paloalto TECHDOCS

Cloud NGFW pour Azure

1.0

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

Last Revised

May 31, 2024

Table of Contents

Démarrer avec Cloud NGFW pour Azure

Le pare-feu cloud nouvelle génération de Palo Alto Networks - un service ISV natif Azure, est un pare-feu nouvelle génération (NGFW) alimenté par ML et fourni sous forme de service cloud natif entièrement géré par Palo Alto Networks sur la plateforme Microsoft Azure. Ce modèle de déploiement combine la puissance du NGFW de Palo Alto avec la facilité d'utilisation. Le service Cloud NGFW offre une visibilité avancée des applications et un contrôle d'accès à l'aide des technologies de filtrage App-ID et des URL de Palo Alto Networks. Il assure la prévention et la détection des menaces grâce à des services de sécurité fournis dans le cloud et à des signatures de prévention des menaces.

Cloud NGFW pour Azure

Cloud NGFW est un pare-feu nouvelle génération d'apprentissage machine (ML) fourni sous forme de service cloud natif. Avec Cloud NGFW, vous pouvez exécuter plusieurs applications en toute sécurité à la vitesse du cloud et évoluer avec une véritable expérience cloud native. Cloud NGFW combine la meilleure sécurité réseau de sa catégorie avec une facilité d'utilisation afin de fournir un service cloud natif entièrement géré. Il étend les capacités de prévention des menaces de Palo Alto Networks aux fournisseurs de cloud, tout en étant nativement intégré aux diverses offres de services des fournisseurs cloud. Cloud NGFW :

- Minimise la gestion de l'infrastructure.
- Bloque les menaces Zero Day basées sur le Web en temps réel.
- Sécurise les applications lorsqu'elles se connectent à des services Web légitimes.
- Simplifie l'expérience du fournisseur cloud natif avec une gestion simple et cohérente des politiques de pare-feu sur plusieurs comptes.
- Automatise les flux de travail de bout en bout avec la prise en charge de l'API, des modèles ARM et de Terraform.

Le Cloud NGFW bloque les attaques, vulnérabilités, exploits et autres contournements connus basés sur le Web, y compris les attaques sophistiquées basées sur les fichiers, à l'aide de la technologie brevetée de classification du trafic App-ID. Cloud NGFW :

- Sécurise le trafic tout en dépassant les limites de confiance, comme les réseaux virtuels Azure et les vWAN. Le service géré fourni par Cloud NGFW empêche les attaquants d'accéder aux ressources et arrête l'exfiltration de données et le trafic de commande et contrôle (C2). Il est spécialement conçu pour arrêter les mouvements latéraux est-ouest ou non autorisés.
- Il est conçu dans un souci d'automatisation. Avec la configuration rulestack et les profils de sécurité automatisés, Cloud NGFW est conçu pour répondre facilement aux exigences de sécurité du réseau avec une interface utilisateur intuitive qui simplifie la création de ressources du pare-feu résilientes qui évoluent avec le trafic de votre réseau.
- Intègre un modèle de pare-feu cloud automatisé qui évolue dynamiquement avec le trafic de votre réseau et répond aux demandes de débit imprévisibles avec l'équilibrage de la charge de la passerelle (GWLB) pour une haute disponibilité à la demande et une mise à l'échelle élastique. Vous pouvez accéder à autant de capacité ou aussi peu que vous le souhaitez, et évoluer selon vos besoins.
- Intègre la sécurité aux flux de travail gérés par les fournisseurs cloud. Avec Cloud NGFW, le premier pare-feu nouvelle génération à s'intégrer aux fournisseurs cloud, vous pouvez éviter de longs cycles de déploiement et être opérationnel rapidement, même lors de la configuration des rulestacks requises et des profils de sécurité automatisés. Vous pouvez tirer parti du modèle de sécurité fourni par le fournisseur cloud choisi tout en intégrant ses capacités d'intégration, de surveillance et de journalisation. Cloud NGFW offre un avantage unique lors de l'intégration aux fournisseurs cloud. Vous pouvez profiter d'une mise à l'échelle automatique et d'une haute disponibilité sans aucune maintenance. Cette intégration permet une gestion cohérente des politiques de pare-feu sur plusieurs comptes de fournisseurs cloud.

Vous pouvez utiliser le Cloud NGFW pour Azure. Avec le Cloud NGFW, vous pouvez accéder aux fonctionnalités NGFW de base, notamment App-ID, le filtrage des URL basé sur les catégories d'URL et les géolocalisations et le décryptage SSL/TLS.

Fonctionnalités prises en charge

Le Cloud NGFW pour Azure fournit les fonctionnalités suivantes :

- **Déploiement et gestion cloud natifs**. Activez les fonctionnalités du pare-feu nouvelle génération dans votre environnement Azure tout en gérant de manière transparente les opérations du jour 0 et du jour N sur les ressources Cloud NGFW, comme vous le feriez avec n'importe quel autre service Azure. Pour les autorisations, utilisez le contrôle d'accès basé sur les rôles (RBAC) Azure pour contrôler les ressources Cloud NGFW.
- **Visibilité et contrôle avancés des applications**. Cloud NGFW offre une connaissance avancée des applications et un contrôle des accès à l'aide de App-ID et de techniques de filtrage des URL.
- **Prévention des menaces de nouvelle génération** Les fonctionnalités NGFW de Palo Alto Networks, avec des services de sécurité fournis dans le cloud et des signatures de prévention des menaces, sont fournies sur la base du matériel physique et des logiciels installés.

Le modèle Cloud NGFW pour Azure

Le Cloud NGFW est un service ISV natif Azure. Cette approche permet à Palo Alto Networks de développer et de gérer le FWaaS à l'aide d'hameçons fournis par le service Azure pour exploiter nativement le FWaaS via les API et l'interface utilisateur Azure. Le Cloud NGFW pour Azure est accessible dans l'Azure Marketplace. Vous pouvez utiliser tous les avantages du NGFW de Palo Alto Network pour les VNet et vWAN d'Azure.

Composants Cloud NGFW

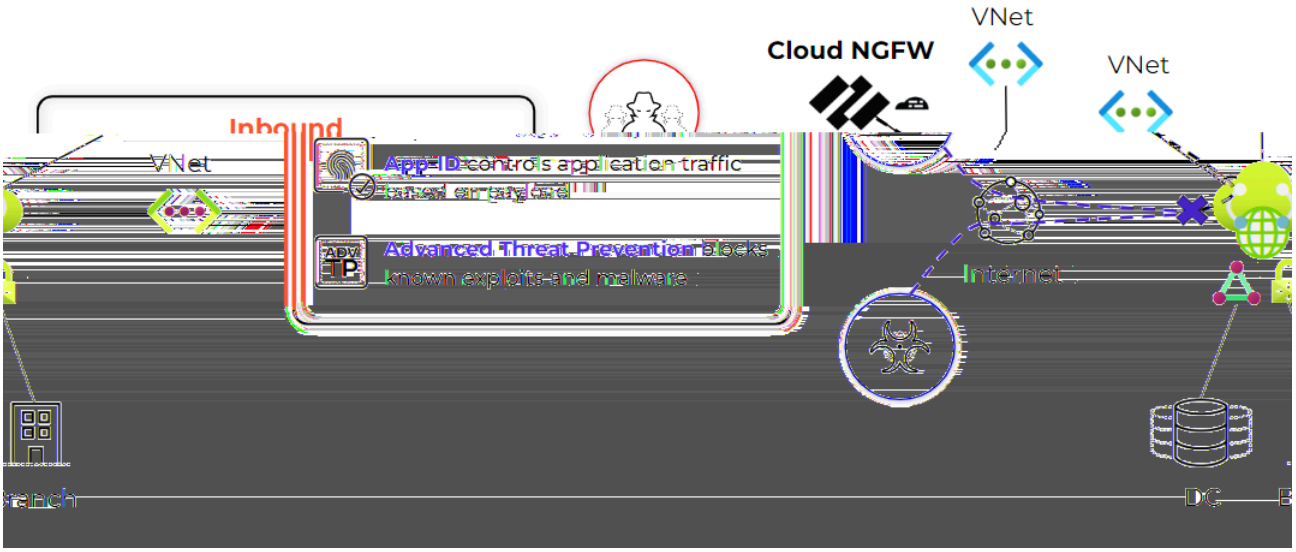
Le Cloud NGFW pour Azure comprend les composants clés suivants :

- **Le Cloud NGFW**. Le Cloud NGFW est un service régional Azure géré, disponible dans certaines régions Azure clés.
- **NGFW**. Palo Alto Networks utilise le NGFW comme ressource associée au hub vNET ou vWAN du client. Il offre résilience, évolutivité et gestion du cycle de vie. Le NGFW se manifeste sous la forme d'adresses IP privées dans le sous-réseau NGFW spécifié par l'utilisateur. Pour utiliser la ressource NGFW, mettez à jour les UDR VNet pour envoyer le trafic via les adresses IP privées.
- **Rulestack NGFW**. Cette ressource comprend un ensemble de règles de sécurité ainsi que des objets et des profils de sécurité associés pour permettre le contrôle d'accès avancé, à l'aide de App-ID et du filtrage des URL, ainsi que des fonctionnalités de prévention des menaces. Vous pouvez associer une rulestack locale à un ou plusieurs NGFW.

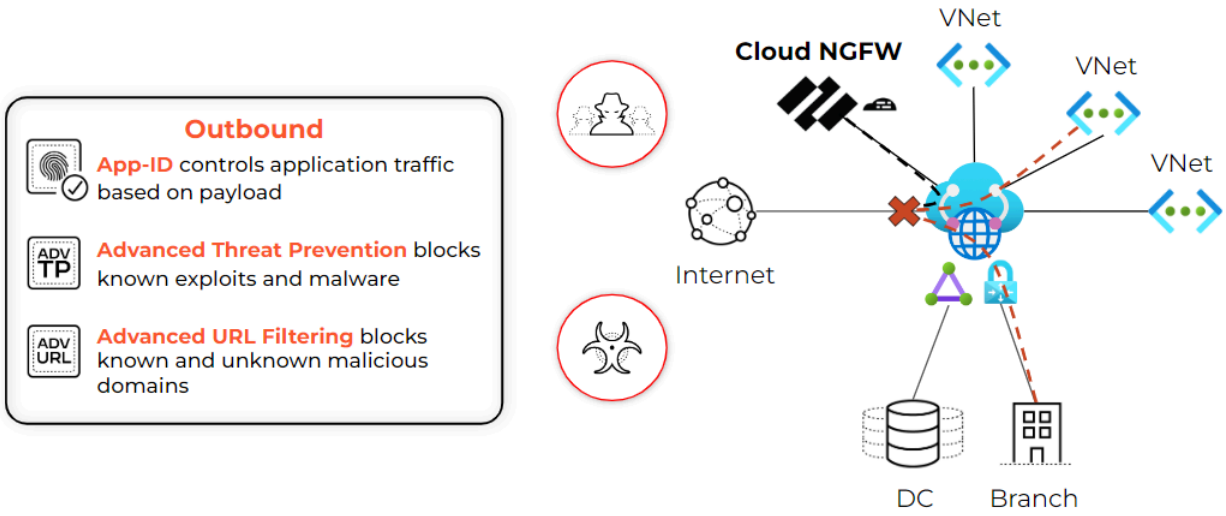
Sécuriser le trafic avec le Cloud NGFW

Cloud NGFW vous fournit les outils et les fonctionnalités nécessaires pour sécuriser le trafic entrant, le trafic sortant et le trafic est-ouest.

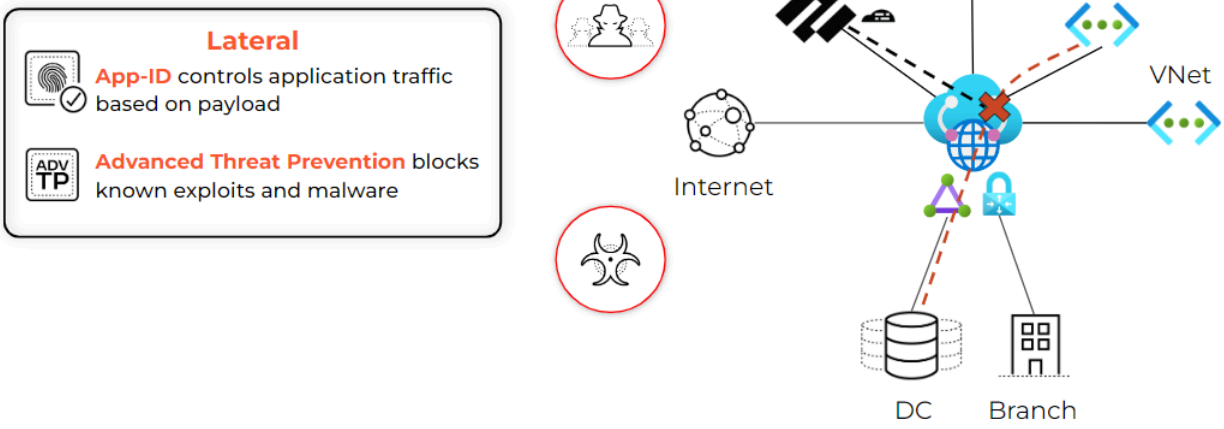
Le trafic **entrant** fait référence à tout trafic provenant de l'extérieur de votre région Azure et destiné à des ressources situées à l'intérieur des VNet de l'application, comme des serveurs ou des équilibreurs de charge. Cloud NGFW peut empêcher les logiciels malveillants et les vulnérabilités d'entrer dans votre VNet dans le trafic entrant autorisé par les groupes de sécurité Azure.



Le trafic **sortant** fait référence au trafic provenant du VNet de l'application et est destiné à des ressources situées en dehors de la région Azure. Cloud NGFW protège les flux de trafic sortant en garantissant que les ressources du VNet de l'application se connectent aux services et URL autorisés tout en empêchant l'exfiltration de données et d'informations sensibles.



Le trafic **est-ouest** se déplace au sein d'une région Azure. Plus précisément, le trafic entre la source et la destination est déployé dans deux VNet d'application différents ou dans deux sous-réseaux différents dans le même VNet. Cloud NGFW peut arrêter la propagation de logiciels malveillants dans votre environnement Azure.



Composants Cloud NGFW

Cloud NGFW pour Azure crée un certain nombre de composants qui fonctionnent ensemble pour sécuriser votre environnement Azure.

- La **ressource Cloud NGFW** (ou simplement NGFW) est associée à votre hub VNet ou vWAN et peut couvrir plusieurs zones de disponibilité. Cette ressource intègre la résilience, l'évolutivité et la gestion du cycle de vie.
- Les **rulestacks** définissent le comportement de filtrage du trafic NGFW, tel que le contrôle d'accès avancé (App-ID, filtrage des URL) et la prévention des menaces. Une rulestack inclut un ensemble de règles de sécurité ainsi que les objets et profils de sécurité associés. Pour utiliser une rulestack, vous devez l'associer à une ou plusieurs ressources NGFW.

Régions prises en charge par Cloud NGFW pour Azure

Une région Azure prend en charge jusqu'à trois zones de disponibilité, avec une seule machine virtuelle attribuée requise dans chaque zone. Le trafic dans chaque zone utilise un réseau virtuel, éliminant ainsi tous les frais interzones. Le tableau suivant illustre la disponibilité des zones pour une région spécifique.

Nom de la région	Indicatif régional
Est de l'Australie	australiaeast
Australie Sud-Est	australiasoutheast
Sud du Brésil	brazilsouth
Centre du Canada	canadacentral
Est du Canada	canadaeast
Centre de l'Inde	centralindia
Centre des États-Unis	centralus
Asie orientale	eastasia
Est États-Unis	eastus
Est États-Unis 2	eastus2
Centre de la France	francecentral
Centre-Ouest Allemagne	germanywestcentral
Centre d'Israël	israelcentral
Nord de l'Italie (Milan)	italynorth
Est du Japon	japaneast
Ouest du Japon	japanwest
Centre-Nord États-Unis	northcentralus
Europe du Nord	northeurope
Est de la Norvège	norwayeast
Nord de l'Afrique du Sud (Johannesburg)	southafricanorth

Nom de la région	Indicatif régional
Centre-Sud des États-Unis	southcentralus
Asie du Sud-Est	southeastasia
Centre de la Suède (Gävle)	swedencentral
Nord de la Suisse	switzerlandnorth
Nord des EAU (Dubaï)	uaenorth
Sud du Royaume-Uni	uksouth
Ouest du Royaume-Uni	ukwest
Ouest Europe	westeurope
Centre-Ouest des États-Unis (Wyoming)	westcentralus
Ouest États-Unis	westus
Ouest États-Unis 2	westus2
Ouest États-Unis 3	westus3

Limites et quotas de Cloud NGFW pour Azure

Les tableaux suivants répertorient les limites et données de performances pour votre locataire Cloud NGFW. Sauf indication contraire, vous pouvez demander une augmentation de ces limites.

Utilisez l'estimateur de tarification Cloud NGFW pour Azure pour vous aider à déterminer les limites et les quotas Azure pour votre abonnement Cloud NGFW.

Gestion des politiques de rulestacks locales

Nom	Limites par défaut par client Cloud NGFW
Nombre de comptes Cloud (Azure) dans un locataire	200

Gestion native des politiques (rulestack)

Attribut	Limite maximale par ressource Cloud NGFW
Règles de sécurité	1 000
Objets d'adresses (liste FQDN et listes de préfixes IP)	1 000
Nombre de listes de préfixes IP	1 000
Objets FQDN dans toutes les listes FQDN	2 000
Objets préfixes pour chaque liste de préfixes IP	2 500
Catégories d'URL personnalisées	500
URL dans toutes les catégories d'URL	25 000
Flux intelligents (notamment les cinq flux prédéfinis)	30
Adresses IP dans tous les flux	50 000
Objets certificats	100

Gestion des politiques de Panorama

Attribut	Limite maximale par ressource Cloud NGFW*
Politique	
Règles de sécurité	10,000
Règles de décryptage	1 000
Objets	
Objets d'adresse	10,000
Groupes d'adresses	1 000
Membres par groupe d’adresses	2 500
Groupes d’adresses FQDN	2 000
Objets de service	2 000
Groupes de services	500
Membres par groupe de service	500
EDL	
Nombre maximal de DNS par système de domaine	500 000
Nombre maximal d’adresses IP par système	50 000
Nombre maximal d’URL par système	100 000
Nombre maximal de listes personnalisées	30
Filtrage d'URL	
Nombre total d’entités pour la liste d’autorisation, la liste de blocage et les catégories personnalisées	25 000
Nombre maximal de catégories personnalisées	500

* Les limites sur la politique et les objets spécifiés sont un maximum unidimensionnel. Palo Alto Networks recommande des tests supplémentaires au sein de votre environnement pour garantir que vous atteignez vos objectifs de création de politique.

Performances de Cloud NGFW pour Azure

Le tableau suivant fournit des informations sur les performances de votre locataire Cloud NGFW pour Azure.

Les informations contenues dans le tableau suivant supposent un maximum de 40 instances.

Attribute (Attribut)	Performance metric (Mesure des performances)
Firewall Throughput (App-ID enabled) (Débit du pare-feu (App-ID activé))	Débit maximal : 100 Gbit/s ; 2,92 Gbit/s par instance Démarrage à froid : 8,55 Gbit/s *La détection des menaces de contenu est activée pour le trafic à démarrage à froid. Sans protection contre les menaces de contenu, chaque instance du pare-feu est limitée à 3,00 Gbit/s en raison du type d'instance. Il s'agit d'une limitation voulue par Azure.*
Débit de prévention des menaces	Débit maximal : 92 Gbit/s ; 2,31 Gbit/s par instance
Débit du trafic crypté	44 Gbit/s (avec détection des menaces de contenu) ; 1,11 Gbit/s par instance 60 Gbit/s (sans détection des menaces de contenu) ; 1,52 Gbit/s par instance

Tarification de Cloud NGFW pour Azure

Cloud NGFW est disponible sous forme d'abonnement à l'utilisation (PAYG) sur l'Azure Marketplace. Avec ce modèle, vous ne payez que ce que vous utilisez chaque mois et vous bénéficiez également des avantages d'Azure Marketplace tels que la facturation consolidée et le crédit pour le programme Microsoft Azure Consumption Commitment (MACC) d'une organisation.

Cloud NGFW pour Azure facture la consommation à l'aide du service de mesure Azure Marketplace. Ce modèle offre une flexibilité tarifaire basée sur les heures de déploiement de tous les NGFW Cloud, le volume total de trafic traité et les fonctionnalités de sécurité utilisées. La facturation de la **ressource NGFW de base** repose sur les dimensions et les unités suivantes :

Dimension	Prix	Équivalent en crédits Cloud NGFW
Utilisation de la ressource NGFW de base	1,50 $ par heure de déploiement	125
Trafic sécurisé (15 premiers To/mois) par locataire	0,065 $ par 1 Go traité	5,416666667
Trafic sécurisé (15 To suivants/mois) par locataire	0,045 $ par 1 Go traité	3,75
Trafic sécurisé (au-delà de 30 To/mois) par locataire	0,030 $ par 1 Go traité	2,5
Modules complémentaires	0,12 $ par tranche de 10 unités	Pour connaître les informations de facturation spécifiques à chaque module complémentaire, reportez-vous ci-dessous.
Frais de mise en réseau Azure	0,01 $ par 1 Go traité	

Cloud NGFW pour Azure facture l'utilisation de sortie (trafic entrant, sortant et est-ouest) sous la dimension des frais de mise en réseau Azure, puis les détails de la consommation sont partagés sur l'Azure Marketplace. La tarification du réseau virtuel Azure détermine ces frais. Pour plus d'informations, reportez-vous à la section Tarification du réseau virtuel.

Protection avancée contre les menaces, Filtrage des URL avancé, Modules complémentaires Wildfire avancés

L'utilisation de ces services de sécurité est facturée selon la **dimension des modules complémentaires**. L'utilisation est mesurée en $/heure et en $/Go comme détaillé dans le tableau suivant.

Trafic sécurisé	Prix par heure	Prix par Go	Équivalent en crédits Cloud NGFW
Heure d’utilisation	0,450 $	-	37,5
15 premiers To/mois		0,020 $	1,6
15 To suivants/mois		0,014 $	1,125
Au-delà de 30 To/mois		0,009 $	0,75

Modules complémentaires de sécurité DNS et WildFire

L’utilisation de ces services de sécurité est facturée selon la **dimension des modules complémentaires**. L’utilisation est mesurée en $/heure et en $/Go comme détaillé dans le tableau suivant.

Trafic sécurisé	Prix par heure	Prix par Go	Équivalent en crédits Cloud NGFW
Heure d’utilisation	0,300 $	-	25
15 premiers To/mois		0,013 $	1,083333333
15 To suivants/mois		0,009 $	0,75
Au-delà de 30 To/mois		0,006 $	0,5

Module complémentaire de gestion centralisée de Panorama

L’utilisation de ce service de sécurité est facturée selon la **dimension des modules complémentaires**. L’utilisation est mesurée en $/heure et en $/Go comme détaillé dans le tableau suivant.

Trafic sécurisé	Prix par heure	Prix par Go	Équivalent en crédits Cloud NGFW
Heure d’utilisation	0,300 $	-	25
15 premiers To/mois		0,003 $	0,2166666667
15 To suivants/mois		0,002 $	0,15
Au-delà de 30 To/mois		0,001 $	0,1

Frais de mise en réseau Azure

Palo Alto Networks supporte les coûts d'appairage VNet associés aux interfaces réseau utilisées pour exposer la ressource Cloud NGFW dans l'abonnement du client. Ces coûts seront transmis au client sur la base de la tarification de l'appairage du réseau virtuel Azure.

Consommation de crédits et visibilité de l'utilisation

Il est désormais possible d'utiliser les crédits NGFW pour la consommation de Cloud NGFW dans le cadre de contrats à long terme que vous pouvez allouer à vos ressources de pare-feu dans les environnements Cloud Azure au niveau du locataire. Vous pouvez acheter vos crédits Cloud NGFW via les canaux et processus de vente standard de Palo Alto Networks.

Pour cela, vous aurez besoin d'un abonnement PAYG. Contactez votre équipe commerciale pour en savoir plus.

Tenez compte de ce qui suit :

- Le pool de crédits a une heure de début et une heure de fin. L'unité de la valeur est le crédit/heure (également appelé capacité).
- La capacité est calculée en fonction de la combinaison des Services et de la quantité de trafic traité dans le temps (par heure, par exemple).
- Pour estimer le crédit requis pour le pare-feu Cloud NGFW dans Azure, utilisez l'estimateur de tarification Cloud NGFW pour Azure. Celui-ci indiquera le nombre de crédits requis pour la quantité de ressources, de services et de trafic saisie. Le crédit en dollars sera également affiché.
- Une fois les crédits achetés et réclamés, ils seront ajoutés au compte Azure au niveau du locataire :
  - Toutes les ressources déployées au sein du locataire consommeront les crédits du même pool.
  - Si l'utilisation excède le montant de crédit alloué, le dépassement sera facturé en tant que PAYG (mode de paiement par défaut).
  - Ces frais seront comptabilisés comme frais de partenaire Marketplace sur la facture mensuelle Azure.

Si vous avez souscrit à *x* capacité, alors *x * 24 (heures) * 30 (nombre de jours dans un mois)* crédits seront ajoutés à votre compte chaque mois dans votre portefeuille de crédits. Les crédits sont déduits du portefeuille de crédits selon votre utilisation pour le mois jusqu'à la date de fin du contrat. Vous pouvez augmenter la capacité des crédits via votre canal de vente. Après expiration des crédits, vous pouvez renouveler les crédits pour une capacité et une date de fin différentes.

Comment réclamer vos crédits

Pour réclamer vos crédits, vous aurez besoin du numéro de série du produit Cloud NGFW et d'un ID de compte de support CSP (portail de support client de Palo Alto Network). Il existe deux méthodes pour générer le numéro de série du produit Cloud NGFW :

- Créez un pare-feu.
- Créez une rulestack.

Vous pouvez ensuite créer un compte de série CSP à l'aide du numéro de série du produit (numéro de série CSP du locataire) ou lier un compte CSP existant à l'aide du lien *Register your Azure tenant to a new or existing Palo Alto Networks support account (Enregistrer votre locataire Azure sur un compte de*

support Palo Alto Networks nouveau ou existant) dans la section New Support Request (Nouvelle demande d'assistance).

Une fois le locataire enregistré, vous pouvez l'utiliser pendant la période d'essai gratuit de 30 jours. Si vous avez utilisé les crédits gratuits avant la fin de la période d'essai gratuit de 30 jours, des frais supplémentaires seront facturés aux taux PAYG.

Si vous ajoutez des crédits Cloud NGFW pendant la période d'essai gratuit, votre contrat commence immédiatement et remplace l'essai gratuit.

Vous pouvez vérifier vos informations d'utilisation des crédits dans la section **New Support Request (Nouvelle demande d'assistance)** dans l'Azure Marketplace.

Si votre consommation mensuelle moyenne excède les crédits achetés, les dépassements sont facturés aux taux PAYG.

*Les crédits sont réinitialisés le premier jour de chaque mois. Si vos crédits expirent, votre compte applique les taux PAYG. Les crédits inutilisés ne sont pas reportés sur le mois suivant. Utilisez l'*estimateur de tarification Cloud NGFW pour Azure *pour vous aider à déterminer la tarification Azure pour votre locataire Cloud NGFW.*

Essai gratuit de Cloud NGFW pour Azure

Lorsque vous créez le premier Cloud NGFW ou la première rulestack de votre locataire Azure AD, vous bénéficiez automatiquement d'un essai gratuit de 30 jours. La période d'essai gratuite commence dès la création de votre premier Cloud NGFW pour la ressource Azure.

L'essai gratuit est effectif sur tous les abonnements du locataire Azure AD.

Pendant la période d'essai gratuite, vous pouvez utiliser gratuitement :

- Deux ressources Cloud NGFW
- Un To de trafic inspecté au total (moyenne de 500 Go par ressource Cloud NGFW)
- Intégration de Panorama
- Prévention des menaces et filtrage des URL avec services de sécurité fournis par le cloud (CDSS) activés

Sachez que des frais s'appliquent selon les modalités décrites dans la liste d'abonnement Azure Marketplace **Palo Alto Networks Cloud NGFW Pay-As-You-Go** à la fin de votre période d'essai gratuit ou lorsque votre utilisation dépasse les limites de l'essai gratuit. Tenez compte des éléments suivants lorsque vous profitez de l'essai gratuit.

- Vous ne pouvez pas interrompre la période d'essai gratuite
- À la fin de votre période d'essai gratuite, des frais s'appliqueront lorsque vous utiliserez le Cloud NGFW.

Commencer avec Cloud NGFW pour Azure

Vous devez commencer par enregistrer Palo Alto Networks en tant que **Resource Provider (Fournisseur de ressources)**. Dans la section **Settings (Paramètres)** de la console Azure, sélectionnez **Resource providers (Fournisseurs de ressources)**. Recherchez Palo Alto Networks Cloud NGFW et sélectionnez **PaloAltoNetworksCloudngfw**, puis cliquez sur **Register (Enregistrer)**.

Connectez-vous ensuite au portail Azure pour créer un Cloud NGFW et ses règles de politique. Lorsque vous créez un NGFW, vous devez spécifier les vNet ou vWAN Azure et les sous-réseaux que vous devez sécuriser. Après avoir créé le NGFW, vous devez mettre à jour les tables de routage de vos passerelles et sous-réseaux afin d’acheminer tout le trafic vers le NGFW pour inspection.

Gérer les rôles Cloud NGFW pour les utilisateurs Azure

À tout moment, vous pouvez modifier le ou les rôles d'un utilisateur pour étendre ou réduire son accès et ses autorisations. Vous pouvez également supprimer un utilisateur. Et les utilisateurs individuels peuvent afficher leurs rôles et modifier leur nom ou leur mot de passe si nécessaire. Les informations fournies ici sont utiles pour la création de rôles personnalisés, comme la création d'un utilisateur de pare-feu en lecture seule. Par défaut, Cloud NGFW requiert un rôle propriétaire ou contributeur sur l'abonnement pour s'abonner au fournisseur de ressources et utiliser la ressource Cloud NGFW.

Pour plus d'informations sur la gestion des rôles Cloud NGFW, reportez-vous à la section Attribuer des rôles Azure à l'aide du portail Azure.

Intégrer Single Sign-On (ouverture de session unique - SSO)

Vous pouvez intégrer le flux de connexion SSO de votre organisation à votre compte du portail de support client (CSP) de Palo Alto Networks pour votre abonnement Azure Cloud NGFW.

Activer le fournisseur d'identité tiers (IDP)

L'activation d'un fournisseur d'identité tiers (IDP) dans le portail de support client (CSP) vous permet de vous connecter au CSP de Palo Alto Networks à l'aide de vos propres identifiants de connexion d'entreprise. Étant donné que vous configurez l'IDP au niveau du domaine, les membres du domaine peuvent se connecter à plusieurs comptes CSP à l'aide des identifiants de connexion SSO de l'entreprise. Toutefois, les *comptes Administrateur de domaine* doivent continuer d'utiliser les identifiants de connexion Palo Alto Networks.

Pour activer l'IDP tiers pour votre domaine :

- Vous devez disposer du rôle administrateur de domaine dans le CSP pour configurer l'accès IDP tiers pour votre compte.
- Vous devez disposer d'un accès administrateur sur le fournisseur d'identité pour mettre à jour les détails de configuration SSO fournis par Palo Alto Networks.
- Vous avez besoin d'un compte non administrateur de domaine pour la vérification.

STEP 1 | Connectez-vous au portail Azure et recherchez **Active Directory**.

STEP 2 | Dans Active Directory, sélectionnez **Enterprise Application (Application d'entreprise)** et sélectionnez **New Application (Nouvelle application)**.

STEP 3 | Saisissez le nom de votre application SSO (par exemple, panorama-sso) et cliquez sur **Create (Créer)**.

STEP 4 | Dans la fenêtre**Create your own application (Créer votre propre application)**, sélectionnez **Integrate any other application you don't find in the gallery (Non-gallery) (Intégrer toute autre application que vous ne trouvez pas dans la galerie))**.

STEP 5 | Cliquez sur **Create (Créer)**.

STEP 6 | Dans la section **Manage (Gérer)**, cliquez sur **Single sign-on (Ouverture de session unique)**.

STEP 7 | Sélectionnez la méthode d'ouverture de session unique **SAML**. La page de connexion SAML contient les informations dont vous avez besoin pour lier votre nouvelle application d'entreprise SSO à votre compte CSP Palo Alto Networks.

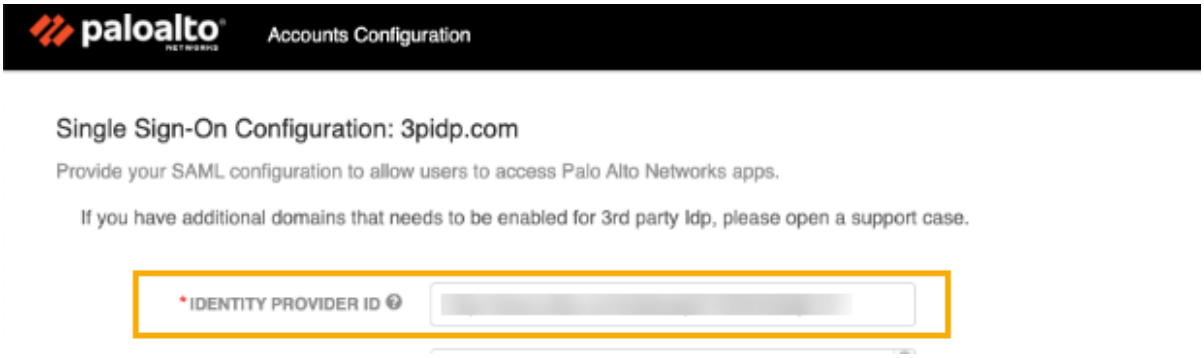
STEP 8 | Dans la page de connexion SAML, faites défiler vers le bas pour rechercher les URL dans la section **Set up [your SSO application name] (Configurer [nom de votre application SSO])**. Copiez l'**identifiant Azure AD**.

STEP 9 | Connectez-vous au CSP.

STEP 10 | Dans le CSP, sélectionnez **Account Management (Gestion du compte) > Account Details (Détails du compte)**.

STEP 11 | Dans la section **SSO**, cliquez sur **View Single Sign-On settings for your domain (Afficher les paramètres SSO de votre domaine)**.

STEP 12 | Dans **Accounts Configuration (Configuration des comptes)**, collez l'**identifiant Azure AD** copié à l'étape 8 dans le champ **Identifier Provider ID (ID du fournisseur d'identifiant)**.



STEP 13 | Revenez à l'écran **de connexion SAML** dans le portail Azure. Faites défiler vers le bas pour rechercher les URL dans la section **Set up [your SSO application name] (Configurer [nom de votre application SSO])**. Copiez l'**URL de connexion**.

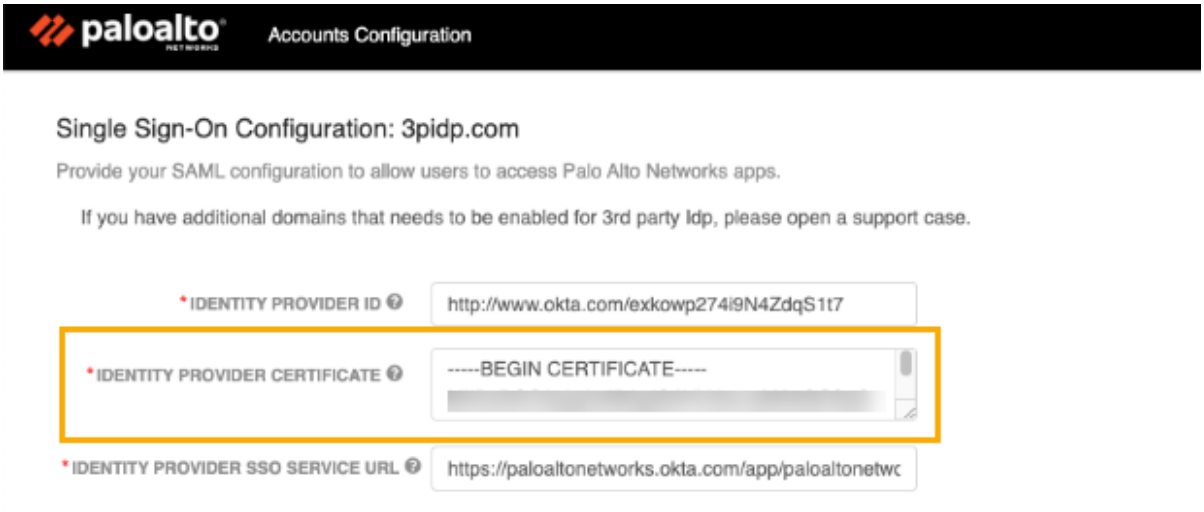
STEP 14 | Revenez à la page **Accounts Configuration (Configuration des comptes)** dans le CSP. Collez l'**URL de connexion** copiée (à l'étape précédente) dans le champ **Identity Provider SSO Service URL (URL du service SSO du fournisseur d'identité)**.

STEP 15 | Utilisez la même adresse**Identity Provider SSO Service URL (URL du service SSO du fournisseur d'identité)** pour le champ **Identity Provider Destination URL (URL de destination du fournisseur d'identité)**.

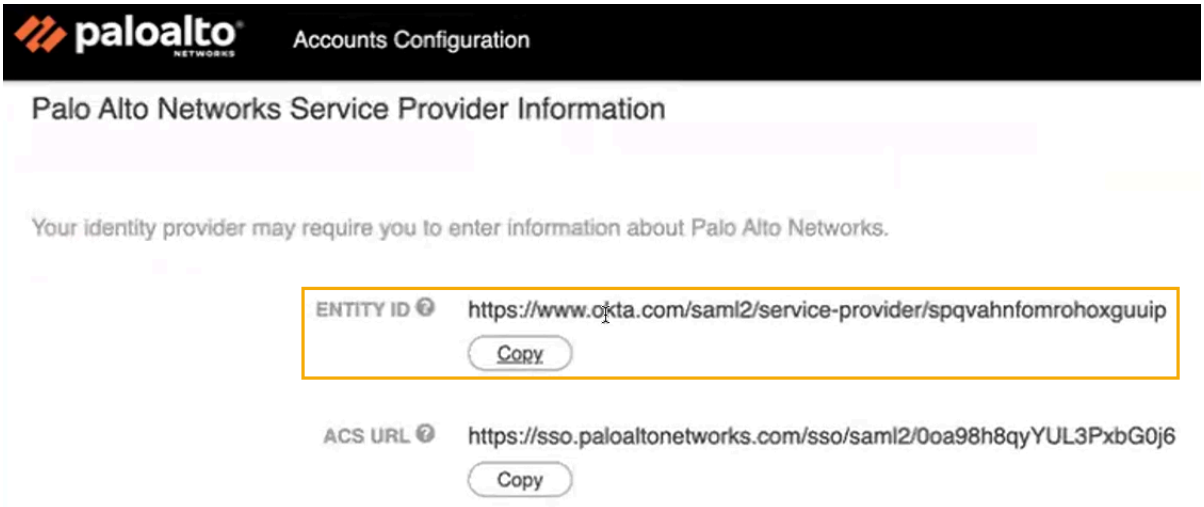
STEP 16 | Revenez à l'écran de **connexion SAML** dans le portail Azure. Faites défiler vers le bas pour rechercher la section **SAML Certificates (Certificats SAML)**.

STEP 17 | Dans la section SAML Certificates (Certificats SAML), téléchargez le **Certificat (Base64)**.

STEP 18 | Revenez à la page **Account Management (Gestion du compte) > Account Details (Détails du compte)** dans le CSP. Collez le certificat téléchargé (à l'étape précédente) dans le champ **Identity Provider Certificate (Certificat de fournisseur d'identité)**.



STEP 19 | La page **Accounts Configuration (Configuration des comptes)** affiche alors **Palo Alto Service Provider Information (Informations sur le fournisseur de services Palo Alto)**. Copiez l'URL **Entity ID (ID d'entité)**.



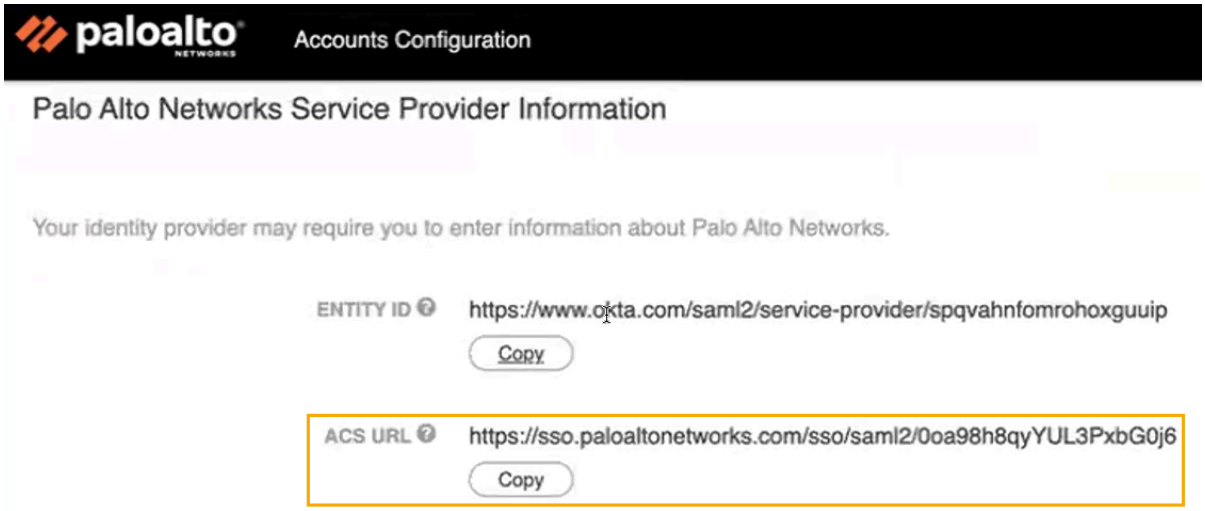
STEP 20 | Revenez à l'écran de **connexion SAML** dans le portail Azure.

STEP 21 | Dans l'écran **Basic SAML Configuration (Configuration SAML de base)**, cliquez sur **Edit (Modifier)**.

STEP 22 | Dans le champ **Identifier (Entity ID) (Identifiant (ID d'entité))**, cliquez sur **Add Identifier (Ajouter un identifiant)**.

STEP 23 | Collez l'**Entity ID (ID d'entité)** Palo Alto Networks (de l'étape 21) dans le champ **Identifier (Identifiant)**.

STEP 24 | Revenez à la page **Account Management (Gestion du compte) > Account Details (Détails du compte)** dans le CSP. Copiez l'**URL ACS**.



STEP 25 | Revenez à l'écran de **connexion SAML** dans le portail Azure.

STEP 26 | Dans l'écran **Basic SAML Configuration (Configuration SAML de base)**, cliquez sur **Edit (Modifier)**.

STEP 27 | Saisissez l'URL ACS (copiée à l'étape 24) dans le champ **Reply URL (URL de réponse) (URL du service consommateur d'assertion)**.

STEP 28 | Revenez à la page **Accounts Configuration (Configuration des comptes)** dans le CSP. Utilisez le bouton d'activation/de désactivation pour **activer le fournisseur d'identité**.

STEP 29 | Cliquez sur **Save (Enregistrer)**.

STEP 30 | Revenez au portail Azure. Dans la section **Manage (Gérer)** de votre application SSO, cliquez sur **Users and groups (Utilisateurs et groupes)**.

STEP 31 | Utilisez l'option **Add user/group (Ajouter un utilisateur/groupe)** pour activer l'utilisation de la connexion SSO pour chaque utilisateur spécifié.

Vérifier la connexion SSO

Après avoir activé le fournisseur d'identité, tous les utilisateurs (à l'exception des administrateurs de domaine) sont obligés d'utiliser la connexion SSO. Pour vérifier que la connexion SSO est correctement configurée :

- Renseignez une adresse e-mail sur la page de connexion. N'utilisez pas les information d'identification de connexion de l'administrateur de domaine.
- Vérifiez que vous êtes redirigé vers la page de connexion de l'IDP pour l'authentification.
- Une fois l'authentification effectuée, la page du portail de support client de Palo Alto Networks s'affiche.

Intégrer la connexion SSO au CSP pour un utilisateur n'appartenant pas au domaine à l'aide de l'Azure Marketplace

Pour intégrer un utilisateur à un compte CSP à l'aide de l'Azure Marketplace :

STEP 1 | Connectez-vous à votre compte Azure.

STEP 2 | Dans **Azure Services (Services Azure)**, sélectionnez **Cloud NGFWs by Palo Alto Networks (Cloud NGFW par Palo Alto Networks)**.

STEP 3 | Sélectionnez le pare-feu que vous souhaitez intégrer à votre compte CSP.

STEP 4 | Dans la section **Support + Troubleshooting (Assistance + Dépannage)**, cliquez sur **New Support Request (Nouvelle demande d'assistance)**. L'écran Palo Alto Networks Support (Support de Palo Alto Networks) apparaît et affiche l'**ID de locataire** et le **numéro de série du produit**.

STEP 5 | Cliquez sur **Register User account and create a case at Customer Support Portal (Enregistrer un compte utilisateur et créer un dossier sur le portail de support client)**.

STEP 6 | Sur la page **Create New Account / Use Existing Account (Créer un compte/Utiliser un compte existant)**, saisissez votre adresse e-mail et suivez les étapes d'authentification, puis cliquez sur **Next (Suivant)**.

STEP 7 | Dans la section **Device Registration (Enregistrement du périphérique)**, sélectionnez l'abonnement **Cloud Marketplace** dans le menu déroulant. Par exemple *Azure Cloud NGFW*.

STEP 8 | Saisissez l'**ID de locataire** et le **numéro de série** pour votre abonnement Azure Marketplace. Vous pouvez copier ces informations depuis la page de support Palo Alto à l'étape 4. Cliquez sur **Next (Suivant)**.

STEP 9 | Saisissez le **code d'authentification** qui a été envoyé à votre adresse e-mail. Cliquez sur **Next (Suivant)**.

STEP 10 | Une fois l'authentification effectuée à l'aide de la connexion SSO, la page de connexion CSP s'affiche. Saisissez votre adresse e-mail et cliquez sur **Next (Suivant)**.

Intégrer la connexion SSO au CSP pour un utilisateur appartenant au domaine à l'aide de l'Azure Marketplace

Pour intégrer un *utilisateur du domaine* à un compte CSP à l'aide de l'Azure Marketplace, vous aurez besoin de vos informations d'identification de connexion Palo Alto Networks :

STEP 1 | Connectez-vous à votre compte Azure à l'aide des *informations d'identification de connexion d'utilisateur du domaine*.

STEP 2 | Dans **Azure Services (Services Azure)**, sélectionnez **Cloud NGFWs by Palo Alto Networks (Cloud NGFW par Palo Alto Networks)**.

STEP 3 | Sélectionnez le pare-feu que vous souhaitez intégrer à votre compte CSP.

STEP 4 | Dans la section **Support + Troubleshooting (Assistance + Dépannage)**, cliquez sur **New Support Request (Nouvelle demande d'assistance)**. L'écran Palo Alto Networks Support (Support de Palo Alto Networks) apparaît et affiche l'**ID de locataire** et le **numéro de série du produit**.

STEP 5 | Cliquez sur **Register User account and create a case at Customer Support Portal (Enregistrer un compte utilisateur et créer un dossier sur le portail de support client)**.

STEP 6 | Sur la page **Create New Account / Use Existing Account (Créer un compte/Utiliser un compte existant)**, saisissez votre adresse e-mail et suivez les étapes d'authentification, puis cliquez sur **Next (Suivant)**.

STEP 7 | Dans la section **Device Registration (Enregistrement du périphérique)**, sélectionnez l'abonnement **Cloud Marketplace** dans le menu déroulant. Par exemple *Azure Cloud NGFW*.

STEP 8 | Saisissez l'**ID de locataire** et le **numéro de série** pour votre abonnement Azure Marketplace. Vous pouvez copier ces informations depuis la page de support Palo Alto à l'étape 4. Cliquez sur **Next (Suivant)**.

STEP 9 | Saisissez le **code d'authentification** qui a été envoyé à votre adresse e-mail. Cliquez sur **Next (Suivant)**.

STEP 10 | Une fois l'authentification effectuée à l'aide de la connexion SSO, la page de connexion CSP s'affiche. Saisissez votre adresse e-mail et cliquez sur **Next (Suivant)**.

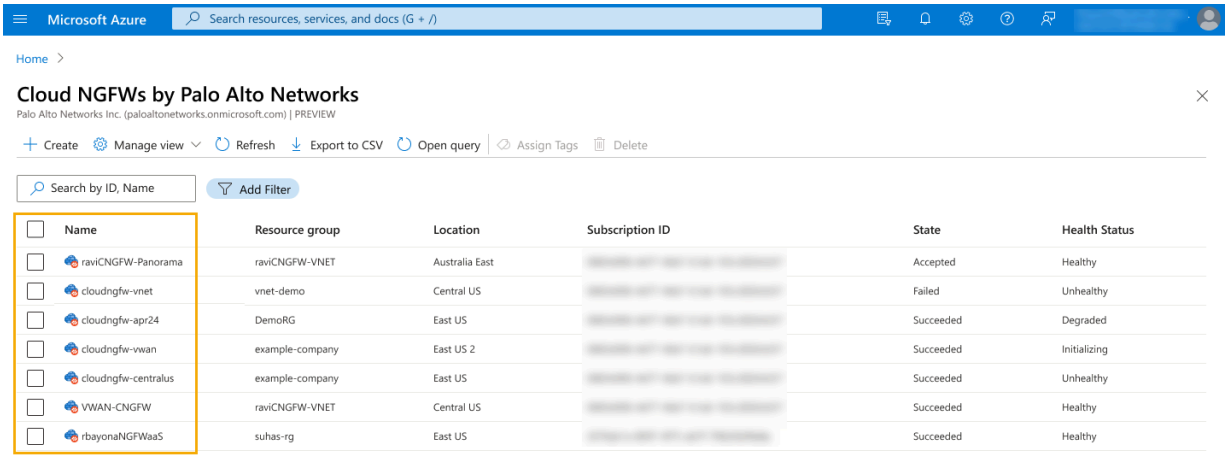
Surveiller l’état de santé du Cloud NGFW

Cloud NGFW prend en charge la surveillance de l’état de santé à l’aide du portail Azure. Affichez l’état de santé global du pare-feu et de la connexion, ainsi que les informations de diagnostic que vous pouvez utiliser pour déterminer la cause d’un état de pare-feu défectueux.

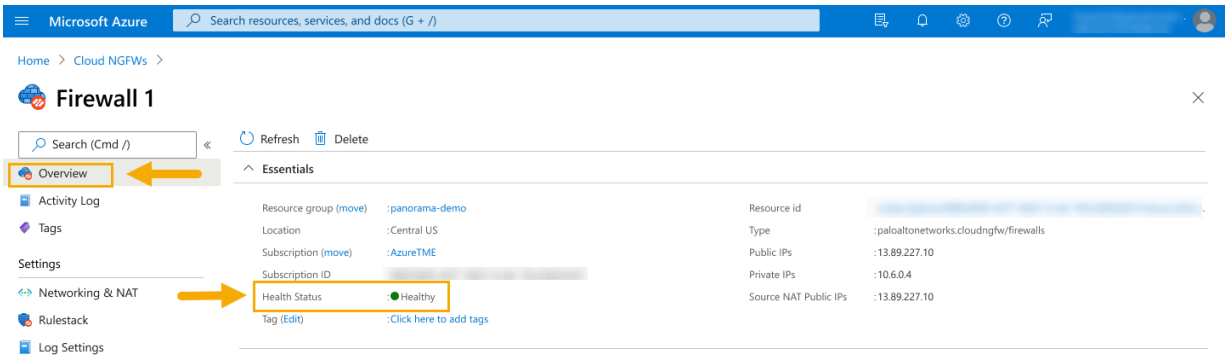
Pour surveiller l’état de santé de votre Cloud NGFW :

STEP 1 | Connectez-vous au portail Azure et recherchez **Cloud NGFW by Palo Alto Networks (Cloud NGFW par Palo Alto Networks)**. Les instances Cloud NGFW que vous avez enregistrées auprès d’Azure s’affichent.

STEP 2 | Sélectionnez le Cloud NGFW que vous souhaitez surveiller.



STEP 3 | Sur la page **Overview (Aperçu)**, développez **Essentials (Informations de base)**. La section Essentials (Informations de base) affiche l'état de santé du Cloud NGFW sélectionné.



États du moniteur de santé

L'état de santé apparaît sous forme d'icônes à code couleur. Il est représenté à la fois pour *la sécurité réseau* et la *sécurité cloud*.

État de santé pour *la sécurité réseau* :

- **Sain** (icône verte). Indique que les appareils virtuels Panorama principal et secondaire sont connectés à la ressource Cloud NGFW pour les applications de sécurité réseau.
- **Dégradé** (icône jaune). La sécurité réseau est dégradée sur la ressource Cloud NGFW.
- **Défectueux** (icône rouge). Indique que le Cloud NGFW ne peut pas se connecter à l'appareil virtuel Panorama. Assurez-vous que votre Cloud NGFW est enregistré auprès de Panorama.

L'état de santé de la *sécurité cloud* s'applique à la création et à la mise à jour d'un pare-feu :

- **Sain** (icône verte). Indique l'état individuel de la rulestack associée à la ressource Cloud NGFW, affichant l'état des appareils virtuels Panorama principal et secondaire connectés à la ressource Cloud NGFW. Ces informations apparaissent dans la section **Associate rulestack (Rulestack associée)** et sont affichées comme **Connected (Connecté)** ou **Not Connected (Non connecté)**.
- **Dégradé** (icône jaune). La sécurité cloud est dégradée.
- **Défectueux** (icône rouge). Indique que la rulestack Cloud NGFW n'a été correctement validée sur aucune instance. Une fois le problème résolu, le moniteur de santé change pour refléter un état sain (icône verte).

- **Initialisation** (icône bleue). Indique que la ressource Cloud NGFW est en cours d’initialisation.

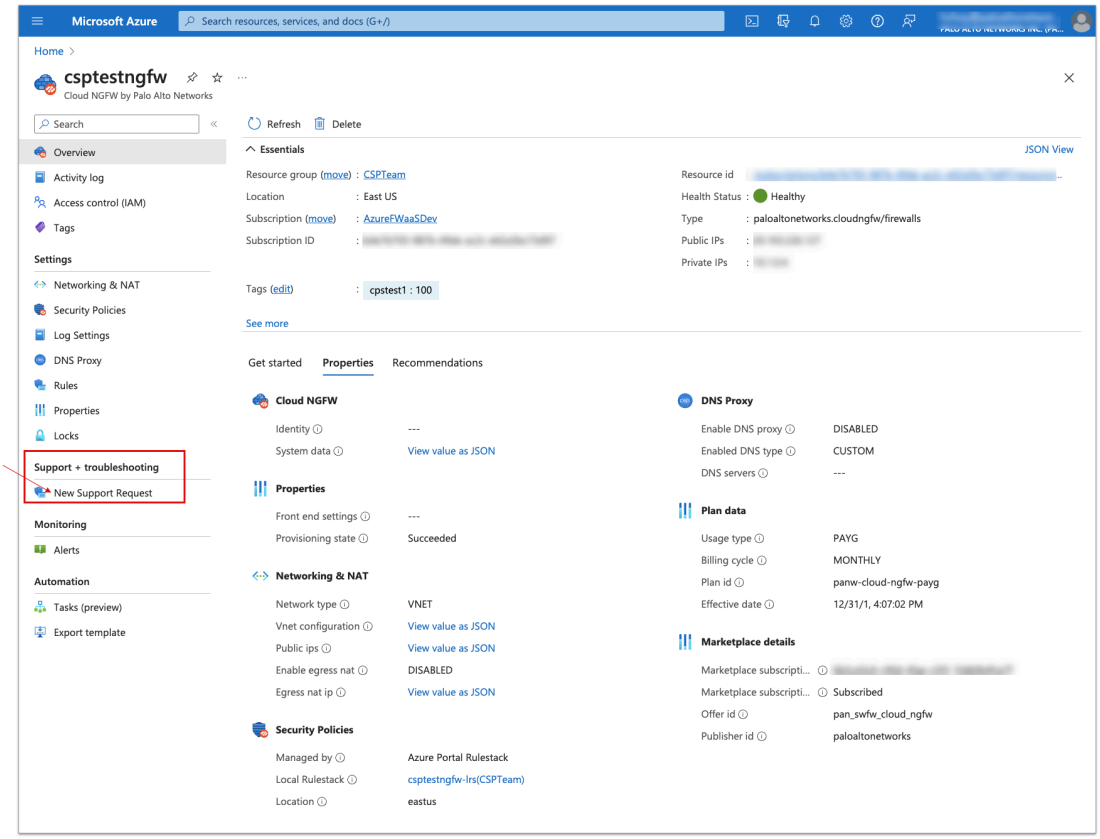
Créer un dossier d’assistance

Pour créer un dossier d’assistance à l’aide du portail Azure :

STEP 1 | Connectez-vous au portail Azure.

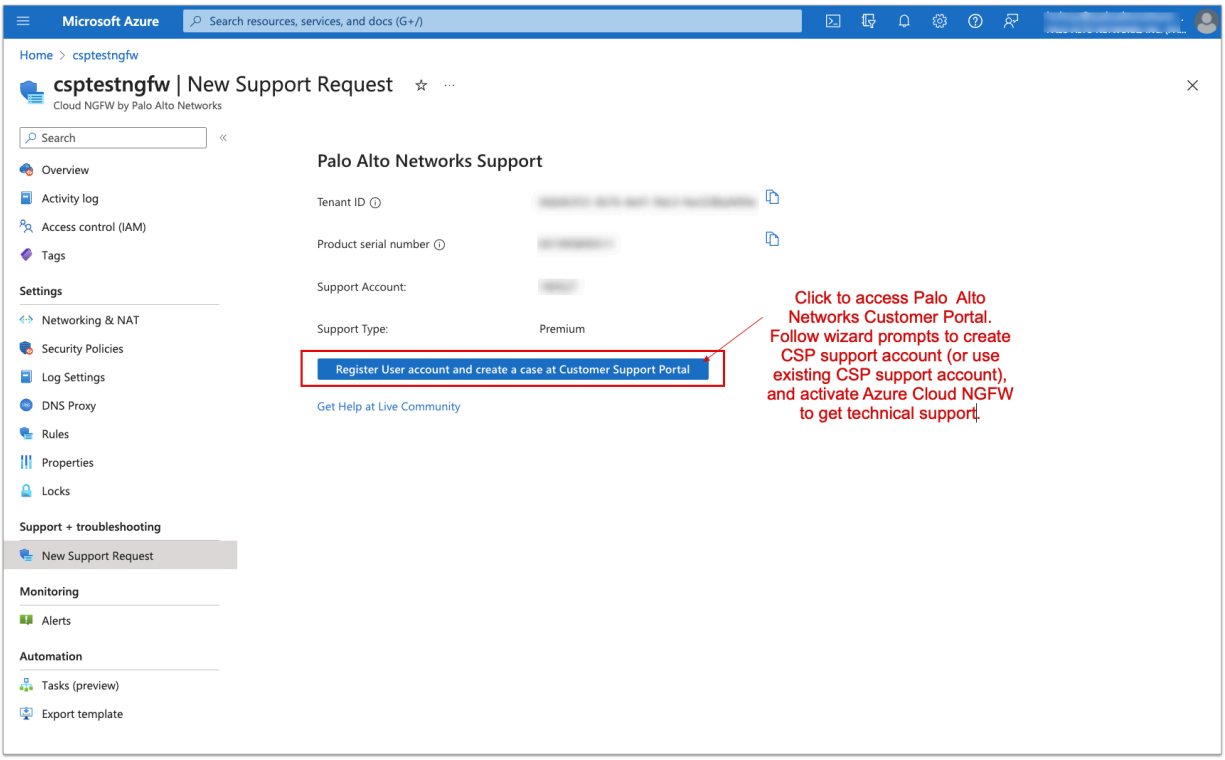
STEP 2 | Dans la section **Support + Troubleshooting (Assistance + Dépannage)**, cliquez sur **New Support Request (Nouvelle demande d’assistance)**.

1.



STEP 3 | Sur la page **New Support Request (Nouvelle demande d’assistance)**, cliquez sur **Register User account and create a case at Customer Support Portal (Enregistrer un compte utilisateur et créer un dossier sur le portail de support client)**.

2.



STEP 4 | Suivez les invites pour créer un compte sur le portail de support client (CSP) de Palo Alto Networks. Si vous possédez déjà un compte CSP, utilisez vos informations d'identification de connexion existantes.

Déployer Cloud NGFW pour Azure

Les informations contenues dans cette section servent de référence pour le déploiement de Cloud NGFW à l'aide du portail Azure. Vous pouvez utiliser le portail Azure pour déployer le Cloud NGFW sur plusieurs comptes Azure. Le portail Azure utilise la console Cloud NGFW pour créer des rulestacks locales.

Deux méthodes de déploiement sont prises en charge : les VNet Azure et les vWAN Azure. Un vNET Azure permet une communication sécurisée avec les autres ressources Azure, Internet et les réseaux sur site. Un vWAN Azure représente un service de mise en réseau qui combine les fonctionnalités de réseau, de sécurité et de routage pour fournir une interface opérationnelle unique. Le déploiement dans votre environnement Azure exige la console Cloud NGFW et le portail Azure.

Le débit pour un vNET ou vWAN est limité à 100 Gbit/s.

- Déployer le Cloud NGFW dans un vNET
- Déployer le Cloud NGFW dans un vWAN

Déployer le Cloud NGFW dans un vNET

Le Cloud NGFW se manifeste sous la forme de deux adresses IP privées (publique et privée) dans votre vNET. À l'aide d'itinéraires définis par l'utilisateur (avec l'adresse IP privée du Cloud NGFW comme saut suivant), vous pouvez rediriger le trafic vers le Cloud NGFW pour l'inspection des paquets et la prévention des menaces.

Le Cloud NGFW pour Azure communique avec le Cloud NGFW pour ajouter des rulestacks. Le Cloud NGFW mesure en permanence l'utilisation de la ressource Cloud NGFW, envoyant des enregistrements d'utilisation pour chaque abonnement Azure au service de mesure Azure. Ce service est responsable de la facturation.

*Après avoir déployé le Cloud NGFW dans un réseau virtuel, consultez la page d'*exemple de configuration *pour plus d'informations.*

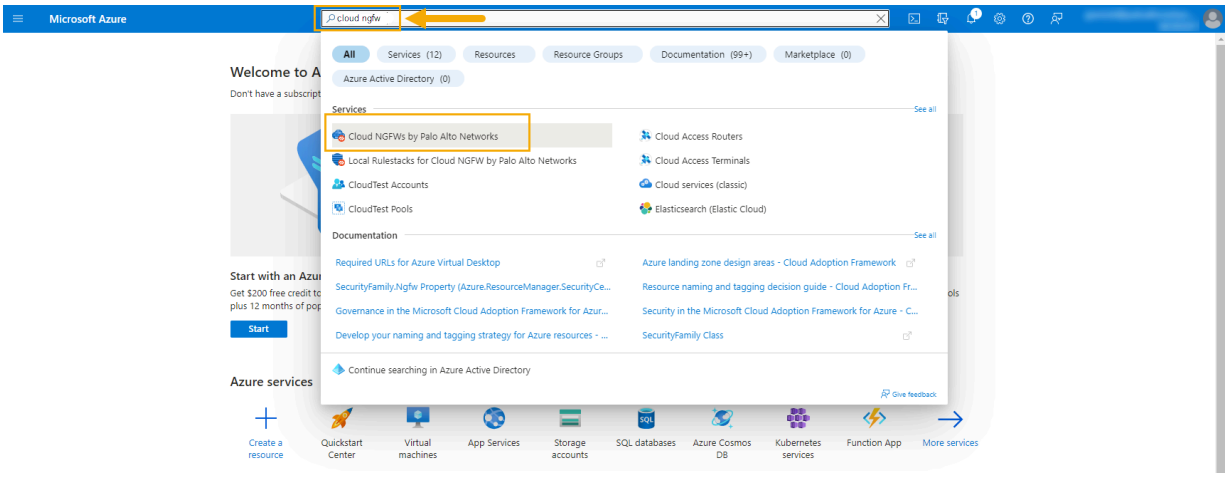
Prérequis

Pour déployer Cloud NGFW dans un réseau virtuel, vous aurez besoin d'un abonnement Azure. Cet abonnement doit avoir un rôle propriétaire ou contributeur.

Lors du déploiement du Cloud NGFW dans un vNET à l'aide d'un hub vNET existant, la taille minimale doit être /25. Vous devez disposer de deux sous-réseaux avec une taille minimale de /26 ; ces sous-réseaux doivent être délégués au service ***PaloAltoNetworks.Cloudngfw/firewalls****.*

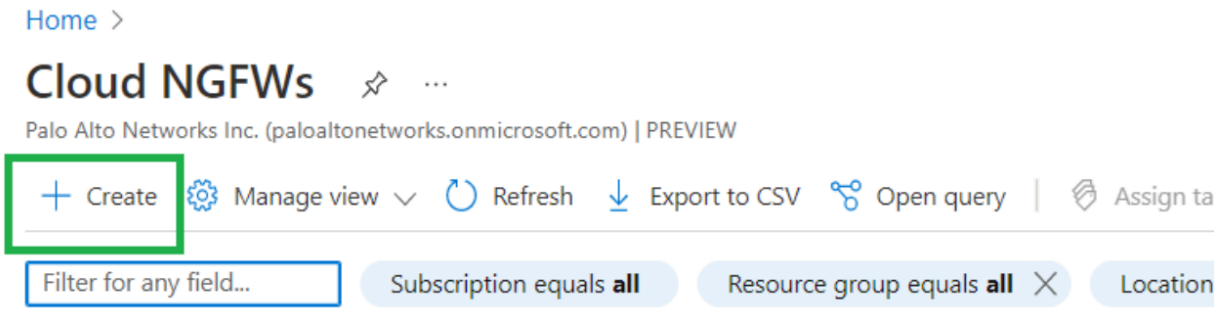
Pour les déploiements prenant en charge 100 Gbit/s, vous avez besoin de 80 adresses IP gratuites au total, soit 40 pour le réseau public et 40 pour le réseau privé.

STEP 1 | Connectez-vous au portail Azure et recherchez **Cloud NGFW**. La recherche affiche le service Cloud NGFW, **Cloud NGFW de Palo Alto Networks**.



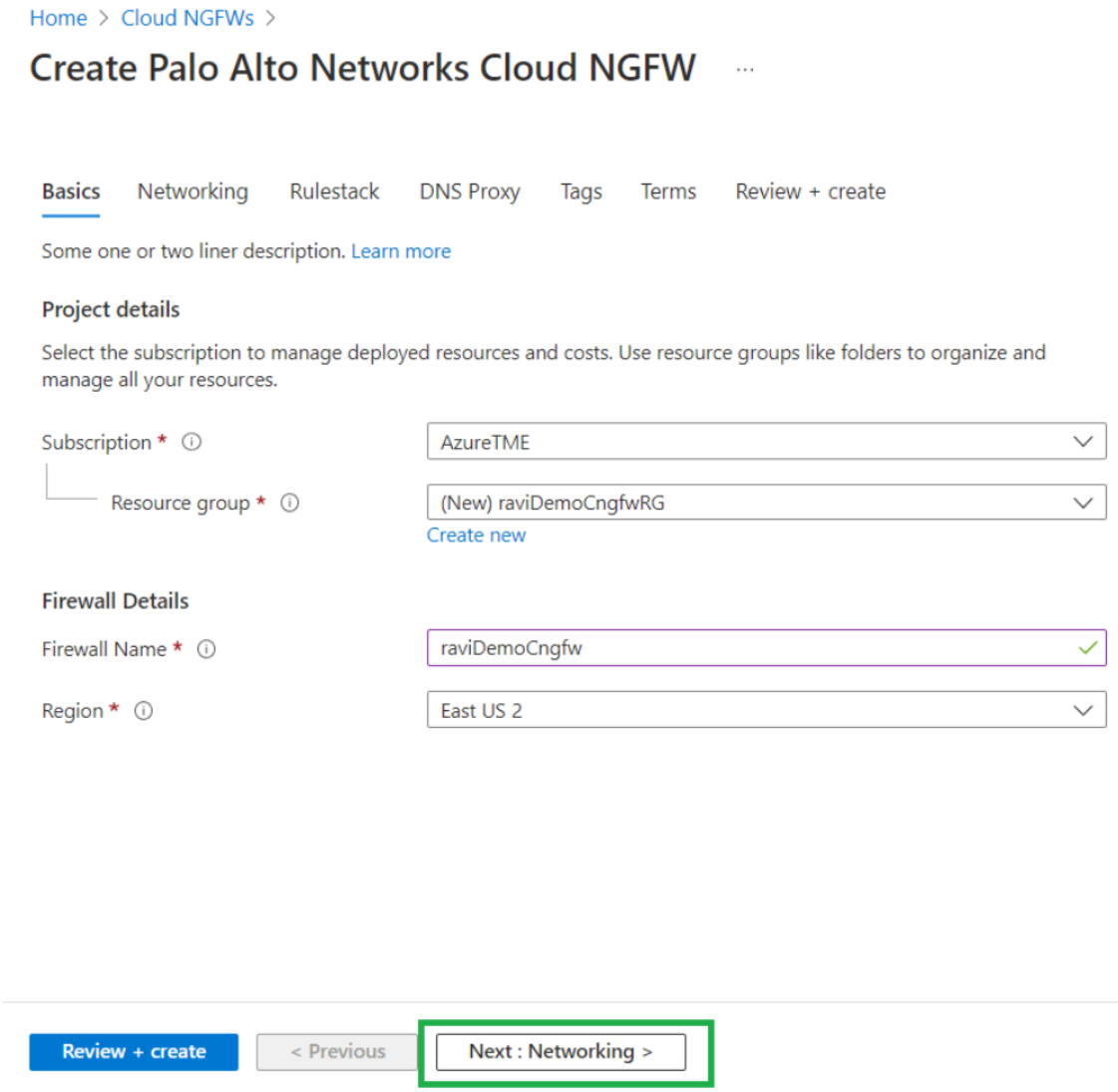
STEP 2 | Cliquez sur **Cloud NGFW** pour commencer à créer le service Palo Alto Networks Cloud NGFW pour Azure.

STEP 3 | Sur la page de renvoi de la ressource Cloud NGFW, cliquez sur **Create (Créer)** pour commencer à créer la ressource Cloud NGFW.



Si votre abonnement a déjà été créé, la page de renvoi contient des informations sur les ressources Cloud NGFW.

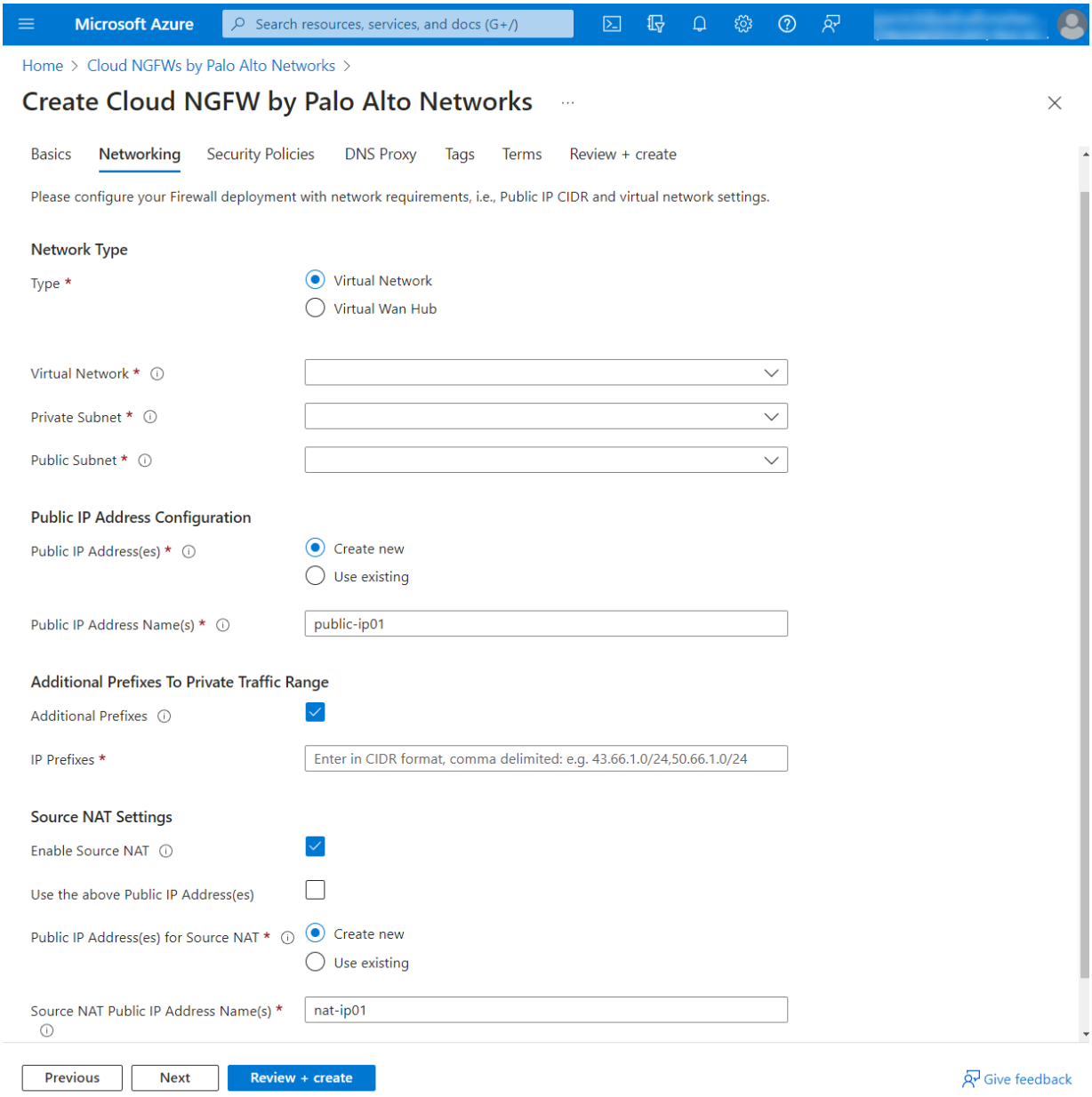
STEP 4 | Après avoir cliqué sur **Create (Créer)**, l'écran **Create Palo Alto Networks Cloud NGFW (Créer Palo Alto Networks Cloud NGFW)** apparaît.



Utilisez les informations du tableau suivant pour fournir des informations **de base** , puis cliquez sur **Next:Networking (Suivant : Réseau)** :

Champ	Description
Abonnement	Sélectionné automatiquement en fonction de l'abonnement utilisé lors de la connexion.
Groupe de ressources	Utilisez l'un des groupes de ressources existants ou créez-en un nouveau (à l'aide de l'option **Create New (Créer un nouveau)**) dans lequel la ressource Cloud NGFW est créée.
Nom du pare-feu	Nom de la ressource du pare-feu Cloud NGFW.  *Pour les pare-feu gérés par Panorama, n'utilisez pas uniquement des lettres majuscules pour le nom du pare-feu.*
Région	Région dans laquelle Cloud NGFW est provisionné.

STEP 5 | Fournissez des informations sur le déploiement du pare-feu dans l’écran **Networking (Réseau)** :



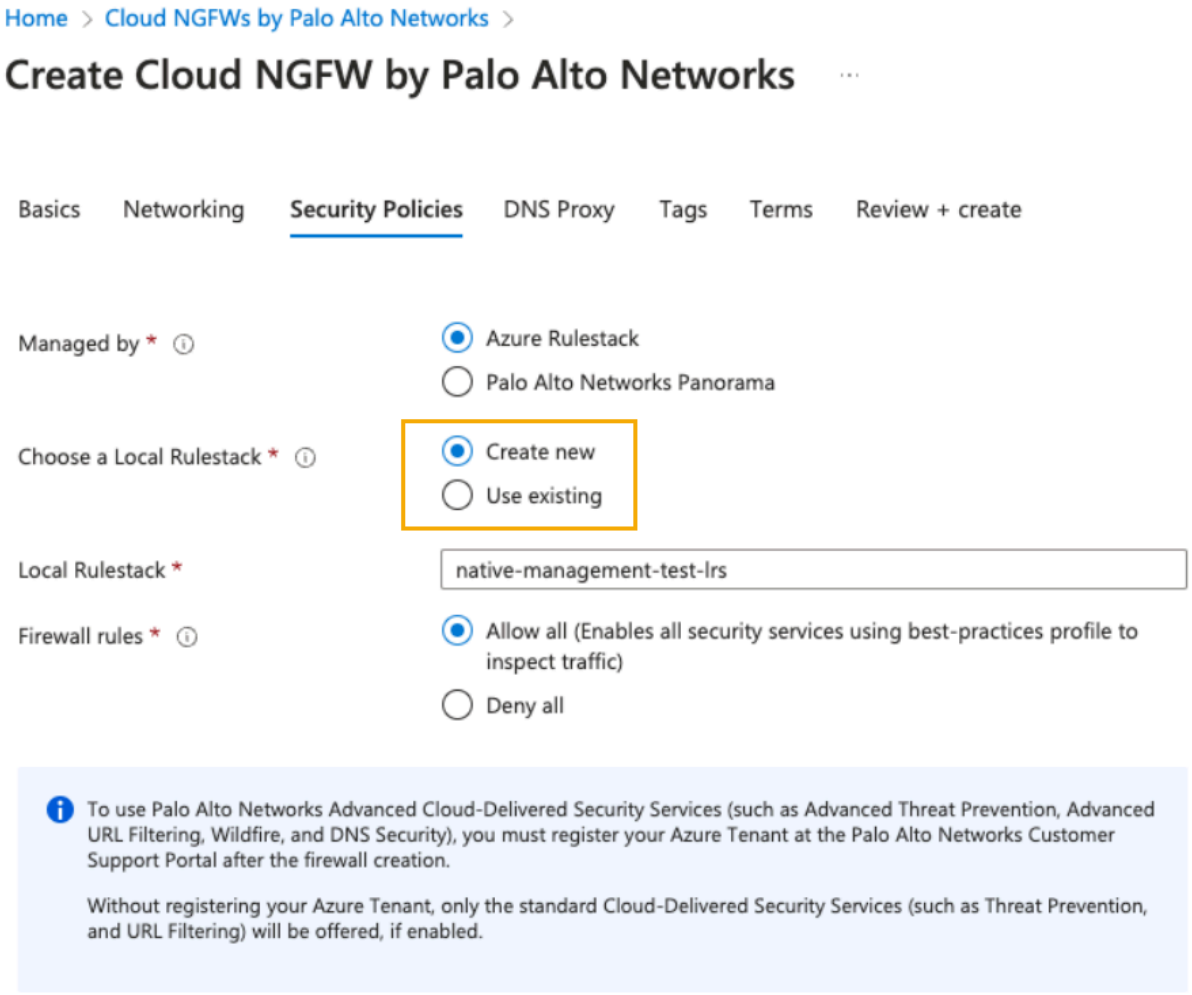
L’écran **Networking (Réseau)** comprend les champs du tableau suivant :

Champ	Description
Type	Sélectionné automatiquement en fonction de l’abonnement utilisé lors de la connexion.
Réseau virtuel	Choisissez **Virtual network (Réseau virtuel)**. Créez un réseau virtuel ou sélectionnez un réseau virtuel existant.
Sous-réseau privé	Choisissez un sous-réseau privé.
Sous-réseau public	Choisissez un sous-réseau public.
Configuration de l’adresse IP publique	Spécifiez les **adresses IP publiques**. Cliquez sur **Create new (Créer)** pour établir une nouvelle adresse ou cliquez sur **Use existing (Utiliser existante)** pour spécifier une adresse existante.
Préfixes supplémentaires à la plage de trafic privé	Si vous souhaitez prendre en charge des plages d’adresses IP privées supplémentaires en plus de celles spécifiées dans RFC 1918, utilisez l’option **Additional Prefixes to Private Traffic Range (Préfixes supplémentaires à la plage de trafic privé)**. Avec cette prise en charge, vous pouvez utiliser des blocs d’adresses IP publiques dans votre réseau privé sans acheminer le trafic vers Internet. Cochez la case **Additional Prefixes (Préfixes supplémentaires)**. Saisissez les adresses au format CIDR (par exemple, 40.0.0.0/24). Utilisez une liste délimitée par des virgules pour inclure plusieurs adresses. *Par défaut, les préfixes RFC 1918 sont automatiquement inclus dans la plage de trafic privé. Si votre organisation utilise des plages d’adresses IP publiques, spécifiez explicitement ces préfixes IP. Vous pouvez spécifier ces préfixes IP publics individuellement ou sous forme d’agrégats.* *Consultez la section Modifier un pare-feu existant pour ajouter des adresses privées supplémentaires pour la prise en charge non-RFC 1918 pour ajouter des préfixes supplémentaires après le déploiement du pare-feu.*
Paramètres NAT source	Incluez l’option **Source NAT (NAT source)** si la traduction d’adresses réseau (NAT) est utilisée sur le trafic sortant vers Internet.

STEP 6 | Cliquez **sur Next:Security Policies (Suivant : Politiques de sécurité)**.

STEP 7 | Sur la page **Security Policies (Politiques de sécurité)**, créez une rulestack locale ou sélectionnez une rulestack existante. Une rulestack nouvellement créée ne contient aucune règle. Vous pouvez définir des règles de sécurité après le déploiement de la ressource Cloud NGFW.

En tant qu'administrateur, vous pouvez soit gérer une politique de sécurité à l'aide d'une rulestack Azure native, soit utiliser Palo Alto Networks Panorama pour la gestion des politiques. Pour plus d'informations, reportez-vous à la section Lier le Cloud NGFW à Palo Alto Networks Management.

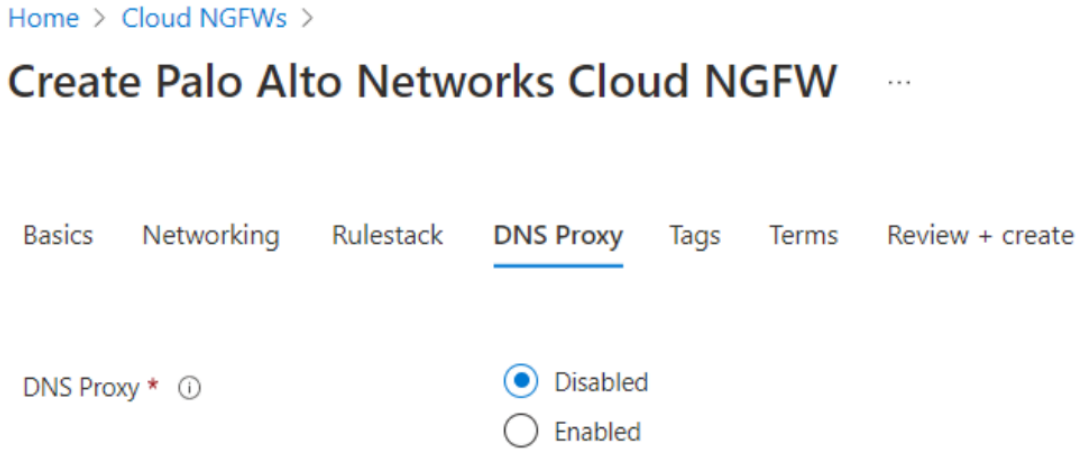


Si vous souhaitez utiliser les services de sécurité avancés de Palo Alto Networks (notamment Advanced Threat Prevention et Advanced URL Filtering), vous devez enregistrer votre locataire Azure sur le portail de support client de Palo Alto Networks *après avoir créé votre pare-feu. Pour en savoir plus sur l'enregistrement d'un locataire, reportez-vous à la section* Démarrer avec Cloud NGFW pour Azure.

1.

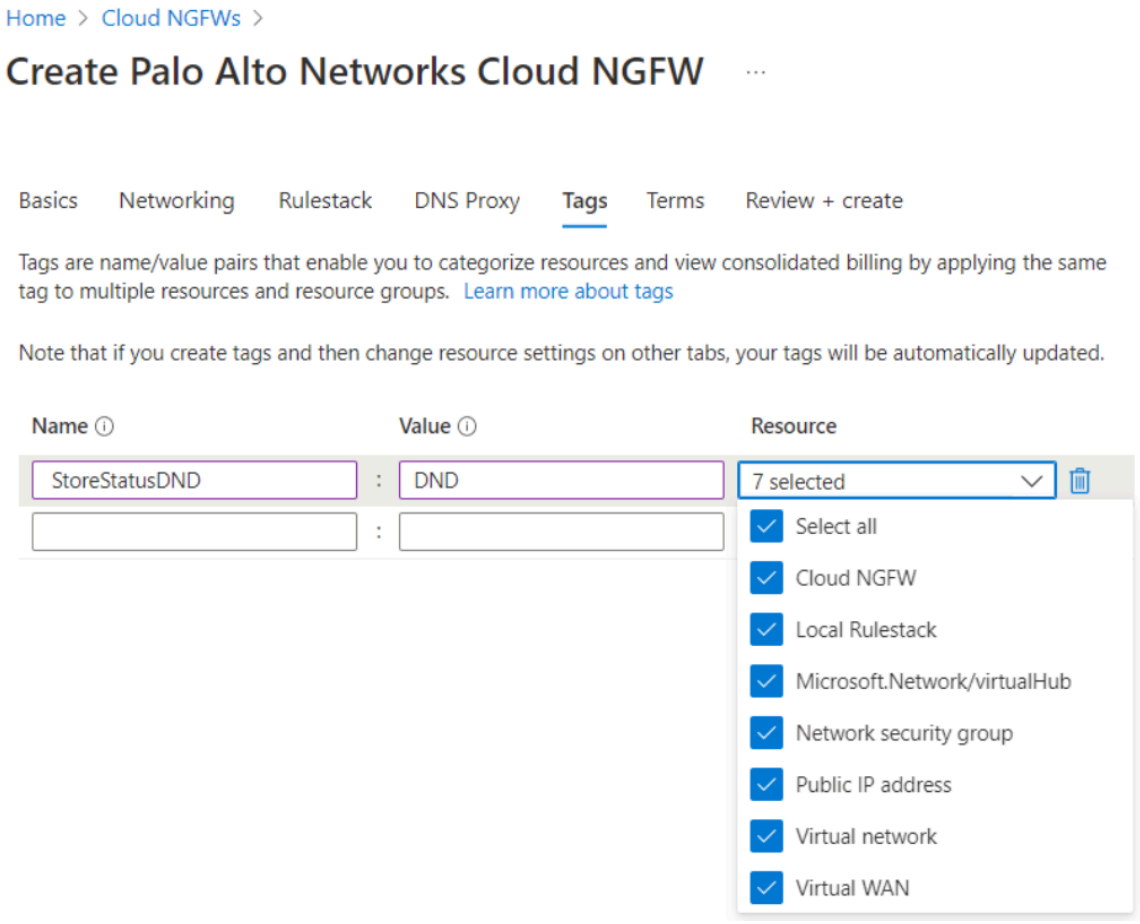
STEP 8 | Cliquez sur **Next: DNS Proxy (Suivant : Proxy DNS)** pour configurer la ressource Cloud NGFW en tant que proxy DNS. Vous pouvez configurer le Cloud NGFW pour inspecter tout le trafic DNS en agissant en tant que proxy pour les ressources vNET. Une fois configuré, le proxy DNS transfère la

requête DNS au serveur DNS Azure par défaut ou à un serveur DNS que vous spécifiez. Par défaut, DNS Proxy (Proxy DNS) est désactivé.



STEP 9 | Cliquez sur **Next:Tags (Suivant : Étiquettes)** pour spécifier les étiquettes correspondant à vos exigences Azure. Les étiquettes sont des libellés prédéfinis qui peuvent vous aider à gérer les vulnérabilités de votre environnement et à afficher la facturation consolidée liée à votre

compte Azure. Elles sont déterminées de manière centralisée et peuvent être définies en tant que vulnérabilités et exceptions à la politique.



Les étiquettes sont utilisées comme :

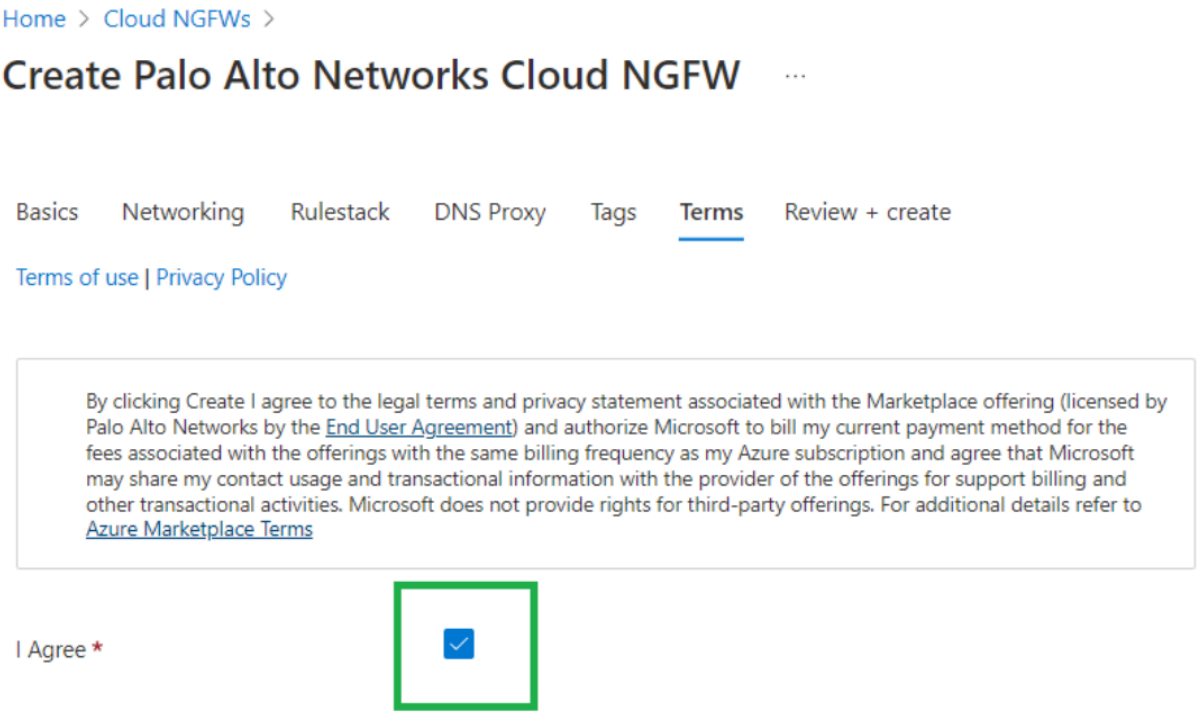
- Libellés de vulnérabilité Elles constituent un moyen pratique de catégoriser les vulnérabilités de votre environnement.
- Exceptions à la politique Elles peuvent faire partie de vos règles afin d'avoir un effet spécifique sur les vulnérabilités étiquetées.
- Affichez la facturation consolidée pour votre compte Azure.

  Les étiquettes sont utiles en cas de grands déploiements de conteneurs avec plusieurs équipes travaillant dans le même environnement. Vous pouvez par exemple avoir plusieurs équipes qui gèrent des types de vulnérabilités différents. Vous pouvez ensuite définir les étiquettes pour définir les responsabilités sur les vulnérabilités. D'autres utilisations seraient de définir l'état de correction de la vulnérabilité, ou de marquer les vulnérabilités à ignorer lorsqu'il s'agit d'un problème connu qui ne peut pas être résolu dans un avenir proche.

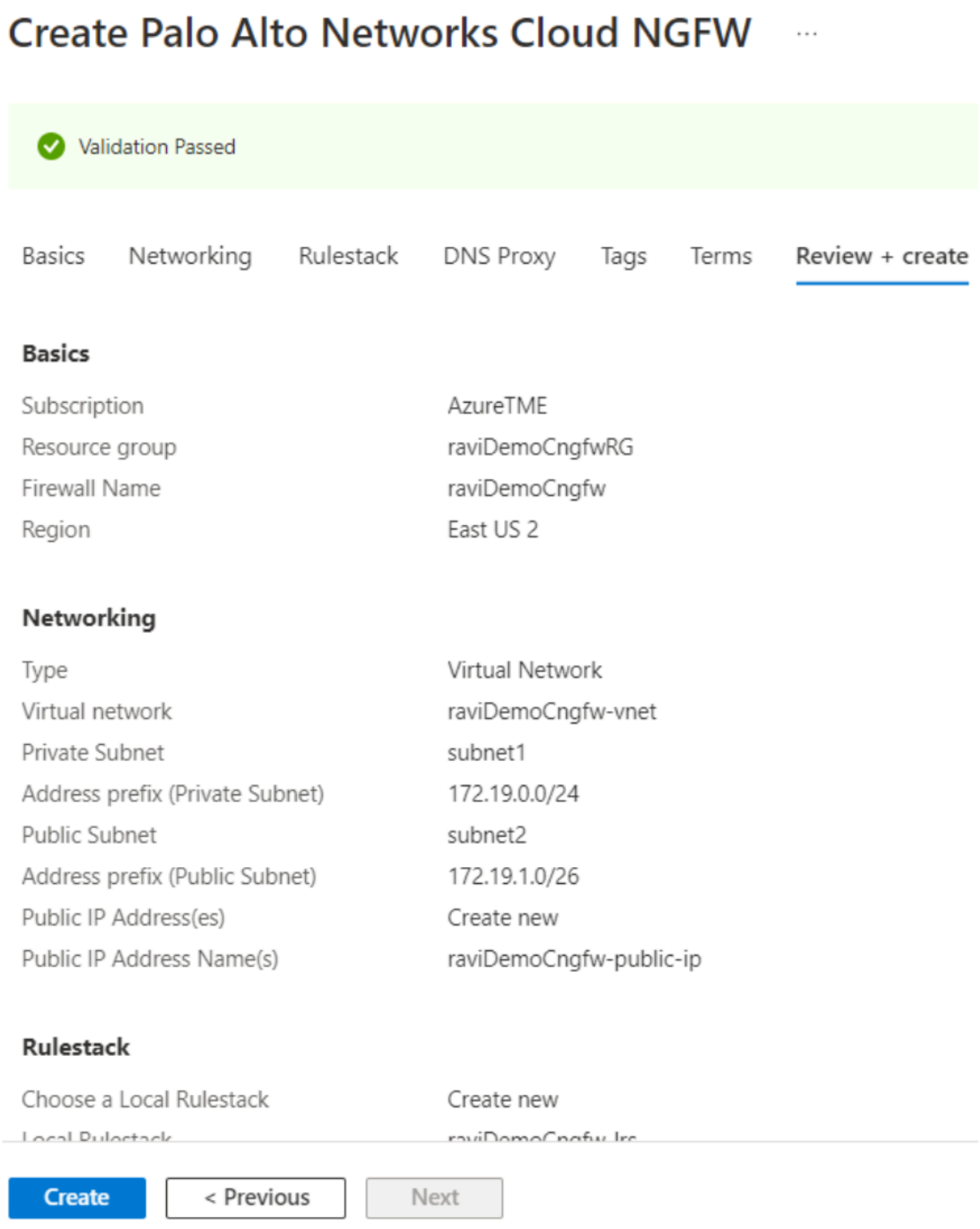
  Vous pouvez définir autant d'étiquettes que vous le souhaitez. Pour plus d'informations sur la création d'étiquettes pour votre compte Azure, reportez-vous à la section Utiliser les étiquettes pour organiser vos ressources Azure et votre hiérarchie de gestion.

STEP 10 | Cliquez sur **Next:Terms (Suivant : Conditions)** et acceptez les conditions générales de déploiement.



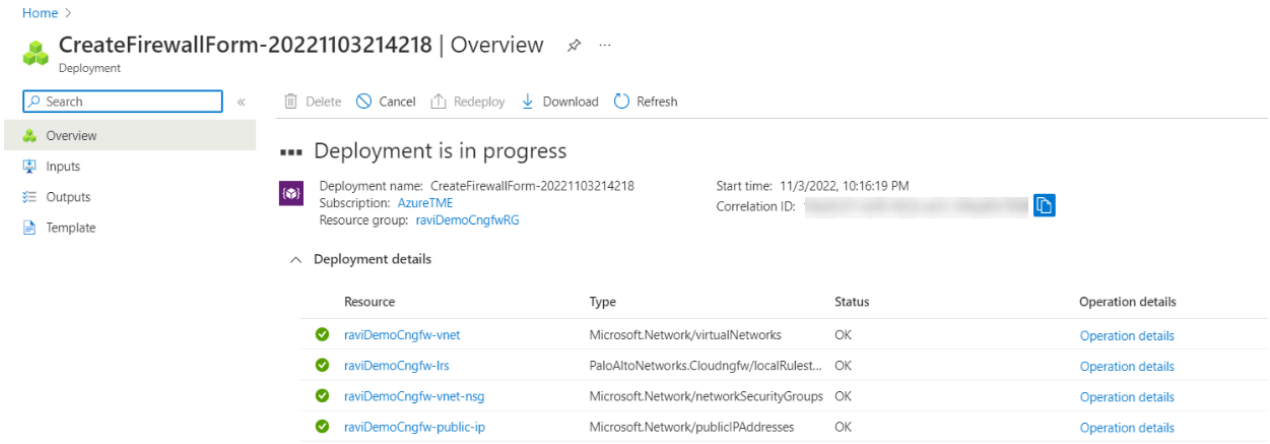
STEP 11 | Cliquez sur **Next:Review + create (Suivant : Revoir + créer)** pour revoir et valider votre abonnement Azure pour la ressource Cloud NGFW. La ressource est d'abord validée, puis créée.

L’écran affiche **Validation Passed (Validation réussie)**. Cliquez sur **Create (Créer)** pour déployer le service Cloud NGFW :



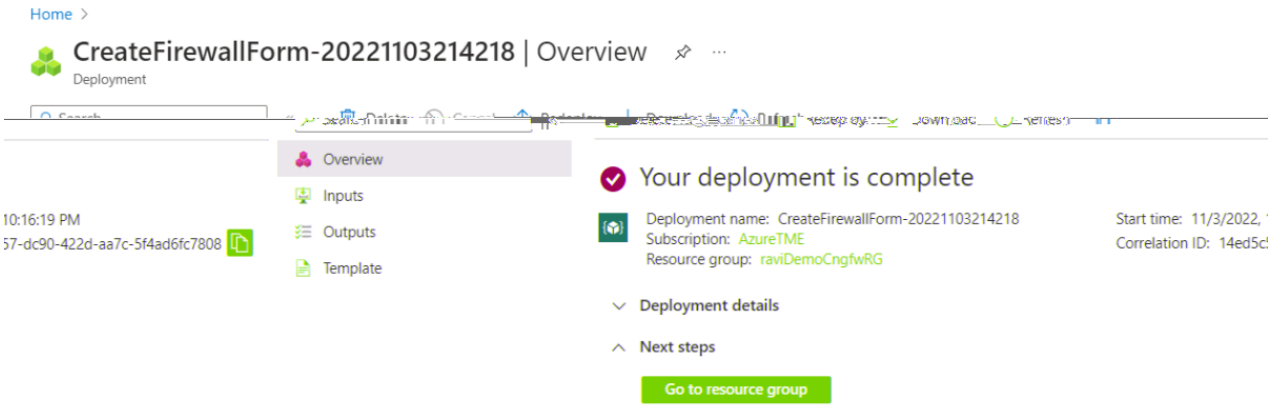
Vérifier le déploiement du Cloud NGFW dans le vNET

Après avoir créé le service Cloud NGFW, la progression du déploiement apparaît.

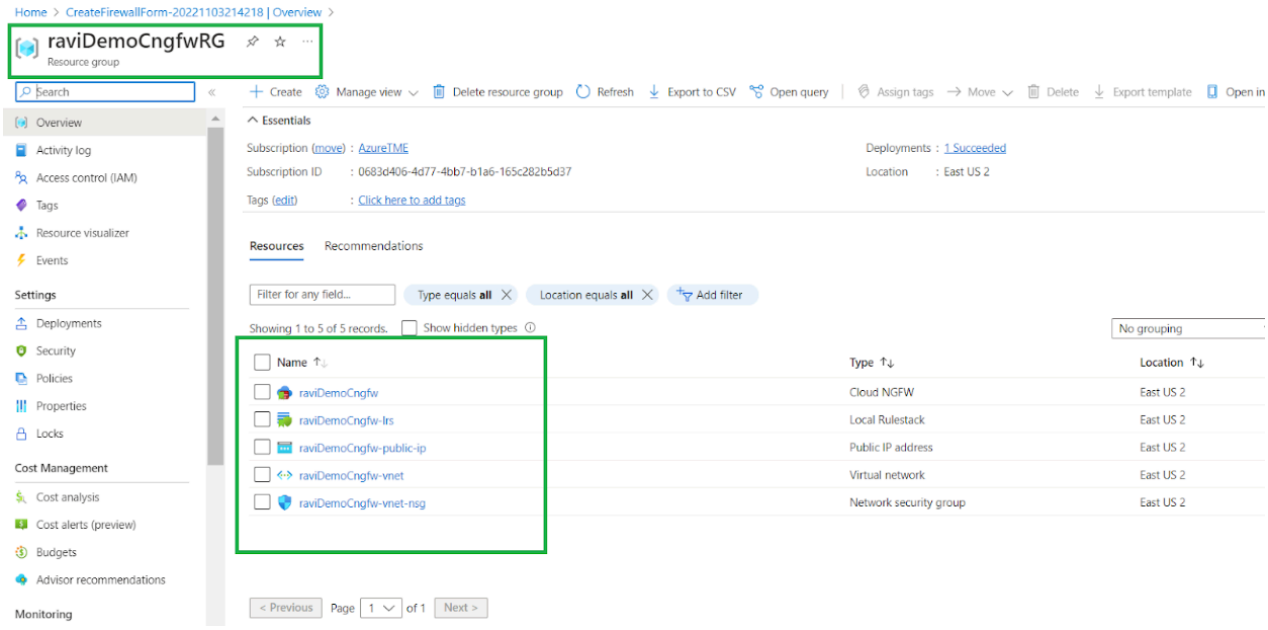


Le déploiement d'une ressource Cloud NGFW prend environ 30 minutes.

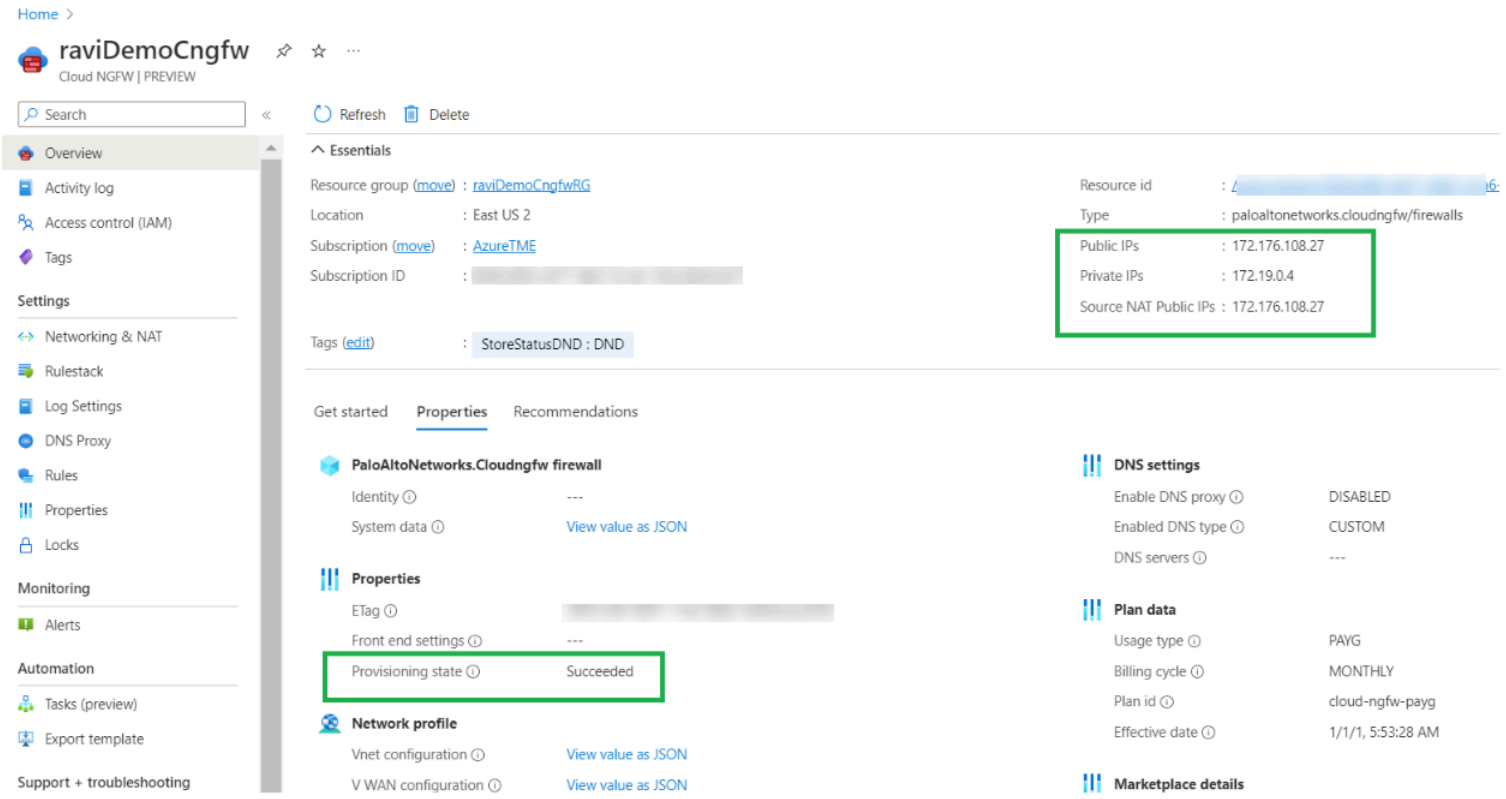
En cas de déploiement réussi, l'écran suivant apparaît. Cliquez sur **Go to resource group (Aller au groupe de ressources)** pour vérifier les ressources créées pour ce déploiement :



Cinq ressources sont créées : le Cloud NGFW, la rulestack locale, l’adresse IP publique, le réseau virtuel et le groupe de sécurité :



Une fois la ressource Cloud NGFW créée, sélectionnez-la pour vérifier que l'état de provisionnement indique **Succeeded (Réussi)**. Cet écran affiche également les adresses IP publiques et privées associées au service Cloud NGFW.



*Après avoir déployé Cloud NGFW dans un vNET, consultez l'*exemple de configuration *pour plus d'informations.*

Modifier un pare-feu existant pour ajouter des adresses privées supplémentaires pour la prise en charge non-RFC 1918

Pour modifier un pare-feu existant afin d'ajouter des adresses privées supplémentaires :

STEP 1 | Recherchez le Cloud NGFW dans le portail Azure.

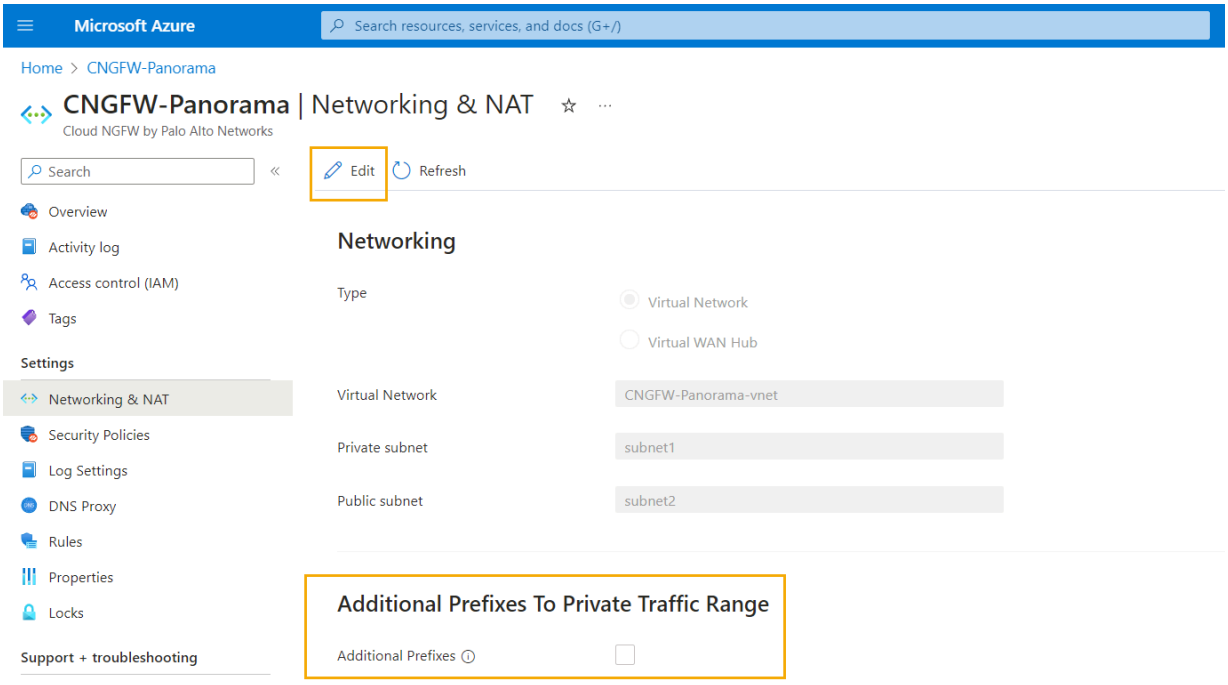
STEP 2 | Dans la section **Settings (Paramètres)**, sélectionnez **Networking & NAT (Réseau et NAT)**.

STEP 3 | Cliquez sur **Edit (Modifier)**.

STEP 4 | Dans la section **Additional Prefixes to Private Traffic Range (Préfixes supplémentaires à la plage de trafic privé)**, cochez la case **Additional Prefixes (Préfixes supplémentaires)**.

STEP 5 | Saisissez les adresses au format CIDR (par exemple, 40.0.0.0/24). Utilisez une liste délimitée par des virgules pour inclure plusieurs adresses.

STEP 6 | Cliquez sur **Save (Enregistrer)**.



Modifier un pare-feu existant pour activer la NAT source privée

Utilisez l'option **Private Source NAT (NAT source privée)** si vous souhaitez traduire l'adresse réseau source sur les requêtes provenant d'une instance dans un sous-réseau ne pouvant pas être acheminé. Cette

option vous permet d'envoyer du trafic vers une adresse IP pouvant être acheminée attribuée à l'équilibreur de charge d'application (ALB). Après avoir activé l'option Private Source NAT (NAT source privée), incluez l'adresse IP de destination.

Le trafic est-ouest de Cloud NGFW s'appuie sur les itinéraires définis par l'utilisateur (UDR) pour transférer le trafic vers le pare-feu. Cette dépendance est prise en charge par le trafic est-ouest type lorsque les deux extrémités du réseau font partie du réseau privé. Cependant, cela soulève la question d'un nouveau type de trafic ; un côté du déploiement est le réseau privé, tandis que l'autre côté du déploiement prend en charge un partenaire ou un service PaaS accessible via un terminal privé dans le réseau virtuel. Dans de tels environnements, vous n'avez pas nécessairement accès à la gestion de l'ensemble de l'autre réseau pour configurer l'UDR. Le trafic est dirigé vers le Cloud NGFW par UDR, mais le trafic de retour est envoyé à l'adresse IP source du client sans transiter par le Cloud NGFW. Par conséquent, un problème d'itinéraire asymétrique se pose et le pare-feu ne peut pas établir la liaison TCP qui en résulte. Cloud NGFW utilise ***Private Source NAT (NAT source privée)*** *pour traduire l'adresse IP source en adresse IP de l'interface privée de l'instance du pare-feu, garantissant ainsi que le Cloud NGFW traite le trafic de retour vers l'interface appropriée.*

STEP 1 | Recherchez le Cloud NGFW dans le portail Azure.

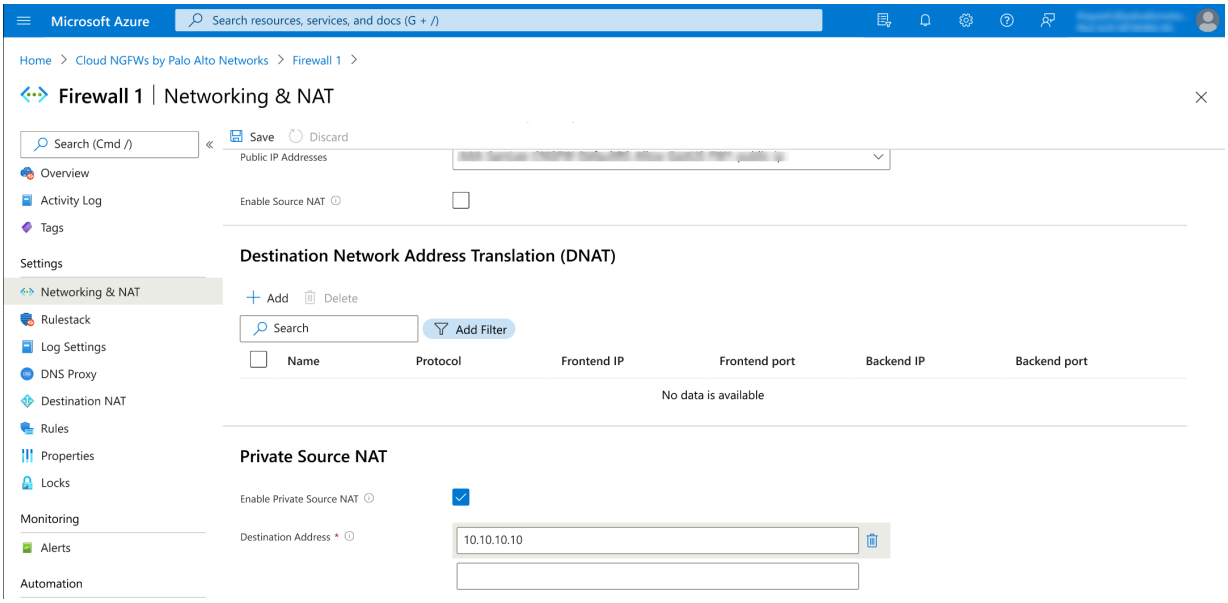
STEP 2 | Dans la section **Settings (Paramètres)**, sélectionnez **Networking & NAT (Réseau et NAT)**.

STEP 3 | Cliquez sur **Edit (Modifier)**.

STEP 4 | Dans la section **Private Source NAT (NAT source privée)**, cochez la case **Enable Private Source NAT (Activer la NAT source privée)**.

STEP 5 | Saisissez l'adresse de destination.

STEP 6 | Cliquez sur **Save (Enregistrer)**.



Exemple de configuration pour le déploiement après le vNET

Après avoir déployé le Cloud NGFW dans un vNET Azure, vous pouvez commencer à configurer le service Cloud NGFW. Les informations fournies dans cette section illustrent les tâches courantes permettant d'exécuter le Cloud NGFW dans votre environnement Azure :

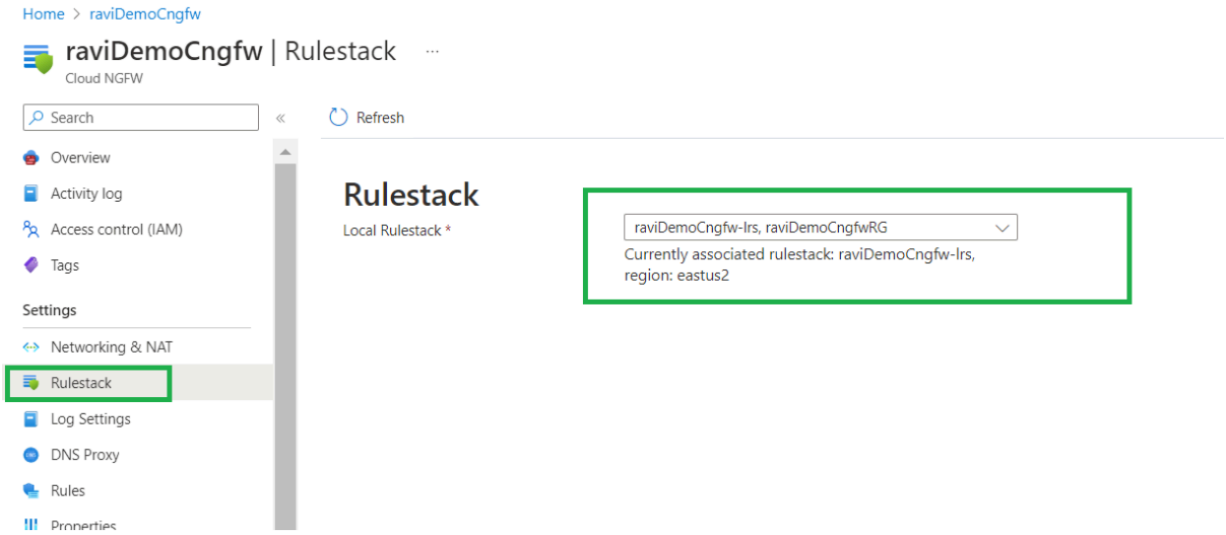
- Créer ou mettre à jour une rulestack
- Ajouter une liste FQDN
- Ajouter une règle
- Configurer une règle NAT source et de destination
- Configurer la journalisation
- Mettre à jour le groupe de sécurité réseau
- Configurer l'appairage vNET
- Ajouter une table de routage

Créer ou mettre à jour une rulestack

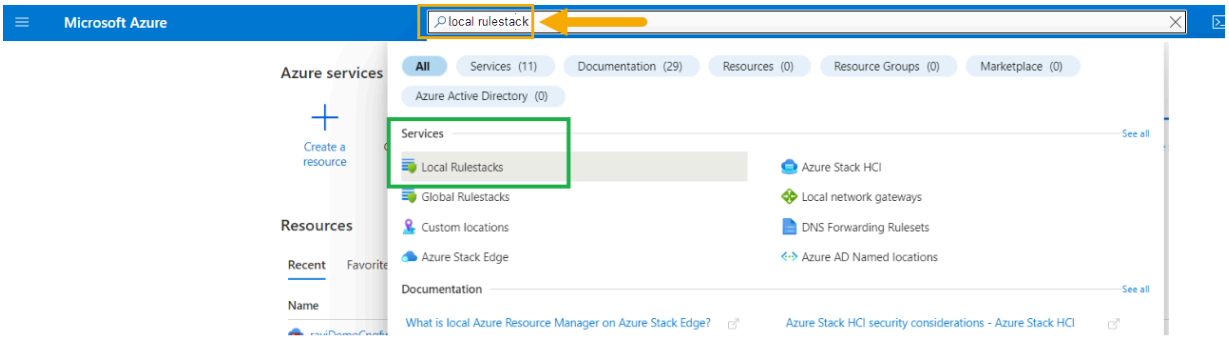
Dans cette section, vous allez mettre à jour une rulestack locale en ajoutant une règle et en activant la journalisation.

Pour mettre à jour une rulestack existante :

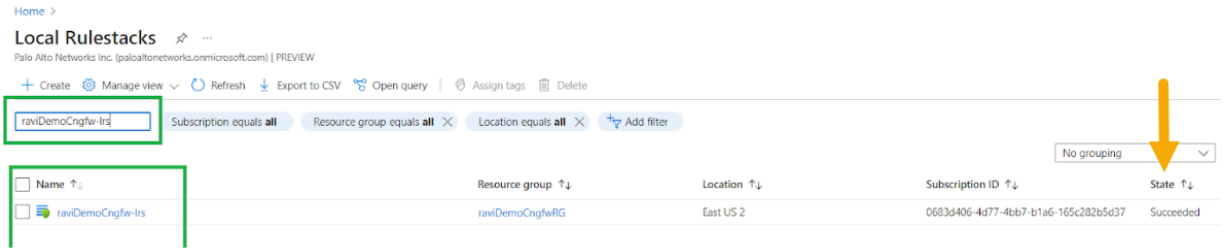
STEP 1 | Dans la console Azure Resource Manager (ARM), cliquez sur **Rulestacks** pour la ressource Cloud NGFW que vous souhaitez configurer. La rulestack associée au service Cloud NGFW apparaît, ainsi que le groupe de ressources.



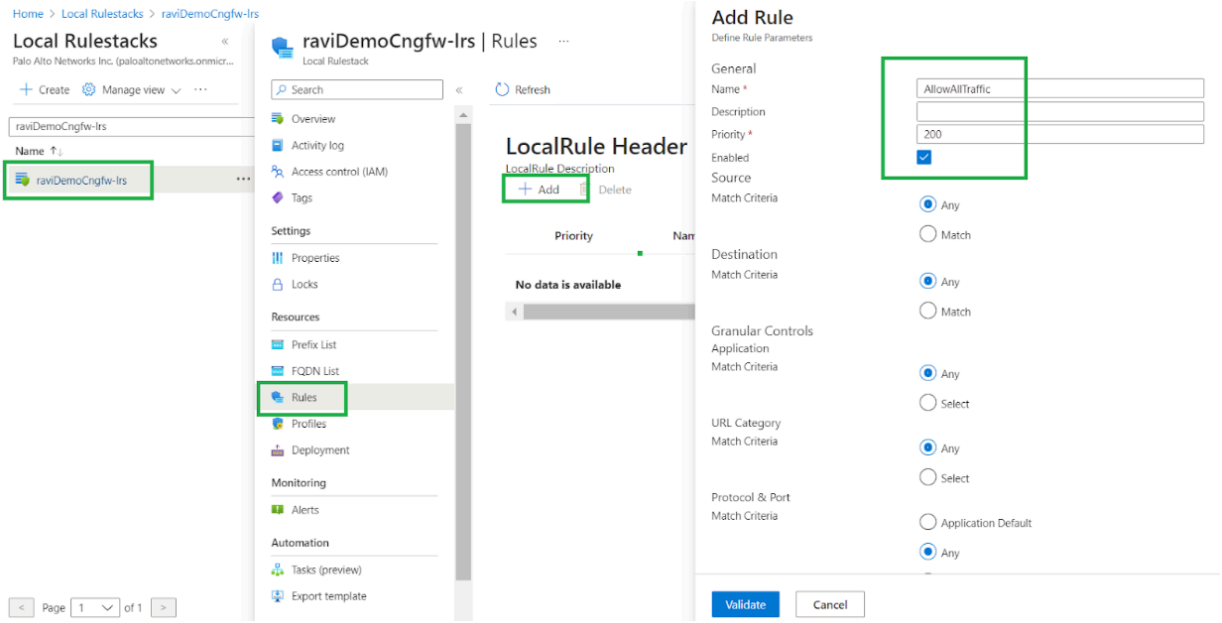
STEP 2 | Modifiez la rulestack pour ajouter des règles de pare-feu. Ces règles autorisent un certain trafic tout en bloquant un trafic spécifique. Par défaut, Cloud NGFW bloque tout le trafic. Recherchez la rulestack locale à l'aide de l'option de recherche globale fournie par le portail Azure.



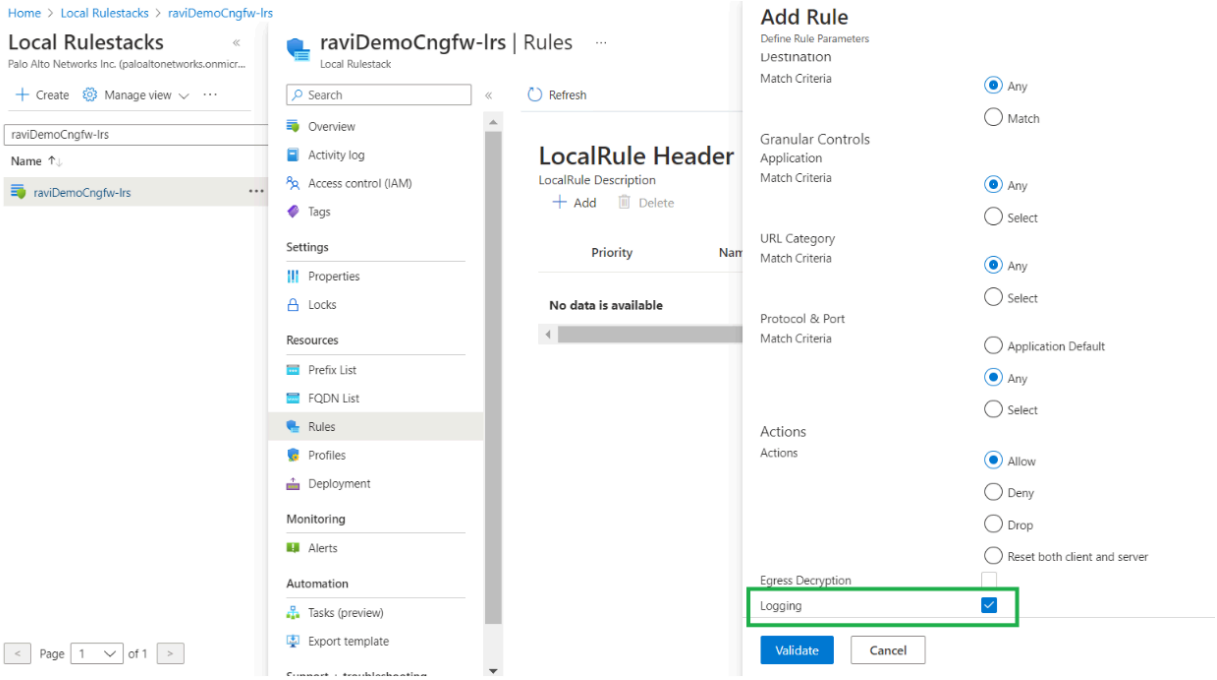
STEP 3 | Sélectionnez le service de rulestacks locales pour accéder à la liste des rulestacks locales associées à votre abonnement Cloud NGFW. Recherchez une rulestack locale et vérifiez que l'état est **Succeeded (Réussi)**.



STEP 4 | Cliquez sur la rulestack pour ajouter des règles. Dans la fenêtre **Add Rule (Ajouter une règle)**, modifiez les règles. Par exemple, ajoutez une règle qui autorise le trafic ; remplissez les champs obligatoires et utilisez les paramètres par défaut pour les champs restants.



STEP 5 | Activez la journalisation pour la règle. Dans la fenêtre Add Rule (Ajouter une règle), sélectionnez **Logging (Journalisation)**.



STEP 6 | Cliquez sur **Validate (Valider)**, puis sur **Add (Ajouter)** pour ajouter la règle à la rulestack.

Ajouter une liste FQDN

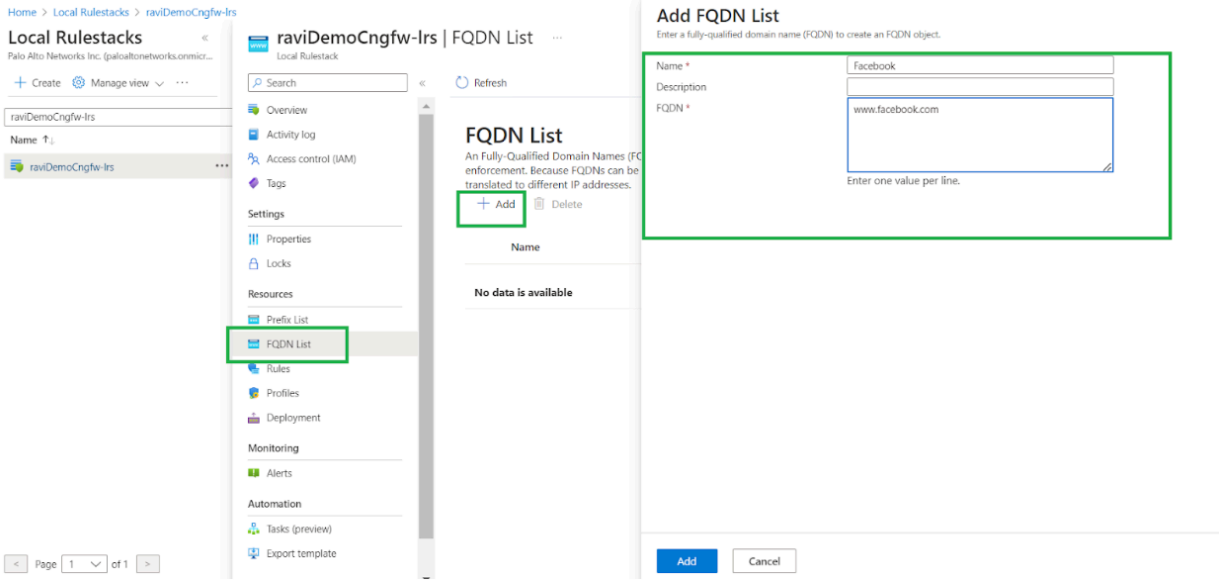
Ajoutez une liste FQDN à la rulestack locale qui inclut Facebook. Utilisez cette liste pour ajouter une règle qui bloque le trafic vers facebook.com

STEP 1 | Dans la page de la rulestack locale de la ressource Cloud NGFW, cliquez sur **FQDN List (Liste FQDN)**.

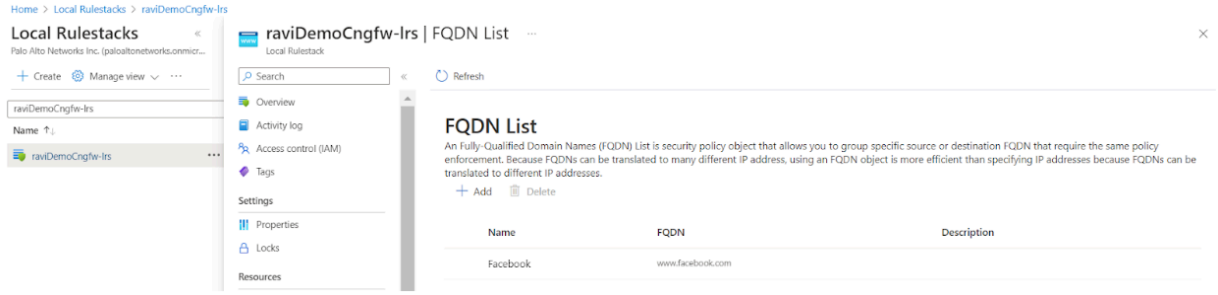
STEP 2 | Cliquez sur **Add (Ajouter)**.

STEP 3 | Dans l'écran **Add FQDN List (Ajouter une liste FQDN)**, saisissez un nom et une description. Dans le champ FQDN, saisissez une ou plusieurs URL, telles que www.facebook.com. Une seule URL FQDN peut exister sur une seule ligne dans le champ FQDN.

STEP 4 | Cliquez sur **Add (Ajouter)**.



STEP 5 | Vérifiez que les URL spécifiées apparaissent dans la liste FQDN.



Ajouter une règle

Ajoutez une règle à la rulestack locale qui correspond à la liste FQDN créée précédemment. Avec la règle, vous pouvez définir une action, comme abandonner le trafic. Par exemple, vous pouvez appliquer une action à la règle FQDN pour abandonner le trafic tentant d'accéder à l'URL www.facebook.com.

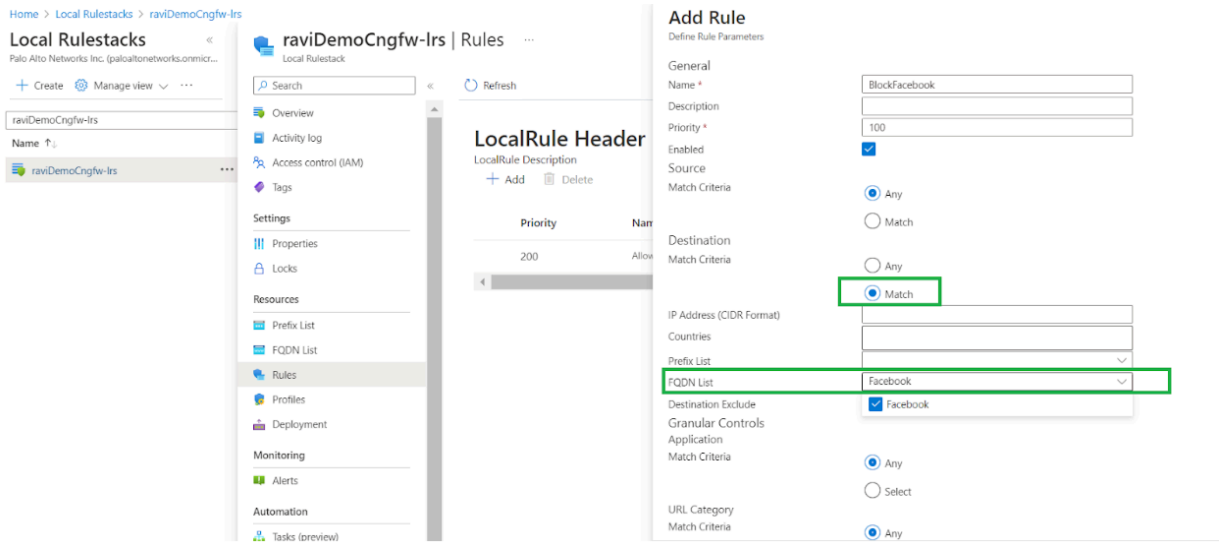
STEP 1 | Dans la page de la rulestack locale de la ressource Cloud NGFW, cliquez sur **Rules (Règles)**.

STEP 2 | Cliquez sur **Add (Ajouter)**.

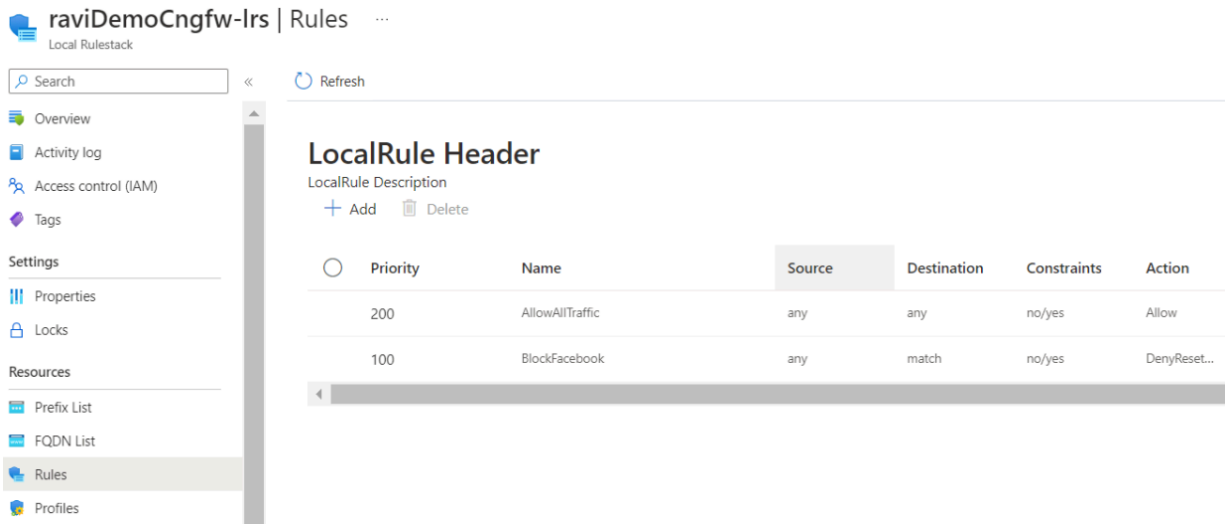
STEP 3 | Dans l'écran **Add Rule (Ajouter une règle)**, définissez les Match Criteria (Critères de correspondance) sur Match (Correspondance). Dans le champ **FQDN List (Liste FQDN)**, utilisez le menu déroulant pour sélectionner Facebook

STEP 4 | Dans le champ **Actions** , sélectionnez **Drop (Abandonner)**.

STEP 5 | Cliquez sur **Add (Ajouter)**.

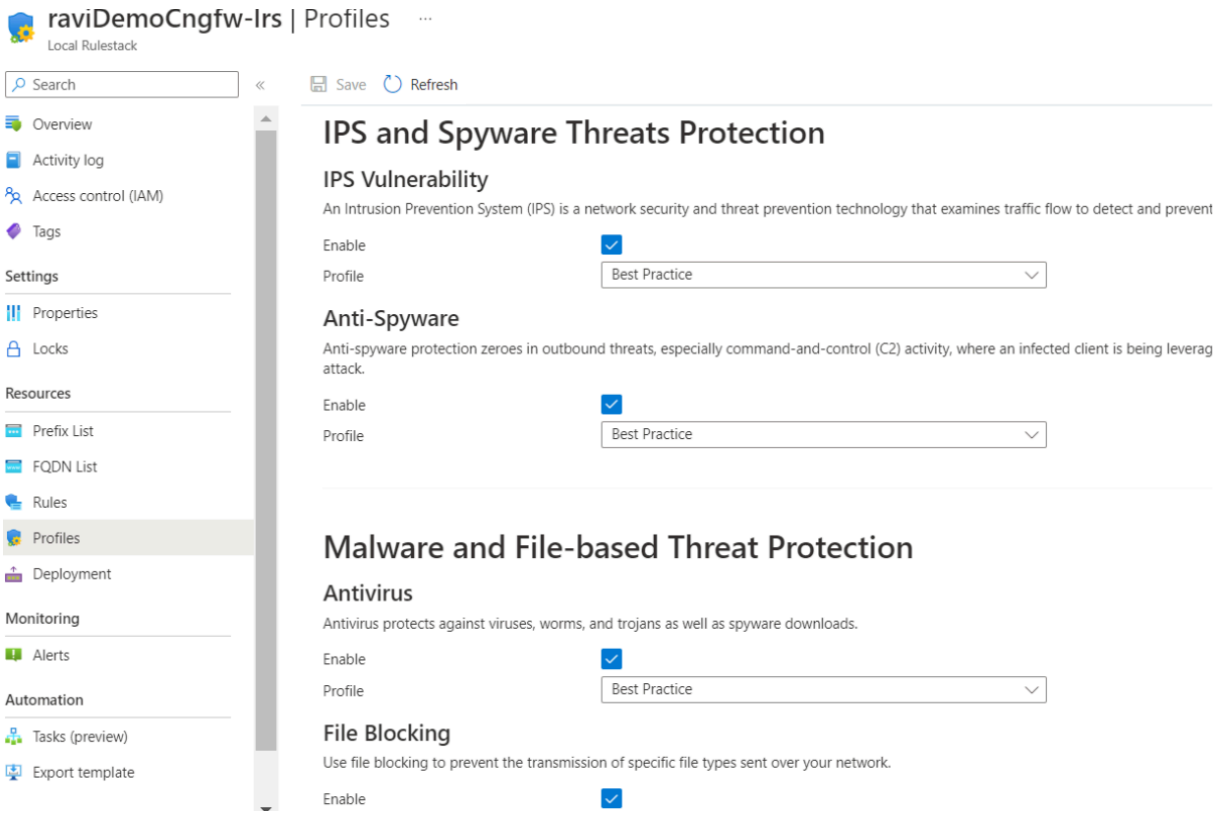


Les deux règles apparaissent sur la page d’en-tête de la rulestack locale.



Dans le cadre de ce service Cloud NGFW, les profils de sécurité sont activés avec les configurations des meilleures pratiques par défaut. Le trafic est sécurisé avec les meilleurs profils de sécurité une

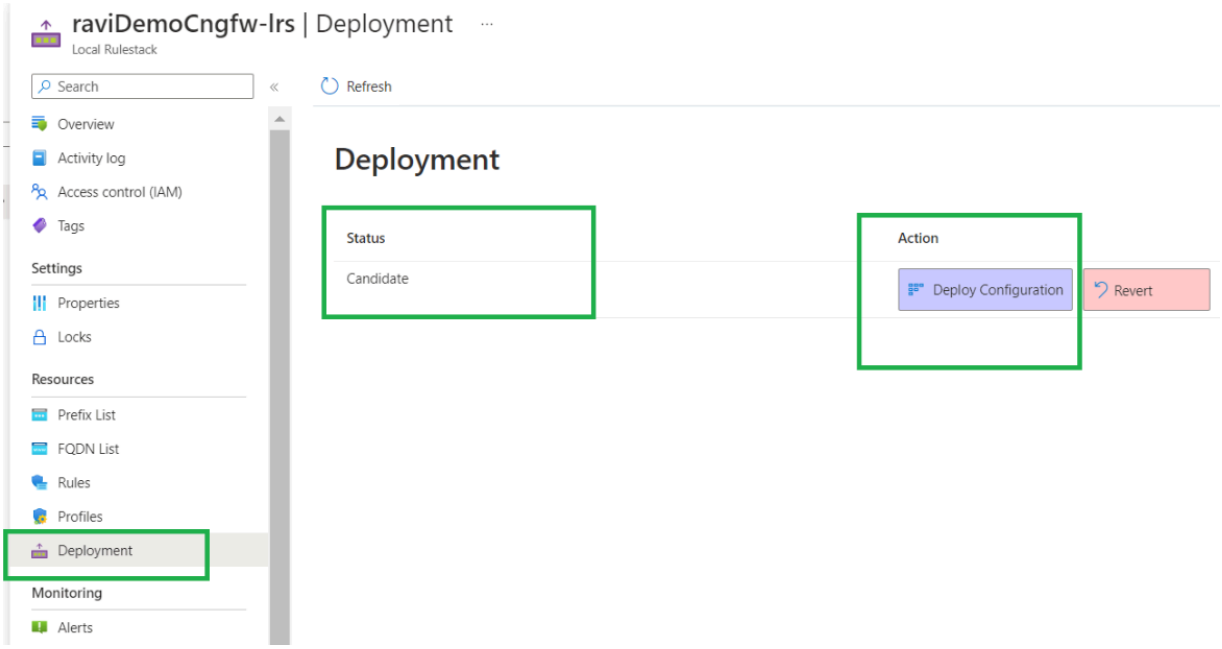
fois le Cloud NGFW déployé dans le réseau. Affichez-les à l'aide de la page **Profiles (Profils)** pour la rulestack locale.



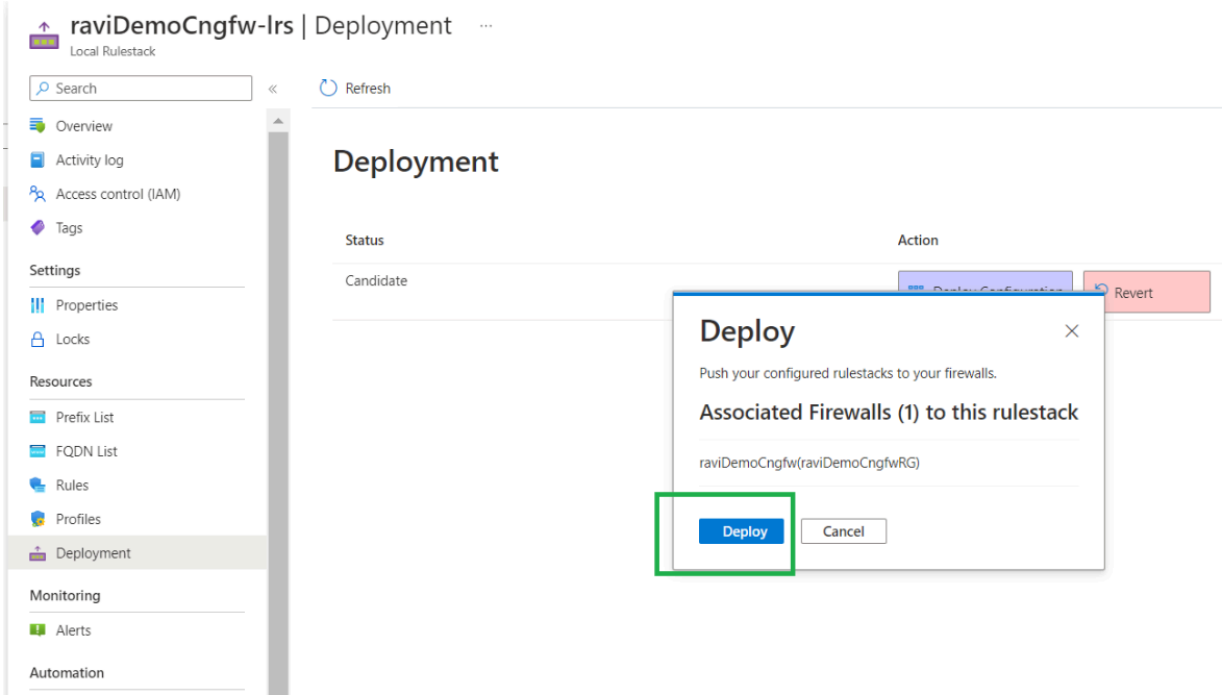
Après avoir modifié les règles, déployez-les sur la rulestack locale associée au service Cloud NGFW.

STEP 6 | Dans la rulestack locale, cliquez sur **Deployment (Déploiement)**. La page d'état du déploiement s'affiche comme Candidate (Candidat) ; cela signifie que la configuration a été définie, mais pas déployée.

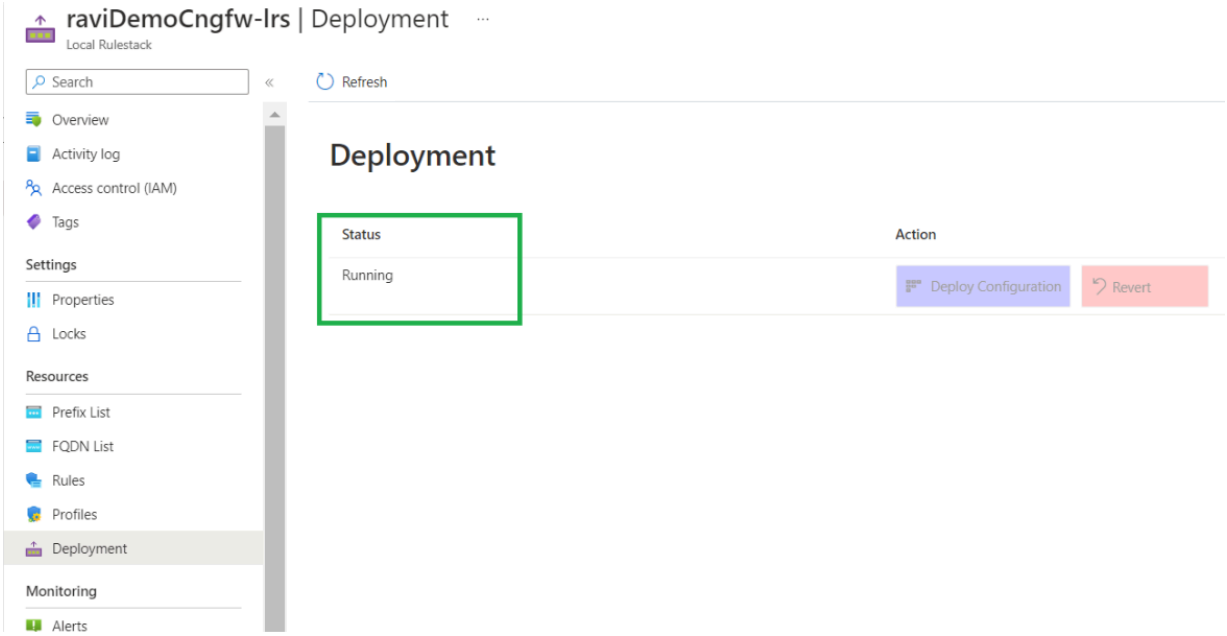
STEP 7 | Cliquez sur **Deploy Configuration (Déployer la configuration)** pour déployer la configuration sur le service Cloud NGFW. Vous devez effectuer cette étape afin de déployer les règles sur la rulestack.



STEP 8 | Après avoir cliqué sur **Deploy Configuration (Déployer la configuration)**, un message contextuel affiche les pare-feu associés à cette rulestack. Cliquez sur **Deploy (Déployer)** pour configurer cette rulestack sur tous les pare-feu associés.



STEP 9 | Une fois la configuration déployée, l'état **du déploiement** est **Running (En cours d'exécution)**.

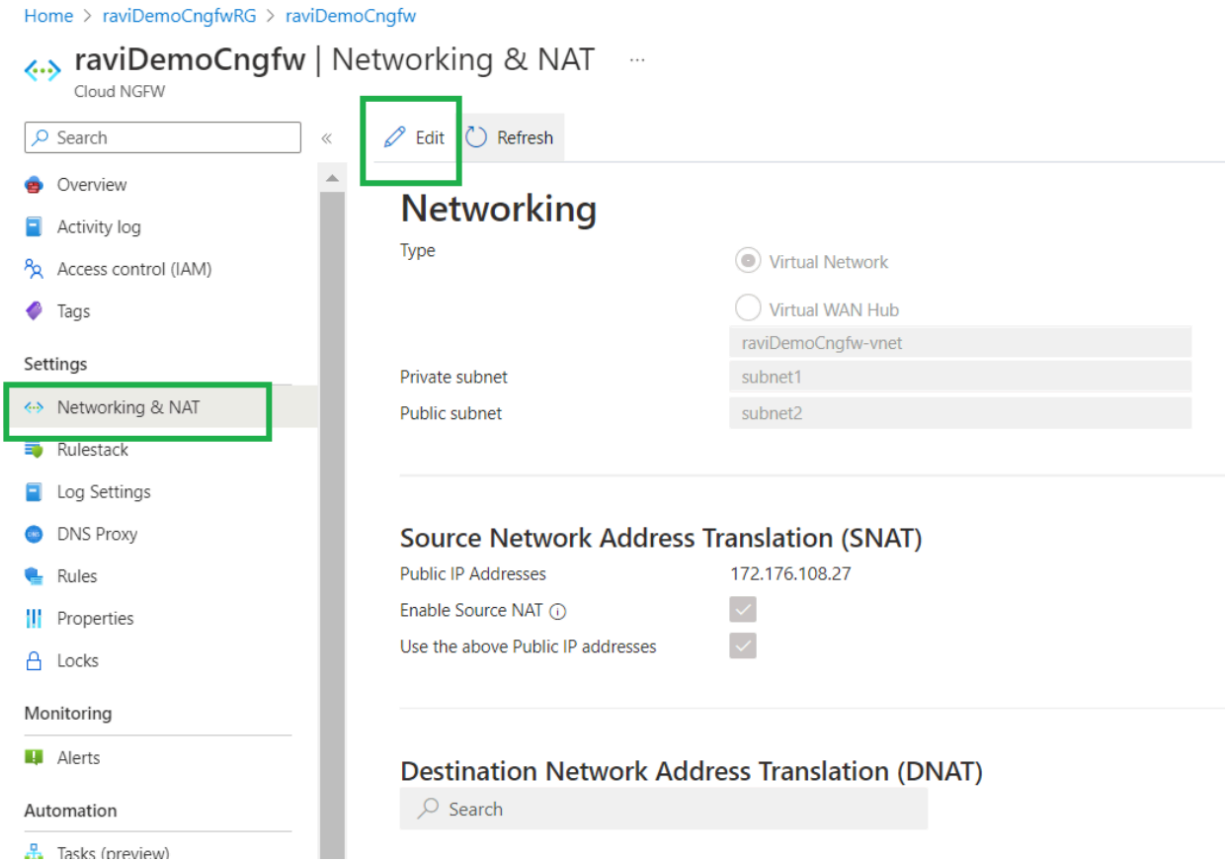


Configurer une règle NAT source et de destination

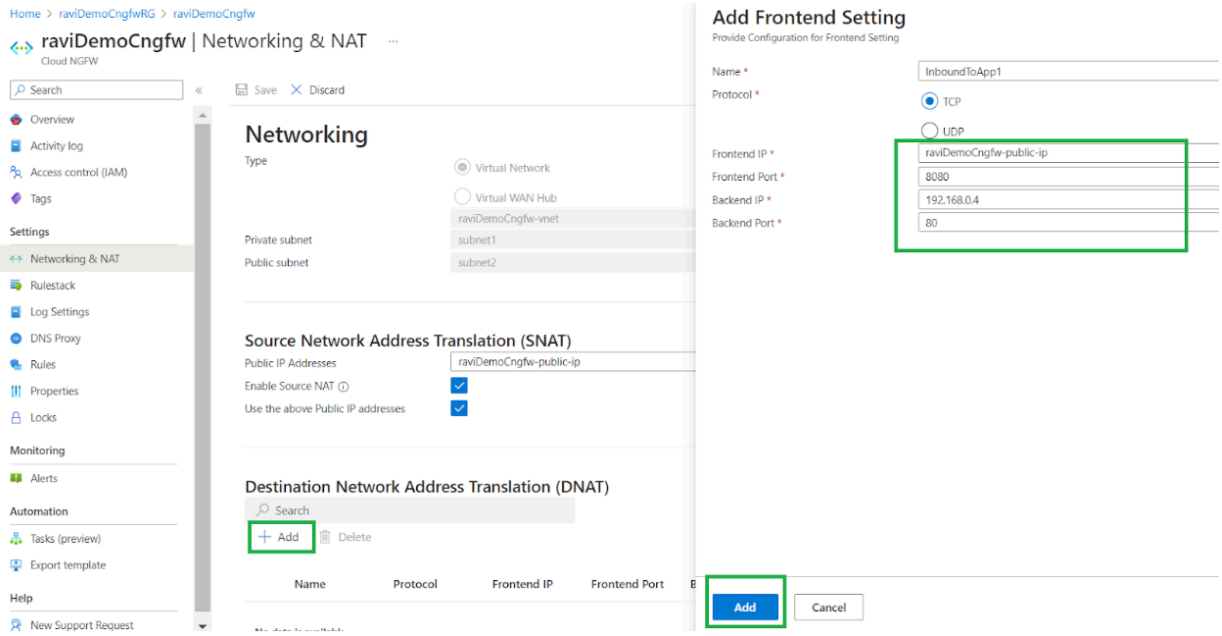
Vous pouvez configurer une règle NAT de destination pour gérer le trafic entrant.

STEP 1 | Accédez aux paramètres **Networking & NAT (Mise en réseau et NAT)** pour la ressource Cloud NGFW. Pour déterminer si le paramètre Source NAT (NAT source) est activé.

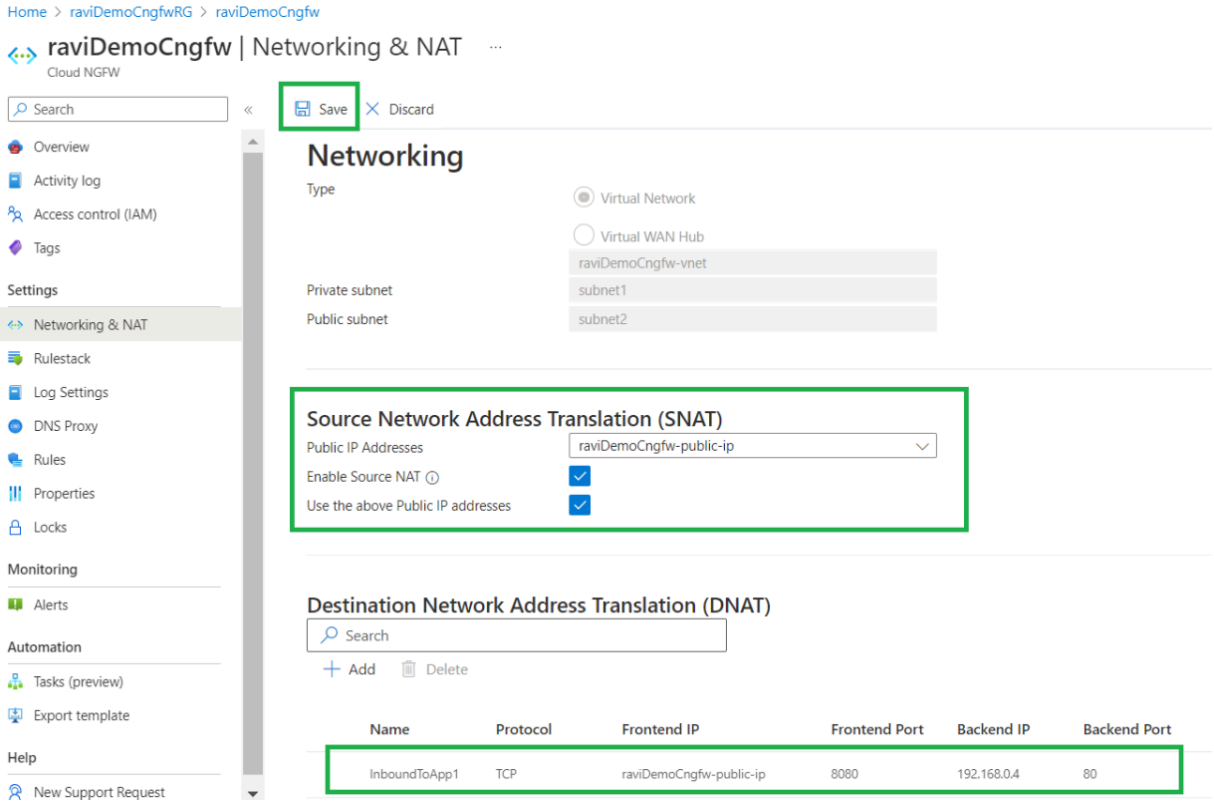
STEP 2 | Cliquez sur **Edit (Modifier)** pour ajouter la règle NAT de destination.



STEP 3 | Ajoutez une règle NAT de destination. L'adresse IP frontale représente l'adresse IP publique associée au Cloud NGFW. Saisissez le numéro de port frontal et cliquez sur **Add (Ajouter)**.



STEP 4 | Après avoir ajouté la règle NAT de destination, cliquez sur **Save (Enregistrer)** pour déployer la configuration sur la ressource Cloud NGFW.



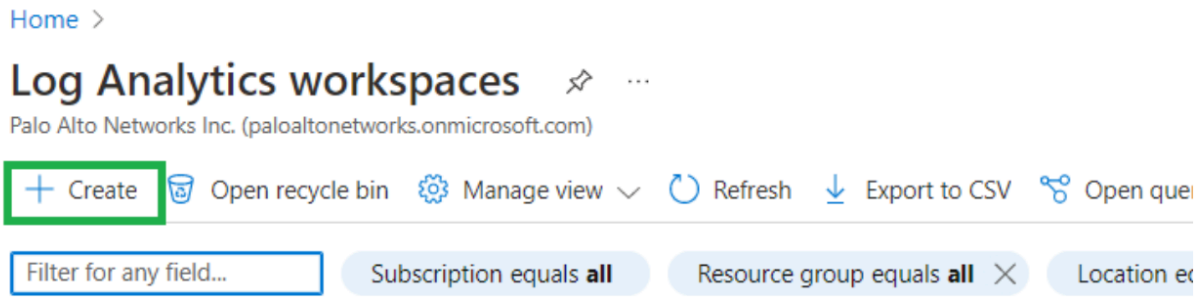
L’adresse frontale est désormais redirigée via le port configuré via Cloud NGFW. Le trafic entrant circule désormais via le Cloud NGFW.

Configurer la journalisation

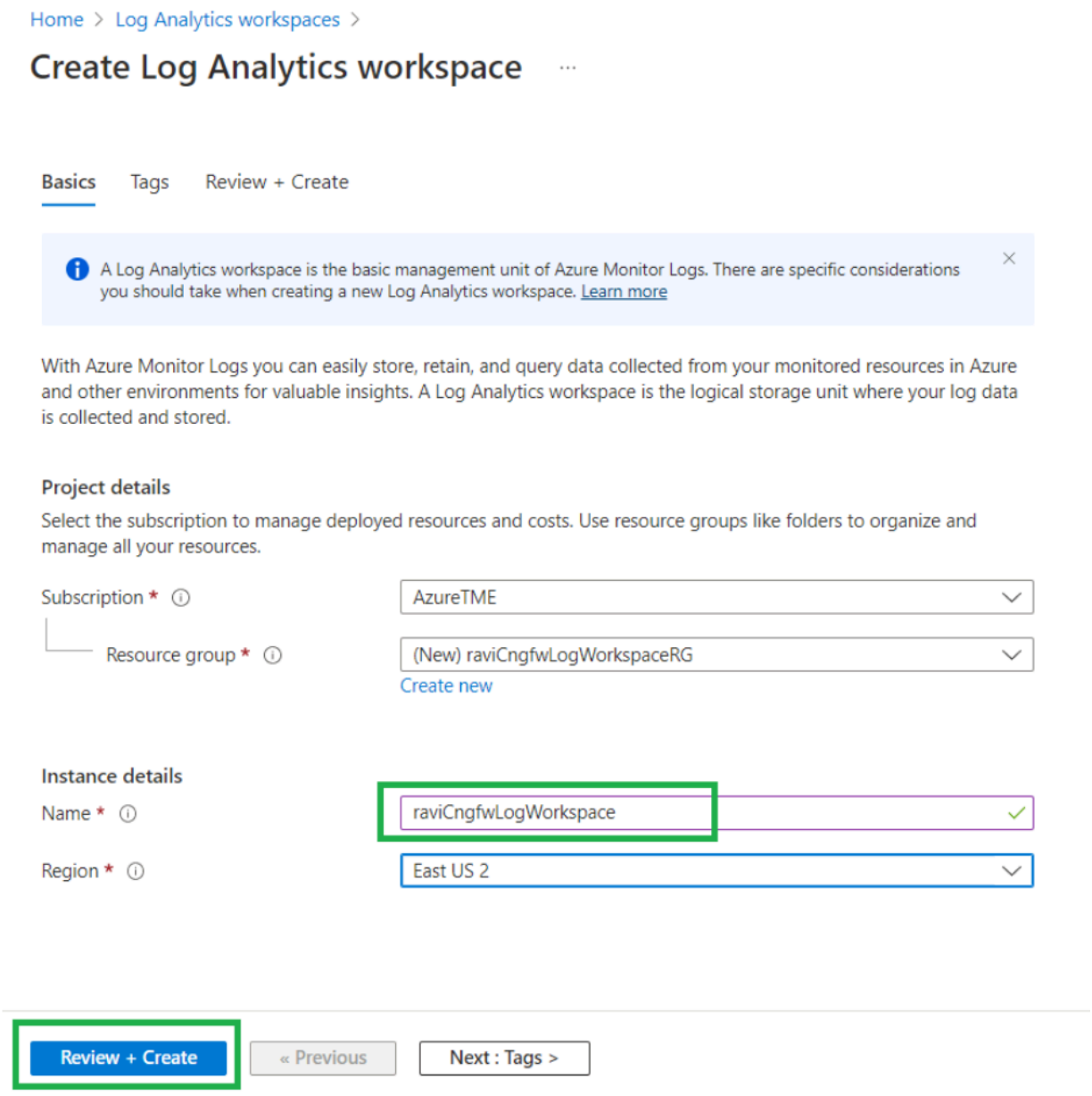
Avant de configurer la journalisation sur le Cloud NGFW, créez l’espace de travail Log Analytics sur Azure.

STEP 1 | Dans le portail Azure, recherchez l’**espace de travail Azure Log Analytics**. Cliquez sur **Log Analytics Workspaces (Espaces de travail Log Analytics)** pour l’ajouter en tant que service.

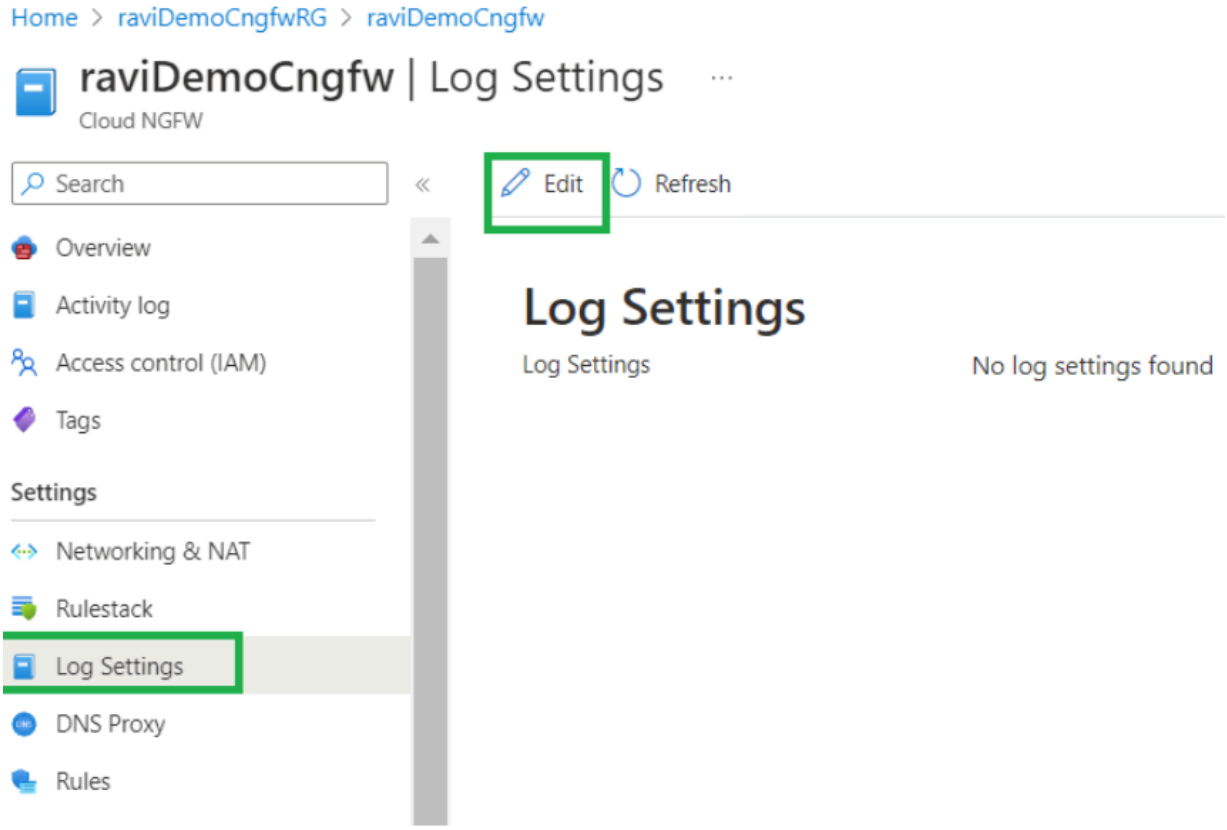
STEP 2 | Cliquez sur **Create (Créer)** pour établir un nouvel espace de travail **Log Analytics** :



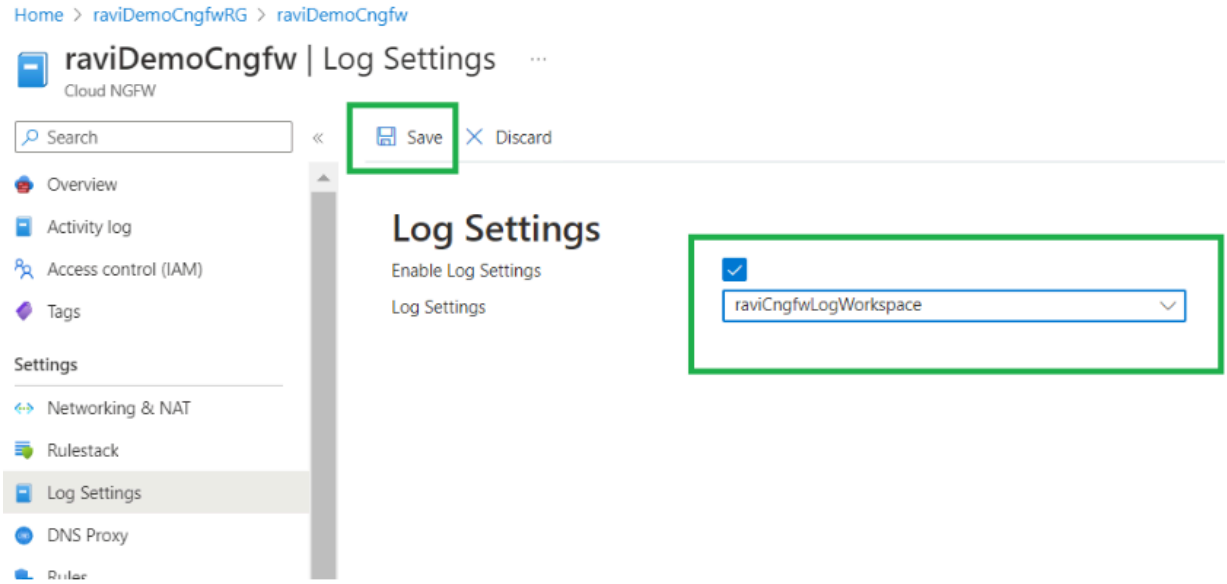
STEP 3 | Dans l’espace de travail Log Analytics ainsi créé, fournissez les détails de l’**instance**. Sélectionnez le **Nom** de l’espace de travail dans le menu déroulant et spécifiez la **Region (Région)**.



STEP 4 | Configurez les paramètres du journal dans la ressource Cloud NGFW. Sélectionnez **Log Settings (Paramètres du journal)**. Cliquez sur **Edit (Modifier)**.



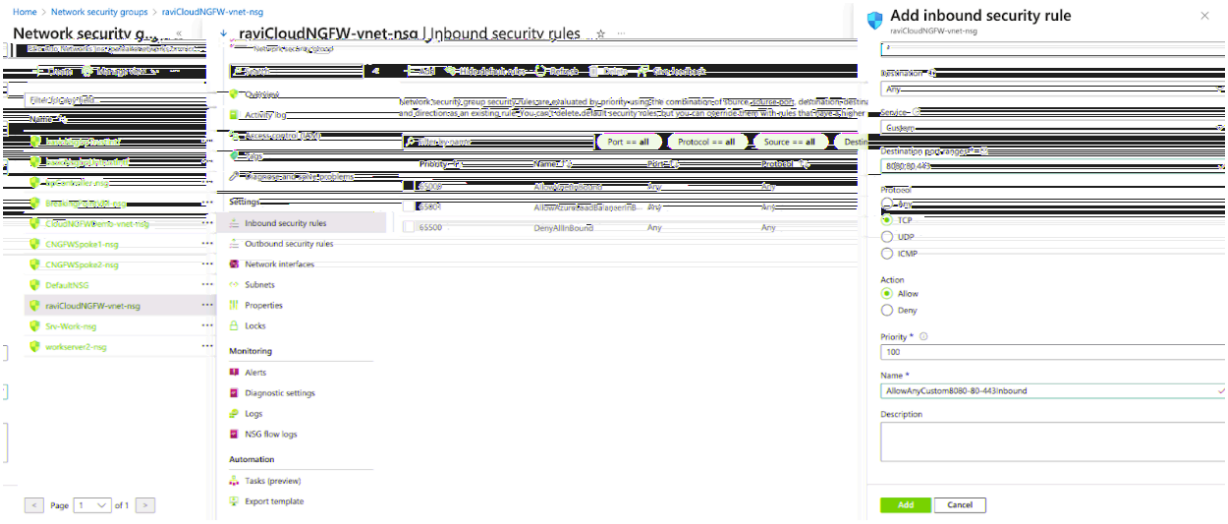
STEP 5 | Dans le champ **Log Settings (Paramètres du journal)**, sélectionnez l'espace de travail Log Analytics créé précédemment, puis cliquez sur **Save (Enregistrer)**.



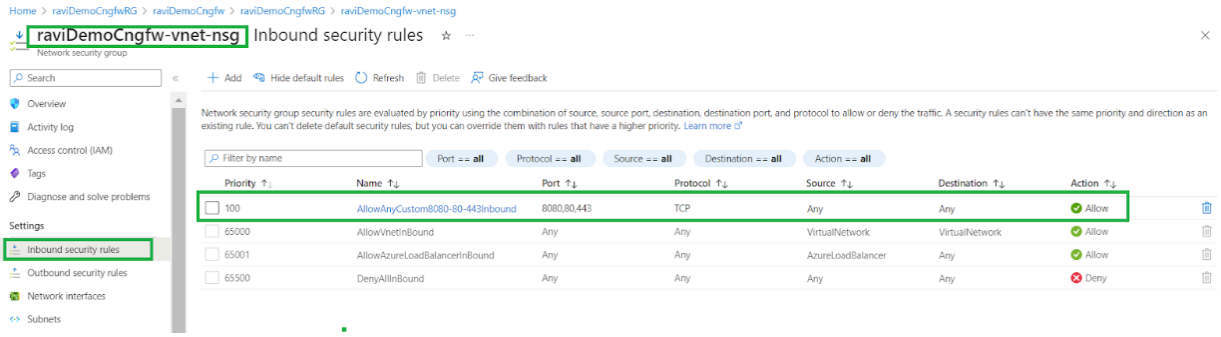
Mettre à jour le groupe de sécurité réseau

Mettez à jour le groupe de sécurité réseau que vous avez créé dans le cadre du déploiement Cloud NGFW. Ce groupe de sécurité est associé à des sous-réseaux privés et publics dans le cadre du vNET dans l'abonnement Cloud NGFW.

STEP 1 | Autorisez le trafic dans le cadre de la configuration des règles NAT (destination) frontales. Autorisez le trafic HTTP et HTTPS afin qu'Internet soit accessible depuis les vNET d'application via le Cloud NGFW.



STEP 2 | Cliquez sur **Add (Ajouter)** pour incorporer cette règle de sécurité entrante :



Configurer l’appairage vNET

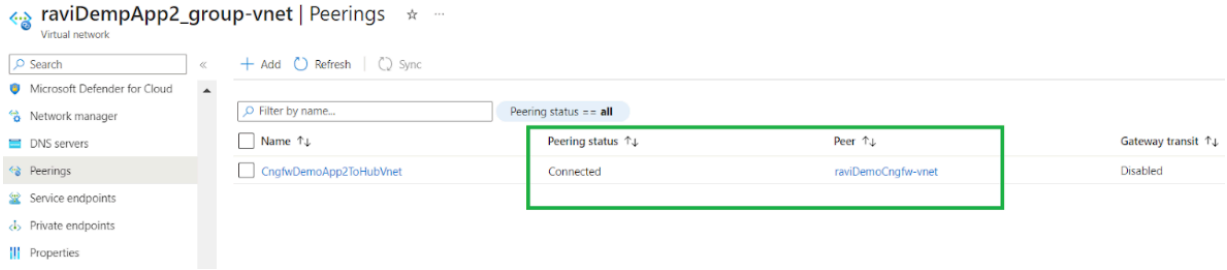
Pour configurer l’appairage VNet :

STEP 1 | Recherchez votre vNET et sélectionnez **Peerings (Appairages)**.

STEP 2 | Cliquez sur **Add (Ajouter)** pour créer un appairage.

STEP 3 | Donnez un nom à l’appairage et conservez les paramètres par défaut.

STEP 4 | Sélectionnez le hub vNET que vous souhaitez appairer. Lors du déploiement du Cloud NGFW dans un vNET à l’aide d’un hub vNET existant, la taille minimale doit être /25. Vous devez disposer de deux sous-réseaux avec une taille minimale de /26 ; ces sous-réseaux doivent être délégués au service **PaloAltoNetworks.Cloudngfw/firewalls**



STEP 5 | Configurez l’appairage vNET entre d’autres réseaux virtuels en répétant les étapes décrites dans cette section.

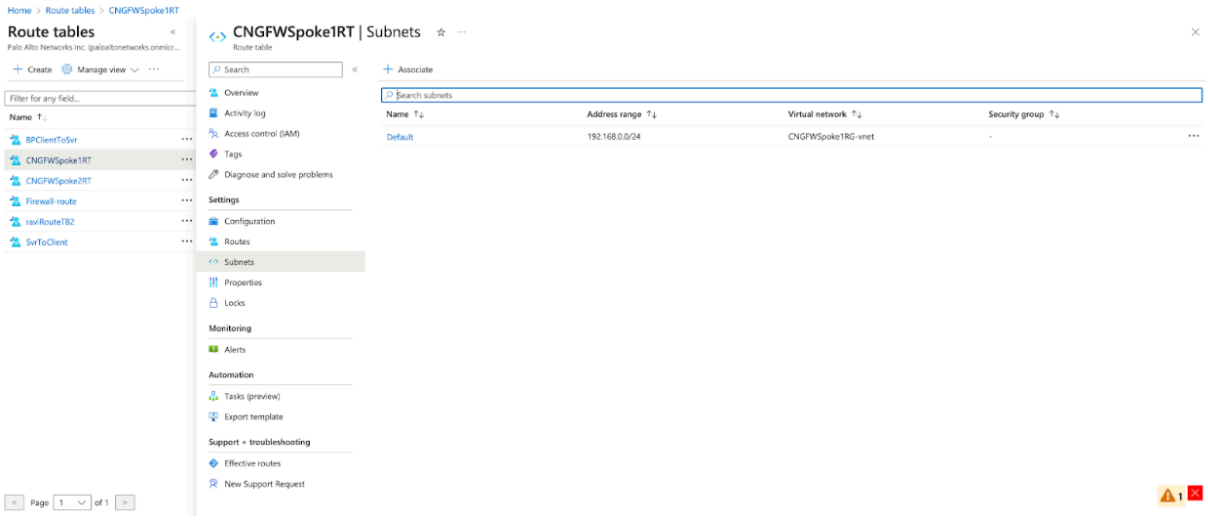
Ajouter une table de routage pour acheminer le trafic via le Cloud NGFW

STEP 1 | Recherchez la **table de routage** dans la barre de recherche du portail Azure.

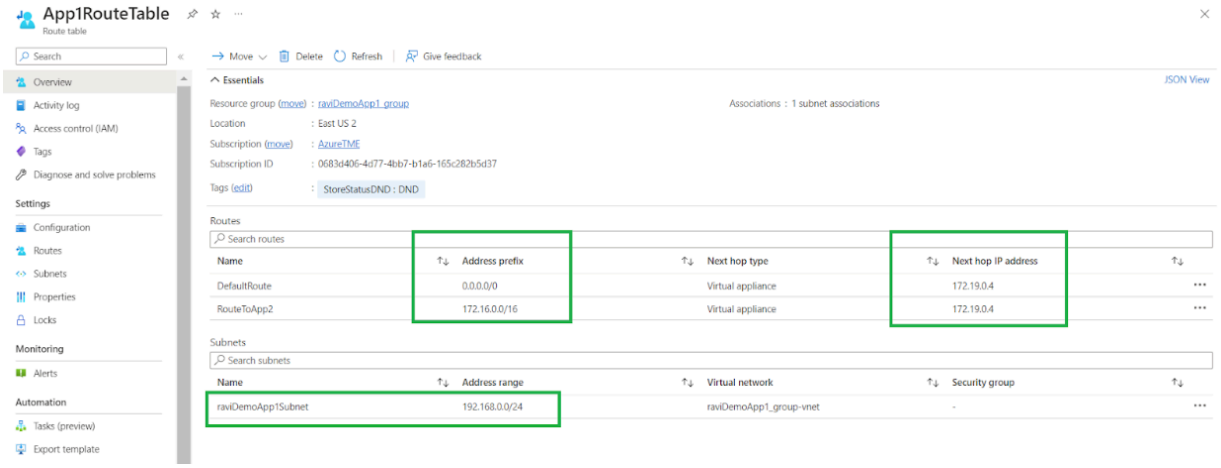
STEP 2 | Cliquez sur **Create (Créer)** pour établir une nouvelle table de routage.

STEP 3 | Remplissez les champs de la table de routage, puis cliquez sur **Review+create (Revoir + créer)**.

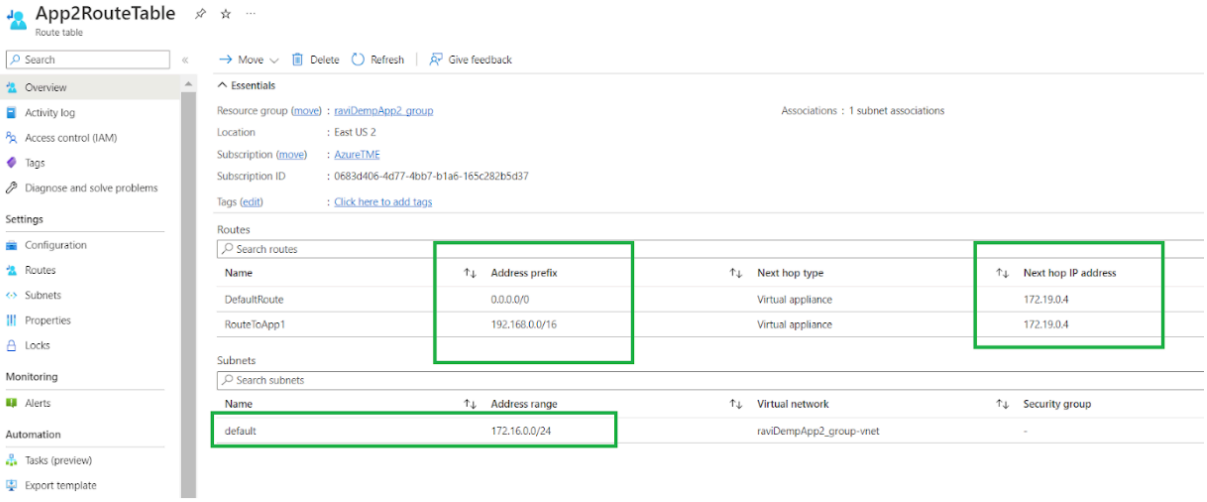
STEP 4 | Après avoir créé la table de routage, sélectionnez la section **Subnets (Sous-réseaux)** et associez la table au sous-réseau.



STEP 5 | Configurez l’itinéraire par défaut pour le trafic sortant et acheminez-le vers le sous-réseau (pour le trafic est-ouest) avec le tronçon suivant comme adresse IP privée Cloud NGFW.



STEP 6 | Associez une ou plusieurs tables de routage à un autre sous-réseau du vNET. Configurez un itinéraire par défaut (pour le trafic sortant) et acheminez-le vers un autre sous-réseau (pour le trafic est-ouest) avec le tronçon suivant comme adresse IP privée Cloud NGFW.



Déployer le Cloud NGFW dans un vWAN

Le Cloud NGFW peut être déployé de manière transparente dans le hub vWAN en tant que solution de pare-feu évolutive pour sécuriser le trafic entre les charges de travail critiques hébergées dans un réseau hybride mondial Azure et sur site. Pour plus d'informations sur le vWAN Azure et les fonctionnalités et capacités disponibles, reportez-vous à la documentation Azure Virtual WAN.

Tenez compte des éléments suivants lors du déploiement du Cloud NGFW dans un vWAN :

- Une adresse IP privée est utilisée pour une ressource NGFW. Pour les environnements vWAN, configurez la politique de routage du hub vWAN de façon à *épingler* le trafic du service. C'est-à-dire que le trafic quitte d'une interface et revient avant de sortir sur Internet.
- Le provisionnement d'un nouveau hub vWAN peut prendre environ 30 minutes. Vous pouvez vérifier l'état d'un hub vWAN nouvellement créé dans le champ **Routing Status (État du routage)** de la section **Essentials (Informations de base)** de la page **Overview (Aperçu)**.

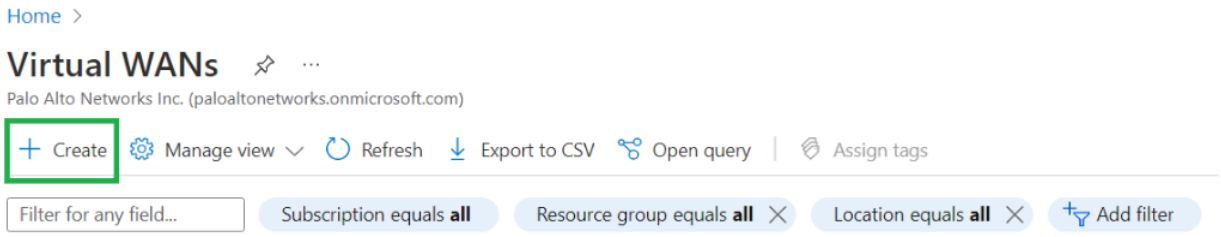
Le déploiement Cloud NGFW pour Azure vWAN :

- Est entièrement intégré dans Azure Virtual WAN à l'aide du framework SaaS.
- Est déployé directement dans le hub virtuel vWAN.
- Utilise l'intention de routage et les politiques pour contrôler quel trafic est inspecté par le service Cloud NGFW.
- Permet l'application d'une politique de sécurité cohérente pour le trafic inter-hub et inter-région

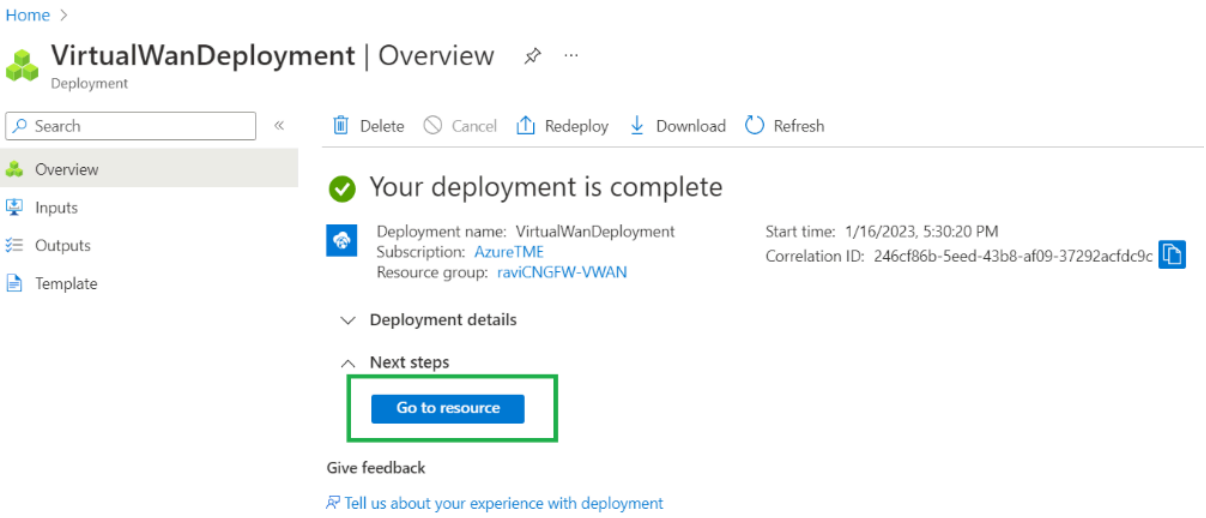
Prérequis

Pour déployer Cloud NGFW dans un vWAN, vous aurez besoin d'un abonnement Azure. Cet abonnement devrait avoir un rôle **propriétaire** ou **contributeur**.

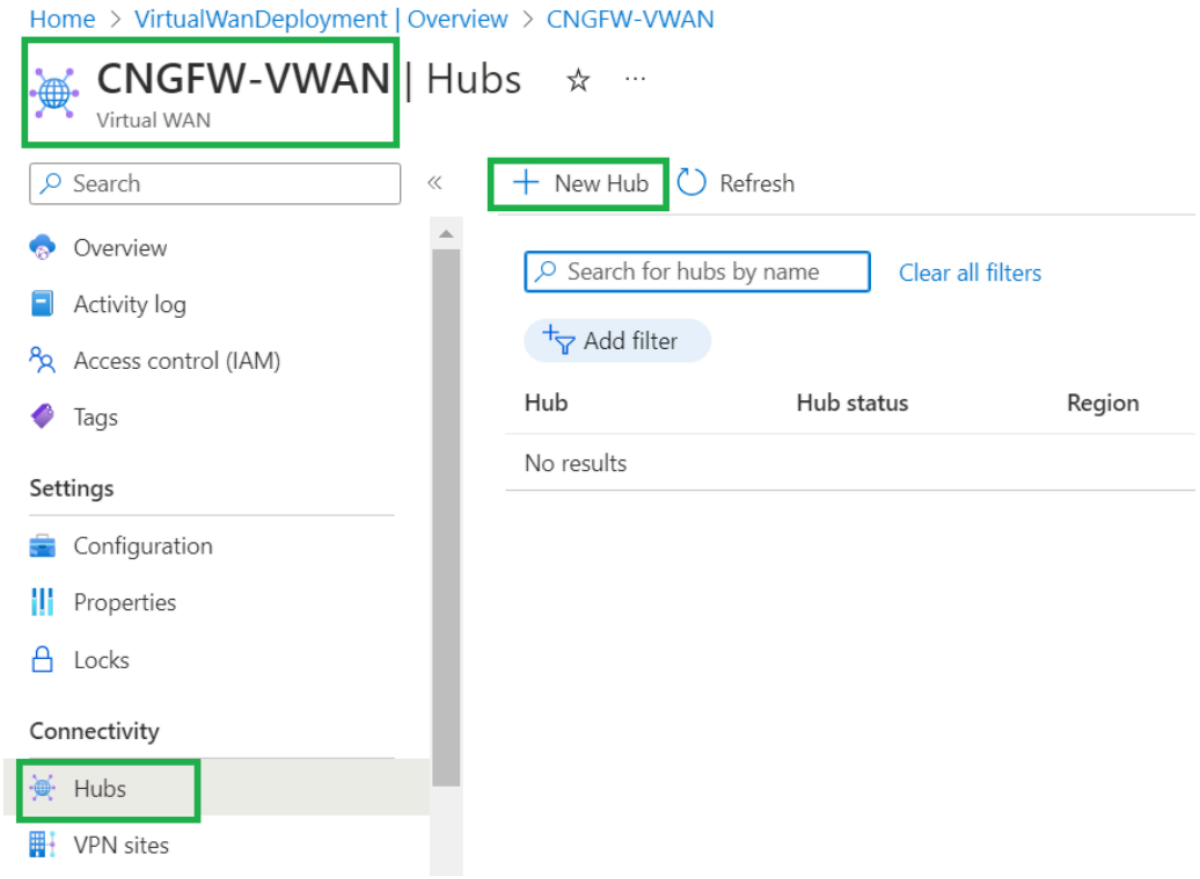
STEP 1 | Connectez-vous au portail Azure et recherchez **Virtual WAN**. Cliquez sur **Create (Créer)** pour créer un service WAN virtuel.



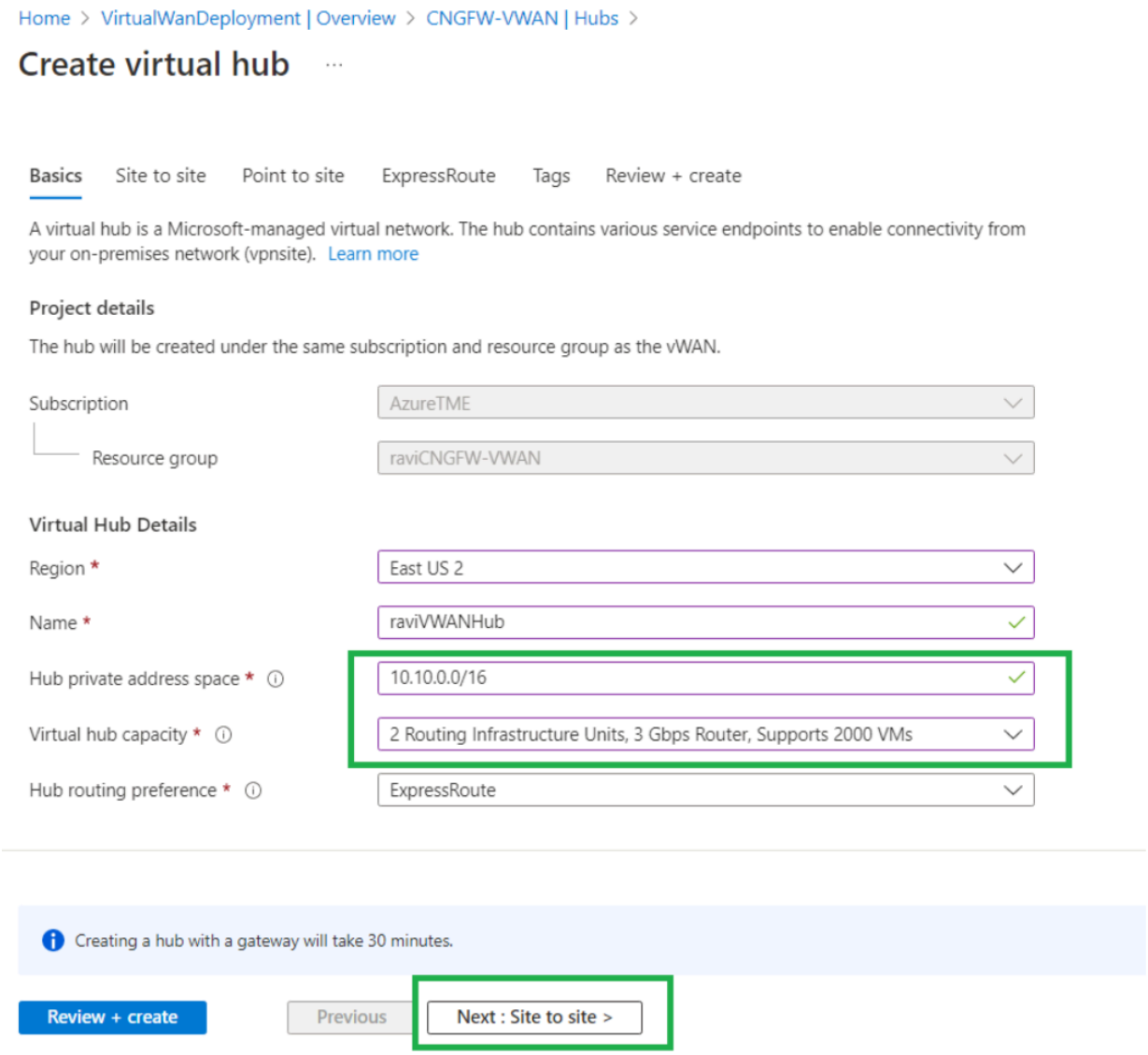
STEP 2 | Une fois le service créé, cliquez sur **Go to resource (Aller à la ressource)**.



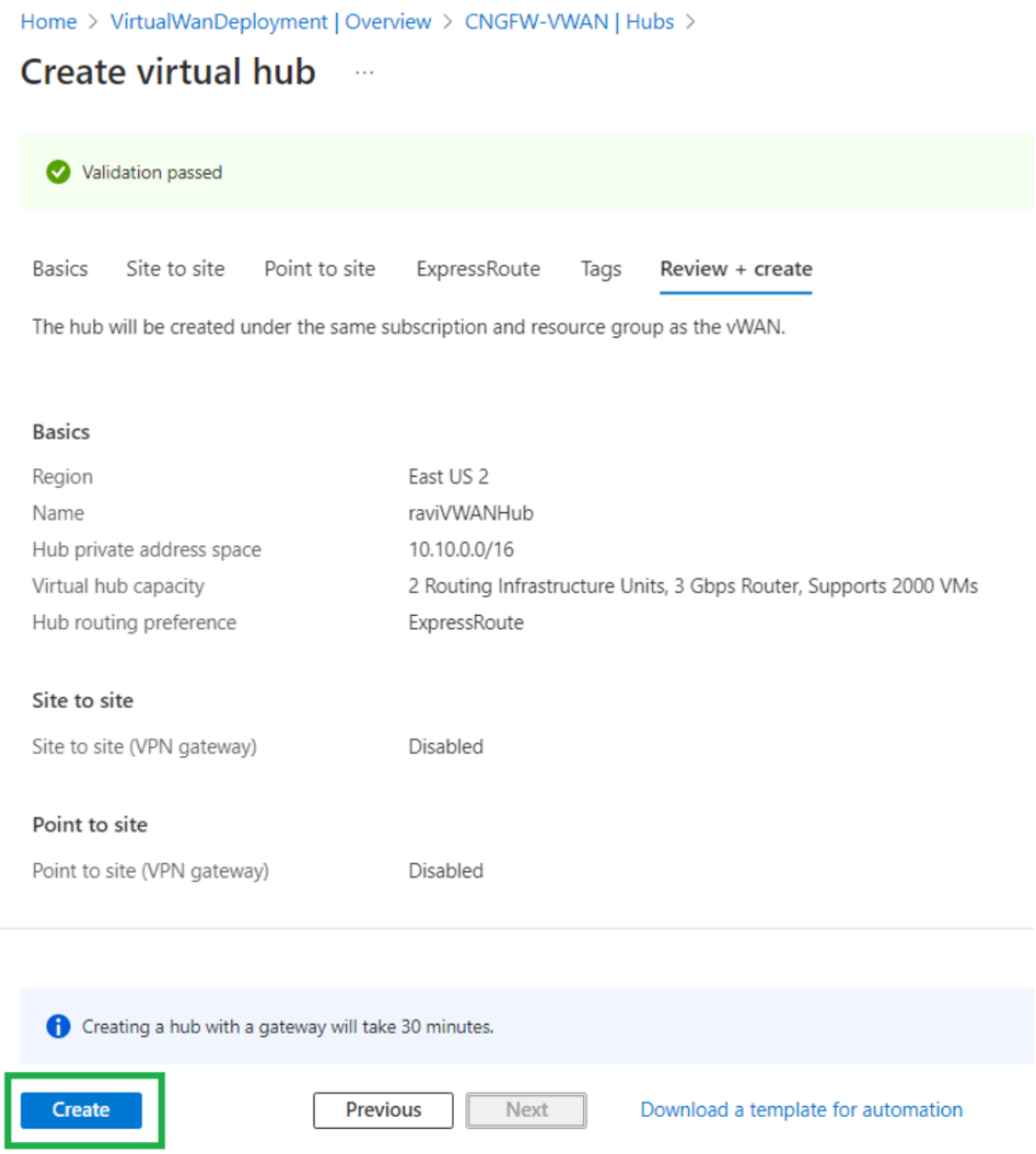
STEP 3 | Ajoutez un hub au WAN virtuel que vous avez créé. Sélectionnez **Connectivity (Connectivité)** > **Hubs**. Cliquez sur **New Hub (Nouveau hub)**.



STEP 4 | Configurez **Virtual Hub Details (Détails du hub virtuel)**. Spécifiez l'**adresse privée** et la **capacité du hub virtuel**, puis cliquez sur **Next: Site to Site (Suivant : Site à site)**.

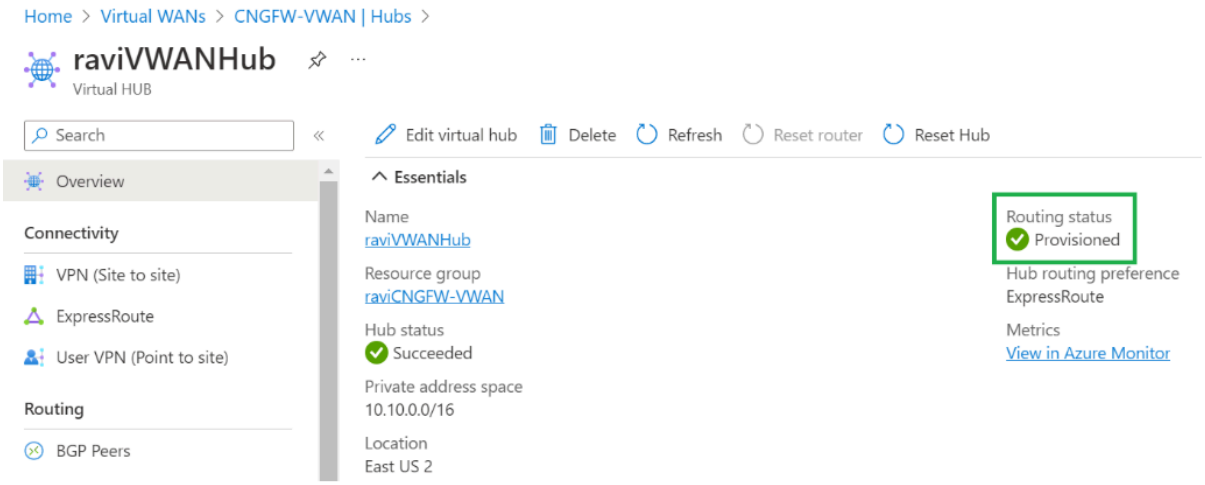


STEP 5 | Après avoir validé la configuration, cliquez sur **Create (Créer)** pour créer le hub WAN virtuel.



STEP 6 | Vérifiez que l'**état du routage** est **Provisioned (Provisionné)**.

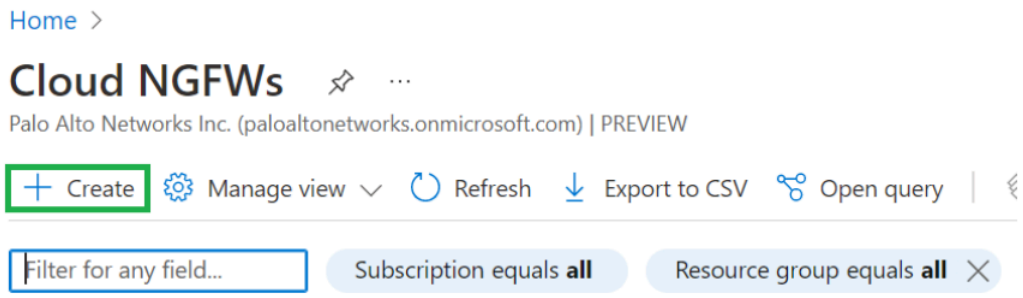
*Le provisionnement du nouveau hub vWAN peut prendre environ 30 minutes. Utilisez la page **Overview (Aperçu)** pour afficher l'état du routage.*



STEP 7 | Connectez-vous au portail Azure et recherchez **Cloud NGFWs by Palo Alto Networks (Cloud NGFWs par Palo Alto Networks)**.

STEP 8 | Cliquez sur **Cloud NGFWs by Palo Alto Networks (Cloud NGFWs par Palo Alto Networks)** pour lancer la création du service Palo Alto Networks Cloud NGFW pour Azure.

STEP 9 | Dans l'écran **Cloud NGFWs (Cloud NGFW)**, cliquez sur **Create (Créer)** ; cette page de renvoi est préremplie avec des instances Cloud NGFW si vous avez déjà créé la ressource.

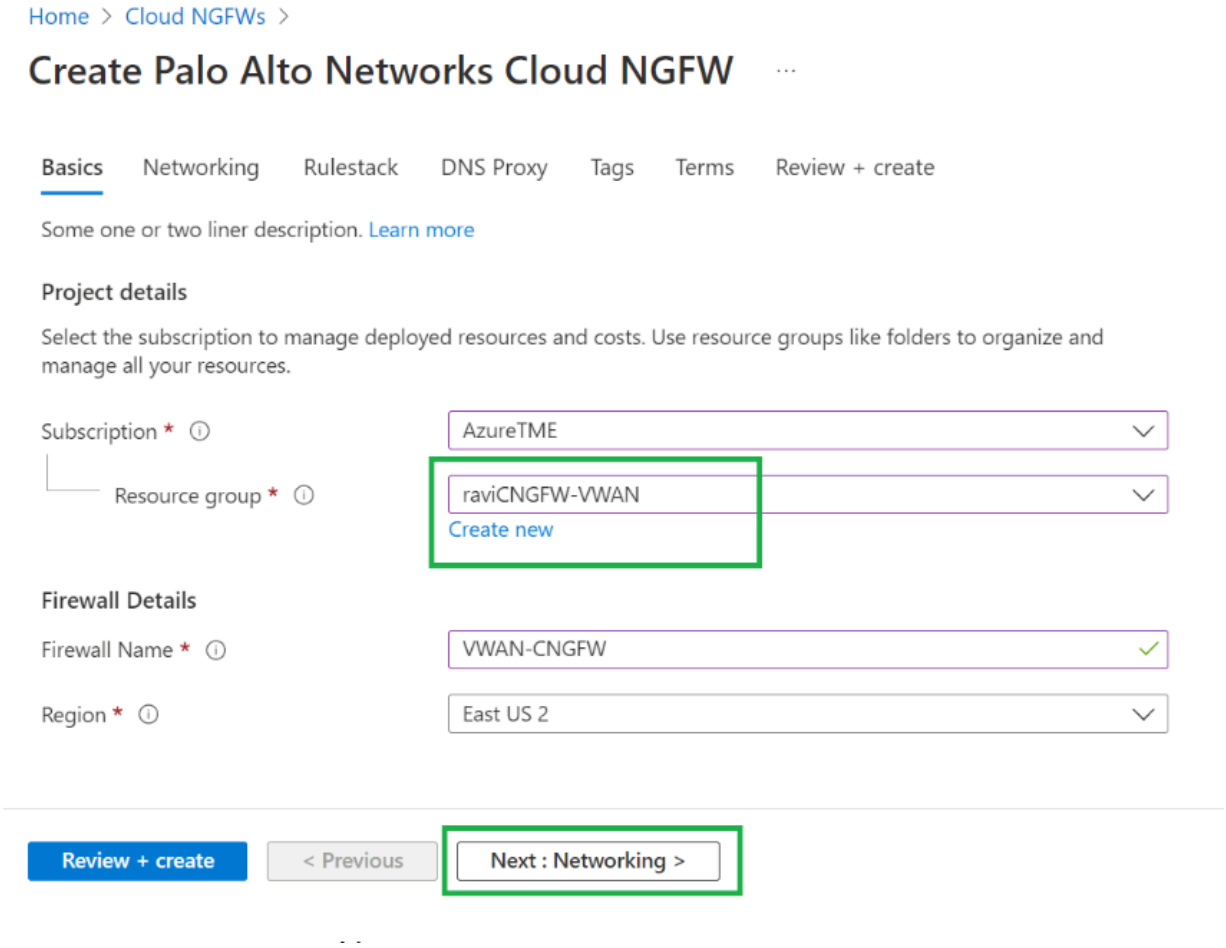


STEP 10 | Dans l’écran **Create Palo Alto Networks Cloud NGFW (Créer Palo Alto Networks Cloud NGFW)**, saisissez les informations de configuration de base dans la section **Project details (Détails du projet)**.

Utilisez les renseignements du tableau suivant pour fournir les **détails du projet**.

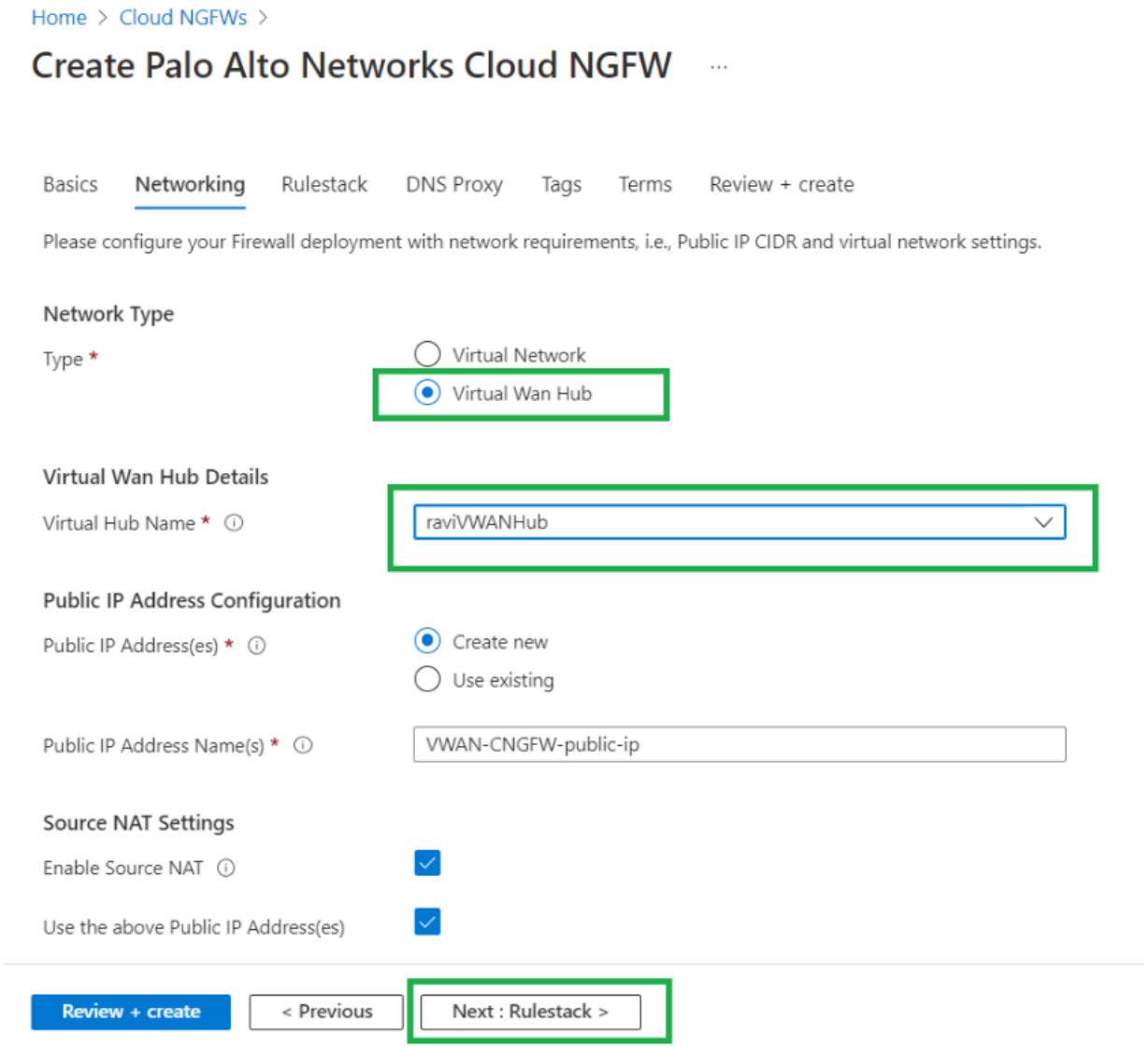
Champ	Description
Abonnement	Sélectionné automatiquement en fonction de l’abonnement utilisé lors de la connexion.
Groupe de ressources	Utilisez l’un des groupes de ressources existants ou créez-en un nouveau (à l’aide de l’option **Create New (Créer un nouveau)**) dans lequel la ressource Cloud NGFW est créée.
Nom du pare-feu	Nom de la ressource de pare-feu Cloud NGFW.

Champ	Description
Région	Région dans laquelle Cloud NGFW est provisionné.

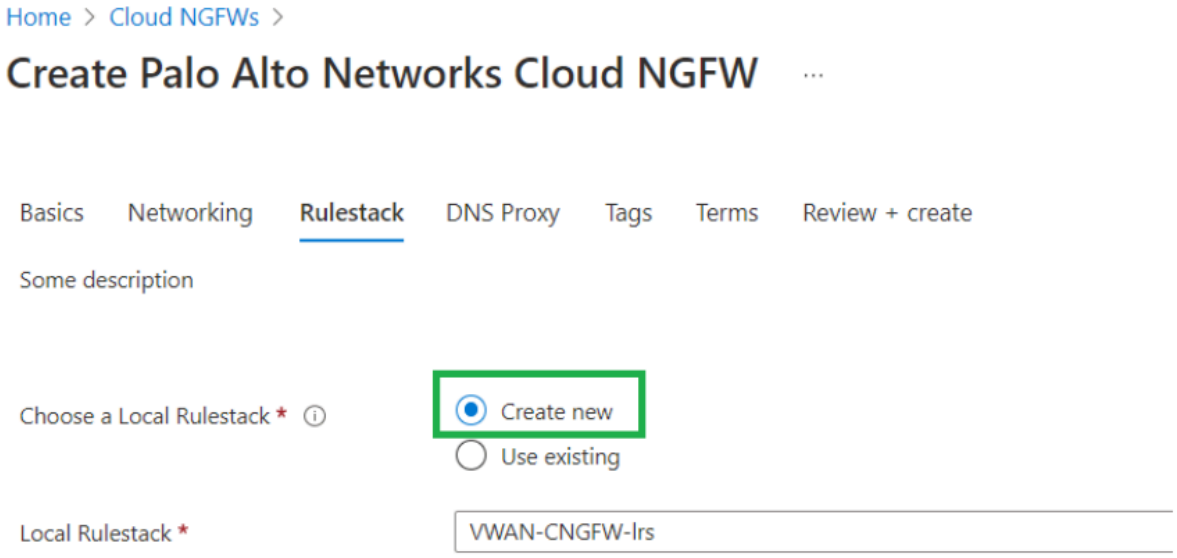


STEP 11 | Cliquez sur **Next: Networking** (Suivant : mise en réseau). Fournissez des informations pour votre environnement réseau. Choisissez le **Virtual WAN Hub (Hub WAN virtuel)** pour le **Network Type (Type de réseau)**. Dans la section **Virtual WAN Hub Details (Détails du hub WAN virtuel)**, sélectionnez le **nom du hub virtuel** que vous avez créé précédemment dans le menu déroulant.

Spécifiez les **adresses IP publiques** et l'option **Source NAT (NAT source)** si la traduction d'adresse est utilisée sur le trafic sortant vers Internet.

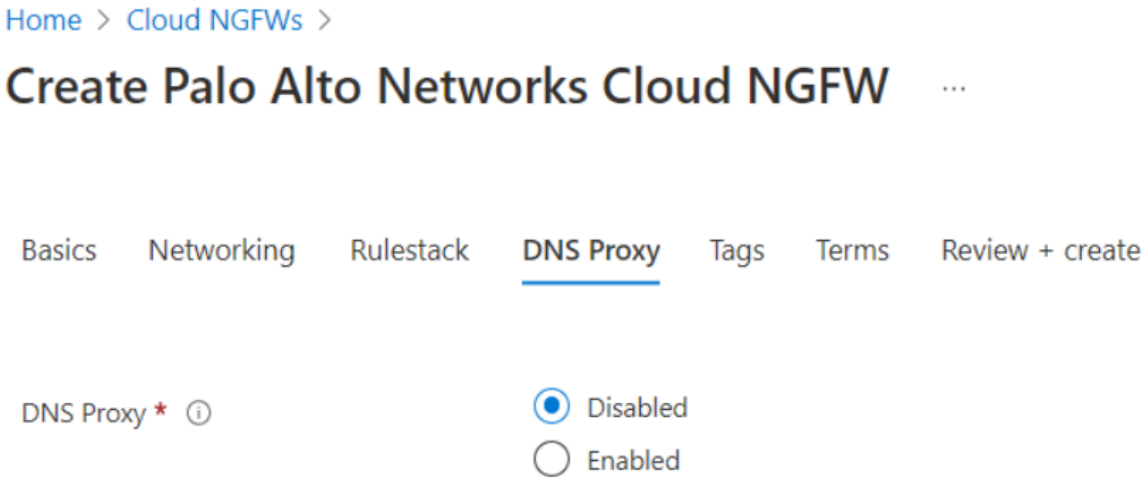


STEP 12 | Cliquez sur **Next: Rulestack (Suivant : Rulestack)** pour créer une rulestack locale où des règles sont définies ; il s'agit d'un espace réservé pour la création de rulestacks locales ; cliquez sur **Create new (Créer)** ou sur **Use existing (Utiliser existante)** (si une rulestack locale existe déjà, sélectionnez-la dans le menu déroulant). Après avoir créé la ressource Cloud NGFW, vous pouvez modifier cette rulestack pour ajouter ou modifier des règles, le FQDN et la liste de préfixes.



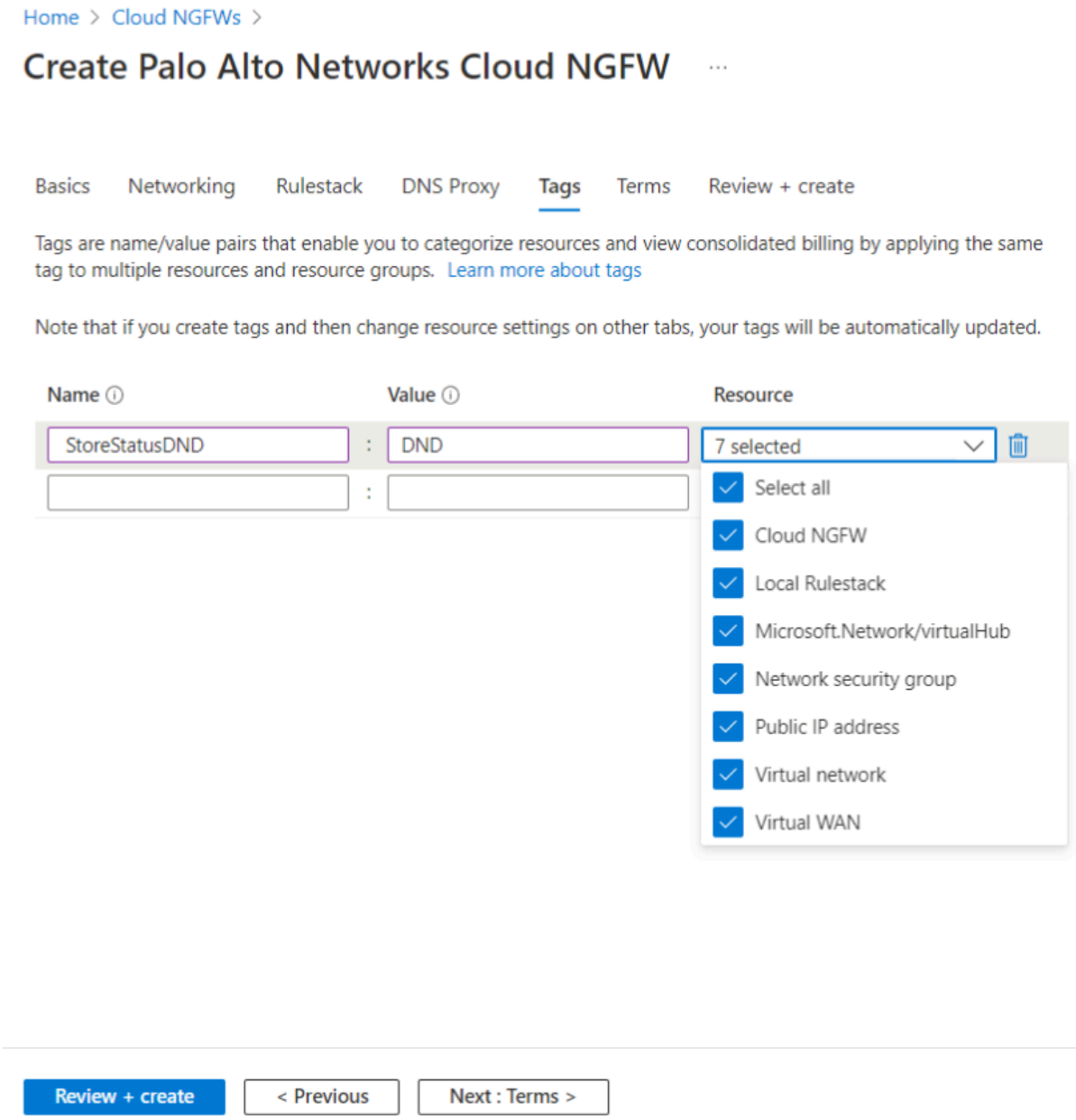
STEP 13 | Cliquez sur **Next: DNS Proxy (Suivant : Proxy DNS)**. Par défaut, DNS Proxy (Proxy DNS) est désactivé. Vous pouvez configurer le Cloud NGFW pour inspecter tout le trafic DNS en agissant

comme proxy pour les ressources vWAN. Une fois configuré, le proxy DNS transfère la requête DNS au serveur DNS Azure par défaut ou à un serveur DNS que vous spécifiez.



STEP 14 | Cliquez sur **Next:Tags (Suivant : Étiquettes)** pour spécifier les étiquettes correspondant à vos exigences Azure. Les étiquettes sont des libellés prédéfinis qui peuvent vous aider à gérer les vulnérabilités de votre environnement et à afficher la facturation consolidée liée à votre

compte Azure. Elles sont déterminées de manière centralisée et peuvent être définies en tant que vulnérabilités et exceptions à la politique.



Les étiquettes sont utilisées comme :

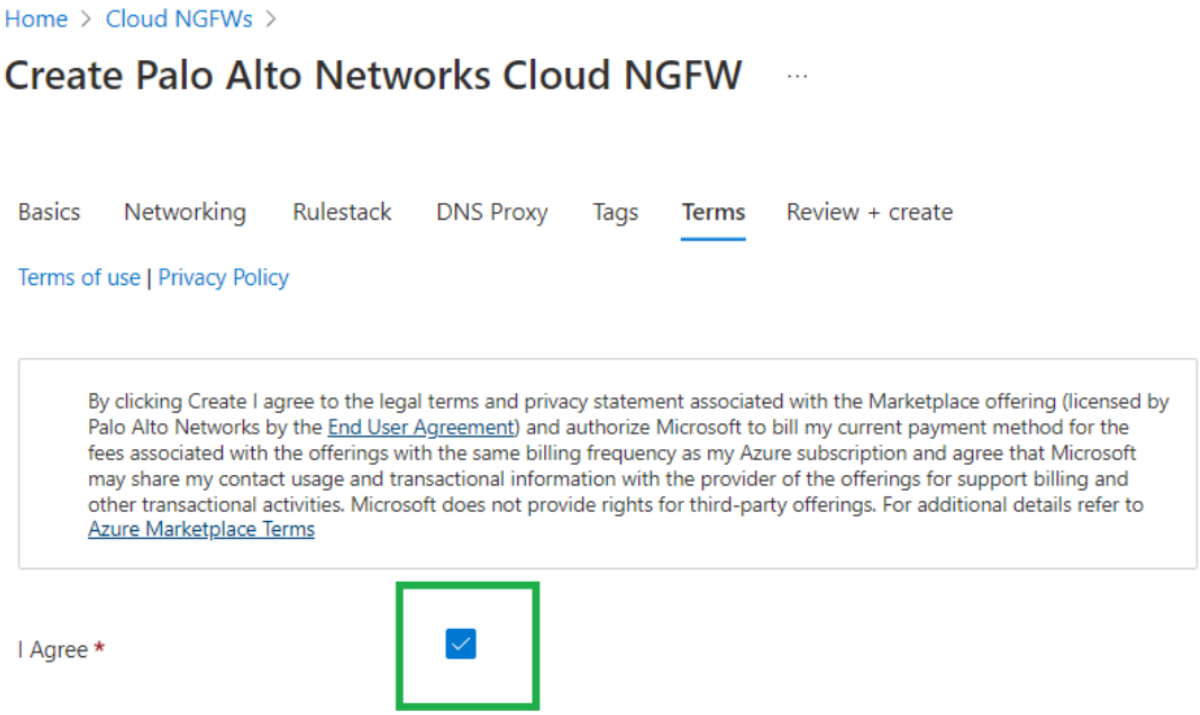
- Libellés de vulnérabilité Elles constituent un moyen pratique de catégoriser les vulnérabilités de votre environnement.
- Exceptions à la politique Elles peuvent faire partie de vos règles afin d'avoir un effet spécifique sur les vulnérabilités étiquetées.
- Affichez la facturation consolidée pour votre compte Azure.

  Les étiquettes sont utiles en cas de grands déploiements de conteneurs avec plusieurs équipes travaillant dans le même environnement. Vous pouvez par exemple avoir plusieurs équipes qui gèrent des types de vulnérabilités différents. Vous pouvez ensuite définir les étiquettes pour définir les responsabilités sur les vulnérabilités. D'autres utilisations seraient de définir l'état de correction de la vulnérabilité, ou de marquer les vulnérabilités à ignorer lorsqu'il s'agit d'un problème connu qui ne peut pas être résolu dans un avenir proche.

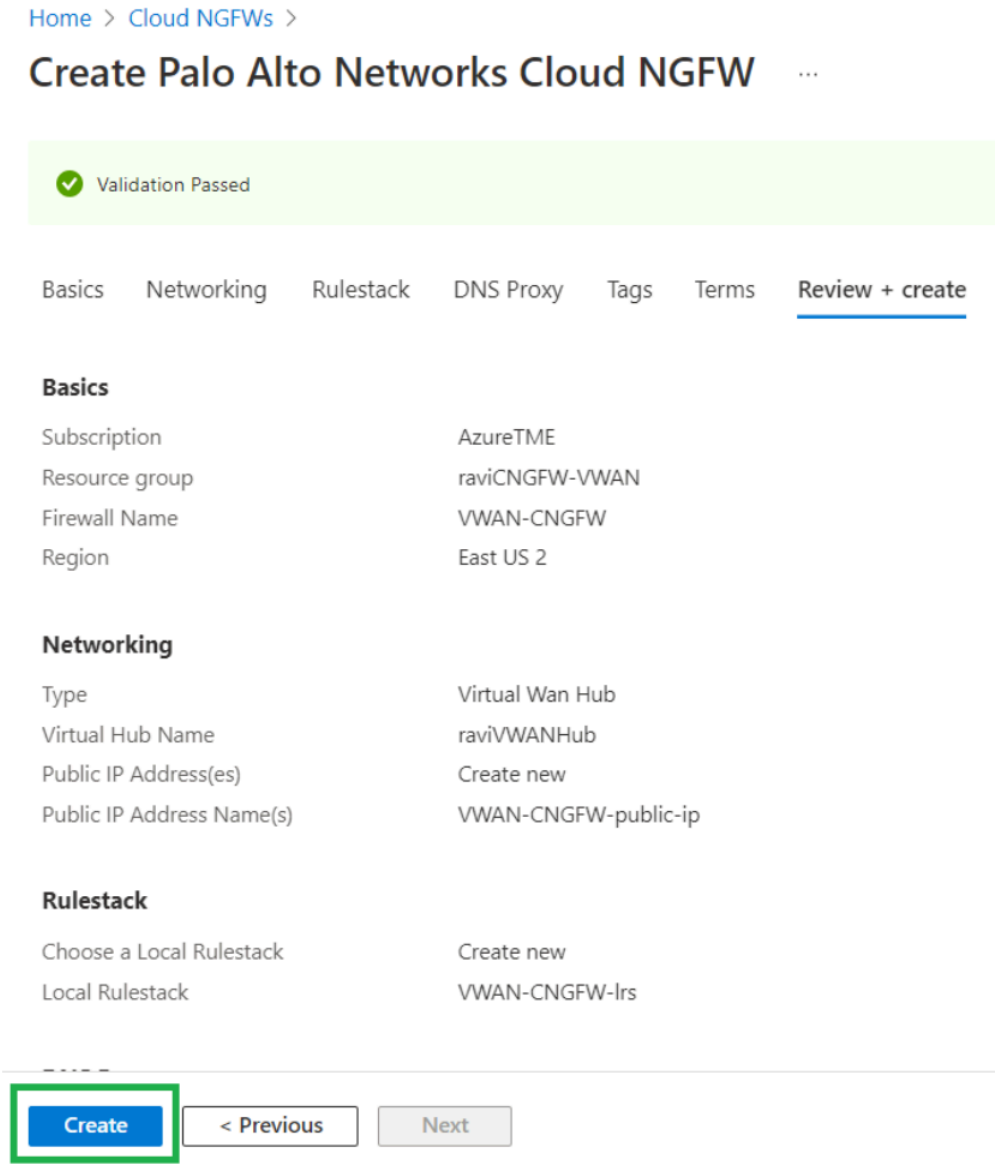
  

  Vous pouvez définir autant d'étiquettes que vous le souhaitez. Pour plus d'informations sur la création d'étiquettes pour votre compte Azure, reportez-vous à la section Utiliser les étiquettes pour organiser vos ressources Azure et votre hiérarchie de gestion.

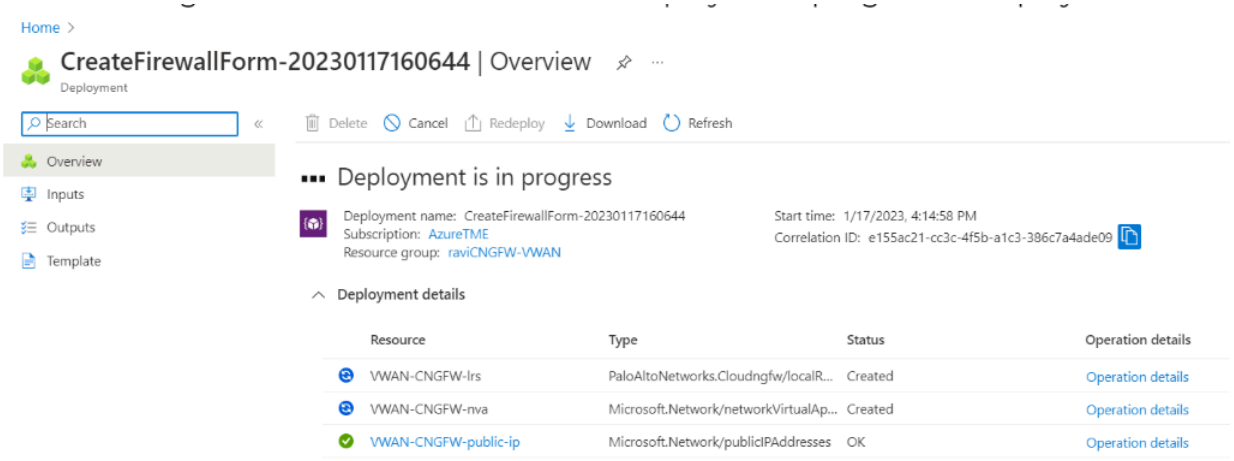
STEP 15 | Cliquez sur **Next:Terms (Suivant : Conditions)** et acceptez les conditions générales de déploiement.



STEP 16 | Cliquez sur **Review + create (Revoir + créer)** pour valider votre abonnement Azure pour la ressource Cloud NGFW. La ressource est d'abord validée, puis créée. L'écran affiche **Validation Passed (Validation réussie)**. Cliquez sur **Create (Créer)** pour déployer le service Cloud NGFW.

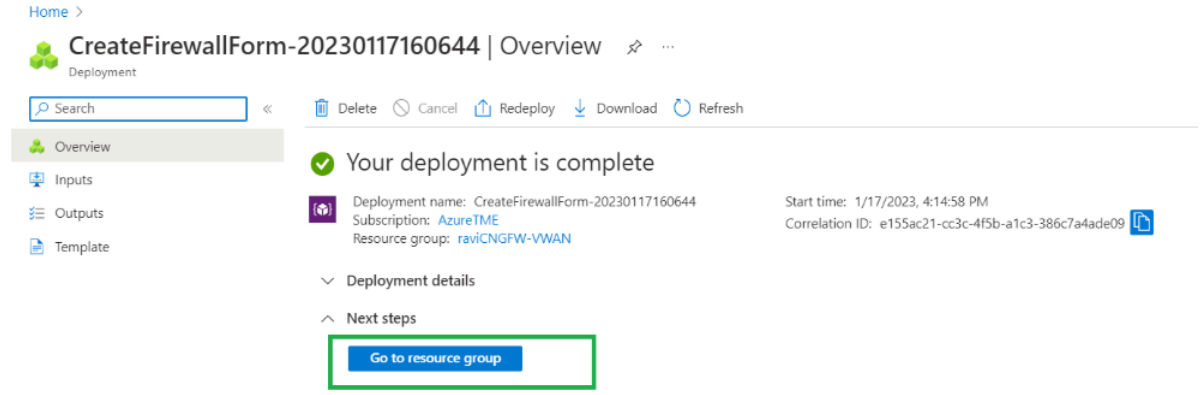


Après avoir créé le service Cloud NGFW, la progression du déploiement s'affiche.

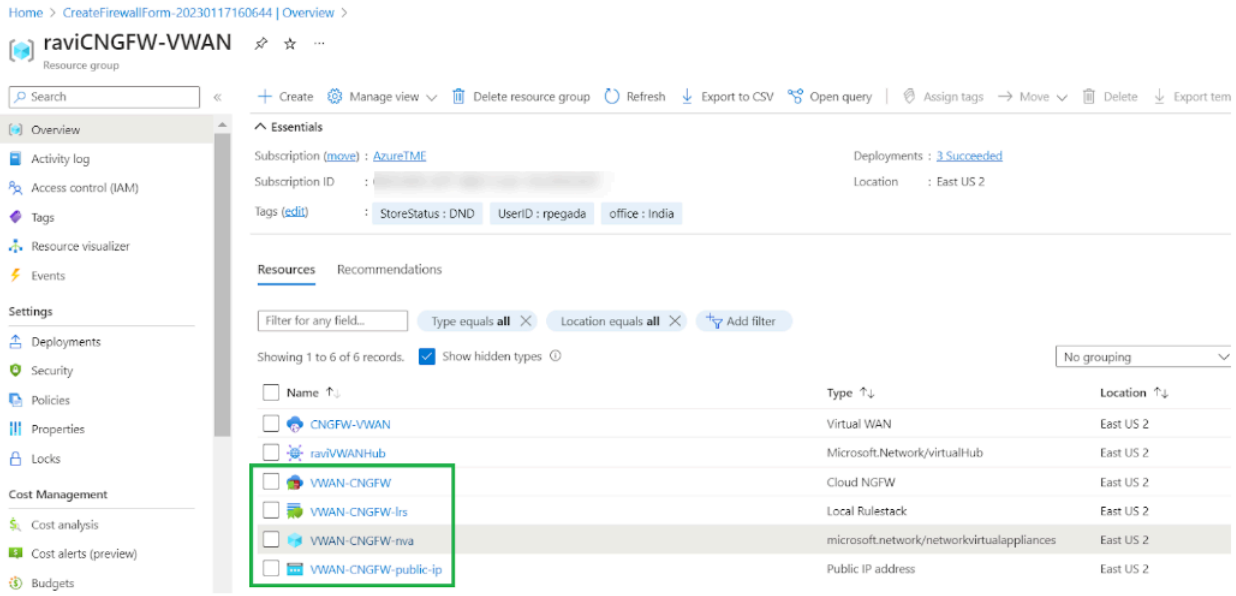


Le déploiement d'une ressource Cloud NGFW prend environ 30 minutes.

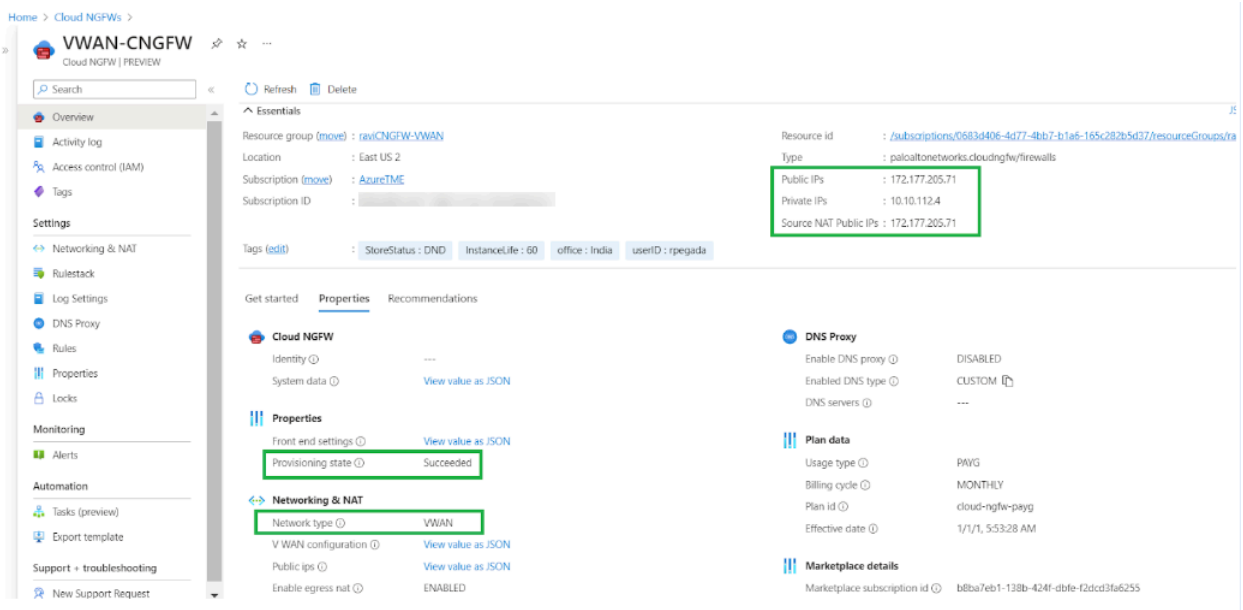
En cas de déploiement réussi, l'écran suivant apparaît.



STEP 17 | Quatre ressources sont créées, dont Cloud NGFW, une rulestack locale, une adresse IP publique et le Cloud-nva.



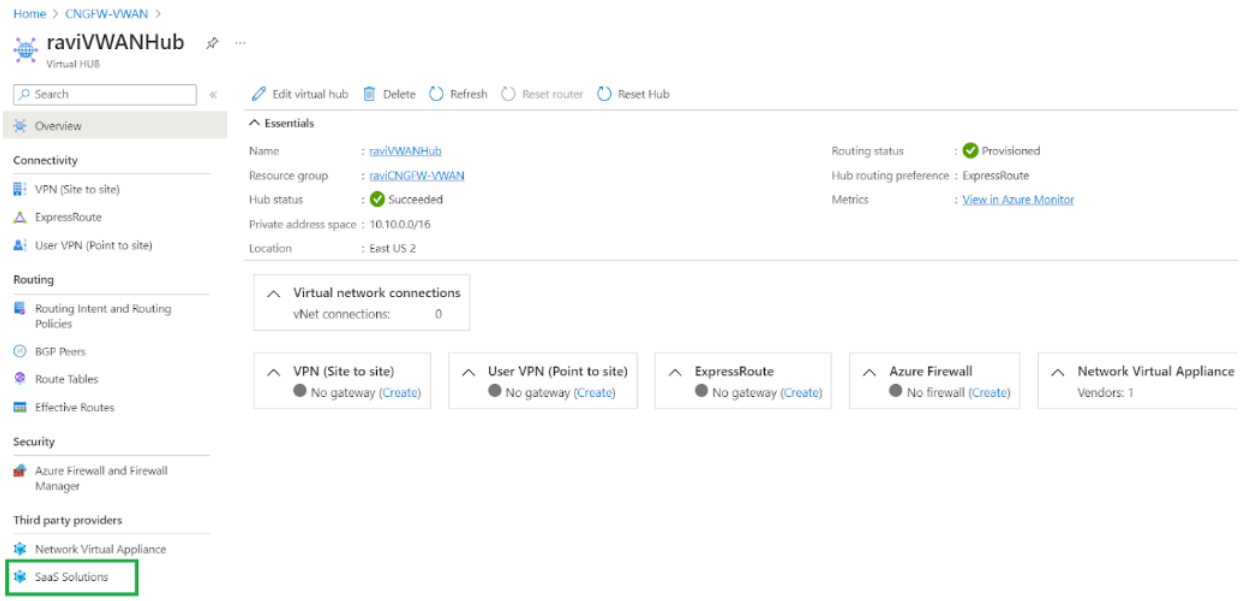
STEP 18 | Une fois la ressource Cloud NGFW créée, sélectionnez-la pour vérifier que l'état de provisionnement indique Succeeded (Réussi). Cette page affiche également les adresses IP publiques et privées associées au service Cloud NGFW. Assurez-vous que le type de réseau est vWAN.



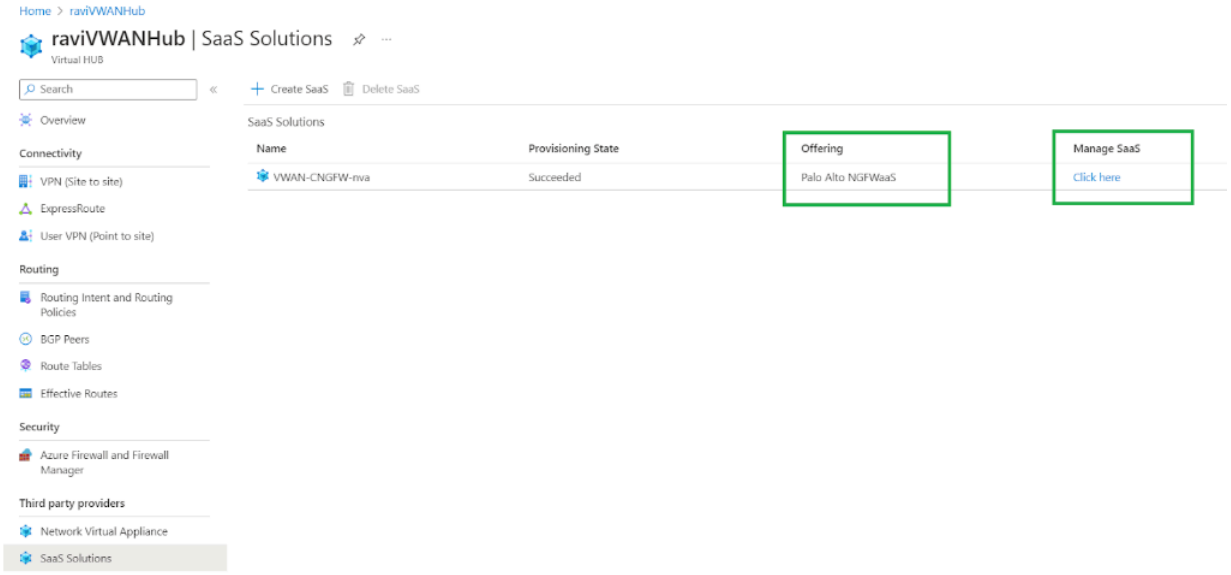
Vérifier le déploiement du Cloud NGFW dans un vWAN

Après avoir créé le service Cloud NGFW pour le type de réseau vWAN, vérifiez que le Cloud NGFW a été ajouté en tant que solution SaaS pour le vWAN.

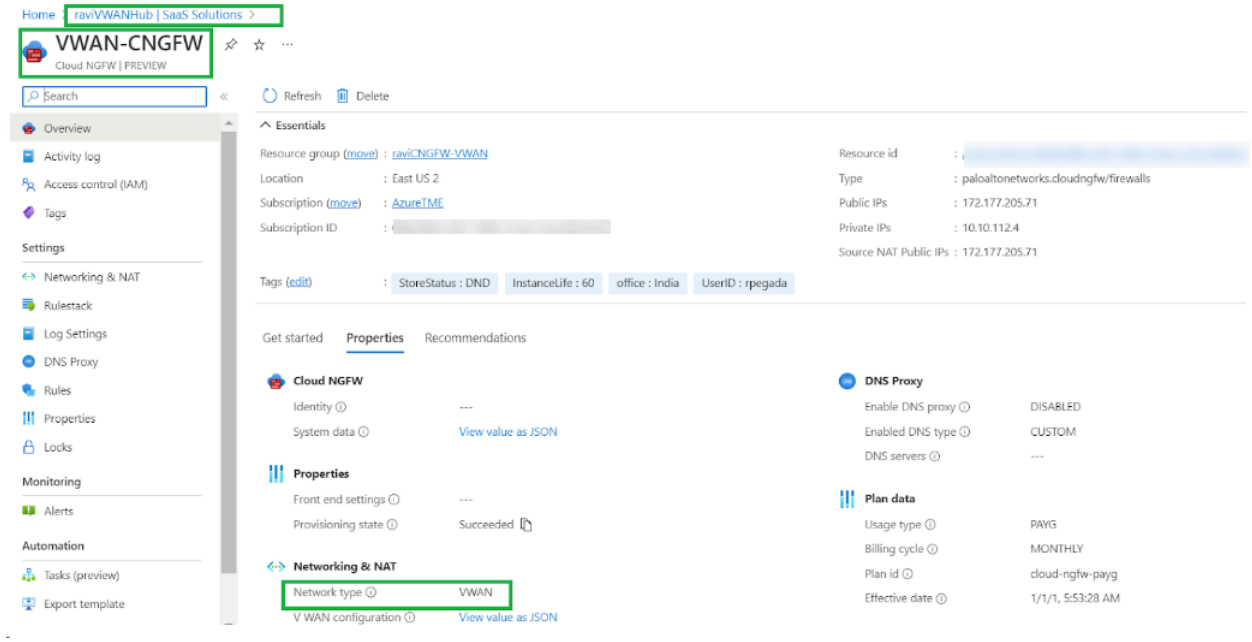
STEP 1 | Accédez au hub virtuel qui a été utilisé lors de la création du service Cloud NGFW. Dans la section **Third party providers (Fournisseurs tiers)**, cliquez sur **SaaS Solutions (Solutions SaaS)**.



STEP 2 | Vérifiez que le Cloud NGFW a été créé ; il est ajouté comme solution SaaS à ce hub. Dans la section **SaaS Solutions (Solutions SaaS)**, sélectionnez **Click here (Cliquez ici)**.



Les informations relatives au déploiement vWAN apparaissent.



Exemple de configuration pour le déploiement après le vWAN

Après le déploiement

Après avoir vérifié le déploiement, effectuez les tâches suivantes :

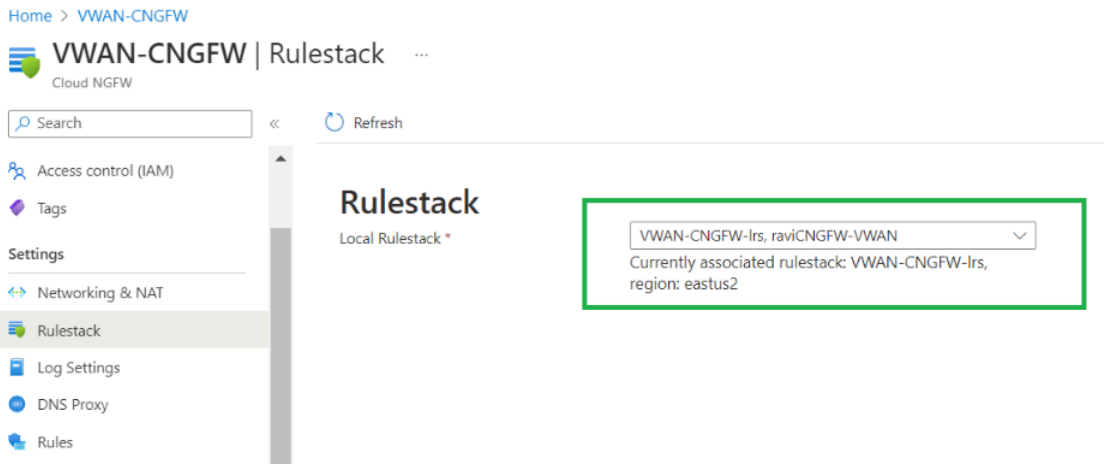
- Créer ou mettre à jour une rulestack
- Règle NAT source/de destination sur le Cloud NGFW
- Configurer la journalisation

- Ajouter des vNET d’application en tant que connexions de réseaux virtuels au WAN virtuel
- Configurer l’intention de routage du hub vWAN et les politiques de routage

Créer ou mettre à jour une rulestack

Pour mettre à jour une rulestack existante :

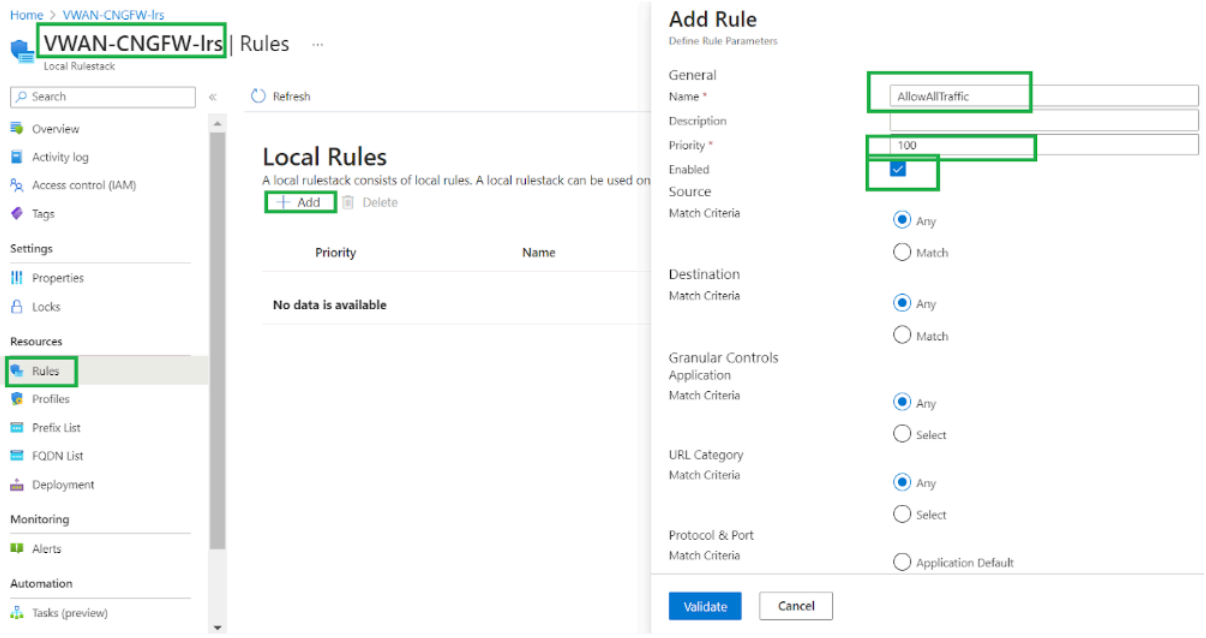
STEP 1 | Dans la console Azure Resource Manager (ARM), cliquez sur **Rulestacks** pour la ressource Cloud NGFW que vous souhaitez configurer. La rulestack associée au service Cloud NGFW apparaît, ainsi que le groupe de ressources.



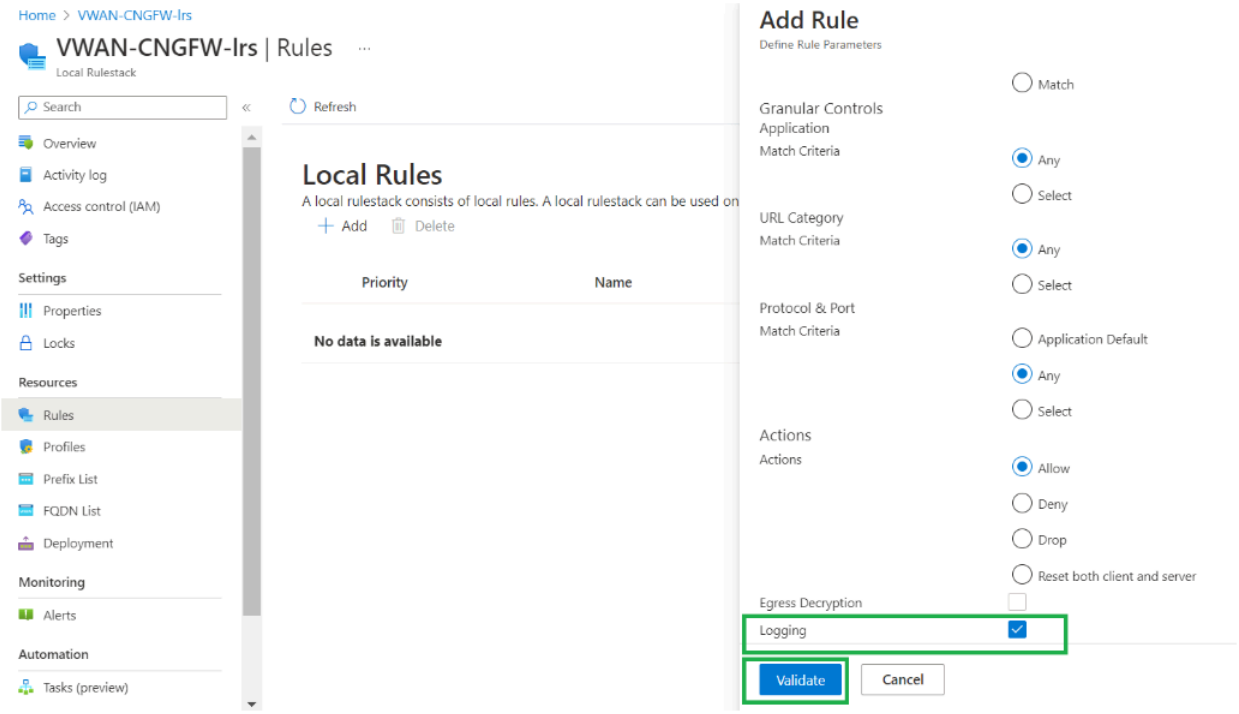
STEP 2 | Modifiez la rulestack pour ajouter des règles de pare-feu. Ces règles autorisent un certain trafic tout en bloquant un trafic spécifique. Par défaut, Cloud NGFW bloque tout le trafic. Recherchez la rulestack locale que vous avez créée précédemment à l’aide de l’option de recherche globale fournie par le portail Azure.

STEP 3 | Sélectionnez la rulestack locale créée précédemment associée à votre abonnement Cloud NGFW, puis sélectionnez **Rules (Règles)**.

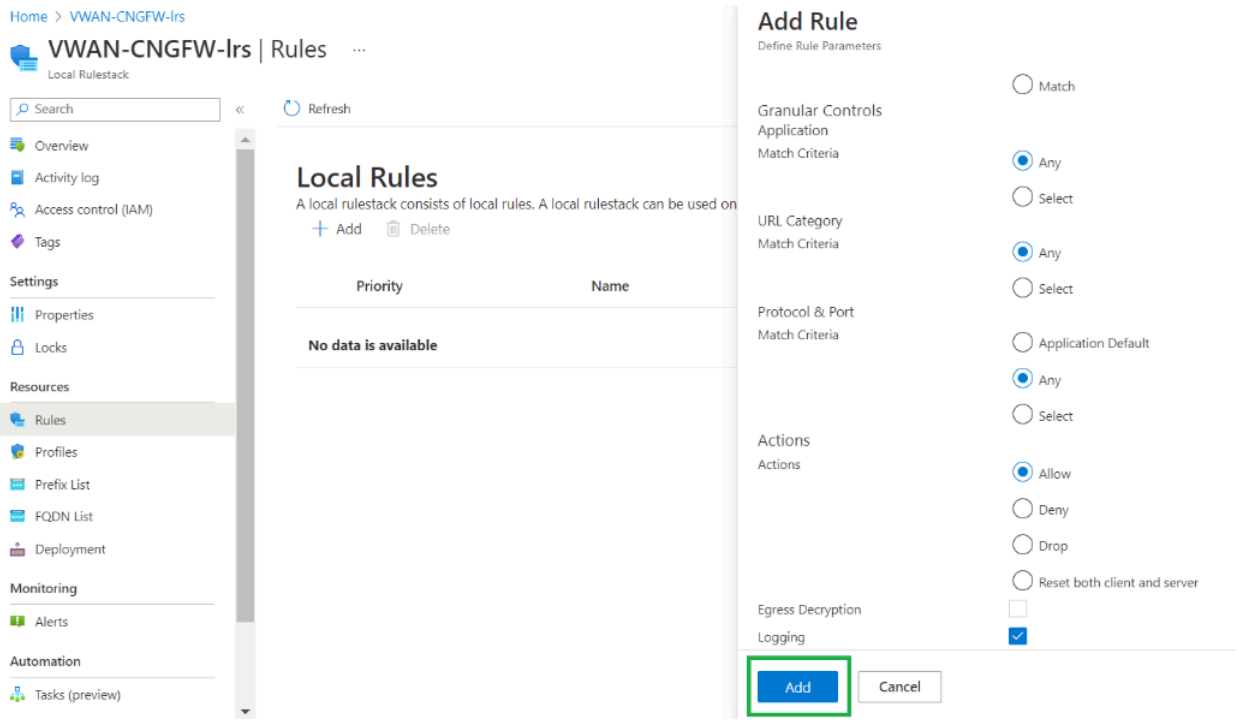
STEP 4 | Dans la section **Local Rules (Règles locales)** , cliquez sur **Add (Ajouter)**. Dans la fenêtre **Add Rule (Ajouter une règle)**, modifiez les règles. Par exemple, ajoutez une règle qui autorise le trafic ; remplissez les champs obligatoires et utilisez les paramètres par défaut pour les champs restants.



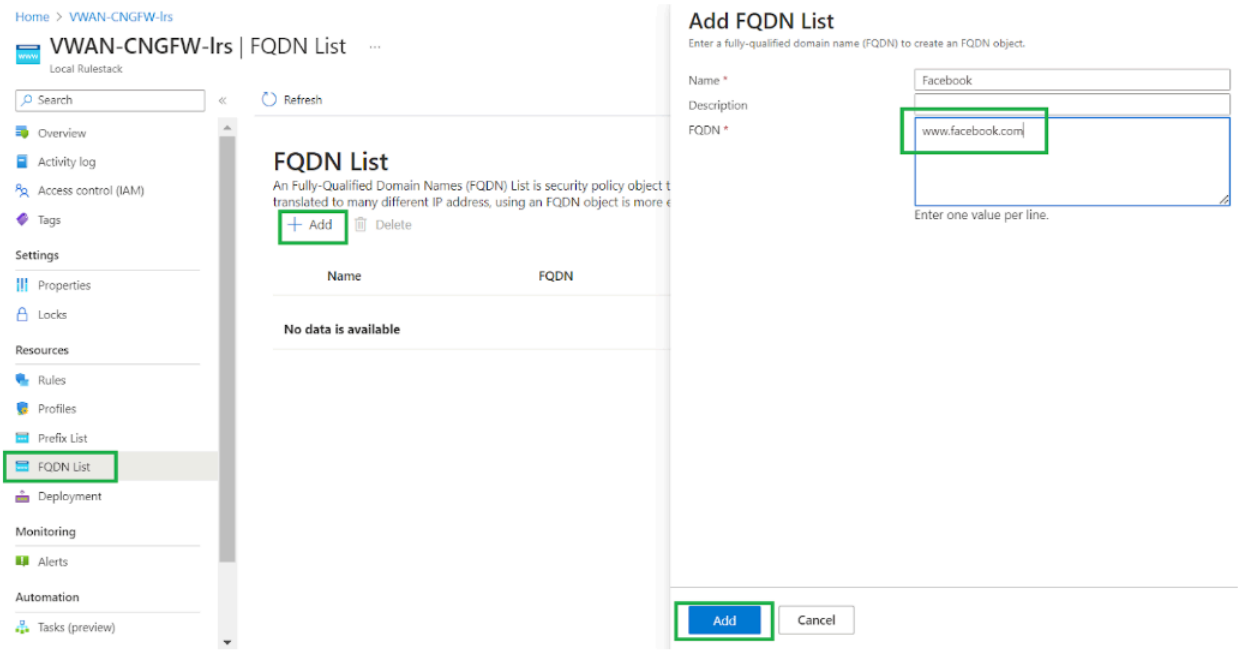
STEP 5 | Activez la journalisation pour la règle. Dans la fenêtre Add Rule (Ajouter une règle), sélectionnez **Logging (Journalisation)**.



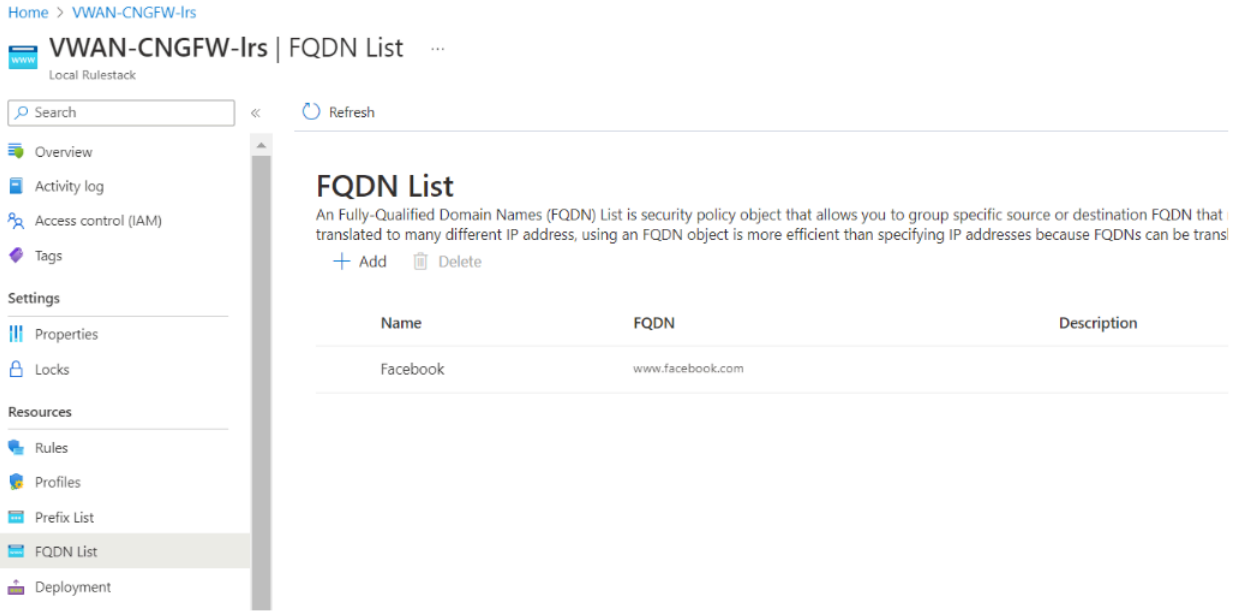
STEP 6 | Cliquez sur **Validate (Valider)**, puis sur **Add (Ajouter)** pour ajouter la règle à la rulestack.



STEP 7 | Ajoutez une **liste FQDN** qui spécifie une URL, puis indiquez une action à entreprendre. Par exemple, vous pouvez appliquer une action à la règle FQDN pour abandonner le trafic tentant d'accéder à l'URL www.facebook.com.



Vérifiez que l'URL que vous avez saisie apparaît dans la liste FQDN.

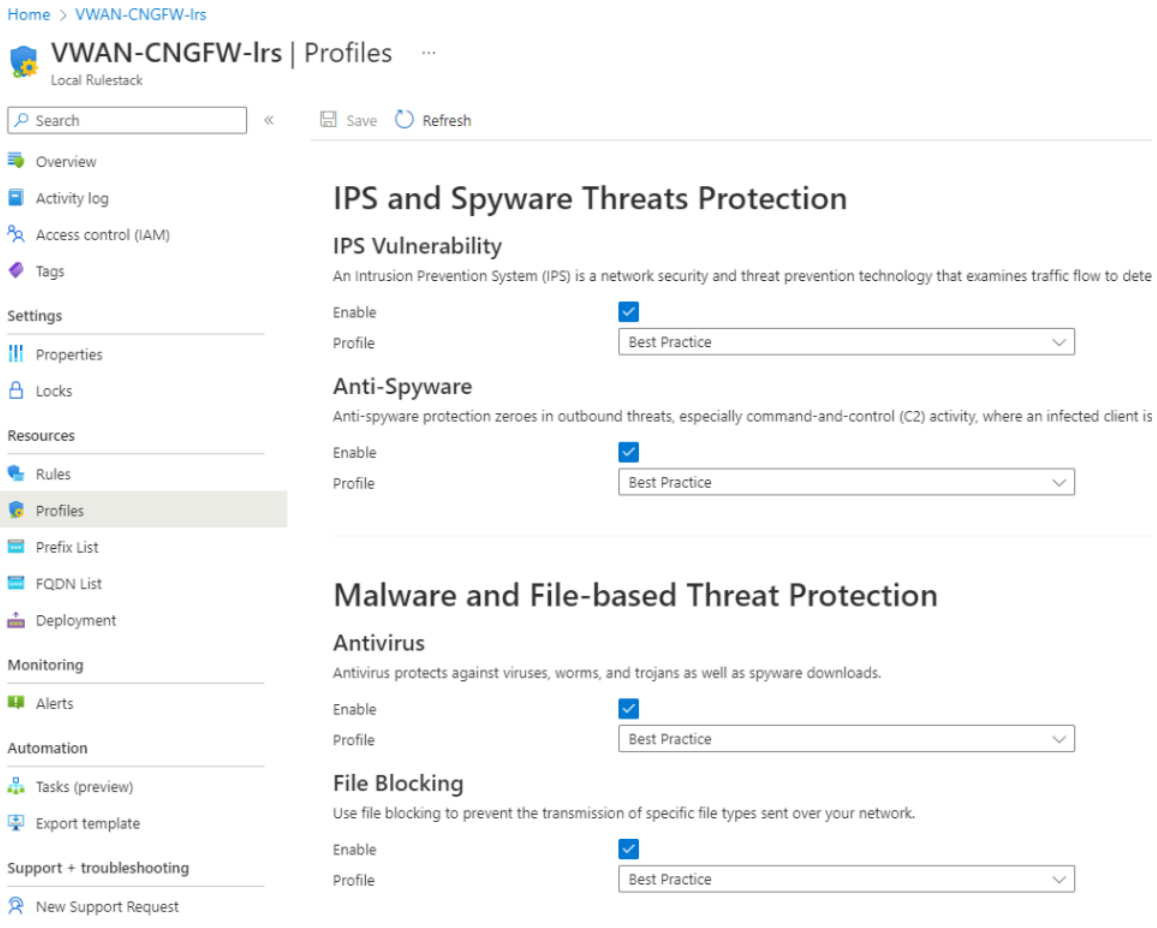


STEP 8 | Revenez à la page de configuration des **règles** et ajoutez une règle qui correspond à la liste FQDN nouvellement créée. Définissez l'action sur **Drop (Abandonner)**le trafic.

Les deux règles apparaissent sur la page des règles locales.

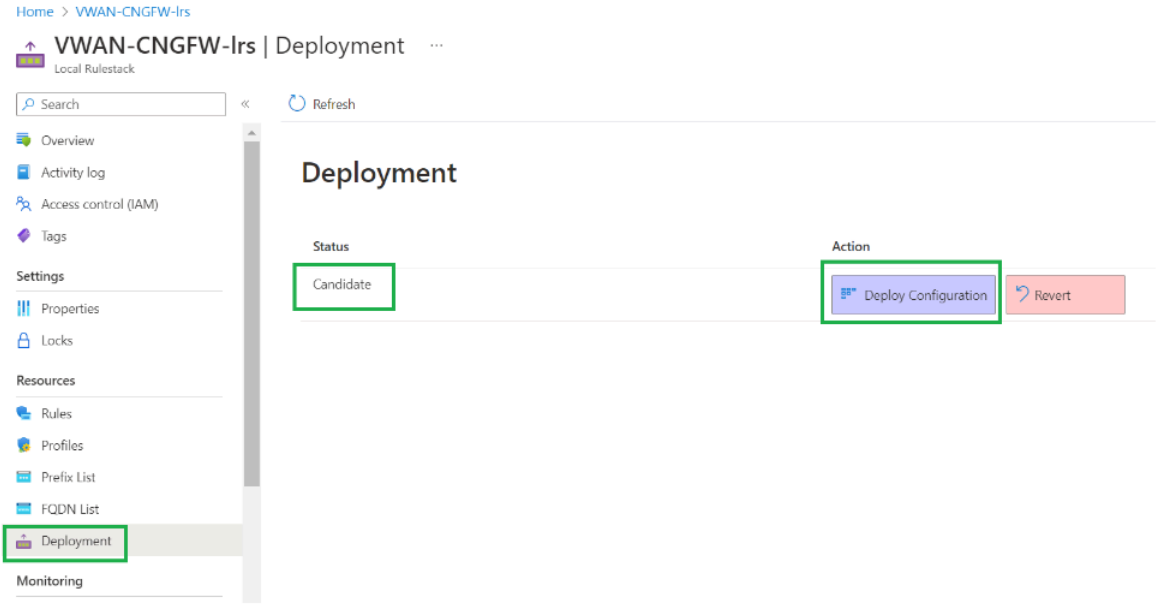
STEP 9 | Dans le cadre du service Cloud NGFW, les profils de sécurité sont activés avec les configurations des meilleures pratiques par défaut. Le trafic est sécurisé avec les meilleurs profils de sécurité lorsque

vous démarrez et déployez le service. Sélectionnez **Profiles (Profils)** pour afficher ces profils de sécurité.

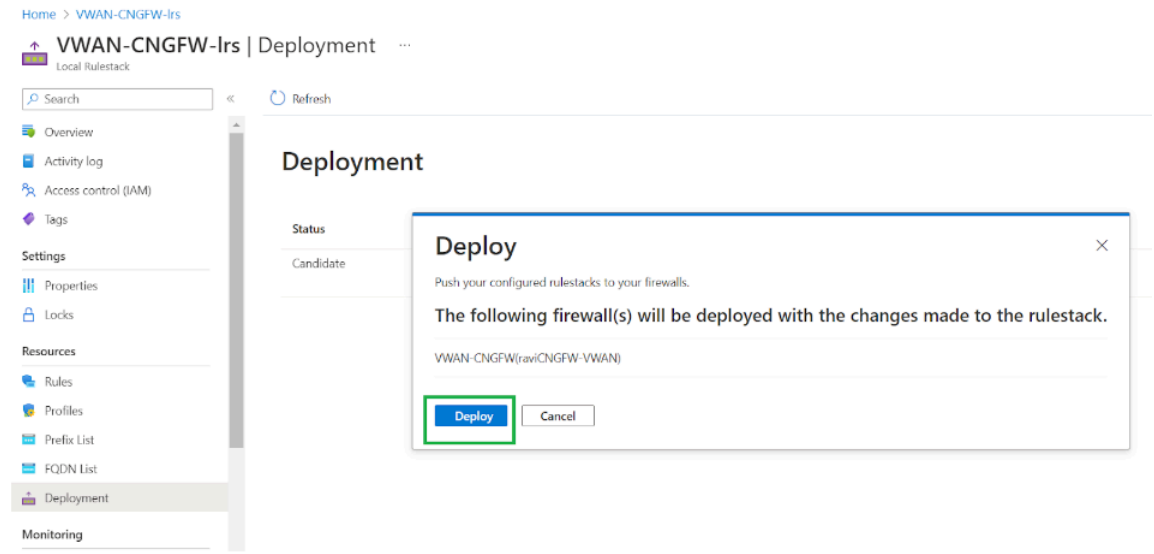


STEP 10 | Après avoir modifié les règles, déployez-les sur la rulestack locale associée au service Cloud NGFW. Cliquez sur **Deployment (Déploiement)**. L'état de déploiement **Candidate (Candidat)** apparaît ; cela signifie que la configuration a été définie, mais pas encore déployée. Cliquez sur **Deploy**

Configuration (Déployer la configuration) pour déployer la configuration sur le service Cloud NGFW. **Vous devez effectuer cette étape pour déployer la rulestack**.



STEP 11 | Après avoir cliqué sur **Deploy Configuration (Déployer la configuration)**, un message affiche les pare-feu associés à la rulestack. Cliquez sur **Deploy (Déployer)** pour configurer cette rulestack sur tous les pare-feu associés à l'aide de la rulestack.



Une fois la configuration déployée, l'écran affiche l'état Running (En cours) pour le déploiement (le Cloud NGFW et la rulestack locale sont correctement déployés).

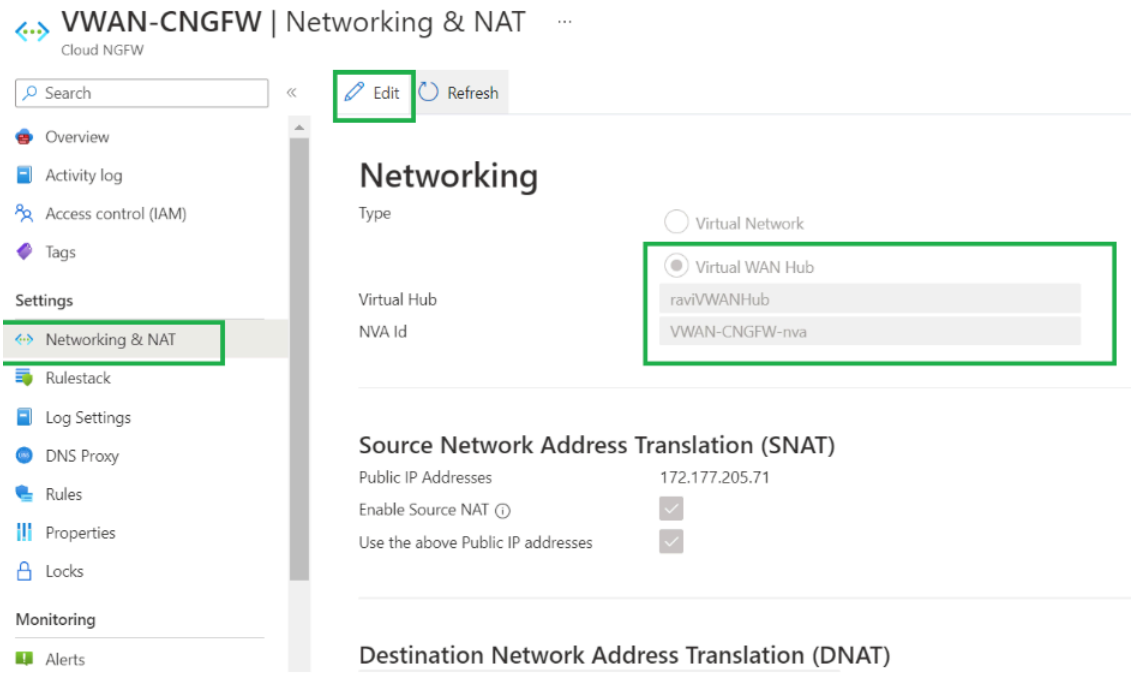
Règle NAT source/de destination sur le Cloud NGFW

Configurez une règle NAT de destination avec une configuration frontale sur le Cloud NGFW pour diriger le trafic entrant vers une application sur le vWAN.

STEP 1 | Accédez à l'écran des paramètres **Networking & NAT (Mise en réseau et NAT)** pour la ressource Cloud NGFW. Dans cet écran, déterminez si le type de réseau est **Virtual WAN Hub (Hub WAN**

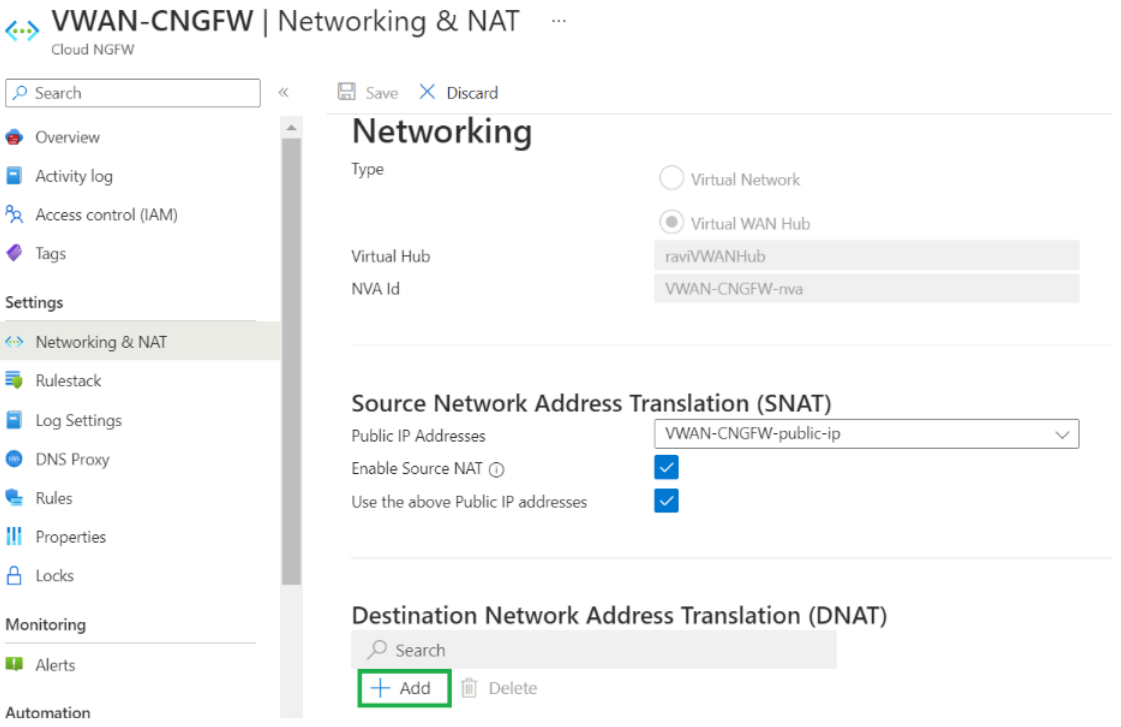
virtuel) et l'état du champ **Source NAT (NAT source)** (activé ou désactivé) ; si ce dernier a été activé, cela apparaît sur cet écran.

STEP 2 | Cliquez sur **Edit (Modifier)** pour ajouter la règle NAT de destination.



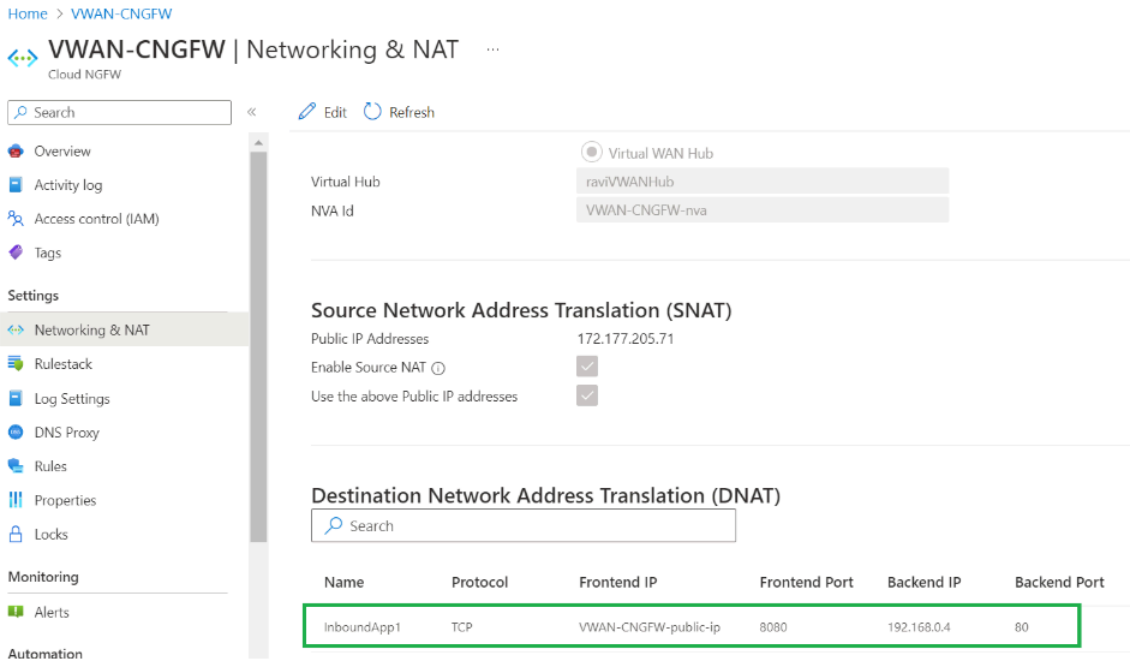
STEP 3 | **Ajoutez** une règle NAT de destination pour la configuration frontale. L'adresse IP frontale représente l'adresse IP publique associée au Cloud NGFW. Utilisez le menu déroulant pour sélectionner l'adresse.

STEP 4 | Ajoutez des informations sur les paramètres frontaux à la règle, puis cliquez sur **Add (Ajouter)**.



Une fois la règle NAT de destination ajoutée, cliquez sur Save (Enregistrer) pour déployer la configuration sur la ressource Cloud NGFW.

Après avoir enregistré la configuration, le champ Destination Network Address Translation (DNAT) (Traduction d'adresse réseau de destination (DNAT)) affiche les mises à jour ; l'adresse http://frontendIP:8080 est redirigée vers l'application notée sur le port spécifié via le Cloud NGFW ; le trafic entrant circule désormais via le Cloud NGFW.



Configurer la journalisation

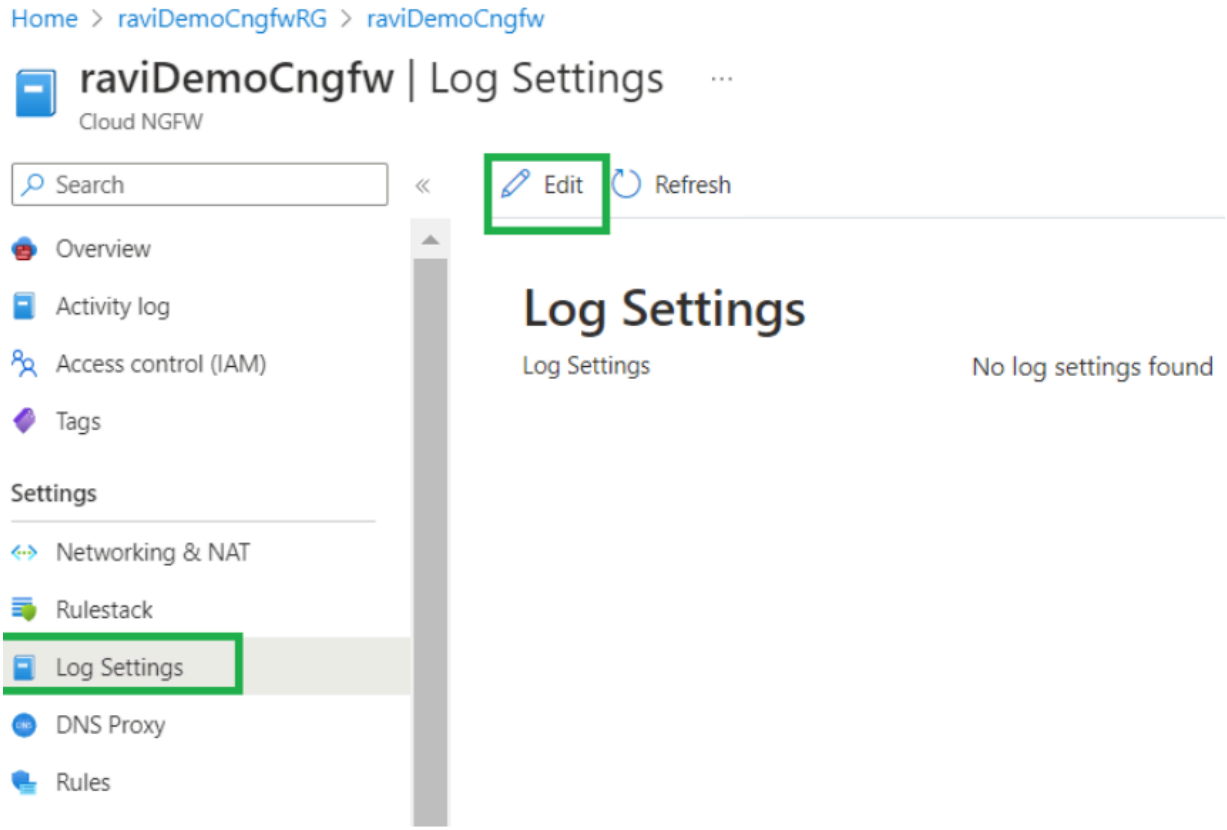
Avant de configurer la journalisation sur le Cloud NGFW, créez l'espace de travail **Log Analytics** sur Azure.

STEP 1 | Dans le portail Azure, recherchez l'**espace de travail Azure Log Analytics**. Cliquez sur **Log Analytics Workspaces (Espaces de travail Log Analytics)** pour l'ajouter en tant que service.

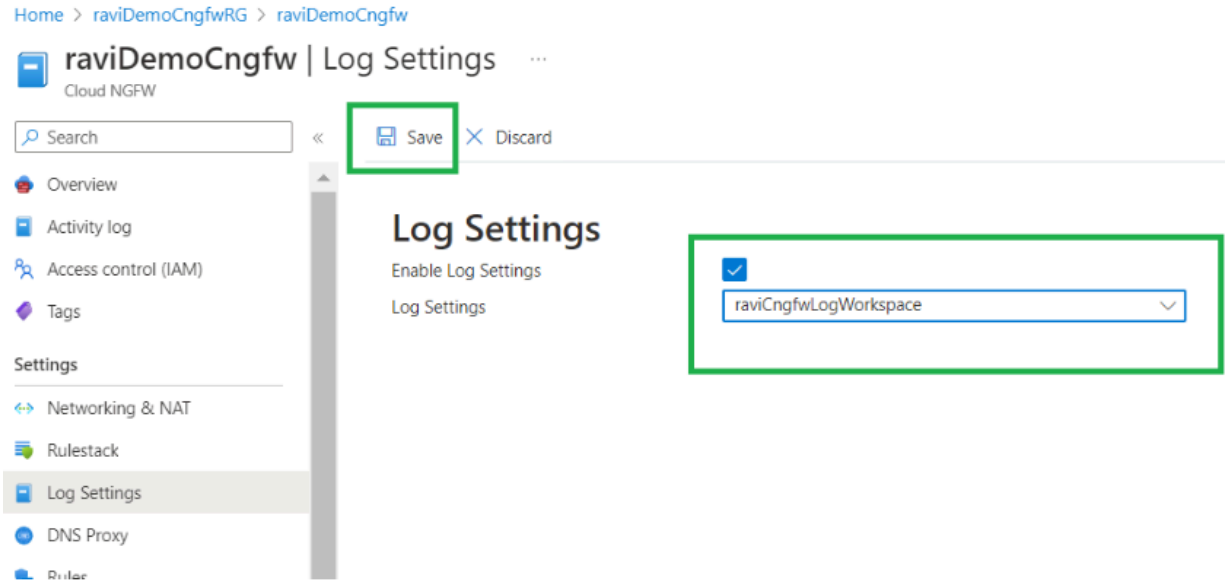
STEP 2 | Cliquez sur **Create (Créer)** pour établir un nouvel espace de travail **Log Analytics**.

STEP 3 | Dans l'espace de travail Log Analytics ainsi créé, fournissez les détails de l'**instance**. Sélectionnez le **Nom** de l'espace de travail dans le menu déroulant et spécifiez la **Region (Région)**.

STEP 4 | Configurez les paramètres du journal dans la ressource Cloud NGFW. Sélectionnez **Log Settings (Paramètres du journal)**. Cliquez sur **Edit (Modifier)**.



STEP 5 | Dans le champ **Log Settings (Paramètres du journal)**, sélectionnez l’espace de travail Log Analytics créé précédemment, puis cliquez sur **Save (Enregistrer)**.

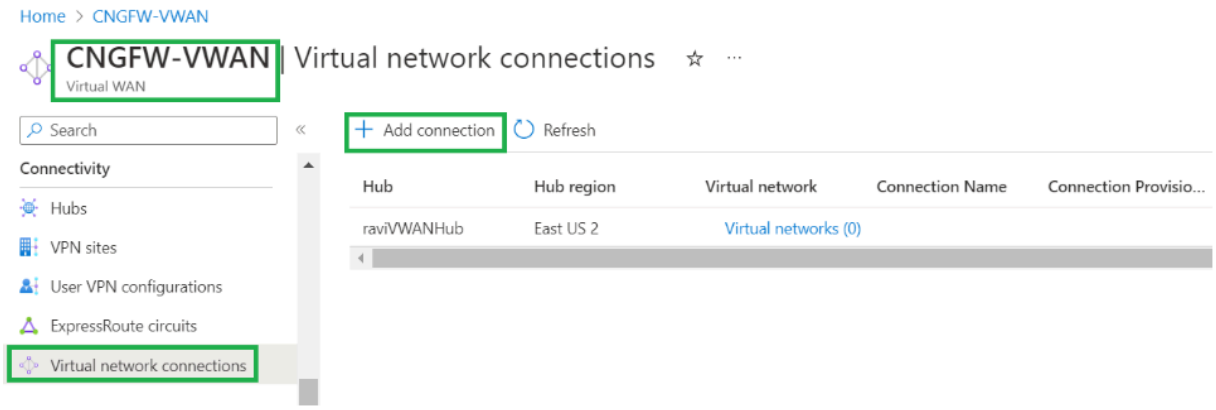


Ajouter des vNET d’application en tant que connexions de réseaux virtuels au WAN virtuel

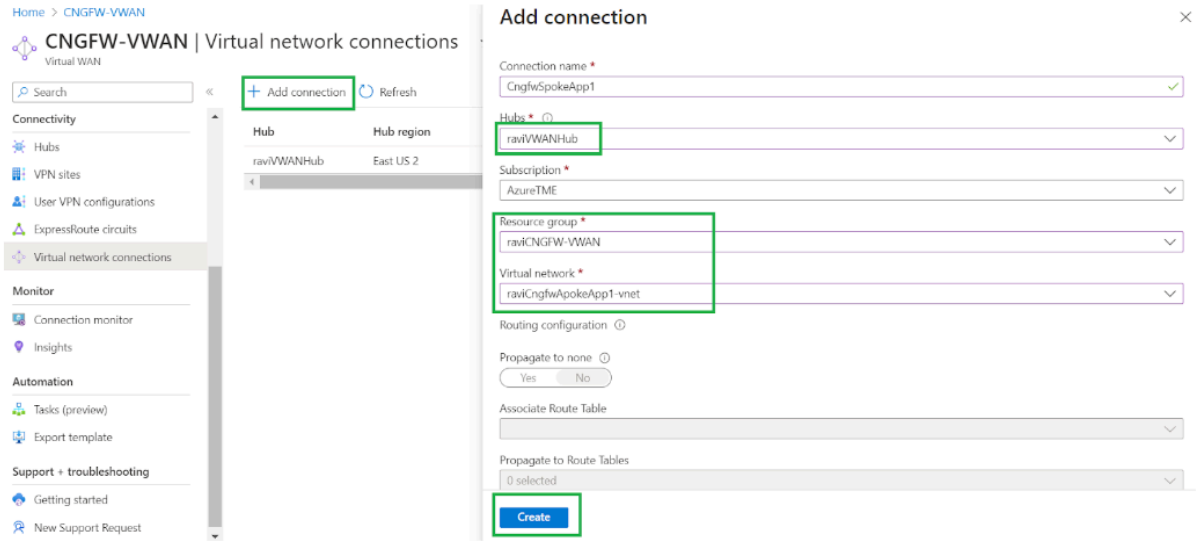
Ajoutez un vNET d’application en tant que connexion de réseau virtuel au hub WAN virtuel.

STEP 1 | Dans votre ressource vWAN, sélectionnez **Virtual Network Connections (Connexions réseau virtuel)**.

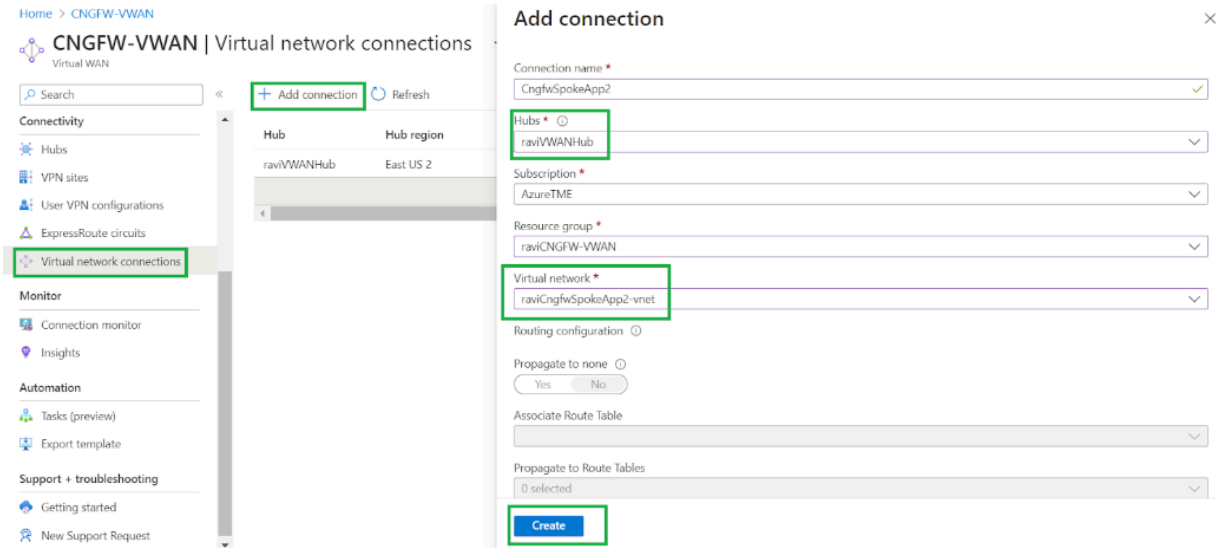
STEP 2 | Cliquez sur **Add connection (Ajouter une connexion)**.



STEP 3 | Sélectionnez le vNET que vous souhaitez configurer comme **réseau virtuel**, puis cliquez sur **Create (Créer)**.



STEP 4 | Sélectionnez un autre vNET pour le deuxième réseau virtuel, puis cliquez sur **Create (Créer)**.



STEP 5 | Après avoir connecté les réseaux virtuels au hub virtuel, vérifiez que l'état est **Connected (Connecté)**.

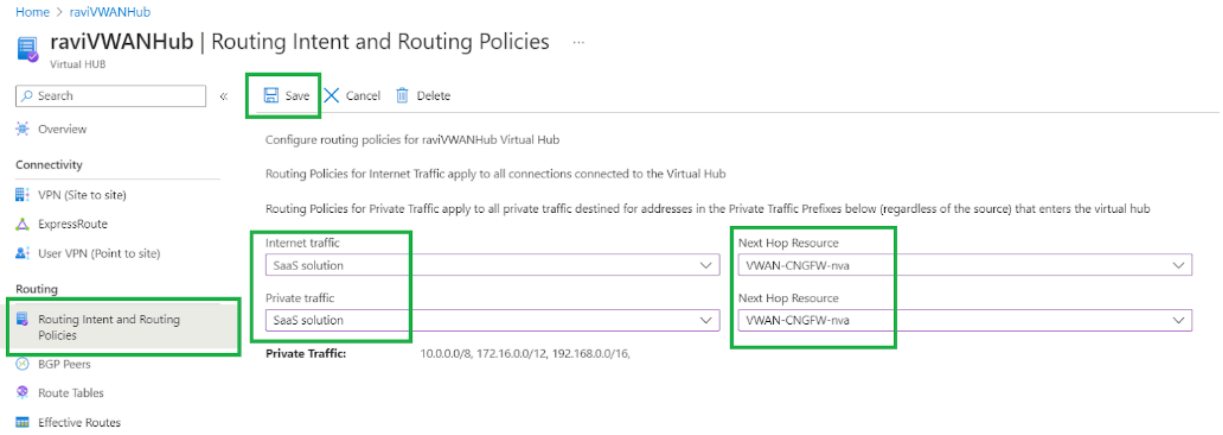
Configurer l'intention de routage du hub vWAN et les politiques de routage

Les politiques de routage dans le hub WAN virtuel sont utilisées pour acheminer le trafic via le service Cloud NGFW. Pour acheminer le trafic lié à Internet et le trafic privé (« spoke to spoke »), vous devez configurer le tronçon suivant en tant que vWAN Cloud NGFW.

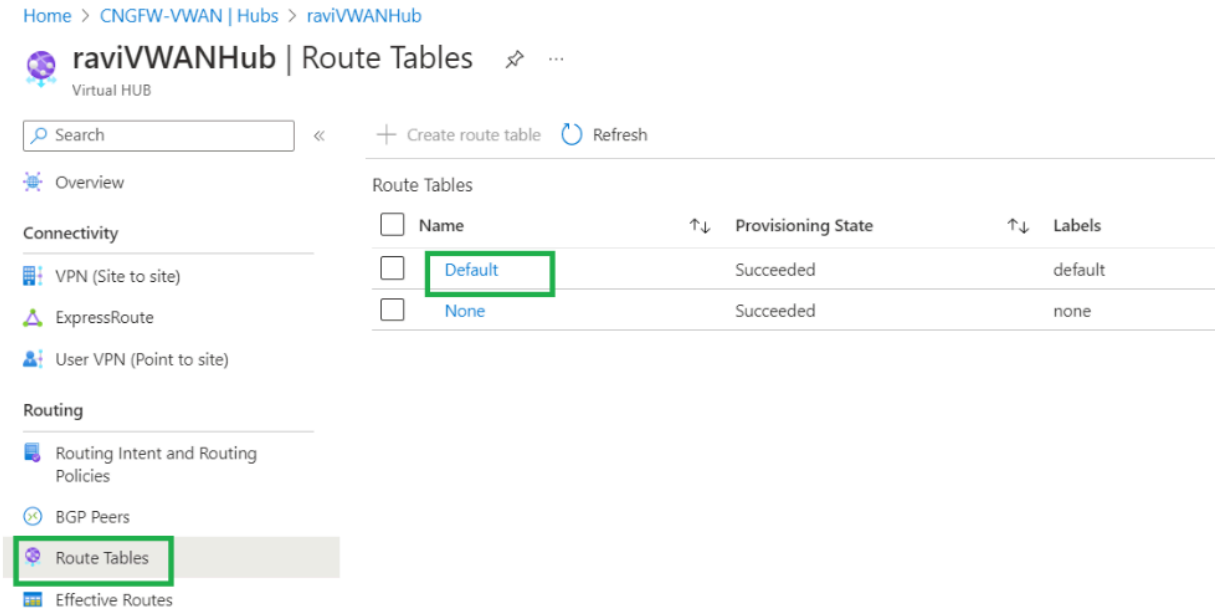
L'intention de routage vWAN, les politiques de routage et les fonctionnalités SaaS sont actuellement développées par Microsoft pour le portail Azure. La date de disponibilité visée pour chaque région où Cloud NGFW est disponible est le mardi 9 mai 2023.

STEP 1 | Dans votre ressource vWAN, sélectionnez **Routing Intent and Routing Policies (Intention de routage et politiques de routage)**.

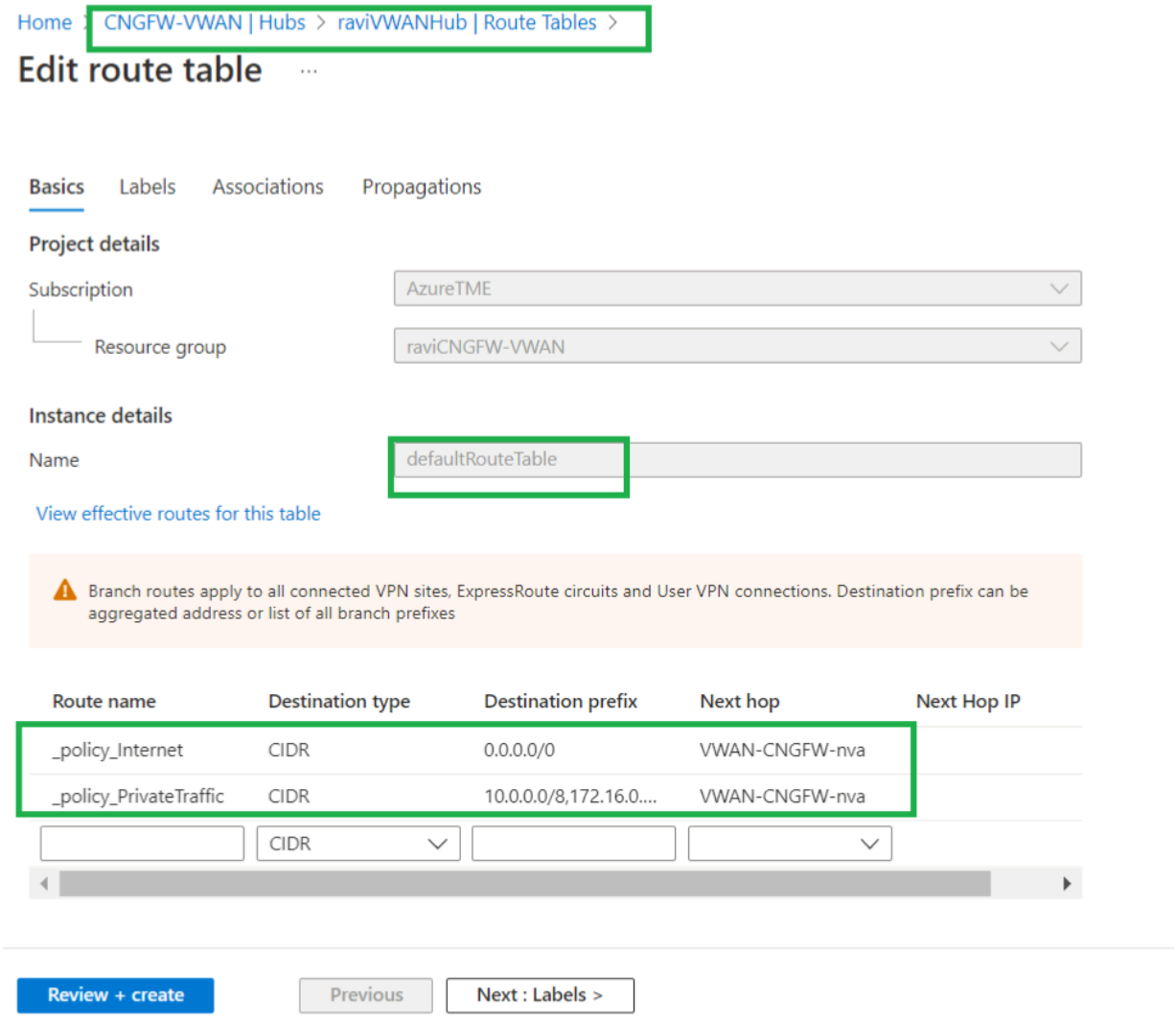
STEP 2 | Sélectionnez le trafic Internet et la ressource du tronçon suivant dans les menus déroulants, puis cliquez sur **Save (Enregistrer)**.



STEP 3 | Après avoir configuré les politiques de routage, vérifiez que la table de routage a été mise à jour pour acheminer le trafic via Cloud NGFW. Cliquez sur **Routing Tables (Tables de routage)** et sélectionnez **Default (Par défaut)** dans la section **Routing Tables (Tables de routage)**.



Vous pouvez **modifier** la table de routage afin de fournir des détails relatifs aux itinéraires associés à la table de routage par défaut. Le trafic sortant vers Internet ou vers d'autres vNET est acheminé via le Cloud NGFW.



STEP 4 | Sélectionnez un autre vNET pour le deuxième réseau virtuel, puis cliquez sur **Create (Créer)**.

STEP 5 | Après avoir connecté les réseaux virtuels au hub WAN virtuel, vérifiez que l'état est **Connected (Connecté)**.

Gestion native des politiques Cloud NGFW à l’aide de rulestacks

Sur Cloud NGFW, vous définissez des règles de politique de sécurité et les regroupez dans une rulestack.

À propos des rulestacks et des règles sur Cloud NGFW pour Azure

Les rulestacks définissent le contrôle d’accès (App-ID, filtrage des URL) et le comportement de prévention des menaces des ressources Cloud NGFW. Une ressource Cloud NGFW utilise vos définitions de rulestack pour protéger le trafic par un processus en deux étapes. Tout d'abord, il applique vos règles pour autoriser ou refuser votre trafic. Deuxièmement, elle effectue une inspection du contenu sur le trafic autorisé en fonction de ce que vous spécifiez sur les profils de sécurité. Une rulestack inclut un ensemble de règles de sécurité, d’objets associés et de profils.

Une rulestack locale se compose de règles locales utilisées pour définir des règles pour des applications ou des utilisateurs spécifiques. L’administrateur du compte associe ces règles à une ressource NGFW pour le compte Azure.

Créer une rulestack sur Cloud NGFW pour Azure

Dans le client Cloud NGFW, vous pouvez créer des rulestacks si le rôle **LocalRuleStackAdmin** vous est attribué.

Effectuez la procédure suivante pour créer une rulestack.

STEP 1 | Cliquez sur l’icône **Local Rulestack (Rulestack locale)** de la page d’accueil de Microsoft Azure. Vous pouvez également accéder à la rulestack souhaitée depuis la barre de recherche de la page d’accueil.

STEP 2 | Cliquez sur **Create (Créer)**.

STEP 3 | Choisissez **Subscription (Abonnement)** et **Resource Group (Groupe de ressources)** dans les listes déroulantes respectives de la section Project details (Détails du projet) de l’onglet **Basics (Base)**.

STEP 4 | Saisissez un **Name (Nom)** descriptif pour votre rulestack.

STEP 5 | Saisissez la **Region (Région)** prise en charge pour votre rulestack.

STEP 6 | Cliquez sur l’onglet **Tags (Étiquettes)**.

1. Saisissez le **Name (Nom)** et la **Value (Valeur)**.
2. Cliquez sur **Review+create (Revoir + créer)**.

STEP 7 | Revoyez les options de la rulestack que vous avez sélectionnées et cliquez sur **Create (Créer)**.

Objets de règle de sécurité Cloud NGFW pour Azure

Un objet de règle de sécurité est un objet unique ou une unité collective qui regroupe des identités discrètes comme des adresses IP, un nom de domaine complet (FQDN) ou des certificats. En général, lors de la création d’un objet de politique, vous regroupez les objets nécessitant des autorisations similaires dans la politique. Par exemple, si votre organisation utilise un ensemble d’adresses IP de serveur pour authentifier les utilisateurs, vous pouvez regrouper cet ensemble en tant qu’objet de liste de préfixes et faire référence à cette liste de préfixes dans une ou plusieurs règles de sécurité. L’objet Group vous permet de réduire considérablement la charge administrative lors de la création de règles.

- Listes de **préfixes** et de **FQDN** : les listes de préfixes et de FQDN vous permettent de regrouper des adresses IP ou des FQDN source ou de destination spécifiques qui nécessitent la même application de politique. Une liste de préfixes peut contenir une ou plusieurs adresses IP ou masques réseau IP en notation CIDR. Avec un objet d’adresse de type IP Netmask (masque réseau IP), vous devez saisir l’adresse IP ou le réseau à l’aide de la notation contenant des barres obliques pour indiquer le réseau IPv4. Par exemple, 192.168.18.0/24. Un objet FQDN (par exemple, paloaltonetworks.com) facilite l’utilisation, car DNS fournit la résolution du FQDN en adresses IP. Vous n'avez donc pas à connaître les adresses IP et à les charger manuellement chaque fois que le FQDN se résout en de nouvelles adresses IP.
- **Certificat** : un objet certificat est une référence à un certificat TLS stocké dans le Azure Key Vault dans votre compte Azure qui est utilisé dans le décryptage sortant.

Veillez à utiliser PAN-OS version 11.0.x lorsque vous utilisez Azure Key Vault pour le décryptage sortant.

Créer une liste de préfixes sur Cloud NGFW pour Azure

Une liste de préfixes vous permet de regrouper des adresses IP spécifiques nécessitant l’application d’une politique identique. Une liste de préfixes peut contenir une ou plusieurs adresses IP ou masques réseau IP en notation CIDR. Avec un objet d’adresse de type IP Netmask (Masque réseau IP), vous devez saisir l’adresse IP ou le réseau à l'aide de la notation contenant des barres obliques pour indiquer le réseau IPv4. Par exemple, 192.168.18.0/24.

STEP 1 | Cliquez sur l’icône **Local Rulestacks (Rulestacks locales)** sur la page d’accueil et sélectionnez une rulestack précédemment créée sur laquelle vous souhaitez configurer une liste de préfixes.

STEP 2 | Cliquez sur **Prefix List (Liste de préfixes)** dans le volet de gauche et cliquez sur **Add (Ajouter)**. Le volet Ajouter une liste de préfixes s’ouvre.

STEP 3 | Saisissez un **Name (Nom)** descriptif pour votre liste de préfixes.

STEP 4 | (facultatif) Saisissez une description pour votre liste de préfixes.

STEP 5 | Entrez une ou plusieurs adresses dans **Address (Adresse)**. Vous pouvez entrer des adresses IP ou des masques réseau IP au format CIDR et une valeur par ligne.

STEP 6 | Cliquez sur **Add (Ajouter)**.

Créer une liste FQDN pour Cloud NGFW sur Azure

Un objet FQDN (par exemple, paloaltonetworks.com) facilite l’utilisation, car DNS fournit la résolution du FQDN en adresses IP. Vous n'avez donc pas à connaître les adresses IP et à les charger manuellement chaque fois que le FQDN se résout en de nouvelles adresses IP.

STEP 1 | Cliquez sur l’icône **Local Rulestacks (Rulestacks locales)** sur la page d’accueil et sélectionnez une rulestack précédemment créée sur laquelle vous souhaitez configurer la liste FQDN.

STEP 2 | Cliquez sur **FQDN List (Liste FQDN)** dans le volet de gauche et cliquez sur **Add (Ajouter)**. Le volet Ajouter une liste FQDN s’ouvre.

STEP 3 | Saisissez un **Name (Nom)** descriptif pour votre liste FQDN.

STEP 4 | (facultatif) Entrez une description pour votre liste FQDN.

STEP 5 | Entrez un ou plusieurs **FQDN**, un par ligne.

STEP 6 | Cliquez sur **Add (Ajouter)**.

Ajouter un certificat à Cloud NGFW pour Azure

Cloud NGFW utilise des certificats pour permettre le décryptage sortant. Ces certificats sont stockés dans Azure Key Vault.

Seuls les certificats auto-signés et signés par la CA racine sont actuellement pris en charge pour le décryptage. Les certificats chaînés ne sont pas pris en charge.

Veillez à utiliser PAN-OS version 11.0.x lorsque vous utilisez Azure Key Vault pour le décryptage sortant.

STEP 1 | Cliquez sur l'icône des **rulestacks locales** de la page d'accueil et sélectionnez une rulestack précédemment créée sur laquelle vous souhaitez créer un certificat.

STEP 2 | Cliquez sur **Certificates (Certificats)** dans le volet de gauche et cliquez sur **Add (Ajouter)**. Le volet Add Certificate List (Ajouter une liste de certificats) s'ouvre.

STEP 3 | Saisissez un **Name (Nom)** descriptif pour votre certificat.

STEP 4 | (facultatif) Saisissez une description pour votre certificat.

STEP 5 | Si le certificat est auto-signé, cochez **Self-signed Certificate (Certificat auto-signé)**.

STEP 6 | Si le certificat n'est pas auto-signé, obtenez l'URI du certificat en accédant à **Azure Key Vault** > **Certificates (Certificats)** et copiez-collez l'URI de l'identifiant secret dans **l'URI du certificat**.

STEP 7 | (facultatif) Dans le champ **Certificate source (Source du certificat)**, choisissez l'option correspondante : **Select from Key vault (Sélectionner dans le coffre de clés)** ou **Paste URI (Coller l'URI)**.

STEP 8 | Cliquez sur **Add (Ajouter)**.

STEP 9 | Créez une identité gérée dans le même groupe de ressources que le coffre de clés. Reportez-vous à la section Créer une identité gérée par l'utilisateur.

STEP 10 | Accédez à **Azure Key Vault**> **Access Policies (Politiques d'accès)**.

STEP 11 | Cliquez sur **Create (Créer)** pour configurer une politique d'accès qui affecte l'**Agent des certificats Key Vault** et l'**Utilisateur des secrets Key Vault** à l'identité gérée créée à l'**étape 9**.

Créer des règles de sécurité sur Cloud NGFW pour Azure

Les règles de sécurité protègent les actifs du réseau des menaces et des défaillances et permettent d’optimiser l’allocation des ressources du réseau afin d’améliorer la productivité et l’efficacité des processus métier. Sur Cloud NGFW pour Azure, des règles de sécurité individuelles déterminent s’il faut bloquer ou autoriser une session en fonction des attributs de trafic, tels que l’adresse IP source et de destination, les FQDN source et de destination ou l’application.

Tout le trafic passant par le pare-feu est mis en correspondance avec une session et chaque session avec une règle. Lorsqu'une correspondance de session se produit, NGFW applique la règle correspondante au trafic bidirectionnel (du client vers le serveur et du serveur vers le client) dans cette session. Pour le trafic qui ne correspond à aucune règle définie, les règles par défaut s'appliquent.

Les règles de politique de sécurité sont évaluées de gauche à droite et de haut en bas. Une correspondance est établie entre un paquet et la première règle répondant aux critères définis et, après avoir déclenché une correspondance, les règles suivantes ne sont pas évaluées. Par conséquent, les règles les plus spécifiques doivent précéder les plus génériques afin d'appliquer les meilleurs critères de correspondance.

Après avoir créé une rulestack, vous pouvez maintenant créer des règles et les ajouter à votre rulestack.

STEP 1 | Cliquez sur l’icône des **rulestacks locales** de la page d’accueil et sélectionnez une rulestack précédemment créée sur laquelle vous souhaitez ajouter des règles.

STEP 2 | Cliquez sur **Rules (Règles)**, puis cliquez sur **Add (Ajouter)**.

STEP 3 | Dans la section General (Général), saisissez un **Name (Nom)** descriptif pour votre règle.

STEP 4 | (Facultatif) Saisissez une **Description** de votre rôle.

STEP 5 | Définissez la **Rule Priority (Priorité de la règle)**.

La priorité des règles détermine l'ordre dans lequel les règles sont évaluées. Les règles avec une priorité inférieure sont évaluées en premier. De plus, chaque règle dans une rulestack.

STEP 6 | Par défaut, la règle de sécurité est **Enabled (Activée)**. Décochez **Enabled (Activée)** pour désactiver la règle. Vous pouvez activer ou désactiver une règle à tout moment.

STEP 7 | Définissez la **Source**.

1. Sélectionnez **Any (N’importe laquelle)**, **Match (Correspondance)**ou **Exclude (Exclure)**.

   La sélection de **Any (N'importe laquelle)** signifie que le trafic est évalué par rapport à la règle, quelle que soit la source.
2. Si vous sélectionnez **Match (Correspondance)**, spécifiez l’adresse IP (CIDR), la liste des préfixes, les pays, les flux intelligents ou la liste des préfixes dynamiques.

STEP 8 | Définissez la **Destination**.

1. Sélectionnez **Any (N’importe laquelle)**, **Match (Correspondance)**ou **Exclude (Exclure)**.

   Si vous sélectionnez **Any (N'importe laquelle)**, le trafic est évalué par rapport à la règle, quelle que soit la destination.
2. Si vous sélectionnez **Match (Correspondance)**, spécifiez la liste des préfixes, la liste des FQDN et les pays.

STEP 9 | Définissez le contrôle granulaire.

1. Choisissez **Any (N'importe lequel)** ou **Select (Sélectionner)**.

   Lorsque vous choisissez **Any (N'importe lequel)**, le trafic est évalué quelle que soit l'application. Si vous spécifiez une ou plusieurs applications, le trafic est évalué par rapport à la règle si le trafic correspond à l'application spécifiée.
2. Si vous choisissez **Select (Sélectionner)**, spécifiez les applications.

STEP 10 | Définissez le contrôle granulaire pour **URL Category (Catégorie d'URL)**.

1. Choisissez **Any (N'importe lequel)** ou **Select (Sélectionner)**.

   Lorsque vous choisissez **Any (N'importe laquelle)**, le trafic est évalué quelle que soit l'URL.
2. Si vous choisissez **Select (Sélectionner)**, choisissez l’une des **catégories prédéfinies** dans la liste déroulante.

STEP 11 | Définissez le contrôle granulaire pour **Port & Protocol (Port et protocole)**.

1. Choisissez **application-default**, **Any (N’importe laquelle)** ou **Select (Sélectionner)**.

   Si vous choisissez **Any (N’importe laquelle)**, le trafic est évalué quels que soient le port et le protocole. Si vous spécifiez un port et un protocole, le trafic est évalué par rapport à la règle si le trafic correspond au port et au protocole spécifiés.
2. Si vous choisissez **Select (Sélectionner)**, sélectionnez le protocole dans la liste déroulante et saisissez le numéro de port. Vous pouvez spécifier un seul numéro de port.

STEP 12 | Définissez les **Actions**.

1. Définissez l’action que le pare-feu entreprend lorsque le trafic correspond à la règle :**Allow (Autoriser)**, **Deny (Refuser)**, **Drop (Abandonner)** ou **Reset both client and server (Réinitialiser le client et le serveur)**.
2. Activez **Egress Decryption (Décryptage de sortie)**.
3. Activez **Logging (Journalisation)**.

STEP 13 | Cliquez sur **Add (Ajouter)**.

STEP 14 | Après avoir créé des règles pour votre rulestack, validez ou déployez votre configuration.

Services de sécurité Cloud NGFW pour Azure

Cloud NGFW utilise vos définitions de rulestack pour protéger votre trafic Azure Virtual Network (VNet) par un processus en deux étapes. Tout d'abord, il applique vos règles pour autoriser ou refuser votre trafic. Deuxièmement, il effectue une inspection du contenu sur le trafic autorisé (URL, menaces, fichiers) en fonction de ce que vous spécifiez dans les profils de sécurité. De plus, il vous aide à définir comment Cloud NGFW doit analyser le trafic autorisé et bloquer les menaces telles que les virus, les logiciels malveillants, les logiciels espions et les attaques DDoS.

IPS et protection contre les menaces de logiciels espions

- **Vulnérabilité IPS** : (activée par défaut et préconfigurée sur la base des meilleures pratiques), un profil de vulnérabilité du système de prévention des intrusions (IPS) arrête les tentatives d’exploitation des failles du système ou d’accès non autorisé aux systèmes. Les profils antispyware permettent d'identifier les hôtes infectés lorsque le trafic quitte le réseau, tandis que les profils des vulnérabilités IPS protègent contre les menaces entrant dans le réseau. Par exemple, les profils de protection contre les vulnérabilités assurent 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 du système. Le profil Protection contre les vulnérabilités protège les clients et les serveurs contre l'ensemble des menaces connues de niveaux de gravité critique, élevé et moyen.

  Configuration des meilleures pratiques

  La configuration suivante des meilleures pratiques en matière de vulnérabilité est activée par défaut sur Cloud NGFW pour Azure.

Gravité de la signature	Action
Critique	Réinitialisez les deux
Élevée	Réinitialisez les deux
Moyenne	Réinitialisez les deux
Pour information	Par défaut
Faible	Par défaut

- **Antispyware** : (activé par défaut et préconfiguré sur la base des meilleures pratiques) un profil antispyware bloque les tentatives de communication phone-home ou de signalement sur les serveurs externes de commande et contrôle (C2) par les logiciels espions sur les hôtes compromis, ce qui vous permet de détecter le trafic malveillant sortant provenant de clients infectés.

Configuration des meilleures pratiques

La configuration suivante des meilleures pratiques en matière d’antispyware est activée par défaut sur Cloud NGFW pour Azure.

Gravité de la signature	Action
Critique	Réinitialisez les deux
Élevée	Réinitialisez les deux
Moyenne	Réinitialisez les deux
Pour information	Par défaut
Faible	Par défaut

Vulnérabilité IPS et signatures antispyware

Le tableau suivant répertorie toutes les signatures possibles pour les catégories Vulnérabilité et Spyware. Ces signatures sont continuellement mises à jour sur vos NGFW.

Catégorie de menaces	Description
Signatures de vulnérabilités	
brute force	Une signature de force brute détecte plusieurs occurrences d'une condition au cours d’une période donnée. Bien que l'activité isolée puisse être bénigne, la signature de force brute indique que la fréquence et le taux auxquels l'activité s'est produite sont suspects. Par exemple, un échec de connexion FTP unique n'indique pas une activité malveillante. Cependant, de nombreux échecs de connexion FTP sur une courte période de temps indiquent la probabilité qu'un pirate tente de combiner des mots de passe pour accéder à un serveur FTP.
code execution	Détecte une vulnérabilité d'exécution de code qu'un pirate peut exploiter pour exécuter du code sur un système disposant des privilèges de l'utilisateur connecté.
Occultation de code	Détecte le code qui a été transformé pour dissimuler certaines données tout en conservant sa fonction. Le code occulté est difficile ou impossible à lire, il est donc difficile de savoir quelles commandes le code est en train d'exécuter ou avec quels programmes il est conçu pour interagir. Le plus souvent, des acteurs malveillants dissimulent du code pour dissimuler des logiciels malveillants. Plus rarement, les développeurs légitimes peuvent dissimuler du code pour protéger la confidentialité ou la propriété intellectuelle ou pour améliorer l'expérience utilisateur. Par exemple, certains types de dissimulation (tels que la minification) réduisent la taille du fichier, ce qui diminue les temps de chargement sur le site Web et l’utilisation de la bande passante.
dos	Détecte une attaque par déni de service, dans le cadre de laquelle un pirate tente de rendre indisponible un système ciblé en interrompant temporairement le système et les applications et services dépendants. Pour

Catégorie de menaces	Description
	effectuer une attaque par déni de service, un pirate peut inonder un système cible de trafic ou envoyer des informations qui entraînent son échec. Les attaques par déni de service privent les utilisateurs légitimes (tels que les employés, les membres et les titulaires de compte) du service ou de la ressource auquel ils souhaitent accéder.
exploit-kit	Détecte une page de renvoi d’un kit d’attaques. Les pages de renvoi d’un kit d’attaques contiennent souvent plusieurs exploits qui ciblent une ou plusieurs vulnérabilités et expositions (CVE) communes, pour plusieurs navigateurs et plugins. Étant donné que les CVE ciblés changent rapidement, les signatures des kits d’attaques se déclenchent en fonction de la page de renvoi du kit d’attaques et non des CVE. Lorsqu'un utilisateur visite un site Web avec un kit d’attaques, ce dernier cherche les CVE ciblés et tente de fournir en mode silencieux une charge malveillante à l'ordinateur de la victime.
info-leak	Détecte une vulnérabilité logicielle qu'un pirate pourrait exploiter pour dérober des informations sensibles ou propriétaires. Souvent, une fuite d'informations peut se produire, car les contrôles complets n'existent pas pour protéger les données et les pirates peuvent exploiter les fuites d'informations en envoyant des requêtes spécialement construites.
identifiants non sécurisés	Détecte l'utilisation de mots de passe faibles, compromis et par défaut du fabricant pour les logiciels, les appareils réseau et les dispositifs IdO.
Dépassement de capacité	Détecte une vulnérabilité de débordement dans le cadre de laquelle un pirate pourrait exploiter le manque de contrôles adéquats des requêtes. Une attaque réussie pourrait entraîner l'exécution de code à distance avec les privilèges de l'application, du serveur ou du système d'exploitation.
phishing	Détecte une situation où un utilisateur tente de se connecter à une page d’hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d’hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.
protocol-anomaly	Détecte les anomalies de protocole, lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur un port non standard sont des exemples d’anomalies de protocole et pourraient servir de techniques d'évasion.
sql-injection	Détecte une technique de piratage courante dans le cadre de laquelle un pirate insère des requêtes SQL dans les requêtes d'une application, afin de lire ou de modifier une base de données. Ce type de technique est souvent utilisé sur

Catégorie de menaces	Description
	des sites Web qui ne suppriment pas complètement les données saisies par l'utilisateur.
Signature de logiciels espions	
logiciel espion	Détecte la communication C2 sortante. Ces signatures sont générées automatiquement ou créées manuellement par les chercheurs de Palo Alto Networks.  *Les signatures de spyware et d'autogen détectent toutes les deux la communication C2 sortante ; cependant, les signatures autogènes sont basées sur la charge utile et peuvent détecter de manière unique les communications C2 avec des hôtes C2 inconnues ou qui changent rapidement.*
adware	Détecte les programmes qui affichent des publicités potentiellement indésirables. Certains logiciels publicitaires modifient les navigateurs pour mettre en évidence et créer des liens hypertextes à partir des mots-clés les plus recherchés sur les pages Web. Ces liens redirigent les utilisateurs vers des sites Web publicitaires. Les logiciels publicitaires peuvent également récupérer des mises à jour à partir d'un serveur C2 (commande-et-contrôle) et les installer dans un navigateur ou sur un système client.
autogen	Ces signatures basées sur la charge détectent le trafic de commande et de contrôle (C2) et sont générées automatiquement. Il est important de souligner que les signatures de l’autogène peuvent détecter le trafic C2 même lorsque l’hôte C2 est inconnu ou change rapidement.
backdoor	Détecte un programme qui permet à un pirate d'obtenir un accès distant non autorisé à un système.
Réseau de robots (Botnet)	Indique une activité de botnet. Un botnet est un réseau d'ordinateurs infectés par des logiciels malveillants (« bots ») qui sont contrôlés par un pirate. Le pirate peut ordonner, de manière centralisée, à chaque ordinateur d’un réseau de botnets d’effectuer simultanément une action coordonnée (par exemple, le lancement d’une attaque par déni de service).
browser-hijack	Détecte la présence d’un plugin ou d’un logiciel qui modifie les paramètres du navigateur. Un pirate de navigateur peut prendre en charge la recherche automatique ou suivre l’activité Web des utilisateurs et envoyer cette information à un serveur C2.
cryptominer	(Parfois connu sous le nom de cryptojacking ou de mineurs) Détecte la tentative de téléchargement ou le trafic réseau généré par des programmes malveillants conçus pour utiliser des ressources informatiques afin de miner des cryptomonnaies à l'insu de l'utilisateur. Les binaires Cryptominer sont souvent livrés par un téléchargeur de script shell qui tente de déterminer

Catégorie de menaces	Description
	l'architecture du système et de tuer d'autres processus de mineurs sur le système. Certains mineurs s'exécutent dans le cadre d'autres processus, tels qu'un navigateur web rendant une page web malveillante.
data-theft	Détecte un système qui envoie des informations à un serveur C2 connu.
dns	Détecte les requêtes DNS visant la connexion à des domaines malveillants.
téléchargeur	(Aussi connu sous le nom de droppers, stagers ou loaders) Détecte les programmes qui utilisent une connexion Internet pour se connecter à un serveur distant afin de télécharger et d'exécuter des logiciels malveillants sur le système compromis. Le cas d'utilisation le plus courant est celui d'un téléchargeur déployé comme point culminant de la *première étape* d'une cyber-attaque, où l'exécution de la charge utile récupérée par le téléchargeur est considérée comme la *deuxième étape*. Les scripts shell (Bash, PowerShell, etc.), les chevaux de Troie et les documents de leurre malveillants (également appelés maldocs) tels que les fichiers PDF et Word sont des types de téléchargeurs courants.
fraude	(y compris le détournement de formulaires, le hameçonnage et les escroqueries) Détecte l'accès à des sites web compromis dont il a été déterminé qu'ils ont été injectés avec du code JavaScript malveillant pour recueillir des informations sensibles sur les utilisateurs. (par exemple, nom, adresse, e-mail, numéro de carte de crédit, CVV, date d'expiration) à partir des formulaires de paiement qui sont saisis sur les pages de paiement des sites de commerce électronique.
outil de piratage	Détecte le trafic généré par des outils logiciels qui sont utilisés par des acteurs malveillants pour effectuer une reconnaissance, attaquer ou accéder à des systèmes vulnérables, exfiltrer des données, ou créer un canal de commande et de contrôle pour contrôler subrepticement un système informatique sans autorisation. Ces programmes sont fortement associés aux logiciels malveillants et aux cyber-attaques. Les outils de piratage peuvent être déployés de manière bénigne lorsqu'ils sont utilisés dans les opérations de l'Équipe rouge et bleue, les tests de pénétration et la R&D. L'utilisation ou la possession de ces outils peut être illégale dans certains pays, quelle que soit l'intention.
networm	Détecte un programme qui se réplique et se propage automatiquement d'un système à l'autre. Les « net-worms » peuvent utiliser des ressources partagées ou exploiter les défaillances de sécurité pour accéder aux systèmes cibles.
Hameçonnage	Détecte une situation où un utilisateur tente de se connecter à une page d’hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d’hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.

Catégorie de menaces	Description
post-exploitation	Détecte des activités qui indiquent la phase post-exploitation d'une attaque, dans le cadre de laquelle un pirate tente d'évaluer la valeur d'un système compromis. Cela peut inclure l'évaluation de la sensibilité des données stockées sur le système et de l'utilité du système pour compromettre davantage le réseau.
webshell	Détecte les shells web et le trafic des shells web, y compris la détection des implants et l'interaction de commande et de contrôle. Les shells web doivent d'abord être implantés par un acteur malveillant sur l'hôte compromis, le plus souvent en ciblant un serveur ou un cadre web. La communication ultérieure avec le fichier shell web permet souvent à un acteur malveillant de prendre pied dans le système, d'effectuer le dénombrement des services et du réseau, l'exfiltration des données et l'exécution du code à distance dans le contexte de l'utilisateur du serveur web. Les types de shells web les plus courants sont les scripts PHP, .NET et les scripts de balisage Perl. Les attaquants peuvent également utiliser des serveurs web infectés par un shell (les serveurs web peuvent être à la fois orientés vers Internet ou des systèmes internes) pour cibler d'autres systèmes internes.
Keylogger	Détecte les programmes qui permettent aux pirates de suivre secrètement l'activité des utilisateurs en enregistrant les touches de clavier et en enregistrant des captures d'écran. Les enregistreurs de frappe utilisent diverses méthodes C2 pour envoyer périodiquement des journaux et des rapports à une adresse électronique prédéfinie ou à un serveur C2. Par la surveillance des enregistreurs de frappe, un pirate pourrait récupérer des informations d'identification qui lui permettraient d’accéder au réseau.

Protection contre les logiciels malveillants et les menaces basées sur les fichiers

- **Antivirus** : (activé par défaut et préconfiguré sur la base des meilleures pratiques) les profils antivirus protègent contre les virus, les vers et les chevaux de Troie ainsi que contre les téléchargements de logiciels espions. À l'aide d'un moteur de prévention des logiciels malveillants basé sur les flux, qui inspecte le trafic dès la réception du premier paquet, la solution antivirus de Palo Alto Networks peut offrir aux clients une protection sans que les performances du pare-feu soient significativement altérées. Ce profil recherche une grande variété de logiciels malveillants dans les exécutables et les fichiers PDF,

de virus HTML et JavaScript ; elle permet également l'analyse des fichiers compressés et des schémas de codage de données.

Configuration des meilleures pratiques

La configuration suivante des meilleures pratiques en matière d’antivirus est activée par défaut sur Cloud NGFW pour Azure.

Protocole	Action
FTP	Réinitialisez les deux
HTTP	Réinitialisez les deux
HTTP2	Réinitialisez les deux
IMAP	Réinitialisez les deux
POP3	Alerte
SMB	Réinitialisez les deux
SMTP	Réinitialisez les deux

- **Blocage des fichiers** : (activé par défaut et préconfiguré sur la base des meilleures pratiques) les profils de blocage des fichiers vous permettent d’identifier des types de fichiers spécifiques que vous souhaitez bloquer ou surveiller. Le pare-feu utilise les profils de blocage des fichiers pour bloquer des types de fichiers précis sur des applications données et dans le sens du flux de session donné (entrant, sortant ou les deux). Vous pouvez configurer le profil de manière à alerter ou bloquer le chargement et/ou le téléchargement et indiquer les applications soumises au profil de blocage des fichiers.
  - **Alerte** : lorsque le type de fichier donné est détecté, un journal est généré dans le journal de filtrage des données.
  - **Blocage** : lorsque le type de fichier spécifié est détecté, le fichier est bloqué. Une entrée est également générée dans le log de filtrage des données.

Configuration des meilleures pratiques

La configuration suivante des meilleures pratiques en matière de blocage des fichiers est activée par défaut sur Cloud NGFW pour Azure.

Types de fichiers	Application	Direction	Action
Tous les types de fichiers à risque : • 7z • bat • cab • chm • class	Tous	Les deux (chargement et téléchargement)	Bloquer

Types de fichiers	Application	Direction	Action
• cpl • dll • exe • flash • hip • hta • msi • Multi-Level-Encoding • ocx • PE • pif • rar • scr • tar • torrent • vbe • wsf • encrypted-rar • encrypted-zip			
Tous les types de fichiers restants	Tous	Les deux (chargement et téléchargement)	Alerte

Signatures antivirus

Le tableau suivant répertorie toutes les signatures possibles pour la catégorie Antivirus. Ces signatures sont continuellement mises à jour sur vos NGFW.

Catégorie de menaces	Description
Signatures antivirus	
apk	Fichiers malveillants d'application Android (APK).
MacOSX	Fichiers MacOSX malveillants, notamment : • Fichiers d’image disque Apple (DMG). • Les fichiers objet Mach (Mach-O) sont des exécutables, des bibliothèques et du code objet.

Catégorie de menaces	Description
	• Packages d’installation de logiciels Apple (PKG)
flash	Applets Adobe Flash et contenu Flash intégré à des pages Web.
jar	Applets Java (types de fichiers JAR/Class).
ms-office	Fichiers Microsoft Office, y compris les documents (DOC, DOCX, RTF), les cahiers de travail (XLS, XLSX) et les présentations PowerPoint (PPT, PPTX). Cela inclut également les documents Office Open XML (OOXML) 2007+.
pdf	Fichiers Portable Document Format (PDF).
pe	Les fichiers exécutables portatifs (PE) peuvent s’exécuter automatiquement sur un système Windows de Microsoft et ne devraient être autorisés que lorsqu’ils sont autorisés. Ces types de fichiers comprennent ce qui suit : • Code d’objet. • Polices (FON). • Fichiers système (SYS). • Fichiers lecteur (DRV). • Éléments du panneau de configuration Windows (CPL). • DLL (bibliothèque à liaisons dynamiques) • OCX (bibliothèques des contrôles personnalisés OLE ou des contrôles ActiveX). • Fichiers d’économiseur d’écran Windows (SCR). • Fichiers EFI (Extensible Firmware Interface), qui s'exécutent entre un système d'exploitation et un microprogramme afin de faciliter les mises à jour de périphériques et les opérations de démarrage. • Fichiers d'informations sur le programme (PIF).
Linux	Fichiers Executable and Linkable Format (format exécutable et liable ; ELF).
archive	Fichiers d'archive Roshal Archive (RAR) et 7-Zip (7z).

Protection contre les menaces Web

Filtrage et catégories d’URL : (activé par défaut et préconfiguré sur la base des meilleures pratiques) les profils de filtrage des URL vous permettent de surveiller et de contrôler la manière dont les utilisateurs accèdent au Web via les protocoles HTTP et HTTPS. Le pare-feu est livré avec un profil par défaut qui est configuré pour bloquer des sites Web tels que les sites renfermant des logiciels malveillants, les sites de hameçonnage et les sites pour adultes connus. Le profil de filtrage des URL n'est pas activé par défaut. Lorsque vous activez le profil de filtrage des URL dans votre rulestack, Cloud NGFW applique le profil de

filtrage des URL conforme aux meilleures pratiques sur votre trafic. Vous avez la possibilité de modifier l’option d’accès par défaut sur chacune des catégories, en fonction de vos besoins.

Configuration des meilleures pratiques

Par défaut, le filtrage des URL est activé et utilise une politique de sécurité basée sur les meilleures pratiques.

Catégories d’URL	Accès au site	Soumission des informations d’identification
Catégories malveillantes et d’exploitation : • adulte • commande et contrôle • violation des droits d’auteur • DNS dynamique • extrémisme • malware • parqué • hameçonnage • contournement de proxy et anonymiseurs • inconnu	Bloquer	Bloquer
Toutes les autres catégories d’URL	Alerte	Alerte

Catégories d’URL prédéfinies pour Cloud NGFW pour Azure

Le tableau suivant décrit les catégories d’URL prédéfinies disponibles sur Cloud NGFW sur Azure. Vous pouvez utiliser ces catégories dans les règles de sécurité pour bloquer ou autoriser l’accès aux sites Web qui en font partie.

Catégorie d'URL	Description
Catégories de risque	
À risque élevé	Sites dont la malveillance a déjà été confirmée, mais qui ont affiché une activité bénigne pendant au moins 30 jours. Sites hébergés sur des ISP pare-balles ou utilisant une adresse IP d’un ASN dont le contenu malveillant est connu. Sites partageant un domaine avec un site malveillant connu. Tous les sites de la catégorie « Inconnu » présenteront un risque élevé.

Catégorie d'URL	Description
À risque modéré	Les sites confirmés comme malveillants, mais ayant affiché une activité bénigne pendant au moins 60 jours. Tous les sites de la catégorie « Stockage et sauvegarde en ligne » présenteront un risque moyen par défaut.
À risque faible	Tout site qui n’est pas à risque élevé ou modéré. Cela inclut les sites qui ont déjà été confirmés comme malveillants, mais qui ont affiché une activité bénigne pendant au moins 90 jours.
Catégories de menaces	
Commande et contrôle	Les URL et les domaines de commande et contrôle utilisés par les logiciels malveillants et/ou autres systèmes compromis pour communiquer discrètement avec le serveur à distance d’un pirate afin de recevoir des commandes malveillantes ou d'exfiltrer des données.
Logiciel malveillant	Sites qui sont reconnus pour héberger des logiciels malveillants ou qui sont utilisés pour du trafic de commande et de contrôle (C2). Ils peuvent également contenir des kits d’attaque.
Catégories adjacentes aux menaces	
DNS dynamique	Noms d’hôtes et de domaines de systèmes dont les adresses IP sont dynamiquement attribuées et qui sont souvent utilisés pour transmettre des charges utiles malveillantes ou du trafic C2. De plus, les domaines DNS dynamiques ne passent pas par le même processus de contrôle que les domaines qui sont enregistrés par une société spécialisée dans l’enregistrement de noms de domaine qui est digne de confiance ; ils sont dont moins fiable.
Logiciel indésirable	Contenu Web qui ne constitue pas une menace directe pour la sécurité, mais qui affiche un autre comportement gênant et incite l’utilisateur final à accorder un accès à distance ou à effectuer d’autres actions non autorisées. Les logiciels indésirables comprennent les activités illégales, les activités criminelles, les roguewares, les logiciels publicitaires et autres applications indésirables ou non sollicitées, telles que les cryptomineurs intégrés ou les pirates qui modifient les éléments du navigateur. Les domaines de typosquattage qui ne font pas preuve de malveillance et qui ne sont pas détenus par le domaine ciblé seront classés dans la catégorie des logiciels indésirables.
Piratage	Sites relatifs à l’accès illégal ou douteux ou à l’utilisation d’équipements / logiciels de communication. Élaboration et distribution de programmes, de conseils pratiques et/ou de

Catégorie d'URL	Description
	conseils pouvant compromettre les réseaux et les systèmes. Comprend également les sites qui facilitent le contournement des systèmes de licences et de droits numériques.
Hameçonnage	Contenu Web qui tente secrètement de tromper l'utilisateur afin de collecter des informations, y compris les informations de connexion, les informations de carte de crédit (volontairement ou involontairement) les numéros de compte, les codes PIN et toute information considérée comme une information personnellement identifiable (PII) des victimes via des techniques d'ingénierie sociale. Les escroqueries au support technique et les scarewares sont également inclus comme hameçonnage.
Suspect	
Contenu insuffisant	Les sites Web et les services qui présentent des pages de test, n’ont pas de contenu, fournissent un accès API non destiné à l’affichage de l’utilisateur final ou nécessitent une authentification sans afficher aucun autre contenu suggérant une catégorisation différente. Ne doit pas inclure les sites Web fournissant un accès à distance, comme les solutions VPN basées sur le Web, les services de messagerie Web ou les pages d’hameçonnage d’informations d’identification identifiées.
Domaine nouvellement enregistré	Les domaines nouvellement enregistrés sont souvent générés volontairement ou par des algorithmes de génération de domaines et utilisés pour mener des activités malveillantes.
Parqué	Domaines enregistrés par des personnes ; on découvre souvent plus tard qu’ils ont servi à usurper des informations de connexion . Ces domaines peuvent ressembler à des domaines légitimes, par exemple, pal0alto0netw0rks.com ; ils servent toutefois à usurper des informations de connexion ou des informations personnelles. Il peut également s'agir de domaines pour lesquels une personne a acheté les droits dans l'espoir qu'un jour ils aient de la valeur, par exemple panw.net.
Contournement de proxy et anonymiseurs	URL et services souvent utilisés pour contourner les produits de filtrage de contenu.
inconnue	Sites qui n’ont pas encore été identifiés par Palo Alto Networks. Si la disponibilité est importante pour votre entreprise et que vous devez autoriser le trafic, demandez qu’une alerte soit envoyée en présence de sites inconnus, appliquez au trafic les profils de sécurité recommandés et enquêtez sur les alertes.

Catégorie d'URL	Description
Juridique/Politique	
Avortement	Sites qui se rapportent à des informations ou des groupes en faveur ou contre l’avortement, des détails concernant les procédures d’avortement, des forums d’aide ou de soutien pour ou contre l’avortement, ou des sites qui fournissent des informations sur les conséquences / effets de la poursuite (ou non) d’un avortement.
Drogues abusées	Sites qui font la promotion de l’abus de drogues légales et illégales, de l’utilisation et de la vente d’accessoires liés à la drogue, de la fabrication et/ou de la vente de drogues.
Adulte	Matériel sexuellement explicite, médias (y compris la langue), œuvres d’art et/ou produits, groupes ou forums en ligne de nature sexuellement explicite. Sites qui font la promotion de services pour adultes tels que la vidéoconférence / conférence téléphonique, les services d’escorte, les clubs de strip-tease, etc. Tout ce qui contient du contenu pour adultes (même s’il s’agit de jeux ou de bandes dessinées) sera classé comme adulte.
Alcool et tabac	Sites qui se rapportent à la vente, à la fabrication ou à la consommation d’alcool et/ou de produits du tabac et d’accessoires connexes. Comprend les sites liés aux cigarettes électroniques.
Enchères	Sites qui favorisent la vente de biens entre particuliers.
Affaires et économie	Marketing, gestion, économie et sites liés à l’entrepreneuriat ou à la gestion d’une entreprise. Comprend les entreprises de publicité et de marketing. Ne devrait pas inclure les sites Web d’entreprise, car ils devraient être classés avec leur technologie. Aussi les sites d’expédition, tels que fedex.com et ups.com.
Informations sur les ordinateurs et Internet	Informations générales concernant les ordinateurs et Internet. Devrait inclure des sites sur l’informatique, l’ingénierie, le matériel, les logiciels, la sécurité, la programmation, etc. La programmation peut avoir un certain chevauchement avec les références, mais la catégorie principale devrait rester l’informatique et l’information Internet.
Réseaux de distribution de contenu	Sites dont l’objectif principal est de fournir du contenu à des parties 3rd telles que des publicités, des médias, des fichiers, etc. Inclut également les serveurs d’images.
Violation des droits d’auteur	Domaines dont le contenu est illégal, par exemple du contenu qui permet le téléchargement illégal de logiciels ou d’autres

Catégorie d'URL	Description
	propriétés intellectuelles, ce qui présente un risque de responsabilité éventuel. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l’industrie de l’éducation ainsi que des lois des pays qui exigent que les fournisseurs Internet empêchent les utilisateurs de partager du matériel protégé par des droits d’auteur via leur service.
Cryptomonnaie	Les sites Web qui font la promotion des cryptomonnaies, les sites Web de minage de cryptomonnaies (mais pas les mineurs de cryptomonnaies intégrés), les échanges et les fournisseurs de cryptomonnaies, et les sites Web qui gèrent les portefeuilles et les registres de cryptomonnaie. Cette catégorie n’inclut pas les sites Web de services financiers traditionnels qui font référence aux cryptomonnaies, les sites Web qui expliquent et décrivent le fonctionnement des cryptomonnaies et des blockchains, ou les sites Web qui contiennent des mineurs de cryptomonnaie intégrés (logiciels indésirables).
Rencontres	Sites Web offrant des services de rencontres en ligne, des conseils et d’autres annonces personnelles.
Établissements d’enseignement	Sites Web officiels pour les écoles, collèges, universités, districts scolaires, cours en ligne et autres établissements d’enseignement. Il s’agit d’établissements d’enseignement plus grands et établis tels que les écoles primaires, les écoles secondaires, les universités, etc. Les académies de tutorat peuvent également y aller.
Spectacles et arts	Sites pour films, télévision, radio, vidéos, guides/outils de programmation, bandes dessinées, arts du spectacle, musées, galeries d’art ou bibliothèques. Comprend des sites de divertissement, de célébrités et de nouvelles de l’industrie.
Extrémisme	Sites Web faisant la promotion du terrorisme, du racisme, du fascisme ou d’autres points de vue extrémistes discriminant des gens ou des groupes d’origines ethniques différentes, d’autres religions ou d’autres croyances. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l’industrie de l’éducation. Dans certaines régions, les lois et règlements peuvent interdire l’accès aux sites extrémistes, et l’autorisation de l’accès peut présenter un risque de responsabilité.
Services financiers	Sites Web contenant des renseignements ou des conseils financiers personnels, tels que les services bancaires en ligne, les prêts, les prêts hypothécaires, la gestion de dettes, les sociétés émettrices de cartes de crédit et les compagnies

Catégorie d'URL	Description
	d’assurance. N’inclut pas les sites relatifs aux marchés boursiers, aux maisons de courtage ou aux services de trading. Comprend les sites de change de devises. Comprend les sites de change de devises.
Jeux d’argent	Sites Web de loterie ou de jeux d’argent qui facilitent l’échange d’argent réel et/ou virtuel. Sites Web connexes qui fournissent des informations, des didacticiels ou des conseils concernant les jeux d’argent, y compris les cotes de paris et les pools. Les sites Web d’entreprise pour les hôtels et les casinos qui n’autorisent pas les jeux d’argent sont classés dans la catégorie Voyages.
Jeux	Sites qui fournissent des jeux vidéo et/ou des téléchargements en ligne de jeux vidéo et/ou informatiques, des critiques de jeux, des conseils ou des tricheurs, ainsi que des sites pédagogiques pour les jeux non électroniques, la vente/échange de jeux de société ou des publications/médias connexes. Comprend les sites qui prennent en charge ou hébergent des tirages au sort et/ou des cadeaux en ligne.
Gouvernement	Sites Web officiels pour les gouvernements locaux, étatiques et nationaux, ainsi que les agences, services ou lois connexes.
Santé et médecine	Sites contenant des informations sur la santé générale, des problèmes et des conseils, remèdes et traitements traditionnels et non traditionnels. Comprend également des sites pour diverses spécialités, pratiques et installations médicales (comme des gymnases et des clubs de fitness) ainsi que des professionnels. Les sites relatifs à l’assurance médicale et à la chirurgie esthétique sont également inclus.
Maison et jardin	Information, produits et services concernant la réparation et l’entretien de la maison, l’architecture, la conception, la construction, la décoration et le jardinage.
Chasse et pêche	Conseils de chasse et de pêche, instructions, vente d’équipement connexe et d’accessoires.
Communications Internet et téléphonie	Sites qui prennent en charge ou fournissent des services de chat vidéo, de messagerie instantanée ou de téléphonie.
Portails Internet	Sites qui servent de point de départ pour les utilisateurs, généralement en agrégeant un large éventail de contenus et de sujets.
Recherche d’emploi	Sites qui fournissent des offres d’emploi et des avis d’employeurs, des conseils et des astuces d’entrevue, ou

Catégorie d'URL	Description
	des services connexes pour les employeurs et les candidats potentiels.
Juridique	Information, analyse ou conseil concernant le droit, les services juridiques, les cabinets d’avocats ou d’autres questions juridiques connexes
Militaire	Informations ou commentaires concernant les branches militaires, le recrutement, les opérations actuelles ou passées, ou tout accessoire connexe.
Véhicules à moteur	Informations relatives aux examens, aux ventes et aux échanges, aux modifications, aux pièces et autres discussions connexes pour les automobiles, les motocyclettes, les bateaux, les camions et les véhicules récréatifs.
Musique	Vente, distribution ou information musicale. Comprend des sites Web pour les artistes musicaux, les groupes, les labels, les événements, les paroles et d’autres informations concernant l’industrie de la musique. N’inclut pas la musique en streaming.
Actualité	Publications en ligne, agences de presse et autres sites Web qui regroupent l’actualité, la météo ou d’autres questions contemporaines. Comprend les journaux, les stations de radio, les magazines et les podcasts.
Non résolu	Indique que le site Web est introuvable dans la base de données de filtrage des URL locale et que le pare-feu n’a pas pu se connecter à la base de données cloud pour vérifier la catégorie. Lorsqu’une recherche de catégorie d’URL est effectuée, le pare-feu vérifie d’abord le cache du plan de données pour l’URL, si aucune correspondance n’est trouvée, il vérifie ensuite le cache du plan de gestion, et si aucune correspondance n’y est trouvée, il interroge la base de données d’URL dans le cloud. Lorsque vous décidez de l’action à entreprendre pour le trafic classé comme non résolu, sachez que la définition de l’action sur blocage peut être très perturbante pour les utilisateurs.
Nudité	Sites qui contiennent des représentations nues ou semi-nues du corps humain, indépendamment du contexte ou de l’intention, telles que des œuvres d’art. Comprend les sites nudistes ou naturistes contenant des images des participants.
Stockage et sauvegarde en ligne	Sites Web qui fournissent le stockage en ligne de fichiers gratuitement et en tant que service.

Catégorie d'URL	Description
Poste à poste	Sites qui fournissent un accès ou des clients pour le partage peer-to-peer de torrents, de programmes de téléchargement, de fichiers multimédias ou d’autres applications logicielles. Ceci est principalement pour les sites qui fournissent des capacités de téléchargement BitTorrent. N’inclut pas les sites de partagiciel ou de logiciels gratuits.
Sites personnels et blogs	Sites Web personnels et blogs d’individus ou de groupes. Devrait d’abord essayer de catégoriser en fonction du contenu. Par exemple, si quelqu’un a un blog sur les voitures, alors le site devrait être classé sous « véhicules à moteur ». Cependant, si le site est un blog pur, il doit rester sous « sites personnels et blogs ».
Philosophie et plaidoyer politique	Sites contenant des informations, des points de vue ou des campagnes concernant des opinions philosophiques ou politiques.
Adresses IP privées	Cette catégorie inclut les adresses IP définies dans la RFC 1918, « Address Allocation for Private Intranets ». Il inclut également les domaines non enregistrés auprès du système DNS public (*.local et *.onion).
Douteux	Sites web contenant de l'humour de mauvais goût, des contenus offensants ciblant des groupes ou des individus spécifiques.
Immobilier	Informations sur la location de propriétés, les ventes et conseils ou informations connexes. Comprend des sites pour les agents immobiliers, les entreprises, les services de location, les listes (et les agrégats) et l’amélioration de la propriété.
Loisirs et passe-temps	Informations, forums, associations, groupes et publications sur les loisirs et les loisirs.
Référence et recherche	Portails, documents ou services de référence personnelle, professionnelle ou académique. Comprend des dictionnaires en ligne, des cartes, des almanachs, des données de recensement, des bibliothèques, des renseignements généalogiques et scientifiques.
Religion	Informations concernant diverses religions et des activités ou événements connexes. Comprend les sites Web des organisations religieuses, des responsables et des lieux de culte. Comprend des sites de voyance.
Moteurs de recherche	Sites qui fournissent une interface de recherche utilisant des mots-clés, des expressions ou d’autres paramètres qui peuvent

Catégorie d'URL	Description
	renvoyer des informations, des sites Web, des images ou des fichiers sous forme de résultats.
Éducation sexuelle	Informations sur la reproduction, le développement sexuel, les pratiques sexuelles sans risque, les maladies sexuellement transmissibles, la contraception, des conseils pour une meilleure sexualité, ainsi que tout produit connexe ou accessoire connexe. Comprend les sites Web de groupes, de forums ou d’organisations connexes.
Partagiciels et logiciels gratuits	Sites donnant accès gratuitement à des logiciels, des économiseurs d’écran, des icônes, des fonds d’écran, des utilitaires, des sonneries, des thèmes ou des widgets. Inclut également les projets open source.
Achats	Sites qui facilitent l’achat de biens et de services. Comprend les marchands en ligne, les sites Web des grands magasins, les magasins de détail, les catalogues, ainsi que les sites qui regroupent et surveillent les prix. Les sites énumérés ici devraient être des marchands en ligne qui vendent une variété d’articles (ou dont le but principal est la vente en ligne). Une page Web pour une entreprise de cosmétiques qui autorise également l’achat en ligne devrait être classée avec des cosmétiques et non des achats.
Mise en réseau social	Les communautés d’utilisateurs et les sites où les utilisateurs interagissent les uns avec les autres, publient des messages, des images ou communiquent avec des groupes de personnes. N’inclut pas les blogs ou les sites personnels.
Société	Sujets relatifs à la population en général, questions qui touchent une grande variété de personnes, telles que la mode, la beauté, les groupes philanthropiques, les sociétés ou les enfants. Comprend également les sites Web des restaurants. Comprend des sites Web conçus pour les enfants ainsi que des restaurants.
Sports	Informations sur les événements sportifs, les athlètes, les entraîneurs, les responsables, les équipes ou les organisations, les résultats sportifs, les horaires et les nouvelles connexes, et tout accessoire connexe. Comprend des sites Web concernant les sports fantastiques et d’autres ligues sportives virtuelles.
Conseils et outils boursiers	Informations concernant le marché boursier, la négociation d’actions ou d’options, la gestion de portefeuille, les politiques d’investissement, les cotations ou les nouvelles connexes.

Catégorie d'URL	Description
Diffusion multimédia en continu	Sites qui diffusent du contenu audio ou vidéo gratuitement et/ou à l’achat. Comprend les stations de radio en ligne et autres services de musique en streaming.
Maillots de bain et sous-vêtements	Sites qui contiennent des informations ou des images concernant des maillots de bain, des vêtements intimes ou d’autres vêtements suggestifs
Formations et outils	Sites qui offrent des services d’éducation et de formation en ligne et du matériel connexe. Peut inclure des écoles de conduite/circulation, la formation sur le lieu de travail, etc.
Traduction	Sites qui fournissent des services de traduction, y compris les entrées utilisateur et les traductions d’URL. Ces sites peuvent également permettre aux utilisateurs de contourner le filtrage lorsque le contenu de la page cible est présenté dans le contexte de l’URL du traducteur.
Voyage	Informations concernant les conseils de voyage, les offres, les informations sur les prix, les informations sur la destination, le tourisme et les services connexes. Comprend les sites Web des hôtels, des attractions locales, des casinos, des compagnies aériennes, des croisiéristes, des agences de voyages, des locations de véhicules et des sites qui fournissent des outils de réservation tels que des moniteurs de prix. Comprend des sites Web pour les points d’intérêt locaux / attractions touristiques tels que la Tour Eiffel, le Grand Canyon, etc.
Armes	Ventes, critiques, descriptions ou instructions concernant les armes et leur utilisation.
Publicités Web	Publicités, médias, contenu et bannières.
Hébergement Web	Services d’hébergement gratuits ou payants de pages Web, y compris des informations sur le développement Web, la publication, la promotion et d’autres méthodes visant à augmenter le trafic.
Messagerie Web	Tout site Web qui donne accès à une boîte de réception de courrier électronique et la possibilité d’envoyer et de recevoir des e-mails.

Activer la sécurité DNS sur Cloud NGFW pour Azure

Le service de noms de domaine (DNS) est un protocole Internet essentiel et fondamental, tel que décrit dans les RFC principales du protocole. Des acteurs malveillants ont utilisé les canaux de communication de Commande et contrôle (C2) sur le DNS et, dans certains cas, ont même utilisé le protocole pour exfiltrer des données. L'exfiltration DNS peut se produire lorsqu'un acteur malveillant compromet une instance d'application dans votre réseau, puis utilise la recherche DNS pour envoyer des données à l'extérieur du réseau vers un domaine qu'il contrôle. Des acteurs malveillants peuvent également infiltrer des données/charges utiles malveillantes dans les charges de travail du réseau via DNS. Au fil des ans, les recherches de l'unité 42 de Palo Alto Networks ont décrit différents types d'abus de DNS découverts.

Cloud NGFW pour Azure vous permet de protéger votre trafic vNet et vWAN contre les menaces DNS avancées en surveillant et contrôlant les domaines interrogés par vos ressources réseau. Avec Cloud NGFW pour Azure, vous pouvez refuser l'accès aux domaines que Palo Alto Networks considère comme malveillants ou suspects et autoriser le passage des autres requêtes.

Pour ce faire, Cloud NGFW s'appuie sur le service de sécurité DNS de Palo Alto Networks, qui détecte proactivement les domaines malveillants en générant des signatures DNS à l'aide d'une analyse prédictive avancée et de l'apprentissage machine, avec des données provenant de plusieurs sources (telles que l'analyse du trafic WildFire, le DNS passif, l'exploration active du Web et l'analyse du contenu Web malveillant, l'analyse de la sandbox URL, le réseau Honeynet, l'ingénierie DGA inverse, les données télémétriques, whois, l'organisation de recherche Unité 42 et la Cyber Threat Alliance). Le service de sécurité DNS distribue ensuite ces signatures DNS sur vos ressources Cloud NGFW pour vous défendre proactivement contre les logiciels malveillants utilisant le DNS pour la commande et le contrôle (C2) et le vol de données.

Lorsque la sécurité DNS est activée, le Cloud NGFW exécute les actions suivantes pour chaque catégorie de sécurité DNS.

Catégorie	Gravité des journaux	Action
Domaines de suivi des publicités	Pour information	Autoriser
Domaines de commandement et contrôle (C2)	Élevée	Bloquer
Domaines DNS dynamiques (DDNS)	Pour information	Autoriser
Domains de logiciels indésirables	Faible	Bloquer
Domaines de logiciels malveillants	Moyenne	Bloquer
Domaines nouvellement enregistrés	Pour information	Autoriser
Domaines parqués	Pour information	Autoriser

Catégorie	Gravité des journaux	Action
Domaines de hameçonnage	Faible	Bloquer
Contournement de proxy et anonymiseurs	Faible	Bloquer

Pour inspecter le trafic DNS, vous devez activer le proxy DNS sur votre Cloud NGFW pour Azure.

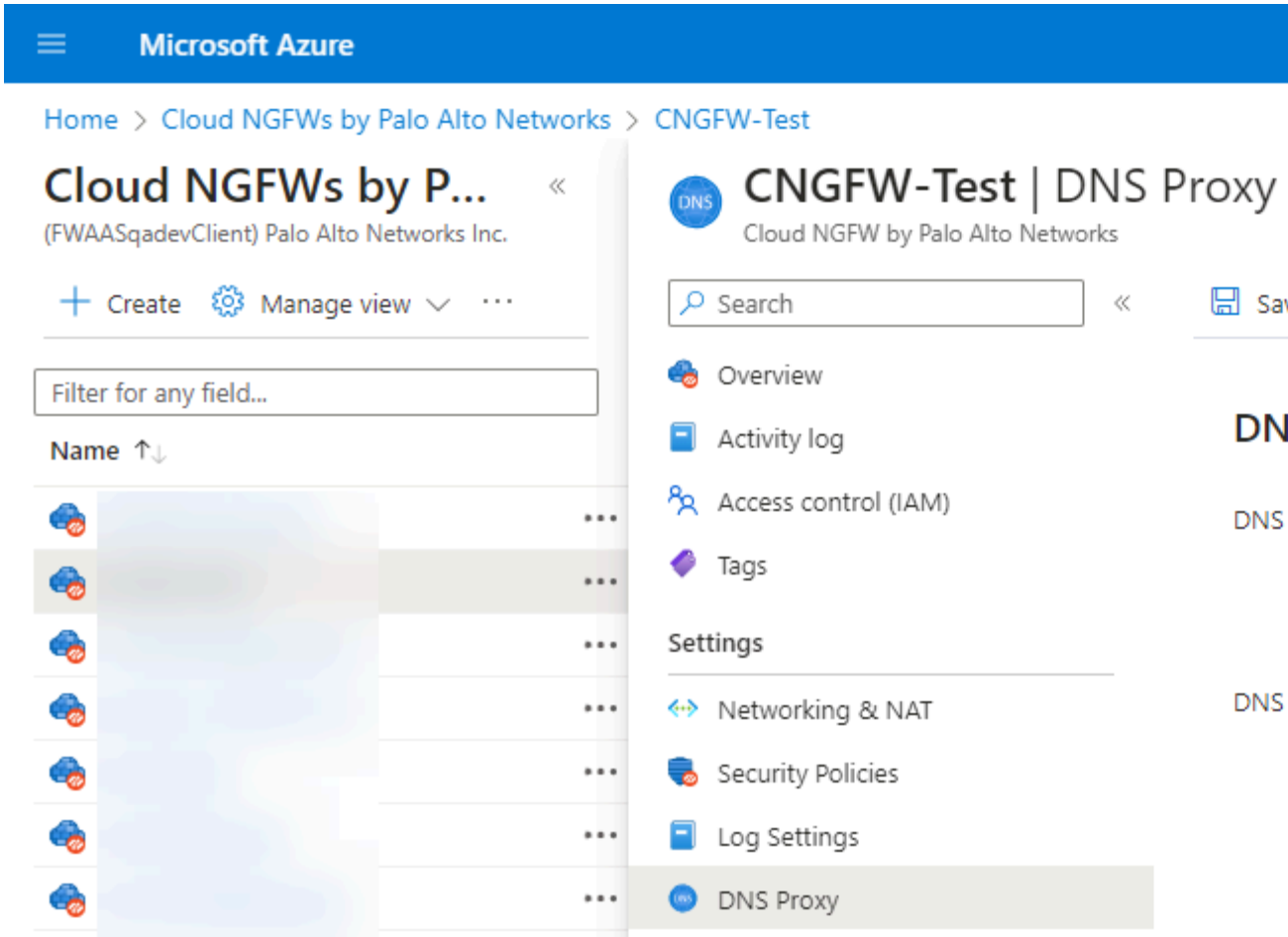
STEP 1 | Connectez-vous au portail Azure.

STEP 2 | Cliquez sur l’icône Cloud NGFW sous Azure services (Services Azure).

STEP 3 | Sélectionnez votre instance Cloud NGFW.

STEP 4 | Activez le proxy DNS.

1. Sélectionnez **Settings (Paramètres)** > **DNS Proxy (Proxy DNS)**.
2. Sélectionnez le bouton radio **Enabled (Activé)**.
3. Utilisez le serveur DNS par défaut ou sélectionnez **Custom (Personnalisé)** et spécifiez un serveur DNS précédemment configuré dans votre réseau virtuel.
4. Cliquez sur **Save (Enregistrer)**.

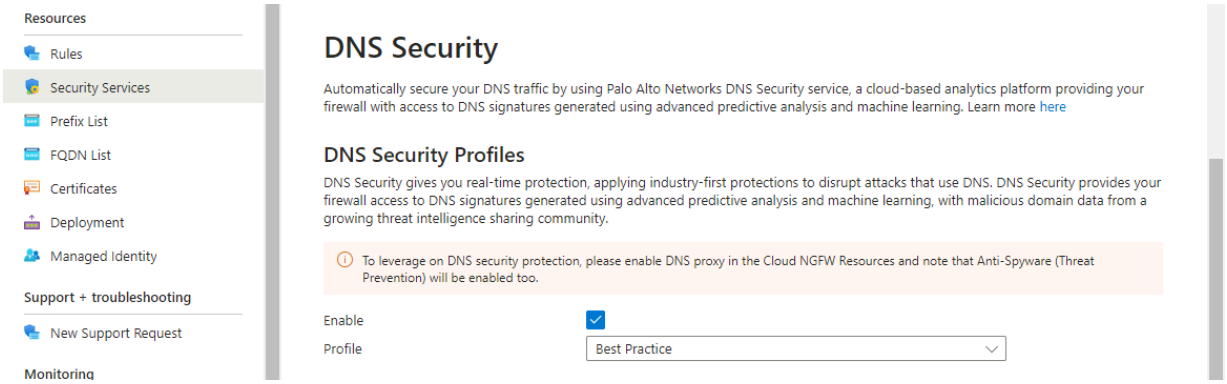


STEP 5 | Accédez à la rulestack locale associée à votre instance Cloud NGFW.

STEP 6 | Sélectionnez **Security Services (Services de sécurité)**.

STEP 7 | Activez **DNS Security (Sécurité DNS)**.

L’activation de la sécurité DNS nécessite également l’activation de l’antispyware. De plus, la sécurité DNS et l’antispyware doivent être définis sur Best Practices (Meilleures pratiques).



Configurer le décryptage sortant sur Cloud NGFW pour Azure

Avec le décryptage sortant, Cloud NGFW se comporte comme un proxy de transfert SSL et utilise ses certificats associés pour s’établir en tant que tiers de confiance (man-in-the-middle) pour la session client-serveur. Cependant, Cloud NGFW conserve vos en-têtes de paquets de trafic et votre charge utile intacts, offrant une visibilité complète de l’identité de la source vers vos destinations.

Veillez à utiliser PAN-OS version 11.0.x lorsque vous utilisez Azure Key Vault pour le décryptage sortant.

Le décryptage sortant utilise deux objets de certificat : Trust et Untrust. NGFW présente le certificat d’approbation aux clients pendant le décryptage SSL si le client tente de se connecter à un serveur dont le certificat est signé par une autorité de certification (CA) approuvée. Alternativement, NGFW présente le certificat de non-approbation au client qui tente de se connecter à un serveur dont le certificat est signé par une autorité de certification que NGFW n’approuve pas.

Vous pouvez configurer la ressource NGFW pour décrypter le trafic SSL quittant votre vNet ou sous-réseau. Vous pouvez ensuite appliquer App-ID et les paramètres de sécurité sur le trafic en texte brut, notamment les profils Antivirus, Vulnérabilité, Antispyware, Filtrage des URL et Blocage de fichiers. Une fois que le trafic est décrypté et inspecté, le pare-feu chiffre de nouveau le trafic en texte brut dès sa sortie du pare-feu pour garantir la confidentialité et la sécurité.

Cette procédure définit uniquement les certificats que le pare-feu utilise pour le décryptage TLS sortant. Vous devez activer le décryptage TLS sortant lors de la création des règles.

STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment à laquelle appliquer le certificat.

STEP 2 | Sélectionnez **Security Profiles (Profils de sécurité)** > **Egress Decryption (Décryptage de sortie)**.

STEP 3 | Sélectionnez un certificat.

- Sélectionnez un **Untrust Certificate (Certificat de non-approbation)**.
- Sélectionnez un **Trust Certificate (Certificat d’approbation)**.

Si ce n’est déjà fait, Ajouter un certificat à Cloud NGFW pour Azure.

Le certificat et la clé privée sont stockés dans Azure Key Vault, et la charge de travail utilise ces informations pour décrypter le trafic.

Le certificat doit être un certificat CA. Définissez la valeur CA dans les contraintes de base sur TRUE (VRAI). Voici un exemple de certificat CA privé.

```
Certificat : Données : Version : 3 (0x2) Numéro de série : 4121
 (0x1019) Algorithme de signature : sha256WithRSAEncryption
 Émetteur : C=US, ST=Washington, L=Seattle, O=CA racine
 d’un exemple d’entreprise, OU=Corp, CN=www.example.com/
emailAddress=corp@www.example.com Validité pas avant : 26 février
 20:27:56 2018 GMT Pas après : 24 février 20:27:56 2028 GMT
```



```
Objet : C=US, ST=WA, L=Seattle, O=CA subordonnée d’exemple
d’entreprise, OU=Bureau d’entreprise, CN=www.example.com
Informations de clé publique de l’objet : Algorithme de
clé publique : rsa Clé publique de décryptage : (2048 bits)
Module : 00:c0 : ... a3:4a:51 Exposant : 65537 (0x10001)
Extensions X509v3 : X509v3 Identificateur de clé de l’objet :
F8:84:EE:37:21:F2:5E:0B:6C:40:C2:9D:C6:FE:7E:49:53:67:34:D9
X509v3 Identificateur de clé d’autorité :
keyid:0D:CE:76:F2:E3:3B:93:2D:36:05:41:41:16:36:C8:82:BC:CB:F8:A0
Contraintes de base X509v3 : critique CA:TRUE Utilisation de la
clé X509v3 : critique Signature numérique, Algorithme de signature
de signature CRL : sha256WithRSAEncryption 6:bb:94 : ... 80:d8
```

Si vous utilisez un certificat d’entité finale pour déchiffrer le trafic, seul le certificat d’entité finale avec clé publique et privée doit être stocké dans Azure Key Vault.

PKCS8 est le format de certificat pris en charge.

Les certificats d’approbation ne peuvent pas être auto-signés, mais le certificat de non-approbation peut être auto-signé ou signé par la CA.

STEP 4 | Accédez à la **rulestack** précédemment créée et accédez à la page **Managed Identity (Identité gérée)**.

STEP 5 | Dans le menu déroulant **Enable MI (Activer MI)**, sélectionnez l’identité gérée associée au coffre de clés.

STEP 6 | Cliquez sur **Save (Enregistrer)**.

Configurer le décryptage entrant sur Cloud NGFW pour Azure

Cloud NGFW utilise le décryptage SSL entrant pour décrypter et inspecter le trafic entrant SSL/TLS d’un client vers un serveur réseau ciblé (tout serveur pour lequel vous avez le certificat et que vous pouvez importer sur le pare-feu) et bloquer les sessions suspectes. Le pare-feu agit comme un proxy entre le client externe et le serveur interne et génère une nouvelle clé de session pour chaque session sécurisée. Le pare-feu crée une session sécurisée entre le client et le pare-feu et une autre session sécurisée entre le pare-feu et le serveur pour décrypter et inspecter le trafic. Cependant, Cloud NGFW conserve intacts les en-têtes et la charge utile de vos paquets de trafic, offrant une visibilité complète de l’identité de la source à vos applications dans vos réseaux virtuels.

Vous devez concaténer le certificat Web et la clé privée en un seul fichier `pem` ou `pfx` et le télécharger sur Azure Key Vault pour effectuer une inspection SSL entrante. Le pare-feu vérifie que le certificat envoyé par le serveur ciblé lors de la poignée de main SSL/TLS correspond à un certificat de votre règle de politique de décryptage. En cas de correspondance, le pare-feu transmet le certificat du serveur au client demandant l'accès au serveur et établit une connexion sécurisée.

Vous ne devez pas télécharger le certificat et la clé séparément dans le coffre de clés Azure.

-

STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment à laquelle appliquer le certificat.

STEP 2 | Sélectionnez **Rules (Règles)**, puis **Create (Créer)** pour créer une nouvelle **Security Rule (Règle de sécurité)** pour le décryptage.

STEP 3 | Fournissez les détails suivants sous **General (Général)**.

- **Name (Nom)** : nom de la règle.
- **Description** : description de la règle.
- **Priority (Priorité)** : priorité unique pour la règle.
- **Enabled (Activé)** : activez le champ pour associer la rulestack à la règle. Ce champ est activé par défaut.

STEP 4 | Définissez des critères de correspondance pour les champs d'adresse IP **Source** et de **Destination**.

STEP 5 | Configurez les **Granular Controls (Contrôles granulaires)**.

- Spécifiez les **critères de correspondance d’application** que vous souhaitez que la règle autorise ou bloque.

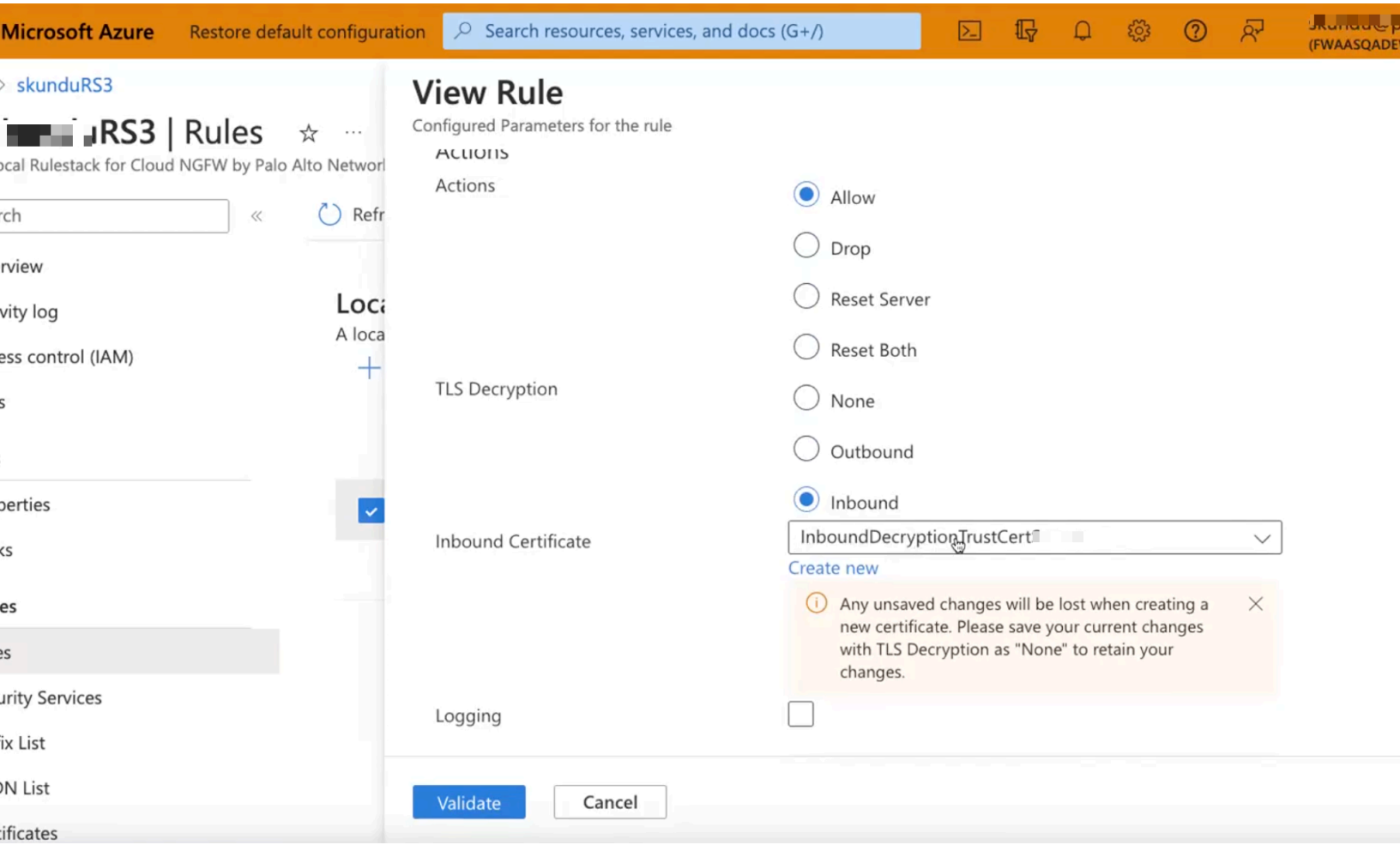
  *Vous pouvez créer des règles de décryptage TLS avec **Applications(App-ID™) – Any (N’importe laquelle)** ou **SSL – Match (Correspondance)** uniquement.*

- Précisez une **URL Category (Catégorie d'URL)** en tant que critère de correspondance de la règle.
- Spécifiez le **protocole et les ports** que vous souhaitez que la règle autorise ou bloque.

  Étape 6 Spécifiez le **A**

- **Allow (Autoriser)** : autoriser le trafic.
- **Deny (Refuser)** : bloque le trafic et applique l’**action d’abandon** définie par défaut pour l’application refusée.
- **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.

STEP 6 | Sous **TLS Decryption (Décryptage TLS)**, sélectionnez **Inbound (Entrant)** et sélectionnez un **Inbound Inspection Certificate (Certificat d'inspection entrante)**.



- *Si ce n'est déjà fait, créez un certificat. L'Amazon Resource Name (ARN) du secret doit être utilisé dans l'ARN du certificat lors de la création de l'objet de certificat.*
- *PKCS8 est le format de certificat pris en charge.*
- *Le décryptage entrant prend en charge les certificats auto-signés et signés par l'autorité de certification racine et ne prend pas en charge les certificats chaînés.*
- *Le profil de décryptage pour le décryptage TLS est défini sur la politique de sécurité des meilleures pratiques. Voir décrypter le trafic pour une visibilité complète et une inspection des menaces pour plus d'informations.*

STEP 7 | Sélectionnez **Logging (Journalisation)** pour activer la journalisation.

STEP 8 | Cliquez sur **Validate (Valider)**.

STEP 9 | Cliquez sur **Config ActionsDeploy ConfigurationCommit** pour enregistrer la règle dans la configuration en cours du pare-feu.

Gestion des politiques de Panorama

Utilisez les informations de cette section pour configurer et intégrer Cloud NGFW pour Azure à l’appareil virtuel Palo Alto Networks Panorama.

Intégration de Panorama

Cloud NGFW est le seul NGFW alimenté par l'apprentissage machine (ML) du secteur fourni en tant que service cloud natif sur Azure. Grâce à Cloud NGFW, vous pouvez exécuter plus d'applications en toute sécurité à une vitesse et une échelle de cloud avec une expérience cloud native réelle. Vous bénéficiez du meilleur des deux mondes grâce à la sécurité réseau intégrée nativement fournie en tant que service sur Azure.

Ce document explique comment configurer et intégrer Cloud NGFW pour Azure au Panorama de Palo Alto Networks.

Vous pouvez utiliser un appareil Panorama pour gérer un ensemble partagé de règles de sécurité de manière centralisée sur les ressources Cloud NGFW, en même temps que vos appareils de pare-feu physiques et virtuels. Vous pouvez également gérer tous les aspects de la configuration des objets et des profils partagés, transmettre ces règles et générer des rapports sur les modèles de trafic ou les incidents de sécurité de vos ressources Cloud NGFW, le tout depuis une seule console Panorama.

Panorama fournit un emplacement unique à partir duquel vous pouvez centraliser la gestion des politiques et des pare-feu sur les pare-feu matériels, virtuels et cloud, améliorant ainsi l'efficacité opérationnelle de la gestion et de la maintenance d'un réseau hybride de pare-feu.

Comment fonctionne l'intégration ?

Lorsque vous créez une ressource Cloud NGFW à l'aide du portail Azure, vous avez la possibilité d'utiliser Palo Alto Networks Panorama pour gérer vos politiques de sécurité. Vous pouvez ensuite gérer un ensemble partagé de règles de sécurité de manière centralisée sur les ressources Cloud NGFW que vous créez en même temps que vos appareils de pare-feu physiques et virtuels, et vous pouvez utiliser la journalisation, les rapports et l'analytique des journaux, le tout depuis une console Panorama.

Lorsqu'un pare-feu atteint un état défectueux et est déconnecté, il est supprimé de Panorama après un certain temps, généralement 3 jours. Cela garantit qu'il n'est pas supprimé prématurément.

Composants de l'intégration

Les composants Palo Alto Networks suivants sont utilisés pour intégrer votre ressource Cloud NGFW à Panorama.

La gestion des politiques de Palo Alto Networks est le composant principal et obligatoire de la solution. Vous devez utiliser un appareil **Panorama** pour créer et gérer des politiques pour vos ressources Cloud NGFW. Le composant de gestion des politiques permet également d'associer vos politiques et objets créés à plusieurs ressources Cloud NGFW dans différentes régions Azure.

Le plug-in Azure Panorama est un composant obligatoire de cette solution. Le plug-in Azure Panorama vous permet de créer des groupes d'appareils Cloud et des piles de modèles Cloud qui vous aident à gérer les politiques et les objets sur les ressources NGFW liées à Panorama.

Les groupes d'appareils Cloud (Cloud DG) sont des groupes d'appareils Panorama spéciaux qui vous permettent de créer des règles et des objets pour les ressources Cloud NGFW. Vous pouvez créer des Cloud DG à l'aide de l'interface utilisateur du plug-in Azure Panorama en spécifiant la ressource Cloud NGFW et les informations de région Azure. Cloud DG se manifeste sous la forme d'une rulestack globale dans cette région.

- Le plug-in Azure Panorama vous permet de créer plusieurs groupes d'appareils Cloud.

- Vous pouvez utiliser la page du groupe d'appareils de l'interface utilisateur Panorama native pour gérer les configurations de politiques et d'objets dans les groupes d'appareils Cloud, ainsi que les objets et profils de sécurité qui leur sont associés.
- Vous pouvez également exploiter vos objets et profils partagés existants dans vos groupes d'appareils Panorama existants en vous y référant dans les règles de sécurité que vous créez dans vos groupes d'appareils Cloud.
- Vous pouvez également ajouter ces Cloud DG à la hiérarchie du groupe d'appareils que vous gérez dans votre Panorama pour hériter des règles et des objets du DG. Toutefois, les Cloud NGFW ne peuvent actuellement pas appliquer toutes les règles héritées par le groupe de périphériques Cloud, notamment celles qui utilisent des zones de sécurité ou des utilisateurs.
- Vous pouvez associer le même Cloud DG à plusieurs régions de la ressource Cloud NGFW. Ce Cloud DG se manifestera sous la forme d'une rulestack globale dédiée dans chaque région Azure de votre ressource Cloud NGFW.

Les piles de modèles Cloud (Cloud TS) sont des piles de modèles Panorama spéciaux qui permettent à vos règles de sécurité dans les groupes d'appareils Cloud de se référer aux paramètres des objets que Panorama vous permet de gérer à l'aide de modèles. Lors de la création d'un Cloud DG, le plug-in Azure Panorama vous permet de créer ou de spécifier une pile de modèles Cloud. Le plug-in crée automatiquement cette Cloud TS et l'ajoute au groupe d'appareils Cloud en tant que pile de modèles de référence. Vous pouvez désormais utiliser la page Pile de modèles de l'interface utilisateur Panorama native pour configurer vos modèles et les ajouter à ces piles de modèles Cloud.

Vous ne pouvez pas modifier le nom de la pile de modèles après le déploiement de Cloud NGFW.

- Le service Cloud NGFW de Palo Alto Networks gère la plupart des configurations d'appareils et de réseau dans vos ressources Cloud NGFW. Par conséquent, Cloud NGFW va ignorer les paramètres d'infrastructure tels que les interfaces, les zones et les protocoles de routage si vous les avez configurés dans des modèles ajoutés à la Cloud TS.
- Cloud NGFW respecte actuellement la gestion des certificats et les paramètres du journal dans vos modèles, tels que référencés par la configuration Cloud DG. Il ignore tous les autres paramètres.

Vous ne devez pas attribuer des appareils gérés à des groupes d'appareils Cloud et à des piles de modèles Cloud.

Étapes d'intégration

Certaines étapes sont nécessaires pour intégrer Cloud NGFW à Panorama. Vous devez d'abord préparer votre appareil virtuel Panorama à cette intégration en installant le plug-in Azure. Une fois que vous avez lié Cloud NGFW, utilisez Panorama pour gérer les objets et les règles de sécurité.

Pour intégrer le service Cloud NGFW à votre appareil virtuel Panorama :

- Vérifiez que Panorama répond aux Prérequis à l'intégration de Panorama.
- Liez Panorama au Cloud NGFW.
- Utilisez Panorama pour la gestion des politiquesCloud NGFW.

Tenez compte des éléments suivants lors de l'intégration de votre ressource Cloud NGFW à Panorama :

- *Pour déplacer une ressource Cloud NGFW vers un autre Panorama, vous devez la redéployer.*
- *Si vous ajoutez un collecteur de journaux après avoir déployé la ressource Cloud NGFW, vous devez la redéployer.*
- *Si vous modifiez l'adresse IP Panorama, vous devez également la redéployer.*

Prérequis à l’intégration de Panorama

Pour intégrer le service Cloud NGFW à votre appareil virtuel Panorama :

- Configurez Panorama.
  - Déployez Panorama exécutant la version logicielle 11.0.1-h1 et ultérieure ou 10.2.4-h2 et ultérieure.
  - Assurez-vous d’avoir installé une instance Panorama enregistrée avec des licences ayant la capacité nécessaire pour prendre en charge votre déploiement Cloud NGFW pour Azure et activée à l’aide de la licence de support sur le Portail de support client (CSP).

    Vous devez installer le certificat du périphérique sur le serveur de gestion Panorama pour pouvoir authentifier Panorama sur le CSP de Palo Alto Networks et exploiter un ou plusieurs services cloud.
  - Assurez-vous que vous êtes membre du compte CSP de Palo Alto Networks sur lequel votre organisation a enregistré l’appareil Panorama.

    Pour l’intégration Cloud NGFW et Panorama, veillez à utiliser l’adresse e-mail utilisée pour l’enregistrement avec le compte CSP. Si celle-ci diffère, vous ne pourrez pas configurer Cloud NGFW et l’intégrer à Panorama.
- Installez le plug-in Azure version 5.0.0.
- Assurez-vous d’avoir un rôle administrateur Panorama sur votre instance de Panorama.
- Assurez-vous que votre réseau autorise le trafic ciblant les ports suivants vers votre appareil virtuel Panorama pour garantir la communication entre Cloud NGFW et Panorama : 3978, 28443, 28270.

Scénarios de connectivité

En plus des éléments répertoriés ci-dessus, vous devez également prendre en compte la manière dont vos ressources Cloud NGFW se connectent à Panorama. Pour gérer la politique Cloud NGFW à l’aide de Panorama, Panorama doit disposer d’une connectivité avec votre VNet. Cependant, selon la topologie de votre réseau, la connectivité entre Panorama et votre VNet est activée différemment.

- **Accès au réseau privé avec l’adresse IP privée de Panorama** : vous pouvez déployer Panorama directement dans le sous-réseau privé de votre VNet hub ou dans un autre VNet appairé au VNet Cloud NGFW.

  Lorsqu’il est déployé directement dans le sous-réseau privé de votre VNet hub, Panorama se connecte directement à vos ressources Cloud NGFW, car elles se trouvent dans le même sous-réseau. Lorsque vous déployez Panorama dans un VNet appairé avec le sous-réseau privé du VNet hub associé à Cloud NGFW, l’appairage VNet permet à la ressource Cloud NGFW d’atteindre l’adresse IP privée de Panorama.
- **Accès à Panorama sur site via un VPN** : si votre instance de Panorama est déployée sur site, les ressources Cloud NGFW peuvent atteindre l’adresse IP privée de Panorama via un VPN. De plus, ce scénario prend en charge l’appairage VNet.

  Dans ce scénario, Panorama est déployé sur votre réseau sur site et utilise une connexion de passerelle VPN directement au VNet hub Cloud NGFW ou à un VNet hub appairé avec le VNet hub Cloud NGFW. Dans chaque cas, le VNet hub doit avoir un itinéraire pointant vers le tunnel VPN avec

l’adresse IP privée de Panorama comme destination. Pour plus d’informations sur cette configuration, reportez-vous à la section Configurer le transit de passerelle VPN pour l’appairage de réseau virtuel.

- **Accès IP public de Panorama via Internet** : s’il n’y a pas de connectivité d’appairage VNet, VPN ou VWAN entre Panorama et votre VNet hub Cloud NGFW, vos ressources Cloud NGFW peuvent se connecter à l’adresse IP publique de Panorama via Internet. Pour autoriser cette connectivité, vous devez créer une règle de groupe de sécurité réseau dans Azure pour autoriser le trafic entrant depuis l’adresse IP publique Cloud NGFW vers Panorama les ports utilisés par Panorama.
- **Accès à Panorama depuis n’importe où (VWAN)** : Cloud NGFW pour Azure est déployé en tant que service SaaS géré dans le VWAN Azure, il est donc capable de sécuriser tout le trafic transitant par le hub VWAN. Vos ressources Cloud NGFW peuvent se connecter à l’adresse IP privée d’une instance Panorama déployée à n’importe quel emplacement connecté à votre hub VWAN.

Si votre déploiement Azure VWAN dispose d’un groupe de sécurité réseau pour le trafic est-ouest, vous devez créer une règle de groupe de sécurité réseau autorisant le trafic entrant depuis l’adresse IP privée de la ressource Cloud NGFW vers l’adresse IP privée Panorama.

Lier le Cloud NGFW à Palo Alto Networks Management

Créer un groupe d’appareils Cloud

Après avoir préparé votre environnement pour l’intégration, vous pouvez lier votre Cloud NGFW à l’appareil virtuel Panorama et commencer à utiliser la gestion des politiques. Vous commencez par créer un groupe d’appareils Cloud.

Avec Panorama, vous regroupez les pare-feu de votre réseau en unités logiques appelées *groupes d’appareils*. Un groupe d’appareils permet un regroupement basé sur la segmentation du réseau, la localisation géographique, la fonction d’organisation, ou tout autre aspect commun des pare-feu exigeant des configurations de politiques similaires.

En utilisant des groupes de périphériques, vous pouvez configurer les règles de stratégie et les objets auxquels ils font référence. Vous pouvez organiser un groupe d’appareils hiérarchisé, avec des règles communes et des objets en haut, et des règles spécifiques au groupe d’appareils et des objets à des niveaux ultérieurs. Cela vous permet de créer une hiérarchie de règles qui appliquent la manière dont les pare-feu gèrent le trafic.

Pour plus d’informations, reportez-vous à la section Gérer les groupes d’appareils.

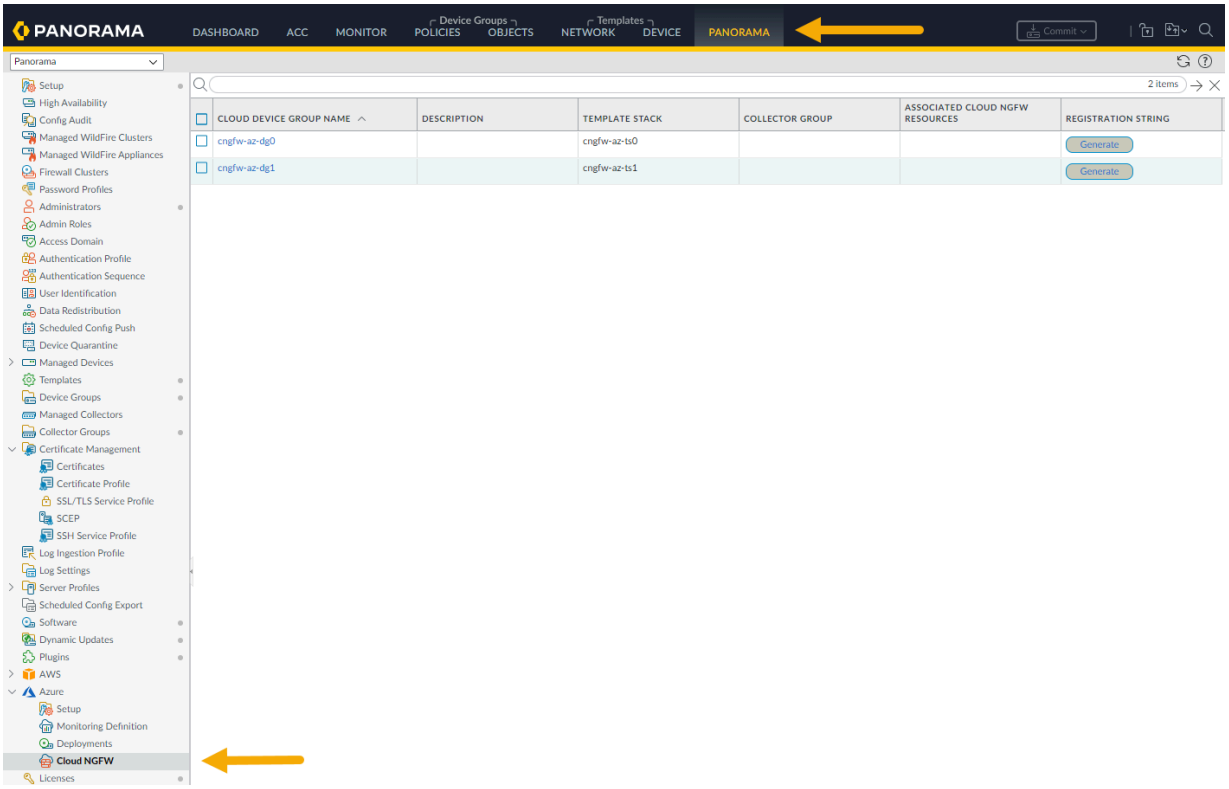
Pour ajouter un groupe d’appareils cloud et une pile de modèles à l’aide de la console Panorama :

STEP 1 | Dans la console Panorama, sélectionnez **Panorama**.

STEP 2 | Dans l’arborescence de navigation, sélectionnez le plug-in **Azure**.

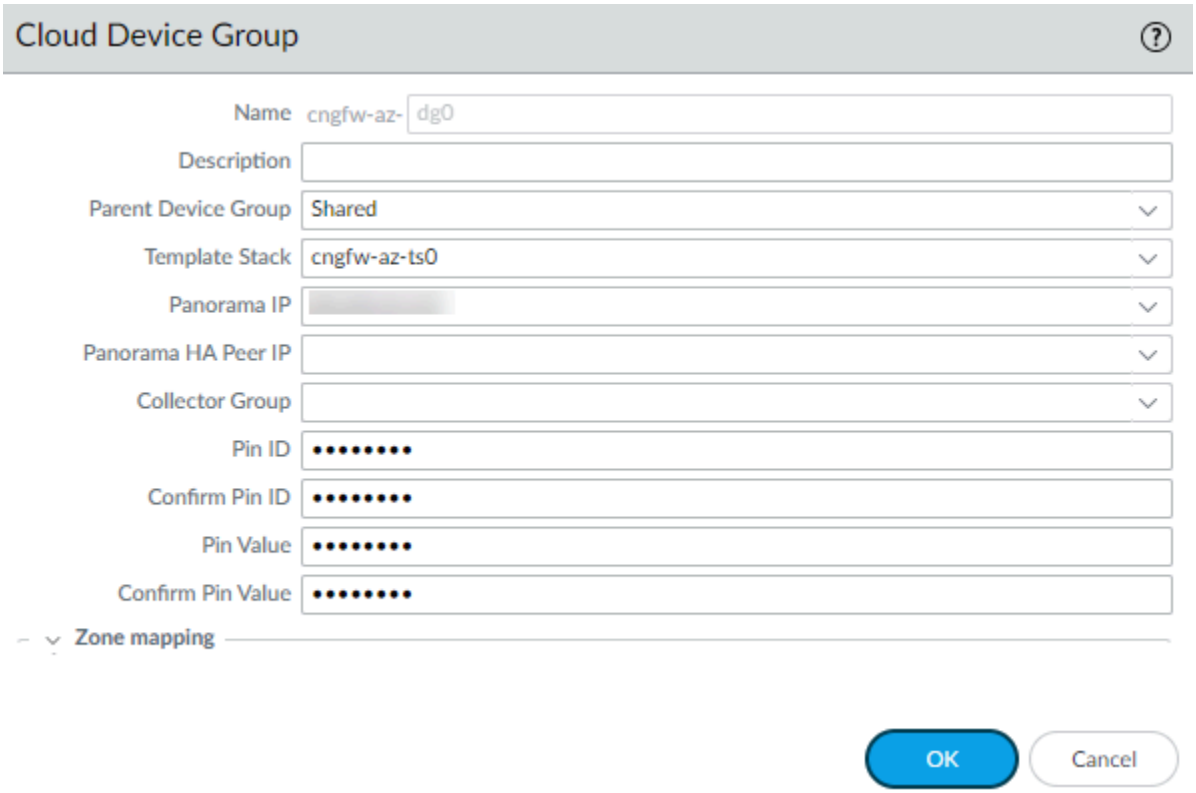
STEP 3 | Développez le plug-in Azure pour afficher les options de configuration. Sélectionnez **Cloud NGFW** pour afficher l’écran Cloud Device Group (Groupe d’appareils Cloud). Si l’option Cloud NGFW

n’apparaît pas, vérifiez que vous avez bien installé le plug-in Azure ; sélectionnez **Panorama** > **Plugins (Plug-ins)** pour afficher la liste des plug-ins installés.



STEP 4 | Dans la partie inférieure gauche de la console Panorama, cliquez sur **Add (Ajouter)** pour créer un nouveau groupe d’appareils Cloud.

STEP 5 | Dans l’écran Cloud Device Group (Groupe d’appareils Cloud) :

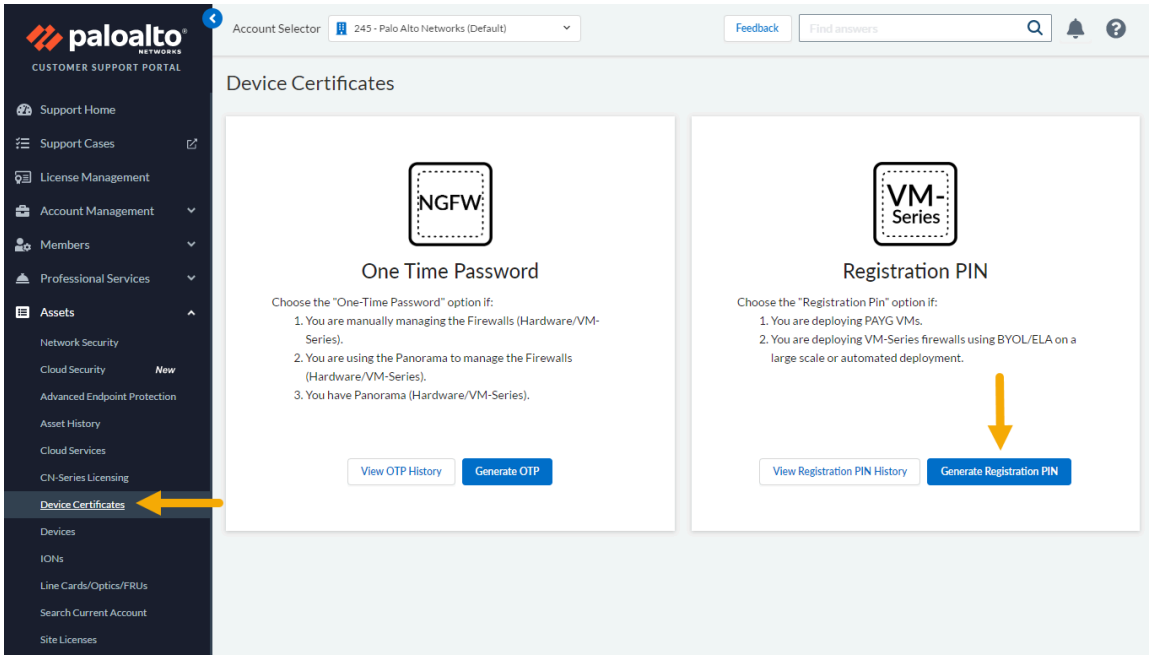


1. Saisissez un **nom** unique pour le groupe d’appareils cloud.
2. Saisissez une **Description (Description)**.
3. Utilisez le menu déroulant pour sélectionner le **groupe d’appareils parent**. Par défaut, cette valeur est partagée.
4. Sélectionnez la Template Stack (Pile de modèles) dans le menu déroulant. Ou cliquez sur **Add (Ajouter)** pour en créer une. Vous ne pouvez pas modifier le nom de la pile de modèles après le déploiement du Cloud NGFW.
5. Sélectionnez l’adresse **IP Panorama** utilisée par le déploiement. Le menu déroulant vous permet de sélectionner l’adresse IP *privée* ou *publique*.
6. Sélectionnez éventuellement l’adresse IP **de l’homologue HA Panorama**.
7. Utilisez éventuellement le menu déroulant pour sélectionner le groupe de collecteurs.
8. Fournissez le**PIN ID (ID de PIN)**. Cette valeur est fournie par le portail de support client.

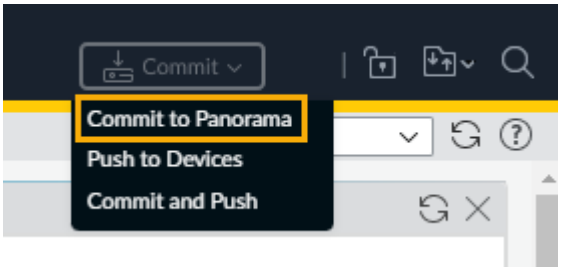
   Pour récupérer le code PIN, vous avez besoin d’un compte sur le portail de support client (CSP) de Palo Alto Networks.

   L’ID de PIN expire au bout d’un an. Cette opération est facultative si vous avez déjà enregistré le numéro de série Cloud NGFW. Si vous ne l’avez pas encore fait, enregistrez votre Cloud NGFW à l’aide du numéro de série sur le même compte CSP où vous avez enregistré votre appareil virtuel Panorama.
9. Pour récupérer l’ID et la valeur PIN, connectez-vous au **portail de support client** en tant qu’utilisateur enregistré.

10. Sur la page du portail de support client, sélectionnez **Assests (Ressources)** > **Device Certificates (Certificats du périphérique)**.
11. Sur la page **Device Certificates (Certificats du périphérique)**, sélectionnez **Generate Registration PIN (Générer un PIN d'enregistrement)** pour le pare-feu VM-Series.



12. Copiez les ID d'enregistrement nouvellement créés et collez-les dans les champs **PIN ID (ID de PIN)** et **PIN Value (Valeur PIN)** de l'écran Cloud Device Group (Groupe d'appareils Cloud).
13. Confirmez l'ID et la valeur PIN.
14. Configurez éventuellement Zone Mapping (Mappage de zone) pour le groupe d'appareils Cloud. Seules 2 zones sont prises en charge : *public*/*privé*.
15. Cliquez sur **OK**.
16. Validez votre modification dans la console Panorama pour créer le groupe d'appareils cloud. Ensuite, générez la chaîne d'enregistrement pour créer la ressource Cloud NGFW et la déployer dans Azure.



Dans certains cas, vous pouvez rencontrer une erreur de validation lors de la configuration d'un groupe d'appareils Cloud. Pour résoudre ce problème, assurez-vous que le plug-in Azure pour Panorama est correctement installé à l'aide des informations d'identification de l'administrateur. Pour les environnements HA, installez le plug-in sur le nœud secondaire, puis installez-le sur le nœud principal.

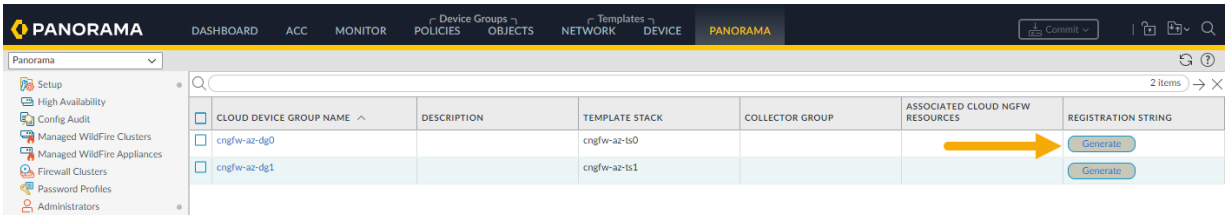
Générer la chaîne d'enregistrement pour créer le Cloud NGFW et le déployer dans Azure

Après avoir validé la modification pour créer le groupe d'appareils cloud, vous pouvez générer la chaîne d'enregistrement. Cette chaîne est utilisée pour créer et déployer le Cloud NGFW dans Azure.

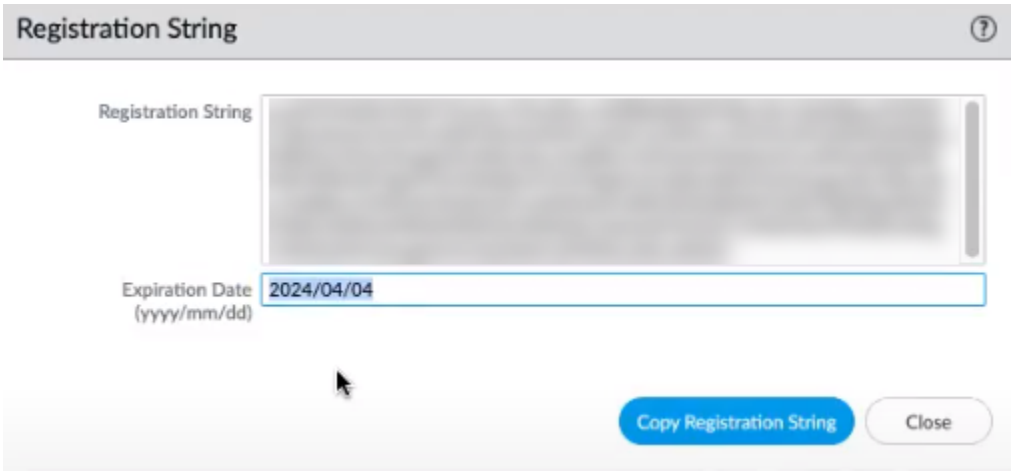
Pour récupérer le code PIN :

STEP 1 | Dans la console Panorama, recherchez le groupe d'appareils Cloud que vous avez créé dans la section précédente.

STEP 2 | Dans le champ Registration String (Chaîne d’enregistrement), cliquez sur **Generate (Générer)**.

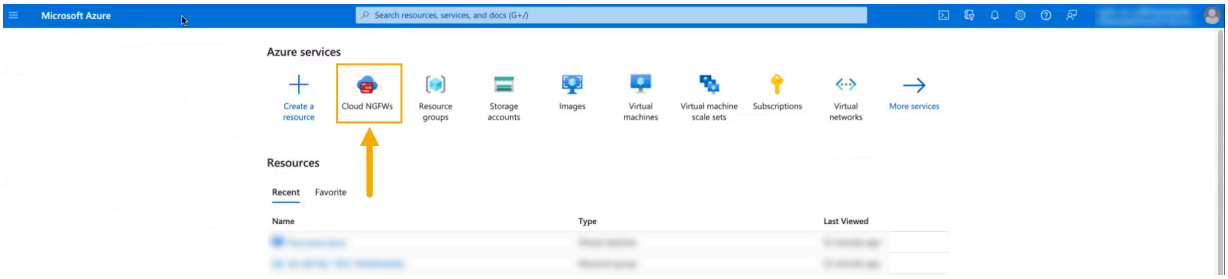


STEP 3 | Sélectionnez **Copy Registration String (Copier la chaîne d’enregistrement)**.

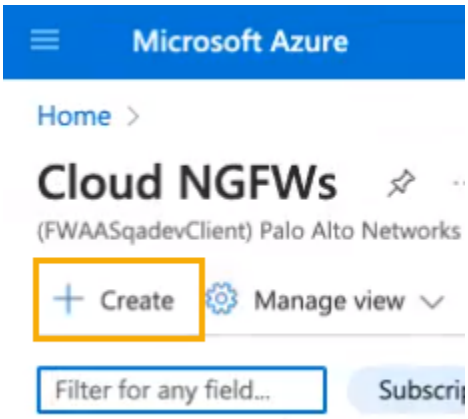


Après avoir copié la chaîne d’enregistrement, accédez à Azure Marketplace pour créer une ressource Cloud NGFW.

STEP 4 | Dans l'Azure Marketplace, sélectionnez **Cloud NGFW**.

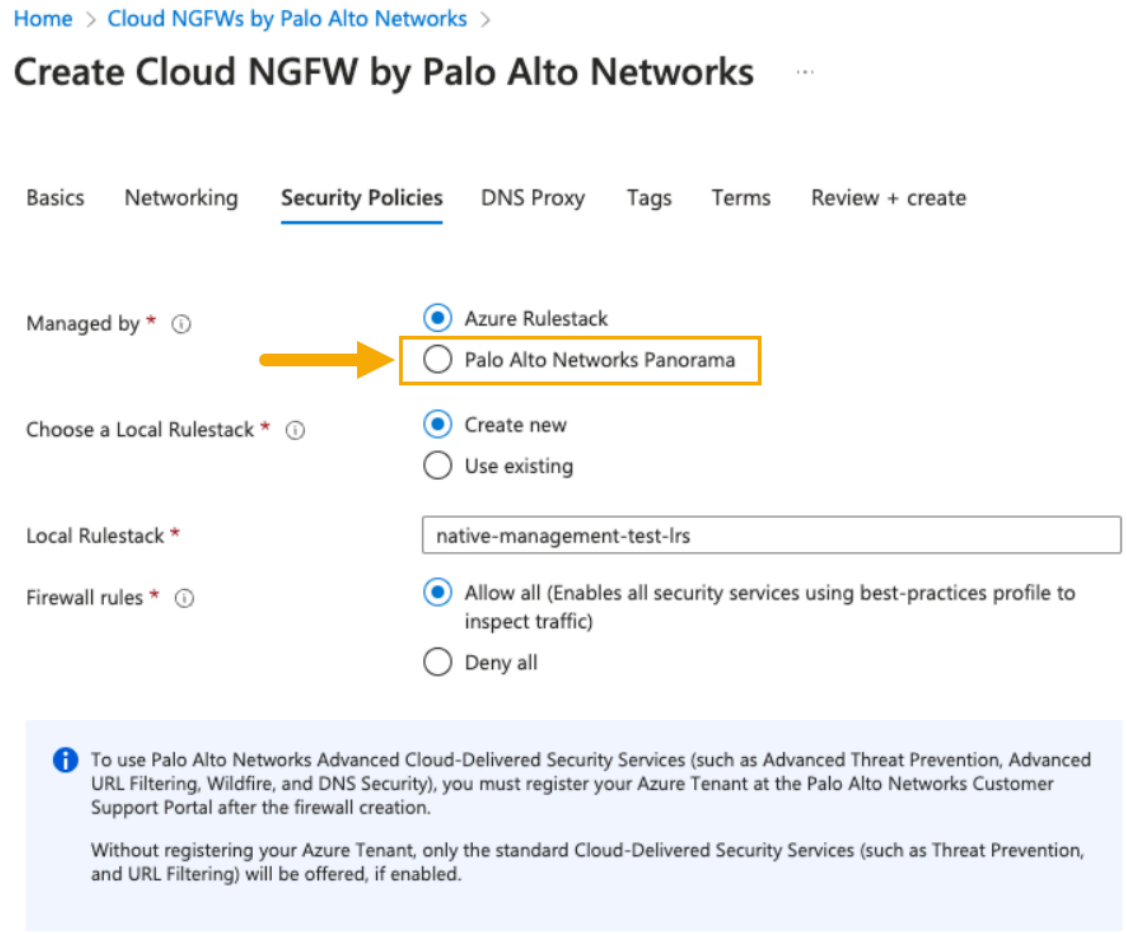


STEP 5 | Cliquez sur **+ Create (+ Créer)** pour créer une ressource Cloud NGFW.



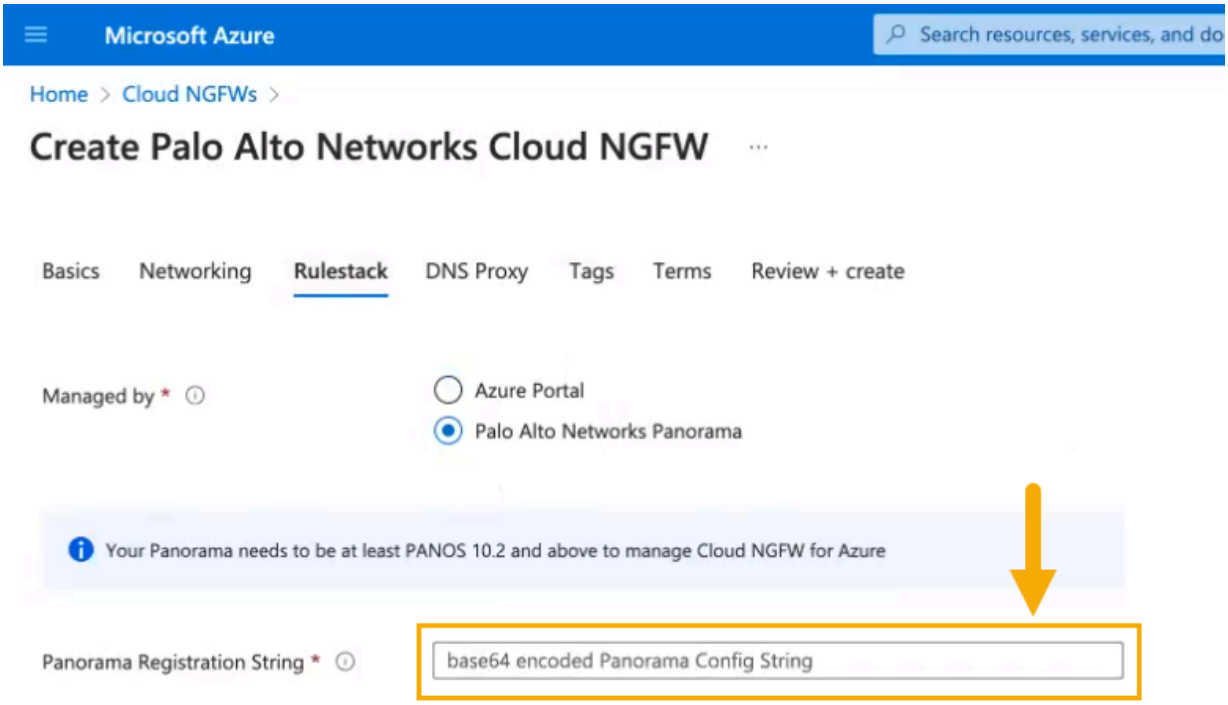
STEP 6 | Suivez les instructions de configuration pour **créer Palo Alto Networks Cloud NGFW**.

1. Configurez les informations de base.
2. Configurez la mise en réseau.
3. Configurez les politiques de sécurité. Dans la section **Managed by (Géré par)**, sélectionnez **Palo Alto Networks Panorama**.



STEP 7 | Après avoir sélectionné **Managed by Palo Alto Networks Panorama (Géré par Palo Alto Networks Panorama)**, la page Security Policies (Politiques de sécurité) inclut le champ **Panorama**

Registration String (Chaîne d’enregistrement Panorama). Saisissez la chaîne d’enregistrement que vous avez copiée à l’étape 3 ci-dessus.



STEP 8 | Poursuivez la création de la ressource Cloud NGFW en renseignant les valeurs DNS Proxy (Proxy DNS), Tags (Étiquettes) et Terms (Conditions). Examinez votre configuration, puis cliquez sur **Create (Créer)**.

La création d’une ressource Cloud NGFW peut prendre environ 10 à 15 minutes.

La console Panorama est désormais liée à la ressource Cloud NGFW.

Utiliser Panorama pour la gestion des politiques Cloud NGFW

Ajouter un groupe d’appareils Cloud

Après avoir lié votre ressource Cloud NGFW à l’appareil virtuel Panorama, vous pouvez commencer à utiliser l’intégration pour des tâches de gestion des politiques, telles que l’ajout de groupes d’appareils et l’application de règles de politique au groupe d’appareils.

Avec Panorama, vous regroupez les pare-feu de votre réseau en unités logiques appelées *groupes d’appareils*. Un groupe d’appareils permet un regroupement basé sur la segmentation du réseau, la localisation géographique, la fonction d’organisation, ou tout autre aspect commun des pare-feu exigeant des configurations de politiques similaires.

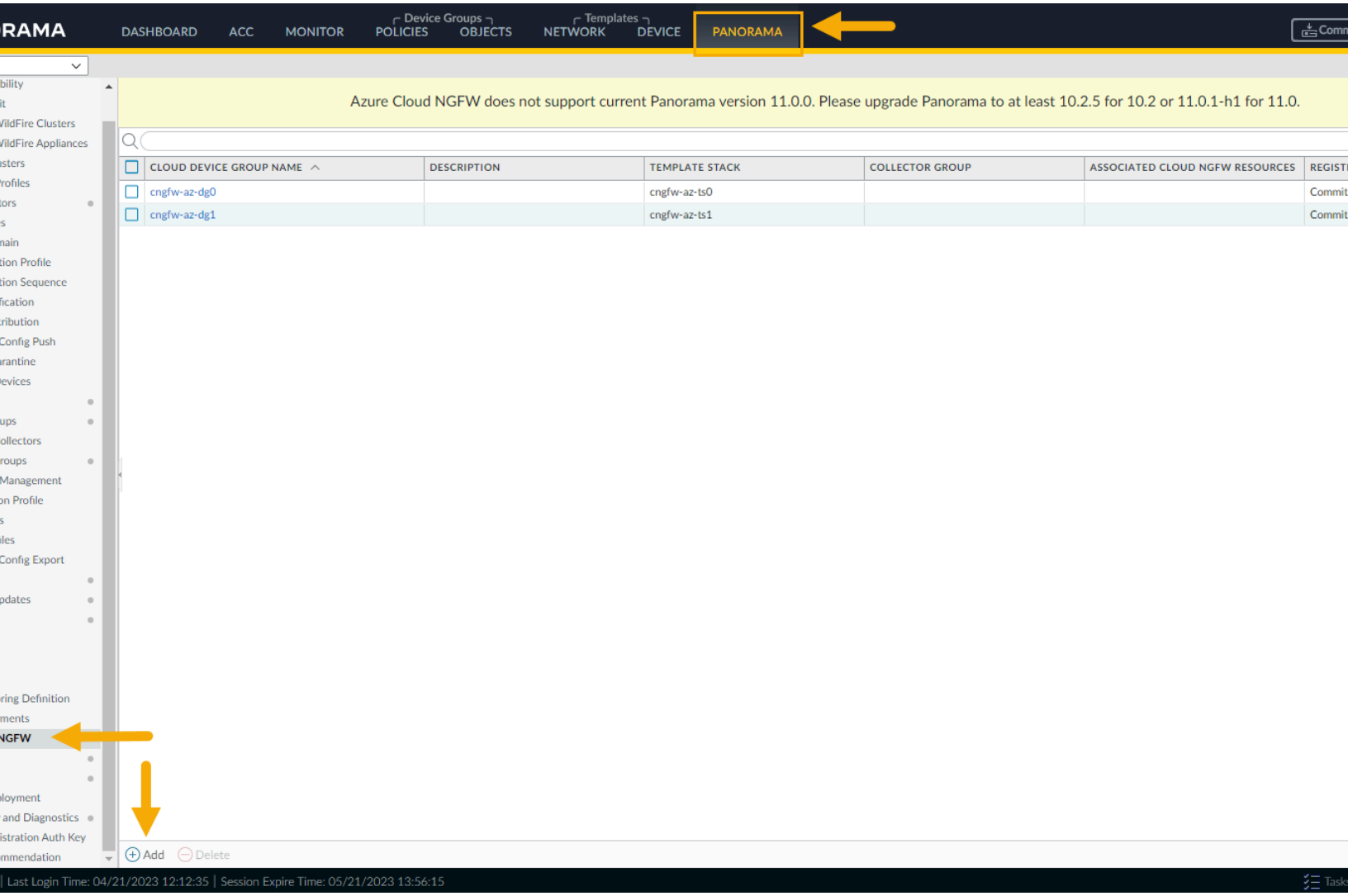
En utilisant des groupes de périphériques, vous pouvez configurer les règles de stratégie et les objets auxquels ils font référence. Vous pouvez organiser un groupe d’appareils hiérarchisé, avec des règles communes et des objets en haut, et des règles spécifiques au groupe d’appareils et des objets à des niveaux ultérieurs. Cela vous permet de créer une hiérarchie de règles qui appliquent la manière dont les pare-feu gèrent le trafic.

Pour plus d’informations, reportez-vous à la section Gérer les groupes d’appareils.

Pour ajouter un groupe d’appareils cloud à l’aide de la console Panorama :

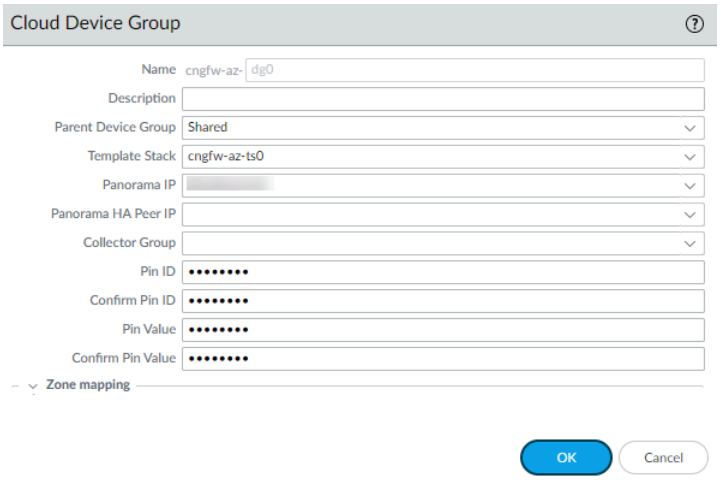
STEP 1 | Dans le plug-in **Azure**, sélectionnez **Cloud NGFW**.

La table Cloud Device Group (Groupe d'appareils Azure) est vide lorsque vous la sélectionnez pour la première fois. Les groupes d'appareils Cloud précédemment créés apparaissent s'ils ont été établis pour la ressource Cloud NGFW à l'aide d'Azure.

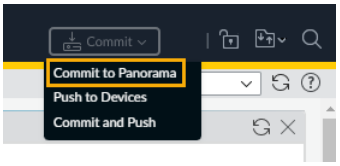


STEP 2 | Cliquez sur **Add (Ajouter)** dans le coin inférieur gauche.

STEP 3 | Dans l’écran **Cloud Device Group (Groupe d’appareils Cloud)** :



1. Saisissez un **nom** unique pour le groupe d’appareils Cloud.
2. Saisissez une **description**.
3. Utilisez la liste déroulante pour sélectionner le **Parent Device Group (Groupe d’appareils parent)**. Par défaut, cette valeur est partagée.
4. Sélectionnez la Template Stack (Pile de modèles) dans le menu déroulant. Ou cliquez sur **Add (Ajouter)** pour en créer une.
5. Sélectionnez l’adresse **IP Panorama** utilisée par le déploiement. La liste déroulante vous permet de sélectionner l’adresse IP *privée* ou *publique*.
6. Sélectionnez éventuellement l’adresse IP **de l’homologue HA Panorama**.
7. Vous pouvez également utiliser la liste déroulante pour sélectionner le groupe de collectionneurs.
8. Configurez éventuellement Zone Mapping (Mappage de zone) pour le groupe d’appareils Cloud. Seules deux zones sont prises en charge : *public ou privé*.
9. Cliquez sur **OK**.
10. Validez votre modification dans la console Panorama pour créer le groupe d’appareils cloud. Ensuite, générez la chaîne d’enregistrement pour créer la ressource Cloud NGFW et la déployer dans Azure.



Supprimer un groupe d’appareils Cloud

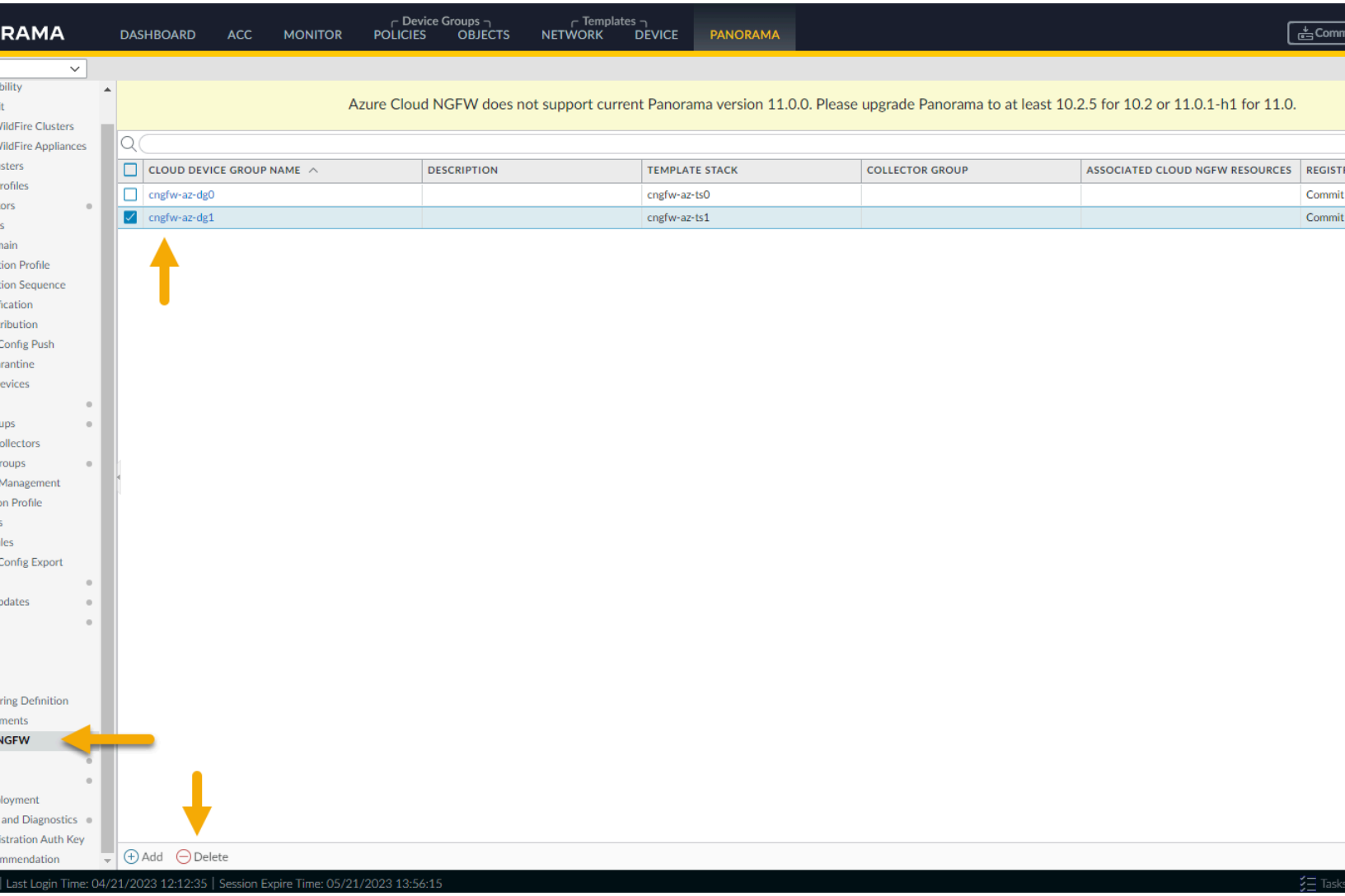
Utilisez la console Panorama pour supprimer un groupe d’appareils Cloud. Vous ne pouvez supprimer un groupe d’appareils Cloud que s’il n’est pas associé à un pare-feu.

Pour supprimer un groupe d’appareils Cloud d’une ressource à l’aide de la console Panorama :

STEP 1 | Dans **Panorama**, sélectionnez **Cloud Device Groups (Groupes d’appareils Cloud)**.

STEP 2 | Sélectionnez le **groupe d’appareils Cloud** que vous souhaitez supprimer.

STEP 3 | Dans la partie inférieure de la console Panorama, cliquez sur **Delete (Supprimer)**.



STEP 4 | Cliquez sur **Yes (Oui)** pour confirmer la suppression.

STEP 5 | Validez la modification.

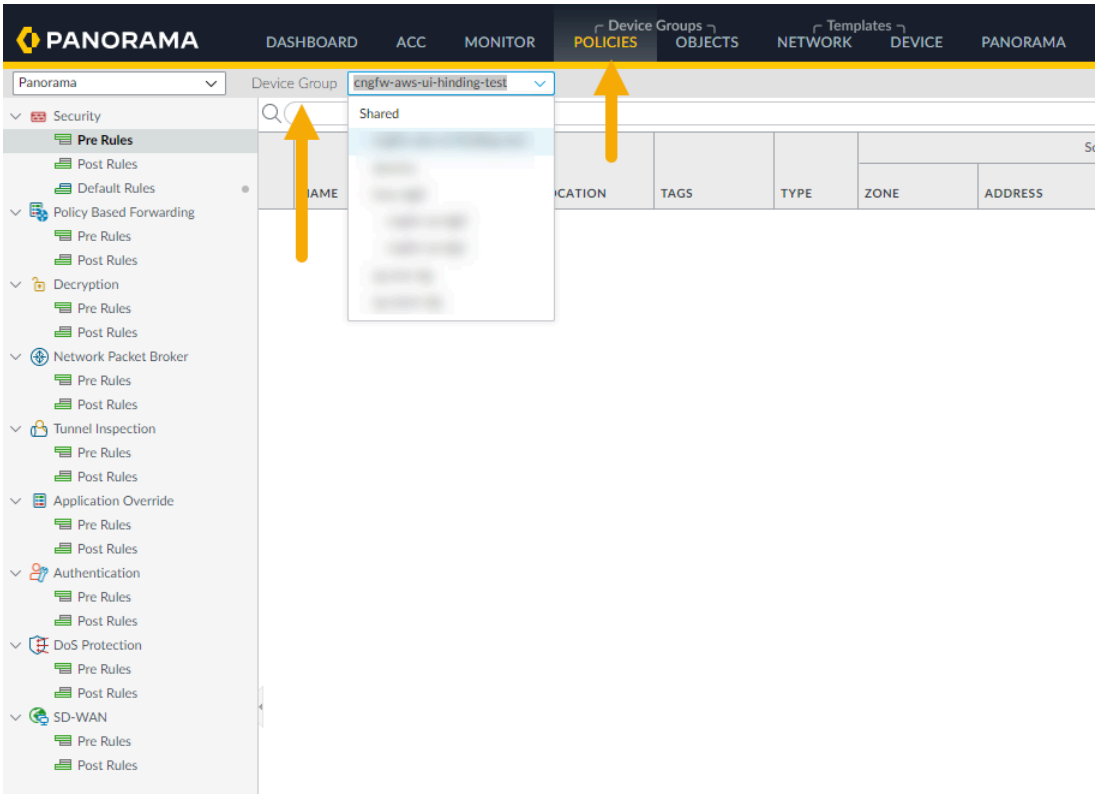
Appliquer la politique

Les groupes d'appareils Cloud sur Panorama vous permettent de gérer de manière centralisée les règles de politique de pare-feu. Vous devez créer les règles de politique sur Panorama en tant que règles « avant » ou règles « après ». Ces règles vous permettent de créer une approche par couches pour la mise en œuvre de la politique. Pour plus d'informations, reportez-vous à la section Définir les politiques sur Panorama.

Pour configurer des règles de politique pour le groupe d'appareils Cloud dans Panorama :

STEP 1 | Sélectionnez **Policies (Politiques)**.

STEP 2 | Dans la section **Device Group (Groupe d'appareils)**, utilisez la liste déroulante pour sélectionner le **groupe d'appareils cloud** précédemment créé.

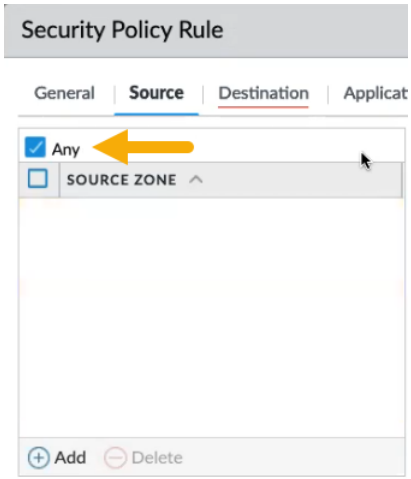


Lorsque vous créez un groupe d'appareils pour Cloud NGFW, le nom commence par *cngfw*. Par exemple *cngfw-démo-azure*

STEP 3 | Dans la partie inférieure gauche de la console, cliquez sur **Add (Ajouter)**.

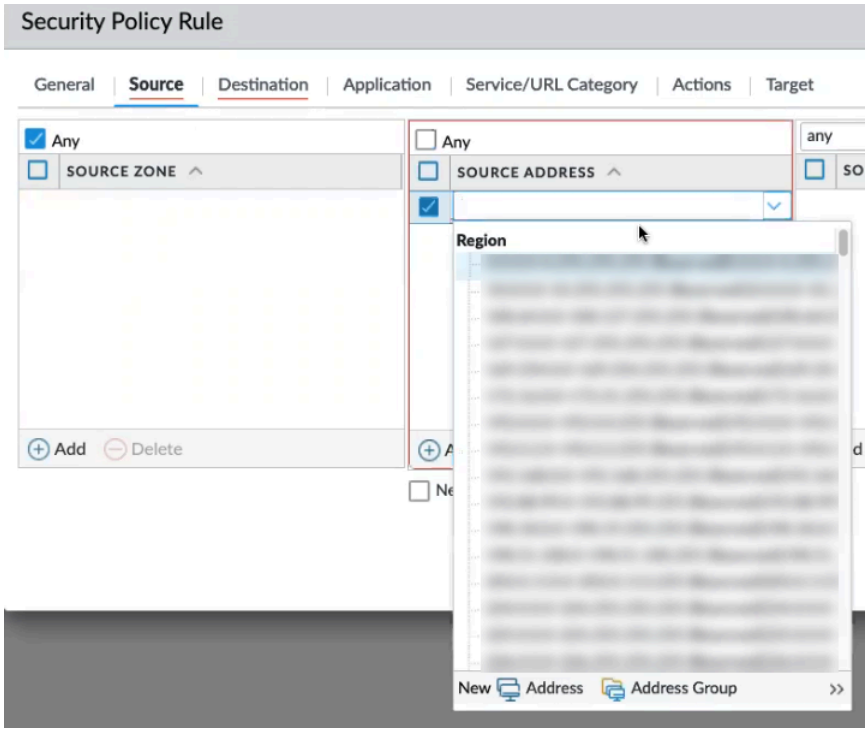
STEP 4 | Dans l’écran Security Policy Rule (Règle de politique de sécurité), configurez les éléments de la politique que vous souhaitez appliquer au groupe d’appareils.

1. Dans l’onglet **General (Général)**, saisissez un nom pour la politique. Fournissez éventuellement des informations supplémentaires.
2. La politique **source** définit la zone source ou l’adresse source qui génère le trafic. Pour **Source Zone (Zone source)**, cliquez sur **Any (N’importe laquelle)**. Vous ne pouvez pas ajouter une zone source spécifique.



Continuez d’appliquer les règles de politique **source** en incluant une **Source Address (Adresse source)**. Cliquez sur **Any (N’importe laquelle)**, ou utilisez la liste déroulante pour sélectionner

une adresse existante, ou utilisez les options pour ajouter une nouvelle adresse ou un nouveau groupe d’adresses.



Pour la politique**Source User (Utilisateur source)** et **Source Device (Périphérique source)**, cliquez sur **Any (N’importe laquelle)**. Cloud NGFW ne prend pas en charge la spécification d’utilisateurs ou d’appareils source spécifiques.

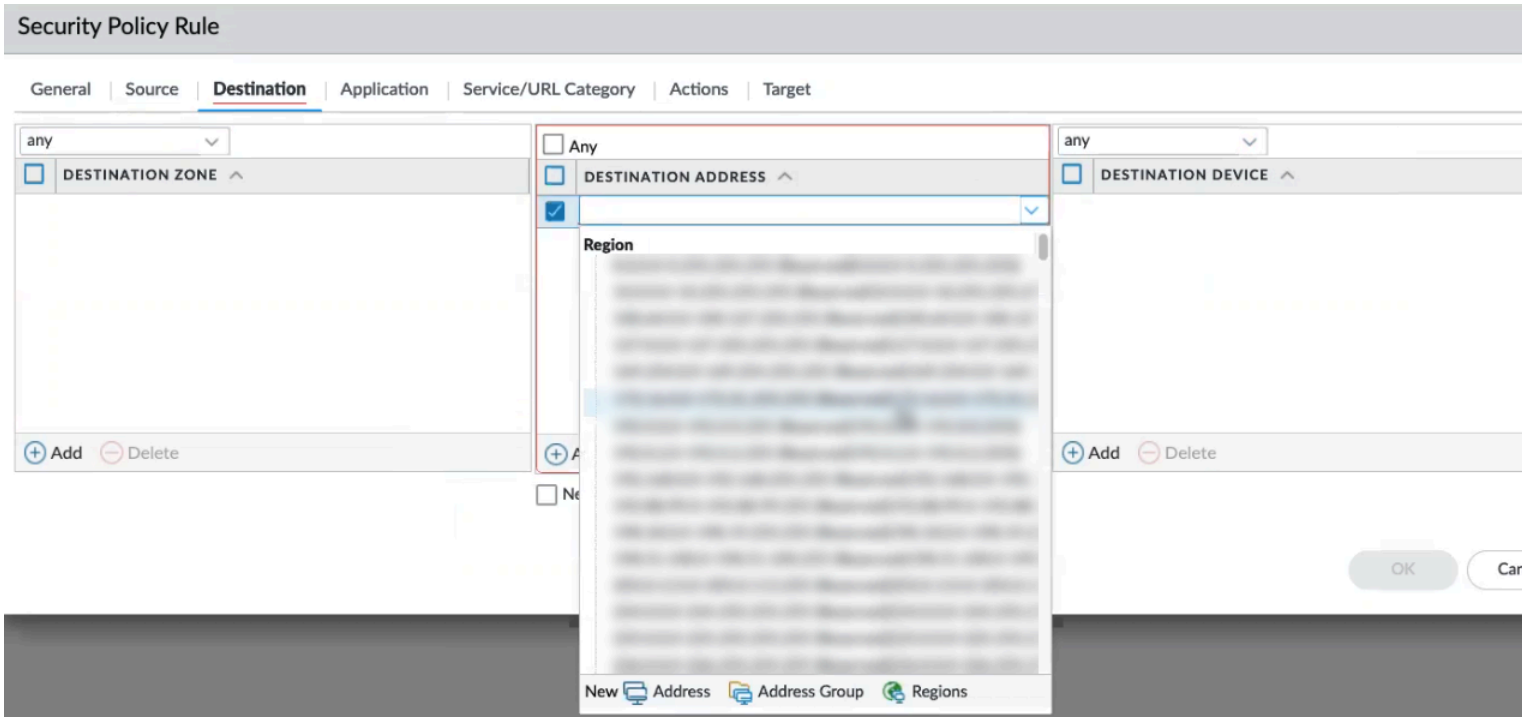
3. La politique de **destination** définit la zone de destination ou l’adresse de destination du trafic. Utilisez la liste déroulante pour sélectionner une adresse existante ou utilisez les options pour

ajouter une nouvelle adresse ou un nouveau groupe d'adresses. La politique de destination comprend les champs pour la zone, l'adresse et l'appareil.

Pour la **Destination Zone (Zone de destination)**, cliquez sur **Any (N'importe laquelle)**. Cloud NGFW ne prend pas en charge l'ajout de zones de destination individuelles.

Pour la **Destination Address (Adresse de destination)**, cliquez sur **Any (N'importe laquelle)**ou utilisez la liste déroulante pour sélectionner une zone existante. Cliquez sur **New (Nouveau)** pour ajouter une adresse, un groupe d'adresses ou une région.

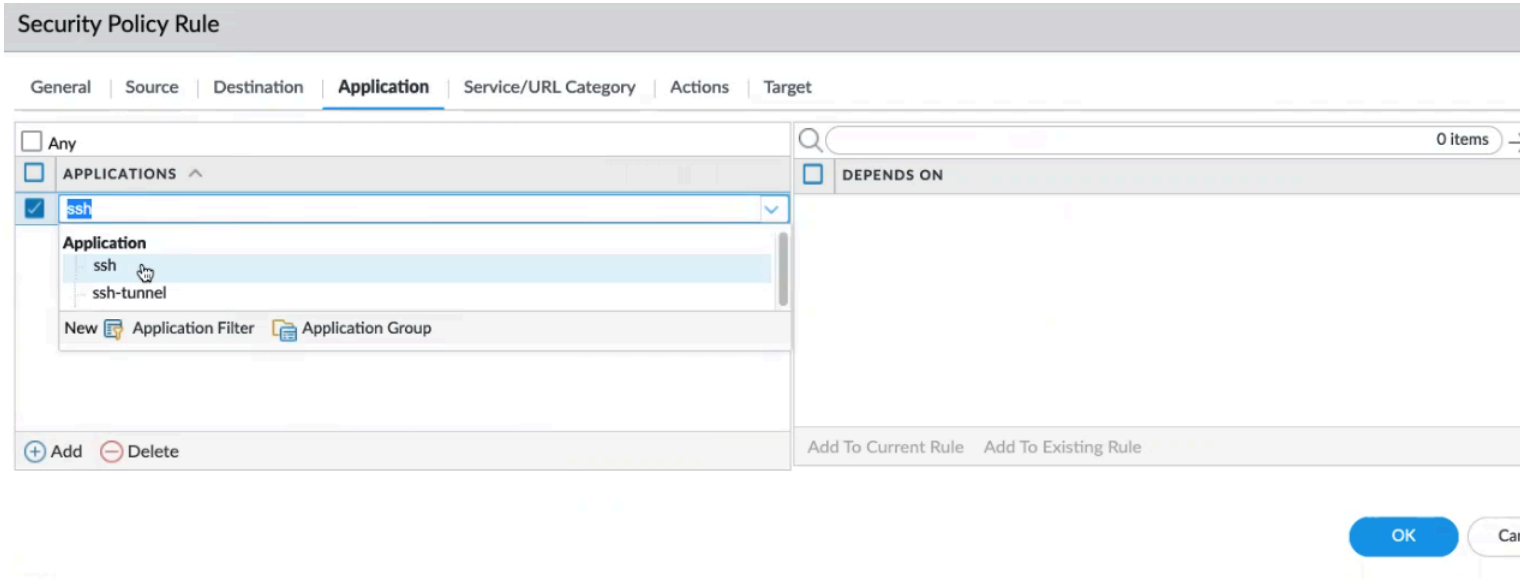
Pour le **Destination Device (Périphérique de destination)**, cliquez sur **Any (N'importe lequel)**. Cloud NGFW ne prend pas en charge l'ajout de périphériques de destination individuels.



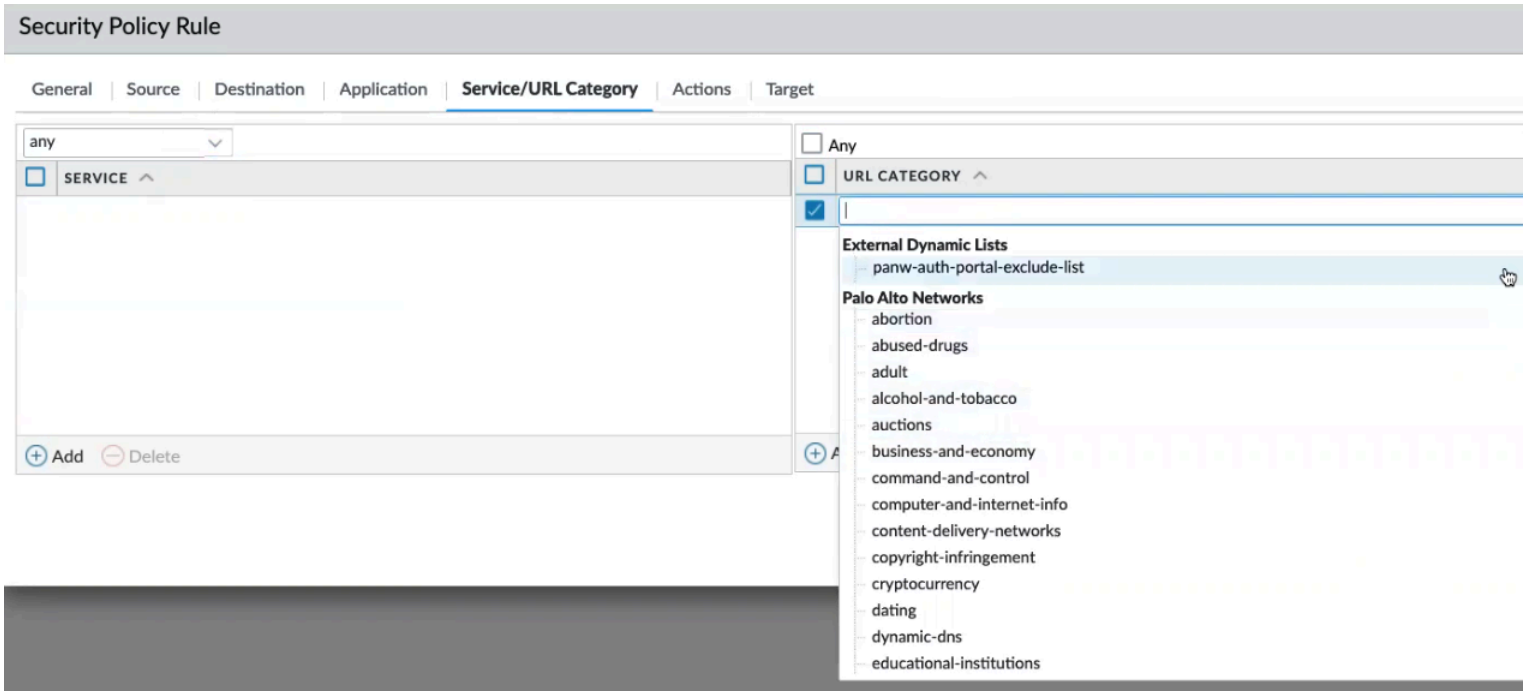
4. Configurez une politique d'**application** pour que l'action de politique se produise en fonction d'une application ou d'un groupe d'applications. Un administrateur peut également utiliser une signature App-ID existante et la personnaliser pour détecter les applications propriétaires ou

certains attributs d’une application existante. Les applications propres à l’entreprise sont définies dans **Objects (Objets) Applications**.

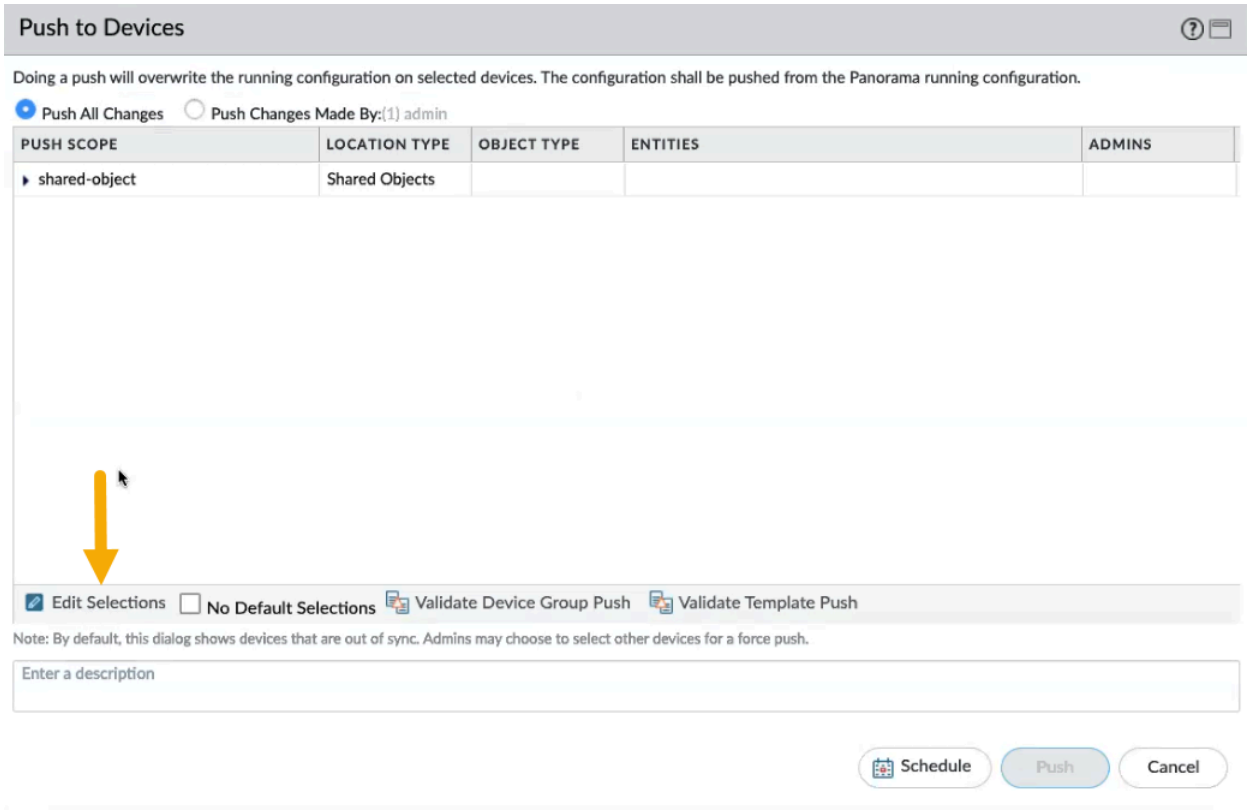
Dans l’écran **Application** , cliquez sur Any (N’importe laquelle) ou indiquez une application spécifique, comme SSH. Cliquez sur **Add (Ajouter)** pour inclure une nouvelle politique d’application.



5. Configurez des règles de politique **Service/URL Category (Catégorie de service/URL)** permettant au pare-feu d’indiquer un numéro de port TCP ou UDP spécifique ou une catégorie d’URL comme critères de correspondance dans la politique. Indiquez des règles de politique de niveau **Service** ou des règles de politique **URL Category (Catégorie d’URL)** en sélectionnant **Any (N’importe laquelle)**,ou utilisez les options de la liste déroulante pour sélectionner individuellement les éléments de la politique que vous souhaitez appliquer. Cliquez sur **Add (Ajouter)** pour créer de nouvelles règles de politique pour le service ou la catégorie d’URL.



STEP 5 | Après avoir appliqué les règles de politique au groupe d'appareils Cloud pour la ressource Cloud NGFW, appliquez les modifications à la console Panorama. Dans l'écran **Push to Devices (Transmettre aux périphériques)**, cliquez sur **Edit Selections (Modifier les sélections)**.



STEP 6 | Sélectionnez les groupes d'appareils Cloud que vous souhaitez transmettre aux ressources, puis cliquez sur **OK** et sur **Push (Transmettre)**.

Activer User-ID sur le Cloud NGFW pour Azure

L'identité de l'utilisateur, contrairement à l'adresse IP, fait partie intégrante d'une infrastructure de sécurité efficace. Le fait de savoir précisément qui utilise chacune des applications de votre réseau, qui a potentiellement introduit une menace ou qui transfert des fichiers, permet de renforcer vos règles de sécurité et de réduire les délais de réponse aux incidents. User-ID™, une fonctionnalité standard sur les pare-feu Palo Alto Networks vous permet de tirer parti des informations utilisateur stockées dans un large éventail de référentiels. Reportez-vous à la documentation PAN-OS pour en savoir plus sur les concepts User-ID.

Pour appliquer la politique depuis User-ID ou Groupes :

- Le pare-feu doit pouvoir mapper les adresses IP aux noms d'utilisateur.
- User-ID fournit divers mécanismes pour collecter les informations de mappage d'utilisateur. Pour en savoir plus, cliquez ici.
- Si les méthodes de mappage ne parviennent pas à capturer le mappage, vous pouvez configurer la politique d'authentification pour rediriger les utilisateurs vers une connexion au portail d'authentification. Les utilisateurs peuvent fournir leurs informations d'identification qui seront vérifiées auprès du fournisseur d'identité et appliquer l'accès en conséquence. Pour en savoir plus sur la politique d'authentification, cliquez ici.

À l'heure actuelle, Cloud NGFW prend en charge le mappage de surveillance du serveur via l'installation de l'agent uniquement.

Pour activer la politique basée sur les utilisateurs et les groupes :

- Le pare-feu exige une liste de tous les utilisateurs disponibles et de leur appartenance aux groupes correspondants.
- Le panorama collecte des informations de mappage de groupe en se connectant directement au serveur LDAP, puis les distribue au Cloud NGFW.

Pour le déploiement Cloud NGFW, nous vous recommandons d'utiliser la surveillance du serveur à l'aide de l'agent Terminal Server de Palo Alto Networks ou d'un agent Windows exécuté sur un serveur de domaine du réseau.

STEP 1 | Activez User-ID.

1. Connectez-vous à Panorama.
2. Sélectionnez **Network (Réseau)** > **Zones**, puis cliquez sur le **nom** de la zone.
3. **Enable User Identification (Activez l'identification de l'utilisateur)**, puis cliquez sur **OK (OK)**.

STEP 2 | Création d'un compte de service dédié pour l'agent User-ID.

STEP 3 | Mappage d'utilisateurs à des groupes.

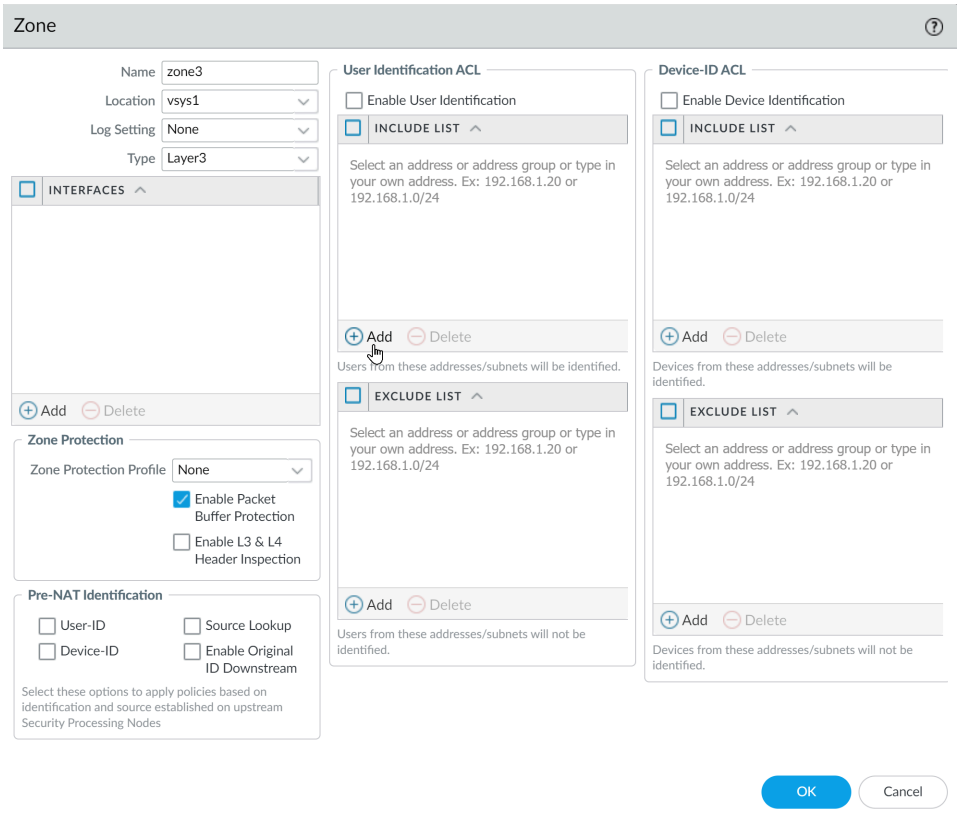
STEP 4 | Configurer le mappage des adresses IP aux utilisateurs. Le Cloud NGFW pour Azure prend en charge le mappage IP à utilisateur à l'aide de l'agent User-ID Windows ou de l'agent Terminal Server.

- Configurer le mappage d'utilisateur à l'aide de l'agent User-ID Windows
- Configurer le mappage d'utilisateur pour les utilisateurs Terminal Server

STEP 5 | Indiquez les réseaux à inclure et à exclure du mappage d'utilisateur.

Il est recommandé de toujours indiquer les réseaux à inclure et à exclure de User-ID. Ainsi, vous pouvez vous assurer que seuls vos actifs de confiance sont sondés et que les mappages d'utilisateur non désirés ne sont pas créés de façon inopinée.

1. Sélectionnez **Network (Réseau)** > **Zones** et sélectionnez Zone où vous configurez User-ID.
2. Ajoutez vos réseaux aux listes **Include (Inclure)** et **Exclude (Exclure)** le cas échéant.
3. Cliquez sur **OK**.



STEP 6 | Activez la mise en œuvre d’une politique basée sur un utilisateur et sur un groupe.

Après avoir activé User-ID sur votre Cloud NGFW, vous pouvez utiliser un nom d’utilisateur ou un nom de groupe comme source ou destination d’une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)** pour créer une règle de politique de sécurité ou cliquez sur un nom de politique de sécurité pour modifier une règle existante.
2. Sélectionnez User (Utilisateur) et spécifiez les utilisateurs et les groupes à mettre en correspondance dans la règle de l’une des manières suivantes :
   - Si vous souhaitez sélectionner des utilisateurs/groupes spécifiques comme critères de recherche, cliquez sur **Add (Ajouter)** dans la section Source User (Utilisateur source) pour afficher la liste des utilisateurs et des groupes détectés par la fonction de mappage de groupe du pare-feu. Sélectionnez les utilisateurs ou les groupes à ajouter à la règle.
   - Si vous souhaitez faire correspondre à tout utilisateur qui a été authentifié ou non et que vous n'avez pas besoin de connaître le nom de l'utilisateur ou du groupe spécifique, sélectionnez

known-user (Utilisateur connu) ou **unknown (Utilisateur inconnu)** dans la liste déroulante Source User (Utilisateur source).

3. Configurez les autres éléments de la règle si nécessaire, puis cliquez sur **OK (OK)** pour l'enregistrer. Pour plus d'informations sur les autres champs de la règle de sécurité, reportez-vous à la section Configuration d’une politique de sécurité de base.

Créez des règles en fonction d'un groupe plutôt que d'un utilisateur lorsque cela est possible. Cela vous évite de continuellement mettre à jour vos règles (ce qui nécessite une validation) lorsque votre base de données d'utilisateurs change.

STEP 7 | Créez les règles de politique de sécurité pour activer User-ID en toute sécurité au sein des zones approuvées et empêcher le trafic User-ID de sortir de votre réseau.

Suivez les Meilleures pratiques de politique de sécurité de la passerelle Internet pour vous assurer que l'application User-ID (`paloalto-userid-agent`) n'est autorisée que dans les zones où les agents (tant vos agents Windows que vos agents intégrés à PAN-OS) surveillent les services et distribuent les mappages aux pare-feu. Plus précisément :

- Autorisez l’application `paloalto-userid-agent` entre les zones où sont situés vos agents et celles où sont situés les serveurs faisant l’objet d’une surveillance (ou, mieux encore, entre les systèmes particuliers qui hébergent l’agent et les serveurs faisant l’objet d’une surveillance).
- Autorisez l’application `paloalto-userid-agent` entre les agents et les pare-feu qui ont besoin des mappages d’utilisateur et entre les pare-feu qui redistribuent les mappages d’utilisateur et les pare-feu qui reçoivent les informations.

Refusez l’application `paloalto-userid-agent` sur toute zone externe, telle que votre zone Internet.

*Il est recommandé de toujours activer l’option **Enable Config Sync (Activer la synchronisation de la configuration)** d’une configuration HA pour vous assurer que les mappages de groupe et les mappages d’utilisateur sont synchronisés entre le pare-feu actif et le pare-feu passif.*

STEP 8 | **Commit (Validez)** vos modifications.

Limitations

- Pour les réseaux de grande envergure, vous pouvez optimiser l’utilisation des ressources en configurant quelques pare-feu pour qu’ils recueillent des données grâce à la redistribution, au lieu de configurer tous vos pare-feu pour qu’ils fassent des requêtes directes auprès des sources de données de mappage. Pour Cloud NGFW dans Azure, la redistribution des fonctionnalités d’information de mappage d’utilisateur n’est pas prise en charge.
- La politique d’authentification et d’autorisation n’est pas prise en charge.
- La méthode de l’agent basé sur PAN-OS pour le mappage User-ID n’est pas prise en charge.
- La méthode XML-API pour le mappage User-ID n’est pas prise en charge.

Configurer les itinéraires de service pour les services sur site

Vous pouvez configurer Cloud NGFW pour Azure pour accéder à des services hébergés sur site comme des serveurs DNS, des listes dynamiques externes, des collecteurs de journaux, syslog, des mises à jour de contenu dynamique, LDAP, MFA, etc. Par défaut, un pare-feu Cloud NGFW accède à ces types de services via son interface de gestion. Cependant, l'utilisation de l'interface de gestion est déconseillée dans certains cas. Palo Alto Networks vous recommande alors de configurer un **itinéraire de service** sur le pare-feu pour accéder à ces services. Lorsque vous utilisez un itinéraire de service, les paquets de service quittent le pare-feu en utilisant un port de données que vous avez attribué à chaque service. En retour, le service envoie sa réponse à l'adresse IP source et à l'interface source configurées.

Panorama et le plug-in Panorama pour Azure 5.1.1 ou version ultérieure sont requis pour configurer un itinéraire de service sur Cloud NGFW pour Azure.

Vous devez utiliser un itinéraire de service dans les scénarios suivants.

- Services hébergés sur votre réseau sur site avec une adresse IP privée. Étant donné que l'interface de gestion Cloud NGFW n'est pas connectée à votre réseau sur site, elle ne peut pas accéder à l'adresse IP privée du service.
- Les services sont accessibles via une adresse IP publique sur Internet, mais une adresse IP source statique est requise dans une configuration de liste d'autorisation. L'interface de gestion Cloud NGFW utilise une adresse IP source traduite par SNAT en adresse IP publique dynamique pour accéder à Internet, ce qui ne fonctionne pas avec une liste d'autorisation. Vous pouvez configurer l'itinéraire de service pour accéder au service sur site à l'aide d'une interface de données publiques et l'adresse IP source du trafic sera traduite par SNAT en adresse IP publique Cloud NGFW.

Par défaut, chaque modèle Cloud NGFW Panorama comprend trois zones : privée, publique et boucle. La zone en boucle utilise une interface loopback.3, qui sert pour l'itinéraire de service.

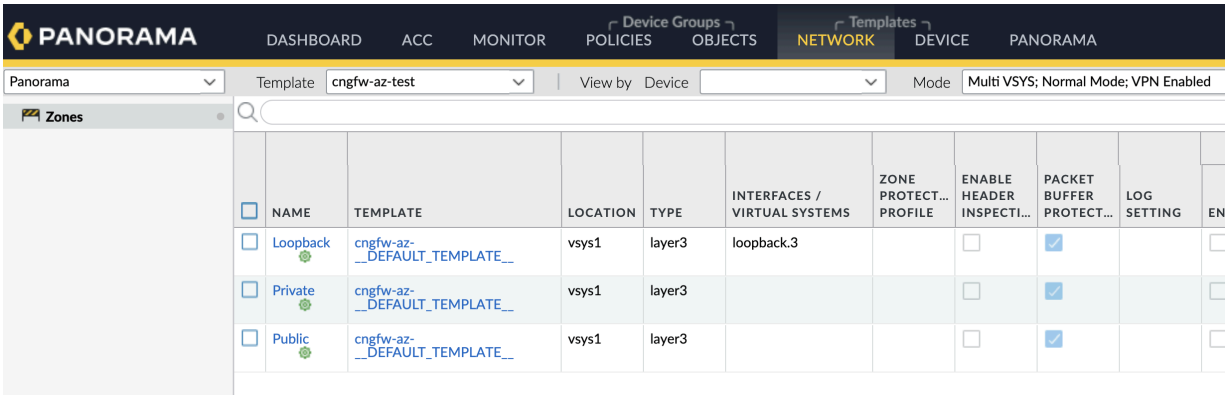
Suivez la procédure suivante pour configurer un itinéraire de service sur Cloud NGFW pour Azure.

STEP 1 | Connectez-vous à Panorama.

STEP 2 | Vérifiez que le plug-in Panorama pour Azure 5.1.1 ou version ultérieure est installé.

STEP 3 | Accédez à **Templates (Modèles)** > **Device (Périphérique)**et sélectionnez votre modèle Cloud NGFW dans la liste déroulante Template (Modèle).

cngfw-az-_DEFAULT_TEMPLATE_ *est visible uniquement après la création de la pile de modèles dans le plug-in Panorama pour Azure sous Cloud NGFW.*



STEP 4 | Accédez à **Setup (Configuration)** > **Services** et cliquez sur **Service Route Configuration (Configuration de l’itinéraire de service)**.

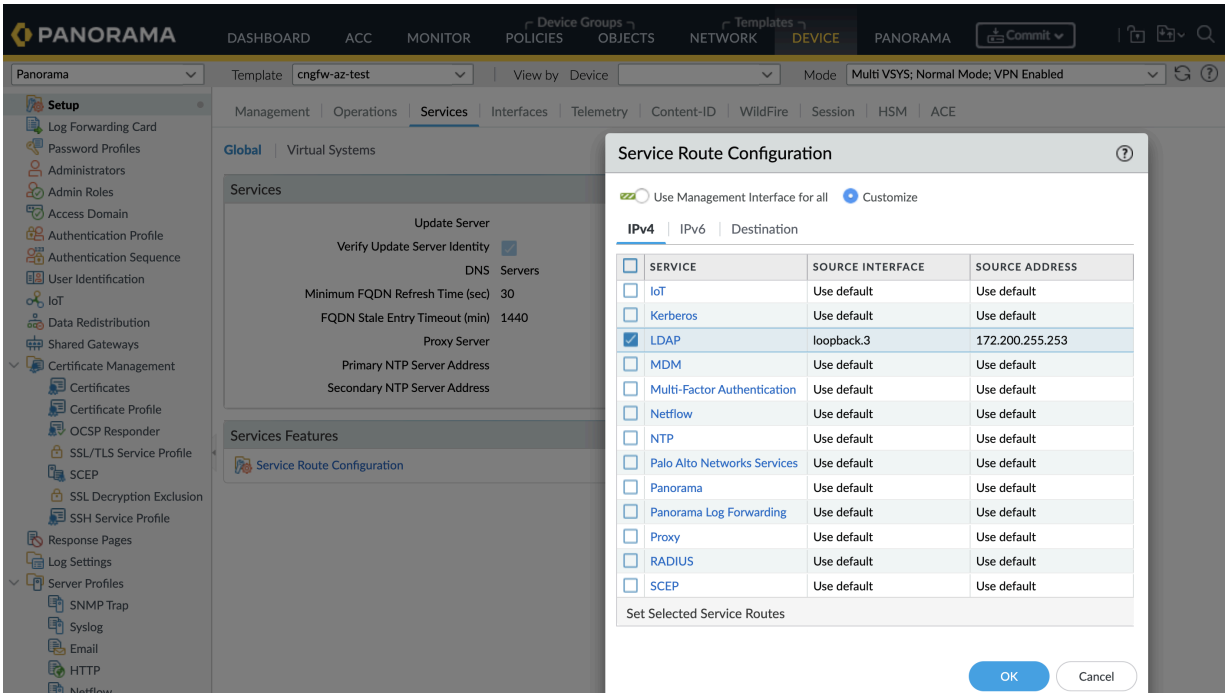
STEP 5 | Sélectionnez **Customize (Personnalisez)** puis l'une des options suivantes pour créer un itinéraire de service :

- Pour un service prédéfini :
  1. Sélectionnez **IPv4** ou **IPv6**, puis cliquez sur le lien du service pour lequel vous souhaitez personnaliser l'itinéraire de service.

     *Pour utiliser facilement les mêmes adresses source pour plusieurs services, cochez les services en question, cliquez sur **Set Selected Routes (Définir les itinéraires de service)**, et passez à l'étape suivante.*
  2. Pour restreindre la liste **Source Address (Adresse source)**, sélectionnez loopback.3 comme **Source Interface (Interface source)**, puis sélectionnez une **Source Address (Adresse source)** (de cette interface) comme itinéraire de service. Un objet d'adresse peut également être référencé en tant qu'adresse source s'il est déjà configuré sur l'interface sélectionnée. Sélectionner **Any (N'importe laquelle)** pour l'interface source rend toutes les adresses IP de toutes les interfaces disponibles dans la liste des adresses source dans laquelle vous sélectionnez une adresse. Ne sélectionnez pas **Use default (Utiliser la valeur par défaut)**, car cela indique au pare-feu d'utiliser l'interface de gestion pour l'itinéraire de service.

     L'adresse source de l'itinéraire de service n'hérite pas des modifications de configuration de l'interface référencée et inversement. La modification d'une adresse IP d'interface en une adresse IP ou un objet d'adresse différent ne mettra pas à jour une adresse source d'itinéraire de service correspondante. Cela peut entraîner un échec de validation et vous obliger à mettre à jour les itinéraires de service vers une valeur d'adresse source valide.
  3. Cliquez sur **OK** pour enregistrer la configuration.
  4. Répétez cette étape si vous voulez définir aussi bien une adresse **IPv4** qu'une adresse **IPv6** pour un service.
- Si le service n'est pas répertorié, sélectionnez l'onglet Destination pour spécifier le service cible par adresses IP :
  1. Sélectionnez **Destination** et **ajoutez** une adresse IP de **destination**. Dans ce cas, si un paquet arrive avec une adresse IP de destination correspondant à cette adresse de **destination** configurée, l'adresse IP source du paquet sera définie sur **Source Address (Adresse source)** configurée à l'étape suivante.
  2. Pour restreindre la liste **Source Address (Adresse source)**, sélectionnez l'interface**loopback.3**, puis sélectionnez Source Address (Adresse source) (de cette interface) comme itinéraire de service. Sélectionner **Any (N'importe laquelle)** pour l'interface source rend toutes les adresses IP de toutes les interfaces disponibles dans la liste des adresses source dans laquelle vous sélectionnez une adresse. Sélectionner MGT force le pare-feu à utiliser l'interface MGT pour l'itinéraire de service.

3. Cliquez sur **OK** pour enregistrer la configuration.



STEP 6 | **Validez** vos modifications.

STEP 7 | Ajoutez une règle de politique de sécurité permettant au Cloud NGFW d’atteindre le service sur site.

La règle de politique de sécurité peut correspondre au trafic de l’itinéraire de service comme :

- Depuis n’importe quelle zone vers la zone publique ou privée, selon que le serveur possède une adresse IP publique ou privée.
- Adresse IP source (172.200.255.253) vers Adresse IP de destination (adresse IP du service).

Utiliser les valeurs d’adresse IP XFF dans une politique

Si vous avez un périphérique en amont, tel qu’un équilibreur de charge, déployé entre les utilisateurs de votre réseau et votre instance Cloud NGFW, ce dernier peut voir l’adresse IP du périphérique en amont comme adresse IP source dans le trafic HTTP/HTTPS que le proxy transmet plutôt que l’adresse IP du client qui a effectué la demande de contenu. Dans de nombreux cas, le périphérique en amont ajoute un en-tête X-Forwarded-For (XFF) aux requêtes HTTP qui incluent l'adresse IPv4 ou IPv6 réelle du client qui a demandé le contenu ou de qui provient la requête.

Dans Microsoft Azure, par défaut, une passerelle d'application insère l'adresse IP source et le port d'origine dans l'en-tête XFF. Pour utiliser les en-têtes XFF dans la politique de votre pare-feu, vous devez configurer la passerelle d'application de manière à omettre le port de l'en-tête XFF. Reportez-vous à la documentation Azure pour savoir comment configurer votre passerelle d’application.

Cette fonctionnalité est prise en charge sur Cloud NGFW géré par Panorama pour Azure uniquement.

Lors de la configuration des règles de politique de sécurité sur Panorama, vous pouvez autoriser Cloud NGFW à utiliser l’adresse IP source dans un champ d’en-tête HTTP XFF pour appliquer la politique de sécurité. Lorsqu’un paquet passe par un serveur proxy unique avant d’atteindre le pare-feu, le champ XFF contient l’adresse IP du point de terminaison d’origine. Toutefois, si le paquet passe par plusieurs périphériques en amont, le pare-feu utilise l'adresse IP la plus récemment ajoutée pour appliquer la politique ou utiliser d'autres fonctionnalités qui reposent sur les informations IP.

STEP 1 | Connectez-vous à Panorama.

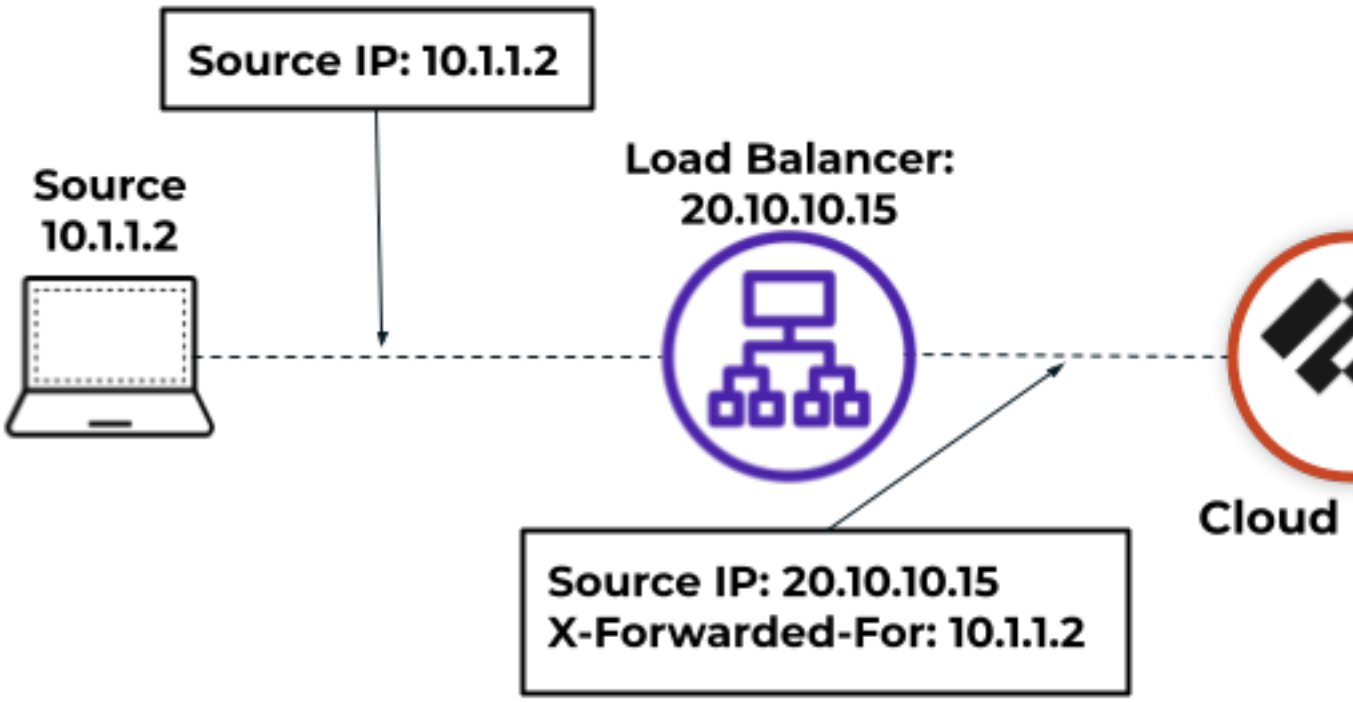
STEP 2 | Sélectionnez votre groupe d’appareils Cloud Cloud NGFW for Azure.

STEP 3 | Sélectionnez **Device (périphérique)** > **Setup (Configurer)** > **Content ID (ID de contenu)** > **X-Forwarded-For Headers (En-têtes X-Forwarded-For)**.

STEP 4 | Cliquez sur l’icône de modification.

STEP 5 | Sélectionnez **Enabled for Security Policy (Activé pour la politique de sécurité)** dans la liste déroulante **Use X-Forwarded-For Header (Utiliser l'en-tête X-Forwarded-For)**.

*Vous ne pouvez pas activer en même temps **Use X-Forwarded-For Header (Utiliser l'en-tête X-Forwarded-For)** pour une politique de sécurité et User-ID.*



STEP 6 | Facultatif Sélectionnez **Strip X-Forwarded-For Header (Enlever l'en-tête X-Forwarded-For)** pour supprimer le champ XFF des requêtes HTTP sortantes.

La sélection de cette option ne désactive pas l'utilisation des en-têtes XFF dans la politique. Le Cloud NGFW pour Azure supprime le champ XFF des requêtes client après l'avoir utilisé pour appliquer la politique.

STEP 7 | Cliquez sur **OK**.

STEP 8 | **Commit (Validez)** vos modifications.

Afficher les journaux et l’activité du Cloud NGFW dans Panorama

Afficher les journaux du Cloud NGFW dans Panorama

Lorsque vos ressources Cloud NGFW sont intégrées à Panorama, les journaux et l’activité sont capturés et affichés dans Panorama dans les onglets Monitoring (Surveillance) et Application Command Center (Centre de commande des applications – ACC). Panorama collecte les journaux générés par Cloud NGFW et les affiche dans l’onglet **Monitor (Surveiller)**. Vous pouvez sélectionner parmi les journaux de trafic, de menace, de filtrage des URL et de décryptage et les filtrer par ID ou par nom. Reportez-vous à la documentation de la journalisation Cloud NGFW pour obtenir des descriptions des champs de journal.

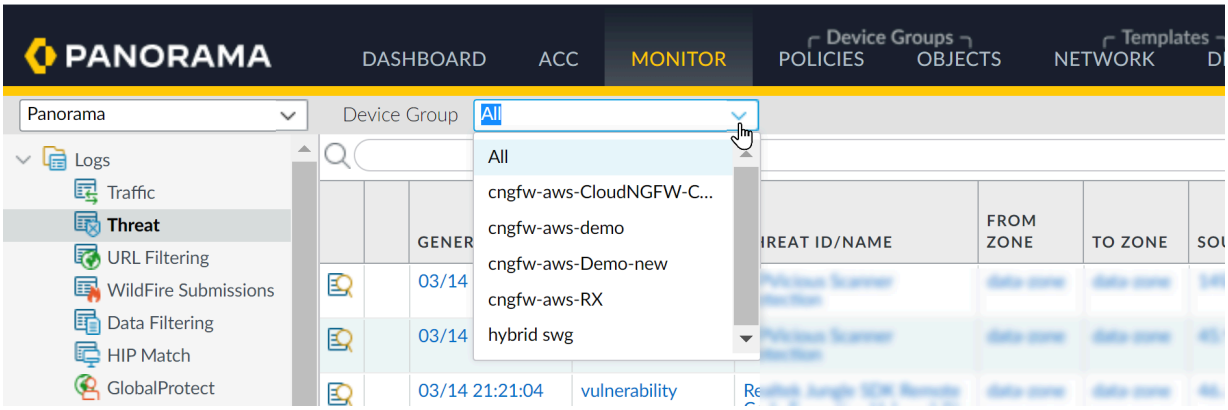
STEP 1 | Connectez-vous à Panorama.

STEP 2 | Sélectionnez **Monitor (Surveiller)**.

STEP 3 | Dans la liste déroulante **Device Group (Groupe d’appareils)**, sélectionnez **Cloud Device Group (Groupe d’appareils Cloud)** pour afficher l’activité.

STEP 4 | Vous pouvez utiliser un filtre Panorama pour afficher le journal d’un groupe d’appareils Cloud individuel. Recherchez le **Device Name (Nom du périphérique)**. Cliquez sur l’icône + dans la partie supérieure droite de l’interface Panorama pour ajouter un nouveau filtre. Saisissez le nom du filtre, puis cliquez sur **Save (Enregistrer)**. Cliquez sur l’icône **Load Filter (Charger le filtre)**. Sélectionnez le filtre nouvellement créé pour afficher les journaux du groupe d’appareils Cloud individuel.

STEP 5 | Vous pouvez choisir un type spécifique de journal à afficher dans le menu **Logs (Journaux)** sur le côté gauche de la console Panorama.



Afficher l’activité du Cloud NGFW dans l’ACC

L’ACC est un outil analytique qui fournit des renseignements exploitables concernant l’activité sur votre réseau. L’ACC utilise les journaux du Cloud NGFW pour représenter graphiquement les tendances du trafic sur votre réseau. Cette représentation graphique vous permet d'interagir avec les données et de

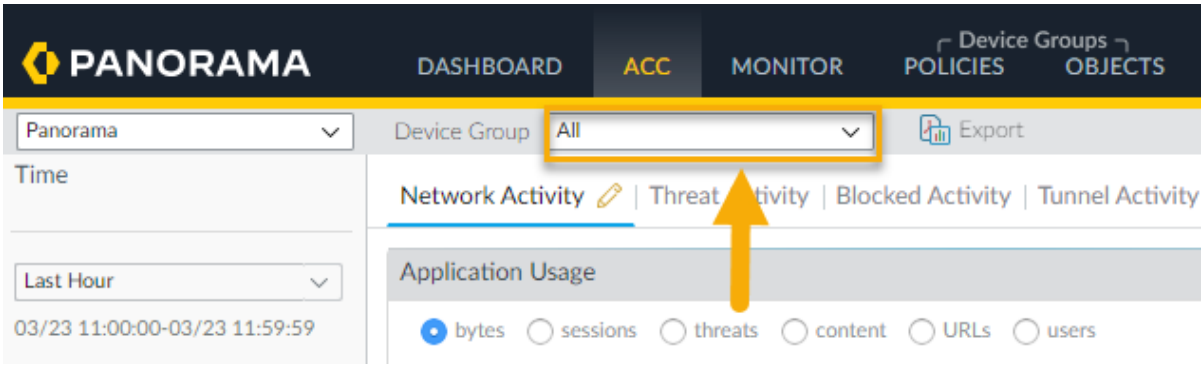
visualiser les relations entre les événements sur le réseau, notamment les modèles d'utilisation réseau, les modèles de trafic, les activités suspectes et les anomalies.

Dans Panorama, vous pouvez filtrer le contenu de l'ACC en fonction du groupe d'appareils Cloud. Pour savoir comment filtrer et afficher des informations spécifiques sur l'activité de vos ressources Cloud NGFW, reportez-vous à la documentation ACC pour PAN-OS.

STEP 1 | Connectez-vous à Panorama.

STEP 2 | Sélectionnez **ACC.**

STEP 3 | Dans la liste déroulante **Device Group (Groupe d'appareils)**, sélectionnez **Cloud Device Group (Groupe d'appareils Cloud)** pour afficher l'activité.



STEP 4 | Vous pouvez utiliser un filtre Panorama pour afficher le journal d'un groupe d'appareils Cloud individuel. Recherchez le **Device Name (Nom du périphérique)**. Cliquez sur l'icône **+** dans la partie supérieure droite de l'interface Panorama pour ajouter un nouveau filtre. Saisissez le nom du filtre, puis cliquez sur **Save (Enregistrer)**. Cliquez sur l'icône **Load Filter (Charger le filtre)**. Sélectionnez le filtre nouvellement créé pour afficher les journaux du groupe d'appareils Cloud individuel.

de journalisation

Le Cloud NGFW peut envoyer des journaux de trafic, de menaces et de décryptage à un espace de travail Azure Log Analytics que vous créerez dans le portail Azure.

Configurer la journalisation pour Cloud NGFW sur Azure

Un journal est un fichier horodaté généré automatiquement qui fournit une piste d'audit pour des événements systèmes qui surviennent sur le pare-feu ou pour des événements de trafic réseau que le pare-feu surveille. Les entrées de journal contiennent des artefacts, qui sont des propriétés, des activités ou des comportements associés avec l'événement journalisé, tels que le type d'application ou l'adresse IP d'un pirate. Chaque type de journal enregistre des informations sur un type d'événement distinct. Par exemple, le pare-feu génère un journal des menaces pour y consigner le trafic qui correspond à la signature d'un logiciel espion, d'une vulnérabilité ou d'un virus, ou une attaque DoS qui correspond aux seuils configurés pour le déclenchement d'une analyse de port ou d'une activité de balayage de l'hôte sur le pare-feu.

Le Cloud NGFW peut envoyer des journaux de trafic, de menaces et de décryptage à un espace de travail Azure Log Analytics que vous créerez dans le portail Azure. L'espace de travail Log Analytics est associé à un ID d'espace de travail, une clé primaire et une clé secondaire qui sont récupérées via l'API de journalisation par le plan de contrôle.

Types de journaux

Cloud NGFW peut capturer et enregistrer trois types de journaux.

- **Trafic** : les journaux de trafic affichent une entrée au début et à la fin de chaque session. Pour plus d'informations, reportez-vous à la section Champs du journal du trafic Cloud NGFW pour Azure.
- **Menaces** : les journaux des menaces affichent des entrées lorsque le trafic correspond à un des profils de sécurité associés à une règle de sécurité définie sur le pare-feu. Chaque entrée inclut les informations suivantes : date et heure ; type de menace (par exemple un virus ou un logiciel espion) ; description ou URL de la menace (colonne Name [Nom]) ; action d'alerte (par exemple autorisation ou blocage) ; niveau de gravité.

  Pour plus d'informations, reportez-vous à la section Champs du journal des menaces Cloud NGFW pour Azure.

Sévérité	Description
Critique	Menaces graves, telles que celles affectant les installations par défaut des logiciels déployés à grande échelle et menant à la compromission des serveurs, dans lesquelles le code d'exploitation est largement accessible aux pirates. Le pirate n'a généralement pas besoin d'informations d'authentification spéciales ni de connaissances relatives à chaque victime, et la cible n'a pas besoin d'être manipulée au point d'effectuer des fonctions spéciales.
Élevée	Menaces pouvant devenir critiques mais ayant des facteurs atténuants; par exemple, elles peuvent être difficiles à exploiter, ne mènent pas à des privilèges élevés ou ne ciblent pas un grand nombre de victimes.
Moyenne	Menaces mineures dans lesquelles l'incidence est minimisée, telles que les attaques DoS qui ne compromettent pas la cible

Sévérité	Description
	ou les exploitations nécessitant qu'un pirate réside sur le même réseau local que la victime, affectent uniquement les configurations non standard ou les applications obscures, ou fournissent un accès très limité.
Faible	Menaces à surveiller ayant très peu d'incidence sur l'infrastructure de l'entreprise. Celles-ci requièrent généralement un accès au système physique ou local et peuvent entraîner des problèmes DoS ou de confidentialité de la victime, ainsi qu'une fuite des informations.
Pour information	Événements suspects qui ne constituent pas une menace immédiate, mais qui sont signalés pour attirer l'attention sur l'existence possible de problèmes plus graves. Les entrées du journal de URL Filtering sont enregistrées sous le niveau de gravité Informations. Les entrées du journal des envois WildFire qui ont reçu un verdict quelconque et dont l’action est définie sur block (bloquer) sont journalisés sous le niveau de gravité Informations.

- **Décryptage** : les journaux de décryptage affichent par défaut les entrées pour les communications TLS avortées et peuvent afficher les entrées pour les communications TLS réussies si vous les activez dans la politique de décryptage. Si vous autorisez les entrées pour les communications réussies, assurez-vous que vous disposez des ressources système (espace de journalisation) pour les journaux. Pour plus d'informations, reportez-vous à la section Champs du journal de décryptage Cloud NGFW pour Azure.

Champs du journal du trafic Cloud NGFW pour Azure

Nom du champ	Description
Adresse source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
Adresse de destination (dst)	Adresse IP de destination de la session d'origine.
Port de destination (dport)	Port de destination utilisé par la session.
Protocole IP (proto)	Protocole IP associé à la session.
Application (app)	Application associée à la session.
Nom de la règle (rule)	Nom de la règle à laquelle la session correspond.
Action (action)	Action prise pour la session. Les valeurs possibles sont : • allow — la session a été autorisée par la politique • deny — la session a été refusée par la politique • reset both — la session a été terminée et une réinitialisation TCP est envoyée aux deux côtés de la connexion • reset client — la session a été terminée et une réinitialisation TCP est envoyée au client • reset server — la session a été terminée et une réinitialisation TCP est envoyée aux serveurs
Octets reçus (bytes_received)	Nombre d'octets dans le sens serveur/client de la session.
Octets envoyés (bytes_sent)	Nombre d'octets dans le sens client/serveur de la session.
Paquets reçus (pkts_received)	Nombre de paquets serveur/client de la session.
Paquets envoyés (pkts_sent)	Nombre de paquets client/serveur de la session.
Heure de début (start)	Heure de début de la session.
Temps écoulé (elapsed)	Durée écoulée de la session.
Nombre de répétitions (repeatcnt)	Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes.

Nom du champ	Description
Catégorie (category)	Catégorie d'URL associée à la session (le cas échéant).
Pays source (srcloc)	Pays ou région source pour les adresses privées ; 32 octets maximum.
Pays de destination (dstloc)	Pays ou région de destination pour les adresses privées. 32 octets maximum.
Motif de fin de session (session_end_reason)	Le motif pour lequel une session s'est terminée. S'il existe plusieurs motifs, ce champ affiche uniquement le motif principal (celui dont la priorité est la plus élevée). Les valeurs de motif de fin de session possibles sont les suivantes, par ordre de priorité (où la première est la plus élevée) : • threat : le pare-feu a détecté une menace associée à une action de réinitialisation, d'abandon ou de blocage (d'adresse IP). • policy-deny : la session a été mise en correspondance avec une règle de sécurité dont l'action est le refus ou l'abandon. • decrypt-cert-validation : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque lorsque la session utilise l'authentification du client ou qu'elle utilise un certificat du serveur ayant l'une ou l'autre des conditions suivantes : expiré, émetteur non approuvé, état inconnu ou expiration de la vérification de l'état. Le motif de fin de session s'affiche également lorsque le certificat du serveur produit une alerte d'erreur fatale de type bad_certificate (mauvais certificat), unsupported_certificate (certificat non pris en charge), certificate_revoked (certificat révoqué), access_denied (accès refusé), ou no_certificate_RESERVED (aucun certificat réservé) (uniquement SSLv3). • decrypt-unsupport-param : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise une version de protocole, un cryptage ou un algorithme non pris en charge. Le motif de fin de session s'affiche lorsque la session produit une alerte d'erreur fatale du type unsupported_extension (extension non prise en charge), unexpected_message (message inattendu), ou handshake_failure (échec de la liaison de segmentation). • decrypt-error : la session s'est terminée, car vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque des ressources sur le pare-feu étaient indisponibles. Le motif de fin de session s'affiche lorsque vous configurez le pare-feu pour qu'il bloque le trafic SSL ayant des erreurs SSH

Nom du champ	Description
	ou qui a produit une alerte d’erreur fatale autre que celles énumérées sous les motifs de fin de session decrypt-cert-validation et decrypt-unsupport-param. • tcp-rst-from-client : le client a envoyé une demande de réinitialisation TCP au serveur. • tcp-rst-from-server : le serveur a envoyé une demande de réinitialisation TCP au client. • resources-unavailable : la session a été abandonnée en raison d'une limitation des ressources système. Par exemple, il se peut que la session ait dépassé le nombre de paquets dans le désordre autorisés par flux ou la file d'attente générale des paquets dans le désordre. • tcp-fin : les deux hôtes de la connexion a/ont envoyé un message TCP FIN pour fermer la session. • tcp-reuse : une session a été réutilisée et le pare-feu a fermé la session précédente. • decoder : le décodeur a détecté une nouvelle connexion via le protocole (proxy HTTP, par exemple) et a fermé la connexion précédente. • aged-out : la session a expiré. • n/a : cette valeur s'applique lorsque le type de journal du trafic n'est pas **end**.
Adresse XFF (xff)	L'adresse IP de l'utilisateur qui a demandé la page web ou l'adresse IP de l'avant-dernier périphérique que la requête a traversé. Si la requête passe par un ou plusieurs proxies, équilibreurs de charge ou autres périphériques en amont, le pare-feu affiche l'adresse IP du périphérique le plus récent.

Champs du journal des menaces Cloud NGFW pour Azure

Nom du champ	Description
Adresse source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
Adresse de destination (dst)	Adresse IP de destination de la session d'origine.
Port de destination (dport)	Port de destination utilisé par la session.
Protocole IP (proto)	Protocole IP associé à la session.
Application (app)	Application associée à la session.
Nom de la règle (rule)	Nom de la règle à laquelle la session correspond.
Action (action)	Action prise pour la session ; les valeurs possibles sont alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url. • alert : menace ou URL détectée mais non bloquée • allow : alerte de détection de saturation • deny : mécanisme de détection de saturation activé et rejet du trafic en fonction de la configuration • drop : menace détectée et session associée arrêtée • reset-client : menace détectée et RST TCP envoyée au client • reset-server : menace détectée et RST TCP envoyée au serveur • reset-both : menace détectée et RST TCP envoyée au client et au serveur • block-url : requête d'URL bloquée car elle correspond à une catégorie d'URL définie pour être bloquée • block-ip : menace détectée et adresse IP du client bloquée • random-drop : saturation détectée et le paquet a fait l’objet d’un abandon aléatoire • sinkhole : mise en entonnoir DNS activée • syncookie-sent : alerte syncookie • block-continue (sous-type d’URL uniquement) : une requête HTTP est bloquée et redirigée vers une page Continue sur laquelle se trouve un bouton de confirmation pour poursuivre

Nom du champ	Description
	• continue (sous-type d’URL uniquement) : réponse à une page block-continue URL continue indiquant qu’une requête block-continue a reçu l’autorisation de poursuivre • block-override (sous-type d’URL uniquement) : une requête HTTP est bloquée et redirigée vers une page de contrôle prioritaire par l'administrateur sur laquelle il faut saisir le mot de passe de l’administrateur du pare-feu pour poursuivre • override-lockout (sous-type d’URL uniquement) : un trop grand nombre de tentatives de saisir le mot de passe de contrôle prioritaire de l'administrateur ont échoué à partir de l'adresse IP source. L’adresse IP est désormais bloquée sur la page de redirection block-override. • override (sous-type d’URL uniquement) : réponse à une page block-override, où le bon mot de passe a été saisi et la requête a été autorisée • block (Wildfire uniquement) : le fichier a été bloqué par le pare-feu et téléchargé sur Wildfire
Catégorie de menace (threat_category)	Décrit les catégories de menace utilisées pour classer les différents types de signatures de menace.
Type de menace/contenu (threat_content_type)	Sous-type de journal des menaces. Les valeurs incluent ce qui suit : • data (données) : modèle de données correspondant à un profil de filtrage des données • file : type de fichiers correspondant à un profil de blocage de fichiers. • flood : saturation détectée via un profil de protection de zone. • packet : protection contre les attaques basées sur le paquet qui est déclenchée par un profil de protection de zone. • scan : analyse détectée via un profil de protection de zone. • spyware : spyware détecté via un profil Antispyware. • url : journal de URL Filtering • ml-virus : virus détecté par WildFire Inline ML via un profil antivirus. • Virus : virus détecté via un profil Antivirus. • vulnerability : exploitation des vulnérabilités détectée via un profil de protection de vulnérabilité. • wildfire : un verdict WildFire généré lorsque le pare-feu envoie un fichier à WildFire via un profil d’analyse WildFire et un verdict (logiciel malveillant, hameçonnage, indésirable ou bénin, selon les informations que vous consignez) est consigné au journal des envois WildFire.

Nom du champ	Description
	• wildfire-virus : virus détecté via un profil Antivirus.
Nom de la menace/ du contenu (threat_content_name)	Identifiant Palo Alto Networks pour les menaces connues et personnalisées. Il s'agit d'une chaîne de description suivie d'un identifiant numérique 64 bits entre parenthèses pour certains sous-types. • 8000 – 8099 : détection d'analyse • 8500 – 8599 : détection de saturation • 9999 : journal de filtrage des URL • 10000 – 19999 : détection du logiciel espion Phone Home • 20000 – 29999 : détection de téléchargement de logiciel espion • 30000 – 44999 : détection d'exploitation des vulnérabilités • 52000 – 52999 : détection du type de fichier • 60000 – 69999 : détection de filtrage des données *Les plages d'ID de menace pour la détection des virus, le flux de signature WildFire et les signatures DNS C2 utilisées dans les versions précédentes ont été remplacées par des ID de menace uniques à l'échelle globale permanents. Reportez-vous aux noms de champ Type de contenu/menace (sous-type) et Catégorie de menace (thr_category) pour créer des rapports à jour, filtrer les journaux des menaces, et l'activité ACC.*
Gravité (severity)	Gravité associée à la menace ; les valeurs possibles sont informational, low, medium, high, critical.
Sens (direction)	Indique le sens de l'attaque, client-to-server ou server-to-client : • 0 — le sens de la menace est du client vers le serveur • 1 — le sens de la menace est du serveur vers le client
Nombre de répétitions (repeatcnt)	Nombre de sessions avec les mêmes adresses IP source et de destination, application et Type de contenu/de menace sur une période de 5 secondes.
Raison (data_filter_reason)	Motif de l'action de filtrage des données.
Adresse XFF (xff)	L'adresse IP de l'utilisateur qui a demandé la page web ou l'adresse IP de l'avant-dernier périphérique que la requête a traversé. Si la requête passe par un ou plusieurs proxies, équilibreurs de charge ou autres périphériques en amont, le pare-feu affiche l'adresse IP du périphérique le plus récent.

Nom du champ	Description
Version du contenu (contentver)	La version des applications et des menaces sur votre pare-feu lorsque le journal a été généré.

Champs du journal de décryptage Cloud NGFW pour Azure

Nom du champ	Description
Adresse IP source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
Adresse de destination (dst)	Adresse IP de destination de la session d'origine.
Port de destination (dport)	Port de destination utilisé par la session.
Protocole IP (proto)	Protocole IP associé à la session.
Application (app)	Application associée à la session.
Règle (rule)	Règle de politique de sécurité qui contrôle le trafic de la session.
Action (action)	Action prise pour la session. Les valeurs possibles sont : • allow — la session a été autorisée par la politique • deny — la session a été refusée par la politique • reset both — la session a été terminée et une réinitialisation TCP est envoyée aux deux côtés de la connexion • reset client — la session a été terminée et une réinitialisation TCP est envoyée au client • reset server — la session a été terminée et une réinitialisation TCP est envoyée aux serveurs
Version TLS (tls_version)	La version du protocole TLS utilisée pour la session.
Algorithme d'échange de clés (tls_keyxchg)	L'algorithme d'échange de clés utilisé pour la session.
Algorithme de chiffrement (tls_enc)	L'algorithme utilisé pour crypter les données de la session, comme AES-128-CBC, AES-256-GCM, etc.
Algorithme de hachage (tls_auth)	L'algorithme d'authentification utilisé pour la session, par exemple, SHA, SHA256, SHA384, etc.

Nom du champ	Description
Courbe elliptique (ec_curve)	La courbe de cryptographie elliptique que le client et le serveur négocient et utilisent pour les connexions qui utilisent les suites de chiffrement ECDHE.
Indication du nom du serveur (server_name_indication)	L’indication du nom de serveur.
Longueur d'indication de nom de serveur (server_name_indication_length)	La longueur de l'indication du nom du serveur (nom d'hôte).
Type de proxy (proxy_type)	Le type de proxy de décryptage, tel que Forward pour Proxy de transfert, Inbound pour Inspection entrante, No Decrypt pour trafic non décrypté, GlobalProtect, etc.
État de la chaîne (chain_status)	Si la chaîne est fiable. Les valeurs sont : • Non inspectée • Non approuvée • Fiable • Incomplet

Activer les paramètres du journal

Pour activer les paramètres du journal :

STEP 1 | Depuis la page d’accueil, accédez au pare-feu Cloud NGFW sur lequel vous souhaitez activer les paramètres du journal.

STEP 2 | Cliquez sur **Log Settings (Paramètres du journal)**.

STEP 3 | Cochez **Enable Log Settings (Activer les paramètres du journal)**.

STEP 4 | Dans la liste déroulante **Log Settings (Paramètres du journal)**, choisissez l’espace de travail Log Analytics pour lequel vous souhaitez activer les paramètres du journal.

STEP 5 | Cliquez sur **Save (Enregistrer)**.

Désactiver les paramètres du journal

Pour désactiver les paramètres du journal :

STEP 1 | Depuis la page d’accueil, accédez au pare-feu Cloud NGFW sur lequel vous souhaitez activer les paramètres du journal.

STEP 2 | Cliquez sur **Log Settings (Paramètres du journal)**.

STEP 3 | Cochez **Disable Log Settings (Désactiver les paramètres du journal)**.

STEP 4 | Dans la liste déroulante **Log Settings (Paramètres du journal)**, choisissez l’espace de travail Log Analytics pour lequel vous souhaitez désactiver les paramètres du journal.

STEP 5 | Cliquez sur **Save (Enregistrer)**.

Activer la journalisation des activités sur Cloud NGFW pour Azure

Suivez l’activité de l’administrateur sur Cloud NGFW pour Azure pour obtenir des rapports en temps réel sur l’activité de votre déploiement. Si vous avez des raisons de croire qu’un compte administrateur est compromis, le journal d’activité vous fournit un historique complet de l’endroit où un administrateur a navigué dans le locataire Cloud NGFW et des modifications de configuration qu’il a apportées afin que vous puissiez analyser en détail et répondre à toutes les actions entreprises sur le compte compromis.

Plusieurs destinations de journalisation sur le cloud NGFW pour Azure

Vous pouvez gérer les journaux et obtenir des informations sur la sécurité du cloud pour vos ressources Cloud NGFW. Envoyez vos journaux générés depuis Cloud NGFW pour Azure vers un espace de travail Azure Log Analytics ou Panorama vers plusieurs destinations en même temps. Ces journaux incluent à la fois les journaux du trafic et des menaces (provenant du filtrage des URL, des soumissions WildFire, du blocage des fichiers, du blocage des données et du décryptage).

Activer le journal du trafic dans l’espace de travail Log Analytics et Panorama

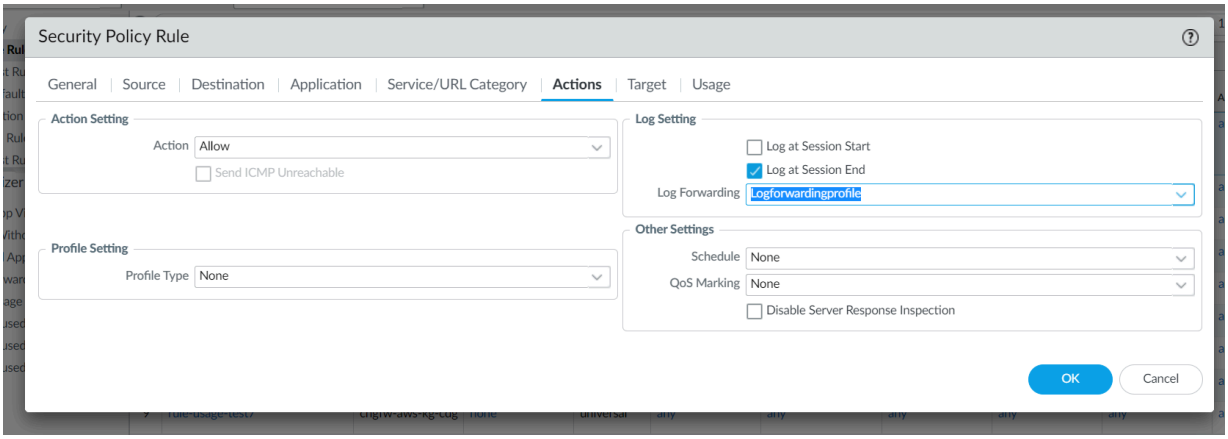
Voici les étapes pour activer le journal du trafic dans l’espace de travail Log Analytics et Panorama :

STEP 1 | Activez les paramètres du journal sur la console Cloud NGFW pour Azure.

STEP 2 | Dans Panorama, accédez à **Policies (Politiques)**.

STEP 3 | Sélectionnez la règle de politique pour votre groupe d’appareils cloud.

STEP 4 | Accédez à l’onglet **Actions** , puis sélectionnez le profil **Log Forwarding (Transfert des journaux)**.



STEP 5 | Cliquez sur **OK**.

STEP 6 | **Validez et appliquez** vos modifications dans la console Panorama.

Une fois le trafic envoyé, vous pouvez afficher les journaux Cloud NGFW dans l'espace de travail Log Analytics et Panorama**.** Pour plus d'informations, reportez-vous aux sections Afficher les journaux et Afficher les journaux Cloud NGFW dans Panorama.

Activer le journal du trafic dans l'espace de travail Log Analytics et le désactiver dans Panorama

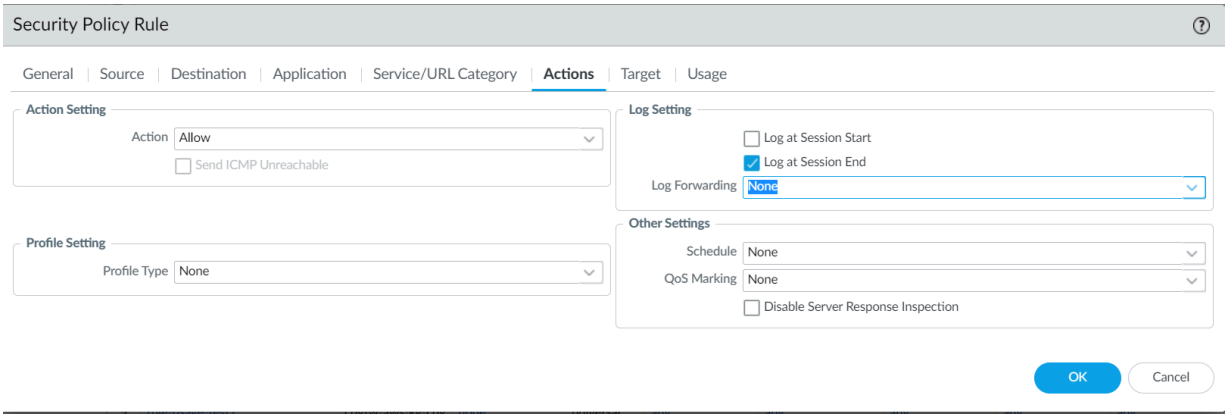
Voici les étapes pour activer le journal du trafic dans l'espace de travail Log Analytics et désactiver les journaux dans Panorama :

STEP 1 | Activez les paramètres du journal sur la console Cloud NGFW pour Azure.

STEP 2 | Dans Panorama, accédez à **Policies (Politiques)**.

STEP 3 | Sélectionnez la règle de politique pour votre groupe d'appareils cloud.

STEP 4 | Accédez à l'onglet **Actions** , puis sélectionnez **None (Aucune)** dans le profil de transfert des journaux.



STEP 5 | Cliquez sur **OK**.

STEP 6 | **Validez et appliquez** vos modifications dans la console Panorama.

Une fois le trafic envoyé, vous pouvez afficher les journaux Cloud NGFW dans l'espace de travail Log Analytics et Panorama**.** Pour plus d'informations, reportez-vous aux sections Afficher les journaux et Afficher les journaux Cloud NGFW dans Panorama.

Désactiver le journal du trafic dans l’espace de travail Log Analytics et l’activer dans Panorama

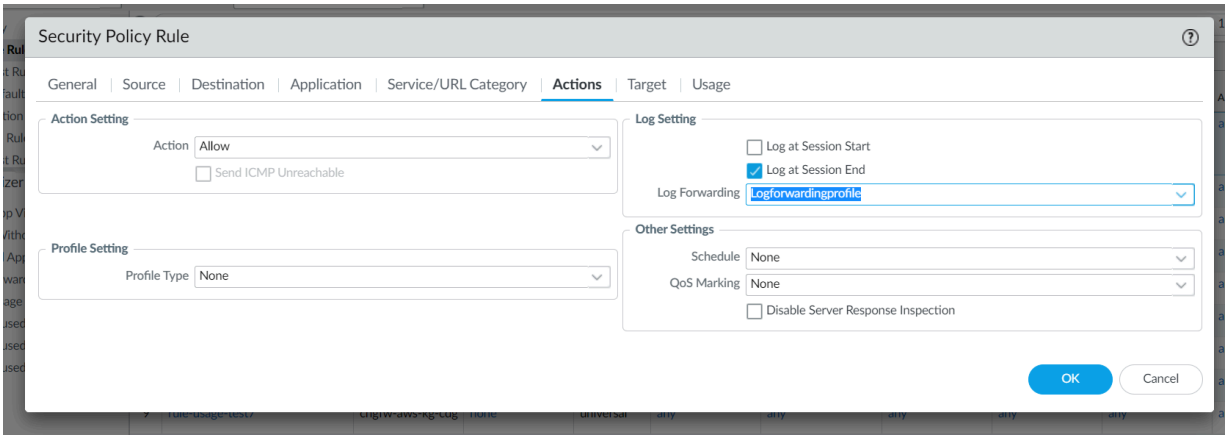
Voici les étapes pour désactiver les journaux dans l’espace de travail Log Analytics et les activer dans Panorama :

STEP 1 | Désactivez les paramètres du journal sur la console Cloud NGFW pour Azure.

STEP 2 | Dans Panorama, accédez à **Policies (Politiques)**.

STEP 3 | Sélectionnez la règle de politique pour votre groupe d’appareils cloud.

STEP 4 | Accédez à l’onglet **Actions** , puis sélectionnez le profil **Log Forwarding (Transfert des journaux)**.



STEP 5 | Cliquez sur **OK**.

STEP 6 | **Validez et appliquez** vos modifications dans la console Panorama.

Une fois le trafic envoyé, vous pouvez afficher les journaux Cloud NGFW dans l’espace de travail Log Analytics et Panorama**.** Pour plus d’informations, reportez-vous aux sections Afficher les journaux et Afficher les journaux Cloud NGFW dans Panorama.

Désactiver le journal du trafic dans l’espace de travail Log Analytics et Panorama

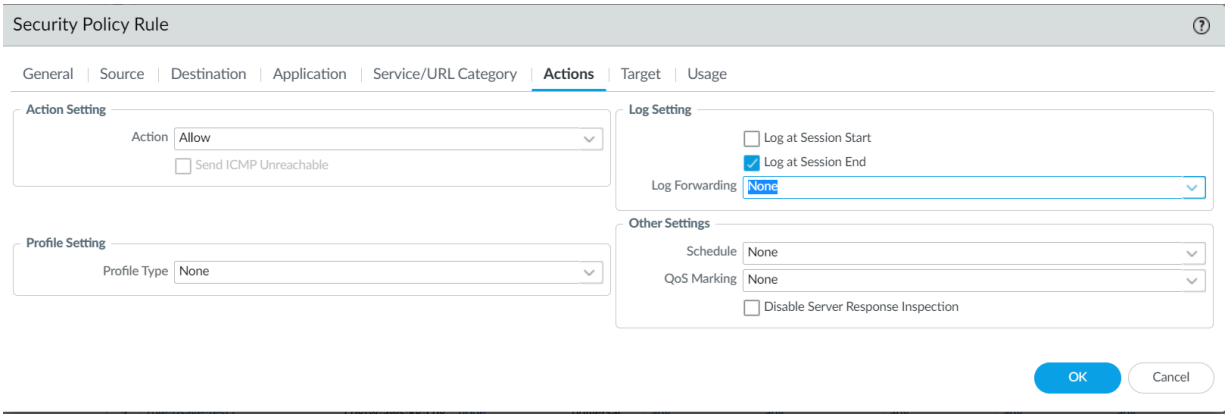
Voici les étapes pour désactiver le journal du trafic dans l’espace de travail Log Analytics et Panorama :

STEP 1 | Désactivez les paramètres du journal sur la console Cloud NGFW pour Azure.

STEP 2 | Dans Panorama, accédez à **Policies (Politiques)**.

STEP 3 | Sélectionnez la règle de politique pour votre groupe d'appareils cloud.

STEP 4 | Accédez à l'onglet **Actions**, puis sélectionnez **None (Aucune)** dans le profil de transfert des journaux.



STEP 5 | Cliquez sur **OK**.

STEP 6 | **Validez et appliquez** vos modifications dans la console Panorama.

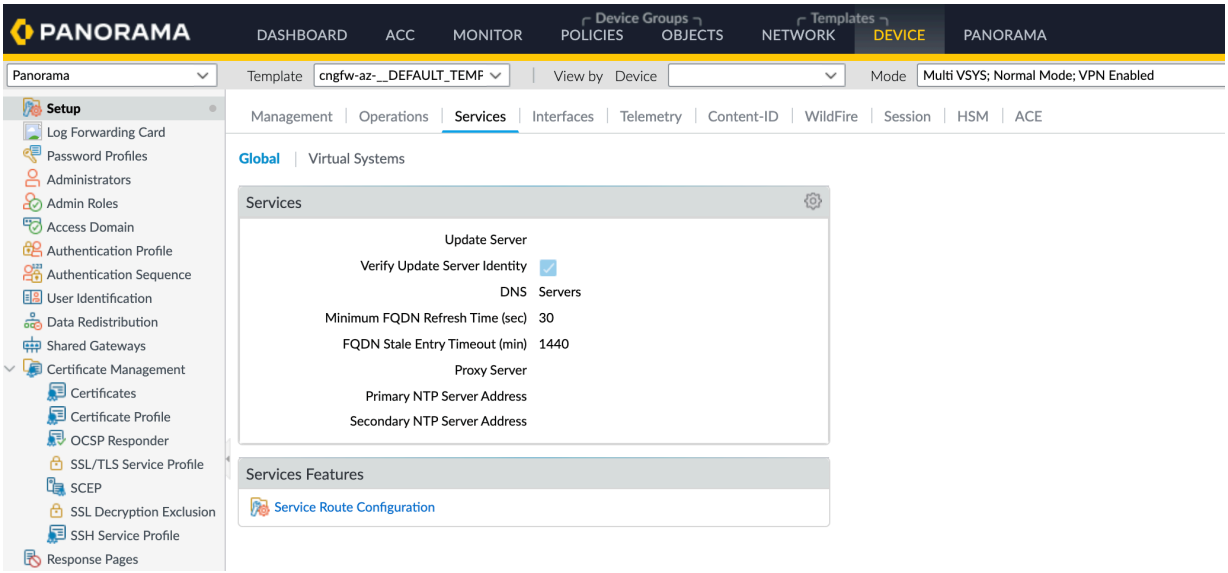
Les journaux Cloud NGFW ne seront plus reflétés dans l'espace de travail Log Analytics et dans Panorama.

Désactivez le journal du trafic dans l'espace de travail Log Analytics et activez-le dans Panorama et Syslog.

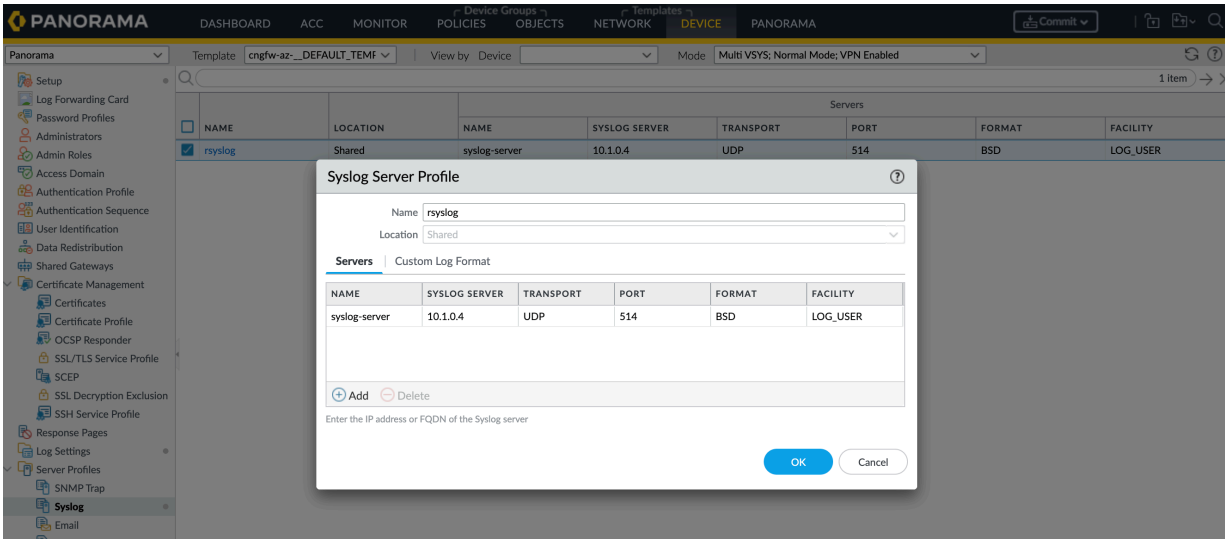
Voici les étapes pour désactiver les journaux dans l'espace de travail Log Analytics et les activer dans Panorama et le serveur syslog :

STEP 1 | Désactivez les paramètres du journal sur la console Cloud NGFW pour Azure.

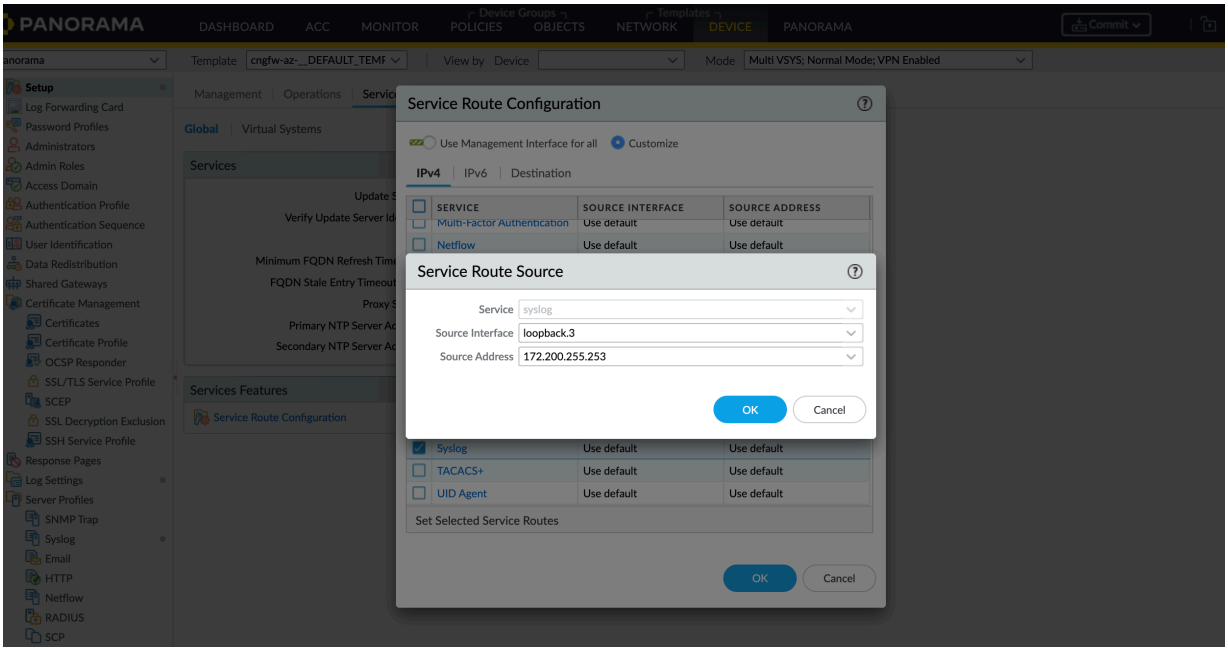
STEP 2 | Dans Panorama, accédez à l'onglet **Device (Périphérique)**, puis sélectionnez le modèle par défaut Azure NGFWAAS (`cngfw-az-__DEFAULT_TEMPLATE__`).



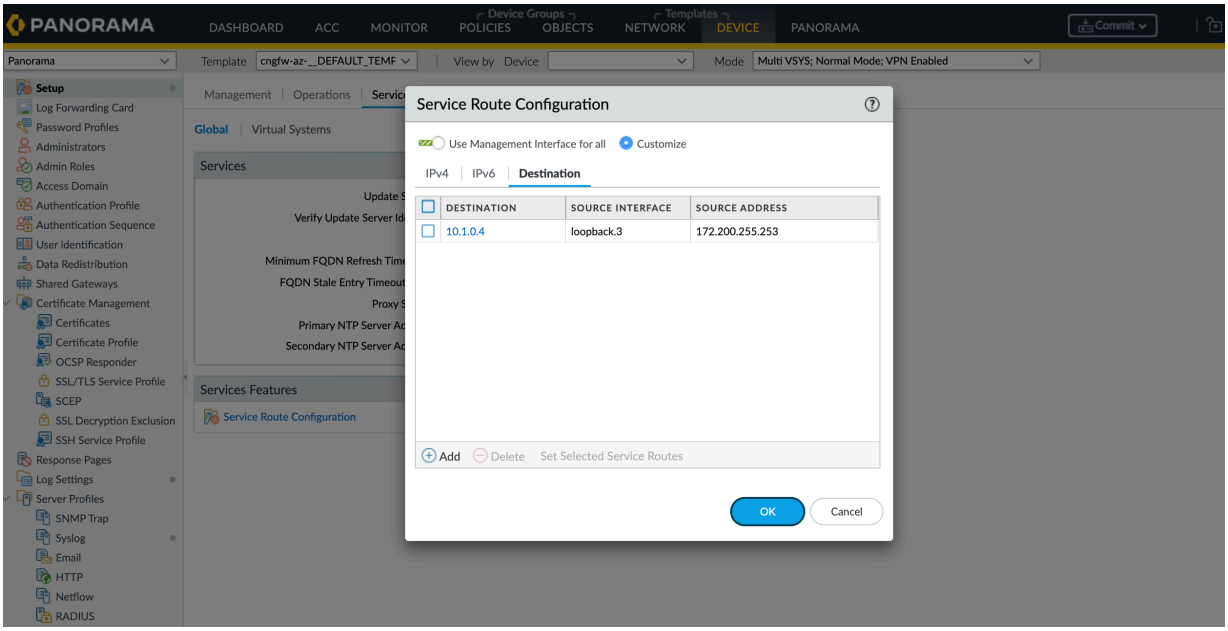
STEP 3 | Accédez à **Server profiles (Profils de serveur)** -> **Syslog,** puis ajoutez l’adresse IP privée de votre serveur syslog.



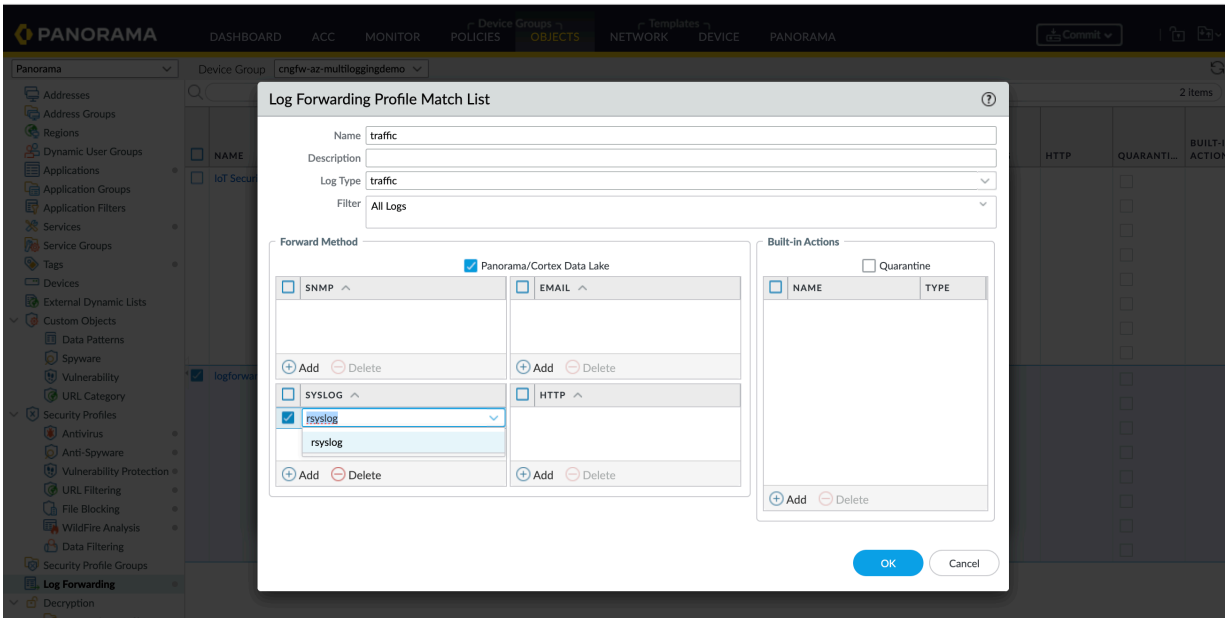
STEP 4 | Accédez à l’onglet Device (Périphérique), cliquez sur **Setup (Configurer),** puis cliquez sur **Service Route Configuration (Configuration de l’itinéraire de service)**.



- Pour configurer l'**itinéraire basé sur les services**, sélectionnez **IPv4** et le service **Syslog**. Veillez à sélectionner **loopback.3** comme interface source.
- Pour configurer **Destination Based Routing (Itinéraire basé sur la destination)**, sélectionnez la destination, ajoutez l'adresse IP privée de votre serveur syslog, puis sélectionnez **loopback.3** en tant qu'interface source.



STEP 5 | Dans le **profil de transfert des journaux**, ajoutez votre serveur syslog.



STEP 6 | Dans Panorama, accédez à l’onglet **Policies (Politiques)**, puis sélectionnez la règle de politique pour votre groupe d’appareils Cloud.

STEP 7 | Accédez à l’onglet **Actions** , puis sélectionnez **Log Forwarding profile (Profil de transfert des journaux)**.

STEP 8 | Cliquez sur **OK**.

STEP 9 | **Validez** et **appliquez** vos modifications dans la console Panorama.

Pour recevoir le trafic dans le serveur syslog, l’appairage VNet doit être effectué entre le réseau virtuel du serveur syslog et le réseau virtuel du hub de pare-feu. Une fois le trafic envoyé, vous pouvez afficher les journaux Cloud NGFW dans Panorama et le serveur syslog.

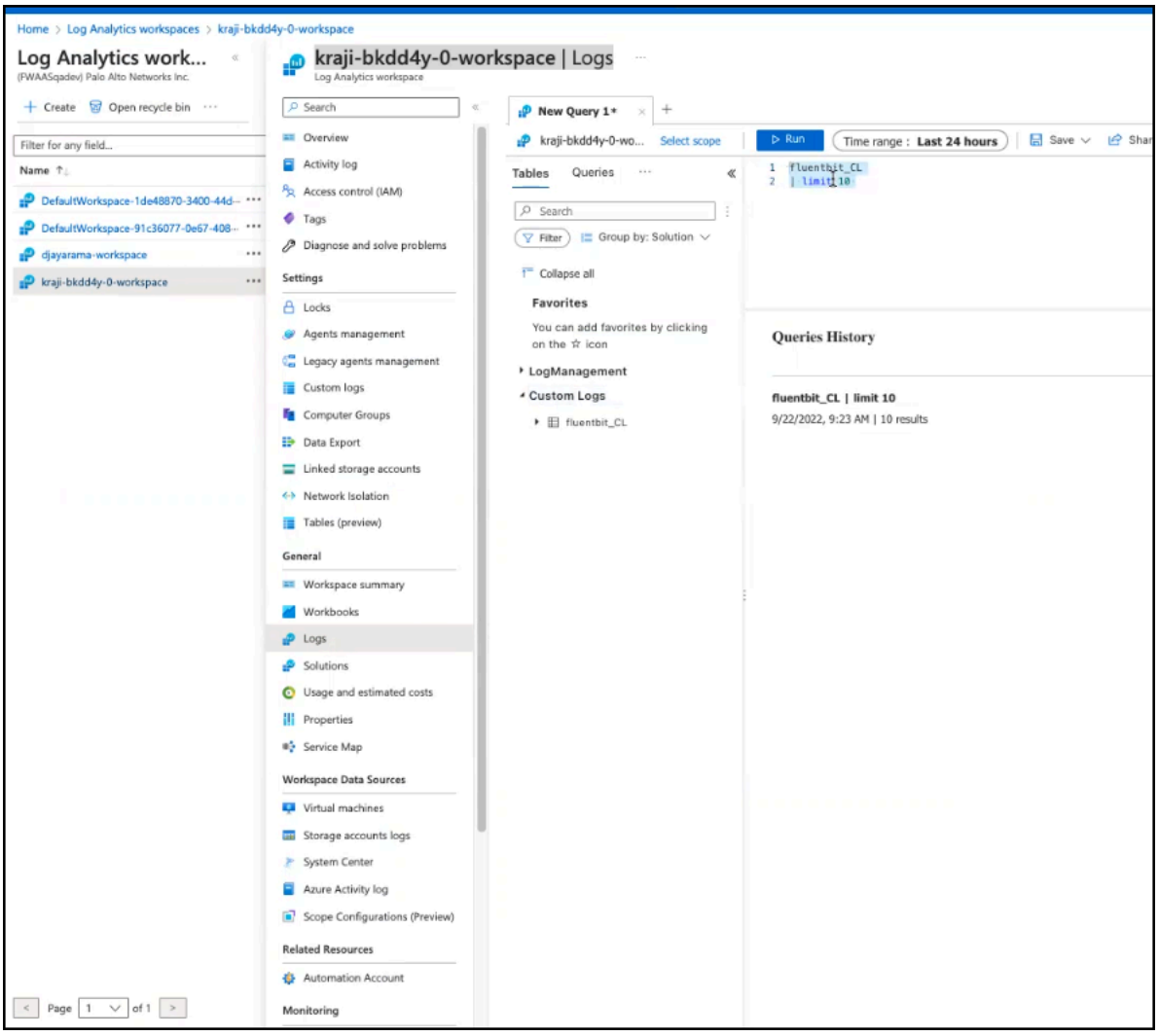
Afficher les journaux

Après avoir créé l’espace de travail Log Analytics, mettez à jour les paramètres du journal sous le pare-feu et commencez à envoyer le trafic. Une fois le trafic envoyé, vous pouvez afficher les journaux comme décrit dans les étapes ci-dessous :

STEP 1 | Cliquez sur l’ **espace de travail Log Analytics** pour lequel vous devez afficher les journaux.

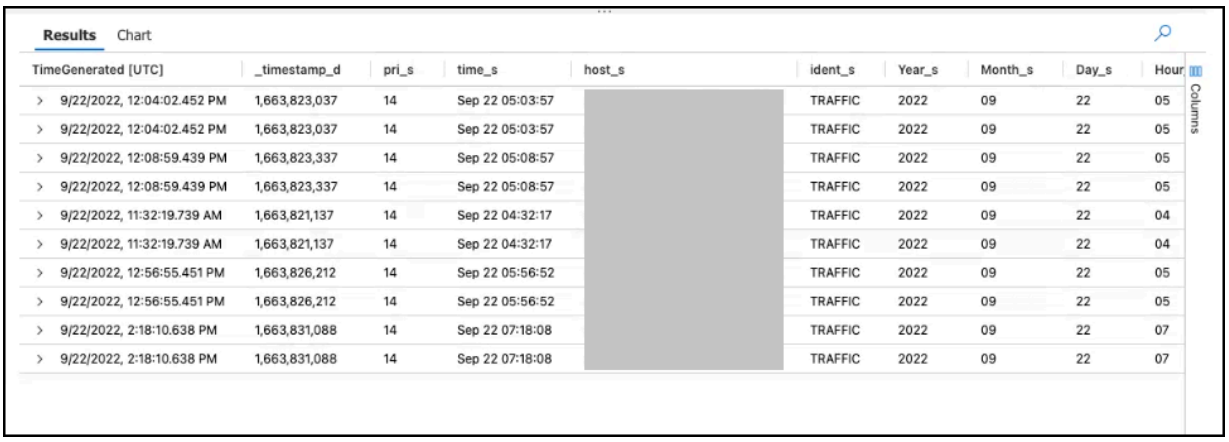
STEP 2 | Cliquez sur **Logs (Journaux)**.

STEP 3 | Cliquez sur **Custom Logs (Journaux personnalisés)** dans la fenêtre de requête puis sur **Run (Exécuter)** pour exécuter une requête que vous avez créée.



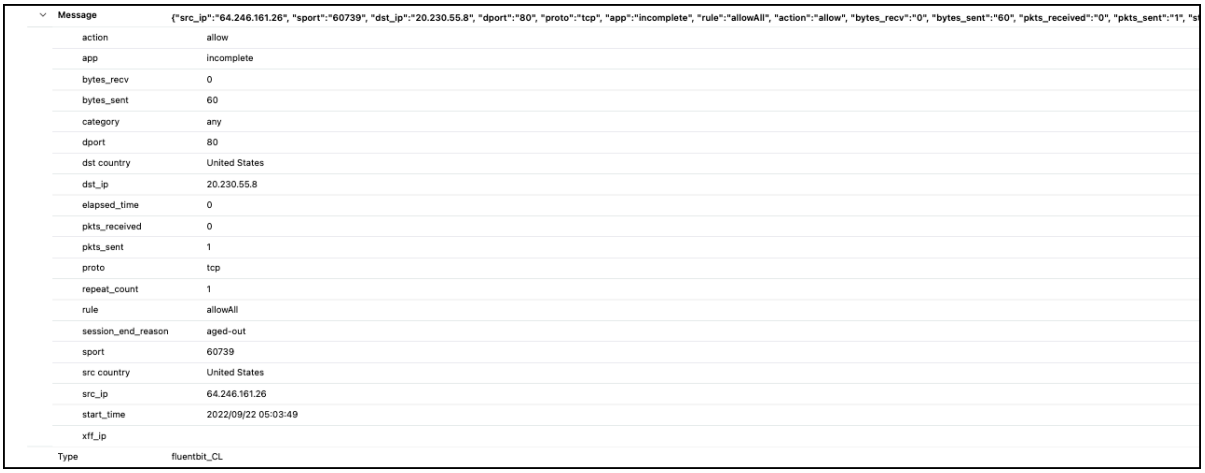
Vous pouvez créer une requête personnalisée avec des paramètres tels que le nombre de journaux, la plage horaire, etc. Par exemple : une requête simple

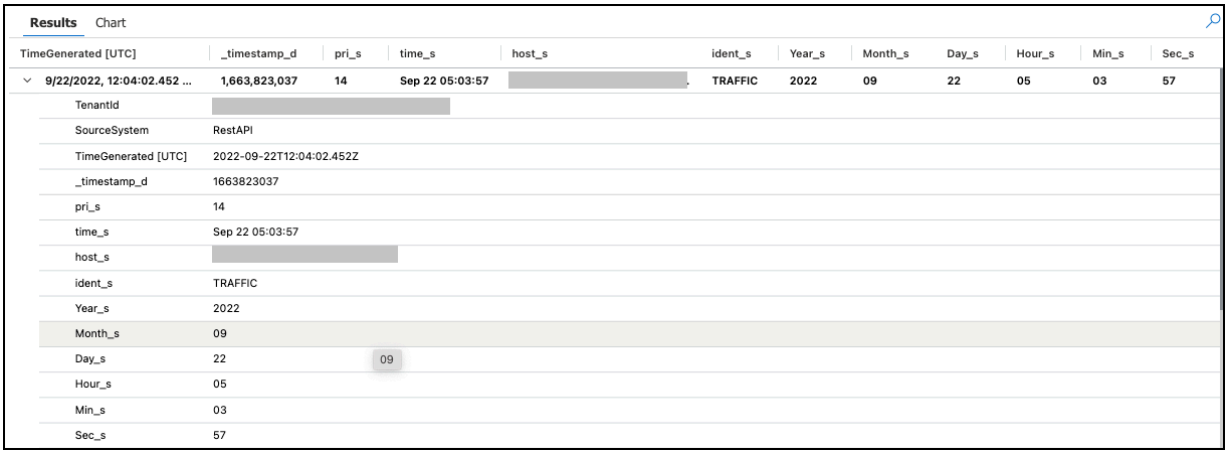
```
fluentbit_CL | limite 10
```

TimeGenerated [UTC]	_timestamp_d	pri_s	time_s	host_s	ident_s	Year_s	Month_s	Day_s	Hour
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:04:02.452 PM	1,663,823,037	14	Sep 22 05:03:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 12:08:59.439 PM	1,663,823,337	14	Sep 22 05:08:57		TRAFFIC	2022	09	22	05
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 11:32:19.739 AM	1,663,821,137	14	Sep 22 04:32:17		TRAFFIC	2022	09	22	04
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 12:56:55.451 PM	1,663,826,212	14	Sep 22 05:56:52		TRAFFIC	2022	09	22	05
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07
9/22/2022, 2:18:10.638 PM	1,663,831,088	14	Sep 22 07:18:08		TRAFFIC	2022	09	22	07

STEP 4 | Cliquez sur l’élément de résultat de la requête souhaité pour lequel vous souhaitez afficher les journaux détaillés.





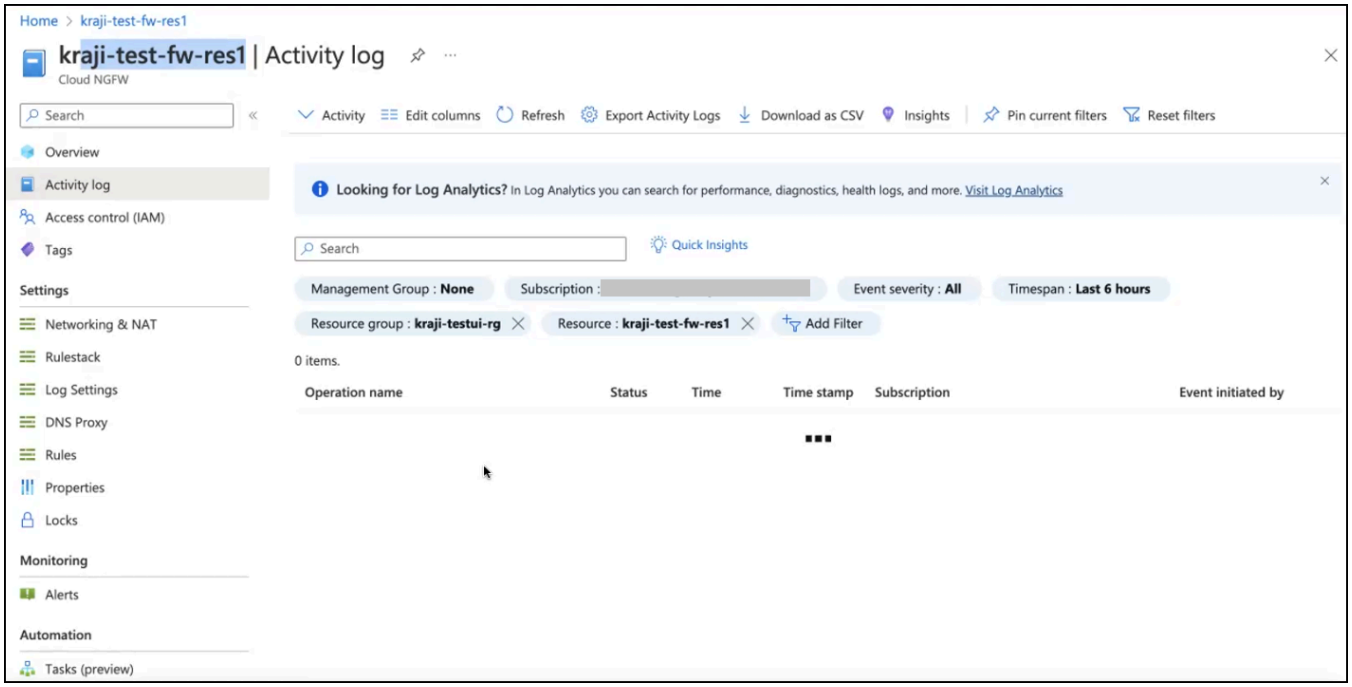
Afficher les journaux d’audit sur une ressource de pare-feu

Pour afficher les journaux d’audit sur la ressource de pare-feu déployée sur un groupe de ressources :

STEP 1 | Depuis la page d’accueil, accédez à la ressource de pare-feu Cloud NGFW sur laquelle vous souhaitez afficher les journaux.

STEP 2 | Cliquez sur **Activity Log (Journal d’activité)** dans le volet gauche, puis sélectionnez la **Timespan (Durée)** pour lesquels vous souhaitez consulter les journaux et cliquez sur **Apply (Appliquer)**. La liste des journaux pour la durée sélectionnée s’affiche.

STEP 3 | Cliquez sur le journal de votre choix pour en afficher le **Summary (Résumé)** et **JSON**.



Afficher les journaux d’audit sur les groupes de ressources

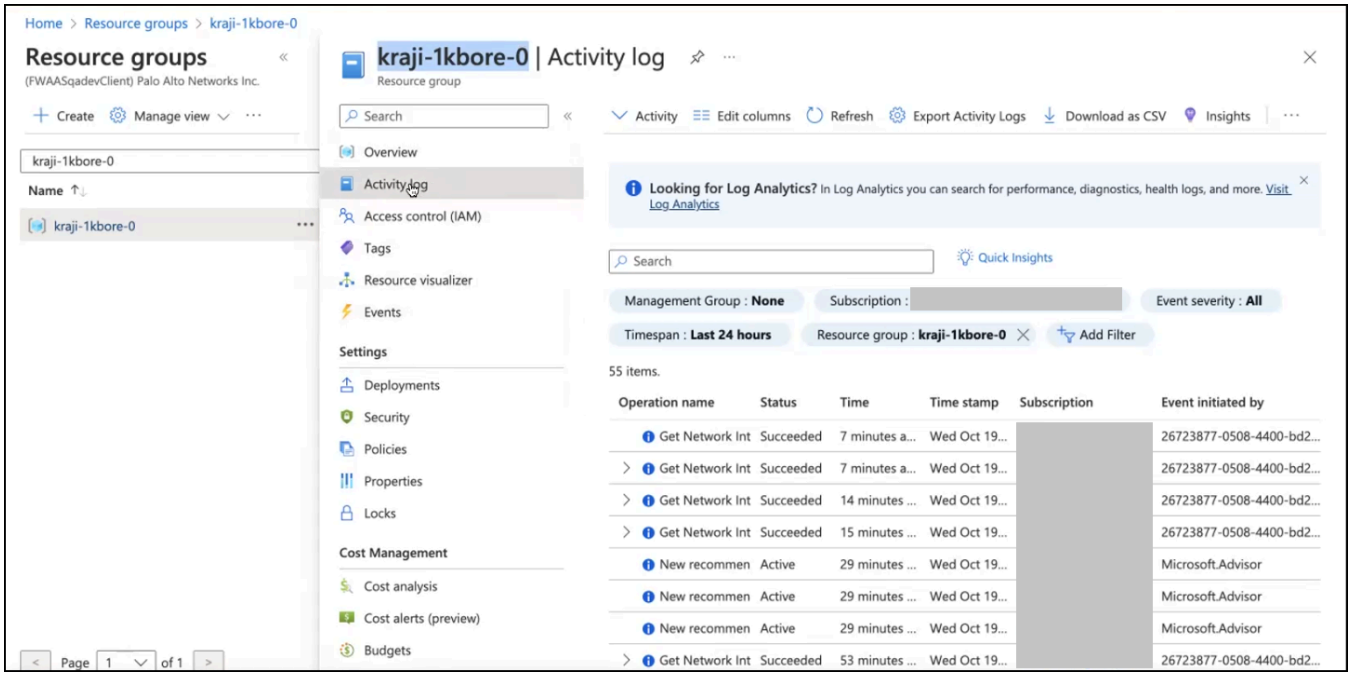
Pour afficher les journaux d’audit sur les groupes de ressources :

STEP 1 | Accédez à **Resource groups (Groupes de ressources)** depuis la page d’accueil.

STEP 2 | Cliquez sur le **groupe de ressources** pour lequel vous souhaitez collecter le journal d’activité.

STEP 3 | Cliquez sur **Activity Log (Journal d’activité)** dans le volet gauche, puis sélectionnez la **Timespan (Durée)** pour lesquels vous souhaitez consulter les journaux et cliquez sur **Apply (Appliquer)**. La liste des journaux pour la durée sélectionnée s’affiche.

STEP 4 | Cliquez sur le journal de votre choix pour en afficher le **Summary (Résumé)** et **JSON**.



Quoi de neuf

Voici les nouveautés de Cloud NGFW pour Azure.

Quoi de neuf en juin 2024

Nouveau	Description
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Ouest du Japon (Osaka) • Centre de la Suède (Gävle) • Nord de l’Italie (Milan) • Nord de l’Afrique du Sud (Johannesburg) • Centre d’Israël • Centre-Ouest des États-Unis (Wyoming) • Nord des Émirats arabes unis (Dubaï) Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.

Quoi de neuf en mai 2024

Nouveau	Description
Utiliser la valeur d’en-tête XFF pour appliquer la politique de sécurité	Votre Cloud NGFW for Azure peut désormais utiliser une adresse IP dans un en-tête X-Forwarded-For (XFF) pour appliquer la politique de sécurité créé sur Panorama.
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Est du Canada Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.
Consommation de crédits et visibilité de l’utilisation	Il est désormais possible d’utiliser des pour la consommation de Cloud NGFW dans le cadre de contrats à long terme que vous pouvez allouer à vos ressources de pare-feu dans les environnements Cloud Azure au niveau du locataire. Pour plus d’informations, reportez-vous à la section Visibilité de l’utilisation des crédits.

Quoi de neuf en mars 2024

Nouveau	Description
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Est de la Norvège • Centre-Ouest de l'Allemagne • Centre de l'Inde • Nord de la Suisse Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.
Frais de mise en réseau Azure	Cloud NGFW pour Azure facture les frais d'appairage du réseau virtuel sous la dimension des frais de mise en réseau Azure. Les détails de la consommation sont partagés sur l'Azure Marketplace. L'utilisation est suivie pour le trafic entrant (depuis Internet vers le réseau virtuel), sortant (vers Internet depuis le réseau virtuel) et est-ouest (entre les réseaux virtuels). Pour plus d'informations sur les frais, reportez-vous à la section Tarification de Cloud NGFW pour Azure.
Prise en charge du décryptage entrant	Cloud NGFW pour Azure utilise le décryptage SSL entrant pour inspecter et déchiffrer le trafic SSL/TLS entrant d'un client vers un serveur réseau ciblé et bloquer les sessions suspectes. Pour plus d'informations, reportez-vous à la section Configurer le décryptage entrant sur Cloud NGFW pour Azure.

Quoi de neuf en février 2024

Nouveau	Description
Plusieurs destinations pour le journal	Vous pouvez désormais envoyer des journaux depuis votre ressource Cloud NGFW pour Azure gérée par Panorama vers un espace de travail Azure Log Analytics, un serveur syslog et Panorama. Pour plus d'informations, reportez-vous à la section Plusieurs destinations pour le journal sur Cloud NGFW pour Azure.
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Centre de la France • Centre-Sud des États-Unis Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.

Quoi de neuf en janvier 2024

Nouveau	Description
Prise en charge de 100 Gbit/s	Cette version permet une mise à l’échelle de Cloud NGFW pour Azure jusqu’à 100 Gbit/s pour les déploiements vNET et vWAN. Pour plus d’informations, reportez-vous aux sections Déployer le Cloud NGFW dans un vNET et Déployer le Cloud NGFW dans un vWAN.

Quoi de neuf en décembre 2023

Nouveau	Description
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Centre-Nord des États-Unis • Asie du Sud-Est Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.
Prise en charge de la NAT source privée	Cette version ajoute la prise en charge de la NAT source privée. Avec cette prise en charge, vous pouvez créer une passerelle NAT privée pour effectuer la traduction d'adresses réseau (NAT). Pour plus d'informations, reportez-vous à la section Modifier un pare-feu existant pour activer la NAT source privée.

Quoi de neuf en novembre 2023

Nouveau	Description
Prise en charge de nouvelles régions Azure	Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes : • Est du Japon • Sud du Brésil Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.
Améliorations de la rulestack	Cette version prend en charge les suppressions de règles implicites dans une rulestack. Avec cette amélioration : • Vous pouvez supprimer des rulestacks non associées qui ne sont pas vides sans supprimer de règles et d'objets. • Vous pouvez supprimer des groupes de ressources tout en conservant des rulestacks non associées vides ou non. • Vous pouvez supprimer des rulestacks qui ne sont ni associées ni vides à l'aide de la CLI Azure, CDK, PowerShell et Terraform. *Cette fonctionnalité de suppression s'applique aux rulestacks non validées et non vides en cours d'exécution.*
Prise en charge du service de sécurité DNS	Cloud NGFW pour Azure ajoute la prise en charge du service de sécurité DNS de Palo Alto Networks. Ce service vous permet de protéger votre trafic vNet et vWAN contre les menaces DNS avancées en surveillant et contrôlant les domaines interrogés par vos ressources réseau. Pour plus d'informations, reportez-vous à la section Activer la sécurité DNS sur Cloud NGFW pour Azure.
Prise en charge non-RFC 1918	Cette version ajoute la prise en charge de plages d'adresses IP privées supplémentaires en plus des adresses spécifiées dans RFC 1918 pour les déploiements vNET et vWAN. Avec cette prise en charge, vous pouvez utiliser des blocs d'adresses IP publiques (par exemple, 40.0.0.0/24) comme réseau privé sans acheminer le trafic vers Internet. Pour plus d'informations sur cette fonctionnalité dans les déploiements vNET, reportez-vous aux informations fournies dans la section **Mise en réseau** (étape 5) Préfixes supplémentaires à la plage de trafic privé.

Quoi de neuf en octobre 2023

<table>
<tr><th>Nouveau</th><th>Description</th></tr>
<tr><td>Prise en charge de nouvelles régions Azure</td><td>Cloud NGFW pour Azure est désormais disponible dans les régions Azure suivantes :
Ouest des États-Unis 2
Europe du Nord
Reportez-vous à la section Régions et zones prises en charge par Cloud NGFW pour Azure pour obtenir la liste complète des régions prises en charge.</td></tr>
<tr><td>Accès par programmation</td><td>L’accès par programmation vous permet de créer et de gérer des NGFW et des rulestacks à l’aide des API. À l’aide de ces API, vous pouvez appeler des actions sur les ressources Cloud NGFW via une application ou un outil tiers. Le tableau ci-dessous fournit des informations sur les outils pris en charge :<table><tr><td>Terraform</td><td>Utilisez le fournisseur Azure pour configurer l’infrastructure à l’aide des API Azure Resource Manager.</td></tr><tr><td>PowerShell</td><td>Utilisez les cmdlets Microsoft Azure PowerShell pour configurer Cloud NGFW pour Azure.</td></tr><tr><td>CLI</td><td>Utilisez ces commandes pour gérer vos ressources Cloud NGFW pour Azure.</td></tr><tr><td>SDK</td><td>Le package SDK pour Python est pris en charge.</td></tr></table></td></tr>
</table>

Quoi de neuf en septembre 2023

Nouveau	Description
Intégrez le flux de connexion SSO à votre compte du portail de support	Intégrez le flux de connexion SSO de votre organisation à votre compte du portail de support client (CSP) de Palo Alto Networks pour votre abonnement Cloud NGFW pour Azure. Pour plus d'informations, reportez-vous à la section Intégrer Single Sign-On (Ouverture de session unique - SSO).
Prise en charge des adresses e-mail de domaine public	Cette version ajoute la prise en charge des adresses e-mail de domaine public pour les comptes duportail de support client. Auparavant, les utilisateurs qui géraient les ressources Cloud NGFW et les demandes de support associées devaient avoir une adresse e-mail d'entreprise pour se connecter au compte. Avec cette fonctionnalité supplémentaire : • Les utilisateurs de domaine public accèdent aux ressources et aux demandes de support dans les comptes dont ils sont membres. • Les contrôles d'accès RBAC sont attribuables et appliqués aux utilisateurs ayant une adresse e-mail de domaine public. • Un utilisateur ayant une adresse e-mail de domaine public d'un compte ne peut pas accéder aux ressources et aux demandes de support d'un autre compte. Résolvez ce problème en ajoutant l'utilisateur avec l'adresse e-mail de domaine public au compte auquel il doit accéder. • Un utilisateur ayant une adresse e-mail de domaine public se voit attribuer n'importe quel rôle, y compris super utilisateur et administrateur de domaine. • Un compte peut avoir un ou plusieurs utilisateurs avec une adresse e-mail de domaine public. Si un compte a été créé par un utilisateur ayant une adresse e-mail de domaine public, le compte est considéré comme *public*. *Un compte ne peut pas comprendre des utilisateurs ayant à la fois des adresses e-mail d'entreprise et publiques.* Les adresses e-mail de domaine public suivantes sont prises en charge : gmail.com, yahoo.*, hotmail.* live.*, outlook.com, aol.com gms.* (gmx.de, gmx.net, gmx.us), icloud.com, msn.com comcast.net**, att.net

Quoi de neuf en août 2023

Nouveau	Description
Disponibilité générale	Cloud NGFW pour Azure a atteint la disponibilité générale. Cette version comprend de nombreux correctifs, la prise en charge de régions supplémentaire et des améliorations apportées au modèle d'abonnement PAYG (paiement à l'utilisation.

Quoi de neuf en juin 2023

Nouveau	Description
Surveillance de l’état	Affichez l’état de santé général du pare-feu Cloud NGFW, l’état de la connexion et les informations de diagnostic. Utilisez ces informations pour déterminer la cause d’un état de pare-feu défectueux. Pour plus d’informations, reportez-vous à la section Surveiller l’état de santé du Cloud NGFW.

Quoi de neuf en mai 2023

Nouveau	Description
Version initiale de Cloud NGFW pour Azure	La version initiale de Cloud NGFW pour Azure inclut les fonctionnalités suivantes : • déploiements de pare-feu vNet et vWAN • Un ou plusieurs hubs pour un vWAN. Pour plus d'informations, reportez-vous à la section Configurer Palo Alto Networks Cloud NGFW dans un WAN virtuel. • Cas d'utilisation pour le trafic entrant, sortant et est-ouest • Gestion des politiques pour les rulestacks, les objets de préfixe, FQDN et de certificat • Prise en charge de la journalisation • Prise en charge de la mise à l'échelle automatique • Décryptage sortant • Mises à jour du contenu et de l'antivirus • Mises à niveau progressives des ressources du pare-feu • Assistance fournie par le portail de support client (CSP) • Prise en charge des rôles intégrés (LocalNGFirewall et LocalRuleStacksAdministrator)

Problèmes connus de Cloud NGFW pour Azure

Les problèmes connus suivants ont été identifiés dans le Cloud NGFW pour Azure Palo Alto Networks.

ID	Description
FWAAS-10519	Lorsque la destination de multijournalisation est activée, les journaux sont affichés sur Panorama et le serveur syslog, mais aucun journal n'est affiché dans l'espace de travail Log Analytics. Workaround (Solution alternative) : Si vous souhaitez utiliser syslog avec l'espace de travail Log Analytics, remplacez l'itinéraire de service basé sur le service par un itinéraire basé sur la destination. Pour configurer **Destination Based Routing (Itinéraire basé sur la destination)**, sélectionnez la destination, ajoutez l'adresse IP privée de votre serveur syslog, puis sélectionnez **loopback.3** en tant qu'interface source.
FWAAS-9688	Les règles par défaut dans Panorama sont remplacées par la ressource Cloud NGFW. Les paramètres tels que **Profile (Profil)** et **Action** ne sont pas conservés. Par exemple, si vous configurez une action sur **Allow (Autoriser)**, le paramètre devient **Deny (Refuser)** ; si vous configurez un profil de journalisation, le paramètre devient **None (Aucun)**.
FWAAS-7531	Un certificat auto-signé peut être associé par erreur à une rulestack, et ce, malgré l'absence de nom de ressource.
FWAAS-7542	Panorama ne transmet pas toujours automatiquement le contenu et les mises à jour antivirus vers les ressources Cloud NGFW pour Azure nouvellement créées.
FWAAS-7547	Les profils QoS (fournis par un modèle de périphérique) ne sont pas supprimés lorsqu'ils sont affichés dans l'appareil virtuel Panorama.
FWAAS-7956	Une rulestack affiche des informations incorrectes lorsqu'elle porte le même nom que le pare-feu.
FWAAS-8642	La création d'un grand nombre de règles locales peut provoquer une erreur HTTP (Erreur serveur 503 : Service indisponible).
FWAAS-9086	Les informations relatives à l'état du déploiement dans le portail Azure sont tronquées sans afficher les informations complètes.
FWAAS-10195	La création du pare-feu échoue lorsque vous activez l'adressage 1918 non-RFC sans activer le proxy DNS.

ID	Description
PAN-217954	Lorsqu'une ressource Cloud NGFW pour Azure se connecte à Panorama pour la première fois, la pile de modèles associée au groupe d'appareils Cloud de la ressource n'est pas synchronisée.
PAN-217459	Les ressources NGFW cloud gérées par une paire HA Panorama peuvent être répertoriées dans le groupe d'appareils Cloud par leur numéro de série (plutôt que par le nom de l'appareil) sur le Panorama secondaire. Cependant, sur le Panorama principal, la ressource Cloud NGFW est répertoriée par son nom.
PAN-217966	Les balises du groupe d'adresses dynamiques et les adresses IP configurées ne sont pas répertoriées dans les groupes d'appareils Cloud enfants lorsqu'aucun groupe d'adresses dynamique n'est configuré pour le groupe d'appareils parent.

Problèmes résolus dans Cloud NGFW pour Azure

Les problèmes suivants ont été résolus dans cette version de Cloud NGFW pour Azure.

ID	Description
FWAAS-3919	Il est apparu que des noms de règles non valides pourraient être générés dans les rulestacks locales, ce qui pourrait entraîner des échecs de validation.
FWAAS-4546	Les entrées de la base de données du compteur Rulehit ne sont pas supprimées après la suppression de la règle, ce qui se traduit par d'anciennes valeurs si une règle est à nouveau créée avec le même nom.
FWAAS-4767	Le proxy DNS ne se met pas à jour simultanément sur le pare-feu après un appel de mise à jour du pare-feu.
FWAAS-4805	Les noms d'hôte du pare-feu sont affichés par erreur dans les journaux.
FWAAS-7430	Si vous essayez de supprimer une nouvelle ressource Cloud NGFW avant la fin de la création, la suppression échoue.
FWAAS-7542	Panorama ne transmet pas toujours automatiquement le contenu et les mises à jour antivirus vers les ressources Cloud NGFW pour Azure nouvellement créées.
FWAAS-8696	Le transfert des journaux vers un appareil virtuel Panorama peut prendre beaucoup de temps.
FWAAS-9041	Les profils de serveur de périphériques (par exemple, LDAP, syslog) apparaissent par erreur désactivés dans les modèles Panorama utilisés pour les périphériques CNGFW.
FWAAS-9050	Dans certains cas, une licence sur un pare-feu VM-Series peut être supprimée de l'appareil virtuel Panorama.
FWAAS-9055	Le périphérique CNGFW atteint un état défectueux et perd la connectivité à Panorama lorsque le nom du groupe d'appareils cloud est modifié.
PAN-217460	Les ressources Cloud NGFW gérées par une paire HA Panorama peuvent apparaître déconnectées sur le Panorama secondaire. Cependant, sur le Panorama principal, la ressource Cloud NGFW apparaît connectée.

