paloalto
TECHDOCS

Déploiement Cloud NGFW pour AWS

docs.paloaltonetworks.com

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

December 5, 2024

Table of Contents

Déploiements centralisés Cloud NGFW pour AWS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle utilisateur (locataire ou administrateur)

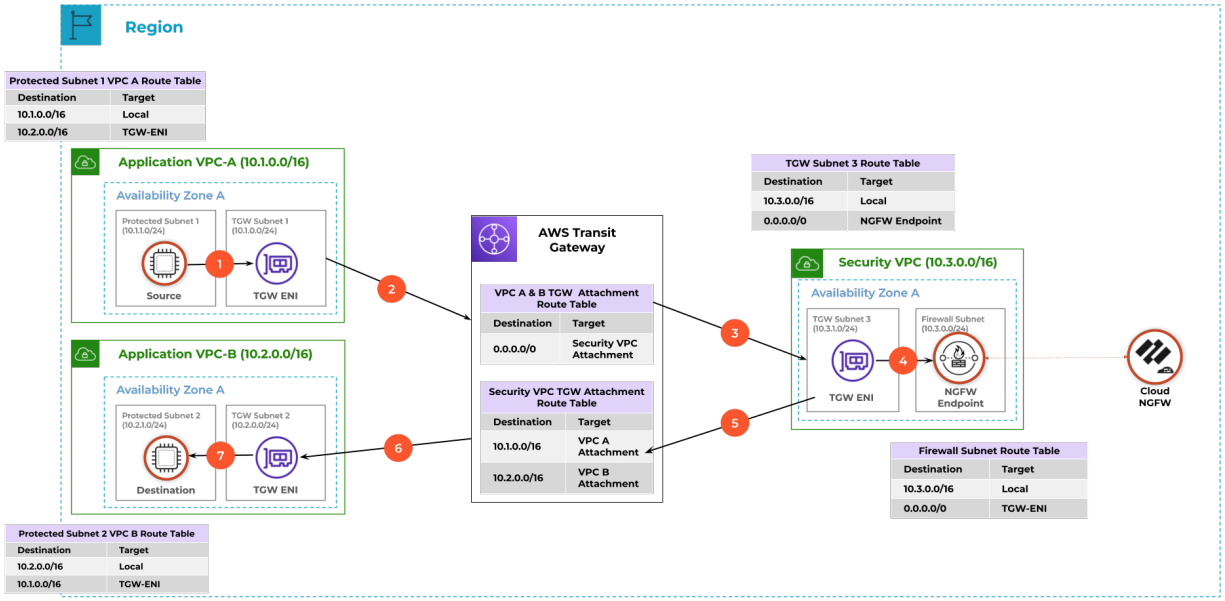
Dans un déploiement centralisé, vos composants de Cloud NGFW se déploient dans un VPC de sécurité centralisé. Le trafic doit toujours passer par une passerelle de transit AWS (TGW), qui agit comme un concentrateur réseau et simplifie la connectivité entre les VPC, ainsi que les réseaux sur site.

Pour obtenir d'autres exemples de déploiements centralisés, consultez Cloud NGFW for AWS Deployment Architectures (Architectures de déploiement Cloud NGFW pour AWS).

Centralisé est-ouest

1. Le trafic de l’instance source est dirigé vers l’interface réseau élastique (ENI) TGW.
2. L’interface réseau élastique TGW dirige le trafic vers la TGW.
3. La TGW achemine le trafic vers l’interface réseau élastique TGW du VPC de sécurité.
4. L’interface réseau élastique TGW envoie le trafic au terminal NGFW, puis au NGFW à des fins d’inspection.
5. Si le trafic est autorisé, le NGFW renvoie le trafic au terminal NGFW. Le trafic est ensuite renvoyé au TGW via le terminal TGW du VPC de sécurité.
6. La TGW transfère le trafic à l’interface réseau élastique TGW dans le VPC de destination.

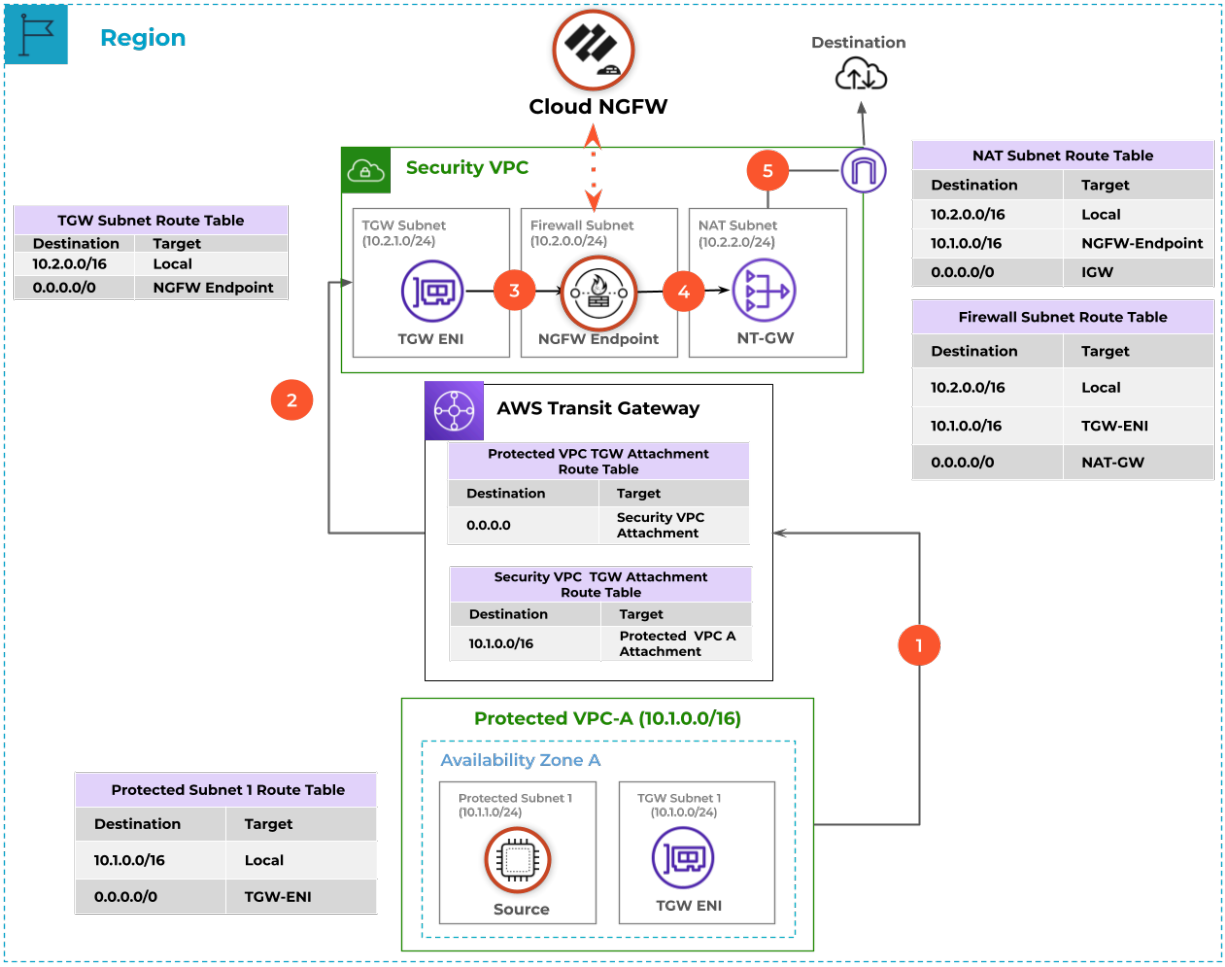
7. Ensuite, l’interface réseau élastique TGW envoie le trafic à la destination.



Sortie centralisée

1. Le trafic de l’instance source est envoyé à l’interface réseau élastique TGW, puis à la TGW.
2. La TGW achemine le trafic vers l’interface réseau élastique TGW du VPC de sécurité.
3. L’interface réseau élastique TGW envoie le trafic au terminal NGFW, puis au NGFW à des fins d’inspection.
4. Si le trafic est autorisé, le terminal NGFW achemine le trafic vers la passerelle NAT.

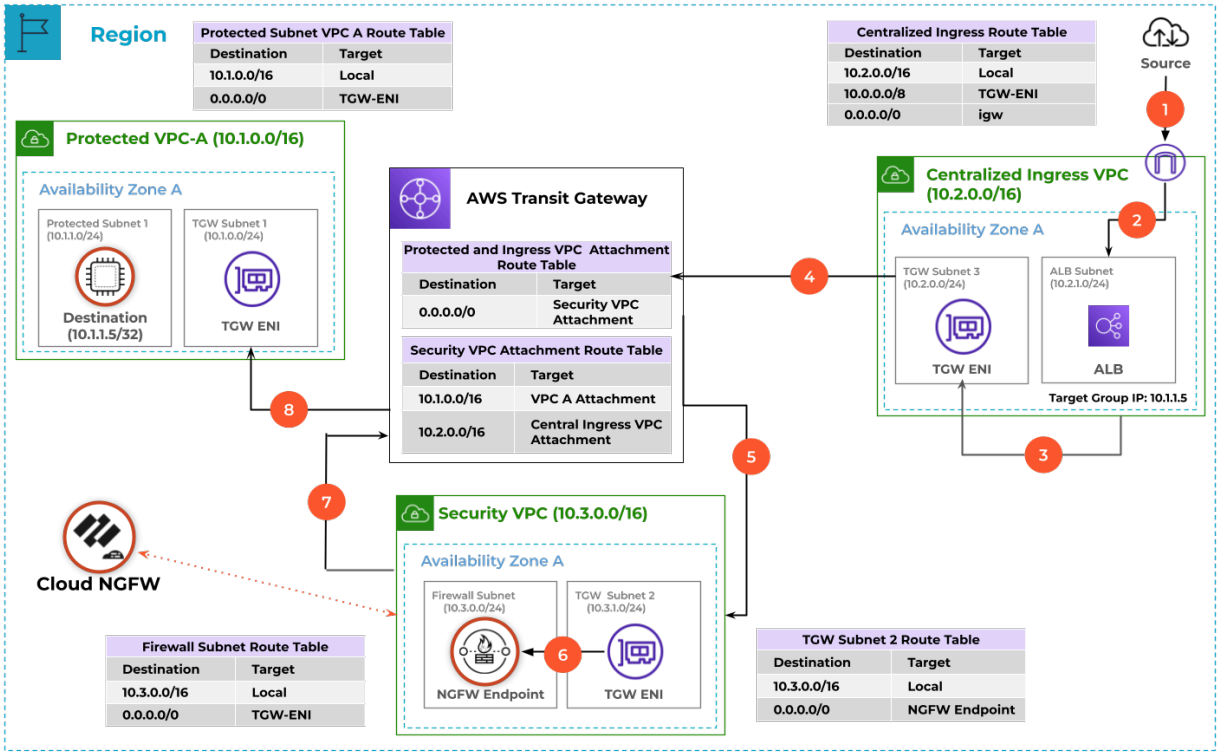
5. La passerelle NAT transmet le trafic à l’IGW et à la destination.



Entrée centralisée

1. Le trafic provenant d’Internet arrive à la passerelle Internet.
2. La passerelle Internet achemine le trafic vers l’équilibreur de charge d’application (ALB).
3. L’ALB envoie ensuite le trafic à l’interface réseau élastique TGW du VPC d’entrée.
4. L’interface réseau élastique TGW envoie le trafic vers la TGW.
5. La TGW achemine le trafic vers l’interface réseau élastique TGW du VPC de sécurité.
6. L’interface réseau élastique TGW envoie le trafic au terminal NGFW, puis au NGFW à des fins d’inspection.
7. Si le trafic est autorisé, le terminal NGFW envoie le trafic à TGW.

8. La TGW achemine ensuite le trafic vers l’interface réseau élastique TGW du VPC protégé, puis vers la destination.



Déploiements distribués Cloud NGFW pour AWS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle utilisateur (locataire ou administrateur)

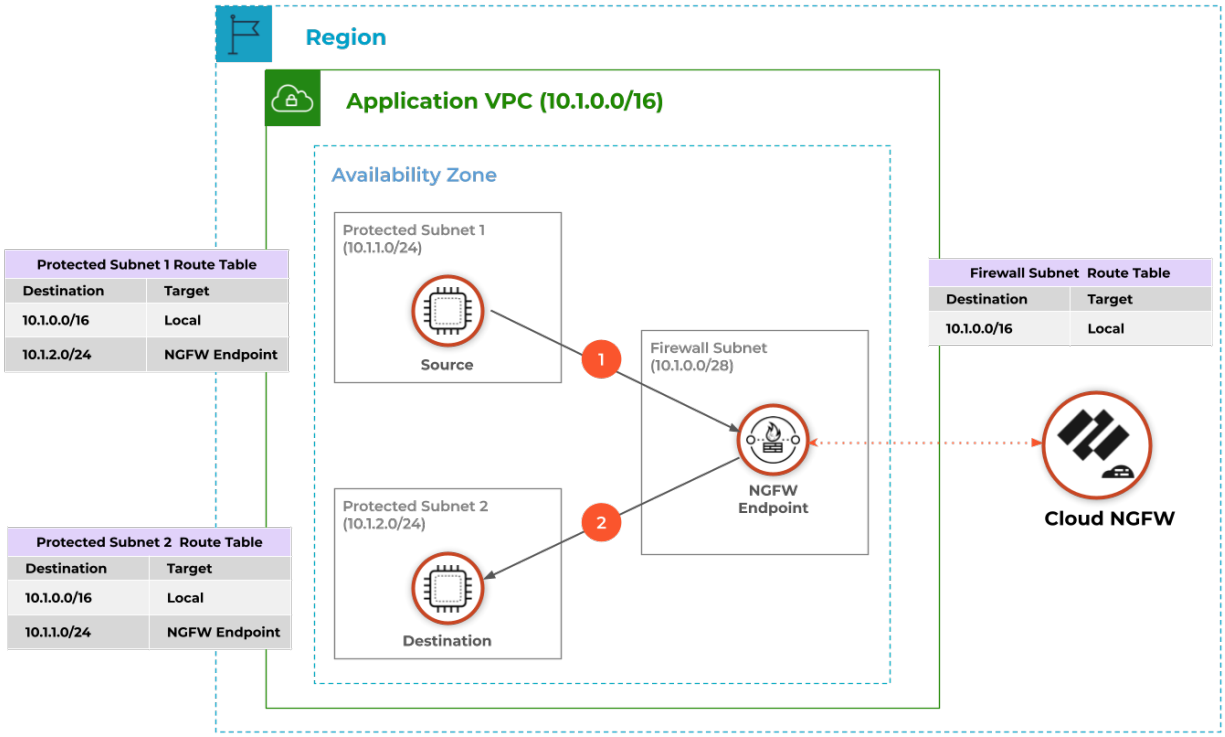
Dans un déploiement distribué, chaque VPC nécessitant une protection possède son propre NGFW. Cette méthode de déploiement est moins compliquée et, par conséquent, réduit les risques d'erreur de configuration.

Pour des exemples supplémentaires de déploiements distribués, consultez Cloud NGFW for AWS Deployment Architectures (Architectures de déploiement Cloud NGFW pour AWS).

Distribué est-ouest (intra-VPC)

1. Le trafic de l'instance source est acheminé vers le terminal NGFW et vers le NGFW pour inspection.

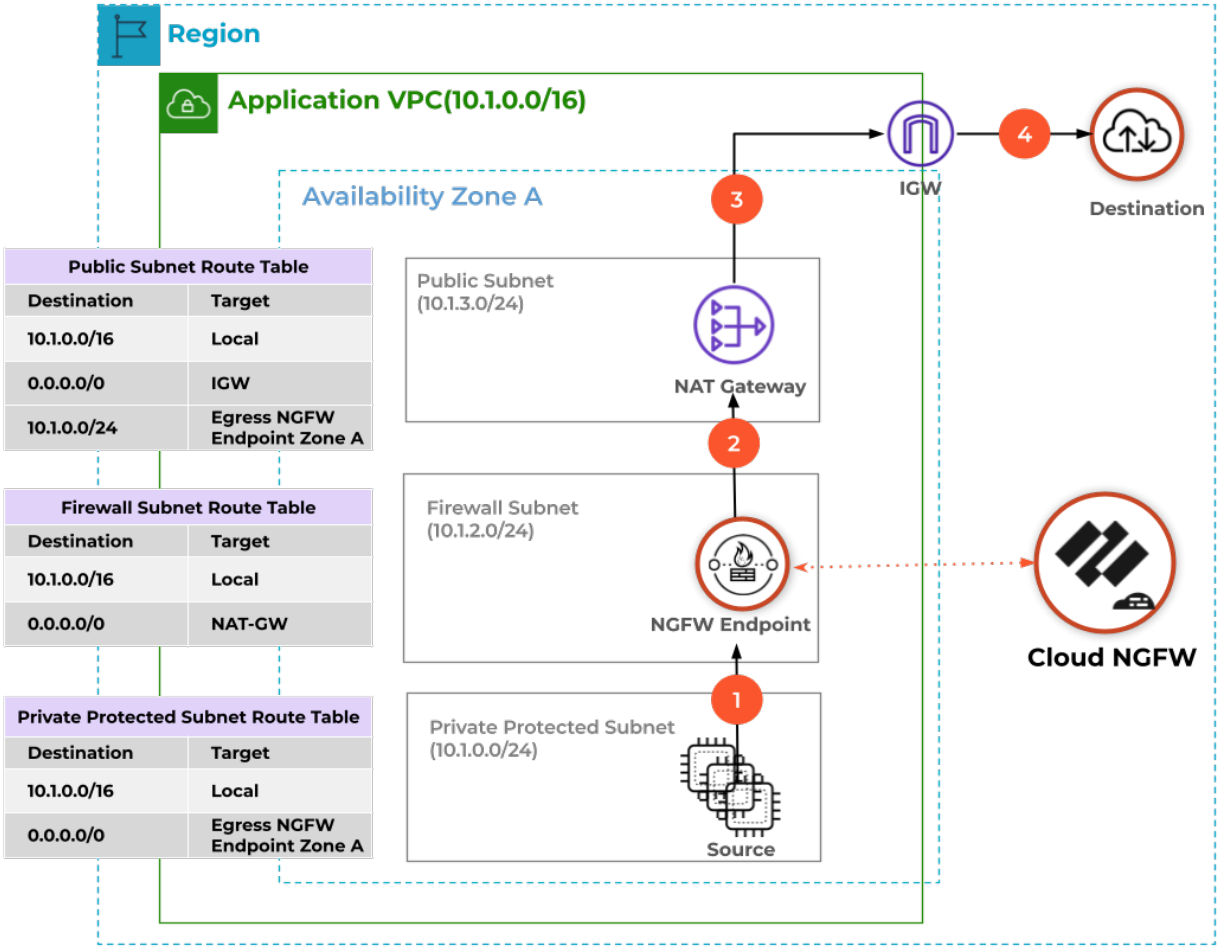
2. Si le trafic est autorisé, le terminal NGFW envoie le trafic vers la destination.



Sortant distribué

1. Le trafic de l'instance source est acheminé vers le terminal NGFW et vers le NGFW pour inspection.
2. Si le trafic est autorisé, le terminal NGFW envoie le trafic inspecté à la passerelle NAT.
3. La passerelle NAT envoie le trafic à la passerelle Internet.

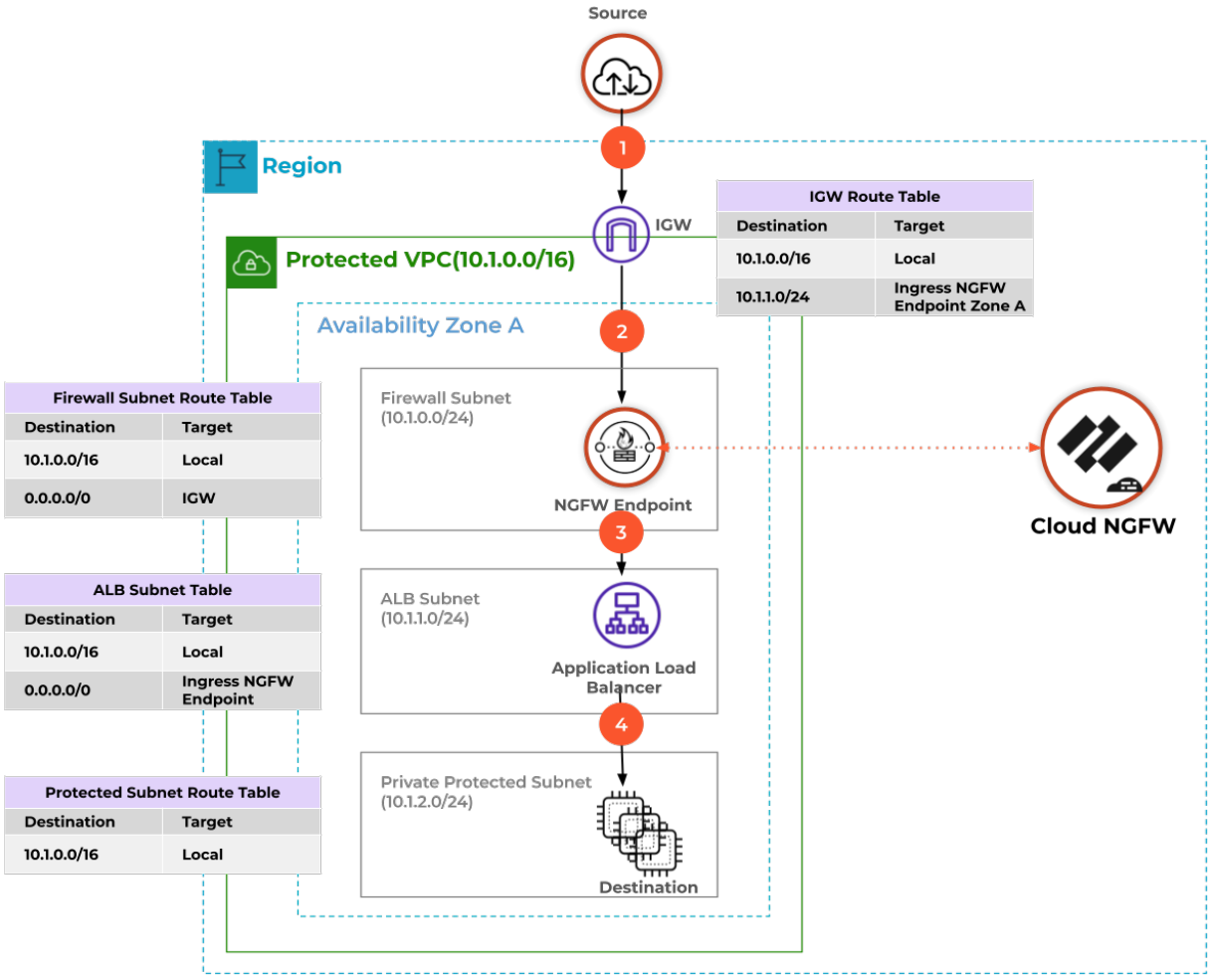
4. Le trafic continue vers Internet et la destination.



Entrant distribué

1. Le trafic provenant de la source arrive à la passerelle Internet.
2. La passerelle Internet achemine le trafic vers le terminal NGFW, puis vers le NGFW pour inspection.
3. Si le trafic est autorisé, le terminal NGFW achemine le trafic vers l'équilibreur de charge d'application.

4. L’équilibreur de charge de l’application transfère le trafic vers la destination.



Intégration de Cloud NGFW avec AWS Cloud WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle utilisateur (locataire ou administrateur)

AWS Cloud WAN est un service de réseau étendu (WAN) géré qui vous permet de créer un réseau unifié qui interconnecte les environnements cloud et sur site. Il fournit un tableau de bord centralisé pour connecter les environnements sur site, les sites de succursales, les centres de données et les clouds privés virtuels (VPC) Amazon sur le réseau mondial AWS et même d'autres fournisseurs de cloud.

Cloud WAN facilite la connectivité au sein d'AWS via le gestionnaire de réseau AWS, une interface qui gère de manière centralisée votre réseau mondial. Un réseau mondial est un réseau privé unique qui agit comme un conteneur au niveau racine pour vos objets réseau et peut contenir à la fois des passerelles de transit et un réseau principal. Le réseau principal se compose de politiques réseau, d'attachements tels que des VPC et de tables de routage de passerelle de transit.

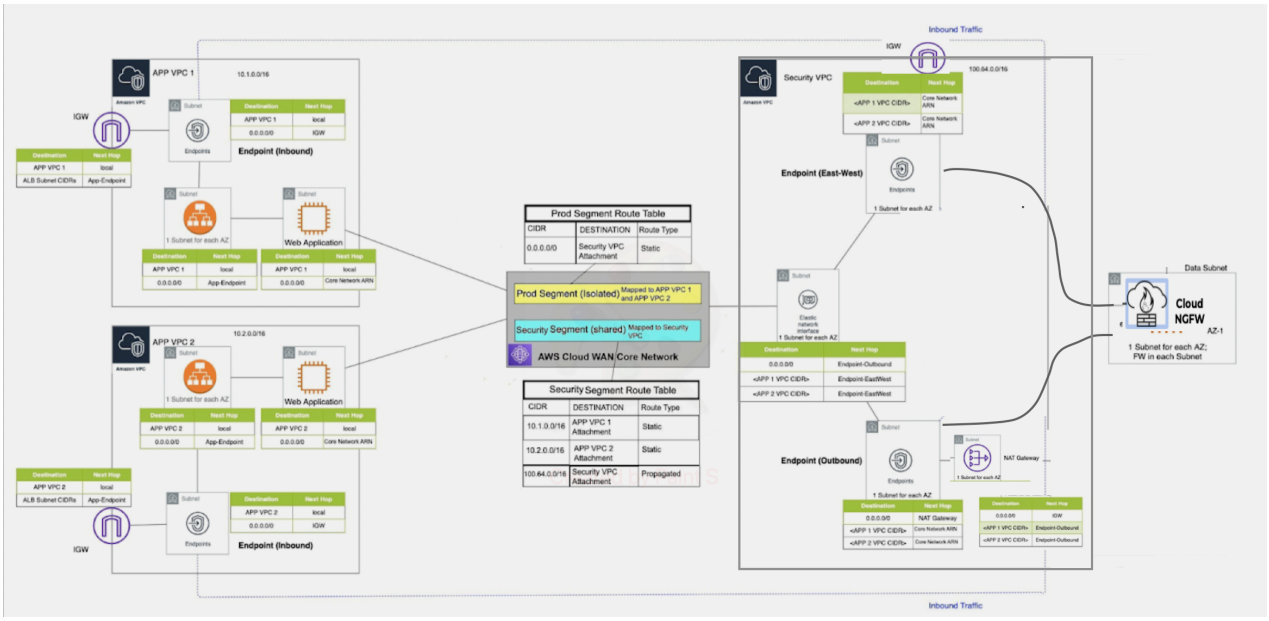
Vous pouvez mapper ces VPC à des segments du réseau principal. Ces segments sont connectés à l'aide d'attachements tels qu'un attachement de VPC ou des attachements de table de routage de passerelle de transit. La segmentation intégrée vous aide à maintenir l'isolation du réseau dans les environnements AWS et sur site. Chaque segment crée un domaine de routage dédié. Vous pouvez créer plusieurs segments de réseau au sein de votre réseau mondial. Cloud WAN restreint les ressources AWS pour communiquer au sein du segment. En résumé, Cloud WAN vous permet d'acheminer le trafic entre :

- des VPC dans le même segment et dans la même région (attachements isolés) ;
- des VPC dans différents segments de la même région ;
- des VPC dans le même segment dans différentes régions (attachements isolés) ;
- des VPC dans différents segments dans différentes régions.

Considérations antérieures au déploiement AWS Cloud WAN :

- L'appairage entre les passerelles de transit et Cloud WAN est pris en charge dans la même région, et non entre les régions.
- Pour les cas d'utilisation qui nécessitent des connexions VPN site à site AWS via Direct Connect à l'aide d'adresses IP privées, assurez-vous de connecter Cloud WAN à une passerelle de transit.
- Lors du déploiement de Cloud WAN avec des passerelles de transit, vérifiez que l'ASN de la passerelle de transit est différent de l'ASN utilisé pour les périphéries du réseau principal de Cloud WAN.
- Lors de la création du réseau principal, assurez-vous d'ajouter toutes les régions pour lesquelles vos VPC sont configurés, dans la section des emplacements périphériques sous les paramètres de

politique du réseau principal. Vous devez également créer des segments et ajouter le type de segment (développement, production, gestion ou sécurité) auquel ces régions appartiennent, sous le nom du segment.



AWS Cloud WAN peut être déployé à l’aide de deux méthodes :

- **Fédération des passerelles de transit avec le Cloud WAN** : cette méthode vous permet de remplacer les connexions d'appairage de passerelle de transit créées de manière statique par le Cloud WAN. Lors de la fédération des passerelles de transit avec le Cloud WAN, vous devrez enregistrer les passerelles de transit à l'aide du gestionnaire de réseau AWS, créer un appairage entre les passerelles de transit, créer des attachements aux passerelles de transit, puis appliquer la configuration le Cloud WAN.
- **Cloud WAN uniquement** : cette méthode permet d'utiliser le Cloud WAN pour toutes les connectivités et les passerelles de transit sont supprimées.

Déployer l'AWS Cloud WAN

Cloud WAN est l'interconnexion des VPC et des réseaux sur site. Examinons maintenant en profondeur comment sécuriser le trafic interconnecté avec le Cloud WAN à l'aide des Palo Alto Networks Cloud NGFW. Bien que Cloud WAN soit une construction mondiale, Palo Alto Networks recommande le déploiement du Cloud NGFW dans chaque région AWS qu'il couvre, afin de maintenir une posture de sécurité à faible latence et à coûts optimisés.

Cloud NGFW peut être déployé dans un VPC de sécurité centralisé dans chaque région. Le VPC de sécurité peut être directement connecté au segment de sécurité du cloud WAN via un attachement. Le routage associé aux attachements et aux segments définit l'acheminement du trafic vers la ressource Cloud NGFW aux fins de la prévention des menaces. Vous pouvez rediriger le trafic provenant des attachements du cloud vers un VPC de sécurité, avant de le transférer vers la destination. Le Cloud NGFW déployé au sein d'une région peut désormais protéger et sécuriser.

- le trafic est-ouest avec des flux interrégionaux et des flux intrarégionaux
- Inspecter et sécuriser le flux de trafic sortant
- Inspecter et sécuriser le trafic provenant de l'environnement sur site et des succursales

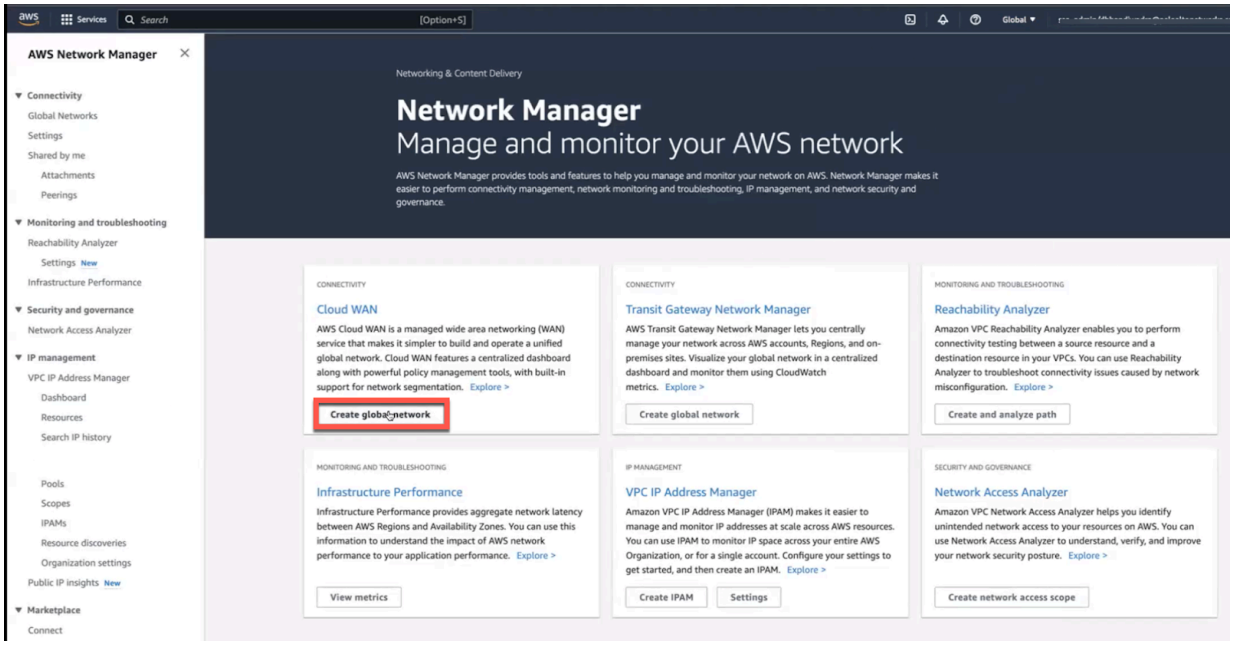
Examinons un cas d'utilisation où les VPC se trouvent dans la même région (attachements isolés). Pour réaliser cette configuration, déployez le pare-feu du Cloud NGFW dans le VPC de sécurité. Vous pouvez déployer le pare-feu du Cloud NGFW dans un VPC de sécurité, directement connecté à un Cloud WAN ou via une passerelle de transit avec un attachement de Cloud WAN.

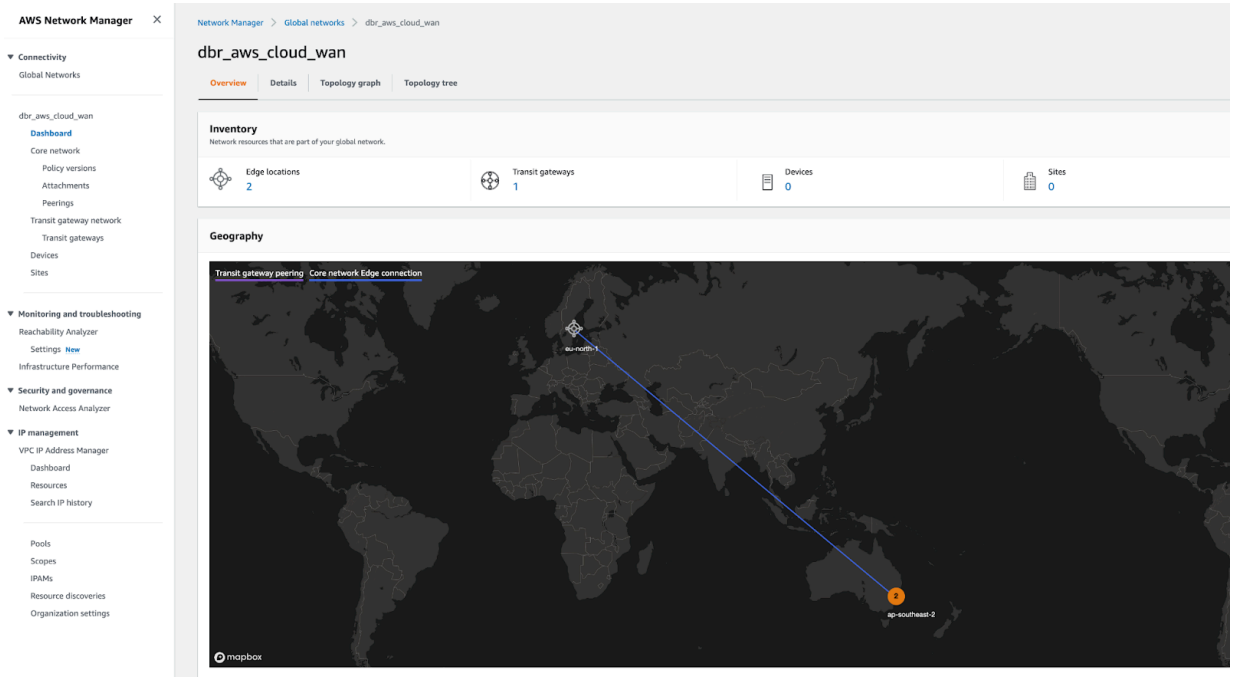
Pour migrer complètement en dehors de la passerelle de transit, vous devez connecter vos VPC directement au Cloud WAN.

Le trafic de sortie du VPC de production est acheminé vers le Cloud WAN, qui est ensuite acheminé vers le VPC de sécurité pour inspection et envoyé via la passerelle NAT et la passerelle interne. Dans le sens inverse, le trafic provenant du VPC de sécurité atteint le segment de sécurité puis, en fonction de la configuration de routage, est envoyé à l'attachement de VPC.

Pour inspecter le trafic entre les VPC du même segment et de la même région avec le déploiement **AWS Cloud WAN (uniquement)**, exécutez les tâches suivantes :

1. Connectez-vous au gestionnaire de réseau AWS et cliquez sur Create global network (Créer un réseau mondial).

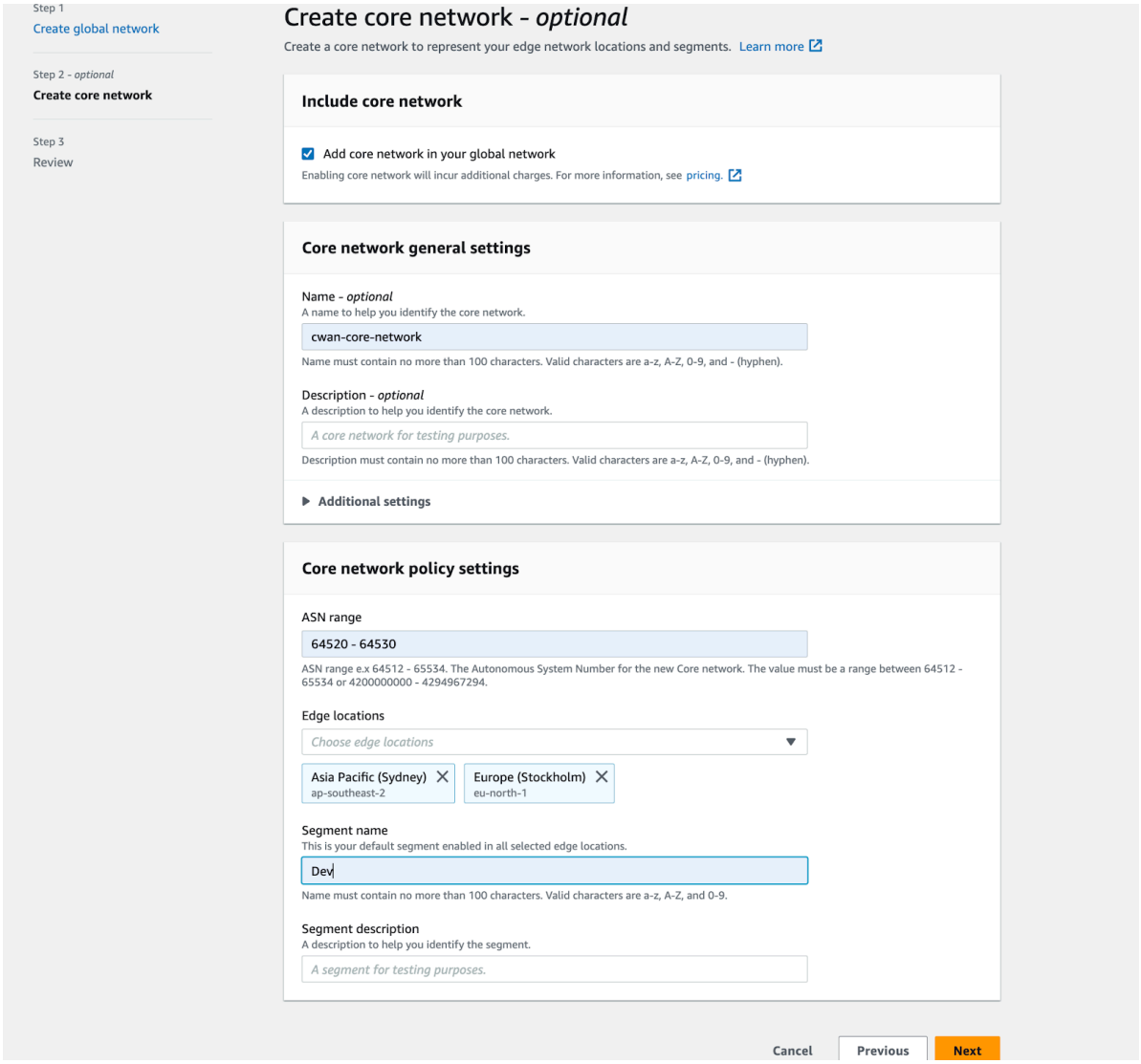




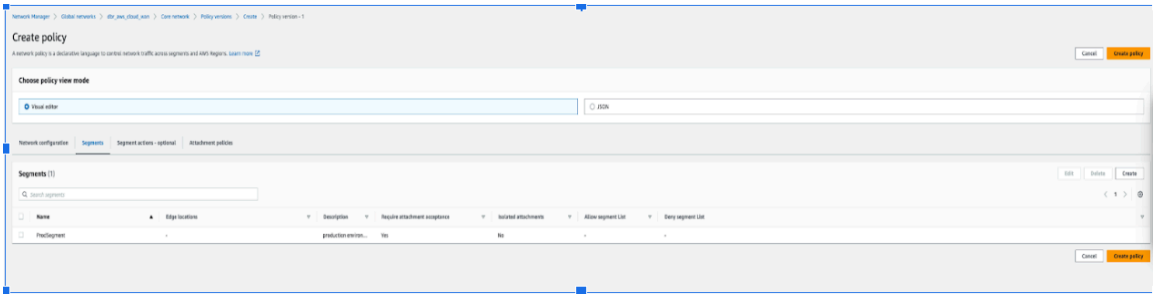
2. Créez un réseau principal et une politique de réseau principal.

   Utilisez la console AWS Cloud WAN pour créer une version de politique de réseau principal en effectuant les tâches suivantes :

   - Configurez les paramètres réseau.

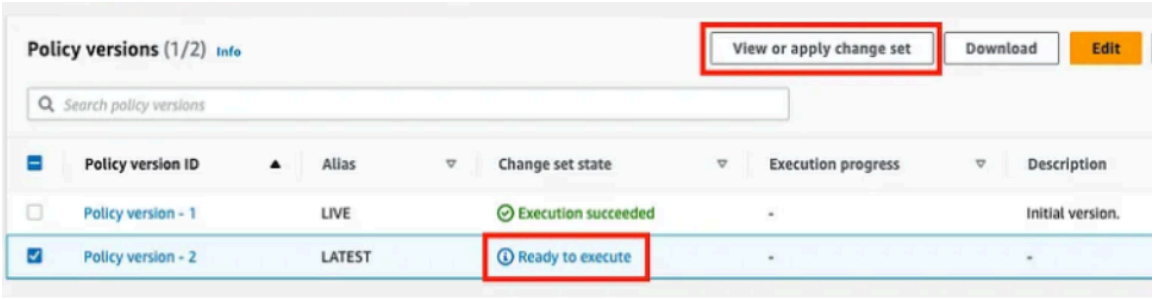


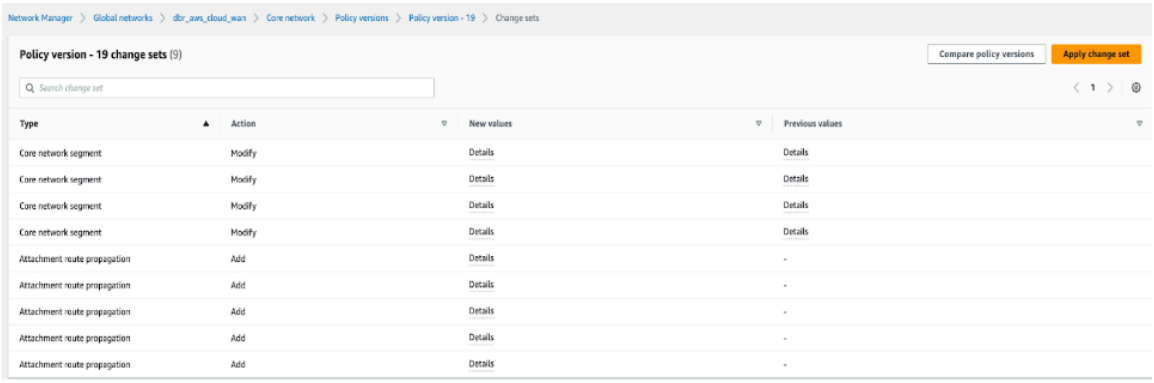
- Pour modifier une version de politique, cliquez sur **Policy versions (Versions de politique)**, sélectionnez la politique requise et cliquez sur **Edit (Modifier)**. Effectuez les modifications nécessaires et cliquez sur **Create Policy (Créer une politique)**.



- Une fois que l’état de l’ensemble des modifications de la version de la politique passe à **Ready to execute (Prêt à exécuter)**, exécutez la politique en cliquant sur **View or apply change set (Afficher ou appliquer l’ensemble des modifications).** Vous pouvez également cliquer sur

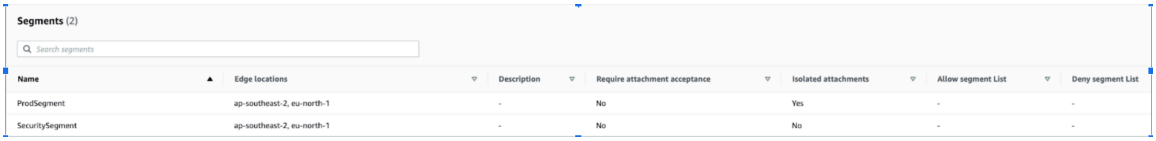
Compare policy version (Comparer la version de la politique) pour afficher le document JSON.



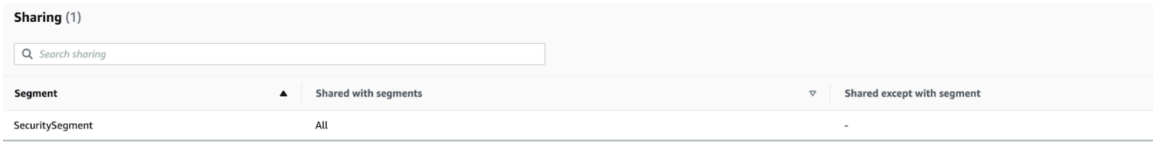


- Créez des segments de politique de réseau au sein de votre réseau principal.

  Lors de la configuration des versions de politique, assurez-vous d'ajouter les applications – APP VPC 1 (10.1.0.0/16) et APP VPC 2 (10.2.0.0/16) dans le segment de production et le pare-feu, ainsi que le VPC de sécurité (100.64.0.0/16) dans le segment de sécurité.



- Créez des actions de partage de segments et de route de segment.

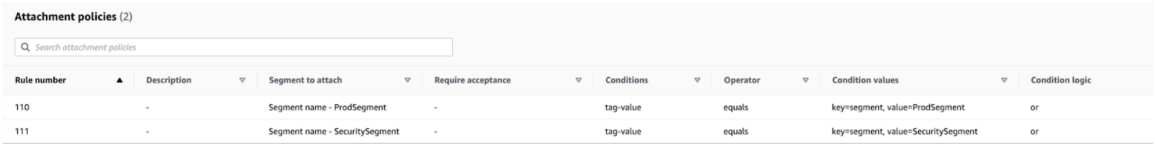


Routes (3)

Search routes

Segment	Destination CIDR block	Destination
ProdSegment	0.0.0.0/0	attachment-0853fd8b1c1a3ed87
SecuritySegment	10.1.0.0/16	attachment-04fd636bdaaf4f6e0
SecuritySegment	10.2.0.0/16	attachment-0ffa029e9effa9ba2

- Créez des attachements de politique.



Attachment policies (2)

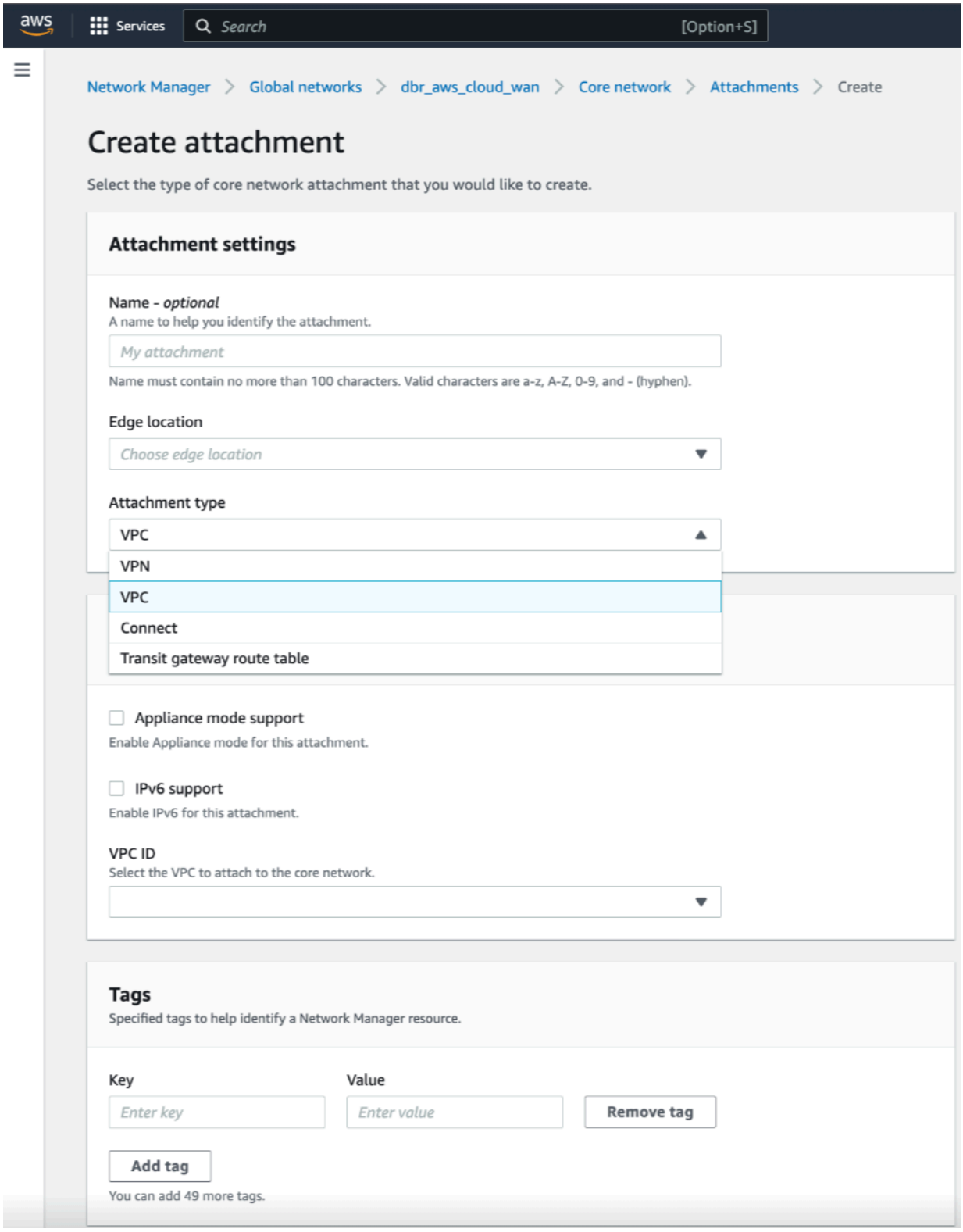
Search attachment policies

Rule number	Description	Segment to attach	Require acceptance	Conditions	Operator	Condition values	Condition logic
110	-	Segment name - ProdSegment	-	tag-value	equals	key=segment, value=ProdSegment	or
111	-	Segment name - SecuritySegment	-	tag-value	equals	key=segment, value=SecuritySegment	or

Vous pouvez choisir d'ajouter des étiquettes telles que le segment de production (valeur) au segment (clé). Ces étiquettes ne sont reflétées qu'après avoir ajouté les segments dans le Cloud WAN.

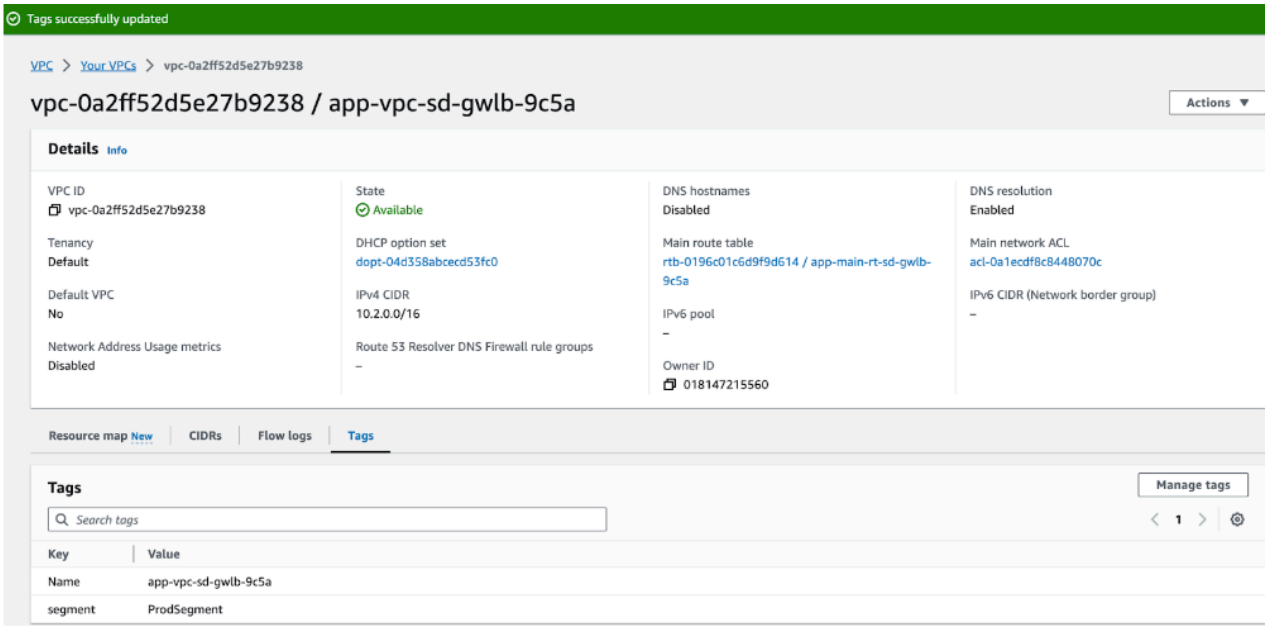
3. Créez un attachement.

- *Utilisez la table de routage d'un VPC ou d'une passerelle de transit comme type d'attachement pendant la création d'un attachement.*
- *Pour que le pare-feu du Cloud NGFW puisse inspecter le trafic acheminé entre les attachements de VPC, vous devez activer le mode appareil sur l'attachement de VPC pour le VPC de sécurité contenant le pare-feu du Cloud NGFW.*

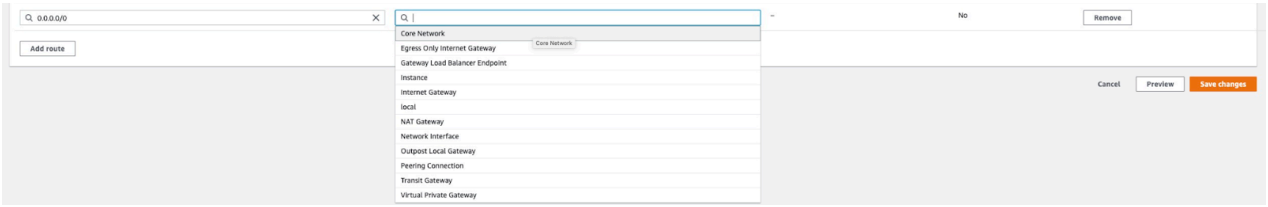


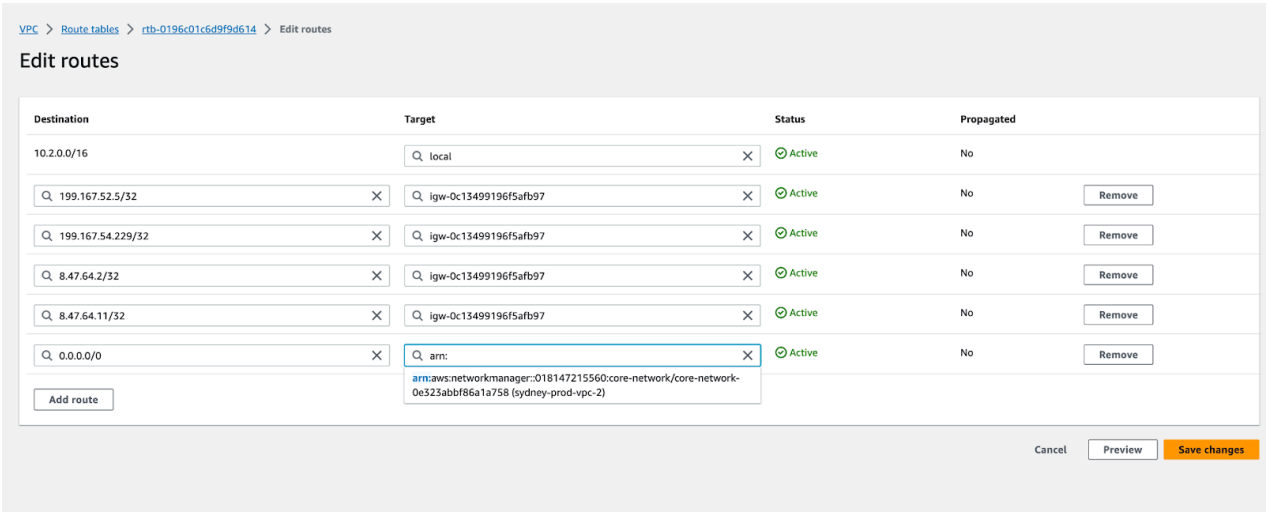
4. Mettez à jour les tables de routage de VPC.

   Maintenant que les constructions Cloud WAN nécessaires sont en place, les VPC doivent être ajustés pour faciliter le transfert des paquets vers le réseau principal. Les instances d'application et de pare-feu ou les VPC respectifs doivent être étiquetés de la même manière que le segment. Ajoutez des étiquettes spécifiques à l'attachement pour le faire correspondre à l'attachement créé lors de la création des attachements de politique de l'étape 2.



Pour activer la communication entre les attachements de VPC et le réseau principal, les tables de routage VPC doivent être mises à jour à partir de la route de la passerelle de transit cible existante vers l'ARN du réseau principal correspondant, comme indiqué ci-dessous.



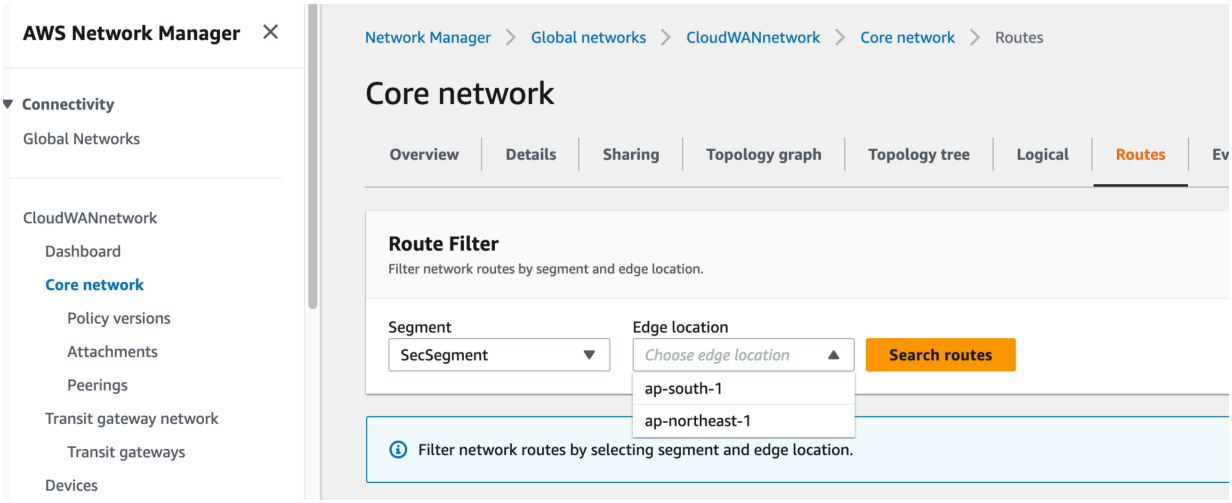


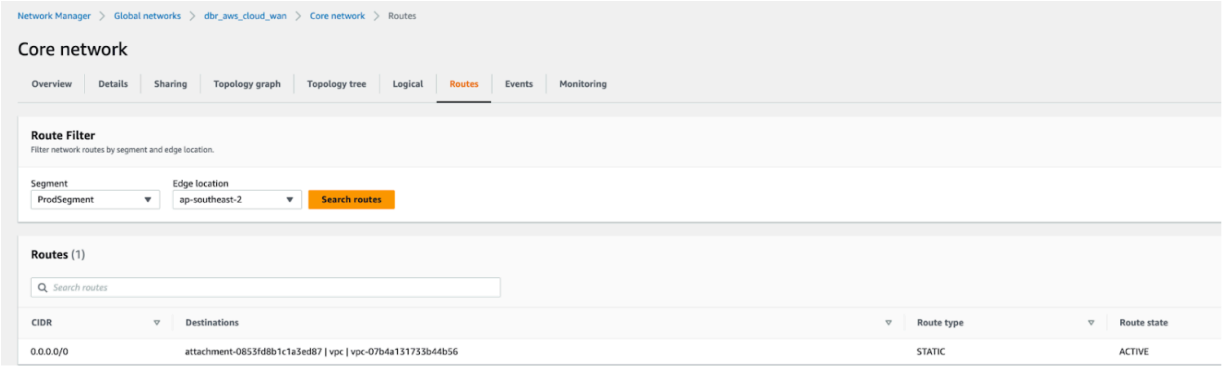
Procédure pas à pas relative aux paquets

Les étapes suivantes décrivent une procédure pas à pas de paquets lorsqu'une instance EC2 du VPC 1 de l'application communique avec une instance EC2 dans le VPC 2 de l'application :

- Lorsqu'un client dans APP VPC 1 (10.1.0.0/16) démarre une connexion à un serveur dans APP VPC 2 (10.2.0.0/16), il effectue une recherche dans la table de routage du VPC (sous-réseau de l'application). Le paquet correspond à l'entrée de la route par défaut avec l'ARN du réseau principal comme cible et le paquet est acheminé vers le réseau principal.
- Lorsque le paquet arrive au réseau principal, il effectue une recherche dans la table de routage du segment de production, car APP VPC 1 est associé au segment de production. Le paquet correspond à

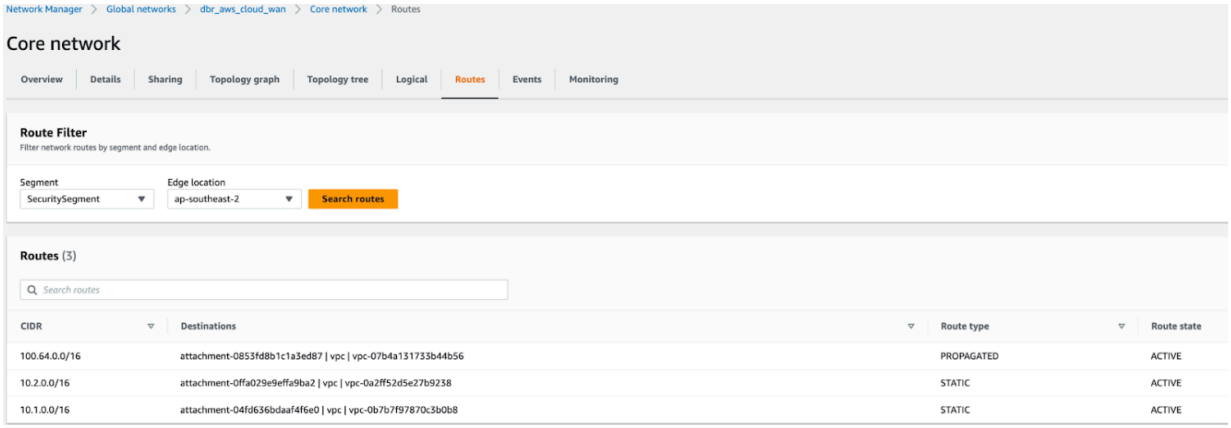
l’entrée par défaut avec l’attachement de sécurité comme cible et le paquet est acheminé vers le VPC de sécurité.





- Lorsque le paquet arrive à l'attachement de sécurité du VPC (100.64.0.0/16), il effectue une recherche dans la table de routage du VPC (sous-réseau CWAN). Le paquet correspond à la route par défaut avec le terminal 1 du pare-feu comme cible et le paquet est acheminé vers un pare-feu, via le terminal du pare-feu, pour inspection.
- Le pare-feu inspecte le trafic, le compare à sa politique de sécurité et le laisse passer. Le pare-feu achemine le paquet vers le terminal du pare-feu, où il effectue une recherche dans la table de routage du VPC (sous-réseau du pare-feu). Le paquet correspond à l'entrée de route par défaut avec l'ARN du réseau principal comme cible, et le paquet est acheminé vers le réseau principal.
- Lorsque le paquet arrive au réseau principal, il effectue une recherche dans la table de routage de sécurité partagée, car le VPC de sécurité est associé au segment de sécurité. Le paquet correspond à

l’entrée APP VPC 2 CIDR (10.2.0.0/16) avec l’attachement APP VPC 2 comme cible et le paquet est acheminé vers APP VPC 2.



- Lorsque le paquet arrive à APP VPC 2, il effectue une recherche dans la table de routage du VPC (sous-réseau CWAN). Le paquet correspond à l’entrée CIDR du VPC avec local comme cible et le paquet est acheminé vers l’instance.

Le trafic de retour suit le même chemin en sens inverse.

