouvelles et modifiées après les mises à jour des menaces ; vous disposeriez ainsi de plus de temps pour évaluer l'incidence des applications nouvelles et modifiées sur votre politique de sécurité, tout en vous assurant que les protections contre les menaces les plus récentes sont installées sur votre pare-feu.

Options des mises à jour dynamiques	Description
Version	Répertorie les versions actuellement disponibles sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel est disponible auprès de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**. Le pare-feu utilise l'itinéraire de service pour se connecter au serveur de mises à jour, y rechercher de nouvelles versions du contenu et, si des mises à jour sont disponibles, les afficher en tête de liste.
Dernière vérification	Affiche la date et l'heure auxquelles le pare-feu s'est connecté pour la dernière fois au serveur de mises à jour et a vérifié si une mise à jour était disponible.
Programmer	Vous permet de planifier la fréquence de récupération des mises à jour. Vous pouvez définir la fréquence et le moment où les mises à jour dynamiques du contenu se produisent, soit la **Recurrence (Récurrence)** et l'intervalle de temps, ainsi que l'option permettant de **Download Only (Télécharger uniquement)** ou de **Download and Install (Télécharger et installer)** les mises à jour planifiées. Dans le cas des mises à jour Antivirus, et Applications et menaces, vous avez l'option de définir un seuil de temps minimum de disponibilité d'une mise à jour de contenu qu'un pare-feu doit attendre avant de l'installer. Il arrive, très rarement, qu'une erreur se glisse dans une mise à jour de contenu. Ce seuil fait en sorte que le pare-feu ne télécharge que des versions de contenu qui sont disponibles et fonctionnent dans les environnements des clients depuis la période de temps indiquée. Pour ce qui est des mises à jour de contenu Applications et Menaces, vous pouvez également définir un seuil qui s'applique spécialement aux mises à jour de contenu des applications nouvelles et modifiées. Un seuil prolongé pour

© 2020 Palo Alto Networks, Inc.

Options des mises à jour dynamiques	Description
	les mises à jour de contenu des applications vous donne plus de temps pour évaluer et ajuster votre politique de sécurité en fonction des changements qui accompagnent les applications nouvelles ou modifiées. *Pour obtenir de l'aide sur l'obtention optimale des mises à jour de contenu Applications et Menaces afin d'assurer la disponibilité continue des applications et la protection contre les dernières menaces, consultez les* Pratiques exemplaires relatives aux mises à jour des applications et des menaces.
File Name (Nom du fichier)	Affiche le nom du fichier'A0;; inclut les informations de version du contenu.
Caractéristiques	Répertorie le type de signatures que la version du contenu peut contenir. Pour les versions du contenu Applications et menaces, ce champ peut afficher une option pour consulter les **Apps, Threats (Applications et menaces)**. Sélectionnez cette option pour afficher les nouvelles signatures d'applications disponibles depuis la dernière version du contenu installée sur le pare-feu. Vous pouvez également utiliser la boîte de dialogue **New Applications (Nouvelles applications)** pour **Enable/Disable (Activer / désactiver)** de nouvelles applications. Vous pouvez choisir de désactiver une nouvelle application incluse dans une version du contenu si vous souhaitez empêcher l'impact sur la politique d'une application identifiée de manière unique (une application pouvant être traitée différemment avant et après l'installation du contenu si une application déjà connue est identifiée et classée différemment).
Type	Indique si le téléchargement inclut une mise à jour complète ou incrémentielle de la base de données.
Taille	Affiche la taille du module de mise à jour du contenu.
Date de version	Date et heure de disponibilité de la version du contenu auprès de Palo Alto Networks.
Téléchargé	Une coche dans cette colonne indique que la version du contenu correspondante a été téléchargée sur le pare-feu.
Actuellement installé	Une coche dans cette colonne indique que la version du contenu correspondante est en cours d'exécution sur le pare-feu.
Action (Action)	Indique l'action que vous pouvez entreprendre pour l'image logicielle correspondante comme suit'A0;: • **Download (Télécharger)** - La version du contenu correspondante est disponible sur le serveur de mises à jour Palo Alto Networks ; cliquez sur **Download (Télécharger)** pour télécharger les versions du contenu. Si le pare-feu ne dispose pas d'un accès à Internet, utilisez un ordinateur branché à l'Internet pour consulter le Portail de support aux clients, puis sélectionner **Mises à jour dynamiques**. Trouvez la version du contenu que vous souhaitez télécharger et cliquez sur **Download (Télécharger)** pour enregistrer le module de mise à jour sur votre ordinateur local. Ensuite cliquez sur **Upload (Charger)** pour charger manuellement l'image

© 2020 Palo Alto Networks, Inc.

Options des mises à jour dynamiques	Description
	logicielle au pare-feu. De plus, le téléchargement d'une version du contenu Applications et menaces active l'option **Review Policies (Réviser les politiques)** qui sont affectées par les nouvelles signatures d'applications incluses dans cette version. • **Review Policies (Réviser les politiques)** (contenu Applications et menaces uniquement) – Révisez l'impact des politiques pour les nouvelles applications incluses dans une version du contenu. Utilisez cette option pour évaluer le traitement d'une application avant et après l'installation d'une version du contenu. Vous pouvez également utiliser la boîte de dialogue Examen de la politique pour ajouter ou supprimer une application en attente (une application téléchargée avec une version du contenu, mais non installée sur le pare-feu) à ou à partir d'une règle de politique de Sécurité existante. Les changements de politiques des applications en attente ne s'appliquent que lorsque la version du contenu correspondante est installée. • **Review Apps (Consulter les applications)** (contenu Applications et Menaces uniquement) – Affichez les signatures d'applications, nouvelles et modifiées, disponibles depuis la dernière version du contenu installée sur le pare-feu. Si une mise à jour de contenu introduit des changements qui pourraient avoir une incidence sur la mise en œuvre des applications critiques, ces applications sont alors marquées et un examen de la politique est recommandé. Cliquez sur Review Policies (Réviser les politiques) pour voir l'incidence des mises à jour de contenu sur votre politique de sécurité existante. Vous pouvez également désactiver une application jusqu'à ce que vous ayez le temps d'examiner son incidence sur la politique. • **Install (Installer)** - La version du contenu correspondante a été téléchargée sur le pare-feu ; cliquez sur **Install (Installer)** pour installer la mise à jour. Lorsque vous installez une nouvelle version du contenu Applications et menaces, vous êtes invité à choisir l'option **Disable new apps in content update (Désactiver les nouvelles applications dans la mise à jour du contenu)**. Cette option vous protège contre les dernières menaces, vous permettant ainsi d'activer des applications après la préparation de mises à jour de politique en raison de l'impact de nouvelles signatures d'applications (pour activer des applications précédemment désactivées, sélectionnez **Apps, Threats (Applications et menaces)** sur la page Mises à jour dynamiques ou sélectionnez **Objects (Objets)** > **Application**). • **Revert (Rétablir)** : la version du contenu correspondante a été précédemment téléchargée. Pour réinstaller la même version, cliquez sur **Revert (Rétablir)**.
Documentation	Cette option fournit un lien vers les notes de version relatives à la version correspondante.
	Supprimez la version du contenu précédemment téléchargée à partir du pare-feu.
Télécharger	Si le pare-feu n'a pas accès au Serveur de mises à jour Palo Alto Networks, vous pouvez télécharger manuellement les mises à jour dynamiques dans la section Mises à jour dynamiques du Site de support de Palo Alto Networks. Après avoir téléchargé une mise à jour sur votre ordinateur, cliquez sur **Upload (Charger)** pour charger la mise à jour du pare-feu. Sélectionnez ensuite **Install**

© 2020 Palo Alto Networks, Inc.

Options des mises à jour dynamiques	Description
	From File (Installer depuis le fichier), puis sélectionnez le fichier que vous avez téléchargé.
Installer depuis le fichier	Après avoir chargé manuellement un fichier de mise à jour sur le pare-feu, utilisez cette option pour installer le fichier. Dans le menu déroulant **Package Type (Type de module)**, sélectionnez le type de mise à jour que vous installez (**Application and Threats (Application et menaces)**, **Antivirus** ou **WildFire**) et cliquez sur **OK**, sélectionnez ensuite le fichier que vous souhaitez installer, puis cliquez sur **OK** pour lancer l'installation.

© 2020 Palo Alto Networks, Inc.

Périphérique > Licences

Sélectionnez **Device (Périphérique)** > **Licenses (Licences)** pour activer des licences sur tous les modèles de pare-feu. Lorsque vous souscrivez à un abonnement auprès de Palo Alto Networks, vous recevez un code d'autorisation pour activer une ou plusieurs clés de licence.

Sur le pare-feu VM-Series, cette page vous permet également de désactiver une machine virtuelle (MV).

Les actions suivantes sont disponibles dans la page Licences :

- Récupérer les clés de licence auprès du serveur de licences'A0;: Sélectionnez cette option pour activer des abonnements souscrits qui requièrent un code d'autorisation et qui ont été activés sur le portail de support.
- Activer la fonction à l'aide du code d'autorisation'A0;: Sélectionnez cette option pour activer des abonnements souscrits qui requièrent un code d'autorisation et qui n'ont pas été activés sur le portail de support. Saisissez ensuite votre code d'autorisation, puis cliquez sur **OK**.
- Charger manuellement la clé de licence : si le pare-feu ne parvient pas à se connecter au serveur de licences et que vous souhaitez charger manuellement des clés de licence, téléchargez le fichier de la clé de licence à l'adresse https://support.paloaltonetworks.com et enregistrez-le localement. Cliquez sur Charger manuellement la clé de licence, sur Parcourir, sélectionnez le fichier, puis cliquez sur OK.

  Pour activer une licence pour le filtrage des URL, vous devez l'installer, télécharger la base de données, puis cliquer sur Activate (Activer). Si vous utilisez PAN-DB pour le filtrage des URL, vous devrez Download (Télécharger) la base de données d'amorçage initiale, puis cliquer sur Activate (Activer).

  Vous pouvez également exécuter la commande de la CLI ***`request url-filtering paloaltonetworks region <nomde la région>`***.
- **Deactivate VM (Désactiver MV)** : Cette option est disponible sur le pare-feu VM-Series avec le modèle Bring Your Own License (apportez votre propre licence) qui prend en charge les licences permanentes et basées sur une durée ; le modèle de licence à la demande ne prend pas en charge cette fonctionnalité. Cliquez sur **Deactivate VM (Désactiver MV)** lorsque vous n'avez plus besoin d'une instance du pare-feu VM-Series. Cela vous permet de libérer toutes les licences actives (licences d'abonnement, licences de Capacité MV et droits de support) qui utilisent cette option. Les licences sont recréditées sur votre compte et vous pouvez les appliquer à une nouvelle instance d'un pare-feu VM-Series lorsque vous en avez besoin. Lorsque la licence est désactivée, la fonctionnalité du pare-feu VM-Series est désactivée et l'état du pare-feu est « sans licence ». Cependant, la configuration demeure intacte.
  - Cliquez sur **Continue Manually (Continuer manuellement)** si le pare-feu VM-Series ne dispose pas d'un accès direct à Internet. Le pare-feu génère un fichier de jeton. Cliquez sur **Export license token (Exporter le jeton de licence)** pour enregistrer le fichier de jeton sur votre ordinateur local, puis redémarrez le pare-feu. Connectez-vous au portail d'Assistance Palo Alto Networks, sélectionnez **Assets (Actifs)** > **Devices (Périphériques)** ainsi que **Deactivate VM (Désactiver MV)** pour utiliser ce fichier de jeton et terminer le processus de désactivation.
  - Cliquez sur **Continue (Continuer)** pour désactiver les licences sur le pare-feu VM-Series. Cliquez sur **Reboot Now (Redémarrer maintenant)** pour terminer le processus de désactivation de licence.
  - Cliquez sur **Cancel (Annuler)** si vous souhaitez annuler et fermer la fenêtre Désactiver MV.
- **Upgrade VM Capacity (Mettre à niveau la capacité de la machine virtuelle)** : cette option vous permet d'améliorer les capacités de votre pare-feu VM-Series actuellement autorisé. Lors de l'amélioration des capacités, le pare-feu VM-Series conserve toute la configuration et les abonnements qu'il avait avant la mise à jour.
  - Si votre pare-feu est connecté au serveur de licence – Sélectionnez **Authorization Code (Code d'autorisation)**, saisissez votre code dans le champ Code d'autorisation et cliquez sur **Continue (Continuer)** pour lancer la mise à jour des capacités.

© 2020 Palo Alto Networks, Inc.

- Si votre pare-feu n'est pas connecté au serveur de licence – Sélectionnez **License Key (Clé de licence)**, cliquez sur **Complete Manually (Compléter manuellement)** pour générer un fichier de jeton et enregistrer le fichier de jeton sur votre ordinateur local. Connectez-vous ensuite au Portail de support de Palo Alto Networks, sélectionnez **Assets (Actifs)** > **Devices (Périphériques)** et cliquez sur **Deactivate License(s) (Désactiver licence(s))** pour utiliser le fichier de jeton. Téléchargez la clé de licence pour votre pare-feu VM-Series sur votre ordinateur local, ajoutez la clé de licence au pare-feu et cliquez sur **Continue (Continuer)** pour terminer la mise à niveau des capacités.
- Si votre pare-feu est connecté au serveur de licence, mais que vous n'avez pas de code d'autorisation – Sélectionnez l'option **Fetch from license server (Récupérer auprès du serveur de licences)**, mettez à jour la licence de capacité du pare-feu sur le serveur de licences avant d'essayer de mettre à jour la capacité, puis, après avoir vérifié que la licence a bien été mise à jour sur le serveur de licences, cliquez sur **Continue (Continuer)** pour lancer la mise à jour de la capacité.

© 2020 Palo Alto Networks, Inc.

Périphérique > Support

- Périphérique > Support
- Panorama > Support

Sélectionnez **Device (Périphérique)** > **Support (Assistance)** ou **Panorama** > **Support (Assistance)** pour accéder aux options relatives au support. Vous pouvez consulter les informations de contact de Palo Alto Networks, la date d'expiration du support, ainsi que les alertes produit et de sécurité de Palo Alto Networks en fonction du numéro de série de votre pare-feu.

Exécutez l'une des fonctions suivantes sur cette page'A0;:

- **Assistance** – Fournit des informations sur l'état de l'assistance de l'appareil et fournit un lien pour activer l'assistance à l'aide d'un code d'autorisation.
- **Alertes de production / alertes d'application et de menace** – Ces alertes sont récupérées à partir des serveurs de mises à jour Palo Alto Networks lorsqu'un utilisateur actualise / accède à cette page. Pour consulter les informations des alertes de production, ou celles des alertes d'application et de menace, cliquez sur le nom de l'alerte. Les alertes de production sont publiées en cas de rappel à grande échelle ou de problème urgent relatif à une version donnée. Les alertes d'application et de menace sont publiées si des menaces significatives sont détectées.
- **Liens** – Fournit des liens communs d'assistance pour vous aider à gérer votre appareil et pour accéder aux coordonnées de l'assistance.
- **Fichier de support technique** – Cliquez sur **Generate Tech Support File (Générer le fichier de support technique)** pour générer un fichier système qui permet à l'équipe d'assistance de vous aider à résoudre les problèmes que vous êtes susceptibles de rencontrer avec le pare-feu. Une fois le fichier généré, cliquez sur **Download Tech Support File (Télécharger le fichier de support technique)**, puis envoyez le fichier au service de support Palo Alto Networks.

  Si votre navigateur est configuré pour ouvrir automatiquement les fichiers après le téléchargement, vous devriez désactiver cette option afin que le navigateur télécharge le fichier de support plutôt que d'essayer de l'ouvrir et de l'extraire.
- **Fichier de collecte des statistiques** (pare-feu uniquement) – Cliquez sur **Generate Stats Dump File (Générer le fichier de collecte des statistiques)** pour générer un ensemble de rapports XML qui récapitulent le trafic réseau au cours des 7 derniers jours. Une fois que le rapport est généré, vous pouvez **Download Stats Dump File (Télécharger le fichier de vidage des statistiques)**. L'ingénieur système de Palo Alto Networks ou d'un partenaire homologué utilise ce rapport pour générer un résumé dans l'application Security Lifecycle Review (SLR). Le résumé de SLR met en évidence ce qui a été trouvé sur le réseau, ainsi que les risques opérationnels ou de sécurité associés pouvant être présents ; celui-ci est généralement utilisé dans le cadre du processus d'évaluation. Pour plus d'informations sur le résumé de l'application SLR, contactez votre ingénieur système de Palo Alto Networks ou d'un partenaire homologué.
- **Fichiers noyau (core)** – Si votre pare-feu connaît une défaillance du système fonctionnel, il générera un fichier noyau qui contient des détails sur le processus et la raison de son échec. Cliquez sur le lien **Download Core Files (Télécharger les fichiers noyau)** pour afficher une liste des fichiers noyaux disponibles, puis cliquez sur le nom d'un fichier noyau pour le télécharger. Après avoir téléchargé le fichier, chargez-le dans un dossier d'assistance de Palo Alto Networks pour obtenir de l'aide sur ce problème.

  Le contenu des fichiers noyaux peut uniquement être interprété par un ingénieur d'assistance de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Périphérique > Clé principale et diagnostics

- **Device (Périphérique)** > **Master Key and Diagnostics (Clé principale et diagnostics)**
- **Panorama** > **Master Key and Diagnostics (Clé principale et diagnostics)**

Modifiez la clé principale qui chiffre tous les mots de passe et les clés privées sur le pare-feu ou Panorama (telle que la clé RSA pour l'authentification des administrateurs qui accèdent à la CLI). Le chiffrement des mots de passe et des clés améliore la sécurité en garantissant que leurs valeurs en clair n'apparaîtront pas sur le pare-feu ou sur Panorama.

La seule façon de restaurer la clé principale par défaut est de rétablir les réglages d'usine.

Palo Alto Networks vous recommande de configurer une nouvelle clé principale plutôt que d'utiliser la clé par défaut, de stocker la clé dans un endroit sûr et de la modifier régulièrement. Pour plus de sécurité, vous pouvez utiliser un module matériel de sécurité pour crypter la clé principale (voir Périphérique > Configuration > HSM). La configuration d'une clé principale unique sur chaque pare-feu ou sur chaque serveur de gestion Panorama garantit qu'un pirate qui découvre la clé principale d'un périphérique ne peut pas accéder aux mots de passe et aux clés privées d'un autre de vos appareils. Toutefois, vous devez utiliser la même clé principale pour plusieurs appareils dans les cas suivants :

- **Configurations de la Haute disponibilité (HD)** – Si vous déployez des pare-feu ou Panorama dans une configuration HD, utilisez la même clé principale pour les pare-feu ou les serveurs de gestion Panorama dans la paire. Dans le cas contraire, la synchronisation HD ne fonctionne pas.
- **Panorama transfère les configurations aux pare-feu** – Si vous utilisez Panorama pour transférer les configurations aux pare-feu gérés, utilisez la même clé principale pour Panorama et pour les pare-feu gérés. Dans le cas contraire, les opérations de transfert de Panorama échoueront.

Pour configurer une clé principale, modifiez les paramètres de la Clé principale et utilisez le tableau suivant pour déterminer quelles sont les valeurs appropriées :

Paramètres de clé principale et de diagnostics	Description
Clé principale	Activez la configuration d'une clé principale unique. Désactivez (décochez) l'utilisation de la clé principale par défaut.
Clé principale active	Indiquez la clé actuellement utilisée pour crypter toutes les clés privées et tous les mots de passe sur le pare-feu.
Nouvelle clé principale Confirmer la clé principale	Pour modifier la clé principale, saisissez une chaîne de 16 caractères et confirmez la nouvelle clé.
Durée de vie	Indiquez le nombre de **Days (Jours)** et **Hours (Heures)** au bout desquels la clé principale arrive à expiration. La valeur doit être comprise entre 1 et 438 000 jours (50 ans). *Vous devez configurer une nouvelle clé principale avant que la clé actuelle n'expire. Si la clé principale expire, le pare-feu ou Panorama redémarre automatiquement en*

© 2020 Palo Alto Networks, Inc.

Paramètres de clé principale et de diagnostics	Description
	mode Maintenance. Vous devez alors procéder à une réinitialisation.
Heure de rappel	Saisissez le nombre de **Days (Jours)** et **Hours (Heures)** avant que la clé principale n'expire lorsque le pare-feu génère une alarme d'expiration. Le pare-feu ouvre automatiquement la boîte de dialogue System Alarms (Alarmes système) pour afficher l'alarme. *Pour s'assurer que l'alarme d'expiration s'affiche, sélectionnez Device (Périphérique) > Log Settings (Paramètres du journal), modifiez les paramètres d'alarme et cliquez sur Enable Alarms (Activer les alarmes).*
Stocké sur le module de sécurité matériel	Activez cette option uniquement si la clé principale est cryptée sur un Module de sécurité matériel (HSM). Vous ne pouvez pas utiliser de module de sécurité matériel sur une interface dynamique telle qu'un client'A0;DHCP ou PPPoE. La configuration du module de sécurité matériel (HSM) n'est pas synchronisée entre les pare-feu homologues en mode HD. Par conséquent, chaque homologue dans une paire'A0;HD peut se connecter à une source différente du module de sécurité matériel. Si vous utilisez Panorama et souhaitez synchroniser la configuration sur les deux homologues, utilisez des modèles Panorama pour configurer la source du module de sécurité matériel sur les pare-feu gérés. Le pare-feu PA-220 ne prend pas en charge HSM.
Renouvellement automatique de la clé principale	Permet le renouvellement automatique de la clé principale du nombre de jours et d'heure spécifiés. Désactivez (décochez) cette option pour autoriser l'expiration de la clé principale à la fin de sa durée de vie configurée. Procédez au **Auto Renew with Same Master Key (Renouvellement automatique de la clé principale)** en indiquant le nombre de **Days (Jours)** et **Hours (Heures)** desquels prolonger le chiffrement de la clé principale (plage de 1 heure à 730 jours).
Critères communs	En mode Critères Communs, d'autres options sont disponibles et vous permettent d'exécuter un auto-test d'algorithme cryptographique et un auto-test d'intégrité logicielle. Un calendrier est également inclus pour définir les heures auxquelles les deux auto-tests seront exécutés.

Déployer la clé principale

Déployez une clé principale ou mettez à jour une clé principale existante d'un pare-feu géré, d'un collecteur de journaux ou d'un appareil WF-500 directement à partir de Panorama.

Champ	Description
Déployer la clé principale	

© 2020 Palo Alto Networks, Inc.

Champ	Description
Filtre	Filtrez les appareils gérés qui doivent s'afficher selon la plateforme, les groupes de périphériques, les modèles, les étiquettes, l'état HA ou la version du logiciel.
Nom du périphérique	Nom du pare-feu géré.
Version du logiciel	La version du logiciel qui s'exécute sur le périphérique géré.
Status (État)	L'état de la connexion du périphérique géré peut être `Connected`, `Disconnected` ou `Unknown`.
État du déploiement de la clé principale	
Nom du périphérique	Nom du pare-feu géré.
Status (État)	État du déploiement de la clé principale.
Résultat	Résultats du déploiement de la clé principale. Les résultats peuvent être `OK` ou `FAIL`.
Progression	Progression (%) du déploiement de la clé principale.
Détails	Détails du déploiement de la clé principale. Si le déploiement échoue, les raisons de l'échec s'affichent ici.
Résumé	
Progression	Affiche une barre de progression qui présente la progression du déploiement de la clé principale. Les informations suivantes s'affichent : • **Results Succeeded (Résultats atteints)** : Nombre de périphériques sur lesquels la clé principale a été déployée avec succès. • **Results Pending (Résultats en attente)** : Nombre de périphériques sur lesquels le déploiement de la clé principale est en attente. • **Results Failed (Résultats échoués)** : Nombre de périphériques sur lesquels le déploiement de la clé principale a échoué.

© 2020 Palo Alto Networks, Inc.

Identification utilisateur

L'identification d'utilisateurs (User-ID™) est une fonctionnalité des pare-feu de nouvelle génération Palo Alto Networks® qui s'intègre harmonieusement avec une gamme d'offres de services d'annuaires d'entreprise et de terminaux afin d'associer des activités et des politiques de sécurité à des noms d'utilisateur et à des, et non seulement à des adresses IP. La configuration de la fonction User-ID permet au Centre de commande de l'application (ACC), à App-Scope, aux rapports et aux journaux d'inclure les noms d'utilisateur en plus des adresses IP d'utilisateur.

- Périphérique > Identification utilisateur > Mappage d'utilisateur
- Périphérique > Identification utilisateur > Sécurité de la connexion
- Périphérique > Identification utilisateur > Agents User-ID
- Périphérique > Identification utilisateur > Agents de Terminal Server
- Périphérique > Identification utilisateur > Paramètres de mappage de groupe
- Périphérique > Identification utilisateur > Paramètres du portail captif

Vous souhaitez en savoir plus ?

Voir User-ID

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Mappage d'utilisateur

Configurez l'agent User-ID intégré à PAN-OS exécuté sur le pare-feu pour Associer les adresses IP vers des noms d'utilisateur.

Que voulez-vous faire ?	Reportez-vous à la section :
Configurer l'agent User-ID intégré à PAN-OS.	Configuration de l'agent User-ID Palo Alto Networks
Gérer l'accès aux serveurs que l'agent User-ID surveille pour extraire les informations d'association d'utilisateur.	Surveillance des serveurs
Gérer les sous-réseaux que le pare-feu inclut ou exclut lors de l'association des adresses IP aux noms d'utilisateurs.	Inclure ou exclure des sous-réseaux pour l'association d'utilisateur
Vous souhaitez en savoir plus ?	Configuration du Mappage d'utilisateur à l'aide de l'Agent User-ID intégré à PAN-OS.

Configuration de l'agent User-ID Palo Alto Networks

Ces paramètres définissent les méthodes que l'agent User-ID utilise pour effectuer le mappage d'utilisateur.

Que voulez-vous faire ?	Reportez-vous à la section :
Permettre à l'agent User-ID d'utiliser Windows Management Instrumentation (WMI, Infrastructure de gestion Windows) pour sonder les systèmes clients ou Windows Remote Management (WinRM) sur HTTP ou HTTPS pour surveiller les serveurs afin d'extraire les informations d'association d'utilisateur.	Compte de surveillance du serveur
Surveiller les journaux des serveurs pour y déceler les informations de mappage d'utilisateur à l'aide de l'agent User-ID.	Surveillance du serveur

© 2020 Palo Alto Networks, Inc.

Que voulez-vous faire ?	Reportez-vous à la section :
Autoriser l'agent User-ID à sonder les systèmes client pour extraire les informations de mappage d'utilisateur.	Sondage du client
Veiller à ce que le pare-feu dispose des informations de mappage d'utilisateur les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP.	Cache
Autoriser l'authentification NTLM (NT LAN Manager) pour le mappage d'utilisateur via le portail captif.	Authentification NTLM
Autoriser les pare-feu à partager les informations de mappage d'utilisateur et de groupe afin de simplifier la gestion de l'agent User-ID.	Redistribution
Configurer l'agent User-ID pour qu'il puisse analyser syntaxiquement les messages Syslog pour extraire les informations de mappage d'utilisateur.	Filtres Syslog
Configurer l'agent User-ID pour qu'il omette des noms d'utilisateur donnés du processus de mappage.	Liste des utilisateurs ignorés

Compte de surveillance du serveur

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup(Configuration de l'agent User-ID Palo Alto Networks)** > **Server Monitor Account (Compte de surveillance du serveur)**

Pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse utiliser l'Instrumentation de gestion Windows (WMI) pour sonder les systèmes clients ou Windows Remote Management (WinRM) sur HTTP ou HTTPS pour surveiller les serveurs afin d'extraire les informations de mappage d'utilisateur, remplissez les champs suivants.

Vous pouvez également Configuration de l'accès aux serveurs surveillés en configurant un serveur Kerberos pour l'authentification de la surveillance du serveur au moyen de Windows Remote Management (WinRM) sur HTTP ou HTTPS.

Étant donné que le sondage WMI se fie à des données renvoyées depuis un terminal, Palo Alto Network ne vous recommande pas d'utiliser cette méthode pour obtenir des informations de mappage User-ID dans un réseau haute sécurité. Si vous configurez l'agent User-ID pour obtenir des informations de mappage en analysant les journaux d'événements de sécurité Active Directory (AD) ou les messages syslog, ou en utilisant l'API XML, Palo Alto Networks vous recommande de désactiver le sondage WMI.

Si vous utilisez le sondage WMI, ne l'activez pas sur des interfaces externes et non fiables. En effet, cela provoque l'envoi des sondes WMI contenant des informations sensibles par l'agent en dehors de votre réseau, par exemple le nom d'utilisateur, le nom de domaine et le hachage du mot de passe du compte de service de l'agent User-ID. Un pirate pourrait potentiellement exploiter ces informations pour pénétrer et accéder à votre réseau.

© 2020 Palo Alto Networks, Inc.

Paramètres d'authentification de Active Directory	Description
Nom d'utilisateur	Saisissez les informations d'identification de domaine (**User Name (Nom d'utilisateur)** et **Password (Mot de passe)**) du compte utilisé par le pare-feu pour accéder aux ressources Windows. Le compte doit être autorisé à effectuer des requêtes WMI sur les ordinateurs client et à surveiller les serveurs Microsoft Exchange et les contrôleurs de domaine. Utilisez la syntaxe domaine\nom d'utilisateur pour définir **User Name (Nom d'utilisateur)**. Si vous Configuration de l'accès aux serveurs surveillés en utilisant Kerberos pour authentifier le serveur, entrez le User Principal Name (nom principal de l'utilisateur ; UPN) Kerberos.
Nom DNS du domaine	Saisissez le nom DNS du serveur faisant l'objet de la surveillance. Si vous Configuration de l'accès aux serveurs surveillés en utilisant Kerberos pour authentifier le serveur, entrez le domaine de la partition Kerberos. Vous devez configurer ce paramètre si vous utilisez **WinRM-HTTP** en tant que protocole de transport lorsque vous Configuration de l'accès aux serveurs surveillés.
Mot de passe/Confirmer le mot de passe	Saisissez et confirmez le mot de passe du compte utilisé par le pare-feu pour accéder aux ressources Windows.
Profil du serveur Kerberos	Sélectionnez le profil du serveur Kerberos qui contrôle l'accès à la partition pour extraire les journaux de sécurité et les informations de sessions du serveur faisant l'objet de la surveillance au moyen de WinRM sur HTTP ou HTTPS.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse surveiller les serveurs et sonder les clients exige l'accomplissement de tâches supplémentaires en plus de la définition des paramètres d'authentification Active Directory.

Surveillance du serveur

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup(Configuration de l'agent User-ID Palo Alto Networks)** > **Server Monitor (Surveillance du serveur)**

Pour permettre à l'agent User-ID d'associer les adresses IP aux noms d'utilisateur en recherchant des événements de connexion dans les journaux d'événements de sécurité des serveurs, configurez les paramètres décrits dans le tableau suivant.

Si la charge de la requête est élevée pour les journaux des serveurs Windows, les sessions du serveur Windows, ou les serveurs eDirectory, le retard observé entre les requêtes pourrait considérablement dépasser la fréquence ou l'intervalle spécifié.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse surveiller les serveurs exige l'accomplissement de tâches supplémentaires en plus de la configuration des paramètres de surveillance du serveur.

© 2020 Palo Alto Networks, Inc.

Paramètres de surveillance du serveur	Description
Activer le journal de sécurité	Sélectionnez cette option pour activer la surveillance des journaux de sécurité sur les serveurs Windows.
Fréquence de surveillance du journal du serveur (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les journaux de sécurité du serveur Windows pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par défaut : 2). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et où le pare-feu envoit la requête suivante.  *Si la surveillance des journaux ne se produit pas assez souvent, le dernier mappage adresse IP/ utilisateur pourrait ne pas être disponible. Une surveillance trop fréquente des journaux par le pare-feu pourrait avoir une incidence sur le contrôleur de domaine, sur la mémoire, sur le processeur et sur l'application de la politique User-ID. Commencez par une valeur se situant entre 2 et 30 secondes, puis revoyez la valeur en fonction de l'incidence sur le rendement ou de la fréquence des mises à jour des mappages d'utilisateur.*
Activer la session	Sélectionnez cette option pour activer la surveillance des sessions d'utilisateur sur les serveurs surveillés. Chaque fois qu'un utilisateur se connecte à un serveur, une session est créée ; le pare-feu peut utiliser ces informations pour identifier l'adresse IP de l'utilisateur.  *Vous ne devez pas Activer la session. Ce paramètre nécessite que l'agent User-ID possède un compte Active Directory avec des privilèges d'Opérateur de serveur afin de pouvoir lire toutes les sessions utilisateur. Au lieu de cela, vous devez utiliser une intégration Syslog ou API XML pour surveiller les sources qui recueillent les événements de connexion et de déconnexion pour tous les types de périphériques et de systèmes d'exploitation (plutôt qu'uniquement les systèmes d'exploitation Windows), tels que les contrôleurs sans fil et les NAC.*
Fréquence de lecture de la session serveur (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les sessions d'utilisateurs Windows pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et commence celui de la suivante.
Intervalle de requête de Novell eDirectory (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les serveurs eDirectory Novell pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par :

© 2020 Palo Alto Networks, Inc.

Paramètres de surveillance du serveur	Description
	30). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et commence celui de la suivante.
Profil de service Syslog	Sélectionnez un profil de service SSL/TLS indiquant le certificat et les versions SSL/TLS autorisées pour les communications entre le pare-feu et des expéditeurs Syslog surveillés par l'agent User-ID. Pour plus de détails, voir Périphérique > Gestion des certificats > Profil de service SSL / TLS et Filtres Syslog. Si vous sélectionnez **none (aucun)**, le pare-feu utilisera son certificat prédéfini et autosigné.

Sondage du client

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks (Configuration de l'agent User-ID Palo Alto Networks)** > **Client Probing (Sondage du client)**

Vous pouvez configurer l'agent User-ID pour qu'il puisse effectuer le sondage du client WMI de chaque système client que le processus d'association d'utilisateur identifie. L'agent User-ID sondera régulièrement chaque adresse IP reconnue pour vérifier que le même utilisateur est toujours connecté. Lorsque le pare-feu rencontre une adresse IP pour laquelle il ne dispose pas de mappage d'utilisateur, il envoie l'adresse à l'agent pour sondage immédiat. Pour configurer les paramètres du sondage du client, remplissez les champs suivants.

N'activez pas l'interrogation du client sur les réseaux haute sécurité. N'activez pas l'interrogation du client sur les interfaces externes non approuvées. Le sondage du client peut entraîner de grande quantité de trafic réseau, peut poser une menace à la sécurité s'il est mal configuré et, si activé sur une zone externe non approuvée, il peut permettre à un pirate d'envoyer un sondage en dehors de votre réseau, ce qui entraînerait une divulgation du nom de compte du service de l'agent User-ID, du nom de domaine et du hachage du mot de passe crypté. Au lieu de cela, collectez des informations de mappage d'utilisateur à partir de sources plus isolées et fiables telles que les contrôleurs de domaine et par l'intermédiaire des intégrations avec Syslog ou l'API XML, qui ont l'avantage supplémentaire de vous permettre de recueillir en toute sécurité des informations de mappage d'utilisateurs à partir de n'importe quel type de périphérique ou de système d'exploitation, plutôt que de se cantonner aux clients Windows.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse sonder les clients exige l'accomplissement de tâches supplémentaires en plus de la configuration des paramètres du sondage du client.

L'agent User-ID intégré à PAN-OS ne prend pas en charge le sondage de NetBIOS, tandis que l'agent User-ID Windows le fait.

Paramètres de Sondage du client	Description
Activer le sondage	Sélectionnez cette option pour activer l'interrogation WMI.
Intervalle de sondage (min)	Saisissez l'intervalle de sondage en minutes (plage de 1 à 1 440, par défaut 20). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière demande et commence celui de la prochaine demande.

© 2020 Palo Alto Networks, Inc.

Paramètres de Sondage du client	Description
	Dans les déploiements massifs, il est important de définir un intervalle approprié permettant le sondage de chaque client qui a été identifié par le processus de mappage d'utilisateur. Par exemple, si vous disposez de 6000 utilisateurs et d'un intervalle de 10 minutes, 10 requêtes WMI par seconde sont nécessaires pour chaque client.  *Si la charge de la requête de sondage est élevée, le retard observé entre les requêtes pourrait considérablement dépasser l'intervalle que vous aurez indiqué.*

Cache

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks)** > **Cache (Mémoire cache)**

Pour veiller à ce que le pare-feu dispose des informations d'association d'utilisateur les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP, configurez les délais de suppression des associations d'utilisateurs de la mémoire cache du pare-feu. Ce délai d'expiration s'applique aux associations d'utilisateurs découverts grâce à toute méthode, à l'exception du Portail captif. Pour les associations découvertes au moyen du Portail captif, définissez le délai d'expiration dans les Paramètres du portail captif (Périphérique > Identification de l'utilisateur > Paramètres du portail captif, champs **Timer (Minuteur)** et **Idle Timer (Minuterie d'inactivité)**).

Pour mettre en correspondance les noms d'utilisateurs recueillis des sources User-ID même si aucune domaine n'est inclus, configurez le pare-feu pour permettre la mise en correspondance des noms d'utilisateurs sans domaines. Vous ne devriez utiliser cette option que si les noms d'utilisateur de votre organisation ne sont pas dupliqués entre les domaines.

Paramètres du cache	Description
Activer le délai d'identification utilisateur	Sélectionnez cette option pour activer une valeur de délai de saisie du mappage d'utilisateur. Quand la valeur de délai de saisie est atteinte, le pare-feu la supprime et extrait un nouveau mappage. Cela permet de s'assurer que le pare-feu dispose des informations les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP.  *Activez le délai pour s'assurer que le pare-feu dispose des plus récentes informations de mappage utilisateur/adresse IP.*
Délai d'identification utilisateur (en minutes)	Définissez la valeur du délai d'expiration en minutes des entrées d'association d'utilisateur (plage de 1 à 3 600 ; valeur par défaut : 45).  *Définissez la valeur du délai à la demi-vie du bail DHCP ou à la durée de vie du ticket Kerberos.*  *Si vous configurez des pare-feu pour redistribuer les informations d'association, chaque pare-feu efface les*

© 2020 Palo Alto Networks, Inc.

Paramètres du cache	Description
	entrées d'association qu'il reçoit en fonction du délai d'expiration que vous avez défini sur ce pare-feu et non sur les délais d'expiration définis dans les pare-feu de transfert.
Autoriser la mise en correspondance des noms d'utilisateurs sans domaines	Sélectionnez cette option pour autoriser le pare-feu à mettre les utilisateurs en correspondance si le domaine n'est pas fourni par la source User-ID. Pour prévenir la mauvaise identification des utilisateurs, ne sélectionnez cette option que si vos noms d'utilisateur ne sont pas dupliqués entre les domaines. *Avant d'activer cette option, vérifiez que le pare-feu a récupéré les mappages de groupe auprès du serveur LDAP.*

Authentification NTLM

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks)** > **NTLM**

Vous pouvez utiliser NT LAN Manager (NTLM) pour authentifier les utilisateurs de Windows uniquement. Lorsqu'une requête Web client correspond à une règle de politique d'Authentification dans laquelle l'objet d'application de l'authentification spécifie un défi de navigation (voir Politiques > Authentification), une stimulation NTLM authentifie le client de manière transparente. Le pare-feu recueille ensuite les informations de mappage d'utilisateur à partir du domaine NTLM.

Vous pouvez activer l'authentification NTLM sur un seul système virtuel par pare-feu, que vous sélectionnez dans la liste déroulante **Location (Emplacement)** qui se trouvent au haut de la page **User Mapping (Mappage d'utilisateur)**.

Si vous le souhaitez, vous pouvez également utiliser le pare-feu pour effectuer le traitement de l'authentification NTLM d'autres pare-feu en l'ajoutant en tant qu'agent User-ID à ces pare-feu. Pour plus de détails, reportez-vous à la Configuration de l'accès aux agents User-ID.

Si vous utilisez l'agent User-ID Windows, les réponses NTLM seront directement adressées au contrôleur de domaine dans lequel l'agent a été installé. Pour plus de détails, reportez-vous au champ **Authentification NTLM** dans Périphérique > Identification utilisateur > Paramètres du portail captif.

Configurez les règles d'Authentification pour utiliser Ouverture de session unique Kerberos au lieu de l'authentification NTLM. Kerberos est une méthode d'authentification plus sûre et plus fiable que NTLM et ne nécessite pas que le pare-feu dispose d'un compte administrateur pour accéder au domaine. Pour plus d'informations sur la configuration des méthodes d'authentification pour les règles d'Authentification, voir Objets > Authentification.

Les procédures complètes pour configurer le Portail captif ou les agents User-ID Windows exigent l'accomplissement de tâches supplémentaires qui activent NTLM.

Pour configurer le traitement d'authentification NTLM, spécifiez les paramètres décrits dans le tableau suivant.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Activer le processus d'authentification NTLM	Sélectionnez cette option pour activer le processus d'authentification NTLM
Domaine NTLM	Saisissez le nom du domaine NTLM.
Le nom d'utilisateur admin (du domaine NTLM)	Saisissez le compte administrateur ayant accès au domaine NTLM. *N'incluez pas le domaine dans le champ Admin User Name (Nom d'utilisateur de l'administrateur). Sinon, le pare-feu ne pourra pas joindre le domaine.*
Mot de passe / Confirmer le mot de passe (du domaine NTLM)	Saisissez le mot de passe du compte administrateur ayant accès au domaine NTLM.

Redistribution

- **Device (Périphérique) > User Identification (Identification utilisateur) > User Mapping (Mappage d'utilisateur) > Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks (Configuration de l'agent User-ID Palo Alto Networks) > Redistribution**

Pour permettre à un pare-feu ou à un système virtuel de servir d'un agent User-ID qui redistribue les informations d'association d'utilisateurs ainsi que les horodatages associés aux défis d'authentification, configurez les paramètres décrits dans le tableau suivant. Lorsque, plus tard, vous connectez ce pare-feu à un appareil (tel que Panorama) qui recevra les informations de cartographie et les horodatages, l'appareil utilise ces champs pour identifier le pare-feu ou le système virtuel en tant qu'agent User-ID.

La procédure complète pour configurer des pare-feu afin de redistribuer les informations d'association d'utilisateurs et les horodatages d'authentification nécessite des tâches supplémentaires en plus de la spécification des paramètres de redistribution.

Par défaut, un pare-feu avec plusieurs systèmes virtuels ne redistribue pas les informations d'association d'utilisateurs sur ses systèmes virtuels, même si vous pouvez les configurer pour la redistribution.

Paramètres de redistribution	Description
Nom du collecteur	Saisissez un nom du collecteur pour identifier le pare-feu ou le système virtuel en tant qu'agent User-ID (255 caractères maximum).
Clé prépartagée/Confirmer la clé prépartagée	Saisissez une clé prépartagée (jusqu'à 255 caractères alphanumériques) pour identifier le pare-feu ou le système virtuel en tant qu'agent User-ID.

Filtres Syslog

- **Device (Périphérique) > User Identification (Identification utilisateur) > User Mapping (Mappage d'utilisateur) > Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks) > Syslog Filters (Filtres Syslog)**

© 2020 Palo Alto Networks, Inc.

L'agent User-ID utilise les profils d'analyse syntaxique Syslog pour filtrer les messages Syslog envoyés par les expéditeurs Syslog que l'agent surveille pour extraire les informations de mappage nom d'utilisateur/adresse IP (voir Configuration de l'accès aux serveurs surveillés). Chaque profil peut analyser les messages Syslog pour l'un des types d'événements suivants, mais pas les deux :

- Événements d'authentification (connexion) - Utilisés pour ajouter des mappages d'utilisateur au pare-feu.
- Événements de déconnexion - Utilisés pour supprimer les mappages d'utilisateurs qui ne sont plus d'actualité. La suppression de mappages obsolètes est utile dans les environnements où les affectations d'adresses IP changent souvent.

Palo Alto Networks fournit au pare-feu des profils d'analyse syntaxique Syslog prédéfinis par l'intermédiaire de Mise à jour de contenu des applications. Pour mettre à jour dynamiquement la liste des profils à mesure que les fournisseurs développent de nouveaux filtres, planifiez ces mises à jour de contenu dynamiques (voir Périphérique> Mises à jour dynamiques). Les profils prédéfinis sont globaux pour le pare-feu, tandis que les profils personnalisés que vous configurez s'appliquent uniquement au système virtuel (**Location (Emplacement)**) sélectionné sous **Device (Périphérique)** > **User Identification (Identification de l'utilisateur)** > **User Mapping (Mapping utilisateur)**.

Les messages Syslog doivent respecter les critères suivants pour qu'un agent User-ID les analyse :

- Chaque message doit être une chaîne de texte sur une seule ligne. Une nouvelle ligne (\n) ou un retour à la ligne et une nouvelle ligne (\r\n) sont les délimiteurs de sauts de ligne.
- La taille maximum pour les messages individuels est de 2 048 octets.
- Les messages envoyés via UDP doivent être contenus dans un seul paquet ; les messages envoyés via SSL peuvent couvrir plusieurs paquets. Un seul paquet peut contenir plusieurs messages.

Pour configurer un profil personnalisé, cliquez sur **Add (Ajouter)** et renseignez les paramètres décrits dans le tableau suivant. Les descriptions de champs dans ce tableau utilisent un exemple d'événement de connexion depuis un message Syslog avec le format suivant :

```
[Tue Jul 5 13:15:04 2005 CDT] Administrator authentication success User:domain
\johndoe_4 Source:192.168.0.212
```

La procédure complète de configuration de l'agent User-ID pour analyser un expéditeur Syslog pour les informations de mappage d'utilisateur nécessite des tâches supplémentaires en plus de la création d'un profil d'analyse syntaxique Syslog.

Champ	Description
Profil d'analyse syntaxique Syslog	Donnez un nom au profil HIP (63 caractères alpha-numériques maximum).
Description	Saisissez une description du profil (255 caractères alpha-numériques maximum).
Type	Définissez le type d'analyse syntaxique du filtrage des informations de mappage d'utilisateur : • **Regex Identifier (Identifiant d'expression régulière)** – Utilisez **Event Regex (Expression régulière d'événements)**, **Username Regex (Expression régulière de nom d'utilisateur)**, et **Address Regex (Expression régulière d'adresse)** pour préciser les expressions régulières (regex) qui décrivent les modèles de recherche utilisés pour identifier et extraire les informations de mappage d'utilisateur des messages Syslog. Le pare-feu utilisera la Regex pour faire correspondre les événements d'authentification ou de déconnexion dans les messages Syslog,

© 2020 Palo Alto Networks, Inc.

Champ	Description
	ainsi que les noms d'utilisateur et les adresses IP dans les messages correspondants. • **Field Identifier (Identificateur de champ)** – Utilisez les champs **Event String (Chaîne d'événements)**, **Username Prefix (Préfixe du nom d'utilisateur)**, **Username Delimiter (Séparateur de nom d'utilisateur)**, **Address Prefix (Préfixe d'adresse)** et **Address Delimiter (Séparateur d'adresse)** pour définir les chaînes à mettre en correspondance avec l'événement d'authentification ou de déconnexion et pour identifier les informations de mappage d'utilisateur dans les messages Syslog. Les champs restants dans la boîte de dialogue varient en fonction de votre sélection. Configurez les champs comme décrit dans les lignes suivantes.
Expression régulière d'événements	Renseignez l'expression régulière qui permet d'identifier les événements d'authentification ou de déconnexion réussis. Pour le message d'exemple utilisé avec ce tableau, l'expression régulière **`(authentication \ success) {1}`** extrait la première **`{1}`**instance de la chaîne `authentication success`. La barre oblique inversée avant l'espace est un caractère d'échappement Regex standard qui indique au moteur Regex de ne pas traiter l'espace comme caractère spécial.
Expression régulière de nom d'utilisateur	Renseignez l'expression régulière pour identifier le champ de nom d'utilisateur dans les messages d'authentification ou de déconnexion réussis. Pour le message d'exemple utilisé avec ce tableau, la Regex **`User: ([a-zA-Z0-9\\\._]+)`** correspond à la chaîne `User:johndoe_4` et extrait acme\johndoe1 comme nom d'utilisateur.
Expression régulière d'adresse	Renseignez l'expression régulière qui permet d'identifier la partie de l'adresse IP dans les messages d'authentification réussis ou de déconnexion. Dans le message d'exemple utilisé avec ce tableau, l'expression régulière **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** correspond à l'adresse IPv4 `Source:192.168.0.212` et ajoute 192.168.0.212 en tant qu'adresse IP dans le mappage nom d'utilisateur.
Chaîne d'événements	Saisissez une chaîne correspondante pour identifier les messages de déconnexion ou de réussite de l'authentification. Pour le message d'exemple utilisé avec ce tableau, vous devez saisir la chaîne **`authentication success`**.
Préfixe du nom d'utilisateur	Saisissez la chaîne correspondante pour identifier le début du champ Nom d'utilisateur dans les messages d'authentification ou de déconnexion Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet). Dans le message d'exemple utilisé avec ce tableau, `Utilisateur :` identifie le début du champ de nom d'utilisateur.
Séparateur de nom d'utilisateur	Saisissez le délimiteur pour marquer la fin du champ Nom d'utilisateur dans un message d'authentification ou de déconnexion. Utilisez \s pour indiquer un espace autonome (comme dans le message d'exemple) et \t pour indiquer un onglet.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Préfixe d'adresse	Saisissez la chaîne correspondante pour identifier le début du champ Adresse IP dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet). Dans le message d'exemple utilisé avec ce tableau, `Source :` identifie le début du champ de l'adresse.
Séparateur d'adresse	Saisissez la chaîne correspondante qui marque la fin du champ Adresse IP dans les messages de réussite d'authentification ou de déconnexion. Par exemple, saisissez \n pour indiquer que le délimiteur est un saut de ligne.

Liste des utilisateurs ignorés

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks (Configuration de l'agent User-ID Palo Alto Networks)** > **User Ignore List (Liste des utilisateurs ignorés)**

La liste des utilisateurs ignorés définit les comptes utilisateur pour lesquels le mappage nom d'utilisateur / adresse IP n'est pas requis (par exemple, les comptes de kiosques). Pour configurer la liste, cliquez sur **Add (Ajouter)** et saisissez un nom d'utilisateur. Vous pouvez utiliser un astérisque comme caractère générique permettant la correspondance de plusieurs noms d'utilisateur. Il ne peut toutefois être placé qu'à la toute fin de l'entrée. Par exemple, **corpdomain\it-admin*** correspond à tous les administrateurs dans le domaine **corpdomain** dont les noms d'utilisateur commencent avec la chaîne it-admin. Vous pouvez ajouter un maximum de 5 000 entrées à exclure du mappage d'utilisateur.

Définissez la liste des utilisateurs ignorés sur le pare-feu faisant office d'agent User-ID, et non pas sur le client. Si vous définissez la liste des utilisateurs ignorés sur le pare-feu client, les utilisateurs qui figurent dans la liste font toujours l'objet d'un mappage lors de la redistribution.

Surveillance des serveurs

- Périphérique > Identification utilisateur > Mappage d'utilisateur

Utilisez la section Surveillance des serveurs pour définir les serveurs Microsoft Exchange, les contrôleurs de domaine Active Directory (AD), les serveurs Novell eDirectory ou les expéditeurs Syslog que l'agent User-ID doit surveiller pour déceler des événements de connexion.

- Configuration de l'accès aux serveurs surveillés
- Gestion de l'accès aux serveurs surveillés
- Inclure ou exclure des sous-réseaux pour l'association d'utilisateur

Configuration de l'accès aux serveurs surveillés

Utilisez la section Surveillance du serveur pour **Add (Ajouter)** des profils de serveur qui indiquent les serveurs que le pare-feu surveillera.

Configurez au moins deux serveurs surveillés par User-ID. Ainsi, en cas d'échec d'un serveur, le pare-feu peut tout de même découvrir les mappages adresse IP/nom d'utilisateur.

© 2020 Palo Alto Networks, Inc.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il surveille les serveurs exige l'accomplissement des tâches supplémentaires outre la création de profils de serveurs.

Paramètres de surveillance du serveur	Description
Name (Nom)	Saisissez un nom de serveur.
Description	Saisissez une description du serveur.
Activé	Sélectionnez cette option pour activer la surveillance des journaux sur ce serveur.
Type	Sélectionnez le type de serveur. Votre sélection détermine les autres champs que ce dialogue affichera. • **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Expéditeur Syslog**
Protocole de transport (Microsoft Active Directory et Microsoft Exchange uniquement)	Sélectionnez le protocole de transport : • **WMI** : (par défaut) Utilisez Windows Management Instrumentation (WMI) pour sonder chaque adresse IP découverte et vérifier que le même utilisateur demeure connecté. • **Win-RM-HTTP** : Utilisez Windows Remote Management (WinRM) sur HTTP pour surveiller les journaux de sécurité et les informations de session sur le serveur. Cette option exige le **Domain's DNS Name (Nom DNS du domaine)** Kerberos dans la Compte de surveillance du serveur. • **Win-RM-HTTPS** : Utilisez Windows Remote Management (WinRM) sur HTTPS pour surveiller les journaux de sécurité et les informations de session sur le serveur. Pour exiger la validation des certificats du serveur avec le serveur Windows lorsque vous utilisez l'authentification Kerberos, veillez à configurer NTP dans les Paramètres des services globaux et à sélectionner l'autorité de certificat racine en tant que profil de certificat (Périphérique > Identification utilisateur > Sécurité de la connexion).
Adresse réseau	Saisissez l'adresse IP du serveur ou le nom de domaine complet du serveur surveillé. Si vous utilisez Kerberos à des fins d'authentification du serveur, vous devez entrer un FQDN. Cette option n'est pas prise en charge si le **Type** est **Novell eDirectory**.
Profil de serveur (Novell eDirectory uniquement)	Sélectionnez un profil de serveur LDAP pour la connexion au serveur eDirectory (Périphérique > Profils de serveurs > LDAP).
Connection Type (Expéditeur Syslog uniquement)	Sélectionnez si l'agent User-ID doit écouter les messages Syslog sur le port **UDP** (514) ou le port **SSL** (6 514). Si vous sélectionnez **SSL**, le **Syslog Service Profile (Profil du service Syslog)** que vous sélectionnez lors de l'activation de la Surveillance du serveur détermine les versions SSL/TLS qui sont autorisées et le certificat que le pare-feu utilise pour sécuriser une connexion avec l'expéditeur Syslog.

© 2020 Palo Alto Networks, Inc.

Paramètres de surveillance du serveur	Description
	En tant que meilleure pratique en termes de sécurité, sélectionnez SSL lorsque vous utilisez l'agent User-ID intégré à PAN-OS pour mapper les adresses IP à des noms d'utilisateur. Si vous sélectionnez UDP, assurez-vous que l'expéditeur Syslog et le client se trouvent tous les deux sur un réseau sécurisé dédié pour empêcher les hôtes non approuvés d'envoyer du trafic UDP au pare-feu.
Filtre (Expéditeur Syslog uniquement)	Si le **Type** de serveur est **Expéditeur Syslog**, vous devez **Ajouter** un ou plusieurs profils profil d'analyse syntaxique Syslog à utiliser pour l'extraction des noms d'utilisateur et des adresses IP des messages syslog reçus de ce serveur. Vous pouvez ajouter un profil personnalisé (reportez-vous à la section Filtres Syslog) ou un profil prédéfini. Pour chaque profil, définissez le **Type d'événement** : • **Connexion** – L'agent User-ID analyse les messages Syslog pour les événements de connexion pour créer des associations d'utilisateurs. • **Déconnexion** – L'agent User-ID analyse les messages Syslog pour les événements de déconnexion pour supprimer les associations d'utilisateurs qui ne sont plus d'actualité. Dans les réseaux où l'affectation des adresses IP est dynamique, la suppression automatique améliore la précision des associations des utilisateurs en veillant à ce que l'agent associe chaque adresse IP uniquement à l'utilisateur actuellement concerné. *Si vous ajoutez un profil d'analyse syntaxique Syslog prédéfini, vérifiez son nom pour déterminer s'il est destiné à correspondre aux événements de connexion ou de déconnexion.*
Nom de domaine par défaut (Expéditeur Syslog uniquement)	(Facultatif) Si le **Type** de serveur est **Syslog Sender (Expéditeur Syslog)**, entrez un nom de domaine pour remplacer le nom de domaine actuel qui se trouve dans le nom d'utilisateur de votre message syslog ou ajouter le domaine au nom d'utilisateur si votre message syslog ne contient pas de domaine.

Gestion de l'accès aux serveurs surveillés

Effectuez les tâches suivantes à la section Surveillance des serveurs afin de gérer l'accès aux serveurs que l'agent User-ID surveille pour extraire des informations de mappage d'utilisateur.

Tâche	Description
Afficher les informations sur les serveurs	Pour chaque serveur surveillé, la page Mappage d'utilisateur affiche l'État de la connexion établie entre l'agent User-ID et le serveur. Après avoir cliqué sur **Add (Ajouter)** pour ajouter un serveur, le pare-feu essaie de s'y connecter. Si la tentative de connexion est réussie, la section Surveillance des serveurs indique Connecté dans la colonne État. Si le pare-feu ne parvient pas à se connecter, la colonne État présente une condition d'erreur, telle que `Connexion refusée` ou `Expiration du délai de connexion`.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	Pour des détails sur les autres champs de la section Surveillance des serveurs, reportez-vous à Configuration de l'accès aux Serveurs surveillés.
Ajouter	Pour effectuer la Configuration de l'accès aux Serveurs surveillés, vous devez **Add (Ajouter)** chaque serveur que l'agent User-ID surveillera pour extraire les informations de mappage d'utilisateur.
Supprimer	Pour supprimer un serveur du processus de mappage d'utilisateur (détection), sélectionnez le serveur et cliquez sur **Delete (Supprimer)**. **Conseil**: Pour supprimer un serveur de la détection sans supprimer sa configuration, modifiez l'entrée du serveur et décochez l'option **Enabled (Activé)**.
Découvrez	Vous pouvez automatiquement **Discover (Détecter)** des contrôleurs de domaine Microsoft Active Directory au moyen de DNS. Le pare-feu détecte les contrôleurs de domaine en fonction du nom de domaine saisi dans la page **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, section **General Settings (Paramètres généraux)**, champ **Domain (Domaine)**. Une fois qu'il a détecté un contrôleur de domaine, le pare-feu crée une entrée pour ce dernier dans la liste Surveillance des serveurs ; vous pouvez ensuite activer le serveur pour qu'il effectue la surveillance. *la fonction de Discover (Détection) fonctionne uniquement pour les contrôleurs de domaine, pas pour les serveurs Exchange ou eDirectory.*

Inclure ou exclure des sous-réseaux pour l'association d'utilisateur

- Périphérique > Identification utilisateur > Mappage d'utilisateur

Utilisez la liste Inclure/Exclure des réseaux pour définir les sous-réseaux que l'agent User-ID inclura ou exclura lorsqu'il effectue le mappage nom d'utilisateur/adresse IP (détection). Par défaut, si vous n'ajoutez pas de sous-réseaux à la liste, l'agent User-ID effectue une détection des sources d'identification utilisateur dans tous les sous-réseaux, sauf lorsqu'il utilise le sondage WMI des systèmes clients qui possèdent des adresses IPv4 publiques. (Les adresses IPv4 publiques sont celles qui sont à l'extérieur de la portée de RFC 1918 et RFC 3927).

Pour activer le sondage WMI des adresses IPv4 publiques, vous devez ajouter leurs sous-réseaux à la liste et définir leur option **Discovery (Détection)** sur **Include (Inclure)**. Si vous configurez le pare-feu pour qu'il puisse redistribuer les informations de mappage d'utilisateurs aux autres pare-feu, les limites de découverte indiquées dans la liste vont s'appliquer aux informations redistribuées.

Utilisez les listes d'inclusion et d'exclusion pour définir les sous-réseaux dans lesquels le pare-feu effectuer le mappage d'utilisateurs.

Vous pouvez exécuter les tâches suivantes sur la liste Inclure/Exclure des réseaux :

Tâche	Description
Ajouter	Pour restreindre la découverte à un sous-réseau donné, **Add (Ajoutez)** un profil de sous-réseau et remplissez les champs suivants : • **Name (Nom)** : saisissez un nom pour identifier le sous-réseau.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	• **Enabled (Activé)** : sélectionnez cette option pour activer l'inclusion ou l'exclusion du sous-réseau lors de la surveillance du serveur. • **Détection (Discovery)** : précisez si l'agent User-ID va **Inclure** ou **Exclude (Exclure)** le sous-réseau. • **Network Address (Adresse réseau)** : saisissez la plage d'adresses IP du sous-réseau. L'agent User-ID applique une règle implicite à la liste qui va tout exclure. Par exemple, si vous ajoutez le sous-réseau 10.0.0.0/8 avec l'option **Inclure,** l'agent User-ID exclut tous les autres sous-réseaux, même si vous ne les ajoutez pas à la liste. Ajoutez des entrées avec l'option **Exclude (Exclure)** uniquement si vous souhaitez que l'agent User-ID exclue un sous-ensemble de sous-réseaux que vous avez implicitement inclus. Par exemple, si vous ajoutez 10.0.0.0/8 avec l'option **Include (Inclure)** et que vous ajoutez 10.2.50.0/22 avec l'option **Exclude (Exclure)**, l'agent User-ID procédera à une découverte sur tous les sous-réseaux de 10.0.0.0/8, sauf 10.2.50.0/22, et exclura tous les sous-réseaux n'appartenant pas à 10.0.0.0/8. Si vous ajoutez des profils **Exclude (Exclure)** sans ajouter de profils **Include (Inclure)**, l'agent User-ID exclura tous les sous-réseaux et pas uniquement ceux que vous avez ajoutés.
Supprimer	Pour supprimer un sous-réseau de la liste, sélectionnez-le et cliquez sur **Delete (Supprimer)**. **Conseil**: Pour supprimer un sous-réseau de la liste Inclure/Exclure des réseaux sans effacer sa configuration, modifiez le profil du sous-réseau et désélectionnez l'option **Enabled (Activé)**.
Séquence Inclure/Exclure les réseaux personnalisée	Par défaut, l'agent User-ID évalue les sous-réseaux dans leur ordre d'ajout, les premiers en tête de liste et les derniers en bas de liste. Pour modifier l'ordre d'évaluation, cliquez sur **Custom Include/Exclude Network Sequence (Séquence réseau d'inclusion/exclusion personnalisée)**. Vous pouvez ensuite **Add (Ajouter)**, **Delete (Supprimer)**, **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** les sous-réseaux pour créer un ordre d'évaluation personnalisé.

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Sécurité de la connexion

Modifiez ( ) les paramètres de Sécurité de la connexion User-ID pour sélectionner le profil du certificat utilisé par le pare-feu afin de valider le certificat présenté par les agents User-ID Windows. Le pare-feu utilise le profil du certificat sélectionné pour vérifier l'identité de l'agent User-ID en validant le certificat du serveur présenté par l'agent.

Tâche	Description
Profil de certificat de User-ID	Dans le menu déroulant, sélectionnez le profil du certificat à utiliser lors de l'authentification des agents User-ID Windows ou sélectionnez Nouveau profil du certificat pour créer un nouveau profil du certificat. Sélectionnez **Aucun** pour supprimer le profil du certificat et utiliser plutôt l'authentification par défaut. Pour exiger la validation des certificats du serveur avec le serveur Windows lorsque vous Configuration de l'accès aux serveurs surveillés à l'aide de Kerberos pour l'authentification du serveur, veillez à configurer NTP dans les Paramètres des services globaux et sélectionnez l'autorité de certificat racine en tant que profil de certificat.
Supprimer tout (Configuration du modèle uniquement)	Supprime le profil du certificat associé à la configuration de la Sécurité de la connexion User-ID pour le modèle sélectionné.

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Agents User-ID

Pour associaer les noms d'utilisateur vers les adresses IP, les agents User-ID surveillent diverses sources, telles que les serveurs d'annuaire. Les agents envoient les associations d'utilisateurs vers les pare-feu, les Collecteurs de journaux ou Panorama et chacun de ces appareils peut alors servir de *point de redistribution* qui transmet les associations à d'autres pare-feu, Collecteurs de journaux ou à Panorama. Pour qu'un pare-feu (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User-ID Agents (Agents User-ID)**) ou que Panorama (**Panorama** > **User Identification (Identification utilisateur)**) collecte les associations d'utilisateurs, vous devez configurer ses connexions avec les agents User-ID ou les points de redistribution.

Pour configurer les Collecteurs de journaux dédiés afin de se connecter aux agents User-ID ou aux points de redistribution, définissez les Paramètres de l'agent User-ID. *Vous ne pouvez pas configurer les Collecteurs de journaux locaux pour vous connecter aux agents User-ID ou aux points de redistribution.*

Bien que vous puissiez configurer un Collecteur de journaux ou Panorama pour redistribuer les associations d'utilisateurs, ces périphériques ne peuvent pas associer les adresses IP vers les noms d'utilisateur. Seuls les agents User-ID basés sur Windows et les agents User-ID intégrés à PAN-OS peuvent effectuer un mappage utilisateur.

La procédure complète relative à la configuration de l'association d'utilisateur *nécessite des tâches supplémentaires en plus de la configuration des connexions aux agents User-ID.*

- Configuration de l'accès aux agents User-ID
- Gestion de l'accès aux agents User-ID

Configuration de l'accès aux agents User-ID

Chaque pare-feu et chaque serveur de gestion Panorama peuvent se connecter à un maximum de 100 agents User-ID ou à des points de redistribution User-ID (ou un mélange des deux). Pour ajouter une connexion, cliquez sur **Ajouter** et renseignez les champs suivants.

Paramètres de l'agent User-ID	Description
Name (Nom)	Saisissez un nom descriptif (de 31 caractères maximum) pour l'agent User-ID ou le point de redistribution. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. *Pour un pare-feu ou un système virtuel servant de point de redistribution, ce champ ne doit pas correspondre au champ* Nom du collecteur.
Ajouter un agent à l'aide de (Pare-feu uniquement)	Sélectionnez la manière dont le pare-feu identifie l'agent User-ID ou le point de redistribution : • **Numéro de série** – Sélectionnez cette option pour un serveur de gestion Panorama qui redistribue les associations User-ID.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'agent User-ID	Description
	• **Hôte et port** – Sélectionnez cette option pour les agents User-ID basés sur Windows ou pour les pare-feu, les systèmes virtuels et les Collecteurs de journaux qui redistribuent les associations de User-ID.
Numéro de série (Pare-feu uniquement)	Sélectionnez le serveur de gestion Panorama qui redistribue les associations d'utilisateurs au pare-feu. Pour les déploiements haute disponibilité (HD), vous pouvez sélectionner le Panorama actif (**panorama**) ou le panorama passif (**panorama2**).  *Il n'est pas nécessaire de spécifier l'hôte, le port ou d'autres informations de connexion parce que vous l'avez fait lors de la configuration initiale du pare-feu.*
Hôte	• **Agent User-ID basé sur Windows** – Saisissez l'adresse IP de l'hôte Windows sur lequel l'agent User-ID est installé. • **Pare-feu (**Agent User-ID intégré à PAN-OS**)** – Saisissez l'adresse IP de l'interface MGT ou de l'itinéraire de service que le pare-feu utilise pour envoyer des associations d'utilisateurs. Pour l'interface MGT, vous pouvez saisir un nom d'hôte au lieu de l'adresse IP. • **Collecteurs de journaux qui redistribuent les associations d'utilisateurs** – Saisissez le nom d'hôte ou l'adresse IP de l'interface que le Collecteur de journaux utilise pour envoyer des associations d'utilisateurs.
Port	Saisissez le numéro de port sur lequel l'agent User-ID écoute les requêtes User-ID. La valeur par défaut est 5 007, mais vous pouvez indiquer n'importe quel port disponible. Différents agents User-ID peuvent utiliser différents ports.  *Le port par défaut pour certaines versions antérieures de l'agent User-ID est 2 010.*
Nom du collecteur Clé prépartagée du collecteur / Confirmer la clé prépartagée du collecteur	Saisissez le **Nom du collecteur** et la **Clé prépartagée** qui identifient le pare-feu ou le système virtuel en tant qu'agent User-ID. Saisissez les mêmes valeurs que lorsque vous avez configuré le pare-feu ou le système virtuel pour redistribuer les associations d'utilisateurs (reportez-vous à la section Redistribution).  *Le collecteur auquel ces champs font référence est l'agent User-ID et non un Collecteur de journaux. Ces champs ne sont configurables que lorsque l'agent est un pare-feu ou un système virtuel.*
Utiliser en tant que proxy LDAP (Pare-feu uniquement)	Sélectionnez cette option pour utiliser cet agent User-ID comme proxy pour surveiller le serveur d'annuaire pour mapper les noms d'utilisateurs à des groupes. Pour utiliser cette option, vous devez configurer l'association de groupe sur le pare-feu (Périphérique > Identification utilisateur > Paramètres d'association de groupe). Le pare-feu diffuse cette configuration à l'agent User-ID pour lui permettre d'effectuer l'association noms d'utilisateurs / groupes. Cette option s'avère utile dans les déploiements où le pare-feu ne peut accéder directement au serveur d'annuaires. Elle est également utile dans les déploiements qui ont avantage à réduire le nombre de requêtes qui doivent être traitées par le serveur d'annuaires ; plusieurs pare-feu peuvent recevoir les informations d'association de groupe

© 2020 Palo Alto Networks, Inc.

Paramètres de l'agent User-ID	Description
	de la mémoire cache d'un seul agent User-ID au lieu de demander à chaque pare-feu d'interroger le serveur directement.
Utiliser pour l'authentification NTLM (Pare-feu uniquement)	Sélectionnez cette option si vous voulez utiliser cet agent User-ID en tant que proxy pour l'authentification NTLM (NT LAN Manager) lorsqu'une requête Web client correspond à une règle de politique d'Authentification. L'agent User-ID surveille le contrôleur de domaine pour les informations relatives aux associations utilisateurs et transmet ces informations au pare-feu. Pour utiliser cette option, vous devez aussi activer l'authentification NTLM sur l'agent User-ID. Cette option s'avère utile dans les déploiements où le pare-feu ne peut accéder directement au contrôleur de domaine pour procéder à l'authentification NTLM. Elle est également utile dans les déploiements qui ont avantage à réduire le nombre de requêtes d'authentification qui doivent être traitées par le contrôleur de domaine ; plusieurs pare-feu peuvent recevoir les informations d'association d'utilisateur de la mémoire cache d'un seul agent User-ID, au lieu de demander que chaque pare-feu interroge le contrôleur de domaine directement. *Configurez les règles d'Authentification pour utiliser Ouverture de session unique Kerberos au lieu de l'authentification NTLM. Kerberos est une méthode d'authentification plus sûre et plus fiable que NTLM et ne nécessite pas que le pare-feu dispose d'un compte administrateur pour accéder au domaine. Pour plus d'informations sur la configuration des méthodes d'authentification pour les règles d'Authentification, voir Objets > Authentification.*
Activé	Sélectionnez cette option pour activer le pare-feu ou Panorama afin de communiquer avec l'agent User-ID ou le point de redistribution.
Rapport HIP	Sélectionnez cette option pour activer ce pare-feu pour qu'il reçoive les rapports HIP des autres pare-feu qui sont configurés en tant qu'agents User-ID (y compris les passerelles GlobalProtect, les collecteurs de journaux distribués, les pare-feu et Panorama). Le pare-feu peut ensuite utiliser les informations tirées des rapports HIP pour la mise en œuvre d'une politique HIP.

Gestion de l'accès aux agents User-ID

Exécutez les tâches suivantes pour gérer les connexions du pare-feu vers les agents User-ID ou les points de redistribution.

Tâche	Description
Affichage de l'information / Actualisation de la connexion	Sélectionnez **Device (Périphérique)** > **User Identification (Identification de l'utilisateur)** > **User-ID Agents (Agents User-ID)** ou **Panorama** > **User Identification (Identification de l'utilisateur)** pour vérifier si le pare-feu ou Panorama est connecté à chaque agent User-ID ou à chaque point de redistribution. La colonne Connecté affiche un icône vert pour indiquer une connexion réussie, un icône jaune pour indiquer une connexion désactivée ou un icône rouge pour indiquer un échec de connexion. Si vous pensez que l'état de la connexion a changé depuis votre premier visionnage de l'état,

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	cliquez sur **Refresh Connected (Actualiser la connexion)** pour mettre à jour l'affichage de l'état. Pour les autres champs affichés, voir Configurer l'accès aux agents User-ID.
Ajouter	**Add (Ajouter)** et ensuite Configurer l'accès aux User-ID.
Supprimer	Pour supprimer la configuration qui permet au pare-feu de se connecter à un agent User-ID ou à un point de redistribution, sélectionnez l'agent ou le point de redistribution et cliquez sur **Delete (Supprimer).**  *Pour désactiver l'accès à un agent User-ID ou à un point de redistribution sans supprimer sa configuration, modifiez-le et désélectionnez l'option Enabled (Activé).*
Séquence des agents personnalisée	Si vous activez les agents User-ID pour qu'ils exécutent l'authentification NTLM (NT LAN Manager) pour le pare-feu, le pare-feu communiquera alors par défaut avec les agents dans l'ordre où vous les avez ajoutés, de haut en bas (reportez-vous au champ **Use for NTLM Authentication (Utiliser pour l'authentification NTLM)** de la section Configuration de l'accès aux agents d'ID utilisateur). Pour modifier l'ordre dans lequel le pare-feu communique avec les agents, cliquez sur **Custom Agent Sequence (Séquence d'agents personnalisée)**, vous devez ensuite **Add (Ajouter)** chaque agent et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** les agents pour les repositionner, enfin, cliquez sur **OK.**
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau de configuration de l'agent User-ID au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Agents de Terminal Server

Sur un système qui prend en charge plusieurs utilisateurs qui partagent une même adresse IP, l'agent Terminal Server (TS) identifie chaque utilisateur en lui affectant une plage de ports spécifiques. L'agent TS indique à chaque pare-feu connecté la plage de ports qui a été affectée afin que les pare-feu puissent appliquer la politique en fonction des utilisateurs et des groupes d'utilisateurs.

Tous les modèles de pare-feu peuvent collecter des informations de mappage de noms d'utilisateur vers des ports à partir de plus de 5 000 systèmes multi-utilisateurs. Le nombre d'agents TS à partir duquel un pare-feu peut collecter les informations de mappage varie selon le modèle de pare-feu.



Vous devez installer et configurer les agents TS avant d'en configurer l'accès. La procédure complète visant à configurer le mappage d'utilisateur pour les utilisateurs de serveurs de terminaux nécessite des tâches supplémentaires en plus de la configuration des connexions aux agents TS.

Vous pouvez exécuter les tâches suivantes pour gérer l'accès aux agents TS :

Tâche	Description
Affichage de l'information / Actualisation de la connexion	À la page **Terminal Server Agents (Agents de Terminal Server)**, la colonne Connecté affiche l'état des connexions du pare-feu vers les agents TS. Une icône verte indique une connexion réussie, une icône jaune indique une connexion désactivée et une icône rouge indique un échec de connexion. Si vous pensez que l'état de la connexion a changé depuis votre première ouverture de la page, cliquez sur **Refresh Connected (Actualisation de la connexion)** pour mettre à jour l'affichage.
Ajouter	Pour configurer l'accès à un agent TS, cliquez sur **Ajouter** et configurez les champs suivants : • **Nom** – Saisissez un nom permettant d'identifier l'agent TS (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. • **Host (Hôte)** - Saisissez l'adresse IP statique ou le nom d'hôte du serveur de terminaux sur lequel l'agent TS est installé. • **Port** – Saisissez le numéro de port (valeur par défaut : 5 009) que le service Agent TS utilise pour communiquer avec le pare-feu. • **Adresses IP de remplacement** – Si le serveur de terminal sur lequel l'agent TS est installé dispose de plusieurs adresses IP qui peuvent apparaître comme adresse IP source du trafic sortant, cliquez sur **Ajouter** et saisissez jusqu'à huit adresses IP statiques ou noms d'hôte supplémentaires. • **Enabled (Activé)** - Sélectionnez cette option pour activer le pare-feu afin de communiquer avec cet agent TS.
Supprimer	Pour supprimer la configuration qui permet l'accès à un agent TS, sélectionnez l'agent et cliquez sur **Delete (Supprimer)**.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	 *Pour désactiver l'accès à un agent TS sans supprimer sa configuration, modifiez-le et désélectionnez l'option Activé.*
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau de configuration du périphérique au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Onglet Paramètres de mappage de groupe

- **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**

Pour baser des politiques de sécurité et des rapports sur des utilisateurs ou un groupe d'utilisateurs, le pare-feu doit récupérer la liste des groupes et la liste des membres correspondante spécifiée et gérée sur vos serveurs d'annuaire. Le pare-feu prend en charge divers serveurs d'annuaires LDAP, notamment Microsoft Active Directory (AD), Novell eDirectory et Sun ONE Directory Server.

Le nombre de groupes distincts d'utilisateurs que chaque pare-feu ou Panorama peut référencer parmi toutes les politiques varie selon le modèle. Cependant, peu importe le modèle, vous devez configurer un profil de serveur LDAP (Périphérique > Profils de serveur > LDAP) avant de pouvoir créer une configuration de mappage de groupe.



La procédure complète pour associer des noms d'utilisateur à des groupes exige l'accomplissement de tâches supplémentaires en plus de la création de configurations d'association de groupe.

Add (Ajoutez) et configurez les champs suivants, au besoin, pour créer une configuration d'association de groupe. Pour supprimer une configuration d'associations de groupe, sélectionnez-la, puis cliquez sur **Delete (Supprimer)**. Si vous souhaitez désactiver une configuration d'association de groupe sans l'effacer, modifiez la configuration et désélectionnez l'option **Enabled (Activée)**.

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
Name (Nom)	**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**	Donnez un nom pour identifier la configuration d'association de groupe (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Profil de serveur	**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres d'association de groupe)** > **Server Profile (Profil de serveur)**	Sélectionnez le profil de serveur'A0;LDAP à utiliser pour le mappage de groupe sur ce pare-feu.
Intervalle de mise à jour		Indiquez l'intervalle en secondes après lequel le pare-feu établit une connexion au serveur d'annulaire LDAP pour obtenir toutes les mises à jour des groupes que les politiques de pare-feu utilisent (plage comprise entre 60 et 86 400).
Domaine d'utilisateur		Par défaut, le champ **User Domain (Domaine d'utilisateur)** est vide : le pare-feu détecte automatiquement les noms de domaine des serveurs Active Directory. Si vous saisissez une valeur, elle remplacera tout nom de domaine que

© 2020 Palo Alto Networks, Inc.

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
		le pare-feu récupère de la source LDAP. Votre entrée doit correspondre au nom NetBIOS. *Ce champ n'affecte que les noms d'utilisateur et de groupe récupérés dans la source LDAP. Pour remplacer le domaine associé à un nom d'utilisateur pour l'authentification de l'utilisateur, configurez le User Domain (Domaine d'utilisateur) et le Username Modifier (Modificateur du nom d'utilisateur) pour le profil d'authentification que vous attribuez à cet utilisateur (voir Périphérique > Profil d'authentification).*
Objets du groupe		• **Search Filter (Filtre de recherche)** : saisissez une requête LDAP qui précise les groupes à récupérer et à suivre. • **Object Class (Classe d'objets)** : saisissez une définition de groupe. Le paramètre par défaut est objectClass=group, ce qui indique que le système récupère tous les objets de l'annuaire correspondant au **Search Filter (Filtre de recherche)** de groupe, dont objectClass=group.
Objets utilisateur		• **Search Filter (Filtre de recherche)** : saisissez une requête LDAP qui précise les utilisateurs à récupérer et à suivre. • **Object Class (Classe d'objet)** : saisissez une définition d'un objet utilisateur. Par exemple, dans Active Directory, cet attribut est *user*.
Activé		Sélectionnez cette option pour activer le profil de serveur pour le mappage de groupe.
Récupérez la liste des périphériques gérés		Pour les déploiements GlobalProtect, sélectionnez cette option pour permettre au pare-feu d'extraire les numéros de série à partir d'un serveur d'annuaires (comme Active Directory). GlobalProtect peut ainsi identifier l'état des points de terminaison qui se connectent et appliquer les politiques de sécurité basées sur HIP en fonction de la

© 2020 Palo Alto Networks, Inc.

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
		présence du numéro de série des points de terminaison.
Attributs utilisateur	**Device (Périphérique) > User Identification (Identification utilisateur) > Group Mapping Settings (Paramètres de mappage de groupe) > User and Group Attributes (Attributs utilisateur et groupe)**	Précisez les attributs d'annuaire pour identifier les utilisateurs : • **Primary Username (Nom d'utilisateur principal)** : spécifiez l'attribut que la source User-ID fournit au nom d'utilisateur (par exemple, **`userPrincipalName`** ou **`sAMAccountName`**). *Le nom d'utilisateur principal est la manière dont le pare-feu identifie l'utilisateur dans les journaux, les rapports et les configurations de politique, même si le pare-feu reçoit d'autres formats des sources User-ID. Si vous ne spécifiez pas de format, le pare-feu utilise le format `sAMAccountName` par défaut pour Active Directory et le format `uid` pour Novell eDirectory et Sun ONE Directory Server.* • **E-Mail (Courriel)** : spécifiez l'attribut que la source User-ID fournit à l'adresse électronique. La valeur par défaut est **`mail`**. • **Alternate Username 1-3 (Nom d'utilsateur 1-3 alternatif)** : précisez un maximum de trois attributs supplémentaires qui correspondent aux formats que vos sources User-ID peuvent envoyer. *Si vous configurez un serveur Active Directory, le nom d'utilisateur alternatif 1 est `userPrincipalName` par défaut.*
Attributs de groupes		Précisez les attributs que les sources User-ID utilisent pour identifier les groupes : • **Group Name (Nom du groupe)** : précisez l'attribut que la source User-ID utilise pour l'attribut nom de groupe. Par défaut, l'attribut d'Active Directory est `name` et celui de

© 2020 Palo Alto Networks, Inc.

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
		Novell eDirectory et de Sun ONE Directory Server est `cn`. • **Group Member (Membre du groupe)** : spécifiez l'attribut que la source User-ID utilise pour le membre du groupe. La valeur par défaut est `member`. • **E-Mail (Courriel)** : spécifiez l'attribut que la source User-ID utilise pour l'adresse électronique. La valeur par défaut est `mail`.
Groupes disponibles Groupes inclus	**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)** > **Group Include List (Liste d'inclusion de groupes)**	Utilisez ces champs pour restreindre le nombre de groupes que le pare-feu affiche lorsque vous créez une règle de sécurité. Parcourez l'arborescence LDAP pour trouver les groupes que vous souhaitez utiliser dans les règles. Pour inclure un groupe, sélectionnez-le et ajoutez-le ( ) dans la liste des Groupes disponibles. Pour supprimer un groupe de la liste, sélectionnez-le et supprimez-le ( ) de la liste des Groupes inclus. Le maximum combiné pour les listes **Included Groups (Groupes inclus)** et **Custom Group (Groupe personnalisé)** correspond à 640 saisies pour chaque configuration d'association de groupe. *N'incluez que les groupes que vous devez inclure pour que le pare-feu ne puisse récupérer les associations de groupe d'utilisateurs que pour les groupes nécessaires et non pas de l'arbre au complet de l'annuaire LDAP.*
Name (Nom) Filtre LDAP	**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)** > **Custom Group (Groupe personnalisé)**	Créez des groupes personnalisés basés sur des filtres LDAP de manière à pouvoir baser les politiques du pare-feu sur les attributs utilisateur qui ne correspondent pas aux groupes d'utilisateurs existants dans le répertoire LDAP. Le service User-ID mappe tous les utilisateurs du répertoire LDAP correspondant au filtre du groupe personnalisé. Si vous créez un groupe personnalisé dont le Nom distingué (ND) est le même que le nom de domaine d'un groupe Active Directory existant, le pare-feu va utiliser le groupe personnalisé dans toutes les références à ce nom (par exemple, dans

© 2020 Palo Alto Networks, Inc.

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
		les politiques et les journaux). Pour créer un groupe personnalisé, cliquez sur **Add (Ajouter)** et configurez les champs suivants : • **Name (Nom)** : saisissez un nom de groupe personnalisé qui est unique dans la configuration d'associationde groupe du pare-feu ou du système virtuel actuel. • **LDAP Filter (Filtre LDAP)** : saisissez un filtre de 2 048 caractères maximum.  *Utilisez uniquement les attributs indexés dans le filtre pour faciliter les recherches LDAP et minimiser l'impact sur les performances sur le serveur d'annuaire LDAP ; le pare-feu ne valide pas les filtres LDAP.* Le maximum combiné pour les listes **Included Groups (Groupes inclus)** et **Custom Group (Groupe personnalisé)** correspond à 640 saisies. Pour supprimer un groupe personnalisé, sélectionnez-le, puis cliquez sur **Delete (Supprimer)**. Pour copier un groupe personnalisé, sélectionnez-le, cliquez sur **Clone (Cloner)**, puis modifiez les champs de manière appropriée.  *Après avoir ajouté ou cloné un groupe personnalisé, vous devez Commit (Valider) vos modifications avant que votre nouveau groupe personnalisé soit disponible dans les politiques et les objets.*

© 2020 Palo Alto Networks, Inc.

Périphérique > Identification utilisateur > Paramètres du portail captif

Modifiez ( ) les paramètres du Portail captif pour configurer le pare-feu afin qu'il puisse authentifier les utilisateurs dont le trafic correspond à une règle de politique d'authentification.

Si le Portail captif utilise un profil de service SSL/TLS (Périphérique > Gestion des certificats > Profil de service SSL/TLS), un profil d'authentification (Périphérique > Profil d'authentification), ou un profil de certificat (Périphérique > Gestion des certificats > Profil du certificat), configurez le profil avant de commencer. La procédure complète pour configurer le Portail captif requiert des tâches supplémentaires en plus de la configuration de ces profils.

Vous devez Activer le portail captif pour appliquer la politique d'authentification (voir Politiques > Authentification).

Champ	Description
Activer le portail captif	Sélectionnez cette option pour activer le Portail captif.
Minuteur d'inactivité (minutes)	Saisissez la valeur TTL (Time-To-Live) de l'utilisateur en minutes pour une session du Portail captif (plage comprise entre 1 et 1 440 ; par défaut 15). Ce minuteur est remis à zéro à chaque activité de l'utilisateur du portail captif. Si la durée d'inactivité d'un utilisateur dépasse la valeur du **Idle Timer (Minuteur d'inactivité)**, PAN-OS supprime le mappage d'utilisateur du Portail captif et l'utilisateur doit se connecter à nouveau.
Temps (minutes)	Il s'agit de la valeur TTL maximale en minutes, c'est-à-dire le délai maximum pendant lequel une session du Portail captif peut demeurer mappée (plage comprise entre 1 et 1 440 ; par défaut 60). Une fois cette durée écoulée, PAN-OS supprime le mappage, et les utilisateurs doivent se réauthentifier même si la session est active. Ce minuteur permet d'éviter les mappages obsolètes et remplace la valeur **Idle Timer (Minuteur d'inactivité)**. *Il est recommandé de toujours définir le Timer (Minuteur) d'expiration sur une valeur supérieure à celle du Idle Timer (Minuteur d'inactivité).*
Profil de service SSL/TLS	Pour indiquer un certificat du serveur de pare-feu et les protocoles autorisés pour sécuriser les requêtes de redirection, sélectionnez un profil de service SSL/TLS (voir Périphérique > Gestion des certificats > Profil de service SSL/TLS). Si vous sélectionnez **None (Aucun)**, le pare-feu utilise son certificat local par défaut pour les connexions SSL/TLS. *Dans le profil de service SSL/TLS, définissez la Min Version (Version min) sur TLSv1.2 et définissez la Max Version (Version max) sur Max pour fournir la sécurité la plus forte contre les vulnérabilités du protocole SSL/TLS. L'établissement de la Max Version (Version max) sur Max garantit que le pare-feu utilise*

© 2020 Palo Alto Networks, Inc.

Champ	Description
	toujours la dernière version au fur et à mesure que les protocoles plus forts deviennent disponibles. Pour rediriger de manière transparente les utilisateurs sans afficher d'erreurs de certificat, assignez un profil associé à un certificat correspondant à l'adresse IP de l'interface vers laquelle les requêtes Web sont redirigées.
Profil d'authentification	Vous pouvez sélectionner un profil d'authentification (Périphérique > Profil d'authentification) pour authentifier les utilisateurs lorsque leur trafic correspond à une règle de politique d'authentification (Politiques > Authentification). Cependant, le profil d'authentification que vous sélectionnez dans les Paramètres du portail captif s'applique uniquement aux règles qui font référence à l'un des objets d'application d'authentification par défaut (Objets > Authentification). Ceci est généralement le cas juste après une mise à niveau vers PAN-OS 8.0, car toutes les règles d'authentification font initialement référence aux objets par défaut. Pour les règles qui font référence aux objets d'application d'authentification personnalisés, sélectionnez le profil d'authentification lorsque vous créez l'objet.
Port réseau GlobalProtect pour les invites d'authentification entrante (UDP)	Indiquez le port utilisé par GlobalProtect™ pour recevoir les invites d'authentification entrantes des passerelles multifacteur (MFA). (La plage est comprise entre 1 et 65 536 ; par défaut 4 501). Pour prendre en charge l'authentification multifacteur, un point de terminaison GlobalProtect doit recevoir et reconnaître les invites UDP qui proviennent de la passerelle MFA. Lorsqu'un point de terminaison GlobalProtect reçoit un message UDP sur le port réseau spécifié et que le message UDP provient d'un pare-feu ou d'une passerelle de confiance, GlobalProtect affiche le message d'authentification (voir Personnaliser l'application GlobalProtect).
Mode	Sélectionnez comment les demandes Web sont capturées pour l'authentification : • **Transparent** – Le pare-feu intercepte les demandes Web conformément à la règle d'Authentification et remplace l'URL de destination d'origine, générant un message HTTP 401 pour inviter l'utilisateur à s'authentifier. Toutefois, étant donné que le pare-feu ne dispose pas du certificat de l'URL de destination, le navigateur affiche une erreur de certificat aux utilisateurs qui tentent d'accéder à un site sécurisé. N'utilisez donc ce mode qu'en cas de nécessité, dans des déploiements de couche 2 ou virtuels par exemple. • **Redirect (Rediriger)** – Le pare-feu intercepte les requêtes Web selon la règle d'authentification et les redirige vers l'Hôte de redirection indiqué. Le pare-feu utilise une redirection HTTP 302 pour inciter l'utilisateur à s'authentifier. Il est recommandé d'utiliser la fonction de **Redirect (redirection)**, car elle fournit une meilleure expérience aux utilisateurs finaux (elle n'affiche aucune erreur de certificat et autorise les cookies de session qui permettent une navigation transparente, car la **Redirect (redirection)** n'effectue aucune réaffection à l'expiration des délais). Cependant, cette étape nécessite que vous activiez les pages de réponses sur le profil de gestion de l'interface affecté à l'interface d'entrée de couche 3 (pour plus de détails, voir Réseau > Profils réseaux > Gestion de l'interface et Interface de couche 3 de la série PA-7000). Un autre avantage du mode Rediriger est qu'il autorise les cookies de session, ce qui permet à l'utilisateur de continuer à consulter des sites authentifiés sans qu'un nouveau mappage soit exigé à chaque expiration du délai. Ceci est particulièrement utile pour les utilisateurs passant d'une adresse IP à une autre (du LAN d'entreprise

© 2020 Palo Alto Networks, Inc.

Champ	Description
	au réseau sans fil par exemple), car ils ne doivent pas nécessairement s'authentifier à nouveau lorsque leur adresse IP change tant que la session est ouverte.  *Le mode Redirect (Rediriger) est requis si le Portail captif utilise l'authentification SSO Kerberos ou NTLM, car le navigateur fournit des informations d'identification uniquement aux sites approuvés. Le mode Redirect (Rediriger) est également requis si le Portail captif utilise l'authentification multifacteur (MFA).*
Cookie de session (Mode Rediriger uniquement)	• **Enable (Activer)** : sélectionnez cette option pour activer les cookies de session. • **Timeout (Délai)** : si vous **Enable (Activez)** les cookies de session, ce minuteur précise le nombre de minutes pendant lesquelles le cookie est valide (intervalle compris entre 60 et 10 080 ; valeur par défaut : 1 440).  *Définissez une valeur de délai assez courte, pour éviter qu'elle n'entraîne d'entrées de mappage utilisateur obsolètes dans les cookies, mais assez longue pour favoriser une bonne expérience utilisateur en évitant d'inviter les utilisateurs à se connecter plusieurs fois au cours d'une session. Commencez par une valeur inférieure ou égale à 480 minutes (8 heures) et ajustez la valeur au besoin.* • **Roaming (Itinérance)** – Sélectionnez cette option pour mettre en mémoire le cookie si l'adresse IP subit une modification lorsque la session est active (par exemple, quand le point de terminaison passe d'un réseau filaire à un réseau sans fil). L'utilisateur doit uniquement se réauthentifier si le cookie expire ou si l'utilisateur ferme le navigateur.
Rediriger l'hôte (Mode Rediriger uniquement)	Indiquez le nom d'hôte intranet qui résout en adresse IP l'interface de couche 3 vers laquelle le pare-feu redirige les requêtes Web.  *Si les utilisateurs s'authentifient via l'ouverture de session unique (SSO) Kerberos, le Redirect Host (Hôte de redirection) doit être identique au nom d'hôte indiqué dans le Keytab Kerberos.*
Profil du certificat	Vous pouvez sélectionner un profil de certificat (Périphérique > Gestion des certificats > Profil du certificat) pour authentifier les utilisateurs lorsque leur trafic correspond à une règle de politique d'authentification (Politiques > Authentification). Pour ce type d'authentification, le Portail captif invite le navigateur du point de terminaison à présenter un certificat client. Par conséquent, vous devez déployer des certificats clients à chaque système utilisateur. En outre, vous devez installer sur le pare-feu le certificat d'autorité de certification (AC) qui a émis les certificats clients et qui a attribué le certificat AC au profil du certificat. Il s'agit de la seule méthode d'authentification permettant une authentification **Transparent (Transparente)** des points de terminaison macOS et Linux.
Authentification NTLM	Lorsque vous configurez le Portail captif pour l'authentification NTLM (NT LAN Manager), le pare-feu utilise un mécanisme de demande / réponse crypté pour obtenir en toute transparence les informations d'identification de l'utilisateur à partir du navigateur sans inviter l'utilisateur à les saisir.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Pour générer une requête d'authentification NTLM, les règles de politique d'Authentification doivent spécifier un objet d'**Authentication Enforcement (Application de l'authentification)** avec la **Authentication Method (Méthode d'authentification)** définie sur **browser-challenge (défi de navigation)** ou **default-browser-challenge (défi de navigation par défaut)** (Objets > Authentification). Si l'objet spécifie un **Authentication Profile (Profil d'authentification)** avec une ouverture de session unique Kerberos (SSO) activée, le pare-feu tente d'abord une authentification Kerberos avant de revenir à NTLM. Si le navigateur ne parvient pas à exécuter l'authentification NTLM ou en cas d'échec de l'authentification NTLM, le pare-feu revient au **web-form (formulaire Web)** ou au **default-web-form (formulaire Web par défaut)**, servant de **Authentication Method (Méthode d'authentification)**. Par défaut, Internet Explorer prend en charge NTLM. Vous pouvez configurer Firefox et Chrome pour qu'ils l'utilisent, mais vous ne pouvez pas utiliser NTLM pour authentifier des points de terminaison non Windows.  *Choisissez l'authentification transparente Kerberos SSO plutôt que l'authentification NTLM lors de la configuration du Portail captif. Kerberos est une méthode d'authentification plus solide et robuste que NTLM et ne nécessite pas que le pare-feu dispose d'un compte administrateur pour joindre le domaine.*  *Ces options ne s'appliquent qu'aux agents User-ID Windows. Lorsque vous utilisez l'agent User-ID intégré à PAN-OS, le pare-feu doit être en mesure de résoudre le nom DNS de votre contrôleur de domaine pour joindre le domaine. Dans la configuration de l'agent User-ID intégré à PAN-OS, vous pouvez ensuite procéder à l'activation de l'authentification NTLM et fournir les informations d'identification pour que le pare-feu puisse joindre le domaine. NTLM n'est disponible que pour Windows Server version 2003 et versions antérieures.* Pour configurer NTLM afin qu'il soit utilisé avec les agents User-ID Windows, définissez les éléments suivants : • **Attempts (Tentatives)** : le nombre de tentatives après lequel l'authentification NTLM échoue (plage de 1 à 60, 1 par défaut). • **Timeout (Délai)** : le nombre de secondes après lequel l'authentification NTLM expire (plage de 1 à 60, 2 par défaut). • **Reversion Time (Temps de restauration)** – Le nombre de secondes après lesquelles le pare-feu tentera à nouveau de contacter le premier agent User-ID énuméré (dans **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User-ID Agents (Agents User-ID)**) après une indisponibilité de cet agent (plage comprise entre 60 et 3 600 ; par défaut 300).

© 2020 Palo Alto Networks, Inc.

GlobalProtect

GlobalProtect™ propose une infrastructure complète pour la gestion de votre personnel mobile pour permettre un accès sécurisé à tous vos utilisateurs, indépendamment des périphériques qu'ils utilisent ou de l'endroit où ils se trouvent. Les pages de l'interface Web du pare-feu suivantes vous permettent de configurer et de gérer les composants de GlobalProtect :

- Réseau > GlobalProtect > Portails
- Réseau > GlobalProtect > Passerelles
- Réseau > GlobalProtect > Gestionnaire de périphériques mobiles
- Réseau > GlobalProtect > Liste de blocage de périphériques
- Réseau > GlobalProtect > Applications sans client
- Réseau > GlobalProtect > Groupes d'applications sans client
- Objets > GlobalProtect > Objets HIP
- Objets > GlobalProtect > Profils HIP
- Périphérique > Client GlobalProtect

Vous souhaitez en savoir plus ?

Reportez-vous au Guide de l'administrateur GlobalProtect pour en savoir plus sur GlobalProtect, y compris à propos des détails sur la configuration de l'infrastructure GlobalProtect, la façon d'utiliser les informations de l'hôte pour appliquer la politique ainsi que les instructions étape par étape pour des configurations standard de déploiements GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Portails

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** pour configurer et gérer un portail GlobalProtect™. Le portail fournit les fonctions de gestion de l'infrastructure GlobalProtect. Chaque terminal qui participe au réseau GlobalProtect reçoit ses informations de configuration du portail, notamment des informations sur les passerelles disponibles ainsi que les certificats clients requis pour que l'application se connecte à une passerelle. De plus, le portail contrôle le comportement et la distribution du logiciel de l'application GlobalProtect à la fois sur les terminaux Windows et MacOS. Pour les points de terminaison Linux, vous devez obtenir le logiciel du site de soutien ; pour les périphériques mobiles, l'application GlobalProtect est distribuée via App Store Apple pour les périphériques iOS, via Google Play pour les périphériques Android et via Microsoft Store pour Windows Phone et d'autres périphériques UWP Windows. Pour les Chromebooks, l'application GlobalProtect est distribuée par la console de gestion Chromebook ou via Google Play).

Pour ajouter une configuration de portail, cliquez sur **Add (Ajouter)** ; la boîte de dialogue Portail GlobalProtect s'affiche alors.

Que voulez-vous faire ?	Reportez-vous à la section :
Quels paramètres généraux devrais-je configurer pour le portail GlobalProtect ?	Onglet Général Portails GlobalProtect
Comment puis-je associer un profil d'authentification à une configuration de portail ou de passerelle ?	Onglet d'Authentification des portails GlobalProtect
Comment puis-je définir les données que l'application GlobalProtect collecte auprès des points de terminaison ?	Onglet Collecte de données du portail GlobalProtect
Quelles options d'authentification client puis-je configurer ?	Onglet Authentification de l'agent des portails GlobalProtect
Comment puis-je assigner une configuration à un groupe spécifique d'appareils, en me basant sur le système d'exploitation, l'utilisateur et/ou le groupe d'utilisateurs ?	Onglet des Critères de sélection de la configuration de l'agent des portails GlobalProtect
Comment puis-je configurer les paramètres et la priorité des passerelles internes ?	Onglet Agent interne des portails GlobalProtect
Comment puis-je configurer les paramètres et la priorité des passerelles externes ?	Onglet Agent externe des portails GlobalProtect
Comment puis-je créer des configurations client pour différents types d'utilisateurs ?	Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect)

© 2020 Palo Alto Networks, Inc.

Que voulez-vous faire ?	Reportez-vous à la section :
Quels paramètres puis-je personnaliser concernant le look et le comportement de l'application GlobalProtect?	Onglet Application de l'agent des portails GlobalProtect
Comment puis-je configurer les options de collecte de données HIP?	Onglet Collecte de données HIP de l'agent des portails GlobalProtect
Comment puis-je configurer le portail GlobalProtect pour permettre l'accès aux applications Web sans installer l'application GlobalProtect ?	Onglet des VPN sans client des portails GlobalProtect
Comment puis-je étendre ma connectivité VPN à un pare-feu qui agit comme un satellite ?	Onglet du satellite du portail GlobalProtect
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées sur la configuration du portail, reportez-vous à la section Configuration d'un portail GlobalProtect du *Guide de l'administrateur de GlobalProtect*.

Onglet Général Portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **General (Général)**

Sélectionnez l'onglet **General (Général)** pour définir les paramètres réseau que l'application GlobalProtect utilise pour se connecter au portail GlobalProtect. En option, vous pouvez désactiver la page de connexion ou spécifier un portail de connexion et des pages d'aide personnalisé pour GlobalProtect. Pour plus d'informations sur la création et l'importation des pages personnalisées, reportez-vous à la section Personnaliser les pages Ouverture de session sur le portail, Accueil et Aide dans le Guide de l'administrateur de GlobalProtect.

Paramètres du portail GlobalProtect	Description
Name (Nom)	Saisissez un nom pour le portail (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel le portail GlobalProtect est disponible. Pour un pare-feu qui n'est pas en mode Plusieurs systèmes virtuels, la sélection **Location (Emplacement)** n'est pas disponible. Après avoir enregistré le portail, vous ne pouvez plus changer **Location (Emplacement)**.
paramètres du réseau	

© 2020 Palo Alto Networks, Inc.

Paramètres du portail GlobalProtect	Description
Interface	Sélectionnez le nom de l'interface de pare-feu qui sera le point d'entrée pour les communications avec les points de terminaison distants et les pare-feu. *N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l'interface de gestion à l'Internet. Reportez-vous à la section* Pratiques exemplaires pour sécuriser l'accès administratif *pour obtenir de plus amples précisions sur la manière de protéger l'accès à votre réseau de gestion.*
Adresse IP	Spécifiez l'adresse IP sur laquelle exécuter le service Web du portail GlobalProtect. Sélectionnez le **Type d'adresse IP**, puis saisissez l'**Adresse IP**. • L'adresse IP peut être de type **IPv4** (pour le trafic IPv4 uniquement), **IPv6** (pour le trafic IPv6 uniquement) ou **IPv4 et IPv6**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. • L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. • Si vous choisissez **IPv4 et IPv6**, saisissez le type d'adresse IP appropriée pour chacun.
Apparence	
Page de connexion au portail	(Facultatif) Choisissez une page de connexion personnalisée pour l'accès utilisateur au portail. Vous pouvez sélectionner la page **factory-default (par défaut)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**. Pour empêcher l'accès à cette page depuis un navigateur Web, vous devez **Désactiver** cette page.
Page d'accueil du portail	(Facultatif) Choisissez une page d'accueil personnalisée pour le portail. Vous pouvez sélectionner la page **factory-default (par défaut)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**.
Page d'aide de l'application	(Facultatif) Choisissez une page d'aide personnalisée facultative pour aider l'utilisateur à utiliser GlobalProtect. Vous pouvez sélectionner la page **factory-default (par défaut)** ou **Import (Importer)** une page personnalisée. La page d'aide programmée par défaut est fournie avec le logiciel de l'application GlobalProtect. Si vous sélectionnez une page d'aide personnalisée, le portail GlobalProtect fournit la page d'aide avec la configuration du portail GlobalProtect. Lorsque vous laissez la valeur par défaut (**None (Aucune)**), l'application GlobalProtect supprime la page et supprime l'option du menu.

© 2020 Palo Alto Networks, Inc.

Onglet d’Authentification des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Authentication (Authentification)**

Sélectionnez l’onglet **Authentication (Authentification)** pour configurer les divers paramètres du portail GlobalProtect™ :

- Un profil de service SSL/TLS que le portail et les serveurs utilisent pour l'authentification. Le profil de service est indépendant des autres paramètres d'Authentification.
- Les schémas d'authentification uniques qui sont basés principalement sur le système d'exploitation de l'utilisateur terminal et secondairement sur un profil d'authentification facultatif.
- (Facultatif) Un **Certificate Profile (Profil du certificat)** qui permet à GlobalProtect d'utiliser un profil de certificat spécifique pour authentifier l'utilisateur. Le certificat du client doit correspondre au profil du certificat (si les certificats clients font partie du plan de sécurité).

Paramètres d’authentification du portail GlobalProtect	Description
Authentification du serveur	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS existant. Le profil indique un certificat et les protocoles autorisés pour protéger le trafic sur l'interface de gestion. Le champ Common Name (nom commun ; CN) et, le cas échéant, le champ Subject Alternative Name (autre nom de l'objet ; SAN) du certificat associé au profil doivent correspondre à l'adresse IP ou au FQDN de l'**Interface** sélectionnée dans l'onglet **General (Général)**. *Dans les configurations VPN GlobalProtect, utilisez un profil associé à un certificat d’une autorité de certification tierce de confiance ou un certificat généré par votre autorité de certification d’entreprise interne.*
Authentification du client	
Name (Nom)	Entrez un nom pour identifier la configuration de l'authentification client. (La configuration de l'authentification du client est indépendante du profil de service SSL/TLS). Vous pouvez créer plusieurs configurations d'authentification du client et les différencier principalement par le système d'exploitation et en outre par des profils d'authentification uniques (pour le même système d'exploitation). Par exemple, vous pouvez ajouter des configurations d'authentification client pour différents systèmes d'exploitation, mais aussi avoir des configurations différentes pour le même système d'exploitation qui sont différenciées par des profils d'authentification unique. (Vous devriez ordonner manuellement ces profils du spécifique au plus général. Par exemple, tous les utilisateurs et tout système d'exploitation sont les plus généraux.) Vous pouvez également créer des configurations que GlobalProtect déploie sur les applications en mode **Pre-logon (Préouverture de session)** (c'est-à-dire avant que l'utilisateur ne se connecte au système) ou qu’il applique à n'importe

© 2020 Palo Alto Networks, Inc.

Paramètres d'authentification du portail GlobalProtect	Description
	quel utilisateur. (Préouverture de session établit un tunnel VPN à une passerelle GlobalProtect avant que l'utilisateur se connecte à GlobalProtect.)
Système d'exploitation	Pour déployer un profil d'authentification client spécifique sur le système d'exploitation d'un point de terminaison, vous devez **Add (Ajouter)** le système d'exploitation (**Tous**, **Android**, **Chrome**, **iOS**, **IoT [IdO]**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**). Le système d'exploitation est le différentiateur principal entre les configurations. (Voir le Profil d'Authentification pour une différenciation plus poussée.) Les options additionnelles du **Browser (Navigateur)** et du **Satellite** vous permettent de spécifier le profil d'authentification à utiliser pour des scénarios spécifiques. Sélectionnez **Browser (Navigateur)** pour spécifier le profil d'authentification à utiliser pour authentifier un utilisateur accédant au portail à partir d'un navigateur Web avec l'intention de télécharger l'application GlobalProtect (Windows et Mac). Sélectionnez **Satellite** pour spécifier le profil d'authentification à utiliser pour authentifier le satellite (LSVPN).
Profil d'authentification	En plus de distinguer une configuration d'authentification de client par le système d'exploitation, vous pouvez différencier davantage en spécifiant un profil d'authentification. (Vous pouvez créer un **New Authentication Profile (Nouveau profil d'authentification)** ou en sélectionnez un existant.) Pour configurer plusieurs options d'authentification pour un système d'exploitation, vous pouvez créer plusieurs profils d'authentification de client. *Si vous configurez un LSVPN dans Gateways (Passerelles), vous ne pouvez pas enregistrer cette configuration sauf si vous sélectionnez un profil d'authentification ici. Aussi, si vous envisagez d'utiliser des numéros de série pour authentifier les satellites, le portail doit avoir un profil d'authentification disponible quand il ne peut pas localiser ou valider un numéro de série de pare-feu.* Reportez-vous à la section Périphérique > Profil d'authentification.
Étiquette de nom d'utilisateur	Indiquez une étiquette de nom d'utilisateur personnalisée pour la connexion au portail GlobalProtect. Par exemple, **Nom d'utilisateur (uniquement)** ou **Adresse électronique (nomd'utilisateur@domaine)**.
Étiquette de mot de passe	Indiquez une étiquette de mot de passe personnalisée pour la connexion au portail GlobalProtect. Par exemple, **Mot de passe (Turc)** ou **Code secret** (pour l'authentification basée sur jeton à deux facteurs).
Message d'authentification	Pour aider les utilisateurs finaux à connaître le type d'informations dont ils ont besoin pour se connecter, entrez un message ou gardez le message par défaut. La longueur est de 256 caractères maximum.
Permettre l'authentification avec les informations d'identification de	Si vous sélectionnez **No (Non)**, les utilisateurs doivent s'authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur et les certificats de client. Si vous sélectionnez **Yes (Oui)**, les utilisateurs

© 2020 Palo Alto Networks, Inc.

Paramètres d'authentification du portail GlobalProtect	Description
l'utilisateur OU le certificat du client	peuvent s'authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur ou les certificats de client.
Profil du certificat	
Profil du certificat	(Facultatif) Sélectionnez le **Certificate Profile (Certificat du profil)** que le portail utilise pour correspondre aux certificats clients qui viennent des extrémités utilisateur. Avec un Profil du certificat, le portail n'authentifie l'utilisateur que si le certificat du client correspond à ce profil. Si vous établissez l'option **Allow Authentication with User Credentials OR Client Certificate (Permettre l'authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **No (Non)**, vous devez sélectionner un **Certificate Profile (Profil de certificat)**. Si vous établissez l'option **Allow Authentication with User Credentials OR Client Certificate (Permettre l'authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **Yes (Oui)**, le **Certificate Profile (Profil de certificat)** est facultatif. Le profil de certificat est indépendant du système d'exploitation. En outre, ce profil est actif même si vous activez Contournement d'authentification, qui remplace le Profil d'authentification pour permettre l'authentification en utilisant des témoins chiffrés.

Onglet Collecte de données du portail GlobalProtect

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config> (<configuration du portail>)** > **Portal Data Collection (Collecte de données du portail)** pour définir les données que l'application GlobalProtect collecte des points de terminaison et pour envoyer les données des critères de sélection de configuration après la connexion des utilisateurs au portail.

Paramètres de collecte de données du portail GlobalProtect	Description
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Vérifications personnalisées	Définissez les informations personnalisées sur l'hôte que l'application doit collecter : • **Windows** : **Add (Ajouter)** pour ajouter une vérification d'une clé de registre et/ou d'une valeur de clé particulière. • **Mac** : **Add (Ajouter)** pour ajouter une vérification d'une clé plist ou d'une valeur de clé particulière.

© 2020 Palo Alto Networks, Inc.

Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect)

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent**

Sélectionnez l'onglet **Agent** pour définir les paramètres de configuration de l'agent. Le portail GlobalProtect déploie la configuration de l'appareil une fois que la connexion est établie en premier.

Vous pouvez également spécifier que le portail déploie automatiquement les certificats de l'autorité de certification (AC) et les certificats intermédiaires. Si les terminaux ne font pas confiance aux certificats de serveur que les passerelles GlobalProtect et GlobalProtect Mobile Manager Security utilisent, les terminaux ont besoin de ces certificats pour établir des connexions HTTPS aux passerelles ou Mobile Security Manager. Le portail pousse les certificats que vous spécifiez ici au client avec la configuration du client.

Pour ajouter un certificat AC de racine de confiance, **Add (Ajouter)** un certificat existant ou **Import (Importer)** un nouveau. Pour installer (transparent) les certificats AC de la racine de confiance qui sont nécessaires pour le décryptage du proxy de transfert SSL dans le magasin de certificats du client, sélectionnez **Install in Local Root Certificate Store (Installer dans le magasin de certificats de la racine locale)**.

Spécifiez le certificat CA racine de confiance que l'application GlobalProtect utilise pour vérifier l'identité du portail et des passerelles GlobalProtect. Si le portail ou la passerelle présente un certificat qui n'a pas été signé ou émis par la même autorité de certification qui a émis la CA racine de confiance, l'applcation GlobalProtect ne peut établir de connexion avec le portail ou la passerelle.

Si vous disposez de différents types d'utilisateurs qui requièrent différentes configurations, vous pouvez créer des configurations d'agent séparées pour les appuyer. Le portail utilise ensuite le nom d'utilisateur ou de groupe et/ou le système d'exploitation du client pour déterminer la configuration de l'agent à déployer. Comme avec les évaluations des règles de sécurité, le portail recherche une correspondance en commençant par le sommet de la liste. Lorsque le portail trouve une correspondance, il fournit la configuration correspondante à l'application. Par conséquent, si vous disposez de plusieurs configurations d'agents, il est important de les ordonner de manière à ce que les configurations plus spécifiques (c'est-à-dire les configurations pour certains utilisateurs ou systèmes) soient au-dessus des configurations plus génériques. Utilisez les boutons **Move Up (Monter)** et **Move Down (Descendre)** pour réordonner les configurations. Au besoin, **Add (Ajouter)** une nouvelle configuration de l'agent. Pour plus d'informations sur la configuration du portail et la création de configurations d'agent, reportez-vous à Portails GlobalProtect dans le Guide de l'administrateur de GlobalProtect. Lorsque vous souhaitez **Add (Ajouter)** une nouvelle configuration d'agent ou modifier une configuration existante, la fenêtre **Configurations** s'ouvre et affiche cinq onglets, qui sont décrits dans les tableaux suivants :

- Onglet Authentification de l'agent des portails GlobalProtect
- Onglet des Critères de sélection de la configuration de l'agent des portails GlobalProtect
- Onglet Agent interne des portails GlobalProtect
- Onglet Agent externe des portails GlobalProtect
- Onglet Application de l'agent des portails GlobalProtect
- Onglet Collecte de données HIP de l'agent des portails GlobalProtect

Onglet Authentification de l'agent des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent** > *<agent-config> (configuration de l'agent)* > **Authentication (Authentification)**

Sélectionnez l'onglet **Authentication (Authentification)** pour configurer les paramètres d'authentification qui s'appliquent à la configuration de l'agent.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du portail client GlobalProtect	Description
Onglet Authentification	
Name (Nom)	Entrez un nom descriptif pour cette configuration pour l'authentification du client.
Certificat du client	(Facultatif) Sélectionnez la source qui distribue le certificat client à un point de terminaison, qui présente ensuite le certificat aux passerelles. Un certificat client est nécessaire si vous configurez l'authentification SSL mutuelle. Si SCEP est configuré pour la pré-connexion dans la configuration du client portail, le portail génère un certificat de la machine qui est stocké dans le magasin de certificats du système pour l'authentification et les connexions de la passerelle. Pour utiliser un certificat **Local** du pare-feu plutôt qu'un certificat généré par le PKI via **SCEP,** sélectionnez un certificat qui est déjà téléchargé sur le pare-feu. Si vous utilisez une autorité de certification interne pour distribuer les certificats aux points de terminaison, sélectionnez **None (Aucun)** (par défaut). Lorsque vous sélectionnez **None (Aucun)**, le portail ne pousse pas un certificat au point de terminaison.
Enregistrer les informations d'identification de l'utilisateur	Sélectionnez **Yes (Oui)** pour enregistrer le nom d'utilisateur et le mot de passe sur l'application ou sélectionnez **No (Non)** pour forcer les utilisateurs à fournir le mot de passe soit de manière transparente via le point de terminaison ou en le saisissant manuellement à chaque fois qu'ils se connectent. Sélectionnez **Save Username Only (Enregistrer nom d'utilisateur seulement)** pour enregistrer seulement le nom d'utilisateur à chaque fois qu'un utilisateur se connecte. Sélectionnez **Only with User Fingerprint (Uniquement à partir de l'empreinte digitale de l'utilisateur)** pour permettre l'ouverture de session avec ses données biométriques. Lorsque l'option d'ouverture de session avec empreintes digitales est activée sur un terminal, GlobalProtect utilise les informations d'identification enregistrées de l'utilisateur lorsque le balayage de l'empreinte digitale correspond à une empreinte digitale de confiance sur le terminal. *N'enregistrez pas les informations d'identification de l'utilisateur, car il pourrait alors être plus facile pour les utilisateurs non autorisés d'obtenir accès à des ressources sensibles et à des informations confidentielles. Les utilisateurs doivent manuellement saisir leurs informations d'identification chaque fois qu'ils se connectent à GlobalProtect.*

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du portail client GlobalProtect	Description
Contournement d'Authentification	
Générer le témoin pour le contournement de l'authentification	Sélectionnez cette option pour configurer le portail pour qu'il génère des témoins spécifiques terminaux chiffrés. Le portail envoie ce témoin au terminal après que l'utilisateur se soit authentifié une première fois avec le portail.
Accepter le témoin pour le contournement de l'authentification	Sélectionnez cette option pour configurer le portail pour authentifier les points de terminaison par le biais d'un témoin crypté valide. Lorsque le terminal présente un témoin valide, le portail vérifie que le témoin a été chiffré par le portail, déchiffre le témoin, puis authentifie l'utilisateur.
Durée de vie du témoin	Spécifiez les heures, les jours ou les semaines pour lesquelles le témoin est valide. La durée de vie typique est de 24 heures. Les plages sont 1 à 72 heures, 1 à 52 semaines ou 1 à 365 jours. Après l'expiration du témoin, l'utilisateur doit entrer les informations de connexion et le portail encrypte ensuite un nouveau témoin à envoyer à l'utilisateur terminal.
Certificat pour chiffrer/déchiffrer le témoin	Sélectionnez le certificat à utiliser pour chiffrer et déchiffrer le témoin. *Veiller à ce que le portail et les passerelles utilisent le même certificat pour chiffrer et déchiffrer les témoins. (Configurer le certificat dans le cadre d'une configuration d'une passerelle client. Voir Réseau > GlobalProtect > Passerelles).*
Composants nécessitant des mots de passe dynamiques (Authentification à deux facteurs)	
Pour configurer GlobalProtect afin qu'il supporte les mots de passe dynamiques, tels que les mots de passe à usage unique (OTP), spécifier les types de portail ou de passerelles qui requièrent que les utilisateurs saisissent des mots de passe dynamiques. Lorsque l'authentification à deux facteurs n'est pas activée, GlobalProtect utilise l'authentification régulière en utilisant les informations de connexion (tels que AD) et un certificat. Lorsque vous activez un portail ou un type de passerelle pour l'authentification à deux facteurs, ce portail ou cette passerelle invite l'utilisateur, après l'authentification initiale du portail, à présenter des informations d'identification et un second OTP (ou un autre mot de passe dynamique). Toutefois, si vous activez également le contournement d'authentification, un témoin crypté est utilisé pour authentifier l'utilisateur (après que l'utilisateur se soit d'abord authentifié pour une nouvelle session) et, par conséquent, est prioritaire sur l'obligation de ré-entrer les informations d'identification (aussi longtemps que le témoin est valide). Par conséquent, l'utilisateur est connecté de manière transparente à chaque fois que nécessaire tant que le témoin est valide. Vous spécifiez la durée de vie du témoin.	
Portail	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter au portail.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du portail client GlobalProtect	Description
Passerelles internes - tout	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à des passerelles internes.
Passerelles externes – manuelles uniquement	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à des passerelles externes qui sont configurées en tant que passerelles **Manual (Manuel)**.
Passerelles externes – détection automatique	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à toute passerelle externe restante que l'application peut automatiquement découvrir (passerelles qui ne sont pas configurées en tant que **Manual (Manuelle)**).

Onglet des Critères de sélection de la configuration de l'agent des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (<configuration du portail>* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Config Selection Criteria (Critères de sélection de la configuration)**

Sélectionnez l'onglet **Config Selection Criteria (Critères de sélection de la configuration)** pour configurer les critères de correspondance utilisés pour identifier le type de point de terminaison dans les déploiements ayant des points de terminaison gérés et non gérés. Le portail peut transmettre des configurations spécifiées au point de terminaison selon le type de point de terminaison.

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
Onglet Utilisateur/Groupe d'utilisateurs	
Système d'exploitation	**Add (Ajoutez)** un ou plusieurs systèmes d'exploitation (OS) de point de terminaison pour spécifier les points de terminaison qui reçoivent cette configuration. Le portail apprend automatiquement le système d'exploitation du point de terminaison et intègre les détails de ce système d'exploitation dans la configuration du client. Vous pouvez sélectionner **Any (Tous)** les systèmes d'exploitation ou un système d'exploitation spécifique (**Android**, **Chrome**, **iOS**, **IoT [IdO]**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**).
Utilisateur/Groupe d'utilisateurs	**Add (Ajouter)** les groupes d'utilisateurs ou les utilisateurs spécifiques auxquels cette configuration s'applique. *Vous devez configurer le mappage de groupe (Device*

© 2020 Palo Alto Networks, Inc.

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
	(Périphérique) > User Identification (Identification utilisateur) > Group Mapping Settings (Paramètres de mappage des groupes)) avant de pouvoir sélectionner les groupes d'utilisateurs. Pour déployer cette configuration à tous les utilisateurs, sélectionnez **any (indifférent)** dans le menu déroulant **User/User Group (Utilisateur/Groupe d'utilisateurs)**. Pour déployer cette configuration uniquement aux utilisateurs disposant d'applications GlobalProtect en mode préouverture de session, sélectionnez **pre-logon (préouverture de session)** dans le menu déroulant **User/User Group (Utilisateur/Groupe d'utilisateurs)**.
Vérifications des périphériques	
Le compte machine existe avec le numéro de série du périphérique,	Configurez les critères de correspondance en fonction de l'existence du numéro de série du point de terminaison dans Active Directory.
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Vérifications personnalisées	
Vérifications personnalisées	Sélectionnez cette option pour définir les informations personnalisées sur l'hôte à faire correspondre.
Clé de registre	Pour rechercher une clé de registre spécifique sur les points de terminaison Windows, **Add (Ajoutez)** la **Registry Key (Clé de registre)** pour effectuer la mise en correspondance. Pour faire correspondre uniquement les points de terminaison qui ne disposent pas de la clé de registre spécifiée ou de la valeur de la clé, activez l'option **Key does not exist or match the specified value data (La clé n'existe pas ou ne correspond pas aux données de la valeur définies)**. Pour la mise en correspondance avec des valeurs spécifiques, **Add (Ajoutez)** la **Registry Value (Valeur de registre)** et les **Value Data (Données de la valeur)**. Pour la mise en correspondance avec les points de terminaison qui ne disposent clairement pas de la valeur ou des données de la valeur spécifiées, sélectionnez **Negate (Inverser)**.

© 2020 Palo Alto Networks, Inc.

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
Plist	Pour rechercher une entrée spécifique dans la Property List (plist) sur les points de terminaison macOS, **Add (Ajoutez)** le nom du **Plist**. Pour la mise en correspondance uniquement avec les points de terminaison qui ne disposent pas du plist spécifié, activez l'option **Plist does not exist (Le plist n'existe pas)**. Pour la mise en correspondance avec des paires de valeurs de clé spécifiques dans la plist, **Add (Ajoutez)** la **Key (Clé)** et la **Value (Valeur)** correspondante. Pour la mise en correspondance avec les points de terminaison qui ne disposent clairement pas de la clé ou de la valeur spécifiée, cochez la case **Negate (Ignorer)**

Onglet Agent interne des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent** > *<agent-config> (configuration de l'agent)* > **External (Externe)**

Sélectionnez l'onglet **Internal (Interne)** pour configurer les paramètres de la passerelle interne pour une configuration d'agent.

Paramètres internes du portail GlobalProtect	Description
Détection d'hôte interne	
Détection d'hôte interne	Sélectionnez cette option pour permettre à l'application GlobalProtect de déterminer si elle est à l'intérieur du réseau d'entreprise. Cette option concerne uniquement les paramètres qui sont configurés pour communiquer avec les passerelles internes ; c'est une pratique exemplaire pour ces points de terminaison. Lorsque l'utilisateur tente de se connecter, l'application effectue une recherche DNS inversée d'un hôte interne en utilisant le **Hostname (Nom d'hôte)** spécifié à l'**IP Address (Adresse IP)** spécifiée. L'hôte sert de point de référence qui est accessible si le terminal est à l'intérieur du réseau d'entreprise. Si l'application trouve l'hôte, le terminal est à l'intérieur du réseau et l'application se connecte à une passerelle interne ; si l'application ne parvient pas à trouver l'hôte interne, le terminal est en dehors du réseau et l'application établit un tunnel à l'une des passerelles extérieures. • L'adresse IP peut être de type **IPv4** (trafic IPv4 uniquement), **IPv6** (trafic IPv6 uniquement) ou les deux. Utilisez **IPv4** et **IPv6** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. • L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. • Si vous choisissez **IPv4** et **IPv6,** saisissez le type d'adresse IP appropriée pour chacun.

© 2020 Palo Alto Networks, Inc.

Paramètres internes du portail GlobalProtect	Description
Nom d'hôte	Saisissez le **Hostname (Nom d'hôte)** permettant de résoudre l'adresse IP ci-dessus sur le réseau interne.
Passerelles internes	
Spécifiez les passerelles internes auxquelles une application peut demander l'accès et également fournir des rapports de HIP (si HIP est activé à l'onglet Collecte de données de l'agent des portails GlobalProtect).	**Add (Ajouter)** les passerelles internes qui comprennent les informations suivantes pour chacune : • **Name (Nom)** – Étiquette de 31 caractères maximum permettant d'identifier la passerelle. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. • **Address (Adresse)** – L'adresse IP ou le nom de domaine complet (FQDN) de l'interface pare-feu pour la passerelle. Cette valeur doit correspondre au nom commun (CN) et SAN (si spécifié) dans le certificat de serveur de passerelle. Par exemple, si vous avez utilisé un FQDN pour générer le certificat, vous devez entrer le nom de domaine complet (FQDN) ici. • **Source Address (Adresse source)** – Une adresse source ou un pool d'adresses pour les points de terminaison. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît l'adresse source du périphérique. Seules les applications GlobalProtect dont les adresses IP sont incluses dans le pool d'adresses source peuvent s'authentifier auprès de cette passerelle et envoyer des rapports HIP. • **DHCP Option 43 Code (Code 43 option DHCP)** (Windows et Mac uniquement) – Les codes de sous-options DHCP pour la sélection de la passerelle. Spécifiez un ou plusieurs codes de sous-options (en décimal). L'application GlobalProtect lit l'adresse de la passerelle à partir des valeurs définies par les codes de sous-options.

Onglet Agent externe des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent** > *<agent-config> (configuration de l'agent)* > **External (Externe)**

Sélectionnez l'onglet **External (Externe)** pour configurer les paramètres de la passerelle externe pour une configuration d'agent.

Paramètres externes du portail GlobalProtect	Description
Heure limite (sec)	Indiquez le nombre de secondes qu'une application attend que toutes les passerelles disponibles répondent avant de sélectionner la meilleure passerelle. Pour les demandes de connexion ultérieures, l'application tente de se connecter uniquement aux passerelles qui ont répondu avant la coupure. Une valeur de 0 signifie que l'application utilise le **TCP Connection Timeout (Délai d'expiration de connexion TCP)** dans la **AppConfigurations (Configuration des applications)** de l'onglet **App (Application)** (la plage est comprise entre 0 et 10 ; 5 par défaut).
Passerelles externes	

© 2020 Palo Alto Networks, Inc.

Paramètres externes du portail GlobalProtect	Description
Spécifiez la liste des pare-feu pour lesquels les applications peuvent essayer de se connecter lors de l'établissement d'un tunnel alors qu'elles ne sont pas sur le réseau d'entreprise.	**Add (Ajouter)** des passerelles externes qui comprennent les informations suivantes pour chacune : • **Name (Nom)** – Étiquette de 31 caractères maximum permettant d'identifier la passerelle. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. • **Address (Adresse)** – L'adresse IP ou le nom de domaine complet (FQDN) où la passerelle est configurée. Cette valeur doit correspondre au nom commun (CN) et SAN (si spécifié) dans le certificat de serveur de passerelle. Par exemple, si vous avez utilisé un FQDN pour générer le certificat, vous devez également saisir le nom de domaine complet (FQDN) ici. • **Source Region (Région source)** – Région source pour les points de terminaison. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît la région du point de terminaison et permet aux utilisateurs de se connecter uniquement aux passerelles configurées pour cette région. En ce qui concerne les choix de passerelle, la région source est considérée en premier, suivie par la passerelle. • **Priority (Priorité)** – Sélectionnez une valeur (**Highest (La plus élevée)**, **High (Élevée)**, **Medium (Moyenne)**, **Low (Faible)**, **Lowest (La plus faible)** ou **Manual only (Manuelle uniquement)**) pour permettre à l'application de déterminer la passerelle à utiliser. **Manual only (Manuelle uniquement)** empêche l'application GlobalProtect de tenter de se connecter à cette passerelle lorsque la **Détection automatique** est activée sur le point de terminaison. L'application commencera par contacter toutes les passerelles marquées d'une priorité **Highest (Absolue)**, **High (Élevée)** ou **Medium (Moyenne)** et établira un tunnel avec la passerelle qui répond le plus rapidement. Si les passerelles ayant la priorité la plus élevée sont inaccessibles, l'application contacte ensuite les autres passerelles qui possèdent des valeurs de priorité inférieures (elle exclut les passerelles **Manual only (Manuelles uniquement)**). • **Manual (Manuelle)** – Sélectionnez cette option pour permettre aux utilisateurs de sélectionner manuellement (ou basculer vers) une passerelle. L'application GlobalProtect peut se connecter à n'importe quelle passerelle externe pour laquelle l'option **Manual (Manuelle)** est configurée. Lorsque l'application se connecte à une autre passerelle, le tunnel existant est déconnecté et un nouveau tunnel est établi. Les passerelles manuelles peuvent également proposer des méthodes d'authentification différentes de celles de la passerelle principale. Si un point de terminaison est redémarré ou si une nouvelle découverte est exécutée, l'application GlobalProtect se connecte à la passerelle principale. Cette fonction est utile si un groupe d'utilisateurs doit se connecter temporairement à une passerelle spécifique afin d'accéder à un segment sécurisé de votre réseau.
VPN tiers	
VPN tiers	Pour indiquer à l'application GlobalProtect d'ignorer les clients VPN tierce partie sélectionnés, afin que GlobalProtect ne soit pas en conflit avec eux, **Add (Ajouter)** le nom du client VPN : Sélectionnez le nom de

© 2020 Palo Alto Networks, Inc.

Paramètres externes du portail GlobalProtect	Description
	la liste, ou entrez le nom dans le champ prévu. GlobalProtect ignore les paramètres d'itinéraire pour les clients VPN spécifiés si vous configurez cette fonctionnalité.

Onglet Application de l'agent des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent** > *<agent-config> (configuration de l'agent)* > **App (Application)**

Sélectionnez l'onglet **App (Appliquer)** pour définir comment les utilisateurs finaux interagissent avec les applications GlobalProtect installées sur leurs systèmes. Vous pouvez définir différents paramètres d'application pour les différentes configurations d'agent GlobalProtect que vous avez créées.

Paramètres de configuration de l'application GlobalProtect	Description
Page d'accueil	Sélectionnez une page d'accueil à afficher aux utilisateurs finaux lors d'une connexion à GlobalProtect. Vous pouvez sélectionner la page **factory-default (par défaut)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**.
Configurations d'application	
Méthode de connexion	• **On-demand (Manual user initiated connection) (Sur demande (Connexion initiée manuellement par l'utilisateur))** – Les utilisateurs doivent lancer l'application GlobalProtect, puis initier une connexion au portail et entrer leurs informations d'identification GlobalProtect. Cette option est principalement utilisée pour les connexions d'accès à distance. • **Connexion-Utilisateur (Toujours Activée)** : L'application GlobalProtect établit automatiquement une connexion au portail après que l'utilisateur se connecte à un terminal. Le portail répond en fournissant à l'application la configuration de l'agent appropriée. Par la suite, l'application met en place un tunnel vers l'une des passerelles spécifiées dans la configuration de l'agent qu'il a reçue du portail. • **Pre-logon (Pré-ouverture de session)** – La pré-ouverture de session garantit que les utilisateurs distants de Windows et Mac sont toujours connectés au réseau d'entreprise et active les scripts d'ouverture de session utilisateur et l'application de règles de domaine lorsque l'utilisateur se connecte au terminal. Étant donné que le terminal peut se connecter au réseau d'entreprise comme s'il était interne, les utilisateurs peuvent se connecter avec de nouveaux mots de passe lorsque leurs mots de passe expirent ou recevoir une aide pour la récupération de mot de passe s'ils oublient leur mot de passe. Avec la préouverture de session, l'application GlobalProtect établit

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	un tunnel VPN vers une passerelle GlobalProtect avant que l'utilisateur se connecte au terminal ; le terminal demande l'authentification en soumettant un certificat de machine pré-installé à la passerelle. Ensuite, sur les terminaux Windows, la passerelle réaffecte le tunnel VPN depuis l'utilisateur de la pré-ouverture de session vers le nom d'utilisateur connecté au terminal. Sur les terminaux Mac, l'application procède à sa déconnexion et crée un nouveau tunnel VPN pour l'utilisateur. Il existe deux méthodes de pré-ouverture de session, dont chacune permet la même fonctionnalité de pré-ouverture de session qui se déroule avant que les utilisateurs ne se connectent au terminal. Cependant, après la connexion des utilisateurs au terminal, c'est la méthode de pré-ouverture de session qui détermine le moment où la connexion de l'application GlobalProtect est établie : • **Pre-logon (Always On) (Pré-ouverture de session (Toujours activée))** – L'application GlobalProtect tente automatiquement de se connecter et de se reconnecter aux passerelles GlobalProtect. Les périphériques mobiles ne prennent pas en charge les fonctionnalités de pré-ouverture de session et utilisent par conséquent la méthode de connexion **User-logon (Always On) (Connexion utilisateur (Toujours activée))** par défaut, si cette méthode de connexion est spécifiée. • **Pre-logon then On-demand (Pré-ouverture de session puis À la demande)** – Les utilisateurs doivent lancer l'application GlobalProtect, puis établir la connexion manuellement. Les périphériques mobiles ne prennent pas en charge les fonctionnalités de pré-ouverture de session et utilisent par conséquent la méthode de connexion **À la demande (Connexion initiée manuellement par l'utilisateur)** par défaut, si cette méthode de connexion est spécifiée.
Intervalle de rafraîchissement de configuration de l'application GlobalProtect (en heures)	Indiquez le nombre d'heures que le portail GlobalProtect attend avant la prochaine actualisation de la configuration d'une application (plage comprise entre 1 et 168 ; 24 par défaut).
Autoriser l'utilisateur à désactiver GlobalProtect App	Indique si les utilisateurs sont autorisés à désactiver l'application GlobalProtect et, si oui, lequel, le cas échéant, ils doivent désactiver avant de pouvoir désactiver l'application : • **Allow (Autoriser)** – Permettre à tout utilisateur de désactiver l'application GlobalProtect au besoin. • **Disallow (Ne pas autoriser)** – Ne pas permettre aux utilisateurs finaux de désactiver l'application GlobalProtect. • **Allow with Comment (Permettre avec commentaire)** – Permettre aux utilisateurs de désactiver l'application

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	GlobalProtect sur leur terminal, mais exiger qu'ils indiquent la raison de la désactivation de l'application. • **Allow with Passcode (Permettre avec code secret)** – Permettre aux utilisateurs d'entrer un code secret pour désactiver l'application GlobalProtect. Cette option nécessite que l'utilisateur entre et confirme une valeur de Code Secret qui, comme un mot de passe, ne s'affiche pas lorsque saisie. En règle générale, les administrateurs fournissent un mot de passe aux utilisateurs avant que des événements non planifiés ou imprévus empêchent les utilisateurs de se connecter au réseau en utilisant le VPN GlobalProtect. Vous pouvez fournir le mot de passe par e-mail ou l'afficher sur le site Web de votre organisation. • **Allow with Ticket (Permettre avec ticket)** – Cette option active un mécanisme basé sur le temps de réponse dans lequel, après qu'un utilisateur tente de désactiver GlobalProtect, le terminal affiche un numéro de requête hexadécimal de 8 caractères. L'utilisateur doit contacter l'administrateur ou l'équipe de soutien du pare-feu (de préférence par téléphone par mesure de sécurité) afin de lui fournir ce numéro. À partir du pare-feu (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**), l'administrateur ou la personne responsable du soutien peut alors cliquer sur **Generate Ticket (Générer le ticket)**, puis entrer le numéro de **Request (requête)** de ticket pour obtenir le numéro de **Ticket** (également un numéro hexadécimal de 8 caractères). L'administrateur ou la personne responsable du soutien fournit ce numéro de ticket à l'utilisateur qui l'entre alors dans le champ de réponse pour désactiver l'application.
Autoriser l'utilisateur à désinstaller l'application GlobalProtect	Indique si les utilisateurs sont autorisés à désinstaller l'application GlobalProtect et, si oui, que doivent-ils faire, le cas échéant, avant de pouvoir désinstaller l'application : • **Allow (Autoriser)** – Permettre à tout utilisateur de désinstaller l'application GlobalProtect au besoin. • **Disallow (Ne pas autoriser)** – Ne pas permettre aux utilisateurs finaux de désinstaller l'application GlobalProtect. • **Allow with Password (Autoriser avec un mot de passe)** - Imposer un mot de passe pour désinstaller l'application GlobalProtect. Cette option nécessite que l'utilisateur saisit et confirme un mot de passe avant de pouvoir procéder à la désinstallation. Vous pouvez fournir le mot de passe par e-mail ou l'afficher sur le site Web de votre organisation. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
Permettre à l'utilisateur de mettre à niveau l'app GlobalProtect	Indique si les utilisateurs finaux peuvent mettre à niveau le logiciel de l'application GlobalProtect et, s'ils le peuvent, s'ils peuvent choisir le moment de la mise à niveau : • **Disallow (Désactiver)** – Empêche les utilisateurs de mettre à niveau le logiciel de l'application. • **Allow Manually (Autoriser manuellement)** – Autoriser les utilisateurs à vérifier manuellement les mises à niveau et à les lancer en sélectionnant **Check Version (Vérifier Version)** dans l'application GlobalProtect. • **Allow with Prompt (Autoriser avec invite)** (par défaut) – Invite les utilisateurs lorsqu'une nouvelle version est activée sur le pare-feu et permet aux utilisateurs de mettre à niveau leur logiciel lorsqu'ils le souhaitent. • **Allow Transparently (Permettre avec transparence)** – Met automatiquement à niveau le logiciel de l'application lorsqu'une nouvelle version est disponible sur le portail. • **Internal (Interne)** – Mettre automatiquement à niveau le logiciel de l'application chaque fois qu'une nouvelle version est disponible sur le portail. Cependant, vous devez attendre que le terminal soit connecté en interne au réseau de l'entreprise. Cela empêche les retards causés par les mises à niveau sur les connexions à bande passante étroite.
Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect (Windows, macOS, iOS, Android et Chrome uniquement)	Indique si les utilisateurs sont autorisés à se déconnecter manuellement de l'application GlobalProtect : • **Yes (Oui)** – Permettre à tout utilisateur de se déconnecter de l'application GlobalProtect au besoin. • **No (Non)** – Ne pas permettre aux utilisateurs finaux de se déconnecter de l'application GlobalProtect. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Utiliser l'ouverture de session unique (Windows)	Sélectionnez **No (Non)** pour désactiver l'authentification unique (SSO). Avec l'ouverture de session unique, l'application GlobalProtect utilise automatiquement les informations d'identification pour s'authentifier et ensuite se connecter au portail et à la passerelle GlobalProtect. GlobalProtect peut également englober des informations d'identification indépendantes afin de garantir l'authentification et la connexion des utilisateurs Windows, même si un fournisseur d'informations d'identification indépendantes est utilisé pour englober les informations d'identification de connexion Windows.
Utiliser l'ouverture de session unique (macOS)	Sélectionnez **No (Non)** pour désactiver l'authentification unique (SSO). Avec l'ouverture de session unique, l'application GlobalProtect utilise automatiquement les informations d'identification de macOS pour s'authentifier et ensuite se connecter au portail et à la passerelle GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Effacer les identifiants d'ouverture de session unique à la fermeture de session (Windows uniquement)	Sélectionnez **No (Non)** pour conserver les inforations d'aitjentification uniques lorsque l'utilisateur se déconnecte. Sélectionnez **Yes (Oui)** (par défaut) pour les supprimer et forcer l'utilisateur à entrer ses informations d'identification lors de la prochaine connexion.
Utiliser l'authentification par défaut en cas d'échec d'authentification Kerberos	Sélectionnez **No (Non)** pour utiliser uniquement l'authentification Kerberos. Sélectionnez **Yes (Oui)** (par défaut) pour recommencer l'authentification en utilisant la méthode d'authentification par défaut après un échec de l'authentification avec Kerberos. Cette fonction est prise en charge uniquement sur les points de terminaison Windows et Mac.
Rétablissement automatique du délai de connexion VPN	Entrez un délai d'attente, en minutes, de 0 à 180, pour préciser l'action que l'application GlobalProtect prend lorsqu'un tunnel est déconnecté en raison de l'instabilité du réseau ou que l'état du terminal est modifié lors de l'entrée ; la valeur par défaut est 30. • 0 : désactive cette fonction ; GlobalProtect ne tente pas de rétablir le tunnel après sa déconnexion. • 1 à 180 : active cette fonction ; GlobalProtect tente de rétablir la connexion du tunnel si le tunnel est indisponible pendant une période de temps qui est inférieure à la valeur du délai que vous indiquez ici. Par exemple, si la valeur du délai est fixée à 30 minutes, GlobalProtect ne tente pas de rétablir le tunnel si celui-ci est déconnecté depuis 45 minutes. Toutefois, si le tunnel est déconnecté pendant 15 minutes, GlobalProtect tente de se reconnecter car le nombre de minutes n'a pas dépassé la valeur de délai. *Avec le VPN toujours activé, si un utilisateur passe d'un réseau externe à un réseau interne avant l'expiration de la valeur de délai, GlobalProtect n'effectue pas de découverte de réseau. Par conséquent, GlobalProtect rétablit le tunnel vers la dernière passerelle externe connue. Pour déclencher la détection d'hôte interne, l'utilisateur doit sélectionner Rediscover Network (Redécouvrir le réseau) dans la console GlobalProtect.*
Temps d'attente entre les tentatives de rétablissement de la connexion VPN	Saisissez la période de temps, en secondes, pendant laquelle l'application GlobalProtect attend entre des tentatives de rétablissement de la connexion avec la dernière passerelle à laquelle elle s'est connectée lorsque vous activez l'option **Automatic Restoration of VPN Connection Timeout**

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	(Rétablissement automatique du délai de connexion VPN). Indiquez un temps d'attente plus long ou plus court selon les conditions de votre réseau. La plage est comprise entre 1 et 60. La valeur par défaut est 5. Cet intervalle de temps est utilisé comme délai d'attente TCP pour la tentative de restauration avec un tunnel SSL VPN ; il est aussi utilisé comme délai d'attente keepalive UDP pour la tentative de restauration avec un tunnel IPSec.  *En mode Toujours actif, l'application GlobalProtect retentera continuellement et indéfiniment selon le Wait Time Between VPN Connection Restore Attempts (délai d'attente entre les tentatives de restauration de la connexion VPN) configuré. Mais en mode À la demande, l'application GlobalProtect essaiera une seule fois pendant la durée du délai configuré au paramètre Wait Time Between VPN Connection Restore Attempts (délai d'attente entre les tentatives de restauration de la connexion VPN) et si l'opération ne réussit pas pendant la durée du délai, l'application renoncera à l'opération, passera à l'état déconnecté et ne réessaiera pas.*
Appliquer la Connexion GlobalProtect pour l'Accès au réseau.	Sélectionnez **Yes (Oui)** pour contraindre la totalité du trafic réseau à traverser un tunnel GlobalProtect. Sélectionnez **No (Non)** (par défaut) si GlobalProtect n'est pas requis pour l'accès au réseau et si les utilisateurs peuvent toujours accéder à Internet même si GlobalProtect est désactivé ou déconnecté. Pour fournir des instructions aux utilisateurs avant le blocage du trafic, configurez un **Traffic Blocking Notification Message (message de notification de blocage du trafic)** et spécifiez éventuellement le message (**Traffic Blocking Notification Delay (retard de notification de blocage du trafic)**). Pour permettre le trafic requis pour établir une connexion avec un portail captif, spécifiez un **Captive Portal Exception Timeout (délai d'attente d'exception du portail captif)**. L'utilisateur doit s'authentifier auprès du portail avant que le délai d'expiration expire. Pour fournir des instructions supplémentaires, configurez un **Captive Portal Detection Message (Message de détection du portail captif)**. Vous pouvez également spécifier le moment où le message doit s'afficher (**Captive Portal Notification Delay [Retard de notification du portail captif]**).  *Dans la plupart des cas, utilisez la sélection par défaut No (Non). En sélectionnant Yes (Oui) vous bloquez tout le trafic réseau depuis et vers le point de terminaison jusqu'à ce que*

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	l'application se connecte à une passerelle interne à l'intérieur de l'entreprise ou à une passerelle externe à l'extérieur du réseau de l'entreprise.
Autoriser le trafic vers les hôtes/ réseaux spécifiés lorsque l'application de la connexion GlobalProtect pour l'accès réseau est activée et que la connexion GlobalProtect n'est pas établie	Si vous le souhaitez, spécifiez un maximum de dix adresses IP ou segments de réseau pour lesquels vous souhaitez autoriser l'accès lorsque vous appliquez GlobalProtect pour l'accès au réseau, mais que la connexion n'est pas établie. Séparez plusieurs valeurs par des virgules. Les exclusions peuvent améliorer l'expérience utilisateur en permettant aux utilisateurs d'accéder aux ressources locales lorsque GlobalProtect est déconnecté. Par exemple, lorsque GlobalProtect n'est pas connecté, GlobalProtect peut exclure les adresses locales de liaison pour autoriser l'accès à un segment de réseau local ou à un domaine de diffusion. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Expiration de l'exception du portail captif (sec)	Afin d'imposer GlobalProtect pour l'accès au réseau, mais fournir un délai supplémentaire pour permettre aux utilisateurs de se connecter à un portail captif, spécifiez le délai d'attente en secondes (entre 0 et 3 600). Par exemple, une valeur de 60 signifie que l'utilisateur doit se connecter au portail captif dans un délai d'une minute après que GlobalProtect l'ait détecté. Une valeur de 0 signifie que GlobalProtect ne permet pas aux utilisateurs de se connecter à un portail captif et bloque immédiatement l'accès.
Lancer automatiquement la page Web dans le navigateur par défaut lors de la détection du portail captif	Pour automatiquement lancer votre navigateur Web par défaut lors de la détection du portail captif afin de permettre aux utilisateurs de se connecter facilement au portail captif, saisissez le Fully Qualified Domain Name (nom de domaine complet ; FQDN) ou l'adresse IP du site Web que vous souhaitez utiliser pour la tentative de connexion initiale qui initie le trafic Web lors du lancement du navigateur Web par défaut (longueur maximale de 256 caractères). Le portail captif intercepte alors cette tentative de connexion et redirige le navigateur Web par défaut à la page de connexion au portail captif. Si le champ est vide (par défaut), GlobalProtect ne lance pas automatiquement le navigateur Web par défaut lors de la détection du portail captif.
Retard de notification de blocage du trafic (sec)	Spécifiez une valeur, en secondes, pour déterminer quand afficher le message de notification. GlobalProtect démarre le compte à rebours pour afficher la notification une fois que le réseau est accessible (la plage est de 5 à 120, la valeur par défaut est 15).
Afficher le message de notification de blocage du trafic	Spécifiez si un message doit apparaître lorsque GlobalProtect est requis pour l'accès au réseau. Sélectionnez **No (Non)** pour

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	désactiver le message. Sélectionnez **Yes (Oui)** pour activer le message (GlobalProtect affiche le message lorsqu'il est déconnecté mais qu'il détecte que le réseau est accessible).
Message de notification de blocage du trafic	Personnalisez un message de notification à afficher aux utilisateurs lorsque GlobalProtect est requis pour accéder au réseau. GlobalProtect affiche le message lorsqu'il est déconnecté mais qu'il détecte que le réseau est accessible. Le message peut indiquer le motif du blocage du trafic et fournir des instructions sur la manière de se connecter. Par exemple : `To access the network, you much first connect to GlobalProtect.` Le message doit contenir un maximum de 512 caractères.
Autoriser l'utilisateur à désactiver les notifications de blocage du trafic	Sélectionnez **No (Non)** pour toujours afficher les notifications de blocage du trafic. Par défaut, la valeur est définie sur **Yes (Oui)**, ce qui signifie que les utilisateurs sont autorisés à désactiver les notifications.
Afficher le message de détection du portail captif	Spécifie si un message s'affiche lorsque GlobalProtect détecte un portail captif. Sélectionnez **Yes (Oui)** pour afficher le message. Sélectionnez **No (Non)** (par défaut) pour supprimer le message (GlobalProtect n'affiche pas de message lorsqu'il détecte un portail captif). *Si vous activez un Message de détection de portail captif, le message apparaît 85 secondes avant l'Expiration de l'exception du portail captif. Donc, si l'Expiration de l'exception du portail de capture est de 90 secondes ou moins, le message apparaît 5 secondes après la détection d'un portail captif.*
Message de détection du portail captif	Personnalisez un message de notification à afficher aux utilisateurs lorsque GlobalProtect détecte le réseau qui fournit des instructions supplémentaires pour se connecter à un portail captif. Par exemple : `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.` Le message doit contenir un maximum de 512 caractères.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
Délai de détection du portail captif	Si vous activez le message de détection du portail captif, vous pouvez spécifier le délai en secondes après lequel, à la suite de la détection du portail captif, GlobalProtect affichera le message de détection (la plage est comprise de 1 à 120 ; par défaut 5).
Recherche dans le magasin de certificats du client	Sélectionnez le type de certificat ou de certificats qu'une application cherche dans son magasin de certificats personnel. L'application GlobalProtect utilise le certificat pour s'authentifier sur le portail ou sur une passerelle, puis pour établir un tunnel VPN vers la passerelle GlobalProtect. • **User (Utilisateur)** – Authentification en utilisant le certificat local au compte de l'utilisateur. • **Machine** – Authentification en utilisant un certificat qui est local au terminal. Ce certificat s'applique à tous les comptes d'utilisateurs autorisés à utiliser le terminal. • **User and machine (Utilisateur et machine)** (par défaut) – Authentification utilisant le certificat d'utilisateur et le certificat de la machine.
Période de renouvellement de certificat SCEP (jours)	Ce mécanisme est pour le renouvellement d'un certificat SCEP généré avant que le certificat n'expire effectivement. Vous spécifiez le nombre maximal de jours avant l'expiration du certificat pendant lequel le portail peut requérir un nouveau certificat du serveur SCEP dans votre système PKI (la plage est de 0 à 30, 7 par défaut). Une valeur de 0 signifie que le portail ne renouvelle pas automatiquement le certificat du client quand il actualise une configuration de client. Pour qu'une application obtienne le nouveau certificat, l'utilisateur doit se connecter au cours de la période de renouvellement (le portail ne demande pas le nouveau certificat pour un utilisateur au cours de cette période de renouvellement à moins que l'utilisateur se connecte). Par exemple, supposons qu'un certificat client a une durée de vie de 90 jours et que cette période de renouvellement du certificat est de 7 jours. Si un utilisateur se connecte au cours des 7 derniers jours de la durée de vie certificat, le portail génère le certificat et le télécharge avec une configuration client rafraîchie. Voir Intervalle de rafraîchissement de configuration de l'application GlobalProtect (heures).
Sélection du Certificat Client selon un OID inclus dans une clé étendue	Entrez l'utilisation de la clé étendue d'un certificat client en spécifiant son identifiant d'objet (OID). Ce paramètre garantit que l'application GlobalProtect sélectionne uniquement un certificat qui est destiné à l'authentification du client et permet à GlobalProtect d'enregistrer le certificat pour une utilisation future.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
Maintenir la connexion lors du retrait de Carte à puce (Windows uniquement)	Sélectionnez **Yes (Oui)** pour conserver la connexion lorsqu'un utilisateur retire une carte à puce contenant un certificat de client. Sélectionnez **No (Non)** (par défaut) pour mettre fin à la connexion lorsqu'un utilisateur retire une carte à puce.
Autoriser le remplacement du nom d'utilisateur d'un certificat du client	Sélectionnez **No (Non)** pour forcer GlobalProtect à utiliser le nom d'utilisateur du certificat du client et empêcher GlobalProtect de le remplacer (activé par défaut).
Activer la visualisation avancée	Sélectionnez **No (Non)** pour restreindre l'interface utilisateur de l'application à la vue minimale, de base (par défaut).
Permettre à l'utilisateur de désactiver la page de bienvenue	Sélectionnez **No (Non)** pour forcer l'affichage de la page de bienvenue chaque fois qu'un utilisateur établit une connexion. Cette restriction empêche l'utilisateur d'ignorer des informations importantes comme les conditions que votre organisation peut exiger pour garantir la conformité.
Activer l'option de Redécouverte du réseau	Sélectionnez **No (Non)** pour empêcher les utilisateurs de lancer manuellement une redécouverte du réseau.
Activer l'option de Renvoi du profil d'hôte	Sélectionnez **No (Non)** pour empêcher les utilisateurs de déclencher manuellement le renvoi des dernières données HIP.
Permettre à l'Utilisateur de modifier l'Adresse du portail	Sélectionnez **No (Non)** pour désactiver le champ **Portal (Portail)** de l'onglet **Home (Accueil)** dans l'application GlobalProtect. Toutefois, comme l'utilisateur peut ensuite définir un portail auquel se connecter, vous devez fournir l'adresse du portail par défaut dans le Registre Windows ou Macplist : • **Windows registry**—`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` with key `Portal` • **Mac plist** – `/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` avec la clé `Portal` Pour plus d'informations sur le prédéploiement de l'adresse du portail, voir Paramètres de l'application à personnaliser dans le Guide de l'Administrateur GlobalProtect.
Permettre à l'utilisateur de continuer avec un certificat de serveur de portail invalide	Sélectionnez **No (Non)** pour empêcher l'application d'établir une connexion au portail si le certificat du portail n'est pas valide.
Afficher l'icône GlobalProtect	Sélectionnez **No (Non)** pour masquer l'icône GlobalProtect sur le point de terminaison. Si l'icône est masquée, les utilisateurs ne peuvent pas effectuer certaines tâches, telles que l'affichage des informations de dépannage, changer les mots de passe, redécouvrir le réseau, ou d'effectuer une connexion à la demande. Cependant, les messages de

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	notification HIP, les invitations de connexion et les dialogues de certificats s'affichent lorsque l'interaction de l'utilisateur est nécessaire.
Délai d'expiration pour renommer le tunnel de bascule d'utilisateur (sec) (Windows uniquement)	Indiquez le nombre de secondes durant lesquelles un utilisateur distant doit être authentifié par une passerelle GlobalProtect après la connexion à un terminal en utilisant le protocole Remote Desktop Protocol (RDP) de Microsoft (la plage est de 0 à 600, 0 par défaut). Exiger que l'utilisateur distant s'authentifie dans un laps de temps limité maintient la sécurité. Après l'authentification du nouvel utilisateur et la commutation du tunnel à l'utilisateur, la passerelle renomme le tunnel. Une valeur de 0 signifie que le tunnel actuel de l'utilisateur n'est pas renommé, mais, au contraire, est immédiatement interrompu. Dans ce cas, l'utilisateur distant obtient un nouveau tunnel et n'a aucune limite de temps pour l'authentification à une passerelle (autre que le délai d'attente TCP configuré).
Délai d'expiration pour renommer le tunnel de pré-ouverture de session (sec) (Windows uniquement)	Ce paramètre contrôle la manière dont GlobalProtect gère le tunnel de pré-ouverture de session qui relie un terminal à la passerelle. Une valeur de -1 signifie que le tunnel de pré-ouverture de session n'expire pas après la connexion d'un utilisateur au terminal ; GlobalProtect renomme le tunnel pour le réaffecter à l'utilisateur. Cependant, le tunnel persiste même si le renommage échoue ou si l'utilisateur ne se connecte pas à la passerelle GlobalProtect. Une valeur de 0 signifie que lorsque l'utilisateur se connecte au terminal, GlobalProtect ferme immédiatement le tunnel de pré-ouverture de session au lieu de le renommer. Dans ce cas, GlobalProtect lance un nouveau tunnel pour l'utilisateur plutôt que de permettre à ce dernier de se connecter sur le tunnel de pré-ouverture de session. Généralement, ce paramètre est très utile lorsque vous définissez la **Connect Method (Méthode de connexion)** sur **Pre-logon then On-demand (Pré-ouverture de session puis À la demande)**, ce qui force l'utilisateur à lancer manuellement la connexion après la connexion initiale. Une valeur de 1 à 600 indique le nombre de secondes pendant lesquelles le tunnel de pré-ouverture de session peut rester actif après qu'un utilisateur se connecte au terminal. Pendant ce temps, GlobalProtect applique des règles au tunnel de pré-ouverture de session. Si l'utilisateur s'authentifie avec la passerelle GlobalProtect avant l'expiration du délai, GlobalProtect réaffecte le tunnel à l'utilisateur. Si l'utilisateur ne s'authentifie pas avec la passerelle GlobalProtect avant

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	l'expiration du délai, GlobalProtect met fin au tunnel de pré-ouverture de session.
Délai de conservation du tunnel après la déconnexion de l'utilisateur (secondes)	Pour que GlobalProtect puisse conserver le tunnel VPN existant après la déconnexion des utilisateurs de leur terminal, spécifiez un **Preserve Tunnel on User Logoff Timeout (Délai de conservation du tunnel après la déconnexion de l'utilisateur)** (plage comprise entre 0 et 600 secondes ; valeur par défaut : 0 seconde). Si vous acceptez la valeur par défaut (`0`), GlobalProtect ne conserve pas le tunnel lorsque l'utilisateur se déconnecte.
Afficher les notifications dans la barre des tâches (Windows uniquement)	Sélectionnez **No (Non)** pour masquer les notifications de l'utilisateur. Sélectionnez **Yes (Oui)** (par défaut) pour afficher des notifications dans la zone de la barre d'état système.
Message personnalisé d'expiration de mot de passe (Authentification LDAP uniquement)	Créer un message personnalisé à afficher aux utilisateurs lorsque leur mot de passe est sur le point d'expirer. La longueur du message est de 200 caractères maximum.
Utiliser automatiquement SSL lorsque IPSec est peu fiable (heures)	Précisez la période de temps (en heures) pendant laquelle vous voulez que l'application GlobalProtect **Automatically Use SSL When IPSec Is Unreliable (Utilise automatiquement SSL lorsque IPSec est peu fiable)** (la plage est comprise entre 0 et 168 heures). Si vous configurez cette option, l'application GlobalProtect ne tente pas d'établir de tunnel IPSec au cours de la période de temps spécifiée. Ce minuteur est lancé chaque fois qu'un tunnel IPSec devient indisponible en raison d'un délai d'expiration keepalive du tunnel. Si vous acceptez la valeur par défaut de `0`, l'application ne recommence pas à établir un tunnel SSL si elle peut établir un tunnel IPSec. Elle revient à l'établissment d'un tunnel SSL uniquement lorsque le tunnel IPSec ne peut être établi.
Se connecter au moyen de SSL uniquement	Spécifiez si vous avez besoin que les utilisateurs se connectent aux passerelles GlobalProtect au moyen de SSL au lieu de IPSec. Les options à votre disposition sont les suivantes : • Oui - Impose l'utilisation de SSL pour se connecter aux passerelles configurées sur le portail. • Non - (par défaut) Utilise le protocole configuré sur la passerelle. • Modification possible par l'utilisateur - Donne à l'utilisateur la souplesse de choisir d'utiliser SSL ou IPSec, si la configuration de la passerelle prend en charge l'utilisation des deux protocoles. Lorsque cette option est configurée sur **User can Change (Modification possible par l'utilisateur)**, l'utilisateur peut cocher ou décocher la case **VPN sur l'application GlobalProtect : Se connecter au moyen de SSL uniquement**

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	pour sélectionner le protocole qui permet la meilleure connectivité pour un accès sécurisé.
Nombre maximum de tentatives de connexion à la passerelle interne	Saisissez le nombre maximum de fois où l'agent GlobalProtect devrait réessayer la connexion à une passerelle interne après que la première tentative échoue (la plage est de 0 à 100 ; 0 par défaut, ce qui signifie que l'application GlobalProtect ne relance pas la connexion). En augmentant la valeur, vous permettez à l'application de se connecter automatiquement à une passerelle interne qui est temporairement indisponible ou inaccessible lors de la première tentative de connexion, mais redevient disponible avant que le nombre spécifié de tentatives soit épuisé. L'augmentation de la valeur assure également que la passerelle interne reçoit les informations de l'utilisateur et de l'hôte les plus à jour.
Délai d'expiration de connexion au portail (sec.)	Le nombre de secondes (entre 1 et 600) avant qu'une requête de connexion au portail n'expire en raison de l'absence de réponse du portail. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 30. À partir de la version de contenu 777-4484, la valeur par défaut est 5.
Délai d'expiration de connexion TCP (sec.)	Le nombre de secondes (entre 1 et 600) avant qu'une demande de connexion TCP n'expire en raison de la non-réponse de l'une ou l'autre extrémité de la connexion. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 60. À partir de la version de contenu 777-4484, la valeur par défaut est 5.
Délai d'expiration de réception TCP (sec)	Le nombre de secondes avant qu'une connexion TCP n'expire en raison de la réponse partielle d'une demande de connexion TCP (la plage est de 1 à 600, 30 par défaut).
Résoudre tous les FQDN à l'aide des serveurs DNS assignés par le tunnel (Windows uniquement)	(GlobalProtect 4.0.3 et versions ultérieures) Configurez les préférences de résolution DNS lorsque le tunnel GlobalProtect est connecté aux points de terminaison Windows : • Sélectionnez **Yes (Oui)** (par défaut) pour que l'application GlobalProtect puisse autoriser les points de terminaison Windows à résoudre toutes les requêtes DNS auprès des serveurs DNS que vous configurez sur la passerelle au lieu d'autoriser le point de terminaison à envoyer certaines requêtes DNS aux serveurs DNS établis sur l'adaptateur physique. • Sélectionnez **No (Non)** pour permettre aux points de terminaison Windows d'envoyer les requêtes DNS au serveur DNS établi sur l'adaptateur physique si la requête initiale envoyée au serveur DNS configuré sur la passerelle n'est pas résolue. Cette option conserve le comportement natif de Windows pour interroger tous les serveurs DNS

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	sur tous les adaptateurs de manière récursive, ce qui peut toutefois se traduire par de longues périodes d'attente pour résoudre certaines requêtes DNS. Pour configurer les paramètres DNS de l'application GlobalProtect 4.0.2 et ses versions antérieures, utilisez l'option **Update DNS Settings at Connect (Mettre à jour les paramètres de DNS à la connexion)**.
Mettre à jour les paramètres de DNS à la connexion (Windows uniquement) (plus utilisé)	(GlobalProtect 4.0.2 et versions antérieures) Configurez les préférences relatives au serveur DNS pour le tunnel GlobalProtect : • Sélectionnez **No (Non)** (par défaut) pour permettre aux points de terminaison Windows d'envoyer les requêtes DNS au serveur DNS établi sur l'adaptateur physique si la requête initiale envoyée au serveur DNS configuré sur la passerelle n'est pas résolue. Cette option conserve le comportement natif de Windows pour interroger tous les serveurs DNS sur tous les adaptateurs de manière récursive, ce qui peut toutefois se traduire par de longues périodes d'attente pour résoudre certaines requêtes DNS. • Sélectionnez **Yes (Oui)** pour permettre aux points de terminaison Windows de résoudre toutes les requêtes DNS auprès des serveurs DNS que vous configurez sur la passerelle au lieu des serveurs DNS établis sur l'adaptateur physique sur le point de terminaison. Lorsque vous activez cette option, GlobalProtect applique strictement les paramètres DNS de la passerelle et remplace les paramètres statiques de tous adaptateurs physiques. *Lorsque ce paramètre est activé, (définir sur Yes (Oui)) il se peut que GlobalProtect n'arrive pas à restaurer les paramètres DNS précédemment enregistrés et, par conséquent, que le point de terminaison ne puisse pas résoudre les requêtes DNS. Cette fonctionnalité n'est plus utilisée et est remplacée par une implémentation améliorée permettant d'éviter que ce scénario ne se produise. Si vous utilisée auparavant cette fonctionnalité, nous vous recommandons de passer à l'application GlobalProtect 4.0.3 ou à une version ultérieure.* Pour configurer les paramètres DNS de l'application GlobalProtect 4.0.3 ou d'une version ultérieure, utilisez l'option **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Résoudre tous les FQDN à l'aide des serveurs DNS assignés par le tunnel)**.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
Détecter le proxy pour chaque connexion (Windows uniquement)	Sélectionnez **No (Non)** pour détecter automatiquement le proxy pour la connexion de portail et utiliser ce proxy pour les connexions ultérieures. Sélectionnez **Yes (Oui)** (par défaut) pour détecter automatiquement le proxy à chaque connexion.
Définissez le proxy du tunnel (Windows et Mac uniquement)	Spécifiez si GlobalProtect doit utiliser ou contourner les proxys. Sélectionnez **No (Non)** pour exiger le contournement des proxys par GlobalProtect. Sélectionnez **Yes (Oui)** pour exiger l'utilisation des proxys par GlobalProtect. Selon l'utilisation des proxys GlobalProtect, des systèmes d'exploitation des points de terminaison et du type de tunnel, le trafic réseau fonctionnera différemment.
Envoyer immédiatement un rapport HIP si l'état du centre de sécurité de Windows (WSC) change (Windows uniquement)	Sélectionnez **No (Non)** pour empêcher l'application GlobalProtect d'envoyer des données de HIP lorsque le statut du Centre de sécurité Windows (WSC) change. Sélectionnez **Yes (Oui)** (par défaut) pour envoyer immédiatement les données HIP lorsque le statut du WSC change.
Activer les invites d'authentification entrantes des passerelles MFA	Pour prendre en charge la Multi-Factor Authentication (authentification multifacteur ; MFA), un point de terminaison GlobalProtect doit recevoir et reconnaître les invites UDP qui proviennent de la passerelle. Sélectionnez **Yes (Oui)** pour permettre à un point de terminaison GlobalProtect de recevoir et d'accepter l'invite. Sélectionnez **No (Non)** (par défaut) pour que GlobalProtect bloque les invites UDP en provenance de la passerelle.
Port réseau pour les invites d'authentification entrante (UDP)	Spécifie le numéro de port qu'un point de terminaison GlobalProtect utilise pour recevoir les invites d'authentification entrantes en provenance des passerelles MFA. Le port par défaut est 4501. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
Passerelles MFA de confiance	Spécifie la liste des pare-feu ou des passerelles d'authentification auxquels un point de terminaison GlobalProtect fait confiance pour l'authentification multifacteur. Lorsqu'un point de terminaison GlobalProtect reçoit un message UDP sur le port réseau spécifié, GlobalProtect affiche un message d'authentification uniquement si l'invite UDP provient d'une passerelle de confiance.
Message d'authentification entrant	Personnalisez un message de notification à afficher lorsque les utilisateurs tentent d'accéder à une ressource qui nécessite une authentification supplémentaire. Lorsque les utilisateurs tentent d'accéder à une ressource qui nécessite une authentification supplémentaire, GlobalProtect reçoit un paquet UDP contenant l'invite d'authentification entrante et affiche ce message. Le paquet UDP contient également l'URL menant à la page du Portail d'authentification que vous

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	avez précisée lors de la Configuration de l'authentification multifacteur. GlobalProtect ajoute automatiquement l'URL au message. Par exemple : `You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at` Le message doit contenir un maximum de 255 caractères.
IPv6 préféré	Spécifie le protocole privilégié pour les communications des points de terminaison de GlobalProtect. Sélectionnez **No (Non)** pour remplacer le protocole privilégié par IPv4. Sélectionnez Oui (par défaut) pour que IPv6 devienne la connexion privilégiée d'un environnement en double pile.
Message de changement de mot de passe	Personnalise un message visant la définition des exigences ou des politiques en matière de mots de passe lorsque les utilisateurs modifient leur mot de passe Active Directory (répertoire actif ; AD). Par exemple : `Passwords must contain at least one number and one uppercase letter.` Le message doit contenir un maximum de 255 caractères pour les langages Unicodes sur 2 octets, comme le chinois simplifié. Pour le japonais, le message doit contenir un maximum de 128 caractères.
Affichez le panneau d'état lors du démarrage (Windows uniquement)	Sélectionnez **Yes (Oui)** pour afficher automatiquement le panneau d'état GlobalProtect lorsque les utilisateurs établissent une connexion pour la première fois. Sélectionnez **No (Non)** pour supprimer le panneau d'état GlobalProtect lorsque les utilisateurs établissent une connexion pour la première fois.
Désactiver l'application GlobalProtect	
Code secret/Confirmer le code secret	Entrez et puis confirmez le code secret si les paramètres pour **Allow User to Disable GlobalProtect App (Permettre à l'Utilisateur de désactiver l'application GlobalProtect)** est **Allow with Passcode (Permettre avec code secret)**. Enregistrez et stockez le code secret dans un endroit sûr. Vous pouvez distribuer le code secret aux nouveaux utilisateurs de GlobalProtect par e-mail ou l'afficher dans une zone de support de votre site Web de l'entreprise. Si les circonstances empêchent le terminal d'établir une connexion VPN et que cette fonction est activée, un utilisateur peut entrer ce code secret dans l'interface de l'application

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	pour désactiver l'application GlobalProtect et obtenir l'accès à Internet sans utiliser le VPN.
Nombre max. de fois qu'un utilisateur peut désactiver	Indiquez le nombre maximum de fois qu'un utilisateur peut désactiver GlobalProtect avant de devoir se connecter à un pare-feu. La valeur par défaut de 0 signifie que les utilisateurs n'ont pas de limite au nombre de fois où ils peuvent désactiver l'application.
Désactiver le délai d'expiration (min)	Spécifiez le nombre maximal de minutes que l'application GlobalProtect peuvent être désactivés. Une fois que le temps spécifié passe, l'application tente de se connecter au pare-feu. La valeur par défaut de 0 indique que la période de désactivation est illimitée.  *Définir une valeur de délai de désactivation pour restreindre la période de temps pendant laquelle les utilisateurs peuvent désactiver l'application. Ainsi, GlobalProtect peut reprendre et établir le VPN lorsque le délai est dépassé afin de protéger l'utilisateur et de sécuriser son accès aux ressources.*
Désinstaller l'application GlobalProtect	
Mot de passe/Confirmer le mot de passe	Entrez et puis confirmez le mot de passe si le paramètre pour **Allow User to Uninstall GlobalProtect App (Permettre à l'utilisateur de désinstaller l'application GlobalProtect)** est **Allow with Password (Permettre avec mot de passe)**. Enregistrez et stockez le mot de passe dans un endroit sûr. Utilisez ce paramètre pour empêcher les utilisateurs de désinstaller l'application GlobalProtect. Une fois configuré, l'utilisateur doit saisir ce mot de passe sur l'interface de l'application GlobalProtect pour désinstaller l'application GlobalProtect.
Paramètres Mobile Security Manager	
Mobile Security Manager	Si vous utilisez le gestionnaire de sécurité mobile de GlobalProtect pour la gestion des périphériques mobiles (MDM), saisissez l'adresse IP ou le nom de domaine complet (FQDN) de l'interface d'inscription/d'enregistrement du périphérique sur l'appareil GP-100.
Port d'inscription	Le numéro de port que le terminal mobile doit utiliser pour l'inscription lors de la connexion au gestionnaire de sécurité mobile de GlobalProtect. Le Gestionnaire de sécurité mobile écoute sur le port 443 par défaut.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration de l'application GlobalProtect	Description
	Gardez ce numéro de port afin qu'un certificat ne soit pas demandé aux utilisateurs finaux mobiles au cours du processus d'inscription (les autres valeurs possibles sont 443, 7443 et 8443).

Onglet Collecte de données HIP de l'agent des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (<configuration du portail>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **HIP Data Collection (Collecte de données HIP)**

Sélectionnez l'onglet **HIP Data Collection (Collecte de données HIP)** pour définir les données que l'application collecte à partir du point de terminaison du rapport HIP :

Paramètres de Configuration de collecte des données HIP GlobalProtect	Description
Collecter les données HIP	Désactivez cette option pour empêcher l'application de collecter et d'envoyer des données HIP. *Activez la collecte des données HIP pour l'application de la politique fondée sur HIP sur GlobalProtect, pour que le pare-feu puisse associer les données HIP des points de terminaison aux objets HIP et/ou aux profils HIP que vous définissez, puis appliquez la politique appropriée.*
Temps d'attente max (sec)	Indiquez le nombre de secondes que l'application doit rechercher des données HIP avant de soumettre les données disponibles (plage comprise entre 10 et 60 ; 20 par défaut).
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Exclure les catégories	Sélectionnez **Exclude Categories (Exclure catégories)** pour définir les catégories d'informations sur l'hôte pour lesquelles vous ne souhaitez pas que l'application collecte des données HIP. Sélectionnez une **Category (Catégorie)** (comme la prévention de la perte de données) à exclure de la collecte HIP. Après avoir sélectionné une catégorie, vous pouvez **Add (Ajouter)** un Fournisseur particulier, puis vous pouvez **Add (Ajouter)** des produits spécifiques en provenance du fournisseur pour affiner l'exclusion au besoin. Cliquez sur **OK** pour sauvegarder les paramètres dans chaque dialogue.
Vérifications personnalisées	Sélectionnez **Custom Checks (Vérifications personnalisées)** pour définir les informations personnalisées sur l'hôte que l'application doit collecter. Par exemple, si vous disposez d'applications non incluses dans les listes de fournisseurs et/ou de produits, qui sont requises pour la création d'objets HIP, vous pouvez créer une vérification personnalisée qui vous

© 2020 Palo Alto Networks, Inc.

Paramètres de Configuration de collecte des données HIP GlobalProtect	Description
	permet de déterminer si l'application est installée (doit avoir une clé de registre Windows ou Plist Mac correspondante) ou est présentement en cours d'exécution (a un processus en cours d'exécution correspondant) : • **Windows** : **Add (Ajouter)** pour ajouter une vérification d'une clé de registre et/ou d'une valeur de clé particulière. • **Mac** : **Add (Ajouter)** pour ajouter une vérification d'une clé plist ou d'une valeur de clé particulière. • **Process List (Liste des processus)** : **Add (Ajouter)** les processus que vous souhaitez vérifier sur les terminaux de l'utilisateur pour voir s'ils sont en cours d'exécution. Par exemple, pour déterminer si une application est en cours d'exécution, ajoutez le nom du fichier exécutable à la liste des processus. Vous pouvez ajouter une liste de processus dans l'onglet **Windows** ou **Mac**.

Onglet des VPN sans client des portails GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (<configuration du portail>)* > **Clientless VPN (VPN sans client)**

Vous pouvez désormais configurer le portail GlobalProtect pour fournir un accès distant sécurisé aux applications Web d'entreprise communes qui utilisent les technologies HTML, HTML5 et JavaScript. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel GlobalProtect. Cela est utile lorsque vous devez activer l'accès à ces applications pour des partenaires ou des entrepreneurs et pour activer de manière sécurisée les actifs non gérés, y compris les appareils personnels. Cette fonctionnalité nécessite que vous installiez un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client depuis le portail GlobalProtect. Sélectionnez l'onglet **Clientless VPN (VPN sans client)** pour configurer les paramètres du VPN sans client de GlobalProtect sur le portail, comme décrit dans le tableau suivant :

Paramètres de configuration sans client du portail GlobalProtect	Description
Onglet Général	
VPN sans client	Sélectionnez **Clientless VPN (VPN sans client)** pour spécifier des informations générales sur la session VPN sans client :
Nom d'hôte	L'adresse IP ou FQDN pour le portail GlobalProtect qui héberge la page de destination des applications Web. Le VPN sans client GlobalProtect réécrit les URL de l'application avec ce nom d'hôte.  *Si vous utilisez la Traduction des adresses réseau (NAT) pour fournir un accès au portail GlobalProtect, l'adresse IP ou FQDN que vous saisissez doit correspondre à (ou se résoudre en) l'adresse IP NAT du portail GlobalProtect (l'adresse IP publique).*

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration sans client du portail GlobalProtect	Description
Zone de sécurité	La zone pour la configuration VPN sans client. Les règles de sécurité définies dans cette zone contrôlent les applications auxquelles les utilisateurs peuvent accéder.
Proxy DNS	Le serveur DNS qui résout les noms des applications. Sélectionnez un serveur **DNS Proxy (Proxy DNS)** ou configurez un **New DNS Proxy (Nouveau proxy DNS)** (Réseau > Proxy DNS).
Durée de vie de la connexion	Le nombre de **Minutes** (entre 60 et 1 440) ou d'**Hours (Heures)** (entre 1 et 24, la valeur par défaut est 3) durant lequel une session VPN SSL sans client est valide. Après la durée spécifiée, les utilisateurs doivent se réauthentifier et démarrer une nouvelle session VPN sans client.
Délai d'inactivité	Le nombre de **Minutes** (entre 5 et 1 440, la valeur par défaut est 30) ou d'**Hours (Heures)** (entre 1 et 24) durant lequel une session VPN SSL sans client peut rester inactive. S'il n'y a pas d'activité de la part d'un utilisateur pendant la durée spécifiée, il doit se réauthentifier et démarrer une nouvelle session VPN sans client.
Nombre max. d'utilisateurs	Le nombre maximum d'utilisateurs qui peuvent être connectés sur le portail en même temps (la valeur par défaut est 10, la plage est de 1 à aucun maximum). Lorsque le nombre maximum d'utilisateurs est atteint, les utilisateurs VPN sans client supplémentaires ne peuvent pas se connecter au portail.
Onglet Applications	
Mappage des applications aux utilisateurs	Vous pouvez **Ajouter** un ou plusieurs **Association des applications aux utilisateurs** pour correspondre aux utilisateurs avec des applications publiées. Cette association définit quels utilisateurs ou groupes d'utilisateurs peuvent utiliser un VPN sans client pour accéder aux applications. Vous devez définir les applications et les groupes d'applications avant de les associer aux utilisateurs (Réseau > GlobalProtect > Applications sans client et Réseau > GlobalProtect > Groupes d'applications sans client). • **Name (Nom)** : donnez un nom au mappage (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. • **Display application URL address bar Allow user to launch unpublished applications (Afficher la barre d'adresse URL d'application)** – Sélectionnez cette option pour afficher une barre d'adresse URL à partir de laquelle les utilisateurs peuvent lancer des applications qui ne sont pas publiées sur la page de renvoi des applications. Lorsque cette option est activée, les utilisateurs peuvent cliquer sur le lien **Application URL (URL de l'application)** qui figure sur la page et indiquer une URL.
Utilisateur/Groupe d'utilisateurs	Vous pouvez **Add (Ajoutez)** des utilisateurs individuels ou des groupes d'utilisateurs auxquels appliquer la configuration d'application actuelle. Ces utilisateurs ont la permission de lancer les applications configurées à l'aide d'un VPN sans client GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration sans client du portail GlobalProtect	Description
	Vous devez configurer l'association de groupe (Device (Périphérique) > User Identification (Identification utilisateur) > Group Mapping Settings (Paramètres d'association des groupes)) avant de pouvoir sélectionner les groupes. En plus des utilisateurs et des groupes, vous pouvez spécifier quand ces paramètres sont applicables aux utilisateurs ou groupes : • **any (tous)** : la configuration de l'application s'applique à tous les utilisateurs (pas besoin d'**Add (Ajouter)** des utilisateurs ou des groupes d'utilisateurs). • **select (sélectionner)** : la configuration d'application s'applique uniquement aux utilisateurs et groupes d'utilisateurs que vous souhaitez **Add (Ajouter)** à cette liste.
Applications	Vous pouvez **Ajouter** des applications individuelles ou des groupes d'applications à l'association. Les **Source Users (Utilisateurs source)** que vous avez inclus à la configuration peuvent utiliser le VPN sans client GlobalProtect pour lancer les applications que vous ajoutez.
Onglet Paramètres Crypto	
Versions du protocole	Sélectionnez les versions TLS/SSL minimales et maximales requises. Plus la version TLS est élevée, plus la connexion est sécurisée. Les choix comprennent **SSLv3**, **TLSv1.0**, **TLSv1.1** ou **TLSv1.2**.
Algorithmes d'échange de clés	Sélectionnez les types d'algorithmes pris en charge pour l'échange de clés. Les choix comprennent **RSA**, Diffie-Hellman (**DHE**) ou Diffie-Hellman basé sur les courbes elliptiques éphémères (**ECDHE**).
Algorithmes de chiffrement	Sélectionnez les algorithmes de cryptage pris en charge. **AES128** ou supérieur est recommandé.
Algorithmes d'authentification	Sélectionnez les algorithmes d'authentification pris en charge. Les choix sont les suivants : **MD5**, **SHA1**, **SHA256** ou **SHA384**. **SHA256** ou supérieur est recommandé.
Vérification des certificats du serveur	Choisissez les mesures à prendre pour les problèmes suivants, qui peuvent survenir lorsqu'une application présente un certificat de serveur : • **Block sessions with expired certificate (Bloquer les sessions avec un certificat expiré)** : si le certificat du serveur a expiré, bloquez l'accès à l'application. • **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)** : si le certificat du serveur est émis à partir d'une autorité de certification non approuvée, bloquez l'accès à l'application. • **Block sessions with unknown certificate status (Bloquer les sessions dont l'état du certificat est inconnu)** : si le service OCSP ou CRL renvoie un

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration sans client du portail GlobalProtect	Description
	état de révocation de certificat `unknown (inconnu)`, bloquez l'accès à l'application. • **Block sessions on certificate status check timeout (Bloquer les sessions dont le délai d'attente de vérification de l'état du certificat a expiré)** : si l'état du certificat vérifie les délais avant de recevoir une réponse de tout service d'état du certificat, bloquez l'accès à l'application.
Onglet Proxy	
Name (Nom)	Une étiquette qui se compose d'un maximum de 31 caractères afin de permettre l'identification du serveur proxy que le portail GlobalProtect utilise pour accéder aux applications publiées. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Domaines	Ajoutez les domaines servis par le serveur proxy.
Utiliser le proxy	Sélectionnez cette option pour autoriser le portail GlobalProtect à utiliser le serveur proxy pour accéder aux applications publiées.
Serveur Port	Spécifiez le nom d'hôte (ou l'adresse IP) et le numéro de port du serveur proxy.
Utilisateur Mot de passe	Spécifiez le nom d'utilisateur et le mot de passe nécessaires pour se connecter au serveur proxy. Saisissez à nouveau le mot de passe pour le vérifier.
Onglet Paramètres avancés	
Réécrire la liste des domaines d'exclusion	(Facultatif) Vous pouvez **Ajouter** des noms de domaine, des noms d'hôte ou des adresses IP pour **Rewrite Exclude Domain List (Réécrire la liste des domaines d'exclusion)**. Le VPN sans client agit comme un proxy inversé et modifie les pages renvoyées par les applications publiées. Lorsqu'un utilisateur distant accède à l'URL, les demandes passent par le portail GlobalProtect. Dans certains cas, l'application peut comporter des pages auxquelles il n'est pas nécessaire d'accéder via le portail. Spécifiez les domaines qui doivent être exclus des règles de réécriture et qui ne peuvent pas être réécrits. Les chemins ne sont pas pris en charge dans les noms d'hôte et de domaine. Le caractère générique (*) pour les noms d'hôte et de domaine ne peut apparaître qu'au début du nom (par exemple, * .etrade.com).

Onglet du satellite du portail GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Satellite**

Un satellite est un pare-feu Palo Alto Networks®, généralement dans une succursale, qui agit en tant qu'application GlobalProtect pour permettre au satellite d'établir une connectivité VPN avec une

© 2020 Palo Alto Networks, Inc.

passerelle GlobalProtect. Comme une application GlobalProtect, le satellite reçoit sa configuration initiale du portail, qui inclut les certificats et les informations de routage de configuration VPN lui permettant de se connecter à toutes les passerelles configurées pour établir une connectivité VPN.

Avant de définir les paramètres de configuration satellite GlobalProtect sur le pare-feu de la succursale, vous devez configurer une interface dotée de la connectivité WAN, puis paramétrer une zone de sécurité et une politique, afin d'autoriser le réseau LAN de la succursale à communiquer avec Internet. Vous pouvez ensuite sélectionner l'onglet **Satellite** pour configurer les paramètres de configuration satellite GlobalProtect sur le portail, comme décrit dans le tableau suivant :

Paramètres de configuration satellite du portail GlobalProtect	Description
Général	• **Name (Nom)** : un nom pour cette configuration satellite sur le portail GlobalProtect. • **Configuration Refresh Interval (hours) (Intervalle d'actualisation de la configuration (heures))** : la fréquence à laquelle le satellite doit rechercher des mises à jour de la configuration sur le portail (par défaut 24, plage de 1 à 48).
Périphériques	**Add (Ajouter)** un satellite en utilisant le **Serial Number (Numéro de série)** du pare-feu. Le portail peut accepter un numéro de série ou les informations d'identification pour identifier qui demande une connexion ; si le portail ne reçoit pas un numéro de série, il demande des informations d'identification. Si vous identifiez le satellite par son numéro de série de pare-feu, vous n'avez pas besoin de fournir les informations d'identification de l'utilisateur lorsque le satellite se connecte d'abord pour acquérir le certificat d'authentification et sa configuration initiale. Une fois que le satellite s'authentifie soit par un numéro de série ou les informations d'identification, le **Satellite Hostname (Nom d'hôte du satellite)** est automatiquement ajouté au portail.
Utilisateur/Groupe d'utilisateurs d'inscription	Le portail peut utiliser les paramètres **Enrollment User/User Group (Inscription utilisateur/groupe d'utilisateurs)** avec ou sans les numéros de série pour faire correspondre un satellite à cette configuration. Les satellites ne correspondant pas au numéro de série doivent s'authentifier soit en tant qu'utilisateur individuel ou membre de groupe. **Add (Ajouter)** l'utilisateur ou le groupe que vous souhaitez contrôler avec cette configuration. *Avant de pouvoir limiter la configuration à des groupes spécifiques, vous devez activer Mappage du groupe dans le pare-feu (Device (Périphérique) > User Identification (Identification utilisateur) > Group Mapping Settings (Paramètres de mappage de groupe)).*
Passerelles	Cliquez sur **Add (Ajouter)** pour saisir l'adresse IP ou le nom d'hôte de la ou des passerelles par lesquelles les satellites dans cette configuration peuvent établir des tunnels IPSec. Dans le champ **Gateways (Passerelles)**, saisissez le nom de domaine complet, FQDN, ou l'adresse IP de l'interface sur laquelle la passerelle est configurée. Les adresses IP peuvent être spécifiées en tant que **IPv6**, **IPv4**, ou les deux. Sélectionnez **IPv6 Preferred (IPv6 Privilégié)**

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration satellite du portail GlobalProtect	Description
	pour spécifier la préférence des connexions IPv6 dans un environnement en double pile. (Facultatif) Si vous ajoutez deux passerelles ou plus à la configuration, la **Routing Priority (Priorité de routage)** aide le satellite à choisir la passerelle préférée (plage de 1 à 25). Les nombres inférieurs ont une priorité plus élevée (pour les passerelles qui sont disponibles). Le satellite multiplie la priorité de routage par 10 pour déterminer la mesure de routage. *Les itinéraires publiés par la passerelle sont installés sur le satellite en tant qu'itinéraires statiques. La mesure de l'itinéraire statique correspond à 10 fois la priorité de routage. Si vous disposez de plusieurs passerelles, veillez à définir également la priorité d'itinéraire pour s'assurer que les itinéraires publiés par les passerelles de secours incluent des mesures supérieures aux mêmes itinéraires publiés par les passerelles principales. Par exemple, si vous définissez la priorité de routage de la passerelle principale et de la passerelle de secours sur 1 et 10, respectivement, le satellite utilisera la mesure 10 pour la passerelle principale et 100 pour la passerelle de secours.* Le satellite partage également son réseau et les informations de routage avec les passerelles si vous **Publish all static and connected routes to Gateway (Publiez toutes les routes statiques et connectées à la passerelle)** (**Network (Réseau)** > **IPSec tunnels (Tunnels IPSec)** > **<tunnel** > **Advanced (Avancé)** - disponible uniquement lorsque vous sélectionnez **GlobalProtect Satellite on the <tunnel (Satellite GlobalProtect sur le <tunnel** > **General (Général)**).
CA racine approuvée	Cliquez sur **Add (Ajouter)**, puis sélectionnez le certificat AC utilisé pour générer les certificats serveur de passerelle. Les certificats de l'autorité de certification racine de confiance sont transmis aux points de terminaison en même temps que la configuration de l'agent du portail. *Spécifiez une autorité de certification racine de confiance pour vérifier les certificats du serveur de la passerelle et pour établir des connexions de tunnel VPN aux passerelles GlobalProtect. Il est recommandé que toutes vos passerelles utilisent le même émetteur.* *Vous pouvez cliquer sur Import (Importer) ou Generate (Générer) un certificat AC racine pour la délivrance de certificats de vos serveurs de passerelle si un n'existe pas déjà sur le portail.*
Certificat du client	
Local	• **Issuing Certificate (Publication du certificat)** – Sélectionnez l'AC racine qui émet le certificat utilisé par le portail pour émettre des certificats à un satellite après la réussite de son authentification. Si le certificat

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration satellite du portail GlobalProtect	Description
	nécessaire n'existe pas déjà sur le pare-feu, vous pouvez **Import (Importer)** ou**Generate (Générer).** *Si un certificat ne réside pas déjà sur le pare-feu, vous pouvez Import (Importer) ou Generate (Générer) un certificat d'émission.* • **OCSP Responder (Répondeur OCSP)** – Sélectionnez le Répondeur OCSP utilisé par le satellite pour vérifier le statut de révocation des certificats présentés par le portail et les passerelles. Sélectionnez **None (Aucun)** pour spécifier qu'OCSP n'est pas utilisé pour la vérification de la révocation d'un certificat. *Activez un répondeur OCSP de satellite de sorte que vous soyez avisé de la révocation éventuelle d'un certificat afin de pouvoir prendre les mesures appropriées pour établir une connexion sécurisée au portail et aux passerelles. Pour activer un répondeur OCSP de satellite, vous devez également activer CRL et OCSP dans les paramètres Certificate Revocation Checking (Vérification de la révocation du certificat) (Device [Périphérique] > Setup [Configuration] > Session > Decryption Settings [Paramètres de déchiffrement]).* • **Validity Period (Période de validité)** (jours) – Spécifiez la durée de vie du certificat du satellite GlobalProtect (la plage est de 7 à 365 ; 7 par défaut). • **Certificate Renewal Period (Période de renouvellement du certificat)** (jours) – Indiquez le nombre de jours avant l'expiration pendant lesquels les certificats peuvent être renouvelés automatiquement (plage est de 3 à 30 ; 3 par défaut).
SCEP	• **SCEP** – Sélectionnez un profil SCEP pour générer des certificats clients. Si le profil n'est pas dans le menu déroulant, vous pouvez créer un **Nouveau** profil. • **Certificate Renewal Period (Période de renouvellement du certificat)** (jours) – Indiquez le nombre de jours avant l'expiration pendant lesquels les certificats peuvent être renouvelés automatiquement (plage est de 3 à 30 ; 3 par défaut).

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Passerelles

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** pour configurer une passerelle GlobalProtect. Une passerelle peut fournir des connexions VPN pour les applications GlobalProtect ou pour les satellites GlobalProtect.

À partir de la boîte de dialogue Passerelle GlobalProtect, **Ajouter** une nouvelle configuration de passerelle ou sélectionnez une configuration de passerelle existante pour la modifier.

Que voulez-vous faire ?	Reportez-vous à la section :
Quels paramètres généraux puis-je configurer pour la passerelle GlobalProtect ?	Onglet Général des passerelles GlobalProtect
Comment puis-je configurer l'authentification de la passerelle client ?	Onglet d'authentification de la passerelle GlobalProtect
Comment puis-je configurer les tunnels et les paramètres réseau qui permettent à une application d'établir un tunnel VPN avec la passerelle ?	Onglet Agent de passerelles GlobalProtect
Comment puis-je configurer les paramètres du tunnel et de réseau pour permettre aux satellites d'établir des connexions VPN avec une passerelle agissant comme un satellite?	Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect)
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées sur la configuration du portail, reportez-vous à la section Configuration d'un portail GlobalProtect du Guide de l'administrateur de GlobalProtect.

Onglet Général des passerelles GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (configuration de la passerelle)* > **General (Général)**

Sélectionnez l'onglet **General (Général)** pour définir l'interface de passerelle à laquelle les applications peuvent se connecter et indiquer comment la passerelle authentifie les points de terminaison.

Paramètres généraux d'une passerelle GlobalProtect	Description
Name (Nom)	Donnez un nom à la passerelle (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'une passerelle GlobalProtect	Description
	GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. *Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son Location (Emplacement).*
Paramètres de la zone réseau	
Interface	Sélectionnez le nom de l'interface pare-feu qui servira de l'interface d'entrée pour les terminaux distants. (Ces interfaces doivent déjà exister.) *N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l'interface de gestion à l'Internet. Reportez-vous à la section Pratiques exemplaires pour sécuriser l'accès administratif pour obtenir de plus amples précisions sur la manière de protéger l'accès à votre réseau de gestion.*
Adresse IP	(Facultatif) Spécifiez l'adresse IP d'accès à la passerelle. Sélectionnez le **Type d'adresse IP**, puis saisissez l'**Adresse IP**. • L'adresse IP peut être de type **IPv4** (trafic IPv4 uniquement), **IPv6** (trafic IPv6 uniquement) ou **IPv4 et IPv6**. Utilisez **IPv4 et IPv6** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. Si vous choisissez **IPv4 et IPv6**, saisissez le type d'adresse appropriée pour chacun.

Onglet d'authentification de la passerelle GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (configuration de la passerelle)* > **Authentication (Authentification)**

Sélectionnez l'onglet **Authentication (Authentification)** pour identifier le profil de service SSL/TLS et pour configurer les détails de l'authentification du client. Vous pouvez ajouter plusieurs configurations d'authentification du client.

Paramètres d'authentification de la passerelle GlobalProtect	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS pour sécuriser cette passerelle GlobalProtect. Pour obtenir des renseignements sur les contenus d'un profil de service, reportez-vous à la section Périphérique > Gestion des certificats > Profil de service SSL/TLS.

© 2020 Palo Alto Networks, Inc.

Paramètres d’authentification de la passerelle GlobalProtect	
Zone d'Authentification du Client	
Name (Nom)	Saisissez un Nom unique pour identifier cette configuration.
Système d’exploitation	Par défaut, la configuration s'applique à tous les points de terminaison. Vous pouvez filtrer la liste des points de terminaison par système d’exploitation (**Android**, **Chrome**, **iOS**, **IoT [IdO]**, **Linux**, **Mac**, **Windows** ou**WindowsUWP**), par périphériques **Satellite**, ou par clients VPN IPSec tiers (**X-Auth**). Le système d'exploitation est le différentiateur principal entre plusieurs configurations. Si vous avez besoin de plusieurs configurations pour un système d'exploitation, vous pouvez en outre distinguer les configurations par votre choix de profil d'authentification.  *Ordonnez les configurations des plus spécifiques au sommet de la liste aux plus générales en bas.*
Profil d'authentification	Choisissez un profil ou une séquence d'authentification de la liste déroulante pour l'accès à la passerelle. Reportez-vous à la section Périphérique > Profil d’authentification.  *Aux fins d'authentification du client, assurez-vous que le profil d'authentification utilise RADIUS ou SAML avec l’authentification à deux facteurs. Si vous n’utilisez pas RADIUS ou SAML, vous n'avez pas à configurer un profil de certificat en plus d’un profil d’authentification.*
Étiquette de nom d’utilisateur	Indiquez une étiquette de nom d’utilisateur personnalisée pour la connexion à la passerelle GlobalProtect. Par exemple, **Nom d’utilisateur (uniquement)** ou **Adresse électronique (nomd’utilisateur@domaine)**.
Étiquette de mot de passe	Indiquez une étiquette de mot de passe personnalisée pour la connexion à la passerelle GlobalProtect. Par exemple, **Mot de passe (Turc)** ou **Code secret** (pour l’authentification basée sur jeton à deux facteurs).
Message d'authentification	Pour aider les utilisateurs finaux à connaître les informations d'identification qu'ils doivent utiliser pour se connecter à cette passerelle, vous pouvez saisir un message ou garder le message par défaut. Le message peut avoir un maximum de 256 caractères.

© 2020 Palo Alto Networks, Inc.

Paramètres d'authentification de la passerelle GlobalProtect	
Permettre l'authentification avec les informations d'identification de l'utilisateur OU le certificat du client	Si vous sélectionnez **No (Non)**, les utilisateurs doivent s'authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur et les certificats de client. Si vous sélectionnez **Yes (Oui)**, les utilisateurs peuvent s'authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur ou les certificats de client.
Profil du certificat	
Profil du certificat	(Facultatif) Sélectionnez le **Profil du certificat** que le portail utilise pour correspondre aux certificats clients qui proviennent des points d'extrémité utilisateur. Avec un Profil de certificat, la passerelle n'authentifie l'utilisateur que si le certificat du client correspond à ce profil. Si vous établissez l'option **Allow Authentication with User Credentials OR Client Certificate (Permettre l'authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **No (Non)**, vous devez sélectionner un **Certificate Profile (Profil de certificat)**. Si vous établissez l'option **Allow Authentication with User Credentials OR Client Certificate (Permettre l'authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **Yes (Oui)**, le **Certificate Profile (Profil de certificat)** est facultatif. Le profil de certificat est indépendant du système d'exploitation.

Onglet Agent de passerelles GlobalProtect

- **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent**

Sélectionnez l'onglet **Agent** pour configurer les paramètres du tunnel qui permettent à l'application d'établir un tunnel VPN avec la passerelle. En outre, cet onglet vous permet de spécifier les délais d'attente pour les VPN, les services de réseau de DNS et WINS, et les messages de notification de HIP pour les utilisateurs finaux sur la correspondance ou non à un profil de HIP attaché à une règle de politique de Sécurité.

Configurer les paramètres de l'Agent sur les onglets suivants :

- Onglet Paramètres du tunnel
- Onglet Paramètres du client
- Onglet Pools d'adresses IP du client
- Onglet Services du réseau
- Onglet Paramètres de connexion
- Onglet Trafic vidéo
- Onglet Notification HIP

© 2020 Palo Alto Networks, Inc.

Onglet Paramètres du tunnel

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Tunnel Settings (Paramètres du tunnel)**

Sélectionnez l'onglet **Tunnel Settings (Paramètres du tunnel)** pour activer la tunnellisation et configurer les paramètres du tunnel.

Les paramètres de tunnel doivent être définis si vous configurez une passerelle externe. Si vous configurez une passerelle interne, les paramètres de tunnel sont facultatifs.

Paramètres de configuration du mode tunnel du client GlobalProtect	Description
Mode tunnel	Sélectionnez le **Tunnel Mode (Mode tunnel)** pour activer le mode tunnel, puis spécifiez les paramètres suivants : • **Tunnel Interface (Interface de tunnel)** - Choisissez une interface de tunnel pour l'accès à la passerelle. • **Max User (Nombre max. d'utilisateurs)** - Précisez le nombre maximum d'utilisateurs pouvant accéder à la passerelle simultanément, pour l'authentification ainsi que les mises à jour HIP et de l'application GlobalProtect. Si le nombre maximum d'utilisateurs est atteint, les utilisateurs suivants se voient refuser l'accès et un message d'erreur indiquant que le nombre maximum d'utilisateurs est atteint s'affiche (la plage varie d'une plateforme à l'autre et s'affiche lorsque le champ est vide). • **Enable IPSec (Activer IPSec)** - Sélectionnez cette option pour activer le mode IPSec pour le trafic des points de termnaison, IPSec devenant ainsi la méthode principale et SSL-VPN la méthode de secours. Les autres options ne sont pas disponibles jusqu'à ce qu'IPSec soit activé. • **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtect)** - Sélectionnez un profil crypto IPSec GlobalProtect qui définit les algorithmes d'authentification et de cryptage pour les tunnels VPN. Le profil **default (par défaut)** utilise le cryptage AES-128-CBC et l'authentification SHA1. Pour plus d'informations, reportez-vous à Réseau > Profils réseau > Crypto IPSec GlobalProtect. • **Enable X-Auth Support (Activer la prise en charge X-Auth)** - Sélectionnez cette option pour activer la prise en charge Extended Authentication (X-Auth) dans la passerelle GlobalProtect lorsque le mode IPSec est activé. La prise en charge X-Auth permet aux clients VPN IPSec tiers prenant en charge X-Auth (le client VPN IPSec sur les périphériques Apple iOS et Android et le client VPNC sous Linux, par exemple) d'établir un tunnel VPN avec la passerelle GlobalProtect. L'option X-Auth permet au client VPN d'accéder à distance à une passerelle GlobalProtect. Comme l'accès X-Auth fournit des fonctionnalités GlobalProtect limitées, songez à utiliser l'application GlobalProtect pour pouvoir accéder facilement à l'ensemble des fonctions de sécurité offertes par GlobalProtect sur les périphériques iOS et Android.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du mode tunnel du client GlobalProtect	Description
	En sélectionnant **X-Auth Support (Prise en charge X-Auth)** pour activer les options **Group Name (Nom du groupe)** et **Group Password (Mot de passe du groupe)** : • Si le nom et le mot de passe de groupe sont précisés, la première phase d'authentification requiert que les deux parties utilisent ces informations d'identification pour s'authentifier. La seconde phase requiert un nom d'utilisateur et un mot de passe valides, qui sont définis dans le profil d'authentification configuré dans la section Authentification. • Si aucun nom et mot de passe de groupe n'est défini, la première phase d'authentification est basée sur un certificat valide présenté par le client VPN tiers. Ce certificat est ensuite validé dans le profil du certificat configuré dans la section Authentification. • Par défaut, l'utilisateur ne doit pas se réauthentifier lorsque la clé utilisée pour établir le tunnel IPSec expire. Pour exiger que l'utilisateur se réauthentifie, décochez l'option **Skip Auth on IKE Rekey (Ignorer l'authentification lors du renouvellement de la clé)**.

Onglet Paramètres du client

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Client IP Pool (Pool d'adresses IP du client)**

Sélectionnez l'onglet **Client Settings (Paramètres du client)** pour configurer les paramètres de la carte réseau virtuelle sur le point de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

Certaines options Paramètres du client sont uniquement disponibles si vous avez activé le mode tunnel et défini une interface de tunnel dans l'onglet Paramètres du tunnel*.*

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Onglet Config Selection Criteria (Critères de sélection de la configuration)	
Name (Nom)	Saisissez un nom pour identifier la configuration des paramètres du client (jusqu'à 31 caractères). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Source User (Utilisateur source)	**Add (Ajouter)** les groupes d'utilisateurs ou les utilisateurs spécifiques auxquels cette configuration s'applique. *Vous devez configurer le mappage de groupe (Device (Périphérique) > User Identification (Identification Utilisateur) > Group Mapping*

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	Settings (Paramètres de mappage des groupes)) avant de pouvoir sélectionner les utilisateurs et les groupes. Pour déployer cette configuration à tous les utilisateurs, sélectionnez **any (indifférent)** dans le menu déroulant **Source User (Utilisateur source)**. Pour déployer cette configuration uniquement aux utilisateurs disposant d'applications GlobalProtect en mode préouverture de session, sélectionnez **pre-logon (préouverture de session)** dans le menu déroulant **Source User (Utilisateur source)**.  *La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour Source User (Utilisateur source), OS (Système d'exploitation) et Source Address (Adresse source).*
Système d'exploitation	Pour déployer cette configuration selon le système d'exploitation du point de terminaison, vous devez **Add (Ajouter)** un système d'exploitation (**Android**, **Chrome**, **iOS**, **IdO**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**). Vous pouvez également définir cette valeur sur **Any (Indifférente)**, de sorte que la configuration de déploiement est basée uniquement sur le groupe d'utilisateurs ou l'utilisateur et non pas sur le système d'exploitation du point de terminaison.  *La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour Source User (Utilisateur source), OS (Système d'exploitation) et Source Address (Adresse source).*
Source Address (Adresse source)	Pour déployer cette configuration selon l'emplacement de l'utilisateur, **Add (Ajoutez)** une **Region** source ou une **IP Address (Adresse IP)** locale (IPv4 et IPv6). Pour déployer cette configuration à tous les emplacements d'utilisateurs, ne précisez aucune **Region (Région)** ou **IP Address (Adresse IP)**. Vous devez également laisser ces champs vides si vos utilisateurs utilisent la version 4.0 ou une version antérieure de l'application GlobalProtect, car cette fonction n'est pas prise en charge sur les versions antérieures de l'application GlobalProtect.  *La correspondance de la Source Address (Adresse source) réussit si l'emplacement d'un utilisateur se connectant correspond à la Region (Région) ou à la IP Address (Adresse IP) que vous configurez.*

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour Source User (Utilisateur source), OS (Système d'exploitation) et Source Address (Adresse source).
Onglet de Contournement d'authentification	
Contournement d'Authentification	Activer la passerelle pour utiliser des témoins sécurisés, spécifiques au périphérique et chiffrés pour authentifier l'utilisateur une fois que l'utilisateur s'identifie pour la première fois en utilisant le régime d'authentification spécifié par le profil d'authentification ou le certificat. • **Generate cookie for authentication override (Générer témoin pour contournement de l'authentification)** : Pendant la durée de vie du témoin, l'agent présente ce témoin chaque fois que l'utilisateur s'authentifie avec la passerelle. • **Cookie Lifetime (Durée de vie des cookies)** : spécifiez les heures, les jours ou les semaines pour lesquelles le témoin est valide. La durée de vie typique est de 24 heures. Les plages sont 1 à 72 heures, 1 à 52 semaines ou 1 à 365 jours. Après l'expiration du témoin, l'utilisateur doit entrer les informations d'identification et le portail chiffre ensuite un nouveau témoin à envoyer à l'utilisateur terminal. • **Accept cookie for authentication override (Accepter le témoin pour le contournement de l'authentification)** : Sélectionnez cette option pour configurer la passerelle pour accepter l'authentification en utilisant le témoin chiffré. Lorsque l'agent présente le témoin, la passerelle valide que le témoin a été chiffré par la passerelle avant l'authentification de l'utilisateur. • **Certificate to Encrypt/Decrypt Cookie (Certificat pour chiffrer/déchiffrer le témoin)** : Sélectionnez le certificat à utiliser pour chiffrer et déchiffrer le témoin. *Veiller à ce que le portail et la passerelle utilisent le même certificat pour chiffrer et déchiffrer les témoins.*
Onglet Pools d'adresses IP	
Récupérer l'attribut Adresse IP tramée auprès du serveur d'authentification	Sélectionnez cette option pour permettre à la passerelle GlobalProtect d'attribuer des adresses IP fixes à l'aide d'un serveur d'authentification externe. Lorsque cette option est activée, la passerelle GlobalProtect alloue l'adresse IP pour la connexion à des périphériques en utilisant l'attribut Adresse IP adresse tramée du serveur d'authentification.

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Pool d'adresses IP du serveur d'authentification	**Add (Ajouter)** un sous-ensemble ou une plage d'adresses IP à attribuer aux utilisateurs distants. Lorsque le tunnel est établi, la passerelle GlobalProtect affecte l'adresse IP dans cette plage aux périphériques se connectant à l'aide de l'attribut Adresse IP tramée du serveur d'authentification. Vous pouvez ajouter des adresses IPv4 (comme 192.168.74.0/24 et 192.168.75.1-192.168.75.100) ou des adresses IPv6 (comme 2001:aa::1-2001:aa::10). Vous pouvez activer et configurer l'**Authentication Server IP Pool (Authentification du serveur du pool d'adresses IP)** uniquement si vous activez **Retrieve Framed-IP-Address attribute from authentication server (Récupérer l'attribut d'adresse IP du serveur d'authentification)**.  *le pool d'adresses IP du serveur d'authentification doit être suffisamment important pour prendre en charge toutes les connexions simultanées. L'attribution d'adresse IP est fixe et est conservée une fois l'utilisateur déconnecté. Configure plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux clients une adresse IP non conflictuelle avec les autres interfaces du client.* Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple, pour le réseau 192.168.0.0/16, un utilisateur distant peut recevoir l'adresse 192.168.0.10.
Pool d'adresses IP	**Add (Ajouter)** une plage d'adresses IP à attribuer aux utilisateurs distants. Une fois le tunnel établi, une interface est créée sur le terminal de l'utilisateur distant avec une adresse de cette plage. Vous pouvez ajouter des adresses IPv4 (comme 192.168.74.0/24 et 192.168.75.1-192.168.75.100) ou des adresses IPv6 (comme 2001:aa::1-2001:aa::10).  *pour éviter les conflits, le pool d'adresses IP doit être suffisamment important pour prendre en charge toutes les connexions simultanées. La passerelle gère un index de clients et d'adresses IP de sorte que le client reçoive automatiquement la même adresse IP lors de sa connexion suivante. La configuration de plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux clients une adresse IP non conflictuelle avec les autres interfaces du client.* Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple,

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	pour le réseau 192.168.0.0/16, un utilisateur distant peut se voir attribuer l'adresse 192.168.0.10.
Onglet Segmentation du tunnel	
Onglet Itinéraires d'accès	
Aucun accès direct au réseau local	Sélectionnez cette option pour désactiver la segmentation des tunnels, notamment l'accès direct aux réseaux locaux sur les terminaux Windows et MacOS. Cette fonction empêche les utilisateurs d'envoyer du trafic à des proxys ou des ressources locales, une imprimante à domicile par exemple. Lorsque le tunnel est établi, l'ensemble du trafic est acheminé via le tunnel et la mise en œuvre des politiques par le pare-feu s'applique à celui-ci.
Inclure	Veuillez **Ajouter** les itinéraires à inclure dans le tunnel VPN. Ce sont les itinéraires que la passerelle applique au point de terminaison des utilisateurs distants pour préciser les points de terminaison d'utilisateur qui peuvent être envoyés au moyen de la connexion VPN. *Pour inclure tous les sous-réseaux de destination ou les objets d'adresses, Include (Incluez) 0.0.0.0/0 et ::/0 comme itinéraires d'accès.*
Exclure	Veuillez **Ajouter** des itinéraires à exclure du tunnel VPN. Ces itinéraires sont envoyés aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel). Vous pouvez définir les itinéraires que vous envoyez au moyen du tunnel VPN comme des itinéraires que vous incluez dans le tunnel, les itinéraires que vous excluez du tunnel ou une combinaison des deux. Par exemple, vous pouvez paramétrer une segmentation des tunnels pour permettre aux utilisateurs distants d'accéder à Internet sans recourir au tunnel VPN. Les itinéraires exclus doivent être plus spécifiques que les itinéraires inclus pour éviter d'exclure plus de trafic que ce que vous en avez l'intention. Si vous n'incluez ou n'excluez pas d'itinéraires, chaque demande est acheminée à travers le tunnel (pas de segmentation des tunnels). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut permettre d'empêcher un tiers externe d'accéder aux terminaux de l'utilisateur et ainsi accéder au réseau interne (le terminal de l'utilisateur servant alors de pont).
Onglet Domaine et Application	

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Inclure le Domaine	Ajoutez le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez inclure dans le tunnel VPN à l'aide du domaine et du port (facultatif). Ce sont les applications que la passerelle applique au point de terminaison des utilisateurs distants pour préciser les points de terminaison d'utilisateur qui peuvent être envoyés au moyen de la connexion VPN.  *Vous pouvez configurer une liste de ports pour chaque domaine. Si aucun port n'est configuré, tous les ports du domaine spécifié sont assujettis à cette politique.*
Exclure un Domaine	Ajoutez le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez exclure du tunnel VPN à l'aide du domaine et du port (facultatif). Ces applications sont envoyées aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel).  *Vous pouvez configurer une liste de ports pour chaque domaine. Si aucun port n'est configuré, tous les ports du domaine spécifié sont assujettis à cette politique.* Si vous n'incluez ou n'excluez pas de domaines, chaque demande est acheminée à travers le tunnel (pas de segmentation des tunnels). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d'accéder aux points de terminaison utilisateur dans le but d'obtenir l'accès au réseau interne.
Inclure le Nom de processus de l'application client	Ajoutez le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez inclure dans le tunnel VPN à l'aide du nom du processus de l'application. Ce sont les applications que la passerelle applique aux points de terminaison des utilisateurs distants pour préciser ce que ces points de terminaison d'utilisateur peuvent être envoyés au moyen de la connexion VPN.
Exclure le Nom de processus de l'application client	Ajoutez le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez exclure du tunnel VPN à l'aide du nom du processus de l'application. Ces applications sont envoyées aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel). Si vous n'incluez ou n'excluez pas d'applications, chaque demande est acheminée à travers le tunnel (pas de segmentation des tunnels). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d'accéder aux

© 2020 Palo Alto Networks, Inc.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	points de terminaison utilisateur dans le but d'obtenir l'accès au réseau interne.
Onglet Services du réseau	
Serveur DNS	Précisez l'adresse IP du serveur DNS auquel l'application GlobalProtect disposant de cette configuration de paramètres du client envoie des requêtes DNS. Vous pouvez ajouter plusieurs serveurs DNS en séparant chaque adresse IP avec une virgule.
Suffixe DNS	Spécifiez le suffixe DNS que le point de terminaison doit utiliser localement lorsqu'un nom d'hôte non qualifié que le point de terminaison ne peut pas résoudre est saisi. Vous pouvez saisir plusieurs suffixes DNS (maximum de 100) en séparant chaque suffixe par une virgule.

Onglet Pools d'adresses IP du client

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Client IP Pool (Pool d'adresses IP du client)**

Sélectionnez l'onglet **Client IP Pool (Pool d'adresses IP du client)** pour configurer le pool d'adresses IP globales qui est utilisé pour affecter les adresses IPv4 ou IPv6 à tous les points de terminaison qui se connectent à la passerelle GlobalProtect™.

Paramètres de configuration du pool d'adresses IP du client de la passerelle GlobalProtect	Description
Pool d'adresses IP	**Add (Ajouter)** une plage d'adresses IPv4 ou IPv6 à attribuer aux utilisateurs distants. Après avoir établi le tunnel, la passerelle GlobalProtect attribue les adresses IP de cette plage à toutes les terminaisons qui se connectent via ce tunnel. *Si vous configurez des pools d'adresses IP au niveau de la passerelle (Network (Réseau) > GlobalProtect (GlobalProtect) > Gateways (Passerelles) > <gateway-config> (configuration de la passerelle) > GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect) > Agent (Agent) > Client IP Pool (Pool d'adresses IP du client)), ne configurez pas de pools d'adresses IP au niveau du client (Network (Réseau) > GlobalProtect (GlobalProtect) >*

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du pool d'adresses IP du client de la passerelle GlobalProtect	Description
	Gateways (Passerelles) > <gateway-config> (configuration-passerelle) > GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect) > Agent (Agent) > Client Settings (Paramètres du client) > <client-setting> (<passerelle-client>) > Configs (Configurations) > IP Pools (Pool d'adresses IP)).

Onglet Services du réseau

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Network Services (Services du réseau)**

Sélectionnez l'onglet **Network Services (Services du réseau)** pour configurer les paramètres DNS qui sont affectés à la carte réseau virtuelle sur le point de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

*Les options Services réseau sont disponibles uniquement si vous avez activé le mode tunnel et défini une interface de tunnel dans l'*onglet Paramètres de tunnel.

Paramètres de configuration des services réseau du client GlobalProtect	Description
Source de l'héritage	Sélectionnez une source pour la propagation du serveur DNS et d'autres paramètres entre le client DHCP ou l'interface client PPPoE sélectionné et la configuration des applications GlobalProtect. Grâce à ce paramètre, l'ensemble des configurations du réseau client, les serveurs DNS et WINS par exemple, est hérité de la configuration de l'interface sélectionnée dans Source de l'héritage.
Vérifier l'état de la source de l'héritage	Cliquez sur Source de l'héritage pour consulter les paramètres du serveur actuellement attribués aux interfaces client.
DNS principal DNS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service DNS aux clients.
WINS principal WINS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service Windows Internet Name Service (Service d'attribution de nom Internet Windows ; WINS) aux points de terminaison.
Hériter des suffixes DNS	Sélectionnez cette option pour hériter des suffixes DNS de la source de l'héritage.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration des services réseau du client GlobalProtect	Description
Suffixe DNS	**Add (Ajouter)** un suffixe que le point de terminaison doit utiliser localement lorsqu'un nom d'hôte non qualifié, qu'il ne peut pas résoudre, est saisi. Vous pouvez saisir plusieurs suffixes (maximum de 100) en les séparant chaque suffixe par une virgule.

Onglet Paramètres de connexion

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Connection Settings (Paramètres de connexion)**

Sélectionnez l'onglet **Connection Settings (Paramètres de connexion)** pour définir les paramètres des délais d'expiration et les restrictions d'utilisation de l'authentification par cookie pour l'application GlobalProtect™.

Paramètres de connexion du mode tunnel du client GlobalProtect	Description
Configuration du délai avant expiration	
Durée de vie de la connexion	Indiquez le nombre de jours, heures ou minutes autorisés pour une session de connexion de passerelle.
Déconnexion en cas d'inactivité	Indiquez le nombre de jours, heures ou minutes après lesquels une session inactive est déconnectée automatiquement.
Déconnecter en cas d'Inactivité	Précisez la durée de temps (en minutes) qui passe avant la déconnexion d'un point de terminaison de l'application GlobalProtect après que l'application arrête le trafic de routage via le tunnel VPN.
Restrictions d'utilisation de l'authentification par cookie	
Désactivez le rétablissement automatique de SSL VPN	Activez cette option pour empêcher le rétablissement automatique des tunnels SSL VPN. *Si vous activez cette option, GlobalProtect ne prendra pas en charge le VPN résilient.*
Restreindre l'utilisation de l'authentification par cookie (pour la restauration automatique du tunnel VPN ou le contrôle prioritaire de l'authentification) afin de	Activer cette option pour restreindre l'utilisation des cookies à des fins d'authentification selon l'une des conditions suivantes : • **L'adresse IP source d'origine pour laquelle le cookie d'authentification a été émis** : restreint l'utilisation des cookies à des fins d'authentification à des points de terminaison ayant la même adresse IP source publique que le point de terminaison pour lequel le cookie a été initialement émis. • **La plage réseau de l'adresse IP source d'origine** : restreint l'utilisation des cookies à des fins d'authentification à des points de terminaison ayant les mêmes adresses IP source publiques au sein de la plage

© 2020 Palo Alto Networks, Inc.

Paramètres de connexion du mode tunnel du client GlobalProtect	Description
	d'adresses IP réseau désignée. Saisissez un **Source IPv4 Netmask (Masque réseau IPv4 source)** pour spécifier une plage d'adresses IPv4 ou saisissez un **Source IPv6 Netmask (Masque réseau IPv6 source)** pour spécifier une plage d'adresses IPv6. Si vous définissez l'un de ces masques réseau sur `0`, cette option est désactivée pour le type d'adresse IP spécifié. Par exemple,vous pouvez définir un masque réseau sur `0` si votre portail ou votre passerelle ne prend en charge qu'un seul type d'adresses IP (IPv4 ou IPv6) ou si vous souhaitez activer cette option pour un seul type d'adresses IP (lorsque votre portail ou votre passerelle prend en charge IPv4 et IPv6). Vous ne pouvez définir qu'un seul masque réseau sur `0` dans une configuration de passerelle donnée ; vous ne pouvez définir simultanément les deux masques réseau sur `0`. Si vous acceptez la valeur de **Source IPv4 Netmask (Masque réseau IPv4 source)** par défaut, soit `32`, l'utilisation des cookies d'authentification est limitée à la même adresse IPv4 publique du point de terminaison auquel le cookie a initialement été émis. Si vous acceptez la valeur de **Source IPv6 Netmask (Masque réseau IPv6 source)** par défaut, soit `128`, l'utilisation des cookies d'authentification est limitée à la même adresse IPv6 publique du point de terminaison auquel le cookie a initialement été émis.

Onglet Trafic vidéo

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **Video Traffic (Trafic vidéo)**

Sélectionnez l'onglet **Video Traffic** (Trafic vidéo) pour exclure le trafic de diffusion vidéo du tunnel VPN.

Paramètres de configuration du trafic vidéo de la passerelle GlobalProtect	Description
Exclure les applications vidéo du tunnel	Sélectionnez cette option pour autoriser l'exclusion du trafic de diffusion vidéo du tunnel VPN.
Applications	**Add (Ajoutez)** les applications de diffusion vidéo que vous souhaitez exclure du tunnel VPN ou **Browse (Recherchez)**-les. La redirection vidéo s'applique à tout type de trafic vidéo provenant des applications suivantes : • YouTube • Dailymotion • Netflix Pour les autres applications de diffusion vidéo, seuls les types de vidéo suivants peuvent être redirigés :

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration du trafic vidéo de la passerelle GlobalProtect	Description
	• MP4 • WebM • MPEG Le trafic de diffusion vidéo peut uniquement être exclu du tunnel VPN. Si vous n'excluez aucune application de diffusion vidéo, toutes les requêtes sont acheminées à travers le tunnel (pas de segmentation des tunnels). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d'accéder aux points de terminaison utilisateur dans le but d'obtenir l'accès au réseau interne.

Onglet Notification HIP

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Agent** > *<agent-config> (<configuration de l'agent)>)* > **HIP Notification (Notification HIP)**

Sélectionnez l'onglet **HIP Notification (Notification HIP)** pour définir les messages de notification à afficher aux utilisateurs finaux lorsqu'une règle de sécurité dotée d'un profil HIP est mise en œuvre.

Ces options ne sont disponibles que si vous avez créé des profils HIP et les avez ajoutés à vos politiques de sécurité.

Paramètres de configuration de notification HIP de l'agent GlobalProtect	Description
Notification HIP	**Ajouter** des notifications HIP et configurer les options. Vous pouvez **Activer** les notifications pour **Mettre le message en correspondance**, **Ne pas mettre le message en correspondance**, ou les deux puis décider de **Montrer la notification en tant qu'infobulle de la barre des tâches** ou **Message contextuel**. Indiquez ensuite le message pour correspondre ou ne pas correspondre. Utilisez ces paramètres pour informer l'utilisateur final de l'état de la machine, par exemple, pour fournir un message d'avertissement indiquant que le système hôte ne dispose pas d'une application requise. Pour Mettre le message en correspondance, vous pouvez également activer l'option **Include Mobile App List (Inclure la liste des applications mobiles)** pour indiquer les applications qui ont déclenché la correspondance HIP. *Vous pouvez formater les messages de notification HIP en HTML enrichi qui peut inclure des liens vers des sites Web externes et des ressources. Utilisez l'hyperlien ( ) dans la barre d'outils des paramètres de texte enrichi pour ajouter des liens.*

© 2020 Palo Alto Networks, Inc.

Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect)

- **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (configuration de la passerelle)* > **Satellite**

Un périphérique satellite est un pare-feu Palo Alto Networks, généralement dans une succursale, qui agit en tant qu'application de GlobalProtect pour lui permettre d'établir une connectivité VPN avec une passerelle GlobalProtect. Sélectionnez l'onglet **Satellite** pour définir les paramètres réseau et de tunnel de la passerelle pour que les satellites puissent établir des connexions VPN. Vous pouvez également configurer les itinéraires annoncés par les satellites.

- Onglet Paramètres du tunnel
- Onglet Paramètres du réseau
- Onglet Filtre itinéraire

Paramètres de configuration satellite GlobalProtect	Description
Onglet Paramètres du tunnel	
Configuration des tunnels	Sélectionnez **Tunnel Configuration (Configuration tunnel)** et sélectionnez une **Tunnel Interface (Interface tunnel)** existante, ou sélectionnez **New Tunnel Interface (Nouvelle interface tunnel)** à partir du menu déroulant. Voir **Réseau > Interfaces > Tunnel** pour plus d'informations. • **Replay attack detection (Détection des attaques par relecture)** – Protégez-vous contre les attaques par relecture. *Activez Replay attack detection (Détection des attaques par relecture) pour protéger les satellites GlobalProtect des attaques par relecture si vous activez la configuration des tunnels des satellites.* • **Copy TOS (Copier ToS)** – Copiez l'en-tête ToS (Type of Service) de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés pour préserver les informations ToS d'origine. • **Configuration refresh interval (hours) (Intervalle d'actualisation de la configuration (heures))** – Spécifiez la fréquence à laquelle les satellites devraient rechercher des mises à jour de la configuration sur le portail (par défaut 2, plage de 1 à 48).
Surveillance du tunnel	Cochez la case **Tunnel Monitoring (Surveillance du tunnel)** pour permettre aux satellites de surveiller les connexions de tunnel de passerelle, leur permettant ainsi de basculer vers une passerelle de secours en cas d'échec de connexion. • **Destination Address (Adresse de destination)** – Indiquez une adresse **IPv4** ou **IPv6** que la surveillance du tunnel utilisera pour déterminer si la connexion à la passerelle a été établie (par exemple, une adresse IP sur le réseau protégé par la passerelle). Si vous avez configuré une adresse IP pour l'interface de tunnel, vous pouvez également ne pas renseigner ce champ. La surveillance des tunnels utilisera alors l'interface de tunnel pour déterminer si la connexion est active.

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration satellite GlobalProtect	Description
	• **Tunnel Monitor Profile (Profil de surveillance du tunnel)** – Le **Failover (Basculement)** vers une autre passerelle est le seul type de surveillance du tunnel pris en charge avec le LSVPN. *Activez la Tunnel Monitoring (Surveillance des tunnels) et configurez un profil de surveillance des tunnels pour contrôler l'action de basculement si vous activez la configuration des tunnels des satellites.*
Profils crypto	Sélectionnez un **IPSec Crypto Profile (Profil crypto IPSec)** ou en créer un nouveau. Un chiffrement détermine les protocoles et algorithmes d'identification, d'authentification et de cryptage des tunnels VPN. Les deux extrémités du tunnel d'un LSVPN étant des pare-feu approuvés au sein de votre entreprise, vous utilisez généralement le profil par défaut qui utilise le protocole ESP, DH groupe 2, le cryptage AES 128 CVC et l'authentification SHA-1. Voir Réseau > Profils réseau > Crypto IPSec GlobalProtect pour plus de détails.
Onglet Paramètres du réseau	
Source de l'héritage	Sélectionnez une source pour la propagation du serveur DNS et d'autres paramètres entre le client DHCP ou l'interface client PPPoE sélectionné et la configuration du satellite GlobalProtect. Grâce à ce paramètre, l'ensemble de la configuration, les serveurs DNS par exemple, est héritée de la configuration de l'interface sélectionnée dans Source de l'héritage.
DNS principal DNS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service DNS aux satellites.
Suffixe DNS	Cliquez sur **Add (Ajouter)** pour saisir un suffixe que le satellite doit utiliser localement lorsqu'un nom d'hôte non qualifié qu'il ne peut pas résoudre est saisi. Vous pouvez saisir plusieurs suffixes en les séparant par des virgules.
Hériter du suffixe DNS	Sélectionnez cette option pour envoyer le suffixe DNS aux satellites à utiliser localement lorsqu'un nom d'hôte non qualifié qu'ils ne peuvent pas résoudre est saisi.
Pool d'adresses IP	**Add (Ajouter)** une plage d'adresses IP à attribuer à l'interface de tunnel sur les satellites lors de l'établissement du tunnel VPN. Vous pouvez spécifier les adresses IPv6 ou IPv4. *le pool d'adresses IP doit être suffisamment important pour prendre en charge toutes les connexions simultanées. L'attribution d'adresse IP est dynamique et ne s'applique plus une fois le satellite déconnecté. La configuration de plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux satellites une adresse IP non conflictuelle avec les autres interfaces des satellites.*

© 2020 Palo Alto Networks, Inc.

Paramètres de configuration satellite GlobalProtect	Description
	Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple, pour le réseau 192.168.0.0/16, un satellite peut se voir attribuer l'adresse 192.168.0.10. Si vous utilisez un routage dynamique, assurez-vous que le pool d'adresses IP que vous désignez pour les satellites ne chevauche pas les adresses IP que vous avez attribuées manuellement aux interfaces de tunnel sur vos passerelles et satellites.
Accéder à l'itinéraire	Cliquez sur **Add (Ajouter)**, puis saisissez les itinéraires comme suit : • Si vous souhaitez acheminer l'ensemble du trafic provenant des satellites via le tunnel, ne renseignez pas ce champ. • Pour n'acheminer qu'un trafic donné via la passerelle (split tunneling), spécifiez les sous-réseaux de destination qui doivent être tunnellisés. Dans ce cas, le satellite acheminera le trafic non destiné à un itinéraire d'accès spécifié selon sa propre table de routage. Par exemple, vous pouvez choisir de ne tunnelliser que le trafic destiné à votre réseau d'entreprise et d'utiliser le satellite local pour autoriser l'accès à Internet en toute sécurité. • Si vous souhaitez autoriser le routage entre des satellites, saisissez l'itinéraire récapitulatif du réseau protégé par chaque satellite.
Onglet Filtre itinéraire	
Accepter les itinéraires publiés	Activez l'option **Accept published routes (Accepter les itinéraires publiés)** pour accepter les itinéraires conseillés par le satellite dans la table de routage de la passerelle. Si vous ne sélectionnez pas cette option, la passerelle n'acceptera aucun itinéraire publié par les satellites.
Sous-réseaux autorisés	Si vous souhaitez limiter davantage les itinéraires acceptés, **Add (Ajouter)** Sous-réseaux autorisés et définissez les sous-réseaux pour lesquels la passerelle doit accepter les itinéraires ; les sous-réseaux publiés par les satellites qui ne font pas partie de la liste sont alors filtrés. Par exemple, si tous les satellites sont configurés avec le sous-réseau 192.168.x.0/24 côté LAN, vous pouvez configurer un itinéraire autorisé de 192.168.0.0/16 sur la passerelle. Cette configuration fera en sorte que la passerelle n'accepte que les itinéraires du satellite uniquement s'ils se trouvent sur le sous-réseau 192.168.0.0/16.

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Gestionnaire de périphériques mobiles

Si vous utilisez un gestionnaire de sécurité mobile pour gérer les points de terminaison mobiles des utilisateurs finaux et que vous avez activé l'option de mise en œuvre des politiques HIP, vous devez configurer la passerelle pour communiquer avec le gestionnaire de sécurité mobile et récupérer les rapports HIP pour les points de terminaison gérés.

Il est nécessaire d'**Ajouter** des informations MDM pour le Gestionnaire de sécurité mobile pour permettre à la passerelle de communiquer avec le Gestionnaire de sécurité mobile.

Paramètres du gestionnaire de périphériques mobiles de GlobalProtect	Description
Name (Nom)	Donnez un nom au gestionnaire de sécurité mobile (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
	Si le pare-feu est en mode Plusieurs systèmes virtuels, les paramètres MDM affichent le système virtuel (vsys) sur lequel le gestionnaire de sécurité mobile est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'apparaît pas dans la boîte de dialogue MDM. Après avoir enregistré le gestionnaire de sécurité mobile, vous ne pouvez plus changer son emplacement.
Paramètres de connexion	
Serveur	Saisissez l'adresse IP ou le nom de domaine complet de l'interface sur le gestionnaire de sécurité mobile où la passerelle se connecte pour récupérer les rapports HIP. Assurez-vous de disposer d'un itinéraire de service sur cette interface.
Port de connexion	Le port de connexion est l'endroit où le gestionnaire de sécurité mobile écoute les demandes de rapports de HIP. Par défaut, le port d'écoute du gestionnaire de sécurité mobile de GlobalProtect est 5008. Si vous utilisez un gestionnaire de sécurité mobile tiers, saisissez le numéro de port d'écoute du serveur pour les demandes de rapports HIP.
Certificat du client	Choisissez le certificat client de la passerelle à présenter au gestionnaire de sécurité mobile, lors de l'établissement d'une connexion HTTPS. Ce certificat est requis uniquement si le gestionnaire de sécurité mobile est configuré pour utiliser l'authentification mutuelle.
CA racine approuvée	Cliquez sur **Add (Ajouter)** et sélectionnez le certificat AC de la racine utilisé pour générer le certificat pour l'interface sur laquelle la passerelle se connectera pour récupérer les rapports HIP. (Ce certificat de serveur peut être différent du certificat délivré pour l'interface d'enregistrement du point

© 2020 Palo Alto Networks, Inc.

Paramètres du gestionnaire de périphériques mobiles de GlobalProtect	Description
	de terminaison sur le gestionnaire de sécurité mobile). Vous devez importer le certificat AC racine et l'ajouter à cette liste.

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Liste de blocage de périphériques

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Device Block List (Liste de blocage de périphériques)** (pare-feu uniquement) pour ajouter des points de terminaison à la liste d'interdictions de périphériques de GlobalProtect. Les points de terminaison de cette liste ne sont pas autorisés à établir une connexion VPN GlobalProtect.

Paramètres de la liste d'interdictions de périphériques	Description
Name (Nom)	Donnez un nom à la liste de blocage des périphériques (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.
ID d'hôte	Entrez l'ID unique qui identifie le point de terminaison, une combinaison du nom d'hôte et de l'ID de périphérique unique. Pour chaque ID d'hôte, indiquez le nom d'hôte correspondant.
Nom d'hôte	Donnez un nom de domaine pour identifier le périphérique (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Applications sans client

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless Apps (Applications sans client)** pour ajouter des applications accessibles au moyen du VPN sans le client GlobalProtect. Vous pouvez ajouter des applications sans client individuelles, puis sélectionner **Network (Réseau)** > **GlobalProtect** > **Clientless App Groups (Groupes d'applications sans client)** pour définir les groupes d'applications.

VPN sans client GlobalProtect fournit un accès à distance sécurisé aux applications Web d'entreprise courantes qui utilisent les technologies HTML, HTML5 et JavaScript. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel GlobalProtect. Ceci est utile lorsque vous devez activer l'accès partenaire ou fournisseur aux applications et activer de manière sécurisée les actifs non gérés, y compris les périphériques personnels.

Vous avez besoin des mises à jour dynamiques de **GlobalProtect Clientless VPN (VPN sans client GlobalProtect)** pour utiliser cette fonctionnalité. Cette fonctionnalité requiert également l'installation d'un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client du portail GlobalProtect.

Paramètres des applications sans client	Description
Name (Nom)	Saisissez un nom qui décrit l'application (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.
URL d'accueil de l'application	Saisissez l'URL à laquelle se trouve l'application (jusqu'à 4 095 caractères).
Description de l'application	(Optionnel) Saisissez une description pour l'application (255 caractères maximum). Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Icône de l'application	(Facultatif) Téléchargez une icône pour identifier l'application sur la page d'application publiée. Vous pouvez parcourir pour télécharger l'icône.

© 2020 Palo Alto Networks, Inc.

Réseau > GlobalProtect > Groupes d’applications sans client

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless App Groups (Groupes d’applications sans client)** pour regrouper des applications accessibles au moyen du VPN sans client GlobalProtect. Vous pouvez ajouter des applications sans client existantes à un groupe ou configurer de nouvelles applications sans client pour le groupe. Les groupes sont utiles pour travailler avec plusieurs applications simultanément. Par exemple, vous pouvez avoir un ensemble standard d’applications SaaS (comme Workday, JIRA ou Bugzilla) que vous souhaitez configurer pour l’accès VPN sans client.

Paramètres des groupes d’applications sans clients	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d’applications (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d’union et traits de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.
Applications	Vous devez **Ajouter** une **Application** à partir du menu déroulant ou configurer une nouvelle application sans client et l’ajouter au groupe. Pour configurer une nouvelle application sans client, reportez-vous à Réseau > GlobalProtect > Clientless Applications .

© 2020 Palo Alto Networks, Inc.

Objets > GlobalProtect > Objets HIP

Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** pour définir des objets pour un profil d'information sur l'hôte (HIP). Les objets HIP fournissent les critères de correspondance pour filtrer les données brutes rapportées par une application que vous souhaitez utiliser pour appliquer la politique. Par exemple, si les données brutes de l'hôte comprennent des informations sur plusieurs packages antivirus sur une terminaison, vous pourriez être intéressé par une application particulière parce que votre organisation l'exige. Pour ce scénario, vous créez un objet HIP pour correspondre à l'application spécifique que vous souhaitez appliquer.

Pour définir les objets HIP dont vous avez besoin, vous devez déterminer comment vous allez utiliser les informations sur l'hôte collectées pour mettre en œuvre la politique. N'oubliez pas que les objets HIP forment simplement des blocs qui vous permettent de créer les profils HIP utilisés dans les politiques de sécurité que vous pouvez utiliser. Par conséquent, vous voudrez peut-être garder vos objets simples, en fonction d'une chose, comme la présence d'un type particulier de logiciel requis, l'appartenance à un domaine spécifique ou la présence d'un OS de terminaison spécifique. Avez cette approche, vous pouvez créer une politique HIP très granulaire.

Pour créer un objet HIP, cliquez sur **Add (Ajouter)** ; la boîte de dialogue Objet HIP s'affiche alors. Pour obtenir une description de chaque champ, reportez-vous aux tableaux suivants.

- Onglet Général des objets HIP
- Onglet Périphérique mobile des objets HIP
- Onglet Gestion des correctifs des objets HIP
- Onglet Pare-feu des objets HIP
- Onglet Anti-logiciels malveillants des objets HIP
- Onglet Sauvegarde du disque des objets HIP
- Onglet Cryptage du disque des objets HIP
- Onglet Prévention des pertes de données des objets HIP
- Onglet HIP Objects Certificate (Certificat d'objets HIP)
- Onglet Vérifications personnalisées des objets HIP

Pour plus d'informations sur la création de politiques de sécurité HIP, reportez-vous à la section Configuration de la mise en œuvre d'une politique HIP du *Guide de l'administrateur de GlobalProtect*.

Onglet Général des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **General (Général)**

Sélectionnez l'onglet **General (Général)** pour donner un nom au nouvel objet HIP et configurer l'objet pour correspondre aux informations générales sur l'hôte, telles que le domaine, le système d'exploitation ou le type de connectivité réseau de l'hôte.

Paramètres généraux d'un objet HIP	Description
Name (Nom)	Donnez un nom à l'objet HIP (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé	Si vous sélectionnez **Shared (Partagé)**, les objets HIP actuels deviennent disponibles à :

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'un objet HIP	Description
	Chaque système virtuel (vsys) sur le pare-feu, si vous êtes connecté à un pare-feu en mode Plusieurs systèmes virtuels. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le système virtuel sélectionné **Virtual System (Système virtuel)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'est pas disponible dans la boîte de dialogue Objet HIP. Tous les groupes de périphériques sur Panorama™. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le groupe de périphériques sélectionné dans **Device Group (Groupe de périphériques)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Après avoir enregistré l'objet, vous ne pouvez plus changer son paramètre **Shared (Partagé)**. Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** pour connaître le **Location (Emplacement)** actuel.
Description	(Facultatif) Saisissez une description.
Infos sur l'hôte	Sélectionnez cette option pour activer les options pour configurer les informations d'hôte.
Géré	Filtrez selon que le point de terminaison est géré ou non géré. Pour la mise en correspondance avec les points de terminaison gérés, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les points de terminaison non gérés, sélectionnez **No (Non)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Contrôle l'accès forcé à l'objet HIP dans des groupes de périphériques descendants du **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**. Sélectionnez cette option pour empêcher les administrateurs de créer des copies locales de l'objet dans les groupes de périphériques descendants en appliquant un contrôle prioritaire sur ses valeurs héritées. Cette option est désactivée par défaut (le contrôle prioritaire est activé).
Domain (Domaine)	Pour la mise en correspondance avec un nom de domaine, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Système d'exploitation	Pour la mise en correspondance avec un système d'exploitation hôte, choisissez **Contains (Contient)** dans la première liste déroulante, sélectionnez un fournisseur dans la seconde, puis une version de système d'exploitation dans la troisième, ou vous pouvez sélectionner **All (Tout)** pour la mise en correspondance avec n'importe quelle version du fournisseur sélectionné.
Version du client	Pour la mise en correspondance avec un numéro de version spécifique, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne à mettre en correspondance ou non dans la zone de texte.
Nom de l'hôte	Pour la mise en correspondance avec nom d'hôte spécifique, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne de à mettre en correspondance ou non, selon l'opérateur sélectionné) dans la zone de texte.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux d'un objet HIP	Description
ID d'hôte	L'ID hôte est un ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur d'ID hôte varie selon le type de périphérique : • **Windows** – GUID machine stocké dans le registre Windows (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS** – Adresse MAC de la première interface de réseau physique intégrée • **Android** – ID Android • **iOS** – UDID • **Linux** – Product UUID extrait du tableau du système DMI • **Chrome** – La chaîne alphanumérique unique d'une longueur de 32 caractères affectée par GlobalProtect. Pour la mise en correspondance avec un nom d'hôte spécifique, sélectionnez l'opérateur dans la liste déroulante, puis saisissez une chaîne à mettre en correspondance (ou non, selon l'opérateur sélectionné) dans la zone de texte.
Numéro de série	Pour la mise en correspondance avec la totalité ou une partie du numéro de série d'un périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Réseau	Ce champ vous permet de filtrer une configuration réseau de périphérique mobile spécifique. Ce critère de correspondance s'applique uniquement aux périphériques mobiles. Sélectionnez un opérateur dans la première liste déroulante, puis le type de connexion réseau à filtrer dans la seconde : **Wi-Fi**, **Mobile**, **Ethernet** (disponible uniquement pour les filtres **Is Not (N'est pas)**) ou **Unknown (Inconnu)**. Une fois le type de réseau sélectionné, saisissez toute chaîne supplémentaire à mettre en correspondance, le cas échéant, notamment l'**Carrier (Opérateur)** mobile ou le **SSID** Wi-Fi.

Onglet Périphérique mobile des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Mobile Device (Périphérique mobile)**

Sélectionnez l'onglet **Mobile Devise (Périphérique mobile)** pour activer la correspondance HIP en fonction des données collectées à partir des périphériques mobiles exécutant l'application GlobalProtect.



Pour recueillir les attributs des périphériques mobiles et les utiliser dans les politiques de mise en œuvre HIP, GlobalProtect a besoin d'un serveur MDM. À l'heure actuelle, GlobalProtect prend en charge l'intégration HIP via le serveur MDM AirWatch.

Paramètres de périphérique mobile d'un objet HIP	Description
Périphérique mobile	Sélectionnez cette option pour activer le filtrage sur les données d'accueil collectées à partir d'appareils mobiles qui exécutent l'application

© 2020 Palo Alto Networks, Inc.

Paramètres de périphérique mobile d'un objet HIP	Description
	GlobalProtect et pour activer les onglets Périphérique, Paramètres et Applications.
onglet Périphérique	• **Model (Modèle)** : pour la mise en correspondance avec un modèle de périphérique spécifique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance. • **Tag (Étiquette)** : pour la mise en correspondance avec une valeur d'étiquette définie sur le gestionnaire de sécurité mobile de GlobalProtect, choisissez un opérateur dans la première liste déroulante, puis une étiquette dans la seconde. • **Phone Number (Numéro de téléphone)** : pour la mise en correspondance avec tout ou partie d'un numéro de téléphone de périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance. • **IMEI** : pour la mise en correspondance avec tout ou partie d'un numéro IMEI (International Mobile Equipment Identity) de périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Onglet Paramètres	• **Code secret** : filtre basé sur la définition ou non d'un code secret pour le périphérique. Pour la mise en correspondance avec les périphériques pour lesquels un code secret a été défini, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les périphériques pour lesquels aucun code secret n'a été défini, sélectionnez Non. • **Rooted/Jailbroken (Déverrouillé/Débridé)** : filtre basé sur le déverrouillage/débridage ou non du périphérique. Pour la mise en correspondance avec les périphériques déverrouillés ou débridés, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les périphériques non déverrouillés/débridés, sélectionnez **No (Non)**. • **Disk Encryption (Cryptage du disque)** : filtre basé sur le cryptage ou non des données du périphérique. Pour la mise en correspondance avec les périphériques pour lesquels le cryptage du disque est activé, sélectionnez Oui. Pour la mise en correspondance avec les périphériques pour lesquels le cryptage du disque est désactivé, sélectionnez Non. • **Time Since Last Check-in (Temps écoulé depuis le dernier enregistrement)** : filtre basé sur le dernier enregistrement du périphérique auprès du gestionnaire de périphériques mobiles. Sélectionnez un opérateur dans la liste déroulante, puis définissez le nombre de jours depuis le dernier enregistrement. Par exemple, vous pouvez définir un objet correspondant aux périphériques qui n'ont pas été enregistrés au cours des 5 derniers jours.
Onglet Applications	• **Apps (Applications)** : (Périphériques Android uniquement) : Sélectionnez cette option pour activer le filtrage en fonction des applications installées sur le périphérique et de la présence ou non d'applications infectées par des logiciels malveillants. • Onglet **Criteria (Critères)** • **Has Malware (Présente des logiciels malveillants)** – Sélectionnez **Yes (Oui)** pour relier les périphériques qui comportent des applications où

© 2020 Palo Alto Networks, Inc.

Paramètres de périphérique mobile d'un objet HIP	Description
	des logiciels malveillants sont installés. Sélectionnez **No (Non)** pour relier les périphériques qui ne comportent pas d'applications où des logiciels malveillants sont installés. Sélectionnez **None (Aucun)** pour ne pas utiliser **Has Malware (Présente des logiciels malveillants)** en tant que critère de correspondance. • Onglet **Include (Inclure)** • **Package (Paquet)** – Pour relier les appareils qui ont des applications spécifiques installées, vous devez **Add (Ajouter)** une application et saisir le nom de l'application unique au format DNS inversé. Par exemple, com.netflix.mediaclient, puis saisissez ensuite le **Hash (Hachage)** correspondant à l'application, que l'application GlobalProtect calcule et soumet avec le rapport HIP de l'appareil.

Onglet Gestion des correctifs des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Patch Management (Gestion des correctifs)**

Sélectionnez l'onglet **Patch Management (Gestion des correctifs)** pour activer la correspondance HIP en fonction de l'état des correctifs des points de terminaison GlobalProtect.

Paramètres de gestion des correctifs d'un objet HIP	Description
Gestion des correctifs	Sélectionnez cette option pour activer la correspondance sur l'état de la gestion des correctifs de l'hôte et activer les onglets Critères et Fournisseur.
Onglet Critères	Définissez les paramètres suivants : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de gestion des correctifs sur l'hôte. • **Is Enabled (Est activé)** : mise en correspondance en fonction de l'activation ou non du logiciel de gestion des correctifs sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié. • **Severity (Gravité)** : sélectionnez à partir de la liste des opérateurs logiques pour faire correspondre si l'hôte a des correctifs manquants du niveau de gravité spécifié. Servez-vous des mappages suivants entre les valeurs de gravité GlobalProtect et les cotes de gravité d'OPSWAT pour comprendre la signification de chacune des valeurs : • **0** : Faible • **1** : Modérée • **2** : Importante • **3** : Critique • **Check (Vérification)** : mise en correspondance en fonction de l'absence ou non de correctifs sur l'hôte.

© 2020 Palo Alto Networks, Inc.

Paramètres de gestion des correctifs d'un objet HIP	Description
	• **Patches (Correctifs)** : mise en correspondance en fonction de la présence ou non de correctifs spécifiques sur l'hôte. Cliquez sur **Add (Ajouter)** et saisissez les ID d'article Kerberos pour les correctifs donnés à rechercher. Par exemple, saisissez **3128031** pour rechercher la mise à jour de Microsoft Office 2010 (KB3128031), édition 32 bits.
Onglet du fournisseur	Définir des fournisseurs spécifiques de logiciels et de produits de gestion de correctifs pour rechercher sur le terminal pour trouver une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur Ajouter pour choisir un **Product (Produit)** spécifique. Cliquez sur **OK** pour enregistrer les paramètres.

Onglet Pare-feu des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Firewall (Pare-feu)**

Sélectionnez **Firewall (Pare-feu)** pour activer la correspondance HIP en fonction de l'état du logiciel de pare-feu des points de terminaison GlobalProtect.

Paramètres de pare-feu d'un objet HIP
Sélectionnez **Firewall (Pare-feu)** pour activer la correspondance en fonction du logiciel de pare-feu de l'hôte : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de pare-feu sur l'hôte. • **Is Enabled (Est activé)** : mise en correspondance en fonction de l'activation ou non du logiciel de pare-feu sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié. • **Vendor and Product (Fournisseur et produit)** : définissez des produits et/ou des fournisseurs de logiciels pare-feu spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres. • **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Anti-logiciels malveillants des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Anti-Malware**

Sélectionnez l'onglet **Anti-Malware (Anti-logiciels malveillants)** vous permet d'activer la correspondance HIP en fonction de la couverture antivirus ou antispyware des points de terminaison GlobalProtect.

© 2020 Palo Alto Networks, Inc.

Paramètres anti-logiciels malveillants d'un objet HIP

Sélectionnez **Anti-Malware (Anti-logiciels malveillants)** pour activer la correspondance en fonction de la couverture antispyware ou antivirus de l'hôte. Définissez les critères de correspondance supplémentaire comme suit :

- **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel antispyware ou antivirus sur l'hôte.
- **Real Time Protection (Est activé)** : mise en correspondance en fonction de l'activation ou non de la protection antspyware ou antivirus en temps réel sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **None (Aucun)** et ne peut pas être modifié.
- **Virus Definition Version (Version des définitions de virus)** : met en correspondance en fonction de la mise à jour ou non des définitions de virus dans un nombre de jours spécifié ou une version spécifique.
- **Product Version (Version du produit)** : mise en correspondance avec une version spécifique du logiciel antivirus ou anti-spyware. Pour indiquer une version, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne représentant la version du produit.
- **Last Scan Time (Temps écoulé depuis la dernière analyse)** : mise en correspondance en fonction de la dernière analyse antispyware ou antivirus. Sélectionnez un opérateur dans la liste déroulante, puis spécifiez le nombre de **Days (Jours)** ou **Hours (Heures)** pour la mise en correspondance.
- **Vendor and Product (Fournisseur et produit)** : définissez des produits et/ou des fournisseurs de logiciels antispyware ou antivirus spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres.
- **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Sauvegarde du disque des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Disk Backup (Sauvegarde du disque)**

Sélectionnez l'onglet **Disk Backup (Sauvegarde du disque)** pour activer la correspondance HIP en fonction de l'état de sauvegarde du disque des points de terminaison GlobalProtect.

Paramètres de sauvegarde du disque d'un objet HIP

Sélectionnez **Disk Backup (Sauvegarde de disque)** pour activer la correspondance en fonction de l'état de sauvegarde du disque sur l'hôte, puis définissez les critères de correspondance supplémentaires comme suit :

- **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non de sauvegarde du disque sur l'hôte.
- **Last Backup Time (Temps écoulé depuis la dernière sauvegarde)** : mise en correspondance en fonction de la dernière sauvegarde du disque. Sélectionnez un opérateur dans la liste déroulante, puis spécifiez le nombre de **Days (Jours)** ou **Hours (Heures)** pour la mise en correspondance.
- **Vendor and Product (Fournisseur et produit)** : définissez les fournisseurs et les produits de logiciels de sauvegarde de disque spécifiques à rechercher sur l'hôte. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres.

© 2020 Palo Alto Networks, Inc.

Paramètres de sauvegarde du disque d'un objet HIP
• **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Cryptage du disque des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Disk Encryption (Chiffrement du disque)**

Sélectionnez l'onglet **Disk Encryption (Cryptage du disque)** pour activer la correspondance HIP en fonction de l'état cryptage du disque des points de terminaison GlobalProtect.

Paramètres de cryptage du disque d'un objet HIP	Description
Cryptage du disque	Sélectionnez **Disk Encryption (Cryptage du disque)** pour activer la correspondance en fonction de l'état de cryptage du disque sur l'hôte.
Critères	Définissez les paramètres suivants : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de cryptage du disque sur l'hôte. • **Encrypted Locations (Emplacements cryptés)** : cliquez sur **Add (Ajouter)** pour spécifier le lecteur ou le chemin d'accès où rechercher le cryptage du disque, lors de la détermination d'une correspondance : • **Encrypted Locations (Emplacements cryptés)** : saisissez des emplacements spécifiques sur lesquels rechercher le cryptage sur l'hôte. • **State (État)** : spécifiez la correspondance en fonction de l'état de l'emplacement crypté en choisissant un opérateur dans la liste déroulante, puis en sélectionnant un état possible (**full (total)**, **none (aucun)**, **partial (partiel)**, **not-available (non disponible)**). Cliquez sur **OK** pour enregistrer les paramètres.
Constructeur	Définir les fournisseurs et les produits logiciels de chiffrement de disque spécifiques pour correspondre au terminal. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour sauvegarder les paramètres et revenir à l'onglet **Disk Encryption (Cryptage du disque)**.

Onglet Prévention des pertes de données des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (<objet hip>)* > **Data Loss Prevention (Prévention des pertes de données)**

Sélectionnez l'onglet **Data Loss Prevention (Prévention des pertes de données)** pour configurer la correspondance HIP qui est basée sur si les points de terminaison GlobalProtect exécutent un logiciel de prévention des pertes de données.

© 2020 Palo Alto Networks, Inc.

Paramètres de prévention des pertes de données d'un objet HIP
Sélectionnez **Prévention des pertes de données** pour activer la correspondance en fonction de l'état de prévention des pertes de données (DLP) sur l'hôte (hôtes Windows uniquement), puis définissez les critères de correspondance supplémentaires comme suit : • **Is Installed (Est installé)** – Mise en correspondance en fonction de l'installation ou non du logiciel DLP sur l'hôte. • **Is Enabled (Est activé)** – Mise en correspondance en fonction de l'activation ou non du logiciel DLP sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié. • **Vendor and Product (Fournisseur et produit)** – Définissez des produits et/ou des fournisseurs de logiciels DLP spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres. • **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet HIP Objects Certificate (Certificat d'objets HIP)

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Certificate (Certificat)**

Sélectionnez l'onglet **Certificate (Certificat)** pour permettre la correspondance HIP en fonction du profil de certificat et des autres attributs du certificat.

Paramètres du certificat d'objets HIP
Sélectionnez **Validate Certificate (Valider le certificat)** pour permettre la correspondance en fonction des profils de certificat et des attributs du certificat. Puis définissez les critères de correspondance, comme suit : • **Certificate Profile (Profil du certificat)** : Sélectionnez le profil de certificat que la passerelle GlobalProtect utilisera pour valider le certificat de machine envoyé dans le rapport HIP. • **Certificate Field (Champ du certificat)** : Sélectionnez un attribut de certificat utilisé pour la correspondance avec le certificat de machine. • **Value (Valeur)** : Définissez la valeur de l'attribut.

Onglet Vérifications personnalisées des objets HIP

- **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > *<hip-object> (objet HIP)* > **Custom Checks (Vérifications personnalisées)**

Sélectionnez l'onglet **Custom Checks (Vérifications personnalisées)** pour activer la correspondance HIP en fonction des vérifications personnalisées que vous avez définies sur le portail GlobalProtect. Pour plus d'informations sur l'ajout de vérifications personnalisées à la collecte de données HIP, reportez-vous à la section Réseau > GlobalProtect > Portails.

© 2020 Palo Alto Networks, Inc.

Paramètres des vérifications personnalisées d'un objet HIP	Description
Vérifications personnalisées	Sélectionnez **Custom Checks (Vérifications personnalisées)** pour permettre la correspondance sur les contrôles personnalisés que vous avez définis sur le portail GlobalProtect.
Liste des processus	Pour rechercher un processus spécifique sur le système hôte, cliquez sur **Add (Ajouter)** et saisissez le nom du processus. Par défaut, l'application recherche les processus en cours d'exécution ; si vous souhaitez vérifier si un processus spécifique n'est pas en cours d'exécution, décochez **Running (En cours d'exécution)**. Les processus peuvent être des processus au niveau système d'exploitation ou des processus de l'application utilisateur.
Clé de registre	Pour rechercher une clé de registre spécifique sur les hôtes Windows, cliquez sur **Add (Ajouter)** et saisissez la **Registry Key (Clé de registre)** pour la mise en correspondance. Pour faire correspondre uniquement les hôtes qui ne disposent pas de la clé de registre spécifiée ou de la valeur de la clé, cochez la case **Key does not exist or match the specified value data (La clé n'existe pas ou ne correspond pas aux données de la valeur définies)**. Pour la mise en correspondance avec des valeurs spécifiques, cliquez sur **Add (Ajouter)**, puis saisissez la **Registry Value (Valeur de registre)** et les **Value Data (Données de la valeur)**. Pour la mise en correspondance avec les hôtes qui ne disposent clairement pas de la valeur ou des données de la valeur spécifiées, sélectionnez **Negate (Inverser)**. Cliquez sur **OK** pour enregistrer les paramètres.
Plist	Pour rechercher une entrée spécifique dans la Property List (plist) sur les hôtes Mac, cliquez sur **Add (Ajouter)** et saisissez le nom du **Plist**. Pour la mise en correspondance uniquement avec les hôtes qui ne disposent pas du plist spécifié, sélectionnez **Plist does not exist (Le plist n'existe pas)**. Pour la mise en correspondance avec une valeur de clé spécifique dans la plist, cliquez sur **Add (Ajouter)**, puis saisissez la **Key (Clé)** et la **Value (Valeur)** correspondante pour la mise en correspondance. Pour la mise en correspondance avec les hôtes qui ne disposent clairement pas de la clé ou de la valeur spécifiée, cochez la case **Negate (Ignorer)** Cliquez sur **OK** pour enregistrer les paramètres.

© 2020 Palo Alto Networks, Inc.

Objets > GlobalProtect > Profils HIP

Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)** pour créer les profils HIP (un ensemble d'objets HIP à évaluer conjointement pour la surveillance ou pour l'application de la politique de sécurité) que vous utilisez pour configurer les politiques de sécurité activées par HIP. Lors de la création de profils HIP, vous pouvez combiner des objets HIP précédemment créés (ainsi que d'autres profils HIP) à l'aide d'une logique booléenne, notamment lorsqu'un flux de trafic est évalué en fonction d'un profil HIP auquel il correspond ou non. En cas de correspondance, la règle de politique correspondante est mise en œuvre ; s'il n'y a pas de correspondance, le flux est évalué en fonction de la règle suivante (comme avec tout autre critère de correspondance de politique).

Pour créer un profil HIP, cliquez sur **Add (Ajouter)**. Le tableau suivant fournit des informations sur les champs à renseigner dans la boîte de dialogue Profil HIP. Pour plus d'informations sur le paramétrage de GlobalProtect et le flux de travail pour la création de politiques de sécurité HIP, reportez-vous à la section Configuration de la mise en œuvre d'une politique HIP du *Guide de l'administrateur de GlobalProtect*.

Paramètres de profil HIP	Description
Name (Nom)	Donnez un nom au profil HIP (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	(Facultatif) Saisissez une description.
Partagé	Sélectionnez **Shared (Partagé)** pour rendre le profil de HIP courant disponible à : • Chaque système virtuel (vsys) sur le pare-feu, si vous êtes connecté à un pare-feu en mode Plusieurs systèmes virtuels. Si vous désactivez cette sélection, le profil est disponible uniquement aux systèmes virtuels sélectionnés dans le menu déroulant **Virtual System (Système virtuel)** dans l'onglet **Objects (Objets)**. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'apparaît pas dans la boîte de dialogue Profil HIP. • Tous les groupes de périphériques sur Panorama. Si vous décochez cette sélection, le profil sera disponible uniquement sur le groupe de périphériques sélectionné dans **Device Group (Groupe de périphériques)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Après avoir enregistré le profil, vous ne pouvez plus changer son paramètre **Shared (Partagé)**. Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)** pour afficher le **Location (Emplacement)** actuel.
Désactiver le contrôle prioritaire (Panorama uniquement)	Contrôle l'accès contrôle prioritaire au profil HIP dans des groupes de périphériques descendants du **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**. Sélectionnez cette option pour empêcher les administrateurs de créer des copies locales du profil dans les groupes de périphériques descendants en appliquant un contrôle prioritaire sur les valeurs héritées. Cette option est désactivée par défaut (le contrôle prioritaire est activé).

© 2020 Palo Alto Networks, Inc.

Paramètres de profil HIP	Description
Correspondance	Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)** pour HIP Objects/Profiles Builder (ouvrir le générateur de profils/ d'objets HIP). Sélectionnez le premier profil ou objet HIP que vous souhaitez utiliser comme critère de correspondance, puis ajoutez-le (⊕) à la zone de texte **Match (Faire correspondre)** de la boîte de dialogue Générateur de profils/ objets HIP. N'oubliez pas que, si vous souhaitez que le profil HIP évalue l'objet comme correspondance uniquement lorsque le critère de l'objet n'est pas vrai pour un flux, vous devez cocher **NOT (NE PAS)** avant d'ajouter l'objet. Continuez d'ajouter des critères de correspondance appropriés pour le profil que vous créez, en vous assurant de sélectionner l'opérateur booléen correspondant (**AND (ET)** ou **OR (OU)**) entre chaque ajout (et en sélectionner l'opérateur **NOT (NE PAS)**, le cas échéant). Pour créer une expression booléenne complexe, vous devez ajouter manuellement les parenthèses aux bons endroits dans la zone de texte **Match (Faire correspondre)** pour que le profil HIP soit évalué à l'aide de la logique booléenne souhaitée. Par exemple, l'expression suivante indique que le profil HIP correspond au trafic d'un hôte qui dispose du cryptage de disque FileVault (pour les systèmes d'exploitation Mac) ou TrueCrypt (pour les systèmes d'exploitation Windows), appartient au domaine requis et sur lequel un client antivirus Symantec est installé : `(("MacOS" and "FileVault") or ("Windows" and "TrueCrypt")) and "Domain" and "SymantecAV"` Lorsque vous avez terminé d'ajouter les objets et les profils au nouveau profil HIP, cliquez sur **OK**.

© 2020 Palo Alto Networks, Inc.

Périphérique > Client GlobalProtect

Les rubriques suivantes décrivent la configuration et la gestion de l'application GlobalProtect.

Que voulez-vous faire ?	Reportez-vous à la section :
Afficher plus d'informations sur les sorties de logiciels GlobalProtect.	Gestion de l'agent logiciel GlobalProtect
Installer le logiciel GlobalProtect.	Paramétrage de l'agent de GlobalProtect
Utiliser le logiciel GlobalProtect.	Utilisation de l'agent de GlobalProtect
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées étape par étape sur la configuration du logiciel GlobalProtect, reportez-vous à la section Déployer le logiciel des applications GlobalProtect du Guide de l'administrateur GlobalProtect.

Gestion du logiciel de l'application GlobalProtect

Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** (pare-feu uniquement) pour télécharger et activer le logiciel de l'application GlobalProtect sur le pare-feu qui héberge le portail. Par la suite, les terminaux qui se connectent au portail téléchargent le logiciel de l'application. Dans les configurations d'agent que vous spécifiez sur le portail, vous définissez comment et quand le portail pousse le logiciel aux terminaux. Votre configuration détermine si les mises à jour se font automatiquement lorsque l'application se connecte, que les utilisateurs finaux sont invités à mettre à jour ou si la mise à niveau est interdite pour tout ou un ensemble spécifique d'utilisateurs. Pour plus d'informations, reportez-vous à Permettre à l'utilisateur de mettre à niveau l'application GlobalProtect. Pour plus d'informations sur les options de distribution du logiciel de l'application GlobalProtect et pour obtenir des instructions détaillées sur le déploiement du logiciel, reportez-vous à la section Déploiement du logiciel de l'application GlobalProtect du Guide de l'administrateur de GlobalProtect.

Pour le téléchargement et l'installation initiaux de l'application GlobalProtect, l'utilisateur du point de terminaison doit être connecté avec des droits d'administrateur. Des droits d'administrateur ne sont pas nécessaires pour les mises à niveau ultérieures.

Paramètres du client GlobalProtect	Description
Version	Ce numéro de version du logiciel de l'application GlobalProtect est disponible sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel de l'application est disponible auprès de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**. Le pare-feu utilise son itinéraire de service pour se connecter au serveur de mises à jour pour déterminer si de nouvelles versions et les afficher en tête de liste.
Taille	Taille du module logiciel de l'application.
Date de version	Date et heure de disponibilité de la version auprès de Palo Alto Networks.

© 2020 Palo Alto Networks, Inc.

Paramètres du client GlobalProtect	Description
Téléchargé	Une coche dans cette colonne indique que la version correspondante du module logiciel de l'application a été téléchargée sur le pare-feu.
Actuellement activé	Une coche dans cette colonne indique que la version correspondante du module logiciel de l'application a été activée sur le pare-feu et peut être téléchargée par les applications qui s'y connectent. Une seule version du logiciel peut être activée à la fois.
Action (Action)	Indique l'action que vous pouvez entreprendre pour le module logiciel de l'application correspondant comme suit : • **Download (Télécharger)** : la version correspondante du logiciel de l'application est disponible sur le serveur de mises à jour Palo Alto Networks. Cliquez sur **Download (Télécharger)** pour lancer le téléchargement. Si le pare-feu ne dispose d'aucun accès à Internet, utilisez un ordinateur connecté à Internet pour vous rendre sur le site du Support aux clients, puis sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**pour chercher et **Download (Télécharger)** de nouvelles versions du logiciel de l'application sur votre ordinateur local. Ensuite, cliquez sur **Upload (Charger)** pour charger manuellement le logiciel de l'application au pare-feu. • **Activate (Activer)** : la version correspondante du logiciel de l'application a été téléchargée sur le pare-feu, mais les applications ne peuvent pas encore la télécharger. Cliquez sur **Activate (Activer)** pour activer le logiciel et permettre la mise à niveau de l'application. Pour activer une mise à jour logicielle chargée manuellement sur le pare-feu, cliquer **Activate From File (Activer depuis le fichier)** et sélectionner la version que vous souhaitez activer dans la liste déroulante (il se peut que vous deviez actualiser l'écran pour qu'elle s'affiche dans **Currently Activated (Actuellement activé)**). • **Reactivate (Réactiver)** : le logiciel de l'application correspondant a été activé et est prêt à être téléchargé par le point de terminaison. Comme une seule version du logiciel de l'application GlobalProtect peut être active à la fois sur le pare-feu, si vos utilisateurs finaux doivent accéder à une autre version que celle actuellement active, vous devez **Activate (Activer)** cette dernière pour qu'elle devienne la version **Currently Active (Actuellement active)**.
Notes de version	Cette option fournit un lien vers les notes de version GlobalProtect relatives à la version de l'application correspondante.
☒	Supprimez l'image du logiciel de l'application précédemment téléchargé à partir du pare-feu.

Paramétrage de l'application GlobalProtect

L'application GlobalProtect est une application qui est installée sur le point de terminaison (généralement un ordinateur portatif) pour prendre en charge les connexions que GlobalProtect établies avec les portails et les passerelles. L'application est soutenue par le service GlobalProtect (service PanGP).

© 2020 Palo Alto Networks, Inc.

Veillez à sélectionner l'option d'installation appropriée pour votre système d'exploitation hôte (32 ou 64 bits). Si vous installez sur un hôte 64 bits, utilisez le navigateur 64 bits et la combinaison Java pour l'installation initiale.

Pour installer l'application, ouvrez le fichier du programme d'installation et suivez les instructions affichées à l'écran.

Utilisation de l'application GlobalProtect

Les onglets du panneau **Paramètres GlobalProtect**, qui s'ouvre lorsque vous lancez l'application GlobalProtect et sélectionnez **Settings (Paramètres)** dans le menu **Paramètres** du panneal d'état GlobalProtect, contiennent des informations utiles sur l'état et les paramètres et fournissent des informations pour vous aider à régler les problèmes de connexion.

- Onglet Général : affiche le nom d'utilisateur et le ou les portails associés au compte GlobalProtect. Vous pouvez également ajouter, supprimer ou modifier des portails à partir de cet onglet.
- **Connection tab (Onglet Connexion)** : affiche la ou les passerelles qui sont configurées pour l'application GlobalProtect et fournit des informations à propos de chaque passerelle :
  - Nom de la passerelle
  - État du tunnel
  - Statut d'authentification
  - Type de connexion
  - Adresse IP ou FQDN de la passerelle (disponible uniquement en mode externe)

  Pour le mode interne, l'onglet Connection (Connexion) présente la liste complète des passerelles disponibles. Pour le mode externe, l'onglet Connection (Connexion) affiche la passerelle à laquelle vous êtes connecté ainsi que des détails supplémentaires sur la passerelle (comme l'adresse IP de la passerelle et la disponibilité).
- **Host Profile tab (Onglet Profil d'hôte)** : affiche les données sur les points de terminaison que GlobalProtect utilise pour la surveillance et l'application des politiques de sécurité par l'intermédiaire du Host Information Profile (Profil d'informations sur l'hôte ; HIP). Cliquez sur **Resubmit Host Profile (Envoyer de nouveau le profil de l'hôte)** pour procéder au renvoi manuel des données HIP à la passerelle.
- **Troubleshooting tab (Onglet Dépannage)** : sur les points de terminaison macOS, cet onglet vous permet de **Collect Logs (Collecter les journaux)** et de définir le **Logging Level (Niveau de journalisation)**. Sur les points de terminaison Windows, cet onglet vous permet de **Collect Logs (Collecter les journaux)**, de définir le **Logging Level (Niveau de journalisation)** et de consulter les informations suivantes pour vous aider dans le dépannage :
  - **Network Configurations (Configurations du réseau)** : indique la configuration actuelle du système.
  - **Routing Table (Table de routage)** - Fournit des informations sur la méthode d'acheminement actuelle de la connexion GlobalProtect.
  - **Sockets** - Fournit des informations sur les sockets des connexions actives.
  - **Logs (Journaux)** : permet à l'utilisateur de consulter les journaux de l'application et du service GlobalProtect. Choisissez le type de journal et le niveau de débogage. Cliquez sur **Start (Démarrer)** pour commencer la journalisation et sur **Stop (Arrêter)** pour l'arrêter.
- **Notification tab (Onglet Notification)** : affiche la liste de notifications déclenchées sur l'application GlobalProtect. Pour voir plus de détails d'une notification donnée, double-cliquez sur celle-ci.

Interface Web de Panorama

Panorama™ est le système de gestion centralisée pour l'ensemble des pare-feu de dernière génération Palo Alto Networks®. Panorama vous permet de superviser toutes les applications, les utilisateurs et le contenu présents sur votre réseau depuis un emplacement unique, puis utilise les informations obtenues pour créer des politiques permettant de contrôler et de protéger votre réseau. L'utilisation de Panorama pour la gestion centralisée des politiques et des pare-feu accroît votre efficacité opérationnelle lorsque vous gérez votre réseau distribué de pare-feux. Panorama est disponible sous forme de plate-forme d'appareil matériel dédiée (Série M) et d'équipement virtuel VMWare (exécuté sur un serveur ESXi ou la plate-forme vCloud Air).

Bien que de nombreux paramètres et affichages de l'interface Web Panorama soient identiques à ceux que vous voyez sur l'interface Web du pare-feu, les rubriques suivantes décrivent les options disponibles exclusivement sur l'interface Web Panorama pour gérer Panorama, les pare-feu et les Collecteurs de journaux.

- Utilisation de l'interface Web de Panorama
- Commutateur de contexte
- Opérations de validation de Panorama
- Définition des politiques sur Panorama
- Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité
- Panorama > Configuration > Interfaces
- Panorama > Haute disponibilité
- Panorama > Clusters WildFire gérés
- Panorama > Administrateurs
- Panorama > Rôles admin
- Panorama > Domaines d'accès
- Panorama > Périphériques gérés > Récapitulatif
- Panorama > Périphériques gérés > État
- Panorama > Modèles
- Panorama > Groupes de périphériques
- Panorama > Collecteurs gérés
- Panorama > Groupes de collecteurs
- Panorama > Plug-ins
- Panorama > VMware NSX
- Panorama > Profil d'ingestion des journaux
- Panorama > Paramètres des journaux
- Panorama > Exportation programmée des configurations
- Panorama > Logiciel
- Panorama > Déploiement du périphérique

Vous souhaitez en savoir plus ?

Voir le Guide de l'administrateur Panorama pour plus de détails sur la configuration et l'utilisation de Panorama pour la gestion centralisée.

© 2020 Palo Alto Networks, Inc.

Utilisation de l'interface Web de Panorama

Les interfaces Web de Panorama et les pare-feu ont le même aspect. Cependant, l'interface Web de Panorama offre des options supplémentaires et un onglet spécifique à Panorama pour la gestion de Panorama ainsi que pour son utilisation en vue de gérer les pare-feu et les Collecteurs de journaux.

Les champs communs suivants apparaissent dans l'en-tête ou le pied de page de plusieurs pages d'interface Web Panorama.

Champs commun	Description
Contexte	Vous pouvez utiliser la liste déroulante **Contexte** qui se trouve au-dessus du menu latéral pour passer de l'interface Web de Panorama à une interface Web du pare-feu (voir Commutation de contexte).
	Dans les onglets **Tableau de bord** et **Surveillance**, cliquez sur actualiser () dans l'en-tête de l'onglet pour actualiser manuellement les données dans ces onglets. Vous pouvez également utiliser le menu déroulant sans référence sur le côté droit de l'en-tête de l'onglet pour sélectionner un intervalle d'actualisation automatique en minutes (**1 min (1 minute)**, **2 mins (2 minutes)** ou **5 mins (5 minutes)**) ; pour désactiver l'actualisation automatique, sélectionnez **Manuel**.
Domaine d'accès	Un domaine d'accès définit l'accès à des groupes de périphériques spécifiques, des modèles et des pare-feu individuels (à travers le menu déroulant **Contexte**). Si vous vous connectez en tant qu'administrateur avec plusieurs domaines d'accès affectés à votre compte, les onglets **Tableau de bord**, **ACC**, et **Surveillance** affichent des informations (comme les données des journaux) uniquement pour le **Domaine d'accès** que vous sélectionnez dans le pied de page de l'interface Web.  *Si un seul domaine d'accès est affecté à votre compte, l'interface Web n'affiche pas le menu déroulant Domaine d'accès.*
Groupe de périphériques	Un groupe de périphériques englobe des pare-feu et des systèmes virtuels que vous gérez en tant que groupes (voir Panorama > Groupes de périphériques). Les onglets **Tableau de bord**, **ACC**, et **Surveillance** affichent des informations (comme les données des journaux) uniquement pour le **Groupe de périphériques** que vous sélectionnez dans l'en-tête de l'onglet. Dans les onglets **Politiques** et **Objets**, vous pouvez configurer les paramètres pour un **Groupe de périphériques** ou pour tous les groupes de périphériques (sélectionnez **Partagé**).
Modèle	Un modèle est un groupe de pare-feu avec des paramètres réseau et de périphérique communs et une pile de modèles est une combinaison de modèles (voir Panorama > Modèles). Dans les onglets **Réseau** et **Périphérique**, vous configurez les paramètres pour un **Modèle** spécifique ou une pile de modèles. Comme vous pouvez modifier les paramètres uniquement dans les modèles individuels, les paramètres de ces onglets sont en lecture seule si vous sélectionnez un ensemble (stack) de modèles.

© 2020 Palo Alto Networks, Inc.

Champs commun	Description
Visualiser par : Périphérique	Par défaut, les onglets **Réseau** et **Périphérique** affichent les paramètres et les valeurs disponibles pour les pare-feu qui sont en mode de fonctionnement normal et qui prennent en charge plusieurs systèmes virtuels et VPN. Cependant, vous pouvez utiliser les options suivantes pour filtrer les onglets afin d'afficher uniquement les paramètres spécifiques au mode à modifier : • Dans la liste déroulante **Mode**, activez ou désactivez les options **Multi-VSYS**, le **Mode opérationnel** et les options du **Mode VPN**. • Définissez toutes les options de Mode afin de tenir compte de la configuration d'un pare-feu en particulier en le sélectionnant dans le menu déroulant **Visualiser par : périphérique**.
Mode	

L'onglet **Panorama** fournit les pages suivantes pour la gestion de Panorama et des Collecteurs de journaux.

Pages Panorama	Description
setup	Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** pour les tâches suivantes : • Préciser des paramètres généraux (par exemple, le nom d'hôte de Panorama) et des paramètres pour l'authentification, les journaux, les rapports, AutoFocus™, les bannières, le message du jour et la complexité des mots de passe. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > Gestion. • Sauvegarder et restaurer les configurations, redémarrer Panorama et arrêter Panorama. Ces opérations sont similaires à celles que vous effectuer pour les pare-feu : sélectionnez Périphérique > Configuration > Opérations. • Définir les connexions de serveur pour les mises à jour DNS, NTP et Palo Alto Networks. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > Services. • Configurer les paramètres réseau pour les interfaces Panorama. Sélectionnez Panorama > Configuration > Interfaces. • Précisez les paramètres pour l'appareil WildFire™. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > WildFire. • Gérer les paramètres des modules de sécurité matériels. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > HSM.
Haute disponibilité	Vous permet de configurer la haute disponibilité pour une paire de serveurs de gestion Panorama. Sélectionnez Panorama > Haute Disponibilité.
Audit de configuration	Vous permet d'afficher les différences entre les fichiers de configuration. Sélectionnez Périphérique > Audit de configuration.
Profils de mot de passe	Vous permet de définir des profils de mot de passe pour les administrateurs de Panorama. Sélectionnez Périphérique > Profils de mot de passe.
Administrateurs	Vous permet de configurer les comptes administrateur Panorama. Sélectionnez Panorama > Administrateurs.

© 2020 Palo Alto Networks, Inc.

Pages Panorama	Description
	Si un compte administrateur est verrouillé, la page Administrateurs affiche un verrou dans la colonne Utilisateur verrouillé. Vous pouvez cliquer sur le verrou pour déverrouiller le compte.
Rôles administrateur	Vous permet de définir des rôles administrateur qui contrôlent les privilèges et les responsabilités des administrateurs qui ont accès à Panorama. Sélectionnez Panorama > Rôles administrateur.
Domaine d'accès	Vous permet de contrôler l'accès administrateur aux groupes de périphériques, modèles, piles de modèles et à l'interface Web de pare-feu. Sélectionnez Panorama > Domaines d'accès.
Profil d'authentification	Vous permet de préciser un profil pour authentifier l'accès à Panorama. Sélectionnez Périphérique > Profil d'authentification.
Séquence d'authentification	Vous permet de préciser une série de profils d'authentification à utiliser pour autoriser l'accès à Panorama. Sélectionnez Périphérique > Séquence d'authentification.
Identification utilisateur	Vous permet de configurer Panorama pour la réception des informations de mappage d'utilisateurs à partir des agents User-ID™. Sélectionnez Périphérique > Identification utilisateur > Agents User-ID.
Périphériques gérés	Vous permet de gérer les pare-feu, ce qui inclut l'ajout de pare-feu à Panorama en tant que *périphériques gérés*, l'affichage de la connexion des pare-feu et l'état des licences, l'étiquetage des pare-feu, les mises à jour logicielles et de contenu et le chargement des sauvegardes des configurations. Sélectionnez Panorama > Périphériques gérés > Récapitulatif.
Modèles	Vous permet de gérer la configuration des options de configuration dans les onglets **Périphérique** et **Réseau**. Les modèles et les piles de modèles vous permettent de réduire les efforts administratifs grâce au déploiement de plusieurs pare-feu disposant de configurations identiques ou similaires. Sélectionnez Panorama > Modèles.
Groupes de périphériques	Vous permet de configurer les groupes de périphériques, qui regroupent les pare-feu en fonction de leurs fonctionnalités, leur segmentation réseau ou de leur emplacement géographique. Les groupes de périphériques peuvent inclure des pare-feu physiques, des pare-feu virtuels et des systèmes virtuels. Généralement, les pare-feu d'un groupe de périphériques nécessitent des configurations de politiques similaires. À l'aide des onglets **Policies (Politiques)** et **Objects (Objets)** sur Panorama, les groupes de périphériques permettent de mettre en œuvre une approche en couche pour gérer les politiques au sein d'un réseau de pare-feu gérés. Vous pouvez imbriquer des groupes de périphériques à une hiérarchie d'arborescence pouvant comporter un maximum de quatre niveaux. Les groupes descendants héritent automatiquement des politiques et objets des anciens groupes et de l'emplacement Partagé. Sélectionnez Panorama > Groupes de périphériques.

© 2020 Palo Alto Networks, Inc.

Pages Panorama	Description
Collecteurs gérés	Vous permet de gérer les Collecteurs de journaux. Étant donné que vous utilisez Panorama pour configurer et gérer les collecteurs de journaux, ils sont également appelés *les collecteurs gérés*. Un collecteur géré peut être local au serveur de gestion Panorama (appareil de la série M ou appareil virtuel Panorama en mode Panorama) ou un Collecteur de journaux dédié (appareil de la série M en mode Collecteur de journaux). Sélectionnez Panorama > Collecteurs gérés. Vous pouvez également installer les Mises à jour logicielles pour les collecteurs de journaux dédiés. *Vous pouvez* convertir un serveur de gestion Panorama en un Collecteur de journaux dédié.
Groupes de collecteurs	Vous permet de gérer les Groupes de collecteurs. Un Groupe de collecteurs regroupe les Collecteurs de journaux pour que vous puissiez appliquer des paramètres de configuration identiques et leur assigner des pare-feu. Panorama distribue uniformément les journaux entre tous les disques d'un collecteur de journaux et tous les membres du groupe de collecteurs. Sélectionnez Panorama > Groupes de collecteurs.
Plug-ins	Vous permet de gérer les plug-ins pour une intégration tierce, par exemple VMware NSX. Sélectionnez Panorama > VMware NSX.
VMware NSX	Vous permet d'automatiser l'approvisionnement des pare-feu de série VM en activant la communication entre NSX Manager et Panorama. Sélectionnez Panorama > VMware NSX.
Gestion des certificats	Vous permet de configurer et de gérer des certificats, des profils de certificat et des clés. Sélectionnez Gestion des certificats du pare-feu et de Panorama.
Paramètres des journaux	Vous permet de transférer des journaux aux récepteurs de pièges SNMP (Simple Network Management Protocol / protocole de gestion de réseau simple), serveurs Syslog, serveurs e-mail et serveurs HTTP. Sélectionnez Périphérique > Paramètres des journaux.
Profils de serveur	Vous permet de configurer les profils des différents types de serveurs qui fournissent des services à Panorama. Sélectionnez l'une des options suivantes pour configurer un type de serveur spécifique : • Périphérique > Profils de serveur > Messagerie • Périphérique > Profils de serveur > HTTP • Périphérique > Profils de serveur > Piège'A0;SNMP • Périphérique > Profils de serveur > Syslog • Périphérique > Profils de serveur > RADIUS • Périphérique > Profils de serveur > TACACS+ • Périphérique > Profils de serveur > LDAP • Périphérique > Profils de serveur > Kerberos • Périphérique > Profils de serveur > Fournisseur d'identité SAML

© 2020 Palo Alto Networks, Inc.

Pages Panorama	Description
Exportation planifiée des configurations	Vous permet d'exporter les configurations de Panorama et du pare-feu vers serveur FTP ou un serveur SCP (Secure Copy / copie sécurisée) de manière quotidienne. Sélectionnez Panorama > Planifier l'exportation de la configuration.
Logiciels	Vous permet de mettre à jour le logiciel Panorama. Sélectionnez Panorama > Logiciel.
Mises à jour dynamiques	Vous permet de consulter les dernières définitions d'applications et informations sur les nouvelles menaces de sécurité telles que des signatures Antivirus (licence de protection contre les menaces requise) puis de mettre à jour Panorama avec les nouvelles définitions. Sélectionnez Périphérique > Mises à jour dynamiques.
Assistance	Vous permet d'accéder aux alertes produit et de sécurité de Palo Alto Networks. Sélectionnez Panorama > Assistance.
Déploiement de périphériques	Vous permet de déployer des mises à jour logicielles et de contenu sur les pare-feu et les Collecteurs de journaux. Sélectionnez Panorama > Déploiement du périphérique.
Clé principale et diagnostics	Vous permet de préciser une clé principale afin de chiffrer des clés privées sur Panorama. Par défaut, Panorama stocke les clés privées sous forme cryptée, même si vous n'indiquez pas une nouvelle clé principale. Sélectionnez Périphérique > Clé principale et diagnostics.

© 2020 Palo Alto Networks, Inc.

Commutateur de contexte

Dans l'en-tête de chaque interface Web de Panorama, vous pouvez utiliser la liste déroulante **Contexte** qui se trouve au-dessus du menu de gauche pour passer de l'interface Web de Panorama à une interface Web du pare-feu. Lorsque vous sélectionnez un pare-feu, l'interface Web est actualisée pour afficher toutes les pages et options du pare-feu sélectionné pour que vous puissiez le gérer localement. La liste déroulante n'affiche que les pare-feu pour lesquels vous disposez d'un accès administrateur (voir Panorama > Domaines d'accès) et qui sont connectés à Panorama.

Vous pouvez utiliser les Filtres pour rechercher des pare-feu par Plateformes (modèle), Groupes de périphériques, Modèles, Étiquettes ou de l'état HD. Vous pouvez également saisir une chaîne de texte dans la barre de filtrage pour effectuer une recherche par Nom de périphérique.

L'arrière-plan des icônes des pare-feu en mode haute disponibilité (HD) est coloré pour indiquer leur état HD.

© 2020 Palo Alto Networks, Inc.

Opérations de validation de Panorama

Cliquez sur **Commit (Valider)** en haut à droite de l'interface Web et sélectionnez une action pour les modifications en attente pour la configuration Panorama et les modifications apportées par Panorama aux pare-feu, aux collecteurs de journaux et aux appareils et clusters WildFire :

- **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** – Active les changements que vous avez effectués pour la configuration du serveur de gestion Panorama. Cette action valide également les modifications du groupe de périphériques, du modèle, du groupe de collecteurs, du cluster et des appareils WildFire apportées à la configuration Panorama sans appliquer les modifications aux pare-feu, aux collecteurs de journaux ou aux clusters et appareils WildFire. L'application de ces modifications uniquement à la configuration Panorama vous permet d'enregistrer les modifications qui ne sont pas prêtes à être activées sur les pare-feu, les collecteurs de journaux ou les clusters et appareils WildFire.

  Lorsque vous appliquez les configurations aux périphériques gérés, Panorama 8.0 et les versions ultérieures appliquent la configuration actuelle, qui correspond à la configuration qui est activée sur Panorama. Panorama 7.1 et les versions antérieures appliquent la configuration candidate, qui inclut les modifications non validées. Par conséquent, Panorama 8.0 et les versions ultérieures ne vous permettent pas d'appliquer les modifications apportées aux périphériques gérés jusqu'à ce que vous validiez d'abord les modifications apportées à Panorama.
- **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** – Applique la configuration actuelle de Panorama aux groupes de périphériques, aux modèles, aux groupes de collecteurs et aux clusters et appareils WildFire.
- **Commit (Valider)** > **ommit and Push (Valider et appliquer)** – Applique toutes les modifications de configuration à la configuration locale de Panorama, puis applique la configuration actuelle de Panorama aux groupes de périphériques, aux modèles, aux groupes de collecteurs et aux clusters et appareils WildFire.

Vous pouvez filtrer les modifications en attente par administrateur ou *emplacement*, puis vous pouvez confirmer, appliquer, valider ou prévisualiser uniquement ces modifications. L'emplacement peut être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des appareils et des clusters WildFire, des paramètres partagés ou le serveur de gestion Panorama.

Lorsque vous validez des modifications, elles deviennent partie intégrante de la configuration actuelle. Les modifications que vous n'avez pas validées font partie de la configuration candidate. Panorama met les demandes de validation en file d'attente pour que vous puissiez initier de nouvelles validations alors qu'une validation antérieure est en cours d'exécution. Panorama exécute les validations dans l'ordre dans lequel elles sont initiées, mais donne la priorité aux validations que Panorama initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d'attente possède déjà le nombre maximum de validations lancées par l'administrateur, vous devez attendre que Panorama termine le traitement d'une validation en attente avant d'en lancer une nouvelle. Vous pouvez utiliser le Gestionnaire de tâches (Tasks) pour vider la file d'attente des validations ou pour consulter les informations sur les validations. Pour plus d'informations sur les modifications de configuration, les processus de validation, les validations ou la file d'attente des validations, reportez-vous à la section Opérations de validation sur Panorama. Vous pouvez aussi Enregistrer les configurations candidates, Annuler les modifications et importer, exporter ou charger des configurations (Périphérique > Configuration > Opérations).

Les options suivantes sont disponibles pour confirmer, valider ou prévisualiser les modifications de configuration.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Les options suivantes s'appliquent lorsque vous les validez sur Panorama en sélectionnant **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** ou **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.	
Valider toutes les modifications	Confirme toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement l'étendue des modifications de configuration que Panorama valide lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l'étendue de validation : • **Rôle du super-utilisateur** – Panorama valide les changements de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de validation (voir Panorama > Rôles administrateurs). Si le profil inclut le privilège de **Commit For Other Admins (Valider pour les autres administrateurs)**, Panorama valide les modifications configurées par un ou tous les administrateurs. Si votre profil de rôle administrateur n'inclut pas le privilège de **Commit For Other Admins (Valider pour les autres administrateurs)**, Panorama valide uniquement vos modifications et pas celles des autres administrateurs. Si vous avez mis en place des domaines d'accès, Panorama applique automatiquement ces domaines pour filtrer la portée de validation (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur, Panorama ne valide que les modifications de configuration dans les domaines d'accès affectés à votre compte.
Valider les modifications effectuées par	Filtre la portée des changements de configuration que Panorama valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle du super-utilisateur** – Vous pouvez limiter l'étendue de validation aux modifications apportées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de validation (voir Périphérique > Rôles administrateurs). Si le profil inclut le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation aux modifications configurées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtre l'étendue de validation comme suit :

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **Filtrer par administrateur** – Même si votre rôle vous permet de valider les modifications effectuées par les autres administrateurs, par défaut, l'étendue de validation inclut uniquement vos modifications. Pour ajouter d'autres administrateurs à la portée de la validation, cliquez sur le lien *<usernames> (<noms d'utilisateur>)*, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les emplacements spécifiques pour les modifications à Inclure dans la validation. Si vous avez mis en place des domaines d'accès, Panorama filtre automatiquement la portée de validation en fonction de ces domaines (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l'étendue de validation inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte. *Après avoir chargé une configuration (Périphérique > Configuration > Opérations), vous devez Valider toutes les modifications.* Lorsque vous validez des modifications apportées à un groupe de périphériques, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce groupe de périphériques.
Étendue de la validation	Répertorie les emplacements contenant des modifications à valider. Différents facteurs déterminent si la liste inclut toutes les modifications ou un sous-ensemble de modifications, comme il est décrit dans Valider toutes les modifications et Valider les modifications effectuées par. Les emplacements peuvent être l'un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l'emplacement Partagé. • *<device-group> (<groupe de périphériques>)* – Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • *<template> (<modèle>)* – Le nom du modèle ou du groupe de modèles dans lequel les paramètres sont définis. • *<log-collector-group> (<groupe de collecteur de journaux>)* – Le nom du groupe de collecteur dans lequel les paramètres sont définis. • *<log-collector> (<collecteur de journaux>)* – Le nom du collecteur de journaux dans lequel les paramètres sont définis. • *<wildfire-appliances> (<appareils WildFire>)* – Le numéro de série de l'appareil WildFire dans lequel les paramètres sont définis. • *<wildfire-appliance-clusters> (<clusters d'appareils WildFire>)* – Le nom du cluster WildFire dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Panorama** – Paramètres spécifiques à la configuration du serveur de gestion Panorama.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	• **Device Group (Groupe de périphériques)** – Paramètres définis dans un groupe de périphériques spécifique. • **Template (Modèle)** – Paramètres définis dans un modèle ou un groupe de modèles spécifique. • **Log Collector Group (Groupe de collecteurs de journaux)** – Paramètres qui sont spécifiques à une configuration de groupe de collecteur. • **Log Collector (Collecteur de journaux)** – Paramètres spécifiques à une configuration de collecteur de journaux. • **WildFire Appliance Clusters (Clusters d'appareils WildFire)** – Paramètres spécifiques à une configuration de cluster d'appareils WildFire. • **WildFire Appliances (Appareils WildFire)** – Paramètres spécifiques à un appareil WildFire. • **Autres changements** – Paramètres qui ne sont pas spécifiques à l'une des zones de configuration précédentes (telles que les objets partagés).
Inclure dans la validation (Validation partielle uniquement)	Vous permet de sélectionner les modifications que vous souhaitez valider. Par défaut, toutes les modifications de l'**Étendue de validation** sont sélectionnées. Cette colonne s'affiche uniquement après que vous avez choisi de **Valider les modifications effectuées par** des administrateurs spécifiques. *Il peut y avoir des dépendances affectant les modifications que vous incluez dans une validation. Par exemple, si vous ajoutez un objet et qu'un autre administrateur modifie cet objet, vous ne pouvez pas valider la modification pour l'autre administrateur sans valider votre propre modification.*
Regrouper par type	Regroupe la liste des modifications de configuration de l'**Étendue de validation** par **Type d'emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans l'**Étendue de validation** de la configuration en cours d'exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l'interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d'exécution que vous comparez. *Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de*

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.
Modifier le récapitulatif	Répertorie les paramètres individuels pour lesquels vous effectuez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l'objet** – Le nom qui identifie la politique, l'objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d'emplacement** – Indique si le paramètre est défini dans **Groupes de périphériques**, **Modèles**, **Groupes de collecteurs**, **Appareils WildFire** ou **Clusters d'appareils WildFire**. • **Emplacement** – Le nom du groupe de périphériques, du modèle, du groupe de collecteurs, du cluster WildFire ou de l'appareil WildFire où le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas définis dans ces emplacements. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L'administrateur qui a effectué la dernière modification du paramètre. • **Sera validé** – Indique si la validation inclura le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Confirmer la validation	Vérifie que la syntaxe de la configuration de Panorama est correcte et est complète d'un point de vue sémantique. Le résultat inclut les mêmes erreurs et avertissements qu'une validation afficherait, y compris la règle l'occultation et l'application des avertissements de dépendance. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d'exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d'erreur.
Les options suivantes s'appliquent lorsque vous appliquez les modifications de configuration sur les périphériques gérés en sélectionnant **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** ou **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.	
Étendue de la transmission	Liste les emplacements qui ont des modifications à appliquer. Les emplacements que la portée inclut par défaut dépendent des options suivantes que vous sélectionnez : • **Commit (Valider)** > **Commit and Push (Valider et appliquer)** – La portée comprend tous les emplacements avec des modifications nécessitant une validation de la part de Panorama. • **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** – La portée comprend tous les emplacements associés aux entités (pare-feux, systèmes virtuels, collecteurs de journaux,

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
	clusters WildFire, appareils WildFire) qui sont `Out of Sync (Désynchronisées)` avec la configuration actuelle de Panorama (voir Panorama > Périphériques gérés > Récapitulatif et Panorama > Collecteurs gérés pour le statut de synchronisation). Pour les deux sélections, Panorama filtre la **Portée d'application** par : • **Administrateurs** – Panorama applique les mêmes filtres que pour **la Portée de validation** (voir Appliquer tous les changements ou Appliquer les modifications faites par). • **Domaine d'accès** – Si vous avez mis en place des domaines d'accès, Panorama filtre automatiquement la **Portée d'application** en fonction de ces domaines (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l'étendue inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte. Vous pouvez Modifier les sélections pour la **Portée d'application** au lieu d'accepter les emplacements par défaut.
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Groupes de périphériques** – Paramètres définis dans un groupe de périphériques spécifique. • **Modèles** – Paramètres définis dans un modèle ou une pile de modèles spécifique. • **Groupe de collecteurs de journaux** – Paramètres spécifiques à une configuration de groupe de collecteur. • **Clusters WildFire** – Paramètres spécifiques à une configuration de cluster WildFire. • **Appareils WildFire** – Paramètres spécifiques à une configuration d'appareil WildFire.
Entités	Pour chaque groupe de périphériques ou modèle, cette colonne répertorie les pare-feu (par nom de périphérique ou numéro de série) ou les systèmes virtuels (par nom) inclus dans l'opération de validation. *Si vous appliquez les modifications apportées à un groupe de collecteurs, l'opération inclut tous les collecteurs de journaux qui sont des membres du groupe, même s'ils ne sont pas répertoriés.*
Modifier les sélections	Cliquez pour sélectionner les entités à inclure dans l'opération de validation : • Modèles et groupes de périphériques • Groupes de collecteurs de journaux • Appareils et clusters WildFire *Panorama ne vous permettra pas d'appliquer les modifications que vous n'avez pas encore validées dans la configuration de Panorama.*

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Modèles et groupes de périphériques	Cliquez pour **Modifier les sélections** et sélectionnez les **Groupes de périphériques** ou les **Modèles** pour afficher les options dans les lignes suivantes.
Filtres	Filtrez la liste des modèles, des piles de modèles ou des groupes de périphériques et les pare-feu et systèmes virtuels associés.
Name (Nom)	Sélectionnez les modèles, les piles de modèles, les groupes de périphériques, les pare-feu ou les systèmes virtuels à inclure dans l'opération de validation.
État de la dernière validation	Indique si les configurations des pare-feu et des systèmes virtuels sont synchronisées avec les configurations des modèles ou des groupes de périphériques dans Panorama.
État HA	Indique l'état de la haute disponibilité (HA) sur les pare-feu énumérées : • **Active (Actif)** - État opérationnel de gestion du trafic normal. • **Passive (Passif)**- État de sauvegarde normal. • **Initiating (En cours d'initialisation)** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non-functional (Non fonctionnel)** - État d'erreur. • **Suspended (Suspendu)** - Un administrateur a désactivé le pare-feu. • **Tentative (Provisoire)** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
Modifications en attente de validation (Panorama)	Indique si une validation Panorama est requise (`oui`) ou non (`non`) avant d'appliquer les modifications aux pare-feu et aux systèmes virtuels sélectionnés.
Colonne de prévisualisation des modifications	Cliquez pour **prévisualiser les modifications** pour comparer les configurations que vous avez sélectionnées dans la **Portée d'application** pour la configuration actuelle de Panorama. Panorama filtre les résultats pour afficher uniquement les résultats pour les pare-feu et les systèmes virtuels que vous avez sélectionnés dans l'onglet **Groupes de périphériques** ou **Modèles**. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge).  *Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.*
Sélectionner tout	Sélectionne toutes les entrées de la liste.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Désélectionner tout	Désélectionne toutes les entrées de la liste.
Développer tout	Affiche les pare-feu et les systèmes virtuels attribués aux modèles, aux piles de modèles ou aux groupes de périphériques.
Réduire tout	Affiche uniquement les modèles, les piles de modèles ou les groupes de périphériques, mais pas les pare-feu ou les systèmes virtuels qui leur sont attribués.
Regrouper les homologues HA	Regroupe les pare-feu homologues dans une configuration haute disponibilité (HA). La liste qui en résulte affiche alors le pare-feu actif (ou le pare-feu actif / principal dans une configuration active / active) en premier, suivi du pare-feu passif (ou pare-feu actif / secondaire dans une configuration active / active) entre parenthèses. Ceci vous permet d'identifier facilement les pare-feu en mode HA. Lors de l'application de politiques partagées, vous pouvez l'appliquer à la paire regroupée plutôt qu'à chaque homologue. *pour des homologues HA dans une configuration active/passive, envisagez l'ajout des deux pare-feu ou de leurs systèmes virtuels au même groupe de périphériques, au même modèle ou à la même pile de modèles pour que vous puissiez appliquer la configuration aux deux homologues de façon simultanée.*
Appliquer	Cliquez pour valider les configurations que vous appliquez pour les pare-feu et les systèmes virtuels sélectionnés. Le Gestionnaire des tâches s'ouvre automatiquement pour afficher l'état de la validation.
Filtre sélectionné	Si vous souhaitez afficher uniquement certains pare-feu ou systèmes virtuels, sélectionnez-les puis sélectionnez **Filtre sélectionné**.
Fusionner avec la configuration du candidat	(Selectionné par défaut) Fusionne les modifications de configuration transmises par Panorama en prenant en compte les modifications en attente mises en œuvre localement par les administrateurs sur le pare-feu cible. L'opération de validation déclenche PAN-OS® pour valider les modifications fusionnées. Si vous désélectionnez cette option, la validation exclut la configuration candidate sur le pare-feu. *Désélectionnez cette option si vous autorisez les administrateurs de pare-feu à valider les modifications localement sur le pare-feu et si vous ne voulez pas inclure ces modifications locales lors de la validation de modifications à partir de Panorama.* Il est également recommandé de faire un audit de configuration sur le pare-feu afin de passer en revue les modifications locales avant d'appliquer les modifications à partir de Panorama (Reportez-vous à la section Périphérique > Audit de configuration).

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Inclure les modèles de réseaux et de périphériques (Onglet Groupes de périphériques uniquement)	(Sélectionné par défaut) Applique les changements de groupe de périphériques et les modifications du modèle associé aux pare-feu et aux systèmes virtuels sélectionnés en une seule opération. Pour appliquer ces modifications en tant qu'opérations distinctes, désélectionnez cette option.
Forcer les valeurs du modèle	(Désactivé par défaut) Remplace l'ensemble des paramètres de la configuration locale et supprime tous les objets sur les pare-feu sélectionnés qui n'existent pas dans le modèle ou dans la pile de modèles ou qui ont été écrasés par la configuration locale. L'opération de validation restaure l'ensemble de la configuration existante sur le pare-feu et garantit que le pare-feu hérite uniquement des paramètres définis dans le modèle ou dans la pile de modèles. *Si vous transmettez un configuration avec l'option Force Template Values (Forcer les valeurs du modèle) activée, toutes les valeurs forcées du pare-feu sont remplacées par les valeurs du modèle. Avant d'utiliser cette option, vérifiez les valeurs forcées des pare-feu pour garantir que votre validation ne donne pas lieu à des pannes réseau imprévus ou à des problèmes causés par le remplacement de ces valeurs forcées.*
Groupes de collecteurs de journaux	Cliquez pour **Modifier les sélections** et sélectionnez **Groupes de collecteurs de journaux** à inclure dans l'opération de validation. Cet onglet affiche les options suivantes : • **Tout sélectionner** – Sélectionne chaque groupe de collecteurs dans la liste. • **Tout désélectionner** – Désélectionne chaque groupe de collecteurs dans la liste.
Appareils et clusters WildFire	Pour **Modifier les sélections** et sélectionner les **Clusters et appareils WildFire** pour afficher les options suivantes.
Filtres	Filtre la liste des appareils et des clusters WildFire.
Name (Nom)	Sélectionne les appareils et les clusters WildFire sur lesquels Panorama appliquera les modifications.
État de la dernière validation	Indique si les configurations de l'appareil et du cluster WildFire sont synchronisées avec Panorama.
Supprimer les sélections	Supprime tous les pare-feux indiqués dans la portée d'application.
Confirmer la transmission du groupe d'appareils	Valide les configurations que vous appliquez pour les groupes de périphériques dans la liste Portée d'application. Le Gestionnaire des tâches s'ouvre automatiquement pour afficher l'état de la validation.

© 2020 Palo Alto Networks, Inc.

Champ/Bouton	Description
Confirmer la transmission du modèle	Valide les configurations que vous appliquez pour les modèles dans la liste Portée d'application. Le Gestionnaire des tâches s'ouvre automatiquement pour afficher l'état de la validation.
Regrouper par type d'emplacement	À sélectionner pour utiliser le **Type d'emplacement** pour grouper la liste Portée d'application.
Les options suivantes s'appliquent lorsque vous validez la configuration Panorama ou lorsque vous appliquez les modifications apportées aux périphériques.	
Description	Saisissez une description (jusqu'à 512 caractères) pour aider les autres administrateurs à comprendre les modifications que vous avez effectuées.  *Le Journal système pour un événement de validation tronquera la description si elle dépasse 512 caractères.*
Valider / Appliquer / Valider et appliquer	Démarre la validation ou, si d'autres validations sont en attente, ajoute la demande de validation à la file d'attente de validation.

© 2020 Palo Alto Networks, Inc.

Définition des politiques sur Panorama

Sur Panorama™, les groupes de périphériques vous permettent de gérer de façon centralisée les politiques des pare-feu. Vous pouvez créer les politiques sur Panorama en tant que *Règles avant* ou que *Règles après* ; les Règles avant et les Règles après vous permettent de créer une approche progressive de la mise en œuvre des politiques.

Vous pouvez définir les Règles avant et les Règles après dans un contexte partagé, comme politiques partagées pour tous les pare-feu gérés ou dans un contexte de groupe de périphériques pour les rendre spécifiques à un groupe de périphériques. Avant de définir les Règles avant et les Règles après sur Panorama, puis de les transmettre de Panorama vers les pare-feu gérés, vous pouvez les afficher sur les pare-feu gérés, mais vous pouvez modifier les Règles avant et les Règles après uniquement sur Panorama.

- **Pre Rules (Règles avant)** – Règles ajoutées au début de la liste des règles et évaluées en premier. Vous pouvez utiliser les pré-règles pour faire respecter la Politique d'utilisation acceptable d'une organisation. Par exemple, vous pouvez bloquer l'accès à des catégories d'URL spécifiques ou permettre du trafic DNS pour tous les utilisateurs.
- **Règles après** – Les règles ajoutées en fin de liste des règles et évaluées après les règles avant et les règles définies localement sur le pare-feu. Les Règles après comprennent généralement des règles visant à refuser l'accès au trafic sur la base de l'App-ID™, User-ID™ ou d'un Service.
- **Règles par défaut** – Les règles qui indiquent au pare-feu comment traiter le trafic qui ne correspond à aucune Règle avant, Règle après ou règles de pare-feu local. Ces règles font partie de la configuration prédéfinie de Panorama. Pour **Remplacer** et activer l'édition des paramètres sélectionnés dans ces règles, voir Remplacer ou annuler une règle de politique de sécurité.

Cliquez sur l'option **Prévisualiser les règles** pour afficher une liste de toutes les règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de règles, la hiérarchie des règles est marquée visuellement pour chaque groupe de périphériques (et pare-feu géré), afin de faciliter l'analyse d'un grand nombre de règles.

Lorsque vous ajoutez une nouvelle règle, les données opérationnelles statiques de la règle s'affichent. La colonne universally unique identifier (identifiant unique universel ; UUID) affiche l'UUID à 36 caractères pour la règle. Le pare-feu génère l'UUID par règle. Cependant, si vous transférez des règles de Panorama, ces règles possèdent le même UUID, qui s'affiche également dans la prévisualisation des règles combinées. La colonne **Created (Créé)** affiche l'heure et la date auxquelles la règle a été ajoutée à la base de règles. De plus, la colonne **Modified (Modifié)** affiche l'heure et la date de la dernière modification de la règle. Si une règle de politique a été créée avant la mise à niveau vers PAN-OS 9.0, les premières données de **First Hit (Première correspondance)** sont utilisées pour établir la date de **Created (Création)**. Si aucune donnée de **First Hit (Première correspondance)** n'est disponible pour la règle, l'heure et la date de la mise à niveau du serveur de gestion de Panorama ou du pare-feu vers PAN-OS 9.0 sont utilisées pour établir la date de **Created (Création)**.

Lorsque vous ajoutez ou modifiez une règle dans Panorama, un onglet **Cible** s'affiche. Vous pouvez utiliser cet onglet pour appliquer la règle à des pare-feu spécifiques ou à des groupes de périphériques descendants du **Groupe de périphériques** (Ou emplacement partagé) où la règle est définie. Dans l'onglet **Target (Cible)**, vous pouvez sélectionner **Any (Tout)** (par défaut), ce qui signifie que la règle s'applique à tous les pare-feu et à tous les groupes de périphériques descendants. Pour cibler des pare-feu ou des groupes de périphériques spécifiques, décochez **Any (Tout)** et sélectionnez le nom des pare-feu ou des groupes de périphériques souhaités. Pour exclure des pare-feu spécifiques ou des groupes de périphériques, décochez **Any (Tout),** sélectionnez le nom des pare-feu ou des groupes de périphériques souhaités, puis sélectionnez **Target to all but these specified devices (Cibler tous les périphériques sauf ceux spécifiés)**. Si la liste des groupes de périphériques et des pare-feu est longue, vous pouvez appliquer des Filtres pour rechercher les saisies par attributs (telles que les Plates-formes) ou par chaîne de texte pour les noms correspondants.

Après que vous avez ajouté et appliqué une règle à Panorama, **Rule Usage (Utilisation d'une règle)** indique si la règle est Utilisée par tous les périphériques du groupe de périphériques, Partiellement utilisée par certains périphériques du groupes de périphériques ou Inutilisée par les périphériques du groupes

© 2020 Palo Alto Networks, Inc.

de périphériques. Panorama détermine l'utilisation d'une règle en fonction des pare-feu gérés dont le Nombre de correspondance à la règle de politique est activé (activé par défaut). Dans le contexte de Panorama, vous pouvez afficher l'utilisation d'une règle pour une règle de politique partagée sur tous les groupes de périphériques. De plus, vous pouvez modifier le contexte afin de choisir un groupe de périphériques individuels et consulter l'utilisation totale d'une règle de politique sur l'ensemble des périphériques qui forment le groupe de périphériques. **Preview Rules (Prévisualiser les règles)** présentera le **Hit Count (Nombre de correspondances)**, la **Last Hit (Dernière correspondance)** et la **First Hit (Première correspondance)** de chaque règle de politique d'un groupe de périphériques. Le nombre total de mise en correspondance du trafic ainsi les horodatages de la première et de la dernière correspondances perdurent après le redémarrage, la mise à niveau et le rédémarrage du panneau de données. Voir Surveiller l'utilisation d'une règle de politique.

Group Rules by Tag (Regroupez des règles par étiquette) pour appliquer une étiquette qui vous permet de regrouper des règles de politique similaires pour obtenir une meilleure vision des fonctions des règles et faciliter la gestion des règles de politique à l'échelle de la base de règles. Les règles regroupées par étiquettes présentent la liste des groupes d'étiquettes, tout en préservant la liste de priorité des règles. Vous pouvez ajouter les règles à la fin d'un groupe d'étiquettes, déplacer des règles vers un autre groupe d'étiquettes, appliquer des étiquettes supplémentaires aux règles d'un groupe d'étiquettes et filtrer ou effectuer des recherches à l'aide du groupe d'étiquettes.

Pour suivre les changements apportés aux règles de politique, ajoutez un **Audit Comment (Commentaire d'audit)** pour décrire les changements que vous apportez et les raisons pour lesquelles une règle a été créée ou modifiée. Une fois le commentaire d'audit saisi et le changement de configuration validé, le commentaire d'audit est préservé dans le **Audit Comment Archive (Archive des commentaires d'audit)**, où vous pouvez consulter tous les commentaires d'audit précédents pour la règle sélectionnée. Vous pouvez chercher le commentaire d'audit dans la recherche globale. L'archive des commentaires d'audit est en lecture seule.

Les utilisateurs administratifs qui ont accès à l'onglet Politiques peuvent exporter les règles de politique qui sont affichées sur l'interface Web au format **PDF/CSV**. Consultez la section Exportation des données du tableau de configuration.

Pour créer des politiques, reportez-vous à la section correspondante à chaque base de règles'A0;:

- Politiques > Sécurité
- Politiques > NAT
- Politiques > QoS
- Politiques > Transfert basé sur une politique
- Politiques > Déchiffrement
- Politiques > Contrôle prioritaire sur l'application
- Politiques > Authentification
- Politiques > Protection'A0;DoS
- Politiques > SD-WAN

© 2020 Palo Alto Networks, Inc.

Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité

- Panorama > Configuration > Opérations

Par défaut, un appareil virtuel Panorama en mode Hérité comporte une partition de disque unique pour toutes les données et 10,89 Go de cet espace est affecté au stockage de journaux. Accroître la taille du disque n'augmente pas la capacité de stockage des journaux ; cependant, vous pouvez modifier la capacité de stockage des journaux grâce aux options suivantes :

- **Système de fichiers réseau (NFS)** – l'option de montage du stockage NFS n'est disponible que pour les appareils virtuels Panorama en mode héritage et fonctionnant sur un serveur VMware ESXi. Pour monter le stockage NFS, sélectionnez **Storage Partition Setup (Paramétrage de la partition de stockage)** dans la section Divers, définissez la **Storage Partition (Partition de stockage)** sur **NFS V3** et configurez les paramètres comme décrit dans le Tableau : Paramètres de stockage NFS.
- **Stockage interne par défaut** – rétablissez la partition de stockage interne par défaut (applicable uniquement à Panorama sur un serveur ESXi ou sur la plateforme vCloud Air où vous avez précédemment configuré un autre disque de journaux virtuel ou monté sur un NFS). Pour revenir à la partition de stockage interne par défaut, sélectionnez **Configuration de la partition de stockage** dans la section Divers et définissez la **Partition de stockage** sur **Interne**.
- **Disque de journal virtuel** – vous pouvez Ajouter un autre disque virtuel (jusqu'à 8 To) pour Panorama fonctionnant sous VMware ESXi (versions 5.5 et ultérieures) ou pour Panorama fonctionnant sous la plateforme VMware vCloud Air. Par conséquent, Panorama cesse d'utiliser le stockage de journaux de 10,89 Go par défaut sur le disque d'origine et copie tous les journaux existants sur le nouveau disque. (Les versions ESXi antérieures prennent uniquement en charge les disques virtuels de 2 To maximum).

Vous devez redémarrer Panorama après avoir modifié les paramètres de la partition de stockage : sélectionnez Panorama > Setup (Configuration) > Operations (Opérations) et Reboot Panorama (Redémarrer Panorama).

Le stockage NFS n'est pas disponible pour l'appareil virtuel Panorama en mode Panorama ou pour les appareils M-Series.

Table 1: Tableau : Paramètres de stockage NFS

Paramètres de partition de stockage Panorama – NFS V3	Description
Serveur	Indiquez le nom de domaine complet ou l'adresse IP du serveur NFS.
Répertoire des journaux	Précisez le chemin d'accès complet du répertoire dans lequel les journaux seront stockés.
Protocole	Précisez le protocole (UDP ou TCP) de communication avec le serveur NFS.
Port	Précisez le port de communication avec le serveur NFS.

© 2020 Palo Alto Networks, Inc.

Paramètres de partition de stockage Panorama – NFS V3	Description
Taille de lecture	Précisez la taille maximum en octets (intervalle compris entre 256 et 32 768) des opérations de lecture NFS.
Taille d'écriture	Précisez la taille maximum en octets (intervalle compris entre 256 et 32 768) des opérations d'écriture NFS.
Copier lors de la configuration	Sélectionnez pour monter la partition NFS et pour copier les journaux existants dans le répertoire de destination sur le serveur au démarrage de Panorama.
Partition de journalisation test	Sélectionnez pour tester le montage de la partition NFS et afficher un message de réussite ou d'échec.

© 2020 Palo Alto Networks, Inc.

Panorama > Configuration > Interfaces

Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** pour configurer les interfaces que Panorama utilise pour gérer les pare-feu et les Collecteurs de journaux, déployer des logiciels et des mises à jour de contenu sur les pare-feu et les Collecteurs de journaux, collecter les journaux des pare-feu et communiquer avec les Groupes de collecteurs. Par défaut, Panorama utilise l'interface MGT pour toutes les communications avec les pare-feu et les Collecteurs de journaux.

Pour réduire le trafic sur l'interface MGT, configurez d'autres interfaces pour qu'elles déploient des mises à jour, collectent des journaux et communiquent avec les Groupes de collecteurs. Dans un environnement avec un trafic de journaux important, vous pouvez configurer plusieurs interfaces pour la collecte des journaux. De plus, pour améliorer la sécurité du trafic de gestion, vous pouvez définir un sous-réseau distinct (Masque réseau IPv4 ou Longueur de préfixe IPv6) pour l'interface MGT, qui est plus privé que les sous-réseaux pour les autres interfaces.

Les interfaces disponibles varient en fonction du modèle Panorama.

Interface	Vitesse maximum	Appareil M-500	Appareil virtuel Panorama
Management (MGT)	1 Gbits/s	✓	✓
Ethernet1 (Eth1)	1 Gbits/s	✓	—
Ethernet2 (Eth2)	1 Gbits/s	✓	—
Ethernet3 (Eth3)	1 Gbits/s	✓	—
Ethernet4 (Eth4)	10 Gbits/s	✓	—
Ethernet5 (Eth5)	10 Gbits/s	✓	—

Pour configurer une interface, cliquez sur le Nom de l'interface et configurez les paramètres décrits dans le tableau suivant.

Spécifiez toujours l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) ainsi que la passerelle par défaut pour l'interface MGT. Si vous omettez des valeurs pour certains paramètres (comme la passerelle par défaut), vous pouvez uniquement accéder à Panorama via le port de la console pour des modifications ultérieures de la configuration. Vous ne pouvez pas valider les configurations pour d'autres interfaces, sauf si vous spécifiez les trois paramètres.

Paramètres de l'interface	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Vous devez activer une interface pour la configurer. L'interface de gestion est une exception car elle est activée par défaut.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'interface	Description
Adresse IP publique	Si vos pare-feux se connectent à Panorama en utilisant une adresse IP publique qui est translatée en une adresse IP privée (NAT), saisissez l'adresse IP publique de l'interface.
Adresse'A0;IP (IPv4)	Si votre réseau utilise IPv4, affectez une adresse IPv4 à l'interface.
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:400:f00::1/64).  *Une adresse IPv6 est prise en charge pour l'interface MGT par tous les appareils M-Series et les appareils virtuels Panorama déployés dans un environnement de cloud privé (ESXi, vCloud Air, KVM, Hyper-V). Une adresse IPv6 n'est pas prise en charge pour l'interface MGT par un appareil virtuel Panorama déployé dans un environnement de cloud public (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, and Google Cloud Platform).*
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).  *Une adresse IPv6 est prise en charge pour l'interface MGT par tous les appareils M-Series et les appareils virtuels Panorama déployés dans un environnement de cloud privé (ESXi, vCloud Air, KVM, Hyper-V). Une adresse IPv6 n'est pas prise en charge pour l'interface MGT par un appareil virtuel Panorama déployé dans un environnement de cloud public (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, and Google Cloud Platform).*
Vitesse	Réglez la vitesse pour l'interface à 10 Mbit/s, 100 Mbit/s, 1 Gbit/s ou 10 Gbit/s (Eth4 et Eth5 uniquement) en duplex intégral ou semi-duplex. Utilisez le paramètre de négociation automatique par défaut pour que Panorama détermine la vitesse de l'interface.  *Ce paramètre doit correspondre aux paramètres de l'interface de l'équipement réseau voisin. Pour assurer les paramètres de mappage, sélectionnez la négociation automatique si l'équipement voisin prend en charge cette option.*

© 2020 Palo Alto Networks, Inc.

Paramètres de l'interface	Description
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Gestion des périphériques et collecte des journaux de périphérique	Activez l'interface (activée par défaut sur l'interface MGT) pour gérer les pare-feu et les Collecteurs de journaux et collecter leurs journaux. Vous pouvez activer plusieurs interfaces pour effectuer ces fonctions.
Communication avec les groupes de collecteurs	Activez l'interface pour la communication de Groupe de collecteurs (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Déploiement de périphériques	Activez l'interface pour le déploiement de logiciels et de mises à jour de contenu sur les pare-feu et les Collecteurs de journaux (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Services de gestion administrative	• **HTTP** - Autorise l'accès à l'interface Web de Panorama. HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS.  *Activez le protocole HTTPS plutôt que le protocole HTTP pour le trafic de gestion sur l'interface.* • **Telnet** - Autorise l'accès à l'ILC (interface de ligne de commande) de Panorama. Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. • **HTTPS** - Autorise l'accès sécurisé à l'interface Web de Panorama.  *Activez le protocole SSH plutôt que le protocole de Telnet pour le trafic de gestion sur l'interface.* • **SSH** – Permet un accès sécurisé à l'interface de ligne de commande Panorama.
Services de connexion réseau	Le service **Ping** est disponible sur n'importe quelle interface. Vous pouvez utiliser le ping pour tester la connectivité entre l'interface Panorama et les services externes. Dans un déploiement haute disponibilité (HD), les pairs HA utilisent l'envoi de ping pour échanger de l'information sur la sauvegarde de pulsation. Les services suivants sont uniquement disponibles sur l'interface MGT : • **SNMP** - Permet à Panorama de traiter les requêtes de statistiques d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – Permet à Panorama de redistribuer les informations de mappage d'utilisateur reçues des agents User-ID.
Adresses IP autorisées	Saisissez les adresses IP à partir desquelles les administrateurs peuvent accéder à Panorama sur cette interface. Une liste vide (par défaut) indique que l'accès est possible à partir de n'importe quelle adresse IP.

© 2020 Palo Alto Networks, Inc.

Paramètres de l'interface	Description
	Ne laissez pas cette liste vide. Spécifiez les adresses IP des administrateurs Panorama (uniquement) pour empêcher tout accès non autorisé.

© 2020 Palo Alto Networks, Inc.

Panorama > Haute disponibilité

Pour autoriser la haute disponibilité (HD) sur Panorama, configurez les paramètres comme décrits dans le tableau suivant.

Paramètres HA de Panorama	Description
setup Cliquez sur Modifier ( ) pour configurer les paramètres suivants.	
Activer la HA	Sélectionnez cette action pour activer HA.
Adresse IP des HA homologues	Saisissez l'adresse IP de l'interface MGT de l'homologue.
Activer le chiffrement	Lorsque le chiffrement est activé, l'interface MGT crypte la communication entre les homologues HA. Avant d'activer le chiffrement, exportez la clé HA de chacun des homologues HA et importez-la vers l'autre homologue. Vous importez et exportez la clé HD sur la page **Panorama** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** (voir Gestion des certificats du pare-feu et de Panorama). *La connectivité HA utilise le port TCP 28 avec le chiffrement activé et le port TCP 28769 lorsque le chiffrement n'est pas activé.*
Temps d'attente pour la surveillance (ms)	Saisissez le nombre de millisecondes d'attente du système avant d'intervenir à la suite d'un échec de la liaison de contrôle (plage de 1 000 à 60 000 ; valeur par défaut de 3 000).
Paramètres de sélection Cliquez sur Modifier ( ) pour configurer les paramètres suivants.	
Priorité (Obligatoire sur l'équipement virtuel Panorama)	Ce paramètre détermine l'homologue principal pour la réception des journaux du pare-feu. Désignez un homologue **Primary (Principal)** et un homologue **Secondary (Secondaire)** dans la paire HA. Lorsque vous configurez les Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité, vous pouvez utiliser son disque interne (par défaut) ou un système de fichiers réseau (NFS) pour le stockage des journaux. Si vous configurez un NFS, seul le destinataire principal reçoit les journaux du pare-feu. Si vous configurez la mémoire interne du disque, les pare-feu envoient par défaut des journaux à l'homologue primaire et secondaire, mais vous pouvez le modifier en activant **Only Active Primary Logs to Local Disk (Seulement les journaux actifs principaux sur le disque local)** dans les Paramètres de journalisation et de génération de rapports.
Préemptif	Sélectionnez cette option pour permettre à l'homologue Panorama principal de reprendre l'état actif après la récupération d'un échec. Si ce paramètre est

© 2020 Palo Alto Networks, Inc.

Paramètres HA de Panorama	Description
	désactivé, l'homologue Panorama secondaire reste actif même si l'homologue Panorama principal récupère d'un échec.
Paramètres du minuteur de haute disponibilité	Votre sélection détermine les valeurs des paramètres de sélection HA restants, qui contrôlent la vitesse de basculement : • **Recommended (Recommandé)** - Sélectionnez cette option pour les paramètres types du minuteur de basculement (par défaut). Pour visualiser les valeurs associées, sélectionnez **Advanced (Avancé)** et **Load Recommended (Charger le profil recommandé)**. • **Aggressive (Agressif)** - Sélectionnez cette option pour des paramètres plus rapides du minuteur de basculement. Pour visualiser les valeurs associées, sélectionnez **Advanced (Avancé)** et **Load Aggressive (Charger le profil agressif)**. • **Advanced (Avancé)** - Sélectionnez cette option pour afficher les paramètres de sélection HA restants et personnaliser leurs valeurs. Voir la valeur **recommandée** et **agressive** pour les paramètres suivants.
Délai de maintien de promotion (ms)	Saisissez le nombre de millisecondes (plage de 0 à 60 000) pendant lesquelles l'homologue Panorama secondaire attendra avant de prendre le relais après l'arrêt de l'homologue principal. La valeur recommandée (par défaut) est 2 000 ; la valeur du profil agressif est 500.
Intervalle Hello (ms)	Saisissez le nombre de millisecondes (plage de 8 000 to 60 000) entre chaque paquet Hello envoyé afin de vérifier que l'autre homologue est opérationnel. La valeur recommandée (par défaut) et la valeur du profil agressif est 8 000.
Intervalle de pulsation (ms)	Précisez la fréquence en millisecondes (plage de 1 000 to 60 000) à laquelle Panorama envoie des pings ICMP à l'homologue HA. La valeur recommandée (par défaut) est 2 000 ; la valeur du profil agressif est de 1 000.
Délai de maintien de préemption (min)	Ce champ s'applique uniquement si vous sélectionnez également l'option **Preemptive (Préemptif)**. Saisissez le nombre de minutes (plage de 1 à 60) pendant lesquelles l'homologue Panorama passif attendra avant de revenir à l'état actif après avoir récupéré d'un événement ayant entraîné un basculement. La valeur recommandée (par défaut) et la valeur du profil agressif est de 1.
Temps d'attente actif après l'échec de la surveillance (ms)	Précisez le nombre de millisecondes (plage de 0 à 60 000) pendant lesquelles Panorama attendra avant d'essayer de passer de nouveau à l'état passif après l'échec de surveillance du chemin. Pendant cette période, l'homologue passif ne peut pas prendre l'état actif en cas d'échec. Cet intervalle permet à Panorama d'empêcher un basculement dû au battement occasionnel de périphériques à proximité. La valeur recommandée (par défaut) et la valeur du profil agressif est de 0.
Temps d'attente actif principal supplémentaire (ms)	Précisez le nombre de millisecondes (plage de 0 à 60 000) pendant que lesquelles l'homologue de préemption reste à l'état passif avant de devenir l'homologue actif. La valeur recommandée (par défaut) est de 7 000 ; la valeur du profil agressif est de 5 000.

© 2020 Palo Alto Networks, Inc.

Paramètres HA de Panorama	Description
Surveillance des chemins Cliquez sur Modifier ( ) pour configurer la Surveillance des chemins HA.	
Activé	Sélectionnez cette option pour activer la surveillance des chemins. La surveillance des chemins permet à Panorama de surveiller les adresses IP de destination définies en envoyant des messages ping ICMP afin de vérifier qu'elles répondent.
Condition d'échec	Sélectionnez cette option en cas d'échec lorsqu'**Any (Un)** ou **All (Tous)** les groupes de chemins surveillés ne répondent pas.
Groupe de chemins Pour créer un groupe de chemins pour la surveillance de chemins HA, cliquez sur **Add (Ajouter)** et remplissez les champs suivants.	
Name (Nom)	Donnez un nom au groupe de chemins.
Activé	Sélectionnez cette option pour activer le groupe de chemins.
Condition d'échec	Sélectionnez cette option en cas d'échec lorsqu'**Any (Une)** ou **All (Toutes)** les adresses de destination précisées ne répondent pas.
Intervalle des requêtes ping	Précisez le nombre de millisecondes entre les messages echo ICMP qui vérifient que le chemin vers l'adresse de destination est disponible (plage de 1 000 à 60 000 ; valeur par défaut de 5 000).
Nombre de requêtes ping	Précisez le nombre d'échecs de requêtes ping avant de déclarer un échec (plage de 3 à 10 ; valeur par défaut de 3).
Adresses IP de destination	Saisissiez une ou plusieurs adresses IP de destination à surveiller. Utilisez un point-virgule pour séparer plusieurs adresses.

© 2020 Palo Alto Networks, Inc.

Panorama > Clusters WildFire gérés

- Panorama > Clusters WildFire gérés
- Panorama > Appareils WildFire gérés

Vous pouvez gérer les appareils WildFire en clusters ou en tant qu'appareils autonomes, et ce depuis des appareils Panorama virtuels ou de série M. La gestion des clusters (**Panorama** > **Clusters WildFire gérés**) et la gestion des appareils autonomes (**Panorama** > **Appareils WildFire gérés**) ont en commun de nombreuses tâches administratives et de configuration courantes. Ainsi, ces deux gestions figurent dans les rubriques qui suivent.

Après avoir ajouté les appareils WildFire à Panorama, utilisez l'interface Web pour ajouter ces appareils et les gérer en tant que clusters ou pour les gérer en tant qu'appareils autonomes.

- Tâches des clusters WildFire gérés
- Tâches de l'appareil WildFire géré
- Informations WildFire gérées
- Cluster WildFire géré et administration de l'appareil

Tâches des clusters WildFire gérés

Vous pouvez créer et supprimer des clusters d'appareils WildFire à partir de Panorama. Vous pouvez également gagner du temps lors de la configuration en important des configurations d'un cluster à l'autre.

Tâche	Description
Créer un cluster	Si nécessaire, **Créez un cluster**, saisissez un nom pour le nouveau cluster, puis cliquez sur **OK**. Les clusters existants que vous avez configurés localement et ajoutés à Panorama en ajoutant les nœuds d'appareils WildFire individuels sont répertoriés avec leurs nœuds WildFire et les rôles des nœuds (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**). Le nom du cluster doit être un nom de sous-domaine valide commençant par un caractère ou un chiffre minuscule. Ce nom ne peut contenir des traits d'union que s'ils ne correspondent pas au premier ou au dernier caractère du nom du cluster. Aucun espace ou autre caractère n'est autorisé. La longueur maximale d'un nom de cluster est de 63 caractères. Après avoir créé un cluster, vous pouvez ajouter des appareils WildFire gérés au cluster et les gérer sur Panorama. Lorsque vous ajoutez un appareil WildFire à Panorama, vous enregistrez automatiquement l'appareil avec Panorama. Vous pouvez créer un maximum de 10 clusters WildFire gérés sur Panorama ; chaque cluster peut contenir jusqu'à 20 nœuds d'appareils WildFire. Panorama peut gérer jusqu'à un total cumulatif de 200 appareils autonomes et nœuds de cluster.
Importer la config. du cluster	**Importer la Configuration du cluster** pour importer une configuration de cluster existante. Si vous sélectionnez un cluster avant d'**Importer la Configuration du cluster,** les informations appropriées pour le cluster sélectionné sont automatiquement renseignées dans le **Contrôleur** et le **Cluster**. Si vous ne sélectionnez pas un cluster avant d'**Importer la**

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	Configuration du cluster, vous devez sélectionner le **Contrôleur** et le **Cluster** se complète automatiquement en fonction du nœud de Contrôleur que vous sélectionnez. Après avoir importé la configuration, **Validez sur Panorama** pour sauvegarder la configuration candidate importée dans la configuration d'exécution Panorama.
Supprimer de Panorama	Si vous n'avez plus besoin de gérer un cluster WildFire à partir de Panorama, cliquez sur **Supprimer de Panorama** et sélectionnez **Oui** pour confirmer votre action. Après avoir supprimé un cluster de la gestion de Panorama, vous pouvez gérer le cluster localement à partir d'un nœud de Contrôleur. Vous pouvez à tout moment rajouter le cluster dans l'appareil Panorama si vous souhaitez à nouveau gérer le cluster au niveau central plutôt que local.
Crypter les communications entre appareils au sein du cluster WildFire	Pour crypter la communication de données entre les appareils WildFire d'un cluster, **Enable (Activer)** le chiffrement sous **Secure Cluster Communication (Communication sécurisée avec le cluster)**. WildFire utilise un certificat prédéfini ou un certificat personnalisé pour la communication entre les appareils. Les certificat personnalisé ne sont utilisés que lorsque vous **Customize Secure Server Communication (Personnalisez la communication sécurisée avec le serveur)** et activez l'option **Custom Certificate Only (Certificat personnalisé uniquement)**. Le chiffrement est obligatoire pour que les clusters WildFire fonctionnent en mode FIPS-CC. Les certificats personnalisés utilisés en mode FIPS-CC doivent respecter les exigences FIPS-CC. Après avoir activé la communication sécurisée avec le cluster, vous pouvez ajouter d'autres appareils WildFire gérés au cluster. Les appareils nouvellement ajoutés utilisent les paramètres de la communication sécurisée avec le cluster.

Tâches de l'appareil WildFire géré

Vous pouvez ajouter, supprimer et gérer des appareils WildFire autonomes sur un périphérique Panorama. Après avoir ajouté des appareils autonomes, vous pouvez les ajouter aux clusters d'appareils WildFire en tant que nœuds cluster ou vous pouvez les gérer en tant que périphériques autonomes individuels.

Tâche	Description
Ajouter un appareil	**Ajoutez un appareil** pour ajouter un ou plusieurs appareils WildFire à un appareil Panorama pour une gestion centralisée. Saisissez le numéro de série de chaque appareil WildFire sur une ligne séparée (nouvelle ligne). Panorama peut gérer jusqu'à un total cumulatif de 200 nœuds cluster WildFire et d'appareils WildFire autonomes. Sur chaque appareil WildFire que vous souhaitez gérer sur Panorama, configurez l'adresse IP ou FQDN de l'appareil Panorama (serveur Panorama) et, le cas échéant, le serveur Panorama de sauvegarde en utilisant les commandes suivantes de la CLI de l'appareil WildFire :

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	set deviceconfig system panorama-server *<ip-address | FQDN>* set deviceconfig system panorama-server-2 *<ip-address | FQDN>*
Importer la configuration	Sélectionnez un appareil WildFire et une **Configuration d'importation** pour importer (uniquement) vers Panorama la configuration en cours d'exécution pour cet appareil. Après avoir importé la configuration, **Validez sur Panorama** pour sauvegarder la configuration candidate importée dans la configuration d'exécution Panorama.
Supprimer	Si vous n'avez plus besoin de gérer un appareil WildFire à partir de Panorama, **Retirez** l'appareil et sélectionnez **Oui** pour confirmer votre action. Après avoir supprimé un appareil de la gestion de Panorama, vous pouvez gérer l'appareil localement à l'aide de sa CLI. Si nécessaire, vous pouvez rajouter l'appareil à tout moment à l'appareil Panorama si vous souhaitez gérer à nouveau l'appareil au niveau central plutôt que local.

Informations WildFire gérées

Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** pour afficher les informations suivantes pour chaque cluster géré (vous pouvez également sélectionner des appareils autonomes à partir de cette page et afficher les informations s'y rapportant) ou sélectionnez **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** pour afficher les informations pour les appareils autonomes.

Sauf indication contraire, les informations reprises dans le tableau suivant s'appliquent tant aux clusters WildFire qu'aux appareils autonomes. Les informations précédemment configurées pour un cluster ou un appareil sont prérenseignées.

Informations WildFire gérées	Description
Appareil	Le nom de l'appareil. L'affichage Clusters WildFire gérés indique les appareils regroupés par cluster, inclut les appareils autonomes qu'il est possible d'ajouter à un cluster et mentionne le numéro de série (entre parenthèses) avec le nom de l'appareil (le numéro de série ne fait pas partie du nom).
Numéro de série (affichage des appareils WildFire gérés uniquement)	Le numéro de série de l'appareil. L'affichage Clusters WildFire gérés indique le numéro de série dans la même colonne que le nom de l'appareil (le numéro de série ne fait pas partie du nom).
Version du logiciel	La version du logiciel installée et en cours d'exécution sur l'appareil.
Adresse IP	L'adresse IP de l'appareil.

© 2020 Palo Alto Networks, Inc.

Informations WildFire gérées	Description
Connected (Connecté)	Le statut de la connexion entre l'appareil et Panorama ; soit Connecté soit Déconnecté.
Nom du cluster	Le nom du cluster dans lequel l'appareil est inclus comme nœud ; dans le cas d'un appareil autonome, rien ne s'affiche.
Environnement d'analyse	L'environnement d'analyse (vm-1, vm-2, vm-3, vm-4 ou vm-5). Chaque environnement d'analyse représente un ensemble de systèmes d'exploitation et d'applications : • vm-1 prend en charge Windows XP, Adobe Reader 9.3.3, Flash 9, PE, PDF, Office 2003 et les versions antérieures d'Office ; • vm-2 prend en charge Windows XP, Adobe Reader 9.4.0, Flash 10n, PE, PDF, Office 2007 et les versions antérieures d'Office ; • vm-3 prend en charge Windows XP, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office ; • vm-4 prend en charge Windows 7 32 bits, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office. • vm-5 prend en charge Windows 7 64 bits, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office.
Contenu	Le numéro de version de la version du contenu.
Rôle	Le rôle de l'appareil : • **Autonome** – L'appareil n'est pas un nœud de cluster. • **Contrôleur** – L'appareil est le nœud de Contrôleur du cluster. • **SauvegardeContrôleur du </** – L'appareil est le nœud de secours du Contrôleur du cluster. • **Subordonné** – L'appareil est un nœud dans le cluster.
État de config.	Le statut de la synchronisation de la configuration de l'appareil. L'appareil Panorama vérifie les paramètres de l'appareil WildFire et signale les différences de configuration entre la configuration de l'appareil et celle enregistrée sur Panorama pour cet appareil. • **Synchronisé** – La configuration de l'appareil est synchronisée avec sa configuration enregistrée sur Panorama. • **Désynchronisés** – La configuration de l'appareil n'est pas synchronisée avec sa configuration enregistrée sur Panorama. Vous pouvez placer votre souris sur la loupe pour afficher la cause de l'échec de la synchronisation.
État du cluster (page clusters WildFire gérés uniquement)	Le Statut du cluster affiche trois types d'informations pour chaque nœud de cluster : • services disponibles (conditions de fonctionnement normales) : • **wfpc** (WildFire Private Cloud) – Le service d'analyse et de rapportage d'échantillons de logiciels malveillants, • **signature** – Le service de génération de signature locale. • progression des opérations – Le nom de l'opération suivi de deux points (:) et du statut :

© 2020 Palo Alto Networks, Inc.

Informations WildFire gérées	Description
	• **opérations** – Statut de la désactivation, de la suspension et du redémarrage des opérations, • **statut de la progression** – Les notifications du statut de l'opération sont identiques pour chaque opération : demandée, en cours, refusée, réussie ou échouée. Par exemple, si vous suspendez un nœud et que l'opération est en cours, le Statut du cluster affichera `Suspension : en cours` ou, si vous redémarrez un nœud et que l'opération a été demandée, mais qu'elle n'a pas encore commencé, le Statut du cluster affichera `Redémarrage : demandé`. • conditions d'erreur : Le Statut du cluster affiche les conditions d'erreur suivantes : • **cluster** – `cluster : hors ligne` ou `cluster : split-brain`, • **service** – `service : suspendu` ou `service : aucun`.
État de la dernière validation	`Réussite de la validation` si la dernière validation a réussi ou `Échec de la validation` si la validation la plus récente a échoué. Visualisez les détails de la dernière validation en sélectionnant le statut.
Utilisation > Visualisation	
Vue	**Visionnez** les statistiques d'utilisation des clusters ou des appareils. Vous pouvez visualiser les appareils individuels uniquement (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) ou vous pouvez visualiser les statistiques du cluster uniquement (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)**). • **Appareil** – (affichage Appareil autonome uniquement) Le numéro de série de l'appareil. • **Cluster** – (affichage Cluster uniquement) Le nom du cluster. Vous pouvez également sélectionner un autre cluster à afficher. • **Durée** – Affiche la période pendant laquelle les statistiques sont recueillies et affichées. Vous pouvez sélectionner différentes durées : • **15 min.** • **Dernière heure** • **24 dernières heures (par défaut) ;** • **7 derniers jours** • **Toutes** L'**Affichage Utilisation** dispose de quatre onglets ; vous pouvez déterminer ce qui s'affiche pour chaque onglet en fonction de la **Durée** que vous avez configurée.
Onglet Général	L'onglet **Général** affiche les statistiques d'utilisation des ressources agrégées pour un cluster ou un appareil. Les autres onglets affichent des informations plus granulaires concernant l'utilisation des ressources par type de fichier : • **Utilisation totale du disque** – L'utilisation totale du disque du cluster ou de l'appareil.

© 2020 Palo Alto Networks, Inc.

Informations WildFire gérées	Description
	• **Verdict** – Le nombre **Total** de verdicts, le nombre de verdicts de chaque type attribués aux fichiers (**Malveillant**, **Grayware** et **Bénin**) et combien de verdicts étaient des verdicts d'**Erreur**. • **Statistiques des échantillons** – Le nombre total d'échantillons **Soumis** et **Analysés** ainsi que le nombre d'échantillons **En attente** d'analyse. • **Analysis Environment & System Utilization (Environnement d'analyse et utilisation du système)** : • **Type de fichier analysé** – Le type de fichier qui a été analysé : **Exécutable**, **Non exécutable** ou **Liens**. • **Utilisation des machines virtuelles** – Le nombre de machines virtuelles utilisées pour chaque type de fichier analysé et le nombre de machines virtuelles disponibles pour analyser chaque type de fichier. Par exemple, pour les fichiers Exécutables, l'utilisation des machines virtuelles pourrait être de 6/10 (six machines virtuelles utilisées et dix disponibles). • **Fichiers analysés** – Le nombre de fichiers de chaque type qui ont été analysés.
Onglets Exécutables, Non exécutables et Liens	Les onglets **Executable (Exécutable)**, **Non-Executable (Non exécutable)** et **Links (Liens)** affichent des informations similaires à propos de chaque type de fichier : • **verdict** – Détails sur les verdicts par type de fichier. Vous pouvez filtrer les résultats : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer les verdicts. La barre de recherche indique le nombre de types de fichiers (éléments) dans la liste. Après avoir saisi les termes de recherche, appliquez le filtre ( ) ou effacez le filtre ( ) et saisissez une autre suite de termes. • **Type de fichier** – Liste des fichiers par type. Par exemple, l'onglet **Exécutable** affiche les fichiers de type .exe et .dll ; l'onglet **Non exécutable** affiche les fichiers de type .pdf, .jar, .doc, .ppt, .xls, .docx, .pptx, .xlsx, .rtf, class et .swf; et l'onglet **Liens** affiche les informations des fichiers de type elink. • Le nombre total de verdicts pour les fichiers **Malveillants**, **Grayware** et **Bénins**, le nombre de verdicts d'**Erreur** et le nombre **Total** de verdicts sont affichés sous chaque onglet pour chaque **Type de fichier**. • **Statistiques des échantillons** – Détails à propos de l'analyse des échantillons par type de fichier. • **Barre de recherche** – Même chose que la barre de recherche pour les **Verdicts**. • **Type de fichier** – Même chose que le **Type de fichier** pour les **Verdicts**. • Le nombre total de fichiers **Soumis** pour analyse, le nombre total de fichiers **Analysés** et le nombre de fichiers **En attente** d'analyse sont affichés sous chaque onglet pour chaque **Type de fichier**.
Pare-feu connectés > Affichage	

© 2020 Palo Alto Networks, Inc.

Informations WildFire gérées	Description
Vue	**Affiche** des informations concernant les pare-feu connectés au cluster ou à l'appareil. Vous pouvez visualiser les appareils individuels uniquement (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) ou vous pouvez visualiser les statistiques du cluster uniquement (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)**). • **Appareil** – (affichage Appareil autonome uniquement) Le numéro de série de l'appareil. • **Cluster** – (affichage Cluster uniquement) Le nom du cluster ; vous pouvez également sélectionner un autre cluster à afficher. • **Actualiser** – Actualiser l'affichage.
Onglets Échantillons Enregistrés et En cours de soumission	L'onglet **Enregistrés** affiche des informations à propos des pare-feu enregistrés dans le cluster ou l'appareil, que les pare-feu soient en train de soumettre des échantillons ou non. L'onglet **Échantillons en cours de soumission** affiche des informations à propos des pare-feu qui soumettent activement des échantillons au cluster ou à l'appareil WildFire. Le type d'informations affichées sur ces onglets et la manière de filtrer ces informations sont identiques pour ces deux onglets : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des pare-feu. La barre de recherche indique le nombre de pare-feu (éléments) dans la liste. Après avoir saisi les termes de recherche, appliquez le filtre ( ) ou effacez le filtre ( ) et saisissez une autre suite de termes. • **S/N** – Le numéro de série du pare-feu. • **Adresse IP** – L'adresse IP du pare-feu. • **Modèle** – Le numéro de modèle du pare-feu. • **Version du logiciel** – La version du logiciel installée et en cours d'exécution sur le pare-feu.

Cluster WildFire géré et administration de l'appareil

Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez un cluster à gérer ou sélectionnez un appareil WildFire (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) pour gérer un appareil autonome. L'affichage **Panorama** > **Managed WildFire Cluster (Clusters WildFire gérés)** reprend les nœuds cluster (appareils WildFire membres du cluster) et les appareils autonomes pour que vous puissiez ajouter des appareils disponibles à un cluster. Étant donné que c'est le cluster qui gère les nœuds, sélectionner un nœud cluster ne fournit qu'une capacité de gestion limitée.

Sauf contre-indication, les paramètres et les descriptions dans le tableau suivant s'appliquent tant aux clusters WildFire qu'aux appareils autonomes WildFire. Les informations précédemment configurées sur un cluster ou un appareil sont prérenseignées. Vous devez d'abord valider les modifications et les ajouts et les intégrer aux informations qui figurent dans Panorama, puis appliquer la nouvelle configuration aux appareils.

Paramètre	Description
Onglet Général	

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
Name (Nom)	Le cluster ou le **Name (Nom)** de l'appareil ou le numéro de série de l'appareil.
Activer DNS (Clusters WildFire uniquement)	**Enable DNS (Activez le service DNS)** pour le cluster.
Enregistrer le pare-feu sur	Le nom de domaine dans lequel vous enregistrez des pare-feu. Le format doit être le suivant : **`wfpc.service.`***<nom-du-cluster>***`.`***<domaine>*. Par exemple, le nom de domaine par défaut est **`wfpc.service.mycluster.paloaltonetworks.com`**.
Serveur de mise à jour du contenu	Saisissez l'emplacement du **Content Update Server (Serveur de mise à jour de contenu)** ou utilisez la valeur par défaut **`wildfire.paloaltonetworks.com`** pour que le cluster ou l'appareil reçoive des mises à jour du contenu du serveur le plus proche au sein de l'infrastructure du Réseau de distribution de contenu. La connexion au cloud global vous permet d'accéder aux signatures et aux mises à jour en fonction de l'analyse des menaces de toutes les sources connectées au cloud, au lieu de se baser uniquement sur l'analyse des menaces locales.
Vérifier l'identité du serveur	**Check Server Identity (Vérifiez l'identité du serveur)** pour confirmer l'identité du serveur de mise à jour en faisant correspondre le nom commun (CN) dans le certificat avec l'adresse IP ou FQDN du serveur.
Serveur de cloud WildFire	Saisissez l'emplacement du **WildFire Cloud Server (Serveur de cloud WildFire)** global ou utilisez la valeur par défaut **`wildfire.paloaltonetworks.com`** pour que le cluster ou l'appareil puisse envoyer des informations au serveur le plus proche. Vous pouvez choisir si vous souhaitez envoyer des informations au nuage global et, si oui, quel type d'informations (**WildFire Cloud Services (Services de cloud WildFire)**).
Exemple d'image d'analyse	Sélectionnez l'image VM que le cluster ou l'appareil utilise pour l'analyse des échantillons (par défaut : vm-5). Vous pouvez Obtenir un fichier de test des logiciels malveillants (WildFire API) pour voir le résultat de l'analyse des échantillons.
Services de cloud WildFire	Si le cluster ou l'appareil est connecté au serveur de cloud global WildFire, vous pouvez choisir si vous souhaitez **Send Analysis Data (Envoyer des données d'analyse)**, **Send Malicious Samples (Envoyer des échantillons malveillants)** ou **Send Diagnostics (Envoyer des diagnostics)** au nuage global ou à une combinaison des trois. Vous pouvez choisir d'effectuer une **Verdict Lookup (Vérification des verdicts)** dans le nuage global. L'envoi d'informations dans le cloud global profite à toute la communauté d'utilisateurs WildFire, car les informations partagées augmentent la capacité de chaque appareil à identifier le trafic malveillant et à l'empêcher de traverser le réseau.
Conservation des données des échantillons	Nombre de jours de conservation d'échantillons bénins, grayware ou malveillants : • échantillons **Benign/Grayware (bénins / Grayware)** – plage de 1 à 90, 14 par défaut ;

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• échantillons **Malicious (malveillants)** – minimum de 1 et il n'y a pas de durée maximale (indéterminée) ; durée indéterminée par défaut.
Services d'environnement d'analyse	**Environment Networking (Réseaux environnementaux)** permet aux machines virtuelles de communiquer avec Internet. Vous pouvez sélectionner **Anonymous Networking (Réseaux anonymes)** pour que la communication réseau soit anonyme, mais vous devez sélectionner **Environment Networking (Réseaux environnementaux)** avant de pouvoir activer **Anonymous Networking (Réseaux anonymes)**. Différents environnements de réseau produisent différents types de charges d'analyse selon que d'autres documents ou fichiers exécutables doivent être analysés. Vous pouvez configurer votre Environnement d'analyse préféré pour allouer davantage de ressources à **Executables (Exécutables)** ou à **Documents** en fonction des besoins de votre environnement. L'allocation **Default (Par défaut)** est répartie entre **Executables (Exécutables)** et **Documents**. La quantité de ressources disponibles dépend du nombre de nœuds WildFire présents dans le cluster.
Génération de signatures	Sélectionnez si vous souhaitez que le cluster ou l'appareil génère des signatures pour AV, DNS ou URL, ou toute combinaison des trois.
Onglet Appareil	
Nom d'hôte (Appareils WildFire autonomes uniquement)	Saisissez le nom d'hôte de l'appareil WildFire.
Serveur Panorama	Saisissez l'adresse IP ou le nom de domaine complet de l'appareil ou du Panorama principal qui gère le cluster.
Serveur 2 de Panorama	Saisissez l'adresse IP ou le nom de domaine complet de l'appareil ou du Panorama de sauvegarde qui gère le cluster.
Domain (Domaine)	Saisissez le nom de domaine du cluster d'appareils ou de l'appareil.
Serveur DNS principal	Saisissez l'adresse IP du Serveur DNS principal.
Serveur DNS secondaire	Saisissez l'adresse IP du Serveur DNS secondaire.
Fuseau horaire	Sélectionnez le fuseau horaire à utiliser pour le cluster ou l'appareil.
Latitude (Appareils WildFire autonomes uniquement)	Saisissez la latitude de l'appareil WildFire.
Longitude	Saisissez la longitude de l'appareil WildFire.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
(Appareils WildFire autonomes uniquement)	
Serveur NTP principal	Saisissez l'adresse IP du serveur NTP principal et définissez le Type d'authentification sur **None (Aucun)** (par défaut), **Symmetric Key (Clé symétrique)** ou **Autokey (Clé automatique)**. Définir le Type d'authentification sur **Symmetric Key (Clé symétrique)** révèle quatre champs supplémentaires : • **Key ID (ID de la clé)** – saisissez l'ID de la clé d'authentification ; • **Algorithm (Algorithme)** – définissez l'algorithme d'authentification sur **SHA1** ou sur **MD5**. • **Authentication Key (Clé d'authentification)** – saisissez la clé d'authentification ; • **Confirm Authentication Key (Confirmer la clé d'authentification)** – saisissez à nouveau la clé d'authentification pour la confirmer.
Serveur NTP secondaire	Saisissez l'adresse IP du serveur NTP secondaire et définissez le Type d'authentification sur **None (Aucun)** (par défaut), **Symmetric Key (Clé symétrique)** ou **Autokey (Clé automatique)**. Définir le Type d'authentification sur **Symmetric Key (Clé symétrique)** révèle quatre champs supplémentaires : • **Key ID (ID de la clé)** – saisissez l'ID de la clé d'authentification ; • **Algorithm (Algorithme)** – définissez l'algorithme d'authentification sur **SHA1** ou sur **MD5**. • **Authentication Key (Clé d'authentification)** – saisissez la clé d'authentification ; • **Confirm Authentication Key (Confirmer la clé d'authentification)** – saisissez à nouveau la clé d'authentification pour la confirmer.
Bannière de connexion	Saisissez le message de bannière qui s'affichera lorsque les utilisateurs se connecteront au cluster ou à l'appareil.
Onglet Journaux (comprend l'onglet Système et l'onglet Configuration)	
Ajouter	**Add (Ajouter)** des profils de transfert des journaux (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** > <*cluster*> > **Logging (Journalisation)** > **System (Système)** ou **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** > <*cluster*> > **Logging (Journalisation)** > **Configuration**) à transmettre : • journaux de système ou de configuration lorsque SNMP génère des pièges aux récepteurs de pièges SNMP ; • messages Syslog aux serveurs Syslog ; • notifications par courrier électronique aux serveurs de messagerie ; • requêtes HTTP aux serveurs HTTP.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	Aucun autre type de journal n'est pris en charge (voir Périphériques > Paramètres des journauxl). Les profils de Transfert des journaux précisent les journaux à transmettre et les serveurs de destination. Pour chaque profil, procédez comme suit : • **Nom** – un nom qui identifie les paramètres des journaux (jusqu'à 31 caractères) uniquement composé de caractères alphanumériques et de traits de soulignement. Les espaces et les caractères spéciaux ne sont pas autorisés. • **Filtre** – par défaut, l'appareil Panorama transfère **Tous les journaux** du profil précisé. Pour transmettre un sous-ensemble de journaux, sélectionnez un filtre (**gravité EQ critique**, **gravité EQ élevée**, **gravité EQ informationnelle**, **gravité EQ basse** ou **gravité EQ moyenne**) ou sélectionnez **Générateur de filtrage** pour créer un nouveau filtre. • **Description** – saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but du profil.
Ajouter > Filtre > Générateur de filtrage	Utilisez **Générateur de filtrage** pour créer de nouveaux filtres de journaux. Sélectionnez **Créer un filtre** pour élaborer des filtres et, pour chaque requête dans un nouveau filtre, mentionnez les paramètres suivants, puis **Ajoutez** la requête : • **Connecteur** – Sélectionnez la logique de connecteur (**et** ou **ou**). Sélectionner **Refuser** si vous souhaitez appliquer un refus. Par exemple, pour éviter de transmettre un sous-ensemble de descriptions des journaux, sélectionnez **Description** en tant qu'Attribut, sélectionnez **Contient** en tant qu'Opérateur et saisissez la chaîne de description en tant que Valeur pour identifier la ou les description(s) que vous ne souhaitez pas transmettre. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options varient selon le type de journal. • **Opérateur** – Sélectionnez les critères qui déterminent comment un attribut s'applique (tel que « **contient** »). Les options varient selon le type de journal. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. • **Ajouter** – ajouter le nouveau filtre. Pour afficher ou exporter les journaux auxquels le filtre correspond, sélectionnez **Afficher les journaux filtrés**. • Pour trouver des entrées du journal correspondantes, vous pouvez ajouter des artefacts au champ de recherche, comme une adresse IP ou une plage horaire. • Sélectionnez la période de laquelle vous souhaitez voir les journaux : **Last 15 Minutes (15 dernières minutes)**, **Last Hour (Dernière heure)**, **Last 6 Hrs (6 dernières heures)**, **Last 12 Hrs (12 dernières heures)**, **Last 24 Hrs (24 dernières heures)**, **Last 7 Days (7 derniers jours)**, **Last 30 Days (30 derniers jours)** ou **All (Toutes)** (par défaut). • Les options situées à droite de la liste déroulante de période de temps vous permettent d'appliquer, d'effacer, d'ajouter, d'enregistrer et de charger des filtres : • **Appliquer des filtres** ( ) – affiche les entrées des journaux qui correspondent aux termes renseignés dans le champ de recherche.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• **Effacer les filtres** ( ) – efface le champ de filtrage. • **Ajouter un nouveau filtre** ( ) – définit un nouveau critère de recherche (vous atteignez Ajouter un filtre de journal, ce qui est la même chose que créer des filtres). • **Enregistrer un filtre** ( ) – Saisissez un nom pour le filtre puis cliquez sur **OK**. • **Utiliser un filtre enregistré** ( ) – Ajouter un filtre enregistré au champ de filtre. • **Exporter vers CSV** ( ) – exporte les journaux dans un rapport au format CSV, puis **Download file (Télécharge un fichier)**. Par défaut, le rapport comprend un maximum de 2 000 lignes de journal. Pour modifier le nombre maximum de lignes des rapports CSV générés, sélectionnez**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation et génération de rapports de journaux)** et saisissez une nouvelle valeur **Max Rows in CSV Export (Nombre max. de lignes du rapport d'exportation CSV)**. Vous pouvez modifier le nombre et l'ordre des entrées affichées par page. Vous pouvez utiliser les commandes de pagination situées en bas à gauche de la page pour naviguer dans la liste des journaux. Les entrées du journal sont extraites par blocs de 10'A0;pages. • **par page** – utilisez le menu déroulant pour modifier le nombre d'entrées des journaux par page (**20**, **30**, **40**, **50**, **75** ou **100**). • **ASC** ou **DESC** – sélectionnez **ASC** pour classer les résultats dans l'ordre croissant (l'entrée des journaux la plus ancienne en premier) ou **DESC** pour les classer dans l'ordre décroissant (l'entrée des journaux la plus récente en premier). La valeur par défaut est **DESC**. • **Resolve Hostname (Résoudre un nom d'hôte)** – Sélectionnez pour résoudre des adresses IP externes en noms de domaines. • **Highlight Policy Actions (Surligner les actions de politique)** –– Précisez une action et sélectionnez pour surligner les entrées des journaux qui correspondent à l'action. Les journaux filtrés sont surlignés dans les couleurs suivantes : • vert – autoriser ; • jaune – continuer ou forcer ; • rouge – refuser, abandonner, abandonner l'ICMP, réinitialiser le client, réinitialiser le serveur, réinitialiser les deux, bloquer-continuer, bloquer le forçage, bloquer l'URL, abandonner tout, entonnoir.
Supprimer	Sélectionnez puis **Supprimez** les paramètres de transfert des journaux que vous souhaitez supprimer de la liste des journaux du Système ou de la Configuration.
Onglet Authentification	
Authentification à distance	Sélectionnez le **Profil d'authentification** pour l'accès. La valeur par défaut est **None (Aucun)**. S'il n'y a pas de profils d'authentification parmi lesquels choisir, vous pouvez Configurer un Profil et une Séquence d'authentification.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
Authentification locale	Configurez l'authentification locale pour l'administrateur : • **Administrator (Administrateur)** – Toujours **Admin**, car il n'y a qu'un seul utilisateur de niveau administrateur sur un appareil Panorama. • **Mode** – Sélectionnez le mode d'authentification locale, soit **Password (Mot de passe)** soit **Password Hash (Hachage du mot de passe)** : • **Mot de passe** – Saisissez et confirmez un mot de passe utilisateur. • **Password Hash (Hachage du mot de passe)** – Saisissez une chaîne de mot de passe haché. Par exemple, un mot de passe haché est utile si vous souhaitez réutiliser les informations d'identification pour un compte Unix existant, que vous ne connaissez pas le mot de passe en texte clair, mais que vous vous souvenez du mot de passe haché. L'appareil accepte n'importe quelle chaîne comprenant jusqu'à 63 caractères, quel que soit l'algorithme utilisé pour générer la valeur de hachage. Les paramètres de Complexité minimale des mots de passe que vous avez définis pour le pare-feu (**Panorama** > **Setup (Configuration)** > **Management (Gestion)**) ne s'appliquent pas aux comptes qui utilisent un mot de passe haché.
Configuration du délai avant expiration	Configurez les délais d'expiration d'authentification des clusters : • **Délai d'inactivité (min)** – Définit le délai d'inactivité en minutes. Lorsqu'un utilisateur reste plus inactif longtemps que le délai d'inactivité précisé, le système met fin à la session. La valeur par défaut est **Aucune** (pas d'inactivité). • **Tentatives échouées** – Définit le nombre d'échecs de tentatives de connexion avant que le système verrouille un utilisateur hors du système. La valeur par défaut est de 10 échecs de tentatives de connexion. • **Lockout Time (min) (Durée de verrouillage (min))** – Définit la durée de temps (en minutes) qu'un utilisateur verrouillé doit attendre avant de se reconnecter. La valeur par défaut est de 5 minutes.
Onglet Mise en cluster (clusters WildFire gérés uniquement) et onglet Interfaces (appareils WildFire gérés uniquement) Vous devez ajouter des appareils à Panorama pour gérer les interfaces et ajouter des appareils aux clusters pour gérer les interfaces de nœud.	
Appareil (onglet Mise en cluster uniquement)	Sélectionnez un nœud de cluster pour accéder aux onglets Appareils et Interfaces pour ce nœud. Les informations du nœud de l'onglet Appareil sont prérenseignées et ne sont pas configurables, sauf pour le nom d'hôte. L'onglet Interfaces répertorie les nœuds d'interfaces. Sélectionnez une interface à gérer selon les descriptions présentées aux sections suivantes : • Gestion des noms de l'interface • Réseau environnemental d'analyse du nom de l'interface • Nom de l'interface Ethernet 2 • Nom de l'interface Ethernet 3
Gestion des noms de l'interface	L'interface de gestion est Ethernet0. Permet de configurer ou d'afficher les paramètres de l'interface de gestion :

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• **Speed and Duplex (Vitesse et Duplex)** – Sélectionnez **auto-negotiate (négocier automatiquement)** (par défaut), **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**. • **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • **Management Services (Services de gestion)** – Activez les services de gestion que vous souhaitez prendre en charge. Vous pouvez activer **Ping**, **SSH** et les services **SNMP**. Configurez les paramètres proxy si vous utilisez un serveur proxy pour vous connecter à Internet : • **Serveur** – L'adresse IP du serveur proxy. • **Port** – Numéro de port configuré sur le serveur proxy pour écouter les requêtes des périphériques Panorama. • **Utilisateur** – Nom d'utilisateur configuré sur le serveur proxy pour l'authentification. • **Mot de passe** et **Confirmer le mot de passe** – Mot de passe configuré sur le serveur proxy pour l'authentification. • **Services de mise en cluster** (onglet Mise en cluster uniquement) – Sélectionnez le service HD : • **HD** – S'il y a deux noeuds de Contrôleurs dans le cluster, vous pouvez configurer l'interface de gestion en tant qu'Interface HD pour que les informations de gestion soient disponibles pour les deux noeuds de Contrôleurs. Si le nœud de cluster que vous configurez est le noeud de Contrôleur principal, indiquez-le comme étant l'interface **HD**. En fonction de la façon dont vous utilisez les interfaces Ethernet de l'appareil WildFire, vous pouvez également configurer Ethernet 2 ou Ethernet 3 comme étant les interfaces HD et HD de sauvegarde, respectivement sur les noeuds de Contrôleur principal et de sauvegarde. Vous pouvez par exemple utiliser Ethernet 2 comme interface HD et HD de sauvegarde. Les interfaces HD et HD de sauvegarde doivent être les mêmes (gestion, Ethernet 2 ou Ethernet 3) sur les noeuds de Contrôleur principal et de sauvegarde. Vous ne pouvez pas utiliser Ethernet 1 comme interface HD/HD de sauvegarde. • **HD de sauvegarde** – Si le nœud de cluster que vous configurez est le noeud de Contrôleur de sauvegarde, indiquez-le comme étant l'interface **HD de sauvegarde**. Précisez les adresses IP autorisées sur l'interface : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des adresses IP autorisées. La barre de recherche indique le nombre d'adresses IP (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre ( ) ou effacez le filtre ( ) et saisissez une autre suite de termes.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• **Add (Ajouter)**—**Add (Ajouter)** une adresse IP autorisée. • **Supprimer** – Sélectionnez et **Supprimez** la ou les adresses IP dont vous souhaitez supprimer l'accès à l'interface de gestion.
Réseau environnemental d'analyse du nom de l'interface	Configurez les paramètres de l'interface du réseau environnemental de l'analyse du cluster d'appareils WildFire ou de l'appareil WildFire autonome (Ethernet 1, également appelé interface VM) : • **Speed and Duplex (Vitesse et Duplex)** – Définissez sur **auto-negotiate (négocier automatiquement)** (par défaut), sur **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, sur **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, sur **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, sur **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, sur **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou sur **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**. • **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • **Serveur DNS** – Saisissez l'adresse IP du serveur DNS. • **État de liaison** – Définissez l'état des liaisons de l'interface sur **Ascendant** ou **Descendant**. • Services de gestion – Activez **Ping** si vous souhaitez que l'interface prenne en charge les services ping. Précisez les adresses IP autorisées sur l'interface : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des adresses IP autorisées. La barre de recherche indique le nombre d'adresses IP (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre ( ) ou effacez le filtre ( ) et saisissez une autre suite de termes. • **Add (Ajouter)**—**Add (Ajouter)** une adresse IP autorisée. • **Supprimer** – Sélectionnez la ou les adresses IP dont vous souhaitez supprimer l'accès à l'interface de gestion, puis **Supprimez**.
Nom de l'interface Ethernet 2 Nom de l'interface Ethernet 3	Vous pouvez définir les mêmes paramètres pour les interfaces Ethernet 2 et Ethernet 3 : • **Speed and Duplex (Vitesse et Duplex)** – Définissez sur **auto-negotiate (négocier automatiquement)** (par défaut), sur **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, sur **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, sur **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, sur **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, sur **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou sur **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**. • **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • Services de gestion – Activez **Ping** si vous souhaitez que l'interface prenne en charge les services ping. • **Services de Mise en cluster** – Sélectionnez les services de cluster :

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• **HD** – S'il y a deux noeuds de Contrôleurs dans le cluster, vous pouvez configurer l'interface Ethernet 2 ou Ethernet 3 comme une interface HD pour que les informations de gestion soient disponibles pour les deux noeuds de Contrôleurs. Si le nœud de cluster que vous configurez est le noeud de Contrôleur principal, indiquez-le comme étant l'interface **HD**. En fonction de la façon dont vous utilisez les interfaces Ethernet de l'appareil WildFire, vous pouvez également configurer l'interface de gestion (Ethernet 1) comme étant les interfaces HD et HD de sauvegarde, respectivement sur les noeuds de Contrôleur principal et de sauvegarde. Les interfaces HD et HD de sauvegarde doivent être les mêmes (gestion, Ethernet 2 ou Ethernet 3) sur les noeuds de Contrôleur principal et de sauvegarde. Vous ne pouvez pas utiliser Ethernet 1 comme interface HD/HD de sauvegarde. • **HD de sauvegarde** – Si le nœud de cluster que vous configurez est le noeud de Contrôleur de sauvegarde, indiquez-le comme étant l'interface **HD de sauvegarde**. • **Gestion des clusters** – Configurez l'interface Ethernet 2 ou Ethernet 3 comme l'interface utilisée pour la gestion et la communication à l'échelle du cluster.
Rôle (onglet Mise en cluster uniquement)	Lorsqu'un cluster possède des appareils membres, l'appareil peut avoir le rôle de Contrôleur, de Contrôleur de sauvegarde ou de Subordonné. Sélectionnez **Contrôleur** ou **Contrôleur de sauvegarde** pour modifier l'appareil WildFire utilisé pour chaque rôle à partir des appareils du cluster. La modification du Contrôleur entraîne une perte de données pendant le changement de rôle.
Parcourir (onglet Mise en cluster uniquement)	L'onglet **Mise en cluster** répertorie les nœuds de l'appareil WildFire dans le cluster. **Parcourir** pour afficher et ajouter des appareils WildFire autonomes que le périphérique Panorama gère déjà : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des nœuds. La barre de recherche indique le nombre d'appareils (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre ( ) ou effacez le filtre ( ) et saisissez une autre suite de termes. • **Ajout de nœuds** — Ajoutez ( ) des nœuds au cluster. Le premier appareil WildFire que vous ajoutez à un cluster devient automatiquement le nœud de Contrôleur. Le deuxième appareil WildFire que vous ajoutez devient automatiquement le nœud de Contrôleur de sauvegarde. Vous pouvez ajouter jusqu'à 20 appareils WildFire à un cluster. Lorsque vous aurez ajouté les nœuds de Contrôleur et de Contrôleur de sauvegarde, tous les nœuds ajoutés par la suite seront des nœuds Subordonnés.
Supprimer (onglet Mise en cluster uniquement)	Sélectionnez un ou plusieurs appareils dans la liste des Appareils, puis **Supprimez**-les du cluster. Vous pouvez supprimer un nœud de Contrôleur uniquement s'il y a deux nœuds de Contrôleur dans le cluster.
Gérer le contrôleur	Sélectionnez **Gérer le contrôleur** pour définir un **Contrôleur** et un **Contrôleur de sauvegarde** parmi les nœuds d'appareils WildFire appartenant au cluster.

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
(onglet Mise en cluster uniquement)	Le nœud de Contrôleur et le nœud de Contrôleur de sauvegarde actuels sont sélectionnés par défaut. Le nœud de Contrôleur de sauvegarde ne peut pas être le même que le nœud de Contrôleur principal.
Onglet Communication	
Personnaliser la communication sécurisée avec le serveur	• **SSL/TLS Service Profile (Profil de service SSL/TLS)** – Sélectionnez un profil de service SSL/TLS à partir du menu déroulant. Ce profil définit le certificat et les versions SSL/TLS compatibles que les périphériques connectés utilisent pour communiquer avec WildFire. • **Certificate Profile (Profil de certificat)** – Sélectionnez un profil de certificat dans le menu déroulant. Ce profil de certificat définit le comportement de la vérification de la révocation du certificat et le certificat AC racine utilisé pour authentifier la chaîne de certificats présentée par le client. • **Custom Certificate Only (Certificat personnalisé uniquement)** – Lorsque cette option est activée, WildFire accepte uniquement des certificats personnalisés pour l'authentification avec des périphériques se connectant. • **Check Authorization List (Vérification de la liste des autorisations)** – Les périphériques clients connectés à WildFire sont vérifiés par rapport à la liste des autorisations. Un appareil ne doit correspondre qu'à un seul objet de la liste à autoriser. Si aucune correspondance n'est trouvée, le périphérique n'est pas autorisé. • **Authorization List (Liste d'autorisations)** – **Add (Ajoutez)** une liste d'autorisations et complétez les champs suivants pour définir les critères requis pour autoriser les périphériques clients. La Liste d'autorisations prend en charge un maximum de 16 entrées. • **Identifier (Identifiant)** – Sélectionnez **Subject (Objet)** ou **Subject Alt. (Autre nom d'objet)** en tant qu'identifiant d'autorisation. • **Type** – Si vous avez choisi **Subject Alt. (Autre objet).** en tant qu'identifiant, puis sélectionnez **IP**, **hostname (nom d'hôte)** ou **e-mail** comme type d'identifiant. Si vous avez sélectionné **Subject (Objet)**, le nom commun est alors le type d'identifiant. • **Value (Valeur)** – Saisissez la valeur d'identifiant.
Communication sécurisée avec le client	L'utilisation de la **Secure Client Communication (Sécurisation des communications avec le client)** permet de s'assurer que WildFire utilise des certificats personnalisés configurés (plutôt que le certificat prédéfini par défaut) pour authentifier les connexions SSL avec un autre appareil WildFire. • **Predefined (Prédéfini)** – (par défaut) Aucun certificat de périphérique n'est configuré ; WildFire utilise le certificat prédéfini par défaut. • **Local** – WildFire utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d'un serveur PKI d'entreprise existant. • **Certificate (Certificat)** - Sélectionnez le certificat de périphérique local. • **Certificate Profile (Profil du certificat)** - Sélectionnez le Profil de certificat dans le menu déroulant. • **SCEP** – WildFire utilise un certificat de périphérique et une clé privée générée par un serveur Simple Certificate Enrollment Protocol (Protocole d'inscription de certificats simple ; SCEP).

© 2020 Palo Alto Networks, Inc.

Paramètre	Description
	• **SCEP Profile (Profil SCEP)** - Sélectionnez un profil SCEP dans la liste déroulante. • **Certificate Profile (Profil du certificat)** - Sélectionnez le Profil de certificat dans le menu déroulant.
Communication sécurisée avec le cluster	Sélectionnez **Enable (Activer)** pour crypter les communications entre les appareils WildFire. Le certificat par défaut utilise le type de certificat prédéfini. Pour utiliser un certificat personnalisé défini par l'utilisateur, vous devez configurer la **Customize Secure Server Communication (Communication sécurisée avec le serveur)** et activer **Custom Certificate Only (Certificat personnalisé uniquement)**.

© 2020 Palo Alto Networks, Inc.

Panorama > Administrateurs

Sélectionnez **Panorama** > **Administrators (Administrateurs)** pour créer et gérer des comptes pour les administrateurs Panorama.

Si vous vous connectez à Panorama en tant qu'administrateur avec un rôle de super-utilisateur, vous pouvez débloquer les comptes d'autres administrateurs en cliquant sur les icônes de verrouillage dans la colonne Utilisateur verrouillé. Un administrateur bloqué ne peut pas accéder à Panorama. Panorama verrouille les administrateurs qui dépassent le nombre autorisé de tentatives successives échouées pour accéder à Panorama tel que défini dans le **Authentication Profil (Profil d'authentification)** affecté à leurs comptes (voir Périphérique > Profil d'authentification).

Pour créer un compte administrateur, cliquez pour **Ajouter** et configurez les paramètres comme décrits dans le tableau suivant.

Paramètres du compte administrateur	Description
Name (Nom)	Donnez un nom d'utilisateur de connexion à l'administrateur (15 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d'union et des caractères de soulignement.
Profil d'authentification	Sélectionnez un profil ou une séquence d'authentification pour authentifier cet administrateur. Pour plus de détails, voir Périphérique > Profil d'authentification ou Périphérique > Séquence d'authentification.
Utiliser uniquement l'authentification du certificat client (Web)	Sélectionnez cette option pour utiliser l'authentification du certificat du client pour l'accès à l'interface Web. Si vous choisissez cette option, un nom d'utilisateur (**Name (Nom)**) et un **Password (Mot de passe)** ne sont pas nécessaires.
Mot de passe/Confirmer le mot de passe	Saisissez et confirmez un mot de passe sensible à la casse pour l'administrateur (15 caractères maximum). Pour garantir la sécurité, Palo Alto Networks recommande que l'administrateur change son mot de passe régulièrement en utilisant des lettres en minuscules, en majuscules et des chiffres. Veillez à respecter les pratiques exemplaires en matière de robustesse des mots de passe pour vous assurer de créer un mot de passe fort. Les administrateurs de groupes de périphériques et de modèles ne peuvent pas accéder à **Panorama** > **Administrators (Administrateurs)**. Pour modifier leur mot de passe local, ces administrateurs doivent cliquer sur leur nom d'utilisation (à côté de **Logout (Déconnexion)** en bas de l'interface Web). Ce processus s'applique également aux administrateurs ayant un rôle Panorama personnalisé pour lequel l'accès à **Panorama** > **Administrators (Administrateurs)** est désactivé. Vous pouvez utiliser l'authentification de mots de passe conjointement avec un **Authentication Profile (Profil d'authentification)** (ou une séquence) ou pour l'authentification de base de données locale.

© 2020 Palo Alto Networks, Inc.

Paramètres du compte administrateur	Description
	Vous pouvez définir les paramètres d'expiration du mot de passe en sélectionnant un **Profil de mot de passe** (voir Périphérique > Profils de mots de passe) et en définissant des paramètres de Complexité minimale du mot de passe (voir Périphérique > Configuration > Gestion), mais uniquement pour les comptes administratifs que Panorama authentifie localement.
Utiliser l'authentification à clef publique (SSH)	Sélectionnez pour utiliser Authentification de clé publique SSH : cliquez sur **Importer la clé**, puis sur **Navigateur** pour sélectionner le fichier de clé publique, puis cliquez sur **OK**. La boîte de dialogue Administrateur affiche la clé chargée dans la zone de texte en lecture seule. Les formats de fichier de clé pris en charge sont IETF SECSH et OpenSSH. Les algorithmes de clé pris en charge sont DSA (1024 bits) et RSA (768 à 4096 bits). *Si l'authentification de la clé publique échoue, Panorama présente une invite de saisie du nom d'utilisateur et du mot de passe.*
Type d'administrateur	Le type sélectionné détermine les options du rôle administrateur : • **Dynamique** - Rôles qui offrent l'accès à Panorama et aux pare-feu gérés. Lors de l'ajout de nouvelles fonctionnalités, Panorama met automatiquement à jour les définitions des rôles dynamiques. Vous ne devez les jamais les mettre à jour manuellement. • **Admin Panorama personnalisé** - Rôles configurables qui disposent d'un accès en lecture / écriture, d'un accès en lecture seule ou d'aucun accès aux fonctionnalités de Panorama. • **Admin groupe de périphériques et modèle** - Rôles configurables qui disposent d'un accès en lecture / écriture, d'un accès en lecture seule ou d'aucun accès aux fonctionnalités pour les groupes de périphériques et les modèles affectés aux domaines d'accès que vous sélectionnez pour cet administrateur.
Rôle admin (Type d'administrateur dynamique)	Sélectionnez un rôle prédéfini : • **Superuser (Super utilisateur)** : accès complet en lecture/écriture à Panorama et à tous les groupes de périphériques, modèles et pare-feu gérés. • **Superuser (Read Only) (Super utilisateur (Lecture seule))** : accès en lecture seule à Panorama et à tous les groupes de périphériques, modèles et pare-feu gérés. • **Panorama administrator (Administrateur Panorama)** : accès complet à Panorama, à l'exception des actions suivantes : • Créer, modifier ou supprimer des administrateurs de Panorama ou de pare-feu et des rôles. • Exporter, valider, rétablir, enregistrer, charger ou importer une configuration (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**).

© 2020 Palo Alto Networks, Inc.

Paramètres du compte administrateur	Description
	• Configurer une **Scheduled Config Export (Exportation programmée des configurations)** dans l'onglet **Panorama**.
Profil (Type d'administrateur Admin Panorama personnalisé)	Sélectionnez un rôle Panorama personnalisé (reportez-vous à la section Panorama > Périphériques gérés > Récapitulatif).
Domaine d'accès au rôle administrateur (type d'administrateur Groupe de périphériques et modèle Admin)	Pour chaque domaine d'accès (jusqu'à 25) que vous souhaitez affecter à l'administrateur, **Add (Ajoutez)** un **Access Domain (Domaine d'accès)** à partir de la liste déroulante (reportez-vous à la section Panorama > Domaines d'accès), cliquez sur la cellule adjacente au Rôle Administrateur, puis sélectionnez un rôle administrateur de groupe de périphériques et de modèle personnalisé à partir de la liste déroulante (reportez-vous à la section Panorama> Périphériques gérés > Récapitulatif). Lorsque des administrateurs disposant d'un accès à plusieurs domaines se connectent à Panorama, un menu déroulant **Domaine d'accès** apparaît dans le pied de page de l'interface Web. Les administrateurs peuvent sélectionner n'importe quel **Access Domain (Domaine d'accès)** affecté pour filtrer les données de surveillance et de configuration affichées par Panorama. La sélection **Access Domain (Domaine d'accès)** filtre également les pare-feu qui sont affichés dans la liste déroulante **Context (Contexte)**. *Si vous utilisez un serveur RADIUS pour authentifier les administrateurs, vous devez mapper les rôles d'administrateur et les domaines d'accès aux VSA RADIUS. Les chaînes VSA prenant en charge un nombre limité de caractères, si vous configurez le nombre maximum de paires de domaine d'accès/ rôle (25) pour un administrateur, les valeurs Nom de chaque domaine d'accès et de chaque rôle ne doivent pas dépasser une moyenne de 9 caractères.*
Profil de mot de passe	Sélectionnez un **Profil de mot de passe** (voir Périphérique > Profils de mots de passe).

© 2020 Palo Alto Networks, Inc.

Panorama > Rôles admin

Les profils de rôle d'administrateur sont des rôles personnalisés qui définissent les privilèges d'accès et les responsabilités des administrateurs. Par exemple, les rôles attribués à un administrateur contrôlent quels rapports il peut générer et quel groupe de périphériques ou quelles configurations de modèle l'administrateur peut afficher ou modifier.

Pour un administrateur de groupe de périphériques et de modèle, vous pouvez attribuer un rôle distinct pour chaque domaine d'accès qui est affecté au compte administratif (voir Panorama > Domaines d'accès). Le recensement des rôles pour accéder aux domaines vous permet d'obtenir un contrôle très important sur les informations auxquelles les administrateurs peuvent accéder sur Panorama. Par exemple, imaginez un scénario où vous configurez un domaine d'accès qui inclut tous les groupes de périphériques pour les pare-feu dans vos centres de données et où vous attribuez ce domaine d'accès à un administrateur qui est autorisé à surveiller le trafic du centre de données, mais qui n'est pas autorisé à configurer les pare-feu. Dans ce cas, vous pouvez schématiser le domaine d'accès à un rôle qui active tous les privilèges de surveillance, mais qui désactive l'accès aux paramètres du groupe de périphériques.

Pour créer un profil de rôle administrateur, cliquez pour **Ajouter** un profil et configurez les paramètres comme décrits dans le tableau suivant.

Si vous utilisez un serveur RADIUS pour authentifier les administrateurs, mappez les rôles administrateur et les domaines d'accès avec les attributs spécifiques au fournisseur (VSA) RADIUS.

Paramètres du rôle administrateur de Panorama	Description
Name (Nom)	Saisissez un nom pour identifier ce rôle administrateur (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des espaces, des traits d'union et des caractères de soulignement.
Description	(Facultatif) Saisissez une description du rôle.
Rôle	Sélectionnez la portée des responsabilités administratives : **Panorama** ou **Device Group and Template (Groupe de périphériques et modèle)**.
UI Web	Sélectionnez l'une des options suivantes pour définir le type d'accès autorisé pour des fonctions spécifiques dans le contexte de Panorama (**liste UI Web**) et le contexte de pare-feu (**liste IU de commutation de contexte**) : • **Enable (Activer)**( ) - Accès en lecture/écriture • **Read Only (Lecture seule)** ( ) - Accès en lecture seule • **Disable (Désactiver)** ( ) - Aucun accès
Interface API REST/XML (rôle Panorama uniquement)	Sélectionnez le type d'accès à l'API XML/REST (**Enable (Activer)**, **Read Only (Lecture seule)**, ou **Disable (Désactiver)**) pour Panorama et pour les pare-feu gérés : • **Rapport** - Accès à Panorama et aux rapports du pare-feu. • **Journal** - Accès à Panorama et aux journaux du pare-feu.

© 2020 Palo Alto Networks, Inc.

Paramètres du rôle administrateur de Panorama	Description
	• **Configuration** - Autorisations pour récupérer ou modifier les configurations de Panorama et pare-feu. • **Requêtes opérationnelles** - Autorisations pour exécuter des commandes opérationnelles sur Panorama et sur les pare-feu. • **Valider** - Autorisations pour valider les configurations de Panorama et du pare-feu. • **Agent User-ID** - Accès à l'agent User-ID. • **Exporter** - Autorisations pour exporter des fichiers depuis Panorama et les pare-feu (tels que des configurations, des pages de blocage ou de réponse, des certificats et des clés). • **Importer** - Autorisations pour importer des fichiers dans Panorama et les pare-feu (tels que des mises à jour logicielles, des mises à jour de contenu, des licences, des configurations, des certificats, des pages de blocage et des journaux personnalisés).
Ligne de commande (rôle Panorama uniquement)	Sélectionnez le type de rôle d'accès à la CLI : • **Aucun** - (par défaut) L'accès à l'ILC (interface de ligne de commande) de Panorama n'est pas autorisé. • **Super utilisateur** - Accès complet à **Panorama**. • **Super lecteur** - Accès en lecture seule à **Panorama**. • **Admin Panorama -** Accès complet à **Panorama**, à l'exception des actions suivantes : • Créer, modifier ou supprimer des administrateurs de Panorama et des rôles. • Exporter, valider, rétablir, sauvegarder, charger ou importer une configuration. • Planification de l'exportation de la configuration

© 2020 Palo Alto Networks, Inc.

Panorama > Domaines d'accès

Les domaines d'accès contrôlent l'accès dont disposent les administrateurs de groupe de périphériques et de modèles à des groupes de périphériques (pour gérer des politiques et des objets), à des modèles (pour gérer les paramètres de réseau et de périphérique) et à l'interface Web des pare-feu gérés (à travers le changement de contexte) spécifiques. Vous pouvez définir jusqu'à 4 000 domaines d'accès et les gérer localement ou à l'aide d'attributs spécifiques au fournisseur (VSA) RADIUS, de VSA TACACS+ ou d'attributs SAML. Pour créer un domaine d'accès, cliquez pour **Ajouter** un domaine et configurez les paramètres comme décrits dans le tableau suivant.

Paramètres du domaine d'accès	Description
Name (Nom)	Donnez un nom au domaine d'accès (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d'union et des caractères de soulignement.
Objets partagés	Sélectionnez un des privilèges d'accès suivants pour les objets dont les groupes de périphériques de ce domaine d'accès héritent à partir de l'emplacement Partagé. Quel que soit le privilège, les administrateurs ne peuvent pas appliquer un contrôle prioritaire sur des objets partagés ou par défaut (prédéfinis). • **Lecture** : les administrateurs peuvent afficher et cloner des objets partagés mais ne peuvent pas effectuer d'autres opérations sur ceux-ci. Lors de l'ajout d'objets non partagés ou du clonage d'objets partagés, la destination doit être un groupe de périphériques du domaine d'accès, non partagé. • **write (écriture)** : les administrateurs peuvent effectuer toutes les opérations sur des objets partagés. Il s'agit de la valeur par défaut. • **shared-only (partagé uniquement)** : les administrateurs peuvent ajouter des objets à Partagé uniquement. Les administrateurs peuvent également afficher, modifier et supprimer des objets partagés, mais ne peuvent pas les déplacer ou les cloner. Le choix de cette valeur a pour conséquence que les administrateurs ne peuvent pas effectuer d'opérations sur des objets non partagés autres que leur affichage.
Groupes de périphériques	Activez ou désactivez l'accès en lecture/écriture sur des groupes de périphériques donnés dans le domaine d'accès. Vous pouvez également cliquer sur **Enable All (Activer tout)** ou **Disable All (Désactiver tout)**. L'autorisation de l'accès en lecture/écriture sur un groupe de périphériques active automatiquement le même accès sur ses descendants. Si vous désactivez manuellement un descendant, l'accès sur son ancien le plus élevé passe automatiquement à lecture seule. Par défaut, l'accès est désactivé pour tous les groupes de périphériques. Si vous souhaitez que la liste affiche uniquement des groupes de périphériques spécifiques, sélectionnez les noms des groupes de périphériques et le **Filtre sélectionné**.

© 2020 Palo Alto Networks, Inc.

Paramètres du domaine d'accès	Description
	Si vous définissez l'accès aux objets partagés sur Partagés seulement, Panorama applique l'accès en lecture seule à tous les groupes de périphériques pour lesquels vous spécifiez un accès en lecture / écriture.
Modèles	Pour chaque modèle ou pile de modèles que vous souhaitez affecter, cliquez sur **Add (Ajouter)**, puis sélectionnez-le (ou la) dans la liste déroulante.
Contexte du périphérique (Correspond à la colonne Périphériques / Systèmes virtuels qui figure à la page Domaine d'accès)	Sélectionnez les pare-feu pour lesquels l'administrateur peut changer le contexte afin d'effectuer la configuration locale. Si la liste est longue, vous pouvez la filtrer par **Device State (État du périphérique)**, **Platforms (Plates-formes)**, **Device Groups (Groupes de périphériques)**, **Templates (Modèles)**, **Tags (Étiquettes)** ou **HA Status (État HA)**.
Groupes de collecteurs de journaux	Pour chaque groupe de collecteurs que vous souhaitez affecter, cliquez sur **Add (Ajouter)**, puis sélectionnez-le dans la liste déroulante.

© 2020 Palo Alto Networks, Inc.

Panorama > Périphériques gérés > Récapitulatif

Un pare-feu Palo Alto Networks géré par Panorama est appelé un *périphérique géré*. Panorama peut gérer des pare-feux exécutant la même version majeure ou des versions majeures antérieures, mais pas des pare-feux exécutant une version majeure ultérieure. Par exemple, Panorama utilisant PAN-OS 9.1 peut gérer les pare-feux utilisant PAN-OS 9.1 et ses versions antérieures. De plus, il n'est pas recommandé de gérer des pare-feux utilisant une version plus récente que Panorama puisque cela peut faire en sorte que certaines fonctionnalités ne fonctionnent pas comme prévu. Par exemple, il n'est pas recommandé de gérer des pare-feux utilisant PAN-OS 9.1.1 ou une version ultérieure si Panorama utilise PAN-OS 9.1.0. Pour plus d'informations relatives à la version 9.1, reportez-vous à la section Release Notes (Notes de version) de PAN-OS 9.1. Pour plus d'informations sur les versions de PAN-OS prises en charge, reportez-vous à End-of-Life Summary (Récapitulatif de fin de vie).

- Administration du pare-feu géré
- Informations sur les pare-feu gérés
- Mises à jour logicielles et de contenu du pare-feu
- Sauvegardes du pare-feu

Administration du pare-feu géré

Vous pouvez effectuer les tâches administratives suivantes sur les pare-feu.

Tâche	Description
Ajouter	Cliquez sur **Ajouter** et saisissez les numéros de série des pare-feu (un par ligne) pour les ajouter en tant que périphériques gérés. Ensuite, la fenêtre **Périphériques gérés** affichera les Informations sur les pare-feu gérés, y compris l'état de la connexion, les mises à jour installées et les propriétés qui ont été définies lors de la configuration initiale. Cochez la case **Associate Devices (Périphériques associés)** pour associer les pare-feu à un groupe de périphériques ou à une pile de modèles. **Import (Importez)** plusieurs pare-feu au format CSV qui doivent être gérés par le serveur de gestion Panorama. Un fichier CSV type peut être téléchargé. Saisissez ensuite l'adresse IP du serveur de gestion Panorama sur chaque pare-feu (voir Périphérique > Configuration > Gestion) afin que Panorama puisse gérer les pare-feu. *le pare-feu s'enregistre auprès de Panorama via une connexion SSL en utilisant un chiffrement AES-256. Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux.*
Réassocier	Réaffecter un ou plusieurs pare-feu sélectionnées à un autre groupe de périphériques ou à une autre pile de modèles.
Supprimer	Sélectionnez un ou plusieurs pare-feu, puis **Delete (Supprimez)**-les de la liste des pare-feu gérés par Panorama.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
Étiquette	Sélectionnez un ou plusieurs pare-feu, cliquez sur **Tag (Étiquette)**, puis saisissez un texte de 31 caractères maximum ou sélectionnez une étiquette existante. sans espace Lorsque l'interface Web affiche une longue liste de pare-feu (dans la boîte de dialogue d'installation de logiciel, par exemple), les étiquettes permettent de filtrer la liste. Par exemple, vous pouvez utiliser une étiquette libellée Filiale pour définir un filtre pour tous les pare-feu des filiales de votre réseau.
Installer	**Install (Installez)** les mises à jour logicielles ou de contenu du pare-feu.
Regrouper les homologues HA	Sélectionnez **Regrouper les homologues HA** si vous voulez que la page **Périphériques gérés** regroupe les pare-feu homologues dans une configuration haute disponibilité (HA). Vous pouvez ensuite choisir d'effectuer uniquement des actions sur les deux homologues de chaque paire HA ou sur ni l'un, ni l'autre.
Gérer (les sauvegardes)	**Manage (Gérez)** les sauvegardes du pare-feu.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau des pare-feu gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.
Déployer la clé principale	Déployez une nouvelle clé principale ou mettez à jour une clé principale existante d'un ou de plusieurs périphériques.

Informations sur les pare-feu gérés

Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** pour afficher les informations suivantes pour chacun des pare-feu gérés.

Informations sur les pare-feu gérés	Description
Groupe de périphériques	Affiche le nom du groupe de périphériques dont le pare-feu est membre. Cette colonne est masquée par défaut, mais vous pouvez l'afficher en cliquant sur la liste déroulante dans un en-tête de colonne et en sélectionnant **Columns (Colonnes)** > **Device Group (Groupe de périphériques)**. La page affiche les pare-feu dans des clusters en fonction de leur groupe de périphériques. Chaque cluster comporte une ligne d'en-tête qui indique le nom du groupe de périphériques, le nombre total de pare-feu affectés, le nombre de pare-feu connectés, et le chemin du groupe de périphériques dans la hiérarchie. Par exemple, **Data center (2/4 Devices Connected) (Centre de données (2/4 périphériques connectés)) : Shared (Partagé)** > **Europe** > **Data center (Centre de données)** signifie qu'un groupe de périphériques nommé **Data center (Centre de données)** comporte quatre pare-feu membres (dont deux sont connectés) et qu'il est un enfant d'un groupe de périphériques

© 2020 Palo Alto Networks, Inc.

Informations sur les pare-feu gérés	Description
	nommé **Europe**. Vous pouvez réduire ou développer n'importe quel groupe de périphériques pour masquer ou afficher ses pare-feu.
Nom du périphérique	Affiche le nom d'hôte ou le numéro de série du pare-feu. Pour le pare-feu VM-Series édition NSX, le nom de pare-feu s'ajoute au nom d'hôte du hôte ESXi. Par exemple, PA-VM: host-NY5105
Virtual System (système virtuel - vsys)	Répertorie les systèmes virtuels disponibles sur un pare-feu en mode Plusieurs systèmes virtuels.
Modèle	Affiche le modèle du pare-feu.
Étiquettes	Affiche les étiquettes définies pour chaque pare-feu/système virtuel.
Numéro de série	Affiche le numéro de série du pare-feu.
Mode opérationnel	Affiche le mode opérationnel du pare-feu. Il peut s'agir de FIPS-CC ou Normal.
Adresse IP	Affiche l'adresse IP du pare-feu/système virtuel.
	IPv4 : adresse IPv4 du pare-feu/système virtuel.
	IPv6 : adresse IPv6 du pare-feu/système virtuel.
Variables	Crée des définitions de variables de périphérique spécifiques en les copiant d'un périphérique qui se trouve dans la pile de modèles, ou modifie des définitions de variables existantes afin de créer des variables uniques au périphérique. Cette colonne sera vide si le périphérique n'est pas associé à une pile de modèles. Par défaut, les variables sont héritées de la pile de modèles. Reportez-vous à la section Créer ou modifier les définitions de variables sur un appareil.
Modèle	Affiche la pile de modèles à laquelle le pare-feu appartient.
Status (État)	**État du périphérique** : indique l'état de la connexion entre Panorama et le pare-feu. Connecté ou déconnecté. Un pare-feu VM-Series peut présenter deux autres états : • **Désactivé** : indique que vous avez désactivé une machine virtuelle, soit directement sur le pare-feu, soit en sélectionnant **Deactivate VMs (Désactiver la VM)**(**Panorama** > **Device Deployment (Déploiement du périphérique)** > **Licenses (Licences)**) et supprimé toutes les licences et tous les droits sur le pare-feu. Un pare-feu désactivé n'est plus connecté à Panorama car le processus de désactivation supprime le numéro de série sur le pare-feu VM-Series. • **Partiellement désactivé** : indique que vous avez lancé le processus de désactivation de licence à partir de Panorama, mais que le

© 2020 Palo Alto Networks, Inc.

Informations sur les pare-feu gérés	Description
	processus n'est pas terminé car le pare-feu est hors ligne et que Panorama ne peut pas communiquer avec lui.
	État HA : indique si le pare-feu est : • **Actif** - État opérationnel de gestion du trafic normal. • **Passif** - État de sauvegarde normal. • **En cours d'initialisation** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non fonctionnel** - État d'erreur. • **Suspendu** - Un administrateur a désactivé le pare-feu. • **Provisoire** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
	Politique partagée : indique si les configurations de politique et d'objet sur le pare-feu sont synchronisées avec Panorama.
	Modèle - Indique si les configurations réseau et de périphérique sur le pare-feu sont synchronisées avec Panorama.
État (suite)	**Certificat** – indique l'état du certificat client du périphérique géré. • **Prédéfini** – le périphérique géré utilise un certificat prédéfini pour s'authentifier avec Panorama. • **Déployé** – le certificat personnalisé est déployé avec succès sur le périphérique géré. • **Expire dans X jours X heures** – le certificat actuellement installé expire dans moins de 30 jours. • **Expire dans X minutes** – le certificat actuellement installé expire dans moins d'un jour. • **Vérification de l'identité du client réussie** – le nom commun du certificat correspond au numéro de série du périphérique de connexion. • **État OCSP inconnu** – Panorama ne parvient pas à obtenir le statut OCSP du répondeur OCSP. • **État OCSP non disponible** – Panorama ne parvient pas à contacter le répondeur OCSP. • **État CRL inconnu** – Panorama ne parvient pas à obtenir l'état de révocation de la base de données CRL. • **État CRL non disponible** – Panorama ne parvient pas à contacter la base de données CRL.
	• **État OCSP/CRL inconnu** – Panorama ne parvient pas à obtenir l'état OCSP ou de révocation lorsqu'ils sont tous les deux activés. • **État OCSP/CRL non disponible** – Panorama ne parvient pas à contacter la base de données OCSP ou CRL lorsqu'ils sont tous les deux activés. • **Émetteur non approuvé** – le périphérique géré dispose d'un certificat personnalisé, mais le serveur ne le valide pas.

© 2020 Palo Alto Networks, Inc.

Informations sur les pare-feu gérés	Description
	État de la dernière validation - Indique si la dernière validation a réussi ou non sur le pare-feu.
Version du logiciel | Applications et menaces | Antivirus | Filtrage des URL | Client GlobalProtect™ | WildFire	Affiche les versions logicielle et du contenu installées actuellement sur le pare-feu. Pour plus de détails, voir Mises à jour logicielles ou de contenu du pare-feu.
Sauvegardes	À chacune des validations du pare-feu, PAN-OS envoie automatiquement une sauvegarde de la configuration du pare-feu à Panorama. Cliquez sur **Manage (Gérer)** pour afficher les sauvegardes de configuration disponibles et, si vous le souhaitez, en charger une. Pour plus de détails, voir Sauvegardes de pare-feu.
Dernière clé principale transmise	Affiche l'état du déploiement de clé principale de Panorama au pare-feu.
	État : affiche l'état de la dernière transmission de la clé principale. L'état peut être `Success` ou `Failed`. `Unknown` s'affiche si aucune clé principale n'a été transmise au pare-feu depuis Panorama.
	Horodatage : affiche la date et l'heure de la dernière transmission de clé principale depuis Panorama.

Créer une définition de variable de périphérique

Lors du premier ajout d'un périphérique à une pile de modèles, vous avez la possibilité de créer des définitions de variables propres au périphérique que vous copiez à partir des périphériques qui se trouvent dans la pile de modèles. Vous pouvez également modifier les définitions des variables du modèle via **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**. Par défaut, toutes les définitions des variables sont héritées de la pile de modèles et vous ne pouvez remplacer (non pas supprimer) les définitions des variables d'un périphérique individuel. Vous pouvez vous servir de variables pour remplacer des objets d'adresses IP et des littéraux d'adresse IP (masque réseau IP, plage d'adresses IP, FQDN) dans toutes les zones de la configuration, des interfaces de la configuration de la passerelle IKE (Interface) et de la configuration HA (ID du groupe).

Informations sur la création d'une définition de variable de périphérique	Description
Cloner la définition de la variable du périphérique à partir d'un autre périphérique qui se trouve dans la pile de modèles ?	
Non	Affichez les définitions de variables existantes et modifiez-les au besoin. Voir Panorama > Modèles > Variables des modèles.

© 2020 Palo Alto Networks, Inc.

Informations sur la création d'une définition de variable de périphérique	Description
Oui	Sélectionnez un périphérique dans la liste déroulante à partir duquel cloner les définitions de variables, puis sélectionnez les définitions des variables que vous souhaitez cloner.

Mises à jour logicielles et de contenu du pare-feu

Pour installer une mise à jour logicielle ou de contenu sur un pare-feu géré, utilisez d'abord les pages **Panorama** > **Device Deployment (Déploiement du périphérique)** pour télécharger ou charger la mise à jour sur Panorama. Ensuite, sélectionnez la page **Panorama** > **anaged Devices (Périphériques gérés)**, cliquez sur **Install (Installer)** et complétez les champs suivants.



Pour réduire le trafic sur l'interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces*).*

Options d'installation des mises à jour logicielles / de contenu sur le pare-feu	Description
Type	Sélectionnez le type de mise à jour à installer. **Software (Logiciel)** PAN-OS, logiciel **GlobalProtect Client (Client GlobalProtect)**, signatures **Apps and Threats (Applications et menaces)**, signatures **Antivirus**, **WildFire** ou **URL Filtering (Filtrage des URL)**.
Classification	Sélectionnez l'image de mise à jour. La liste déroulante inclut uniquement des images que vous avez téléchargées ou chargées sur Panorama à l'aide des pages **Panorama** > **Device Deployment (Déploiement de périphérique)**.
Filtres	Sélectionnez Filtres pour filtrer la liste Périphériques.
Périphériques	Sélectionnez les pare-feu sur lesquels vous souhaitez installer l'image.
Nom du périphérique	Le nom du pare-feu.
Version actuelle	La version de mise à jour du **Type** sélectionné qui est actuellement installée sur le pare-feu.
État HA	Indique si le pare-feu est : • **Actif** - État opérationnel de gestion du trafic normal. • **Passif** - État de sauvegarde normal. • **En cours d'initialisation** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non fonctionnel** - État d'erreur. • **Suspendu** - Un administrateur a désactivé le pare-feu.

© 2020 Palo Alto Networks, Inc.

Options d'installation des mises à jour logicielles / de contenu sur le pare-feu	Description
	• **Provisoire** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
Regrouper les homologues HA	Sélectionnez pour regrouper les pare-feu homologues dans une configuration haute disponibilité (HA).
Filtre sélectionné	Si vous souhaitez que la liste Périphériques n'affiche que des pare-feu spécifiques, sélectionnez les noms des périphériques correspondants et **Filter Selected (Filtre sélectionné)**.
Charger uniquement sur le périphérique	Sélectionnez pour télécharger l'image sur le pare-feu, mais n'activez pas le redémarrage automatique du pare-feu. L'image est installée lorsque vous redémarrez manuellement le pare-feu.
Redémarrer le périphérique après installation (Logiciel seulement)	Sélectionnez pour télécharger et installer l'image du logiciel. Le processus d'installation entraîne un redémarrage.
Désactiver les nouvelles applications dans la mise à jour de contenu (Applications et menaces uniquement)	Sélectionnez pour désactiver des applications de la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d'activer les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.

Sauvegardes du pare-feu

- Panorama > Périphériques gérés

Panorama sauvegarde automatiquement chaque modification de la configuration que vous avez validée sur des pare-feu gérés. Pour gérer les sauvegardes sur un pare-feu, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**, cliquez sur **Manage (Gérer)** dans la colonne Sauvegardes du pare-feu et exécutez l'une des tâches suivantes.

Pour configurer le nombre de versions de sauvegarde de configuration du pare-feu à conserver sur Panorama, sélectionnez Panorama > Setup (Configuration) > Management (Gestion), modifiez les Paramètres de journalisation et de génération de rapports, sélectionnez Log Export and Reporting (Exportation et génération de rapports de journaux) et saisissez le Number of Versions for Config Backups (Nombre de versions pour les sauvegardes de configuration) (la valeur par défaut est 100).

© 2020 Palo Alto Networks, Inc.

Tâche	Description
Affiche des détails sur la configuration sauvegardée ou validée.	Dans la colonne Version correspondant à la sauvegarde, cliquez sur le fichier de configuration sauvegardé ou le numéro de version de configuration validé pour afficher le contenu du fichier XML associé.
Rétablissez une configuration sauvegardée ou validée vers la configuration candidate.	Dans la colonne Action correspondant à la sauvegarde, cliquez sur **Load (Charger)** et sur **Commit (Valider)**.
Supprimer une configuration sauvegardée.	Dans la colonne Action correspondant à la sauvegarde, cliquez sur Supprimer ( ).

Panorama > Périphériques gérés > État

Panorama™ vous permet de surveiller les ressources matérielles et la performance des pare-feu gérés. Panorama centralise les informations sur la performance (processeur, mémoire, CPS et débit), sur la performance de journalisation, sur l'environnement (comme les ventilateurs, l'état RAID et l'alimentation) en présentant leur évolution au fil du temps et met en corrélation les événements (comme les validations, les installations de contenu et les mises à niveau logicielles) avec les données sur l'état. Lorsqu'un pare-feu s'écarte de sa base de référence calculée, Panorama le signale comme Périphérique anormal pour aider à identifier, à diagnostiquer et à resoudre rapidement les problèmes matériels.

Vous pouvez utiliser cette page pour effectuer ce qui suit :

Afficher une Vue détaillée de l'état du périphérique.	Afficher les mesures sur l'état des périphériques gérés par Panorama.
Regrouper les homologues HA	Afficher les pare-feu qui sont regroupés pour faciliter l'identification de problèmes éventuels et pour déterminer si les pare-feu sont touchés par des problèmes liés à la performance ou aux ressources matérielles (et le cas échéant, lesquels).
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau des pare-feu gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, au besoin, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web sont exportées. Consultez la section Exportation des données du tableau de configuration.

Panorama > Périphériques gérés > État > Tous les périphériques

Utilisez cette page pour consulter les informations suivantes pour chaque pare-feu.

© 2020 Palo Alto Networks, Inc.

Information sur l'état	Description
Nom du périphérique	Nom d'hôte ou numéro de série du pare-feu. Pour le pare-feu VM-Series édition NSX, le nom de pare-feu s'ajoute au nom d'hôte du hôte ESXi. Par exemple, PA-VM: host-NY5105
Modèle	Modèle du pare-feu.
Périphérique	
Débit (en Kbit/s)	Le débit des données au fil du temps (moyenne sur cinq minutes) mesuré en kilobit par seconde.
CPS	Connexions par seconde totales pour le périphérique au fil du temps (moyenne sur cinq minutes).
Session	
Nombre de sessions	Compte de session total au fil du temps (moyenne sur cinq minutes).
Plan de données	
Processeur (%)	Utilisation totale du processeur sur le plan de données.
Plan de gestion	
Processeur (%)	Utilisation totale du processeur sur le plan de gestion.
MEM (%)	Utilisation totale de la mémoire sur le plan de gestion.
Taux de journalisation (journaux par seconde)	Taux auquel les pare-feu transfèrent les journaux vers Panorama ou vers un Collecteur de journaux (moyenne sur une minute).
Ventilateurs	Présente la présence, l'état actuel, le nombre de tours par minute et le dernier échec des ventilateurs de chaque support de ventilateur. L'état des ventilateurs s'affiche au format *A*/*B*, où *A* correspond au nombre de ventilateurs qui fonctionnent bien et *B* au nombre total de ventilateurs sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
Alimentation	Présente la présence, l'état actuel et l'horodatage du dernier échec. L'état de l'alimentation s'affiche au format *A*/*B*, où *A* correspond au nombre de blocs d'alimentation qui fonctionnent bien et *B* au nombre total de blocs d'alimentation sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
du switch	Nombre total de ports utilisés sur le pare-feu. Les ports s'affichent au format *A*/*B*, où *A* correspond au nombre de ports qui fonctionnent bien et *B* au nombre total de ports sur le pare-feu.

© 2020 Palo Alto Networks, Inc.

Panorama > Périphériques gérés > État > Périphériques anormaux

L'onglet Périphériques anormaux présente les périphériques dont les mesures s'écartent de leur base de référence calculée ; les mesures divergentes sont indiquées en rouge. On obtient la base de référence de l'état de santé en calculant la moyenne de la performance de l'état pour une mesure donnée sur une période de sept jours plus l'écart type.

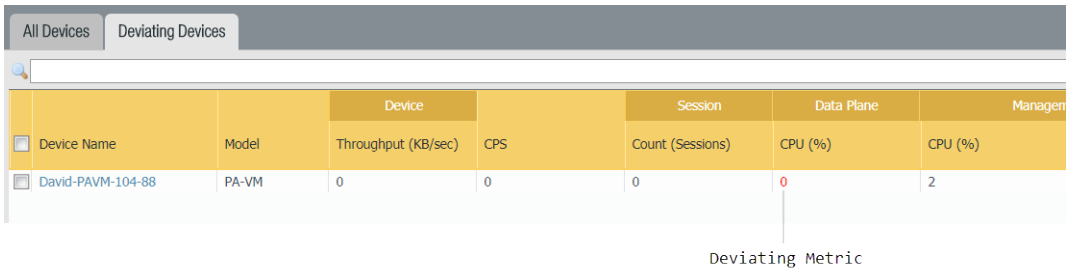


Figure 1: Exemple d'une mesure anormale

État détaillé des périphériques dans Panorama

Vous pouvez afficher un historique de l'état détaillé des périphériques d'un seul pare-feu en cliquant sur le Nom du périphérique dans l'onglet Tous les périphériques ou dans l'onglet Périphériques déviateurs. La Vue détaillée des périphériques présente l'historique de l'état de santé au moyen d'un filtre de temps et affiche les métadonnées associées au périphérique. Les informations sur l'état du périphérique s'affichent sous forme de tableau ou de widget, lorsque possible, afin de fournir une représentation graphique de l'évolution des données dans le temps.

Gestion de la Vue détaillée des périphériques

En plus des métadonnées descriptives associées au pare-feu, la Vue détaillée des périphériques affiche les informations sur l'état détaillé du pare-feu. Le cas échéant, vous pouvez configurer les Paramètres (⚙) des options supplémentaires du widget ou Maximiser le panneau (▭) pour agrandir le widget.

Champ	Description
Actions	
Filtre de temps	Sélectionnez le filtre pour afficher l'historique de l'état des périphériques dans la liste déroulante. Vous pouvez sélectionner **Last 12 hours (12 dernières heures)**, **24 hours (24 heures)**, **7 days (7 jours)**, **15 days (15 jours)**, **30 days (30 jours)** ou **90 days (90 jours)**.
Montrer la moyenne	Sélectionnez la moyenne et la distribution traditionnelle présentée pour les widgets dont l'évolution au fil du temps est analysée. Vous pouvez sélectionnez **None (Aucuns)**, **Last 24 hours (24 dernières heures)**, **7 days (7 jours)** ou **15 days (15 jours)**.
Actualiser	Actualise les informations affichées en y intégrant les données les plus récentes.
Imprimer un PDF	Génère un PDF de l'onglet actuellement affiché.

© 2020 Palo Alto Networks, Inc.

Champ	Description
	Les fenêtres contextuelles doivent être activées pour sélectionner l'emplacement du téléchargement et pour accéder au PDF.
Information système	
Information système	Les métadonnées associées au périphérique : adresse IP, version du logiciel, version de l'antivirus, état HA, numéro de série, version Appplications et menaces, version WildFire, mode VSYS, modèle et mode du périphérique.

Sessions

L'onglet Sessions affiche les informations sur les sessions qui traversent le pare-feu. Ces informations s'affichent sous la forme de six graphiques individuels.

Champ	Description
Débit	Le débit des données au fil du temps (moyenne sur cinq minutes) mesuré en kilobit par seconde (Kbit/s).
Compte de session	Compte de session total au fil du temps (moyenne sur cinq minutes).
Connexions par seconde	Connexions par seconde totales pour le périphérique au fil du temps (moyenne sur cinq minutes).
Paquets par seconde	Paquets par seconde totaux (moyenne sur cinq minutes) qui ont traversé le périphérique.
Pourcentage d'utilisation de la table de sessions globale (appareils PA-7000 et PA-5200 uniquement).	Le pourcentage d'utilisation de la table de sessions globale au fil du temps pour les pare-feu qui disposent d'une table de sessions globale (moyenne sur cinq minutes).
Pourcentage d'utilisation de la table de sessions	Présente le pourcentage d'utilisation de la table de sessions pour chaque panneau de données du pare-feu au fil du temps (moyenne sur cinq minutes).
Informations sur les sessions SSL déchiffrées	Présente le nombre de sessions SSL déchiffrées au fil du temps (moyenne sur cinq minutes).
Pourcentage d'utilisation des sessions de proxy SSL	Présente le nombre de sessions de proxy au fil du temps (moyenne sur cinq minutes).

Environnements

L'onglet **Environments (Environnements)** affiche la présence, l'état et les conditions de fonctionnement du matériel, par exemple l'alimentation électrique, le support de ventilateur et les disques durs. Cet onglet ne s'affiche que pour les pare-feu matériels :

© 2020 Palo Alto Networks, Inc.

Champ	Description
État des ventilateurs	Présente la présence, l'état actuel, le nombre de tours par minute et le dernier échec des ventilateurs de chaque support de ventilateur. L'état des ventilateurs s'affiche au format *A*/*B*, où *A* correspond au nombre de ventilateurs qui fonctionnent bien et *B* au nombre total de ventilateurs sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
Alimentation	Présente la présence, l'état actuel et l'horodatage du dernier échec. L'état de l'alimentation s'affiche au format *A*/*B*, où *A* correspond au nombre de blocs d'alimentation qui fonctionnent bien et *B* au nombre total de blocs d'alimentation sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
État thermique	Indique s'il y a des alarmes thermiques associées à chaque logement du périphérique. S'il existe une alarme active, le pare-feu affiche plus d'informations spécifiques concernant la température exacte et l'emplacement.
État du disque système	Affiche le pourcentage d'utilisation, d'espace disponible et d'espace utilisé sur les supports racine, pancfg, panlogs, and panrepo. L'État du disque système présente également le nom du disque, sa taille et l'état RAID des pare-feu compatibles RAID.

Interfaces

L'onglet Interfaces affiche l'état et les statistiques de l'ensemble des interfaces physiques du pare-feu.

Champ	Description
Nom de l'interface	Le nom de l'interface. Sélectionnez une Interface pour afficher les graphiques Débit binaire, Paquets par seconde, Erreurs et Abandons de l'interface sélectionnée.
Status (État)	L'état de l'interface : `Admin Up`, `Admin Down`, `Operational Up` ou `Operational Down`.
Débit binaire	Affiche le débit binaire (bps) des données reçues et transmises.
Paquets par seconde	Affiche le nombre de paquets par secondes correspondant aux données reçues et transmises.
Erreurs	Affiche le nombre d'erreurs applicables aux données reçues et transmises.
Abandons	Affiche le nombre de connexions abandonnées correspondant aux données reçues et transmises.

de journalisation

L'onglet Journalisation affiche les taux de journalisation et les connexions de l'ensemble des pare-feu gérés.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Taux de journalisation	Affiche le taux moyen mesuré sur une période d'une minute pour les journaux de transfert vers Panorama ou vers un Collecteur de journaux du périphérique.
Connexions de journalisation	Présente toutes les connexions de transfert des journaux disponibles, y compris leur état actif ou inactif.
Transfert des journaux externe	Affiche le taux d'envoi, d'abandon et de transfert moyen (journaux par seconde) pour diverses méthodes de transfert des journaux externe.

Resources

L'onglet Ressources présente les statistiques relatives à la mémoire et au processeur du pare-feu.

Champ	Description
Mémoire du plan de gestion	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de la mémoire du plan de gestion sous forme de pourcentage.
Mémoires tampons des paquets	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de l'utilisation de la mémoire tampon des paquets sous forme de pourcentage. Dans un système qui comporte plusieurs plans de données, cette vue présente différents plans de données, processeurs et mémoires tampons des paquets en diverses couleurs.
Descripteurs de paquet	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de l'utilisation du descripteur de paquet sous forme de pourcentage. Dans un système qui comporte plusieurs plans de données, cette vue présente différents plans de données, processeurs et mémoires tampons des paquets en diverses couleurs.
Plan de gestion du processeur	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) du processeur sous forme de pourcentage.
Plan de données du processeur	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) par utilisation essentielle du plan de données du processeur. Pour les systèmes qui comportent plusieurs plans de données, vous pouvez sélectionner le plan de données à afficher.
Supports	Affiche les informations sur le fichier système du périphérique. Le Nom du support, l'espace alloué (en Ko), l'espace utilisé (en Ko), et l'espace disponible (en Ko) ainsi que le pourcentage d'utilisation s'affichent.

Haute disponibilité

L'onglet Haute disponibilité présente l'état HA du pare-feu et de son homologue HA. Le widget supérieur affiche la configuration et la version de contenu du périphérique et de ses homologues. Le widget inférieur fournit des informations sur les basculements HA antérieurs ainsi que les motifs qui y sont associés et indique notamment le pare-feu qui a échoué.

© 2020 Palo Alto Networks, Inc.

Panorama > Modèles

Grâce aux onglets **Périphérique** et **Réseau**, vous pouvez déployer une configuration à base commune sur plusieurs pare-feu nécessitant des paramètres similaires à l'aide d'un modèle ou d'une pile de modèles (une combinaison de modèles). Lors de la gestion des configurations de pare-feu avec Panorama, vous utilisez une combinaison de groupe de périphériques (pour gérer les politiques et objets partagés) et de modèles (pour gérer les paramètres de périphérique et de réseau partagés).

En plus des paramètres disponibles depuis les boîtes de dialogue pour la création de Modèles ou de Piles de modèles, **Panorama** > **Modèles** affiche les colonnes suivantes :

- **Type** - Identifie les entrées qui sont figurent en tant que modèles ou piles de modèles.
- **Pile** - Énumère les modèles assignés à une pile de modèles.

Que souhaitez-vous faire ?	Reportez-vous à la section :
Ajouter, cloner, éditer ou supprimer un modèle	Modèles
Ajouter, cloner, éditer ou supprimer une pile de modèles	Piles de Modèles
Vous souhaitez en savoir plus ?	Modèles et piles de modèle
	Gérer les modèles et les piles de modèle

Modèles

Panorama prend en charge jusqu'à 1 024 modèles. Vous pouvez **Add (Ajouter)** un modèle et configurer les paramètres comme décrit dans le tableau suivant. Après avoir créé un modèle, vous devez également configurer une pile de modèles et ajouter les modèles et les pare-feu à la pile de modèles avant de pouvoir gérer vos pare-feu. Après avoir configuré un modèle, vous devez valider vos modifications dans Panorama (reportez-vous à la section Opérations de validation de Panorama).

La suppression d'un modèle n'entraînera pas la suppression des valeurs appliquées par Panorama au pare-feu.

Paramètres du modèle	Description
Name (Nom)	Donnez un nom au modèle (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, points et traits de soulignement. Dans les onglets **Périphérique** et **Réseau**, ce nom apparaît dans la liste déroulante **Modèle.** Les paramètres que vous modifiez dans ces onglets s'appliquent uniquement au **Template (Modèle)** sélectionné.
Description	Saisissez une description du modèle.

© 2020 Palo Alto Networks, Inc.

Piles de Modèles

Vous pouvez configurer une pile de modèles ou affecter des modèles à une pile de modèles. L'affectation de pare-feu à une piles de modèles vous permet de transmettre tous les paramètres nécessaires aux pare-feu plutôt que de devoir ajouter chaque paramètre à chaque modèle de manière individuelle. Panorama prend en charge jusqu'à 1 024 piles. Vous pouvez **Add Stack (Ajouter une pile)** pour créer une nouvelle piles de modèles et configurer les paramètres comme décrit dans le tableau suivant. Après avoir configuré une piles de modèles, vous devez valider vos modifications dans Panorama (reportez-vous à la section Opérations de validation de Panorama). De plus, après avoir configuré les paramètres du réseau et du périphérique des pare-feu affectés à la pile, vous devez effectuer une validation du modèle pour appliquer les paramètres aux pare-feu.

La suppression d'une pile de modèles ou la suppression d'un pare-feu d'une pile de modèles ne supprime pas les valeurs que Panorama a précédemment envoyées à ce pare-feu. Toutefois, lorsque vous supprimez un pare-feu d'une pile de modèles, Panorama n'envoie plus de nouvelles mises à jour à ce pare-feu.

Paramètres de la pile de modèles	Description
Name (Nom)	Donnez un nom à la pile (31 caractères maximum). Le nom est sensible à la casse, doit être unique, doit commencer par une lettre et ne peut contenir que des lettres, des chiffres et des caractères de soulignement. Dans les onglets **Device (Périphérique)** et **Network (Réseau)**, la liste déroulante **Template (Modèle)** affiche le nom de la pile et les modèles qui lui sont affectés.
Description	Saisissez une description de la pile.
Modèles	Vous pouvez **Ajouter** chaque modèle que vous voulez inclure dans la pile (jusqu'à 8). Si des modèles comportent des paramètres en double, Panorama n'applique que les paramètres du modèle le plus haut dans la liste lorsqu'il applique les paramètres aux pare-feu affectés. Par exemple, si Modèle_A est situé au-dessus de Modèle_B dans la liste et que les deux modèles définissent l'interface ethernet1/1, Panorama applique alors la définition ethernet1/1 du Modèle_A et non celle du Modèle_B. Pour modifier l'ordre des modèles dans la liste, vous devez sélectionner un modèle et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. *Panorama ne valide pas les combinaisons de modèles dans les piles, planifiez donc l'ordre de vos modèles pour éviter de générer des relations incorrectes.*
Périphériques	Sélectionnez chacun des pare-feu que vous voulez ajouter à la pile. Si la liste de pare-feu est longue, vous pouvez la filtrer par **Platforms (Plates-formes)**, **Device Groups (Groupes de périphériques)**, **Tags (Étiquettes)** ou **HA Status (État HA)**. *Vous pouvez affecter des pare-feu dont les modes ne correspondent pas (VPN, systèmes virtuels multiples ou opérationnel) à la même pile. Panorama applique les paramètres spécifiques des modes aux pare-feu prenant en charge ces modes uniquement.*

© 2020 Palo Alto Networks, Inc.

Paramètres de la pile de modèles	Description
Sélectionner tout	Sélectionne chacun des pare-feu qui figurent dans la liste.
Désélectionner tout	Sélectionne chacun des pare-feu qui figurent dans la liste.
Regrouper les homologues HA	Regroupe les pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Lors de l'application des paramètres de la pile de modèles, vous pouvez les appliquer à la paire regroupée plutôt qu'à chaque des pare-feu individuellement.
Filtre sélectionné	Pour n'afficher que des pare-feu spécifiques, sélectionnez-les, puis l'option **Filter Selected (Filtre sélectionné)**.

Panorama > Modèles > Variables des modèles

- Création de nouvelles variables de modèles
- Modifier les variables de modèles existantes
- Créer ou modifier les définitions de variables sur un périphérique

Vous pouvez définir des variables (**Panorama** > **Templates (Modèles)**) pour des modèles ou des piles de modèles ou vous pouvez modifier les variables existantes d'un appareil individuel (**Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**). Les variables sont des éléments de la configuration définis sur le modèle ou sur la pile de modèles qui procurent souplesse et la possibilité de réutilisation lorsque vous utilisez Panorama pour gérer les configurations d'un pare-feu. Vous pouvez utiliser les variables pour remplacer :

- Une adresse IP (notamment un masque réseau IP, une plage d'adresses IP et un FQDN) dans toutes les zones de configuration.
- Des interfaces dans une configuration de passerelle IKE (Interface) et dans une configuration HA (ID du groupe).

Lorsque vous ajoutez des pare-feu à une piles de modèles, ceux-ci héritent automatiquement des variables que vous avez créées pour un modèle ou une piles de modèles.

Informations sur les variables des modèles	Description
Name (Nom)	Nom de la définition de la variable.
Modèle (périphérique et piles de modèles)	Affiche le nom du modèle auquel la définition de la variable appartient.
Type	Affiche le type de définition de la variable : • **IP Netmask (Masque réseau IP)** : définit une adresse ou une adresse IP statique. • **IP Range (PLage d'adresses IP)** : définit une plage d'adresses IP. Par exemple, 192.168.1.10-192.168.1.20. • **FQDN (FQDN)** : définit un Fully Qualified Domain Name (nom de domaine complet ; FQDN).

© 2020 Palo Alto Networks, Inc.

Informations sur les variables des modèles	Description
	• **Group ID (ID du groupe)** : définit l'ID du groupe haute disponibilité. Pour obtenir de plus amples renseignements, reportez-vous à la section Directives concernant les configurations HA actives/passives. • **Interface** : définit une interface de pare-feu sur le pare-feu. Ne peut être utilisée que pour une configuration de passerelle IKE.
Valeur	Affiche la valeur qui a été configurée pour la définition de la variable.
Ajouter (modèle et piles de modèles)	Ajoute une nouvelle définition de la variable d'un modèle.
Supprimer	Supprime une définition de variable d'un modèle existante.
Cloner	Clone une définition de variable d'un modèle existante.
Remplacer (pile de modèles et périphérique)	Remplace la définition d'une variable d'un modèle existante héritée de la pile de modèles ou du périphérique. Vous ne pouvez modifier le nom de la variable, ni son type, et vous ne pouvez pas remplacer les variables propres aux périphériques.
Rétablir (pile de modèles et périphérique)	Pour supprimer les valeurs remplacées au niveau de la pile de modèles ou du périphérique ; rétablit la variable remplacée par la définition de la variable du modèle initiale.
Obtenir les valeurs utilisées sur le périphérique uniquement (périphérique uniquement)	Renseigne la variable sélectionnée par la valeur utilisée sur le pare-feu. Il faut que la variable d'un modèle ou d'une pile de modèles soit déjà définie et appliquée au pare-feu avant que Panorama puisse récupérer la valeur. Les valeurs tirées du pare-feu **Override (remplaceront)** la variable du modèle ou de la pile de modèles afin de créer une variable propre au périphérique. Si aucune définition de variable n'a été appliquée au pare-feu, Panorama renvoie le message `Value not found` pour cette variable.

Création de nouvelles variables de modèles

Add (Ajoutez) une nouvelle définition de la variable d'un modèle.

Informations sur la définition d'une nouvelle variable d'un modèle	Description
Name (Nom)	Nommez la définition de la variable. Tous les noms des définitions de variables doivent commencer par le symbole du dollar ($).
Type	Sélectionnez le type de définition de la variable : **IP Netmask (Masque réseau IP)**, **IP Range (Plage d'adresses IP)**, **FQDN**, **Group ID (ID du groupe)** ou **Interface**.

© 2020 Palo Alto Networks, Inc.

Informations sur la définition d'une nouvelle variable d'un modèle	Description
Valeur	Entrez la valeur souhaitée pour la définition de la variable.

Modifier les variables de modèles existantes

Vous pouvez modifier la définition d'une variable d'un modèle en tout temps après la création de la variable (**Panorama** > **Templates (Modèles)**). **Manage (Gérez)** les variables du modèle pour sélectionner une variable et modifier les valeurs disponibles, au besoin.

Créer ou modifier les définitions de variables sur un périphérique

Allez à **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** pour créer des définitions de variables ou pour remplacer des variables de modèles qui ont été appliquées à partir d'un modèle ou d'une pile de modèles Panorama. Voici des exemples de variables de modèles :

- Une adresse IP (masque réseau IP, plage d'adresses IP ou FQDN) dans toutes les zones de configuration.
- Des interfaces dans une configuration de passerelle IKE (Interface) ou dans une configuration HA (ID du groupe).

La création d'une variable de périphérique vous permet de copier des variables propres à un périphérique qui ont été remplacées à partir d'un périphérique qui se trouve dans la même pile de modèles sans que vous ayez à les créer de nouveau. Par défaut, toutes les définitions des variables sont héritées du modèle ou de la piles de modèles et ne peuvent être remplacées (vous ne pouvez pas supprimer les définitions des variables d'un périphérique individuel ni en créer de nouvelles).

Create (Créez) des définitions de variables de périphérique en copiant des définitions de variables à partir des périphériques qui se trouvent dans la pile de modèles ou **Edit (Modifiez)** les définitions de variables existantes.

© 2020 Palo Alto Networks, Inc.

Panorama > Groupes de périphériques

Les groupes de périphériques sont constitués de pare-feu et de systèmes virtuels que vous souhaitez gérer en tant que groupe, tels que les pare-feu qui gèrent un groupe de succursales ou de services dans une entreprise. Panorama traite ces groupes comme des unités individuelles lors de l'application de politiques. Un pare-feu ne peut appartenir qu'à un seul groupe de périphériques. Cependant, les systèmes virtuels étant des entités distinctes dans Panorama, vous pouvez attribuer des systèmes virtuels d'un pare-feu à différents groupes de périphériques.

Vous pouvez imbriquer des groupes de périphériques à une hiérarchie d'arborescence pouvant comporter jusqu'à quatre niveaux sous l'emplacement partagé afin de mettre en œuvre une approche en couche pour gérer les politiques au sein de votre réseau de pare-feu. Au niveau inférieur, un groupe de périphériques peut avoir des groupes de périphériques parents, grands-parents et arrière-grands-parents à des niveaux supérieurs successifs (collectivement appelés *anciens*) dont le groupe de périphériques de niveau inférieur hérite des politiques et objets. Au niveau supérieur, un groupe de périphériques peut avoir des groupes de périphériques enfants, petits-enfants et arrière-petits-enfants — collectivement appelés *descendants*. Lorsque vous sélectionnez **Panorama** > **Device Groups (Groupes de périphériques)**, la colonne Nom affiche cette hiérarchie de groupe de périphériques.

Après avoir ajouté, modifié ou supprimé un groupe de périphériques, vous devez effectuer une validation de Panorama et une validation du groupe de périphériques (reportez-vous à la section Opérations de validation de Panorama). Panorama diffuse ensuite les modifications de configuration aux pare-feu affectés au groupe de périphériques. Panorama prend en charge jusqu'à 1 024 groupes de périphériques.

Pour configurer un groupe de périphériques, vous devez en **Ajouter** un et configurer les paramètres comme décrit dans le tableau suivant.

Paramètres du groupe de périphériques	Description
Name (Nom)	Saisissez un nom pour identifier le groupe (31 caractères maximum). Le nom est sensible à la casse, doit être unique sur l'ensemble de la hiérarchie du groupe de périphériques et ne peut contenir que des lettres, des chiffres, des espaces, des traits d'union et des caractères de soulignement.
Description	Saisissez une description du groupe de périphérique.
Périphériques	Sélectionnez chacun des pare-feu que vous voulez ajouter au groupe de périphériques. Si la liste de pare-feu est longue, vous pouvez filtrer par **Device State (État du périphérique)**, **Platforms (Plates-formes)**, **Templates (Modèles)** ou **Tags (Étiquettes)**. La section Filtres affiche (entre parenthèses) le nombre de pare-feu gérés pour chacune de ces catégories. Si l'objectif d'un groupe de périphériques est purement organisationnel (à savoir qu'il est conçu pour contenir d'autres groupes de périphériques), vous ne devez pas nécessairement lui affecter des pare-feu.
Sélectionner tout	Sélectionne chaque pare-feu et système virtuel de la liste.
Désélectionner tout	Désélectionne chaque pare-feu et système virtuel de la liste.

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe de périphériques	Description
Regrouper les homologues HA	Sélectionnez pour regrouper les pare-feu homologues dans une configuration haute disponibilité (HA). La liste affiche alors le pare-feu actif (ou actif/principal dans une configuration active/active), suivi du pare-feu passif (ou actif/secondaire dans une configuration active/active) entre parenthèses. Ceci vous permet d'identifier facilement les pare-feu en mode HA. Lors de l'application de politiques partagées, vous pouvez l'appliquer à la paire regroupée plutôt qu'à chaque homologue. *Pour les homologues HA dans une configuration active/passive, pensez à ajouter les deux pare-feu ou leurs systèmes virtuels au même groupe de périphériques. Ceci vous permet d'appliquer la configuration aux deux homologues simultanément.*
Filtre sélectionné	Si vous souhaitez que la liste Périphériques n'affiche que des pare-feu spécifiques, sélectionnez les pare-feu, puis **Filter Selected (Filtre sélectionné)**.
Groupe de périphériques parent	En fonction du groupe de périphériques que vous définissez, sélectionnez le groupe de périphériques (ou l'emplacement Partagé) situé juste au-dessus de lui dans la hiérarchie (**Shared (Partagé)** est défini par défaut).
Périphérique principal	Pour configurer les règles de politique et les rapports en fonction des noms d'utilisateur et des groupes d'utilisateurs, vous devez sélectionner un **Master Device (Périphérique principal)**. Il s'agit du pare-feu à partir duquel Panorama reçoit des noms d'utilisateur, des noms de groupe d'utilisateurs et des informations de mappage de nom d'utilisateur à un groupe. *Lorsque vous modifiez le Master Device (Périphérique principal) ou que vous le configurez sur None (Aucun), Panorama perd toutes les informations d'utilisateur et de groupe reçues par ce pare-feu.*
Stocker les utilisateurs et les groupes à partir du périphérique principal	Cette option s'affiche uniquement si vous sélectionnez un **Master Device (Périphérique principal)**. L'option permet à Panorama de stocker localement les noms d'utilisateur, les noms des groupes d'utilisateurs et les informations de mappage de nom d'utilisateur à un groupe qu'il reçoit par le **Master Device (Périphérique principal)**. Pour activer le stockage local, vous devez également sélectionner **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifier les paramètres de Panorama et Activer les rapports et le filtrage sur les groupes.
Propriétés du périphérique ajoutées dynamiquement – Lorsqu'un nouveau périphérique est ajouté au groupe de périphériques, Panorama applique dynamiquement le code d'autorisation spécifié et la version du logiciel PAN-OS au nouveau périphérique. Cela s'affiche uniquement après qu'un groupe de périphériques a été associé à une définition de service NSX dans Panorama.	
Code d'autorisation	Saisissez le code d'autorisation à appliquer aux périphériques ajoutés à ce groupe de périphériques.
Version du logiciel	Sélectionnez la version de logiciel à appliquer aux périphériques ajoutés à ce groupe de périphériques.

© 2020 Palo Alto Networks, Inc.

Panorama > Collecteurs gérés

Le serveur de gestion Panorama (appareil de série M ou appareil virtuel Panorama en mode Panorama) peut gérer les Collecteurs de journaux dédiés (appareils de série M ou appareil virtuel Panorama en mode Collecteur de journaux). Chaque serveur de gestion Panorama possède également un Collecteur de journaux local prédéfini (nommé par défaut) afin de traiter les journaux qu'il reçoit directement depuis les pare-feu. (Un équipement virtuel Panorama en Mode hérité stocke les journaux reçus directement des pare-feu sans utiliser un collecteur de journaux dédié.)

Si vous souhaitez utiliser Panorama pour la gestion d'un collecteur de journaux dédié, vous devez ajouter le collecteur de journaux en tant que *collecteur géré*.

Que souhaitez-vous faire ?	Reportez-vous à la section :
Afficher les informations des collecteurs de journaux	Informations sur les collecteurs de journaux
Ajouter, modifier ou supprimer un Collecteur de journaux	Configuration du Collecteur de journaux
Mettre à jour le logiciel Panorama sur un Collecteur de journaux	Mises à jour logicielles pour les collecteurs de journaux dédiés
Vous souhaitez en savoir plus ?	Journalisation centralisée et génération de rapports
	Configurer un Collecteur Géré

Informations sur les collecteurs de journaux

Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour afficher les informations suivantes pour les Collecteurs de journaux. Vous pourrez configurer d'autres paramètres lors de la Configuration du Collecteur de journaux.

Informations sur les collecteurs de journaux	Description
Nom du collecteur	Le nom qui identifie ce collecteur de journaux. Ce nom s'affiche en tant que nom d'hôte du collecteur de journaux.
Numéro de série	Le numéro de série de l'équipement Panorama qui agit en tant que Collecteur de journaux. Si le Collecteur de journaux est local, il s'agit du numéro de série du serveur de gestion Panorama.
Version du logiciel	La version du logiciel Panorama installée sur le collecteur de journaux.
Adresse IP	L'adresse IP de l'interface de gestion installée sur le collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

Informations sur les collecteurs de journaux	Description
Connected (Connecté)	L'état de la connexion établie entre le collecteur de journaux et Panorama.
État/Détail de la configuration	Indique si la configuration sur le collecteur de journaux est synchronisée avec Panorama.
État/Détail d'exécution	L'état de la connexion établie entre ce collecteur de journaux et les autres collecteurs de journaux qui font partie du groupe de collecteurs.
État de la redistribution des journaux	Certaines actions (par exemple, ajout de disques) entraîneront la redistribution, par le collecteur de journaux, des journaux entre ses paires de disques. Cette colonne indique l'état d'achèvement du processus de redistribution en pourcentage.
État de la dernière validation	Indique si la dernière validation du groupe de collecteurs effectuée à l'égard du collecteur de journaux a échoué ou réussi.
Statistiques	Après avoir terminé la Configuration du Collecteur de journaux, cliquez sur **Statistiques** pour afficher les informations sur le disque, les performances du processeur et le taux moyen de journalisation (journaux / secondes). Afin de mieux comprendre la plage de journaux affichée, vous pouvez également consulter les informations du journal le plus ancien que le collecteur a reçu. *Si vous utilisez un Gestionnaire SNMP pour un suivi centralisé, vous pouvez également consulter les statistiques de journaux dans l'objet de la MIB panLogCollector.*

Configuration du Collecteur de journaux

Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour gérer les Collecteurs de journaux. Lorsque vous **Ajoutez** un nouveau Collecteur de journaux en tant que collecteur géré, les paramètres que vous configurez varient selon l'emplacement du Collecteur de journaux et le déploiement ou non de Panorama dans une configuration haute disponibilité (HD) :

- **Collecteur de journaux dédié** – lorsque vous ajoutez le Collecteur de journaux, l'onglet **Interfaces** ne s'affiche pas dans un premier temps. Vous devez saisir le numéro de série (**Collecteur S/N**) du Collecteur de journaux, cliquer sur **OK**, puis éditer le Collecteur de journaux pour afficher les paramètres de l'interface.
- **Collecteur de journaux par défaut local pour le serveur de gestion Panorama solitaire (non HD) ou actif (HD)** – après avoir saisi le numéro de série (**Collecteur S / N**) du serveur de gestion Panorama, la boîte de dialogue Collecteur affiche uniquement les **Disques**, les paramètres de **Communication** et un sous-ensemble de paramètres **Généraux.** Pour tous les autres paramètres, le Collecteur de journaux dérive ses valeurs de la configuration du serveur de gestion Panorama.
- (HD uniquement) **Collecteur de journaux par défaut local au serveur de gestion Panorama passif –** Panorama traite ce Collecteur de journaux comme s'il était situé à distance : vous devez donc le configurer comme vous le feriez pour un Collecteur de journaux dédié.

La procédure complète pour la configuration d'un Collecteur de journaux exige l'accomplissement de tâches supplémentaires.

© 2020 Palo Alto Networks, Inc.

Que voulez-vous faire ?	Reportez-vous à la section :
Identifier le Collecteur de journaux et définir ses connexions au serveur de gestion Panorama et aux services externes.	Paramètres généraux du collecteur de journaux
Configurer l'accès à la CLI du collecteur de journaux.	Paramètres d'authentification CLI du collecteur de journaux
Configurez les interfaces que le Collecteur de journaux dédié utilise pour le trafic de gestion, la communication du Groupe de collecteurs et la collecte des journaux.	Paramètres d'une interface de collecteur de journaux
Configurer les disques RAID qui stockent les journaux recueillis à partir des pare-feu.	Paramètres du disque RAID du collecteur de journaux
Configurez le Collecteur de journaux pour recevoir les informations relatives au mappage des agents User-ID.	Paramètres de l'agent User-ID
Configurez le Collecteur de journaux pour vous authentifier avec les agents User-ID Windows.	Sécurité de la connexion
Configurez les paramètres de sécurité pour la communication avec Panorama, les autres Collecteurs de journaux et les pare-feu.	Paramètres de communication

Paramètres généraux du collecteur de journaux

- Panorama > Collecteurs gérés > Général

Configurez les paramètres comme décrits dans le tableau suivant pour identifier le Collecteur de journaux et définissez ses connexions au serveur de gestion Panorama, aux serveurs DNS et aux serveurs NTP.

Paramètres généraux des collecteurs de journaux	Description
N° de série du collecteur	(Requis) Saisissez le numéro de série de l'équipement Panorama qui agit en tant que Collecteur de journaux. Si le Collecteur de journaux est local, saisissez le numéro de série du serveur de gestion Panorama.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux des collecteurs de journaux	Description
Nom du collecteur	Saisissez un nom pour identifier ce Collecteur de journaux (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. Ce nom s'affiche en tant que nom d'hôte du collecteur de journaux.
Certificat entrant pour Syslog sécurisé	Sélectionnez le certificat que le collecteur géré doit utiliser pour ingérer les journaux du serveur Traps ™ ESM de manière sécurisée. Ce certificat est appelé un certificat entrant car Panorama / le Collecteur géré est le serveur auquel le Traps ESM (client) envoie des journaux. Le certificat est requis si le protocole de **Transport** pour le profil d'ingestion des journaux est **SSL**.
Certificat pour Secure Syslog	Sélectionnez un certificat pour le transfert sécurisé des journaux système à un serveur Syslog externe. L'option **Certificate for Secure Syslog (Certificat pour Secure Syslog)** doit être sélectionnée sur le certificat (voir Gestion des certificats du pare-feu de Panorama). Lorsque vous affectez un profil de serveur Syslog au Groupe de collecteurs qui inclut ce Collecteur de journaux (voir Panorama > Groupe de collecteurs, **Panorama** > **Collector Groups (Groupes de collecteurs)** > **Collector Log Forwarding (Transfert de collecteurs de journaux)**), le protocole de **Transport** du profil du serveur doit être **SSL** (voir (Device (Périphérique) > Server Profiles (Profils de serveur) > Syslog).
Serveur IP de Panorama	Indiquez l'adresse IP du serveur de gestion Panorama qui gère ce collecteur de journaux.
Serveur IP 2 de Panorama	Indiquez l'adresse IP du homologue secondaire si le serveur de gestion Panorama est déployé dans une configuration haute disponibilité (HA).
Domain (Domaine)	Saisissez le nom de domaine du Collecteur de journaux.
Serveur DNS principal	Saisissez l'adresse IP du serveur DNS principal. Le Collecteur de journaux utilise ce serveur pour les recherches DNS (pour rechercher le serveur de gestion Panorama, par exemple).
Serveur DNS secondaire	(Facultatif) Saisissez l'adresse IP d'un serveur DNS secondaire à utiliser si le serveur principal n'est pas disponible.
Serveur NTP principal	Saisissez l'adresse IP ou le nom d'hôte du serveur NTP principal (le cas échéant). Si vous n'utilisez pas de serveurs NTP, vous pouvez définir l'heure du Collecteur de journaux manuellement.
Serveur NTP secondaire	(Facultatif) Saisissez l'adresse IP ou le nom d'hôte de serveurs NTP secondaires à utiliser si le serveur principal n'est pas disponible.
Fuseau horaire	Sélectionnez le fuseau horaire du Collecteur de journaux.
Latitude	Saisissez la latitude (de -90,0 à 90,0) du collecteur de journaux. Les cartes du trafic et des menaces utilisent la latitude d'App Scope.

© 2020 Palo Alto Networks, Inc.

Paramètres généraux des collecteurs de journaux	Description
Longitude	Saisissez la longitude (de -180,0 à 180,0) du collecteur de journaux. Les cartes du trafic et des menaces utilisent la longitude d'App Scope.

Paramètres d'authentification CLI du collecteur de journaux

- Panorama > Collecteurs gérés > Authentification

Un équipement M-Series en mode collecteur de journaux (collecteur de journaux dédié) n'a pas d'interface Web, uniquement un CLI. Vous pouvez utiliser le serveur de gestion Panorama pour configurer la plupart des paramètres sur un collecteur de journaux dédié. Certains paramètres nécessitent toutefois un accès à la CLI. Pour configurer les paramètres d'authentification pour accéder à la CLI, configurez les champs comme décrits dans le tableau suivant.

Paramètres d'authentification des collecteurs de journaux	Description
Users (Utilisateurs)	Indique toujours `admin` et est utilisé pour le nom de connexion à la CLI locale du collecteur de journaux.
Mode	Sélectionnez le **Mode** du mot de passe : • **Mot de passe** – Saisissez un **Mot de passe** en clair et **Confirmez le Mot de passe**. • **Password Hash (Hachage du mot de passe)** – Saisissez une chaîne de mot de passe haché. Cela peut être utile si vous souhaitez par exemple réutiliser le mot de passe d'un compte Unix existant, mais que vous connaissez uniquement le mot de passe haché, et pas le mot de passe en texte clair. Panorama accepte n'importe quelle chaîne comprenant jusqu'à 63 caractères, quel que soit l'algorithme utilisé pour générer la valeur de hachage. Le mot de passe de la commande opérationnelle CLI **`request password-hash password <`***mot de passe***`>`** utilise l'algorithme MD5. Lorsque vous validez vos modifications, Panorama applique la valeur de hachage au Collecteur de journaux et le mot de passe de l'administrateur correspondra au **<***mot de passe***>** spécifié.
Tentatives échouées	Saisissez le nombre d'échecs de tentatives de connexion autorisés pour la CLI avant le verrouillage de l'administrateur (plage de 0 à 10). Une valeur de 0 indique un nombre illimité de tentatives de connexion. La valeur par défaut est de 0 pour les Collecteurs de journaux en mode opérationnel normal et de 10 pour les Collecteurs de journaux en mode FIPS-CC. Limiter les tentatives de connexion peut vous permettre de protéger le Collecteur de journaux contre les attaques en force.  *Si vous définissez le champ Failed Attempts (Tentatives échouées) sur une valeur non nulle, mais que vous laissez le champ Lockout Time (Durée de verrouillage) sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de Failed Attempts*

© 2020 Palo Alto Networks, Inc.

Paramètres d'authentification des collecteurs de journaux	Description
	(Tentatives échouées) et de Lockout Time (Durée de verrouillage) sur et transmettre les changements de configuration au collecteur de journaux. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur 0 par défaut pour les Failed Attempts (Tentatives échouées) et la Lockout Time (Durée de verrouillage).
Durée de verrouillage	Saisissez le nombre de minutes pendant lesquelles le Collecteur de journaux verrouille l'administrateur lorsqu'il a atteint le nombre autorisé de **Failed Attempts (Tentatives échouées)** (plage de 0 à 60, 0 par défaut). *Si vous définissez le champ Failed Attempts (Tentatives échouées) sur une valeur non nulle, mais que vous laissez le champ Lockout Time (Durée de verrouillage) sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de Failed Attempts (Tentatives échouées) et de Lockout Time (Durée de verrouillage) sur et transmettre les changements de configuration au collecteur de journaux. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur 0 par défaut pour les Failed Attempts (Tentatives échouées) et la Lockout Time (Durée de verrouillage).*

Paramètres d'une interface de collecteur de journaux

- Panorama > Collecteurs gérés > Interfaces

Par défaut, les Collecteurs de journaux dédiés (appareils de série M en mode Collecteur de Journaux) utilisent l'interface de gestion (MGT) pour le trafic de gestion, la collecte de journaux et la communication au Groupe de collecteurs. Toutefois, Palo Alto Networks vous recommande d'attribuer des interfaces distinctes pour la collecte des journaux et la communication du Groupe de collecteurs afin de réduire le trafic sur l'interface MGT. Vous pouvez améliorer la sécurité en définissant un sous-réseau distinct pour l'interface de gestion qui est plus privée que les sous-réseaux pour les autres interfaces. Pour utiliser des interfaces distinctes, vous devez d'abord les configurer sur le serveur de gestion Panorama (voir Périphérique > Configuration > Gestion). Les interfaces disponibles pour la collecte des journaux et la Communication du groupe de collecteurs varient en fonction du modèle d'appareil du Collecteur de journaux. Par exemple, l'appareil M-500 comporte les interfaces suivantes : Ethernet1 (1 Gbit/s), Ethernet2 (1 Gbit/s), Ethernet3 (1 Gbit/s), Ethernet4 (10 Gbit/s) Ethernet5 (10 Gbit/s)

Pour configurer une interface, sélectionnez le lien et configurez les paramètres de la manière décrite dans le tableau suivant.

Pour procéder à la configuration de l'interface de gestion, vous devez indiquer l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut. Si vous validez une configuration partielle (par exemple, il se peut que vous omettiez la passerelle par défaut), vous pouvez seulement accéder au pare-feu ou au Panorama par le biais du port de console afin d'apporter des modifications ultérieures à la configuration.

© 2020 Palo Alto Networks, Inc.

Validez toujours une configuration complète de l'interface MGT. Vous ne pouvez pas valider les configurations pour d'autres interfaces à moins d'indiquer l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut.

Paramètres d'une interface de collecteur de journaux	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Vous devez activer une interface pour la configurer. L'interface de gestion est une exception car elle est activée par défaut.
Vitesse et duplex	Configurez un débit de données et une option de duplex pour l'interface. Les choix possibles sont : 10 Mbit/s, 100 Mbit/s et 1 Gbit/s et 10 Gbit/s (Eth4 et Eth5 uniquement) en duplex intégral ou semi-duplex. Utilisez le paramètre de **négociation automatique** par défaut pour que le Collecteur de journaux détermine la vitesse de l'interface. *Ce paramètre doit correspondre aux paramètres d'interface de l'équipement réseau voisin.*
Adresse'A0;IP (IPv4)	Si votre réseau utilise IPv4, affectez une adresse IPv4 à l'interface.
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface MGT).
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:400:f00::1/64).
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Collecte des journaux de périphérique	Activez l'interface pour collecter les journaux à partir des pare-feu. Pour un déploiement avec un trafic de journaux élevé, vous pouvez activer plusieurs interfaces pour effectuer cette fonction. Cette fonction est activée par défaut sur l'interface MGT.
Communication avec les groupes de collecteurs	Activez l'interface pour la communication du Groupe de collecteurs. Seule une interface (par défaut, l'interface MGT) peut effectuer cette fonction.
Services de connexion réseau	Le service **Ping** est disponible sur toutes les interfaces et vous permet de tester la connectivité entre l'interface du Collecteur de journaux et les services externes. Les services suivants sont uniquement disponibles sur l'interface MGT :

© 2020 Palo Alto Networks, Inc.

Paramètres d'une interface de collecteur de journaux	Description
	• **SSH** – Permet un accès sécurisé à l'interface de ligne de commande Panorama. • **SNMP** – Permet à l'interface de recevoir des requêtes de statistiques en provenance d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – permet au Collecteur de journaux de redistribuer les informations de mappage des utilisateurs reçues des agents User-ID.
Adresses IP autorisées	Saisissez les adresses IP des systèmes clients qui peuvent accéder au Collecteur de journaux via cette interface. Une liste vide (par défaut) indique que tous les systèmes clients peuvent y accéder. *Palo Alto Networks vous recommande de ne pas laisser cette liste vide ; précisez les systèmes clients des administrateurs Panorama afin d'éviter tout accès non autorisé.*

Paramètres du disque RAID du collecteur de journaux

- Panorama > Collecteurs gérés > Disques

Après avoir configuré les disques de journalisation sur l'Appareil M-Series ou l'Appareil virtuel Panorama, vous pouvez les **Ajouter** à la configuration du Collecteur de journaux.

Par défaut, les appareils de la série M sont fournis avec la première paire RAID 1 installée dans les baies A1 et A2. Dans le logiciel, la paire de disques des baies A1 et A2 est nommée Paire de disques A. Les baies restantes sont nommées de manière séquentielle : paire de disques B, paire de disques C, etc. Par exemple, l'appareil M-500 prend en charge un maximum de 12 paires de disques. Vous pouvez Installer des paires de disques de 2 To ou 1 To dans le même appareil ; cependant, les deux lecteurs doivent faire la même taille dans chaque paire.

L'appareil virtuel Panorama prend en charge jusqu'à 12 disques de journalisation virtuels pour une capacité de stockage de 24 To.

Une fois les paires de disques ajoutées, le collecteur de journaux redistribue ses journaux existants sur tous les disques, ce qui peut prendre des heures pour chaque téraoctet de journaux. Pendant le processus de redistribution, le taux maximum d'ingestion des journaux est réduit. Dans la page **Panorama** > **Managed Collectors (Collecteurs gérés)**, la colonne État de la redistribution des journaux indique l'état de la progression du processus en pourcentage.

Si vous utilisez un Gestionnaire SNMP pour un suivi centralisé, vous pouvez consulter les statistiques de journaux dans l'objet de la MIB panLogCollector.

Paramètres de l'agent User-ID

- Panorama > Collecteurs gérés > Agents User-ID

Un Collecteur de journaux dédié peut recevoir des mappages d'utilisateurs provenant de jusqu'à 100 agents User-ID. Les agents peuvent être des agents User-ID intégrés à PAN-OS qui s'exécutent sur des pare-feu ou des agents User-ID basés sur Windows. Sur un pare-feu avec plusieurs systèmes virtuels,

© 2020 Palo Alto Networks, Inc.

chaque système virtuel peut servir d'agent User-ID individuel. Le Collecteur de journaux peut ensuite redistribuer les mappages d'utilisateurs aux pare-feu ou au serveur de gestion Panorama.

Les procédures complètes pour la configuration du mappage d'utilisateur et l'activation de la redistribution du mappage d'utilisateur nécessitent des tâches supplémentaires en plus de la connexion à des agents User-ID.

Pour configurer un Collecteur de journaux dédié pour qu'il se connecte à un agent User-ID, vous devez en **Ajouter** un et configurer les paramètres comme décrit dans le tableau suivant.

Paramètres de l'agent User-ID	Description
Name (Nom)	Donnez un nom pour identifier l'agent User-ID (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. *Dans le cas d'un pare-feu qui agit en tant qu'agent User-ID, ce champ n'a pas à correspondre au champ Nom du collecteur.*
Hôte	• **Agent User-ID Windows** - Saisissez l'adresse IP de l'hôte Windows sur lequel l'agent User-ID est installé. • **Pare-feu (agent User-ID intégré à PAN-OS)** – Saisissez le nom d'hôte ou l'adresse IP de l'interface que le pare-feu utilise pour redistribuer les mappages d'utilisateurs.
Port	Saisissez le numéro de port sur lequel l'agent User-ID écoutera les requêtes User-ID. La valeur par défaut est le port 5007, mais vous pouvez indiquer n'importe quel port disponible. Des agents User-ID différents peuvent utiliser des ports différents. *Certaines versions antérieures de l'agent User-ID utilisent par défaut le port 2010.*
Nom du collecteur	Le collecteur auquel ces champs se réfèrent est l'agent User-ID, et pas le Collecteur de journaux. Les champs ne s'appliquent que si l'agent est un pare-feu ou un système virtuel qui redistribue les mappages d'utilisateurs au Collecteur de journaux. Saisissez le **Nom du collecteur** et la **Clé prépartagée** qui identifient le pare-feu ou le système virtuel en tant qu'agent User-ID. Vous devez saisir les mêmes valeurs que lors de la configuration du pare-feu ou du système virtuel pour qu'il serve d'agent User-ID (reportez-vous à la section Redistribution).
Clé prépartagée du collecteur / Confirmer la clé prépartagée du collecteur	
Activé	Sélectionnez pour activer le Collecteur de journaux afin de communiquer avec l'agent User-ID.

Sécurité de la connexion

- Panorama > Collecteurs gérés > Sécurité de la connexion

Pour configurer un profil de certificat utilisé par le Collecteur de journaux pour valider le certificat présenté par les agents User-ID Windows. Le Collecteur de journaux utilise le profil de certificat sélectionné pour vérifier l'identité de l'agent User-ID en validant le certificat de serveur présenté par l'agent.

© 2020 Palo Alto Networks, Inc.

Tâche	Description
Profil de certificat de User-ID	Dans le menu déroulant, sélectionnez le profil de certificat utilisé pour l'authentification avec les agents User-ID Windows ou sélectionnez Nouveau profil de certificat pour en créer un. Sélectionnez Aucun pour supprimer le profil de certificat.

Paramètres de communication

- Panorama > Collecteurs gérés > Communication

Pour configurer l'authentification basée sur certificat personnalisée entre les Collecteurs de journaux et Panorama, les pare-feu et les autres Collecteurs de journaux, configurez les paramètres comme décrit dans le tableau suivant.

Paramètres de communication	Description
Communication sécurisée avec le serveur – Activer **Communication sécurisée avec le serveur** valide l'identité des périphériques clients se connectant au Collecteur de journaux.	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS dans la liste déroulante. Ce profil définit le certificat présenté par le Collecteur de journaux et indique la plage de versions SSL/TLS acceptables pour la communication avec le Collecteur de journaux.
Profil du certificat	Sélectionnez un profil de certificat dans le menu déroulant. Ce profil du certificat définit le comportement de vérification de la révocation du certificat et l'autorité de certification racine utilisée pour authentifier la chaîne de certificats présentée par le client.
Certificat personnalisé uniquement	Lorsqu'il est activé, le Collecteur de journaux n'accepte que les certificats personnalisés pour l'authentification avec des pare-feu gérés et des Collecteurs de journaux.
Autoriser les clients en fonction de leur numéro de série	Le Collecteur de journaux autorise les périphériques clients en fonction de l'utilisation d'un hachage de leur numéro de série.
Vérifier la liste d'autorisation	Les périphériques clients ou les groupes de périphériques se connectant à ce Collecteur de journaux sont vérifiés par rapport à la liste d'autorisations.
Délai d'attente de déconnexion (min)	Le laps de temps pendant lequel le Collecteur de journaux attend avant d'interrompre la connexion actuelle avec ses périphériques gérés. Le Collecteur de journaux rétablit ensuite les connexions avec ses périphériques gérés en utilisant les paramètres de communications sécurisées avec le serveur configurés. Le temps d'attente commence après la validation de la configuration des communications sécurisées avec le serveur.
Liste d'autorisation	**Liste d'autorisations** – Sélectionnez Ajouter et renseignez les champs suivants pour définir les critères. • **Identifier (Identifiant)** – Sélectionnez **Subject (Objet)** ou **Subject Alt. (Autre nom d'objet)** en tant qu'identifiant d'autorisation.

© 2020 Palo Alto Networks, Inc.

Paramètres de communication	Description
	• **Type** – Si Autre nom d'objet est sélectionné en tant qu'Identifiant, sélectionnez **IP**, **nom d'hôte**, ou **e-mail** en tant que type d'identifiant. Si Objet est sélectionné, le nom commun est utilisé en tant que type d'identifiant. • **Value (Valeur)** – Saisissez la valeur d'identifiant.
Communication sécurisée avec le client – Activer **Communication sécurisée avec le client** garantit que le certificat client indiqué est utilisé pour authentifier les connexions Collecteur de journaux sur SSL avec Panorama, les pare-feu ou d'autres Collecteurs de journaux.	
Type de certificat	Sélectionnez le type de certificat de périphérique (Aucun, Local ou SCEP) utilisé pour sécuriser la communication
None	Si **Aucun** est sélectionné, aucun certificat de périphérique n'est configuré et la communication sécurisée avec le client n'est pas utilisée. Il s'agit de la sélection par défaut.
Local	Le Collecteur de journaux utilise un certificat de périphérique local et la clé privée correspondante générée sur le Collecteur de journaux ou importée à partir d'un serveur PKI d'entreprise existant.
	Certificat – Sélectionnez le certificat de périphérique local. Ce certificat peut être unique pour le pare-feu (basé sur un hachage du numéro de série du Collecteur de journaux) ou un certificat de périphérique commun utilisé par tous les Collecteurs de journaux se connectant à Panorama.
	Profil de certificat – Sélectionnez le Profil de certificat dans le menu déroulant. Ce profil du certificat est utilisé pour définir l'authentification du serveur avec le Collecteur de journaux.
SCEP	Le Collecteur de journaux utilise un certificat de périphérique et un serveur de Protocole d'inscription de certificat simple (SCEP) généré par une clé privée.
	Profil SCEP – Sélectionnez le Profil SCEP dans le menu déroulant.
	Profil de certificat – Sélectionnez le Profil de certificat dans le menu déroulant. Ce profil du certificat est utilisé pour définir l'authentification du serveur avec le Collecteur de journaux.
Vérifier l'identité du serveur	Le périphérique client confirme l'identité du serveur en faisant correspondre le nom commun (CN) avec l'adresse IP ou le FQDN du serveur.

Mises à jour logicielles pour les collecteurs de journaux dédiés

- Panorama > Collecteurs gérés

Pour installer une image logicielle sur un Collecteur de journaux dédié, téléchargez ou chargez l'image sur Panorama (voir Panorama > Déploiement du périphérique), cliquez sur **Installer**, puis remplissez les champs suivants.

© 2020 Palo Alto Networks, Inc.

Étant donné que le serveur de gestion Panorama partage son système d'exploitation avec le Collecteur de journaux par défaut local, vous les mettez tous deux à niveau lors de l'installation d'une mise à jour logicielle sur le serveur de gestion Panorama (voir Panorama > Logiciel).

Pour les Collecteurs de journaux dédiés, vous pouvez également sélectionner Panorama > Déploiement de périphériques > Logiciel pour installer des mises à jour (voir Gestion des mises à jour logicielles et de contenu).

Pour réduire le trafic sur l'interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces).

Champs pour l'installation d'une Mise à jour logicielle sur un Collecteur de journaux	Description
Classification	Sélectionnez une image logicielle chargée ou téléchargée.
Périphériques	Sélectionnez les collecteurs de journaux sur lesquels installer le logiciel. Le dialogue affiche les informations suivantes pour chacun des collecteurs de journaux : • **Nom du périphérique** – Le nom du Collecteur de journaux dédié. • **Version actuelle** - La version du logiciel Panorama actuellement installée sur le collecteur de journaux. • **État HA** - Cette colonne ne s'applique pas aux collecteurs de journaux. Les collecteurs de journaux dédiés ne prennent pas en charge la haute disponibilité.
Filtre sélectionné	Pour n'afficher que des collecteurs de journaux spécifiques, sélectionnez les collecteurs de journaux, puis **Filter Selected (Filtre sélectionné)**.
Charger sur le périphérique uniquement (ne pas Installer)	Sélectionnez pour charger le logiciel sur le Collecteur de journaux sans le redémarrer automatiquement. L'image n'est pas installée tant que vous n'avez pas redémarré manuellement en vous connectant à la CLI du Collecteur de journaux et en exécutant la commande opérationnelle **`request restart system`**.
Redémarrer le périphérique après l'Installation	Sélectionnez pour télécharger et installer automatiquement le logiciel. Le processus d'installation redémarre le collecteur de journaux.

© 2020 Palo Alto Networks, Inc.

Panorama > Groupes de collecteurs

Chaque groupe de collecteurs peut être composé d'un maximum de 16 collecteurs de journaux, auxquels vous pouvez assigner des pare-feu pour le transfert des journaux. Vous pouvez ensuite utiliser Panorama pour effectuer une recherche sur les collecteurs de journaux afin d'afficher ou d'interroger les journaux cumulés.



Le groupe de collecteurs prédéfini nommé par défaut contient le collecteur de journaux prédéfini qui est local au serveur de gestion Panorama.

- Configuration du groupe de collecteurs
- Information sur les groupes de collecteurs

Configuration du groupe de collecteurs

Pour configurer un Groupe de collecteurs, cliquez sur **Add (Ajouter)** et renseignez les champs suivants.

Paramètres de groupe de collecteurs	Configuré dans	Description
Name (Nom)	**Panorama** > **Collector Groups (Groupes de collecteurs)** > **General (Général)**	Saisissez un nom pour identifier ce Groupe de collecteurs (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Stockage des journaux		Indique le quota de stockage total des journaux de pare-feu reçus par le Groupe de collecteurs et l'espace disponible. Cliquez sur le lien de quota de stockage pour définir le **Quota (%)** de stockage et la période d'expiration (**Max Days (Jours max)**) pour les types de journaux suivants : • **Detailed Firewall Logs (Journaux détaillés du pare-feu)** – Inclut tous les types de journaux dans **Device (Périphérique)** > **Setup (Configuration)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)**, comme le trafic, la menace, la correspondance HIP, les adresses IP enregistrées de manière dynamique (indicateur d'adresses IP), les PCAP étendus, le GTP et le Tunnel, les Statistiques de l'application, etc. • **Summary Firewall Logs (Journaux récapitulatifs du pare-feu)** – Inclut tous les journaux récapitulatifs inclus dans **Device (Périphérique)** > **Setup (Configuration)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)**, comme le récapitulatif du trafic, le récapitulatif des menaces, le récapitulatif des URL et le récapitulatif GTP et des tunnels.

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
		• **Infrastructure and Audit Logs (Journaux d'infrastructure et d'audit)** – Inclut les journaux de configuration, de système, de User-ID et d'authentification. • **Palo Alto Networks Platform Logs (Journaux de la plate-forme Palo Alto Networks)** – Inclut les journaux de Traps et d'autres produits Palo Alto Networks. • **3rd Party External Logs (Journaux tiers externes)** – Inclut les journaux provenant des intégrations d'un autre fournisseur fournies par Palo Alto Networks. Pour utiliser les paramètres par défaut, cliquez sur **Restore Defaults (Rétablir les valeurs par défaut)**.
Période de conservation minimale (jours)		Saisissez la période de conservation minimale des journaux (de 1 à 2 000 jours) appliquée par Panorama sur tous les collecteurs de journaux du groupe de collecteurs. Si la date actuelle moins la date du plus ancien journal est inférieure à la période de conservation minimale, Panorama génère un journal système à titre d'alerte de violation.
Membres du groupe de collecteurs		Veuillez **Ajouter** les Collecteurs de journaux qui font partie de ce Groupe de collecteurs (jusqu'à 16). Vous pouvez ajouter n'importe quel Collecteur de journaux disponibles dans la page **Panorama** > **Managed Collectors (Collecteurs gérés)**. Tous les Collecteurs de journaux d'un Groupe de collecteurs particulier doivent être du même modèle : par exemple, tous les appareils M-500 ou toutes les applications virtuelles Panorama.  *Une fois des collecteurs de journaux ajoutés à un groupe de collecteurs existant, Panorama redistribue ses journaux existants sur tous les collecteurs de journaux, ce qui peut prendre des heures pour chaque téraoctet de journaux. Pendant le processus de redistribution, le débit de journalisation maximum est réduit. Dans la page Panorama > Collector Groups (Groupes de collecteurs), la colonne État de la redistribution des journaux indique l'état de la progression du processus en tant que pourcentage.*
Activer la redondance		Si vous sélectionnez cette option, chaque journal du groupe de collecteurs aura deux copies et chaque copie

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
des journaux parmi les collecteurs		se trouvera sur un collecteur de journaux distinct. Cette redondance garantit qu'aucun journal n'est perdu en cas d'indisponibilité d'un collecteur de journaux : vous pouvez voir tous les journaux transférés au groupe de collecteurs et générer des rapports sur toutes les données de journal. La redondance des journaux est disponible uniquement si le groupe de collecteurs comprend plusieurs collecteurs de journaux et si chaque collecteur de journaux inclut le même nombre de disques. Une fois la redondance activée, Panorama redistribue les journaux existants sur tous les collecteurs de journaux, ce qui peut prendre des heures pour chaque téraoctet de journaux. Pendant le processus de redistribution, le débit de journalisation maximum est réduit. Dans la page **Panorama** > **Collector Groups (Groupes de collecteurs)**, la colonne État de la redistribution des journaux indique l'état de la progression du processus en tant que pourcentage. Tous les Collecteurs de journaux d'un Groupe de collecteurs particulier doivent être du même modèle : par exemple, tous les appareils M-500 ou toutes les applications virtuelles Panorama. *L'activation de la redondance générant un plus grand nombre de journaux, cette configuration nécessite une capacité de stockage supérieure. L'activation de la redondance multiplie par deux le trafic de traitement des journaux dans un groupe de collecteurs, réduisant ainsi de moitié son débit de journalisation maximum car chaque collecteur de journaux doit distribuer une copie de chaque journal qu'il reçoit. (Lorsque l'espace vient à manquer sur un groupe de collecteurs, il supprime les journaux antérieurs.)*
Transférer à tous les collecteurs de la liste des favoris		(Pare-feu de la série PA-5200 et de la série PA-7000 uniquement) Sélectionnez pour envoyer des journaux à chaque Collecteur de journaux dans la liste des préférences. Panorama utilise l'équilibrage de charge de la permutation circulaire pour sélectionner quel Collecteur de journaux reçoit les journaux à un moment donné. Cette option est désactivée par défaut : les pare-feu n'envoient les journaux qu'au premier Collecteur de journaux de la liste, à moins que ce Collecteur de

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
		journaux ne soit indisponible (voir Périphériques / collecteurs).
Activer la Communication sécurisée entre les collecteurs de journaux		Active l'utilisation de certificats personnalisés pour l'authentification SSL mutuelle entre les Collecteurs de journaux d'un Groupe de collecteurs.
Location (Emplacement)	**Panorama** > **Collector Groups (Groupes de collecteurs)** > **Monitoring (Surveillance)**	Indiquez l'emplacement du Groupe de collecteurs.
Contact		Précisez un contact de messagerie électronique (par exemple, l'e-mail de l'administrateur SNMP qui surveillera les collecteurs de journaux).
Version		Précisez la version SNMP qui doit communiquer avec le serveur de gestion Panorama : **V2c** ou **V3**. SNMP vous permet de recueillir des informations sur les collecteurs de journaux, notamment : l'état de la connexion, les statistiques des lecteurs de disque, la version du logiciel, les performances moyennes du processeur, le nombre moyen de journaux/s et la durée de stockage par type de journal. Les informations SNMP sont disponibles sur la base du groupe de collecteurs.
La chaîne de communauté SNMP (V2c uniquement)		Saisissez la **SNMP Community String (chaîne de communauté SNMP)**, qui identifie une communauté de gestionnaires SNMP et de périphériques surveillés (collecteurs de journaux dans le cas présent), et qui sert de mot de passe pour authentifier les membres de la communauté entre eux. *N'utilisez pas la chaîne de communauté publique définie par défaut ; elle est connue et, par conséquent, n'est pas sécurisée.*
Vues (V3 uniquement)		**Add (Ajoutez)** un groupe de vues SNMP et, dans **Vues**, donnez un nom au groupe. Chaque vue est constituée d'une paire identifiant d'objet (OID)/masque de niveau bit : l'OID définit une base d'information géré (MIB) et le masque (au format hexadécimal) définit les objets SNMP qui sont accessibles à l'intérieur (inclure correspondance) ou à l'extérieur (exclure correspondance) de ce MIB. Pour chaque vue du groupe, **Add (Ajoutez)** les paramètres suivants :

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
		• **View (Vue)** – Saisissez un nom pour une vue. • **OID** - Saisissez l'OID. • **Option** (inclure ou exclure) - Choisissez si la vue doit exclure ou inclure l'OID. • **Mask (Masque)** - Précisez une valeur de masque pour un filtre sur l'OID (par exemple, 0xf0).
Utilisateurs (V3 uniquement)		**Add (Ajoutez)** les paramètres suivants pour chaque utilisateur SNMP : • **Users (Utilisateurs)** - Saisissez le nom d'utilisateur qui permettra de l'authentifier auprès du gestionnaire SNMP. • **View (Vue)** – Sélectionnez un groupe de vues de l'utilisateur. • **Authpwd** – Saisissez un mot de passe pour authentifier l'utilisateur auprès du gestionnaire SNMP (huit caractères minimum). Seul l'algorithme SHA (Secure Hash Algorithm/algorithme de hachage sécurisé) est pris en charge. • **Privpwd** – Saisissez un mot de passe de confidentialité pour crypter les messages SNMP envoyés au gestionnaire SNMP (huit caractères minimum). Seule la norme AES (Advanced Encryption Standard/norme de chiffrement avancé) est prise en charge.
Dispositifs / collecteurs	**Panorama** > **Collector Groups (Groupes de collecteurs)** > **Device Log Forwarding (Transfert des journaux du périphérique)**	La liste des préférences de transfert de journaux contrôle quels pare-feu transmettent les journaux à quels Collecteurs de journaux. Pour chaque saisie que vous allez **Ajouter** à la liste, il faut **Modifier** la liste des Périphériques pour affecter un ou plusieurs pare-feu et **Ajouter** un ou plusieurs Collecteurs de journaux dans la liste des Collecteurs. Par défaut, les pare-feu que vous affectez dans une entrée de liste envoient les journaux uniquement au principal (premier) Collecteur de journaux tant que celui-ci est disponible. En cas d'échec du Collecteur de journaux principal, les pare-feu envoient les journaux au Collecteur de journaux secondaire. En cas d'échec du Collecteur de journaux secondaire, les pare-feu envoient les journaux au Collecteur de journaux tertiaire, et ainsi de suite. Pour changer l'ordre, sélectionnez un collecteur de journaux, puis cliquez sur **Move Up (Déplacer en haut)** ou sur **Move Down (Déplacer en bas)**.  *Vous pouvez remplacer le comportement de transfert des journaux par défaut pour les pare-feu de la*

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
		série PA-5200 et de la série PA-7000 en sélectionnant Transférer à tous les collecteurs dans la liste des préférences *dans l'onglet General (Général).*
system Configuration Correspondance HIP Trafic Prévention WildFire Corrélation GTP Authentification User-id Tunnel Indicateur d'adresse IP	**Panorama** > **Collector Groups (Groupes de collecteurs)** > **Collector Log Forwarding (Transfert des journaux du collecteur)**	Pour chaque type de journaux du pare-feu que vous souhaitez transférer de ce Groupe de collecteurs vers des services externes, il est nécessaire d'**Ajouter** un ou plusieurs profils de liste de correspondance. Les profils indiquent les journaux à transférer et les serveurs de destination. Pour chaque profil, procédez comme suit : • **Name (Nom)** – Saisissez un nom pouvant contenir jusqu'à 31 caractères pour identifier le profil de liste de correspondance. • **Filter (Filtre)** – Par défaut, le pare-feu transfère **All Logs (Tous les journaux)** du type auquel s'applique ce profil de liste de correspondance. Pour transmettre un sous-ensemble de journaux, sélectionnez un filtre existant ou sélectionnez **Filter Builder (Générateur de filtrage)** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez la logique de connecteur (et/ou). Sélectionner **Refuser** si vous souhaitez appliquer un refus. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options varient selon le type de journal. • **Operator (Opérateur)** – Sélectionnez des critères qui déterminent la manière dont un attribut s'applique (comme « **égal** »). Les options varient selon le type de journal. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. Pour afficher ou exporter les journaux auxquels correspond le filtre, sélectionnez **Afficher les journaux filtrés**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
		• **Description** – Saisissez une description pouvant contenir jusqu'à 1 023 caractères pour expliquer l'objectif de ce profil de liste de correspondance. • Serveurs de destination – Pour chaque type de serveur, veuillez **Ajouter** un ou plusieurs profils de serveur. Pour configurer les profils de serveur, voir Périphérique > Profils de serveur > Trap SNMP, Périphérique > Profils de serveur > Syslog, Périphérique > Profils de serveur > E-mail ou Périphérique > Profils de serveur > HTTP. • Actions intégrées – Vous pouvez **Ajouter** des actions pour tous les types de journaux, sauf les journaux système et les journaux de configuration : • Saisissez un nom descriptif pour l'**Action**. • Sélectionnez l'adresse IP que vous souhaitez identifier – **Adresse source** ou **Adresse de destination**. Vous pouvez identifier uniquement l'adresse IP source dans les journaux de Corrélation et les journaux de Correspondance HIP. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Sélectionnez s'il faut enregistrer l'étiquette avec l'agent User-ID local sur ce Panorama ou avec un agent User-ID distant. Pour enregistrer des étiquettes avec un **Remote device User-ID Agent (Agent User-ID du périphérique distant)**, sélectionnez le profil du serveur HTTP qui permet le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de l'indicateur d'adresse IP n'expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l'action Add Tag (Ajouter une étiquette).* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination.
Profil d'ingestion	**Panorama** > **Collector Groups (Groupes de collecteurs)** > **Log**	Veuillez **Ajouter** un ou plusieurs profils d'ingestion de journaux qui permettent à Panorama de recevoir des journaux à partir du serveur Traps ESM. Pour

© 2020 Palo Alto Networks, Inc.

Paramètres de groupe de collecteurs	Configuré dans	Description
	Ingestion (Ingestion des journaux)	configurer un nouveau profil d'ingestion de journaux, voir Panorama > Profil d'ingestion des journaux.

Information sur les groupes de collecteurs

Sélectionnez **Panorama** > **Collector Groups (Groupes de collecteurs)** pour afficher les informations suivantes pour les Groupes de collecteurs. Des champs supplémentaires sont configurables après avoir effectué la Configuration des collecteurs de journaux.

Information sur les groupes de collecteurs	Description
Name (Nom)	Un nom qui identifie le groupe de collecteurs.
Redondance activée	Indique si la redondance des journaux est activée pour le groupe de collecteurs. Vous pouvez activer la redondance de journaux pour un groupe de collecteurs après avoir effectué ou modifié la Configuration des collecteurs de journaux.
Collecteurs	Les collecteurs de journaux affectés au groupe de collecteurs.
État de la redistribution des journaux	Certaines actions (par exemple, activer la redondance des journaux) entraîneront la redistribution, par le collecteur de journaux, des journaux parmi ses collecteurs de journaux. Cette colonne indique l'état d'achèvement du processus de redistribution en pourcentage.

© 2020 Palo Alto Networks, Inc.

Panorama > Plug-ins

- **Panorama** > **Plugins**
- **Device (Périphérique)** > **Plugins**

Sélectionnez **Panorama** > **Plug-ins** pour installer, supprimer et gérer les plug-ins qui prennent en charge les intégrations de tiers sur Panorama.

(Seulement disponible sur les pare-feux VM-Series) Sélectionnez **Device (Périphériques)** > **Plugins (Plug-ins)** pour installer, supprimer et gérer les plug-ins des pare-feu VM-Series.

Plug-ins	Description
Télécharger	Vous permet de télécharger un fichier d'installation de plug-in à partir d'un répertoire local. Cela n'installe pas le plug-in. Après avoir téléchargé le fichier d'installation, le lien d'Installation devient actif.
File Name (Nom du fichier)	Le nom du fichier du plug-in. Lorsque vous installez le plug-in **vm_series** sur Panorama, la page **Device (Périphérique)** > **VM-Series** devient disponible pour la gestion et la validation des configurations du modèle sur les pare-feu VM-Series déployées sur les environnements de cloud public : AWS, Azure et Google.
Version	Le numéro de version du plug-in.
Platform (Plateforme)	Les modèles sur lesquels le plug-in est pris en charge.
Date de publication	La date de sortie de cette version du plug-in.
Taille	La taille du fichier du plug-in.
Installée	Fournit l'état actuel de l'installation de chaque plug-in sur Panorama.
Actions	• **Install (Installer)** : Installe la version spécifiée du plug-in. L'installation d'une nouvelle version du plug-in écrase la version précédemment installée. • **Effacer** – Supprime le fichier de plug-in spécifié. • **Supprimer la configuration** – Supprime toutes les configurations liées au plug-in. • **Uninstall (Désinstaller)** : Supprime l'installation actuelle du plug-in. Cela ne supprime pas le fichier du plug-in de Panorama. Si vous désinstallez le plug-in, vous perdez toute configuration liée à ce plug-in. N'utilisez que lorsque vous supprimez complètement la configuration connexe.

© 2020 Palo Alto Networks, Inc.

Panorama > VMware NSX

Afin d'automatiser la configuration d'un pare-feu VM-Series Édition NSX, vous devez activer la communication entre NSX Manager et Panorama. Lorsque Panorama enregistre le pare-feu VM-Series en tant que service sur NSX Manager, ce dernier dispose des paramètres de configuration nécessaires pour configurer une ou plusieurs instances des pare-feu VM-Series sur chaque hôte ESXi du cluster.

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment puis-je configurer un Groupe de notification ?	Configuration d'un groupe de notification
Comment puis-je définir la configuration du pare-feu VM-Series Édition NSX ?	Création de définitions de services
Comment puis-je configurer Panorama pour communiquer avec NSX Manager ?	Configuration de l'accès à NSX Manager
Comment puis-je définir les règles de redirection du pare-feu VM-série NSX Édition ?	Création de règles de redirection
Comment puis-je configurer le pare-feu afin d'appliquer uniformément la politique dans l'environnement vSphere dynamique ?	Sélectionnez Objets > Groupes d'adresses et Politiques > Sécurité Pour que Panorama et les pare-feu apprennent les changements qui surviennent dans l'environnement virtuel, utilisez les Groupes d'adresses dynamiques en tant qu'objets d'adresses source et destination dans les prérègles de politique de Sécurité.
Vous souhaitez en savoir plus ?	Voir Configuration d'un pare-feu série VM Édition NSX

Configuration d'un groupe de notification

- Panorama > Groupes de notification

Le tableau suivant décrit les paramètres du groupe de notification Panorama.

Paramètres du groupe de notification	Description
Name (Nom)	Saisissez un nom descriptif pour votre groupe de notification.
Informer le périphérique	Cochez les cases des groupes de périphériques qui doivent être informés des modifications ou des ajouts aux machines virtuelles déployées sur le réseau. Lorsque de nouvelles machines virtuelles sont configurées et les machines existantes sont modifiées, les modifications effectuées sur le réseau virtuel sont fournies comme mises à jour de Panorama. Lorsqu'il est configuré pour le faire, Panorama préremplit et met à jour les objets d'adresses dynamiques auxquels font référence les règles de politique afin que les pare-feu des

© 2020 Palo Alto Networks, Inc.

Paramètres du groupe de notification	Description
	groupes de périphériques précisés reçoivent les modifications apportées aux adresses IP enregistrées dans les groupes d'adresses dynamiques. pour activer les notifications, assurez-vous de sélectionner chacun des groupes de périphériques pour lesquels vous voulez activer les notifications. Si vous n'êtes pas en mesure de sélectionner un groupe de périphériques (aucune case à cocher disponible), le groupe de périphériques est automatiquement inclut parce qu'il fait partie d'une hiérarchie de groupe de périphériques. Ce processus de notification crée une sensibilité au contexte et garantit la sécurité des applications sur le réseau. Si, par exemple, vous disposez d'un groupe de pare-feu de périmètre matériels qui doit être averti lorsqu'une nouvelle application ou un nouveau serveur Web est déployé, ce processus actualise automatiquement les groupes d'adresses dynamiques du groupe de périphériques donné. De plus, toutes les règles de politique qui font référence à l'objet adresse dynamique incluent alors automatiquement toute nouvelle application ou tout nouveau serveur Web et peuvent être activées en toute sécurité en fonction de vos critères.

Création de définitions de services

- Panorama > VMware NSX > Définitions du service

Une définition de service vous permet d'enregistrer le pare-feu VM-Series en tant que service de sécurité partenaire sur NSX Manager. Vous pouvez définir un maximum de 32 définitions de service sur Panorama et les synchroniser sur NSX Manager.

Généralement, vous créerez une définition de service pour chaque client d'un cluster ESXi. Chaque définition de service précise l'OVF (version de PAN-OS) utilisé pour déployer le pare-feu et comprend la configuration des pare-feu VM-Series installés sur le cluster ESXi. Pour préciser la configuration, une définition de service doit avoir un modèle unique, un groupe de périphériques unique et les codes d'autorisation des licences pour les pare-feu qui seront déployés au moyen de la définition de service. Une fois le pare-feu déployé, ce dernier se connecte à Panorama et reçoit les deux paramètres de configuration (notamment la ou les zones pour chacun des clients ou des départements que le pare-feu sécurisera) et les paramètres de politique du groupe de périphériques indiqué dans la définition de service.

Pour ajouter une nouvelle définition de service, configurez les paramètres comme décrit dans le tableau suivant.

Champ	Description
Name (Nom)	Saisissez le nom du service que vous voulez afficher sur NSX Manager.
Description	(Facultatif) Saisissez une étiquette pour décrire l'objet ou la fonction de cette définition de service.
Groupe de périphériques	Sélectionnez le groupe de périphériques ou la hiérarchie de groupe de périphériques auquel ces pare-feu VM-Series seront affectés. Pour plus d'informations, voir Panorama > VMware NSX.

© 2020 Palo Alto Networks, Inc.

Champ	Description
Modèle	Sélectionnez le modèle auquel les pare-feu VM-Series seront affectés. Pour plus d'informations, voir Panorama > Modèles. Chaque définition de service doit être assignée à un modèle unique ou à une pile de modèles unique. Des zones multiples (Zones de profil du service NSX pour NSX) peuvent être associées à un modèle. Pour un déploiement d'un client unique, créez une zone (Zone de profil du service du pare-feu NSX) dans le modèle. Si vous disposez d'un déploiement de locataires multiples, créez une zone par sous-client. Lorsque vous créez une nouvelle zone de profil du service du pare-feu NSX, celle-ci est automatiquement liée à une paire de sous-interfaces de câble virtuel. Pour plus d'informations, voir Réseau > Zones.
URL OVF VM-Series	Saisissez l'URL (adresse IP ou nom d'hôte et chemin d'accès) via laquelle NSX Manager peut accéder au fichier OVF pour configurer de nouveaux pare-feu VM-Series.
Groupes de notification	Sélectionnez un groupe de notification dans le menu déroulant.

Configuration de l'accès à NSX Manager

- Panorama > VMware NSX > Gestionnaires de service

Pour permettre à Panorama de communiquer avec le NSX Manager, vous devez **Ajouter** et configurer les paramètres comme décrit dans le tableau suivant.

Gestionnaires de service	Description
Nom du gestionnaire de services	Saisissez un nom permettant d'identifier le pare-feu VM-Series en tant que service. Ce nom s'affiche sur NSX Manager et est utilisé pour déployer le pare-feu VM-Series sur demande. Entrez 63 caractères maximum, n'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Description	(Facultatif) Saisissez une étiquette pour décrire l'objet ou la fonction de ce service.
URL de NSX Manager	Définissez l'URL que Panorama peut utiliser pour établir la connexion à NSX Manager.
Connexion au NSX Manager	Saisissez les informations d'identification d'authentification (nom d'utilisateur et mot de passe) configurées sur NSX Manager. Panorama utilise ces informations d'identification pour s'authentifier auprès de NSX Manager.
Mot de passe NSX Manager	

© 2020 Palo Alto Networks, Inc.

Gestionnaires de service	Description
Confirmer le mot de passe NSX Manager	
Définitions du service	Spécifiez les définitions de service associées à ce gestionnaire de service. Chaque gestionnaire de service prend en charge jusqu'à 32 définitions de service.

Après avoir validé les modifications apportées à Panorama, la page VMware Service Manager affiche l'état de la connexion entre Panorama et NSX Manager.

Statut de synchronisation	Description
Status (État)	Affiche le statut de la connexion entre Panorama et NSX'A0;Manager. Lorsque la connexion a réussi, l'état affiché est Enregistré - Panorama et NSX Manager sont synchronisés et le pare-feu VM-Series est enregistré en tant qu'un service sur NSX Manager. Pour une connexion non réussie, l'état peut être : • **Erreur de connexion** - impossible d'atteindre/établir une connexion réseau avec NS Manager. • **Non autorisé** - Les informations d'identification d'accès (nom d'utilisateur et/ou mot de passe) ne sont pas correctes. • **Non enregistré** - Le gestionnaire de service, la définition de service ou le profil de service n'est pas disponible ou a été supprimé sur NSX Manager. • **Non synchronisé** - Les paramètres de configuration définis sur Panorama sont différents de ceux définis sur NSX Manager. Cliquez sur **Out of sync (Non synchronisé)** pour connaître les détails de la raison de l'échec. Par exemple, NSX Manager peut disposer d'une définition de service ayant le même nom que celui qui est défini sur Panorama. Pour corriger l'erreur, utilisez le nom de la définition de service qui est indiqué dans le message d'erreur afin de valider la définition de service sur NSX Manager. Jusqu'à ce que la configuration sur Panorama et celle sur NSX Manager soient synchronisées, vous ne pouvez pas ajouter de nouvelle définition de service sur Panorama.
Synchroniser les objets dynamiques	Cliquez sur **Synchronize Dynamic Objects (Synchroniser les objets dynamiques)** pour actualiser les informations relatives à l'objet dynamique sur NSX Manager. La synchronisation des objets dynamiques vous permet de conserver le contexte des modifications dans l'environnement virtuel et vous permet d'activer des applications en toute sécurité grâce à la mise à jour automatique Groupes d'adresses dynamiques utilisés dans les règles de politique.  *Sur Panorama, vous pouvez afficher uniquement les adresses IP enregistrées de manière dynamique à partir de NSX Manager. Panorama n'affiche pas les adresses IP enregistrées directement sur les pare-feu. Si vous utilisez des sources d'information de machine virtuelle (non prises en charge sur les pare-feu VM-Series Édition NSX) ou l'API XML pour enregistrer les adresses IP dynamiquement sur les pare-feu, vous devez vous connecter*

© 2020 Palo Alto Networks, Inc.

Statut de synchronisation	Description
	à chacun des pare-feu pour voir la liste complète des adresses IP dynamiques (celles que Panorama applique et celles qui sont enregistrées localement) sur le pare-feu.
Synchronisation de la configuration NSX	Sélectionnez **Synchronisation de la configuration NSX** pour synchroniser les définitions de service configurées sur Panorama avec NSX Manager. Cette option n'est pas disponible si des validations sont en attente sur Panorama. Si la synchronisation échoue, affichez les détails du message d'erreur pour savoir si l'erreur s'est produite sur Panorama ou sur NSX Manager. Par exemple, si vous supprimez une définition de service sur Panorama, la synchronisation avec le NSX Manager échoue si une règle de NSX Manager y fait référence. Utilisez l'information présentée dans le message d'erreur pour déterminer la raison de l'échec ainsi que l'emplacement où les mesures correctives doivent être prises (sur Panorama ou sur NSX Manager).

Création de règles de redirection

- Panorama > VMware NSX > Règles de redirection

Les règles de redirection déterminent le trafic de quels invités du cluster est redirigé vers le pare-feu VM-Series.

Champ	Description
Générer automatiquement les règles de redirection	Génère les règles de redirection en fonction d'une règle de sécurité configurée comme suit : • appartient à un groupe de périphériques parent ou enfant enregistré auprès d'un gestionnaire de services NSX ; • présente la même zone que la source et la destination (pas indifférent pour indifférent) ; • n'a qu'une seule zone ; • n'a aucun groupe d'adresses statiques, plage d'adresses IP ou masque de réseau configuré pour la politique. Par défaut, les règles de redirection générées au moyen de Panorama n'ont pas de services NSX configurés et la Direction du trafic NSX est définie sur entrée-sortie. Après avoir généré des règles de redirection, vous pouvez mettre à jour les règles de redirection individuelles pour modifier la Direction du trafic NSX ou ajouter des services NSX. Panorama renseigne automatiquement les champs suivants (sauf Description et services NSX) lorsque vous générez automatiquement les règles de redirection.
Name (Nom)	Saisissez le nom de la règle de direction que vous voulez afficher sur NSX Manager. Lorsqu'il est généré automatiquement, Panorama ajoute le préfixe « auto_ » à chaque règle de redirection et remplace tout espace dans le nom de la règle de politique de sécurité par un trait de soulignement (_).

© 2020 Palo Alto Networks, Inc.

Champ	Description
Description	(Facultatif) Saisissez une étiquette pour décrire l'objet ou la fonction de cette définition de service.
Direction du trafic NSX	Indiquez la direction du trafic qui est redirigé vers le pare-feu VM-Series. • **Entrée-sortie** – Crée une règle ENTRÉE-SORTIE sur NSX. Le trafic du type spécifié se trouvant entre la source et la destination est redirigé vers le pare-feu VM-Series. Panorama utilise cette direction de trafic pour les règles de redirection générées automatiquement. • **Entrée** – Crée une règle ENTRÉE sur NSX. Le trafic du type spécifié se dirigeant vers la source depuis la destination est redirigé vers le pare-feu VM-Series. • **Sortie** – Crée une règle SORTIE sur NSX. Le trafic du type spécifié se dirigeant vers la destination depuis la source est redirigé vers le pare-feu VM-Series.
Services NSX	Sélectionnez le trafic de l'application (serveur Active Directory, HTTP, DNS, etc.) à rediriger vers le pare-feu VM-Series.
Groupe de périphériques	Sélectionnez un groupe de périphériques dans le menu déroulant. Le groupe de périphériques choisi détermine les politiques de sécurité qui sont appliquées à la règle de redirection. Les groupes de périphériques doivent être associés à une définition du service NSX.
Politique de Sécurité	La règle de politique de sécurité sur laquelle se base la règle de redirection générée automatiquement.

© 2020 Palo Alto Networks, Inc.

Panorama > Profil d'ingestion des journaux

Utilisez le profil d'ingestion de journaux pour permettre à Panorama de recevoir des journaux à partir de sources externes. Dans PAN-OS 8.0.0, Panorama (en mode Panorama) peut servir de récepteur Syslog qui peut ingérer des journaux du serveur Traps ESM à l'aide de Syslog. La prise en charge de nouvelles sources de journaux externes et les mises à jour pour les nouvelles versions de Traps ESM seront appliquées par des mises à jour de contenu.

Pour activer l'ingestion du journal, vous devez configurer Panorama comme un récepteur Syslog sur le serveur Traps ESM, définir un profil d'ingestion de journal sur Panorama et joindre le profil d'ingestion de journal à un groupe de collecteur de journaux.

Pour ajouter un nouveau profil d'ingestion Syslog externe, cliquez sur **Ajouter** un profil et configurez les paramètres comme décrits dans le tableau suivant.

Champ	Description
Name (Nom)	Saisissez le nom du profil d'ingestion Syslog externe. Vous pouvez ajouter jusqu'à 255 profils.
Nom de la source	Saisissez le nom ou l'adresse IP des sources externes qui enverront des journaux. Vous pouvez ajouter jusqu'à 4 sources dans un profil.
Port	Saisissez le port sur lequel Panorama sera accessible sur le réseau et celui qu'il utilisera pour communiquer et écouter. Pour Traps ESM, sélectionnez une valeur comprise entre 23 000 et 23 999. Vous devez configurer le même numéro de port sur le Traps ESM pour permettre la communication entre Panorama et l'ESM.
Transport	Sélectionnez TCP, UDP ou SSL. Si vous sélectionnez SSL, vous devez configurer un certificat entrant pour une communication Syslog sécurisée dans Panorama > Collecteurs gérés > Généralités.
Type de journal externe	Sélectionnez le type de journal dans le menu déroulant.
Version	Sélectionnez la version dans le menu déroulant.

Utilisez Surveillance > Journaux externes pour afficher les informations sur les journaux ingérés dans le serveur Traps ESM vers Panorama.

© 2020 Palo Alto Networks, Inc.

Panorama > Paramètres des journaux

Utilisez la page des **Paramètres du journal** pour transmettre les types de journaux suivants aux services externes :

- les journaux système, de configuration, d'User-ID et de corrélation que le serveur de gestion Panorama (appareil de la série M ou appareil virtuel panoramique en mode panoramique) génère localement ;
- les journaux de tous types qui sont générés localement par l'appareil virtuel Panorama en Mode hérité ou qui sont rassemblés à partir des pare-feu.



Pour les journaux que les pare-feu envoient aux collecteurs de journaux, terminez la Configuration du collecteur de journaux *pour permettre le transfert vers des services externes.*

Avant de commencer, vous devez définir des profils de serveur pour les services externes (voir Périphérique > Profils de serveur > Traps SNMP, Périphérique > Profils de serveur > Syslog, Périphérique > Profils de serveur > E-mail, et Périphérique > Profils de serveur > HTTP). Vous pouvez ensuite **Ajouter** un ou plusieurs profils de liste de correspondance et configurer les paramètres comme décrits dans le tableau suivant.

Paramètres du profil de la liste de correspondance	Description
Name (Nom)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance.
Filtre	Par défaut, Panorama transfère **Tous les journaux** au type pour lequel vous ajoutez le profil de liste de correspondance. Pour transférer un sous-ensemble de journaux, ouvrez le menu déroulant et sélectionnez un filtre existant ou sélectionnez **Filter Builder (Générateur de filtre)** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez le connecteur logique (et/ou) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options dépendent du type de journal. • **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du type de journal. • **Valeur** - Indiquez la valeur de l'attribut à faire correspondre avec la requête. Pour afficher ou exporter les journaux auxquels correspond le filtre, sélectionnez **Afficher les journaux filtrés**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).

© 2020 Palo Alto Networks, Inc.

Paramètres du profil de la liste de correspondance	Description
Description	Saisissez une description contenant jusqu'à 1 024 caractères afin d'expliquer le but de ce profil de liste de correspondance.
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).
Actions intégrées	Tous les types de journaux, à l'exception des Journaux système et des Journaux de configuration, vous permettent de configurer des actions. • Cliquez pour **Ajouter** une action et saisissez un nom pour la décrire. • Sélectionnez l'adresse IP que vous souhaitez identifier – **Adresse source** ou **Adresse de destination**. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez distribuer l'étiquette à l'agent User-ID local de ce périphérique ou à un agent User-ID distant. • Pour distribuer des étiquettes à un **Agent User-ID de périphérique distant**, sélectionnez le profil du serveur HTTP qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/ étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de l'indicateur d'adresse IP n'expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l'action Add Tag (Ajouter une étiquette).* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination. Vous pouvez étiqueter l'adresse IP source uniquement dans les Journaux de corrélation et les Journaux de correspondance HIP.

© 2020 Palo Alto Networks, Inc.

Panorama > Exportation programmée des configurations

Pour planifier une exportation de toutes les configurations en cours d'exécution sur Panorama et les pare-feu, il vous faut **Ajouter** une tâche d'exportation et configurer les paramètres, comme décrit dans le tableau suivant.

Si Panorama est dans une configuration haute disponibilité (HD), vous devez suivre ces instructions sur chaque homologue pour vous assurer que les exportations planifiées continuent après un basculement. Panorama ne synchronise pas les exportations de configuration planifiées entre les homologues HD.

Paramètres d'exportation de configuration programmée	Description
Name (Nom)	Donnez un nom pour identifier la tâche d'exportation de configuration (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Description	Saisissez une description (facultatif).
Activer	Sélectionnez cette option pour activer la tâche d'exportation.
Heure (quotidienne) de début de l'exportation programmée	Indiquez l'heure du jour de démarrage de l'exportation (horloge 24 heures, format HH:MM).
Protocole	Sélectionnez le protocole à utiliser pour l'exportation des journaux entre Panorama et un hôte distant. Secure Copy (**SCP**) est un protocole sécurisé ; **FTP** ne l'est pas.
Nom d'hôte	Saisissiez l'adresse IP ou le nom d'hôte du serveur SCP ou FTP cible.
Port	Saisissez le numéro de port du serveur cible.
Chemin d'accès	Indiquez le chemin d'accès au dossier ou au répertoire sur le serveur cible où les informations exportées seront enregistrées. Par exemple, si l'ensemble de configuration est conservé dans un dossier nommé exported_config dans un dossier racine nommé Panorama, la syntaxe de chacun des types de serveur est : • Serveur SCP : /Panorama/exported_config • Serveur FTP : //Panorama/exported_config Les caractères suivants : **.** (point), **+**, **{** et **}**, **/**, **-**, **_**, **0-9**, **a-z**, et **A-Z**. Les espaces ne sont pas pris en charge dans le fichier **Chemin d'accès**.
Activer le mode passif FTP	Sélectionnez cette option pour utiliser le mode passif FTP.
Username (Nom d'utilisateur)	Indiquez le nom d'utilisateur requis pour l'accès au système cible.

© 2020 Palo Alto Networks, Inc.

Paramètres d'exportation de configuration programmée	Description
Mot de passe/Confirmer le mot de passe	Indiquez le mot de passe requis pour l'accès au système cible. Utilisez un mot de passe d'une longueur maximale de 15 caractères. Si le mot de passe dépasse 15 caractères, la connexion SCP d'essai affichera une erreur, car le pare-feu chiffre le mot de passe lorsqu'il tente de se connecter au serveur SCP et la longueur du mot de passe chiffré peut comporter un maximum de 63 caractères.
Tester la connexion au serveur SCP	Sélectionnez cette option pour vérifier la communication entre Panorama et l'hôte / le serveur SCP. Pour permettre le transfert sécurisé des données, vous devez vérifier et accepter la clé d'hôte du serveur SCP. La connexion n'est pas établie tant que la clé d'hôte n'est pas acceptée. Si Panorama est dans une configuration haute disponibilité (HA), vous devez effectuer cette vérification sur chaque homologue HA afin que chacun accepte la clé d'hôte du serveur SCP.

© 2020 Palo Alto Networks, Inc.

Panorama > Logiciel

Utilisez cette page pour gérer les mises à jour logicielles de Panorama sur le serveur de gestion Panorama.

- Gestion des mises à jour logicielles Panorama
- Affichage des informations sur les mises à jour logicielles Panorama

Gestion des mises à jour logicielles Panorama

Sélectionnez **Panorama** > **Software (Logiciel)** pour effectuer les tâches décrites dans le tableau suivant.

Par défaut, le serveur de gestion Panorama enregistre jusqu'à deux mises à jour logicielles. Pour libérer de l'espace pour les plus récentes mises à jour, le serveur supprime automatiquement la mise à jour la plus ancienne. Vous pouvez modifier le nombre d'images logicielles enregistrées par Panorama *et supprimer manuellement des images afin de libérer de l'espace.*

Pour obtenir plus d'informations sur la compatibilité des versions, reportez-vous à Installer les mises à jour de contenu et logicielles pour Panorama*.*

Tâche	Description
Vérifier maintenant	Si Panorama dispose d'un accès à Internet, cliquez sur **Vérifier maintenant** pour afficher les plus récentes informations sur les mises à jour (voir Affichage des informations sur les mises à jour logicielles Panorama). Si Panorama n'a pas accès au réseau externe, utilisez un navigateur pour vous rendre sur le site de Mise à jour logicielle pour des informations sur la mise à jour.
Télécharger	Pour télécharger une image logicielle lorsque Panorama ne dispose pas d'un accès à Internet, utilisez un navigateur pour vous rendre sur le site de Mise à jour logicielle, trouvez la version désirée et téléchargez l'image logicielle vers un ordinateur auquel Panorama peut accéder. Sélectionnez **Panorama** > **Software (Logiciel)**, cliquez sur **Upload (Télécharger)**, **Browse (Rechercher)** et sélectionnez l'image logicielle, puis cliquez sur **OK**. Une fois le chargement terminé, la colonne Disponible affiche `Chargé`.
Téléchargement	Si Panorama dispose d'un accès à Internet : cliquez sur **Télécharger** (colonne Action) pour obtenir la version souhaitée. Une fois le téléchargement terminé, la colonne Disponible affiche Téléchargé.
Installer	**Installez** (colonne Action) l'image logicielle. À l'issue de l'installation, Panorama vous déconnecte lorsqu'il redémarre. *Panorama contrôle régulièrement l'intégrité du système de fichiers (FSCK) afin d'éviter une corruption des fichiers système de Panorama. Ce contrôle se produit après huit redémarrages ou lors d'un démarrage survenant 90 jours après le dernier FSCK. Un avertissement s'affiche sur l'interface Web et sur les écrans de connexion SSH si un contrôle FSCK est en cours et que vous ne pouvez pas vous connecter tant que celui-ci n'est pas terminé. La durée d'exécution de ce processus varie en fonction de la taille du système de stockage; si système est important, vous devrez*

© 2020 Palo Alto Networks, Inc.

Tâche	Description
	probablement compter plusieurs heures avant de pouvoir vous reconnecter à Panorama. Pour consulter la progression, configurez l'accès de la console à Panorama.
Notes de version	Si Panorama dispose d'un accès à Internet, vous pouvez accéder aux **Notes de version** de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut. Si Panorama n'a pas accès à Internet, utilisez un navigateur pour vous rendre sur le site de Mise à jour logicielle et téléchargez la version appropriée.
	Supprime une image logicielle qui n'est plus nécessaire ou si vous souhaiter libérer de l'espace pour stocker d'autres images logicielles.

Affichage des informations sur les mises à jour logicielles Panorama

Sélectionnez **Panorama** > **Software (Logiciel)** pour afficher les informations suivantes. Pour afficher les dernières informations de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**.

Informations sur les mises à jour logicielles et de contenu	Description
Version	La version de logiciel Panorama
Taille	La taille en mégaoctets de l'image logicielle.
Date de version	Date et heure de disponibilité de la mise à jour auprès de Palo Alto Networks.
Disponible	Indique si l'image est disponible pour son installation.
Actuellement installé	Un crochet indique que la mise à jour est déjà installée.
Action (Action)	Indique les actions (**Download (Télécharger)**, **Install (Installer)**, ou **Reinstall (Réinstaller)**) qui sont disponible pour une image.
Notes de version	Cliquez sur **Release Notes (Notes de version)** pour accéder aux notes de version de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut.
	Supprime une mise à jour qui n'est plus nécessaire ou pour libérer de l'espace pour procéder à d'autres chargements ou téléchargements.

© 2020 Palo Alto Networks, Inc.

Panorama > Déploiement du périphérique

Vous pouvez utiliser Panorama pour déployer des mises à jour de logiciels et de contenu sur plusieurs pare-feu et collecteurs de journaux et pour gérer des licences de pare-feu.

Que voulez-vous faire ?	Reportez-vous à la section :
Déployer les mises à jour de logiciel et de contenu sur les pare-feu et les collecteurs de journaux.	Gestion des mises à jour logicielles et de contenu
Savoir quelles sont les mises à jour de logiciel et de contenu qui ont été installées ou qui sont disponibles pour le téléchargement et l'installation.	Affichage des informations sur les mises à jour logicielles et de contenu
Programmer des mises à jour de contenu automatiques pour les pare-feu et les collecteurs de journaux.	Planification des mises à jour de contenu dynamiques
Rétablir les version de contenu précédentes de un ou plusieurs pare-feu de Panorama.	Rétablissement des versions de contenu précédentes de Panorama
Afficher, activer, désactiver et actualiser les licences. Afficher l'état des licences du pare-feu.	Gestion des licences du pare-feu
Vous souhaitez en savoir plus ?	Gestion des licences et des mises à jour.

Gestion des mises à jour logicielles et de contenu

- Panorama > Déploiement du périphérique > Logiciel

Panorama propose les options suivantes pour déployer des mises à jour logicielles et de contenu sur les pare-feu et les Collecteurs de journaux.

Pour réduire le trafic sur l'interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces).

© 2020 Palo Alto Networks, Inc.

Options de Déploiement du périphérique Panorama	Description
Téléchargement	Pour déployer une mise à jour logicielle ou de contenu lorsque Panorama est connecté à l'Internet, cliquez sur **Download (Télécharger)** la mise à jour. Une fois le téléchargement terminé, la colonne Disponible affiche Téléchargé. Vous pouvez ensuite : • Installer la mise à jour logicielle ou de contenu PAN-OS / Panorama. • Activer la mise à jour logicielle de l'application GlobalProtect™ ou du client VPN SSL.
upgrade	Si une mise à jour de contenu pour le Filtrage des URL BrightCloud est disponible, cliquez sur **Upgrade (Mettre à niveau)**. Après avoir effectué la mise à niveau, vous pouvez procéder à l'Installation de la mise à jour sur les pare-feu.
Installer	Après avoir effectué le Téléchargement ou le Chargement d'un logiciel PAN-OS, d'un logiciel Panorama ou de contenu, cliquez sur **Install (Installer)** dans la colonne Action et sélectionnez : • **Devices (Périphériques)** - Sélectionnez les pare-feu ou les collecteurs de journaux sur lesquels installer la mise à jour. Si la liste est longue, utilisez les filtres. Sélectionnez **Regrouper les homologues HA** pour regrouper des pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Pour n'afficher que des pare-feu spécifiques ou des collecteurs de journaux spécifiques, sélectionnez-les, puis sélectionnez l'option **Filter Selected (Filtre sélectionné)**. • **Upload only to device (Charger uniquement sur le périphérique)** (logiciel uniquement) – Sélectionnez pour charger le logiciel sans l'installer automatiquement. Vous devez installer le logiciel manuellement. • **Reboot device after install (Redémarrer le périphérique après installation)** (logiciel uniquement) – Sélectionnez si vous voulez que le processus d'installation redémarre automatiquement les pare-feu ou les Collecteurs de journaux. L'installation n'est terminée qu'après un redémarrage du pare-feu. • **Disable new apps in content update (Désactiver les nouvelles applis dans la mise à jour de contenu)** (Applications et Menaces uniquement) – Sélectionnez pour désactiver les applications dans la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d'activer les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.  *Vous pouvez également sélectionner Panorama > Managed Devices (Périphériques gérés) pour installer* les mises à jour logicielles et de contenu du pare-feu *ou Panorama > Managed Collectors (Collecteurs gérés) pour installer* les mises à jour logicielles pour les Collecteurs de journaux dédiés.

© 2020 Palo Alto Networks, Inc.

Options de Déploiement du périphérique Panorama	Description
Activate (Activer)	Après avoir effectué le Téléchargement ou le Chargement d'une mise à jour logicielle de l'application GlobalProtect, cliquez sur **Activate (Activer)** dans la colonne Action et sélectionnez les options comme suit : • **Devices (Périphériques)** - Sélectionnez les pare-feu sur lesquels activer la mise à jour. Si la liste est longue, utilisez les filtres. Sélectionnez **Regrouper les homologues HA** pour regrouper des pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Pour n'afficher que des pare-feu spécifiques, sélectionnez-les, puis l'option **Filter Selected (Filtre sélectionné)**. • **Upload only to device (Charger uniquement sur le périphérique)** – Sélectionnez si vous ne voulez pas que PAN-OS active automatiquement l'image chargée. Vous devez vous connecter au pare-feu et l'activer.
Notes de version	Cliquez sur **Release Notes (Notes de version)** pour accéder aux notes de version de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut.
Documentation	Cliquez sur **Documentation** pour accéder aux notes de versions de la version de contenu souhaitée.
	Supprime les mises à jour logicielles ou de contenu qui ne sont plus nécessaires ou si vous souhaitez libérer de l'espace pour procéder à d'autres chargements ou téléchargements.
Vérifier maintenant	**Check Now (Vérifier maintenant)** pour Afficher les informations sur les mises à jour logicielles et de contenu.
Télécharger	Pour déployer une mise à jour logicielle ou de contenu lorsque Panorama n'est pas connecté à Internet, téléchargez la mise à jour vers votre ordinateur à partir du site Mises à jour logicielles ou Mises à jour dynamiques, sélectionnez la page **Panorama** > **Device Deployment (Déploiement du périphérique)** qui correspond au type de mise à jour, cliquez sur **Upload (Télécharger)**, sélectionnez le **Type** de mise à jour (mises à jour de contenu uniquement), sélectionnez le fichier chargé et cliquez sur **OK**. Les étapes suivantes d'installation ou d'activation de la mise à jour dépendent du type : • **Le logiciel PAN-OS ou Panorama** - Une fois le chargement terminé, la colonne Disponible affiche Chargé. Vous pouvez ensuite procéder à l'installation de la mise à jour logicielle. • **Client GlobalProtect ou Logiciel du client VPN SSL** – Activez depuis le fichier. • **Mises à jour dynamiques** – Installation à partir du fichier.
Installer depuis le fichier	Après avoir effectué le téléchargement d'une mise à jour de contenu, cliquez sur **Install from File (Installer depuis le fichier)**, sélectionnez le **Type** de contenu, sélectionnez le nom de fichier de la mise à jour et sélectionnez les pare-feu ou les Collecteurs de journaux.

© 2020 Palo Alto Networks, Inc.

Options de Déploiement du périphérique Panorama	Description
Activer depuis le fichier	Après avoir effectué le téléchargement de la mise à jour logicielle de l'application GlobalProtect, cliquez sur **Activate from File (Activer depuis le fichier)**, sélectionnez le nom de fichier de la mise à jour et sélectionnez les pare-feu.
Calendriers	Sélectionnez pour Planifier des mises à jour de contenu dynamiques.

Affichage des informations sur les mises à jour logicielles et de contenu

- Panorama > Déploiement du périphérique > Logiciel

Sélectionnez **Panorama** > **Device Deployment (Déploiement du périphérique)** > **Software (Logiciel)** pour afficher le **Software (Logiciel)** PAN-OS, le logiciel **GlobalProtect Client (Client GlobalProtect)** et les **Dynamic Updates (Mises à jour dynamiques)** (contenu) actuellement installés ou disponibles pour le téléchargement et l'installation. La page **Dynamic Updates (Mises à jour dynamiques)** regroupe l'information par type de contenu (Antivirus, Applications et menaces, Filtrage des URL et WildFire) et indique la date et l'heure de la dernière vérification des informations mises à jour. Pour afficher les dernières informations relatives aux mises à jour logicielles et de contenu de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**.

Informations sur les mises à jour logicielles et de contenu	
Version	La version de la mise à jour logicielle ou de contenu.
File Name (Nom du fichier)	Le nom du fichier de mise à jour.
Platform (Plateforme)	Le pare-feu ou le modèle de Collecteur de journaux désigné pour la mise à jour. Un nombre indique un modèle de pare-feu matériel (par exemple, `7 000` indique le pare-feu de la série PA-7000), `vm` indique le pare-feu VM-Series et `m` indique l'équipement M-Series.
Caractéristiques	(Contenu seulement) Répertorie le type de signatures que la version du contenu peut contenir.
Type	(Contenu seulement) Indique si le téléchargement inclut une mise à jour complète ou incrémentielle de la base de données.
Taille	La taille du fichier de mise à jour.
Date de version	Date et heure de disponibilité de la mise à jour auprès de Palo Alto Networks.
Disponible	(logiciel PAN-OS ou Panorama seulement) Indique que la mise à jour a été chargée ou téléchargée.

© 2020 Palo Alto Networks, Inc.

Informations sur les mises à jour logicielles et de contenu	
Téléchargé	(logiciel client VPN SSL, logiciel client GlobalProtect ou de contenu seulement) Une coche indique que la mise à jour a été téléchargée.
Action (Action)	Indique l'action que vous pouvez effectuer sur la mise à jour : Télécharger, Mettre à niveau, Installer ou Activer.
Documentation	(Contenu seulement) Fournit un lien vers les notes de version relatives à la version de contenu souhaitée.
Notes de version	(Logiciel seulement) Fournit un lien vers les notes de version relatives à la version logicielle souhaitée.
	Supprime une mise à jour qui n'est plus nécessaire ou si vous souhaitez libérer de l'espace pour procéder à d'autres chargements ou téléchargements.

Planification des mises à jour de contenu dynamiques

- Panorama > Déploiement de périphérique > Mises à jour dynamiques

Pour programmer un téléchargement et une installation automatiques d'une mise à jour, cliquez sur **Schedules (Calendriers)**, cliquez sur **Add (Ajouter)**, puis configurez les paramètres comme décrits dans le tableau suivant.

Paramètres de planification des mises à jour dynamiques	
Name (Nom)	Saisissez un nom pour identifier la tâche planifiée (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d'union et des caractères de soulignement.
Désactivé	Sélectionnez pour désactiver la tâche planifiée.
Type	Sélectionnez le type de la mise à jour de contenu à planifier : **App (Applications)**, **App and Threat (Applications et menaces)**, **Antivirus**, **WildFire** ou **URL Database (Base de données des URL)**.
Récurrence	Sélectionnez l'intervalle auquel Panorama se connecte au serveur de mises à jour. Les options de récurrence varient selon le type de mise à jour.
Période	Pour une mise à jour **Daily (Quotidienne)**, sélectionnez **Time (Heure)** au format d'horloge 24 heures. Pour une mise à jour **Weekly (Hebdomadaire)**, sélectionnez le **Day (Jour)** de la semaine et **Time (Heure)** au format d'horloge 24 heures.
Désactiver les nouvelles applis dans la mise à jour de contenu	Vous pouvez désactiver les nouvelles applications des mises à jour de contenu uniquement si vous définissez le **Type** sur **App (Applications)** ou sur **App and Threat (Applications et menaces)** et uniquement **Action** est définie sur **Download and Install (Télécharger et Installer)**. Sélectionnez pour désactiver des applications de la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d'activer

© 2020 Palo Alto Networks, Inc.

Paramètres de planification des mises à jour dynamiques	
	les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/ Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.
Action (Action)	• **Download Only (Télécharger seulement)** - Panorama téléchargera la mise à jour planifiée. Vous devez « Installer » manuellement la mise à jour sur les pare-feu et les Collecteurs de journaux. • **Download and Install (Télécharger et installer)** - Panorama téléchargera et installera automatiquement la mise à jour planifiée.
Périphériques	Sélectionnez **Devices (Périphériques)**, puis sélectionnez les pare-feu qui recevront les mises à jour de contenu planifiées.
Collecteurs de journaux	Sélectionnez **Log Collectors (Collecteurs de journaux)**, puis sélectionnez les collecteurs gérés qui recevront les mises à jour de contenu planifiées.

Rétablissement des versions de contenu précédentes de Panorama

- Panorama > Déploiement de périphérique > Mises à jour dynamiques

Revert Content (Rétablissez les versions de contenu précédentes) Applications, Applications et Menaces, Antivirus, WildFire et les mises à jour de contenu WildFire d'un ou plusieurs pare-feu à la version de contenu installée précédemment sur Panorama. La version de contenu que vous rétablissez doivent être antérieure à celle qui est actuellement installée sur le pare-feu. Le rétablissement du contenu précédent est disponible sur Panorama 8.1. Le contenu des pare-feu peut être rétabli tant que la fonction de rétablissement est disponible localement sur le pare-feu.

Champ	Description
Filtre	Filtrer les périphériques sur lesquels vous aimeriez rétablir la version de contenu précédente. Vous pouvez appliquer les filtres suivants : • État de l'appareil • Plateformes • Groupes de périphériques • Modèles • Étiquettes • État HA • Version du logiciel (PAN-OS) • Version du contenu actuel
Périphériques	Sélectionnez un ou plusieurs périphériques devant faire l'objet du rétablissement. Affiche les informations sur le périphérique suivantes : • Nom du périphérique : le nom du périphérique. • Version actuelle : la version de contenu actuellement installée sur le périphérique. Un 0

© 2020 Palo Alto Networks, Inc.

Champ	Description
	sera indiqué dans la colonne si aucune version de contenu n'est installée. • Version (de contenu) antérieure : la version de contenu précédemment installée sur les pare-feu exécutant la version 8.1 de PAN-OS ou toute version ultérieure. La colonne sera vide si aucune version de contenu n'était précédemment installée ou si le pare-feu utilise une version de PAN-OS antérieure à 8.1. • Version du logiciel : la version de PAN-OS qui est actuellement installée sur le périphérique. • État HA : affiche l'état HA lorsqu'il s'agit d'une paire HA. La colonne sera vide si le périphérique ne fait pas partie d'une paire HA.
Regrouper les paires HA	Cochez cette case pour regrouper les homologues HA.

Lorsque vous avez sélectionné les périphériques devant faire l'objet du rétablissement, cliquez sur **OK**.

Gestion des licences du pare-feu

- Sélectionnez Panorama > Déploiement de périphérique > Licences

Sélectionnez **Panorama** > **Déploiement de périphérique** > **Licences** pour effectuer les tâches suivantes :

- Mettre à jour les licences des pare-feu qui ne disposent pas d'un accès direct à Internet – Cliquez sur Rafraichir.
- Activer une licence sur des pare-feu – Pour activer une licence sur des pare-feu, cliquez sur **Activer**, sélectionnez les pare-feu et, dans la colonne Code d'authentification, saisissez les codes d'autorisation que Palo Alto Networks a fournis pour les pare-feu.
- Désactiver toutes les licences et tous les abonnements / droits installés sur des pare-feu Série VM – Cliquez sur **Désactiver les VM**, sélectionnez les pare-feu (la liste affiche uniquement les pare-feu qui sont exécutés sur PAN-OS 7.0 ou une version ultérieure), et cliquez sur :
  - **Continue (Continuer)** - Désactive les licences et enregistre automatiquement les modifications sur le serveur de licences. Les licences sont recréditées sur votre compte et peuvent être réutilisées.
  - **Complete Manually (Terminer manuellement)** - Génère un fichier de jeton. Utilisez ceci si Panorama ne dispose d'aucun accès direct à Internet. Pour terminer le processus de désactivation, vous devez vous connecter au Portail d'assistance, sélectionnez **Actifs**, cliquez sur **Désactiver la (les) licence(s)**, téléchargez le fichier de jeton, et cliquez sur **Soumettre**. Terminez ensuite le processus de désactivation.

Vous pouvez également afficher l'état actuel de la licence pour les pare-feu gérés. Dans le cas de pare-feu qui disposent d'un accès direct à Internet, Panorama effectue automatiquement une vérification quotidienne sur le serveur de licences, obtient les mises à jour et les renouvellements des licences et les applique aux pare-feu. La vérification est codée strictement pour s'effectuer entre 1 h et 2 h ; vous ne pouvez pas changer cet horaire.

Informations sur les licences du pare-feu	
Périphérique	Le nom du pare-feu.

© 2020 Palo Alto Networks, Inc.

Informations sur les licences du pare-feu	
Virtual System (système virtuel - vsys)	Indique si le pare-feu prend en charge ou non des systèmes virtuels multiples.
Prévention contre les menaces	Indique si la licence est active, inactive ou expirée (ainsi que la date d'expiration).
URL	
Assistance	
Passerelle GlobalProtect	
Portail GlobalProtect	
WildFire	
Capacité de la série VM	Indique s'il s'agit ou non d'un pare-feu VM-Series.