paloalto TECHDOCS

Cloud NGFW pour AWS

2.0.0

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

July 26, 2022

Table of Contents

Mise en route avec Cloud NGFW pour AWS

Cloud NGFW pour AWS est une fonctionnalité de pare-feu nouvelle génération (NGFW) alimentée par Palo Alto Networks ML fournie en tant que service cloud natif entièrement géré par Palo Alto Networks sur la plateforme Amazon Web Services (AWS). 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.

À propos de Cloud NGFW pour AWS

Vous pouvez découvrir Cloud NGFW dans AWS Marketplace et l'utiliser dans vos clouds privés virtuels (VPC) AWS. Avec Cloud NGFW, vous pouvez accéder aux fonctionnalités NGFW de base telles que App-ID, filtrage des URL basé sur les catégories d'URL et les géolocalisations, décryptage SSL/TLS, etc.

Composants Cloud NGFW

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

- Le **locataire Cloud NGFW** est une instanciation du service Cloud NGFW associé à votre compte AWS lorsque l'un de vos utilisateurs AWS s'abonne au service. Cloud NGFW vous désigne, l'utilisateur AWS abonné, en tant qu'administrateur du locataire Cloud NGFW (le rôle d'utilisateur TenantAdmin), qui pouvez inviter d'autres utilisateurs au locataire. En fonction du rôle attribué, d'autres utilisateurs peuvent créer des ressources Cloud NGFW et configurer des rulestacks avec le locataire.
- La **ressource Cloud NGFW** (ou simplement NGFW) est associée à votre VPC et peut s'étendre sur plusieurs zones de disponibilité. Cette ressource intègre la résilience, l'évolutivité et la gestion du cycle de vie.
- Pour utiliser la ressource Cloud NGFW, vous créez un sous-réseau dédié dans votre VPC pour chaque zone de disponibilité AWS souhaitée, puis créez des **terminaux NGFW** sur les sous-réseaux et mettez à jour les tables de routage VPC pour envoyer le trafic via ces terminaux Cloud NGFW.
- 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 associez la pile de règles à une ou plusieurs ressources NGFW. Cloud NGFW fournit deux types de rulestacks.

  Cloud NGFW prend en charge deux types de rulestacks :

  - **Rulestack locale** : Les administrateurs de compte locaux peuvent associer une rulestack locale à un NGFW dans leur compte AWS. Une rulestack locale inclut des règles locales
  - **Rulestack globale** : L'administrateur d'AWS Firewall Manager peut créer une politique de service Firewall Manager (FMS) et y associer une rulestack globale. AWS Firewall Manager gère la rulestack globale sur tous ces NGFW dans différents comptes AWS d'une organisation AWS. Une rulestack globale inclut des règles « avant » et des règles « après ».

Cloud NGFW en action

1. **S'abonner au service Cloud NGFW** : commencez par vous abonner au service Cloud NGFW pour AWS via AWS Marketplace. Après votre abonnement, vous pouvez créer un locataire Cloud NGFW. L'utilisateur AWS IAM abonné est l'administrateur de locataire (TenantAdmin), ce qui permet à cet utilisateur d'inviter des utilisateurs supplémentaires et d'attribuer des rôles. Vous devez ajouter votre compte AWS au locataire Cloud NGFW. L'ajout de votre compte accorde les autorisations nécessaires à Cloud NGFW pour stocker les journaux, créer des terminaux NGFW et accéder aux clés nécessaires au décryptage.
2. **Créer des rulestacks** : après avoir ajouté des utilisateurs et attribué des rôles dans la console de locataire Cloud NGFW, les administrateurs de rulestack locale peuvent créer des règles et des rulestacks.

3. **Créer des NGFW** : déployez des ressources de pare-feu NGFW pour protéger vos VPC. Lors de la création de vos NGFW, associez les rulestacks locales que vous avez créées précédemment.

   Vous disposez de deux options pour créer des terminaux Cloud NGFW. Dans la première option (service géré), vous créez un sous-réseau dédié dans votre VPC pour chaque zone de disponibilité AWS souhaitée, puis spécifiez ces sous-réseaux lors de la création de ressources Cloud NGFW. Dans cette option, Cloud NGFW crée les terminaux NGFW dans vos sous-réseaux. Sinon, dans la deuxième option (gérée par le client), vous spécifiez les zones de disponibilité AWS souhaitées, où vous souhaitez que la ressource NGFW sécurise le trafic. Dans cette option, Cloud NGFW crée une ressource Cloud NGFW uniquement qui se manifestera en tant que ressources de terminal VPC dans votre compte AWS. Vous êtes ensuite responsable de la création d'un sous-réseau dédié dans votre VPC pour chaque zone de disponibilité AWS souhaitée, ainsi que de la création des terminaux du VPC
4. **Mettre à jour les tables de routage VPC** : après le déploiement de votre ressource Cloud NGFW, vous devez Diriger le trafic vers Cloud NGFW pour AWS en mettant à jour vos tables de routage de VPC. Le trafic est ensuite dirigé vers la ressource de pare-feu NGFW pour inspection et application.

Cas pratiques de 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 AWS et destiné aux ressources de vos VPC d'application, telles que les serveurs ou les équilibreurs de charge. Cloud NGFW peut empêcher les logiciels malveillants et les vulnérabilités d'entrer dans votre VPC dans le trafic entrant autorisé par les groupes de sécurité AWS.
- Le trafic **sortant** fait référence au trafic provenant de votre VPC d'application et pour des destinations en dehors de la région AWS. Cloud NGFW protège les flux de trafic sortant en garantissant que les ressources de votre VPC d'application se connectent aux services autorisés et aux URL autorisées tout en empêchant l'exfiltration de données et d'informations sensibles.
- Le trafic **est-ouest** est le trafic qui se déplace au sein d'une région AWS. Plus précisément, le trafic entre la source et la destination est déployé dans deux VPC d'application différents ou dans deux sous-réseaux différents dans les mêmes VPC. Cloud NGFW peut arrêter la propagation de logiciels malveillants dans votre environnement AWS.

Démarrage dans AWS Marketplace

Il existe plusieurs façons de démarrer avec Cloud NGFW à partir d'AWS Marketplace. Le critère de décision critique réside dans la détermination d'utiliser ou non AWS Firewall Manager pour fonctionner avec Cloud NGFW.

- **Pour démarrer à partir de comptes membres AWS** : vous pouvez vous abonner à la liste des SaaS de Palo Alto Networks Cloud NGFW pour AWS Marketplace à partir de votre compte AWS membre. Chaque abonnement entraîne la création d'un locataire Cloud NGFW unique.

  Vous pouvez ensuite ajouter plusieurs autres comptes AWS au locataire Cloud NGFW. Vous pouvez créer des ressources Cloud NGFW (également appelées des NGFW) et les associer à des VPC dans leurs comptes AWS. Vous pouvez également créer des politiques de sécurité sur ces NGFW. Cloud NGFW surveille l'utilisation du locataire Cloud NGFW et envoie des enregistrements de mesure au service de mesure AWS Marketplace. AWS utilise ces informations pour facturer le client.

  Dans votre compte AWS, vous devez ajouter un terminal NGFW (également appelé terminal VPC) pour cette ressource. Vous devez ensuite ajouter des règles de routage VPC pour acheminer tout le trafic vers le terminal NGFW pour inspection. AWS redirige automatiquement le trafic envoyé au terminal NGFW vers la ressource NGFW pour inspection. Le trafic envoyé à un terminal NGFW est toujours renvoyé au même terminal NGFW : le NGFW se comporte comme une « passerelle de sécurité ».

  Une fois que vous commencez avec cette méthode, vous ne pouvez pas utiliser AWS Firewall Manager avec ce locataire Cloud NGFW.

- **Démarrage à partir d'un compte administrateur AWS Firewall Manager** : si vous utilisez actuellement AWS Firewall Manager pour gérer des groupes de sécurité ou d'autres fonctionnalités de sécurité réseau au sein de votre organisation AWS, vous pouvez utiliser le même AWS Firewall Manager pour déployer des NGFW dans plusieurs comptes et VPC au sein d'une organisation AWS

  Lancez l'abonnement AWS Marketplace pour la liste de Cloud NGFW à partir du compte administratif AWS Firewall Manager désigné par l'organisation AWS.

  Utilisez ensuite le flux de travail de la politique AWS Firewall Manager pour créer une rulestack globale et déployer rapidement des NGFW sur plusieurs comptes AWS dans une organisation AWS. Sous le capot, le Firewall Manager orchestre tous les composants. Il s'agit notamment d'appeler les API Cloud NGFW pour créer les NGFW et d'appeler les API AWS pour créer les terminaux NGFW dans les VPC clients.

  Veuillez vous reporter au blog et à la vidéo sur l'intégration d'AWS Firewall Manager pour en savoir plus sur les façons d'intégrer AWS Firewall Manager à Cloud NGFW pour AWS.

  Une fois que vous commencez avec cette méthode, vous devez toujours utiliser un AWS Firewall Manager pour ajouter des comptes AWS au locataire Cloud NGFW.

Enregistrer votre locataire Cloud NGFW sur un compte de support Palo Alto Networks

Cloud NGFW vous invitera à enregistrer un compte de support pour votre locataire Cloud NGFW après avoir réinitialisé votre mot de passe et avant de vous connecter pour la première fois à la console de votre locataire Cloud NGFW. Si vous êtes un utilisateur enregistré d'un ou de plusieurs comptes de support Palo Alto Networks existants, vous pouvez choisir d'**enregistrer votre locataire Cloud NGFW** sur l'un d'eux **lors de la connexion initiale**.

Il se peut que vous ayez utilisé une autre adresse e-mail pour vous abonner à Cloud NGFW et une adresse différente pour accéder au compte de support de Palo Alto Networks. Vous pouvez également créer un compte de support Palo Alto Networks dédié pour Cloud NGFW. Dans les deux cas, vous devez sauter l'option d'enregistrement lors de la connexion initiale, mais **enregistrer votre locataire Cloud NGFW dans le portail de support client**.

Enregistrer votre locataire cloud NGFW lors de la connexion initiale

Utilisez cette procédure pour enregistrer votre locataire Cloud NGFW auprès de votre compte de support existant :

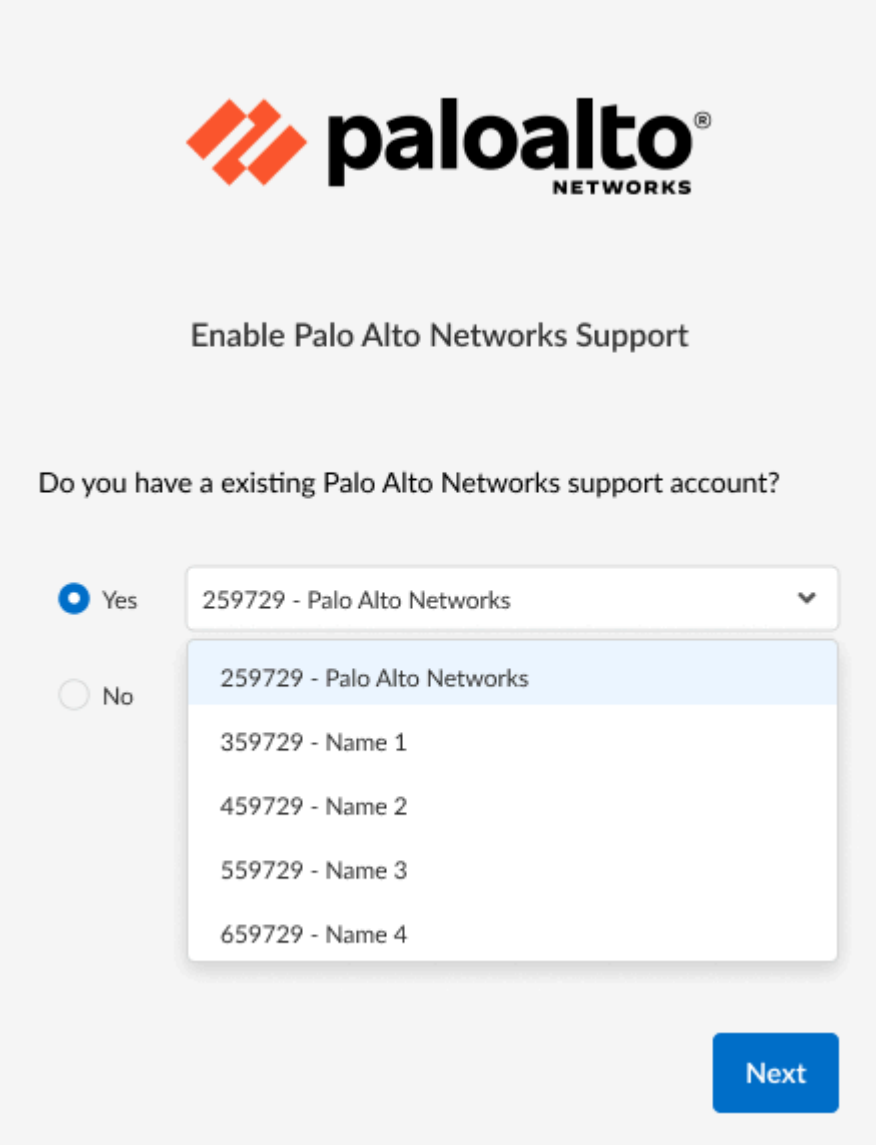
STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sur l'écran **Enable Palo Alto Networks Support (Activer l'assistance Palo Alto Networks)**, sélectionnez **Yes (Oui)**.

> *Si vous sélectionnez **No (Non)** dans l'écran **Enable Palo Alto Networks (Activer Palo Alto Networks)**, vous devez utiliser le Customer Support Portal (Portail de support client – CSP) pour enregistrer votre locataire Cloud NGFW, ou utiliser la console Cloud NGFW pour vous enregistrer sur le CSP. Consultez Enregistrer votre locataire Cloud NGFW à l'aide du portail de support client et*

STEP 3 | Utilisez le menu déroulant pour sélectionner le compte de support.

STEP 4 | Cliquez sur **Next (Suivant)**.



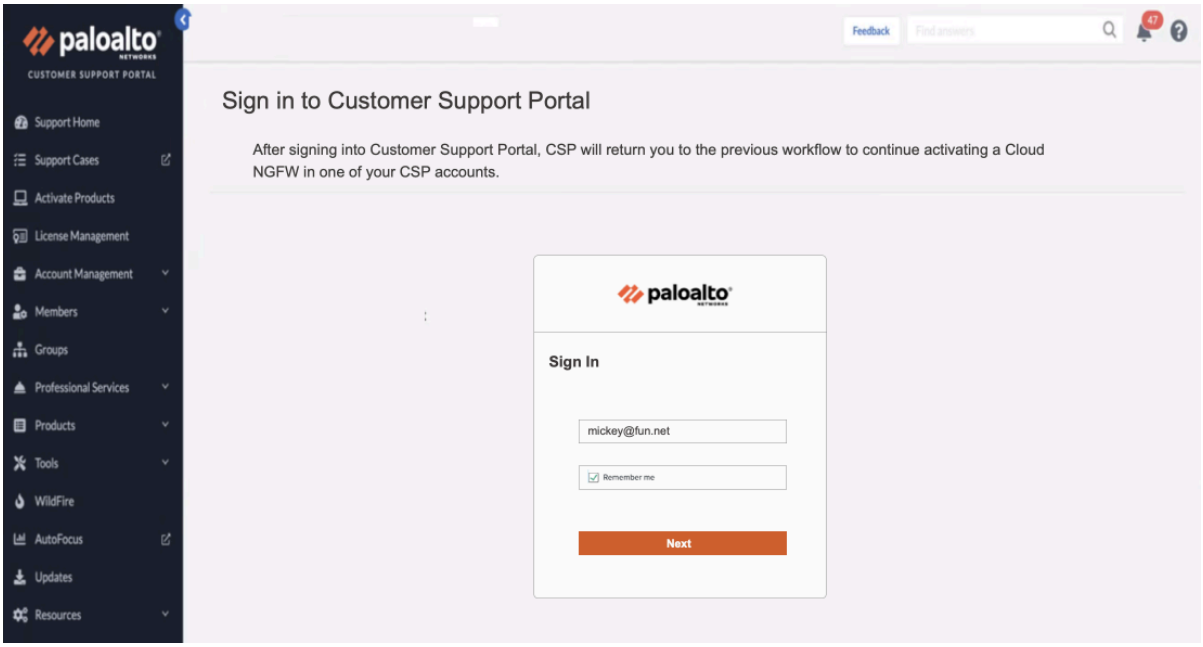
Si vous avez déjà enregistré votre compte de support client (CSP), la liste déroulante est renseignée avec les comptes existants. Toutefois, si vous êtes un nouvel utilisateur et que vous n'avez pas encore de compte, utilisez la page CSP pour créer un compte. Consultez Enregistrer votre locataire Cloud NGFW à l'aide du portail de support client *et* Inscrire votre locataire Cloud NGFW sur le portail de support client à l'aide de la console Cloud NGFW.

Enregistrer votre locataire Cloud NGFW à l'aide du portail de support client

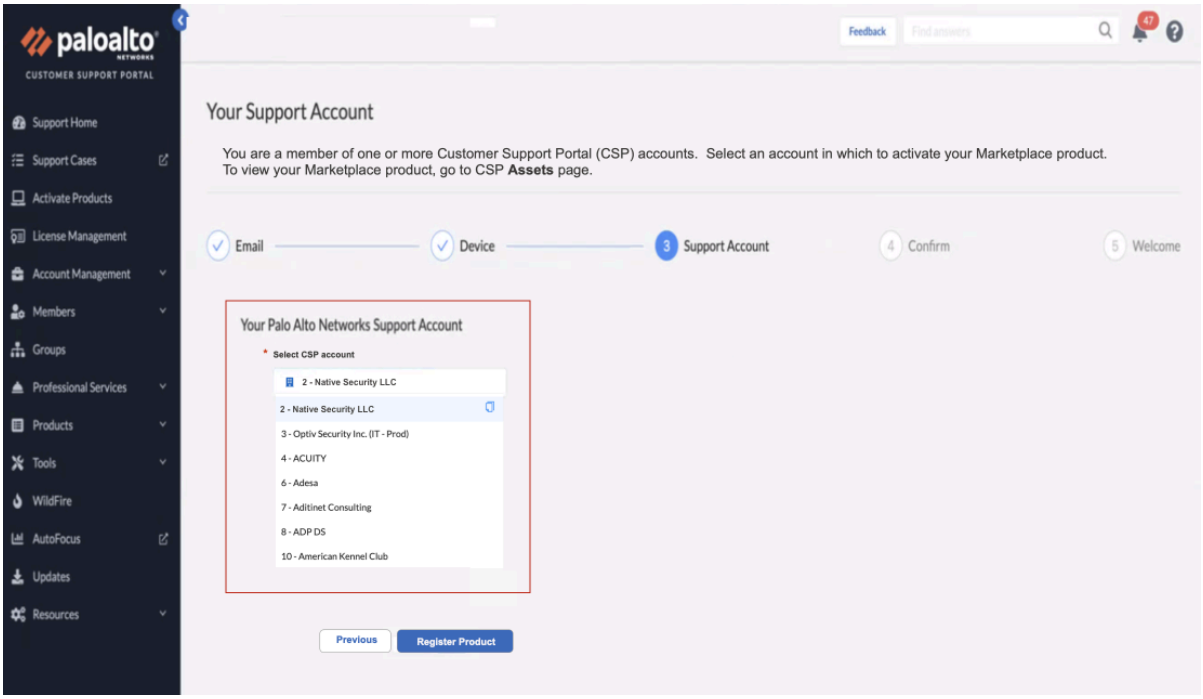
Vous pouvez utiliser le Customer Support Portal (portail de support client) pour enregistrer votre locataire Cloud NGFW.

Il vous faudra un compte pour vous connecter au CSP. Consultez Créer un compte de support client *pour en savoir plus.*

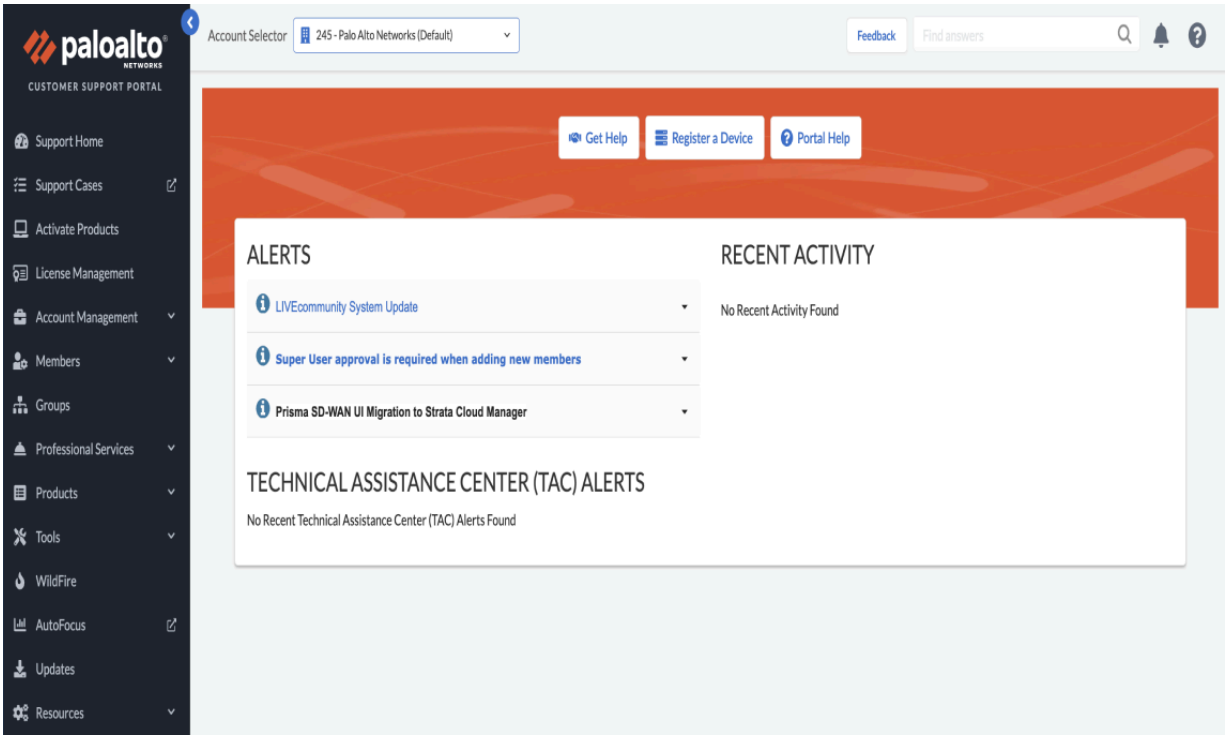
STEP 1 | Dans le Customer Support Portal (Portail de support client), saisissez vos informations d'identification de connexion, puis cliquez sur **Next (Suivant)**.



STEP 2 | La page **Your Support Account (Votre compte de support)** affiche les informations associées à vos informations d'identification de connexion. Sélectionnez le compte de support Palo Alto Networks, puis cliquez sur **Register Products (Enregistrer le produit)**.



Une fois l'enregistrement terminé, une fenêtre de confirmation s'affiche, suivie de la page du portail de support client :



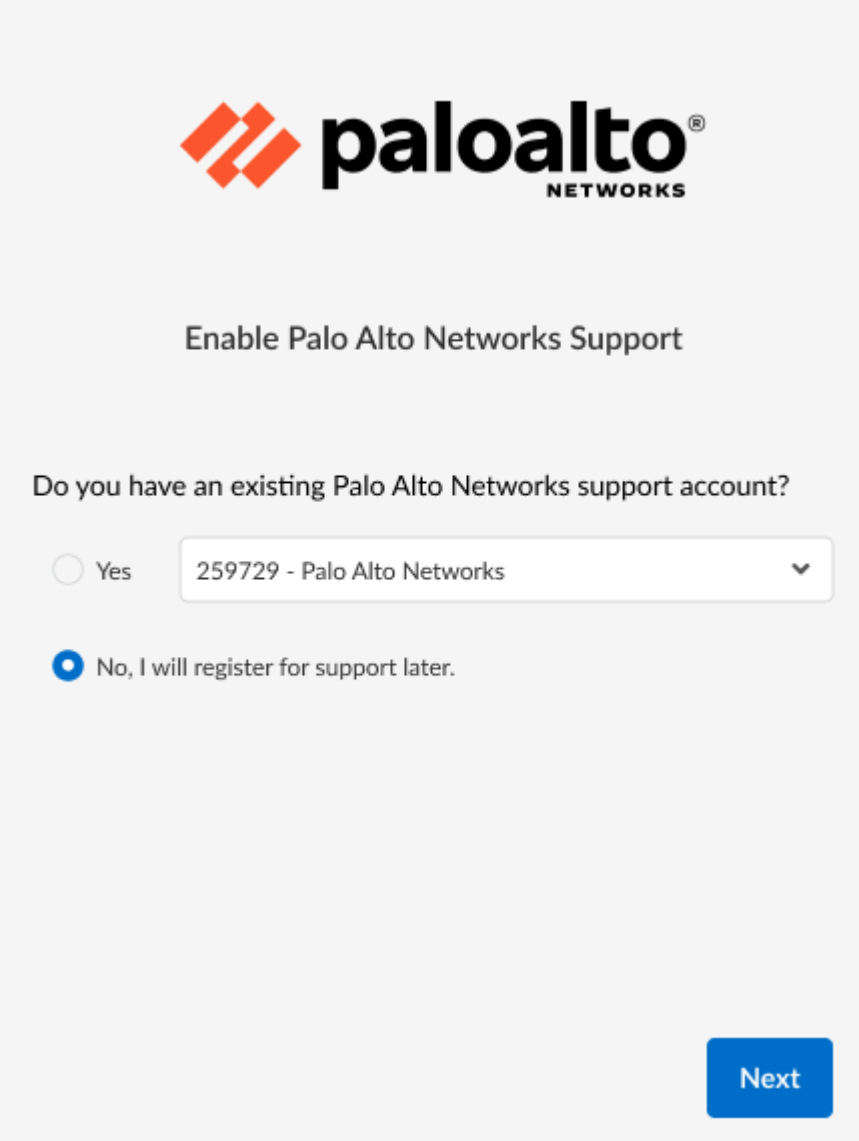
Enregistrer votre locataire Cloud NGFW sur le portail de support client à l’aide de la console Cloud NGFW

Si vous ne disposez pas d’un compte de support Palo Alto Networks existant, vous serez invité à en sécuriser un avant d’utiliser votre locataire Cloud NGFW.

STEP 1 | Connectez-vous à la ressource Cloud NGFW.

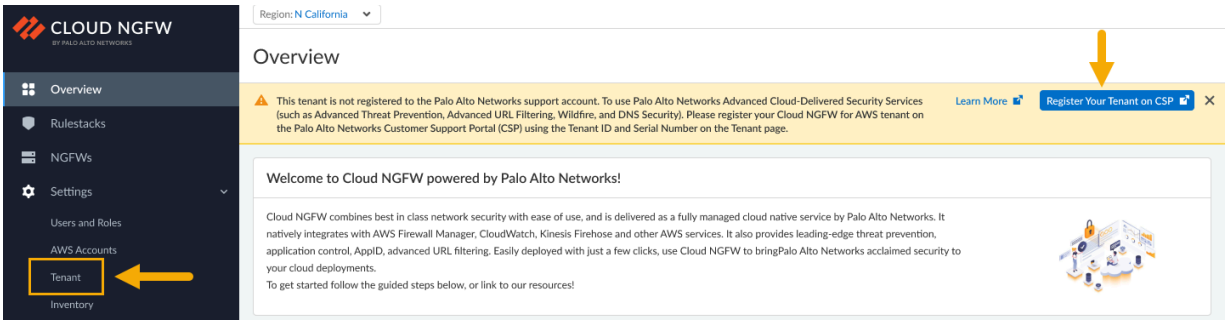
STEP 2 | Dans la page **Enable Palo Alto Networks Support (Activer le support Palo Alto Networks)**, sélectionnez **No (Non)**.

STEP 3 | Cliquez sur **Next (Suivant)**.



STEP 4 | Dans la console Cloud NGFW, cliquez sur **Register Your Tenant on CSP (Enregistrer votre locataire sur CSP)**.

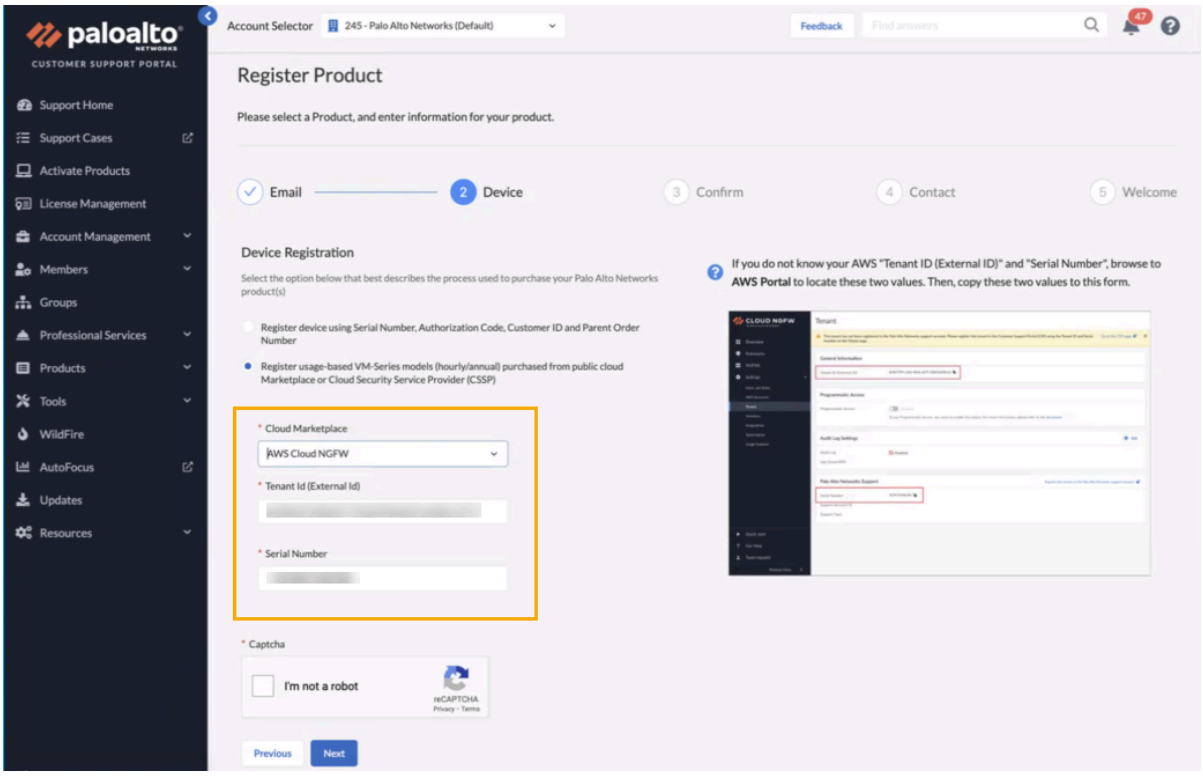
*Pour associer votre locataire Cloud NGFW à un compte sur le portail de support client, vous aurez besoin des informations d'enregistrement de votre périphérique, notamment le **Tenant ID (ID de locataire)** et le **Serial Number (Numéro de série)** de votre ressource Cloud NGFW. Ces informations sont disponibles sur la page **Tenant (Locataire)** dans la console Cloud NGFW. Voir les informations fournies sur la page* Create a Support Case (Créer un dossier de support).



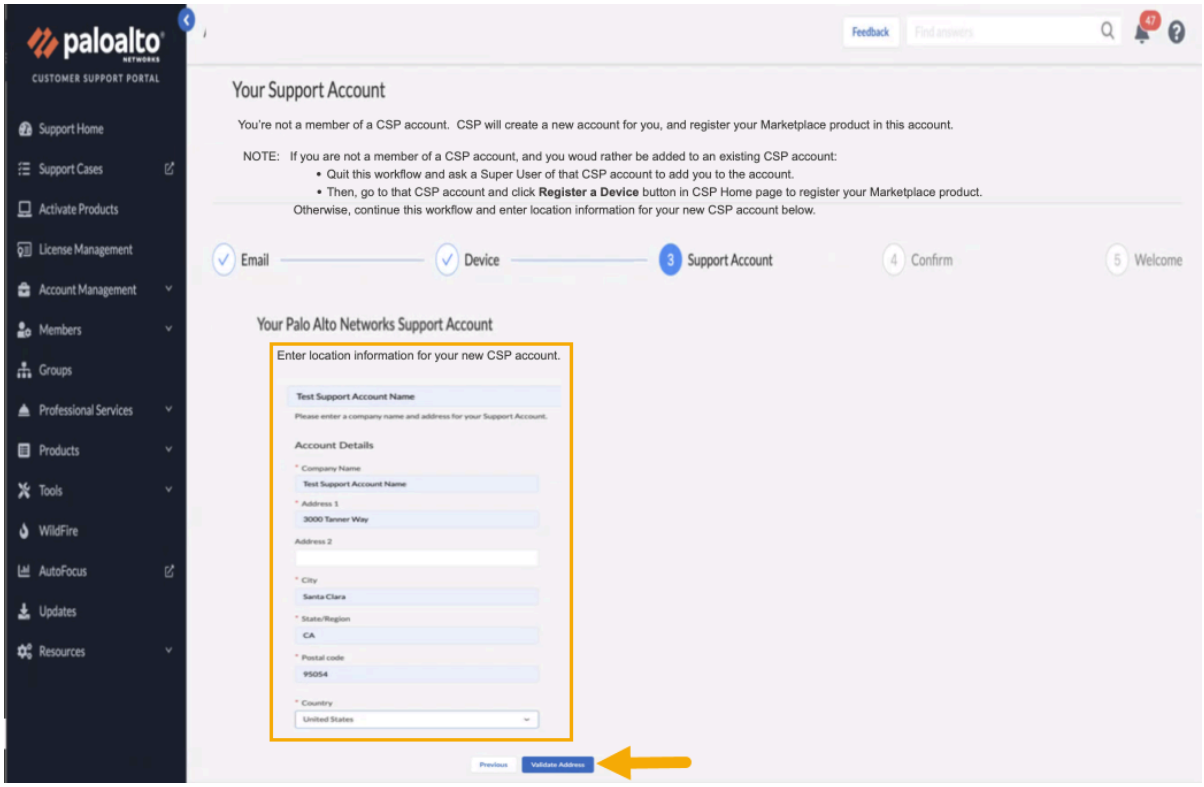
STEP 5 | Sur la page **Register Product (Enregistrer un produit)** du portail de support client, utilisez le menu déroulant pour sélectionner **AWS Cloud NGFW** pour le **Cloud Marketplace (Marketplace du cloud)**. Saisissez le **Tenant ID (ID de locataire)** et le **Serial Number (Numéro de série)** et résolvez le Captcha.

Pour rechercher l'ID de locataire et le numéro de série, consultez les informations fournies sur la page Create a Support Case (Créer un dossier de support).

STEP 6 | Cliquez sur **Next (Suivant)**.

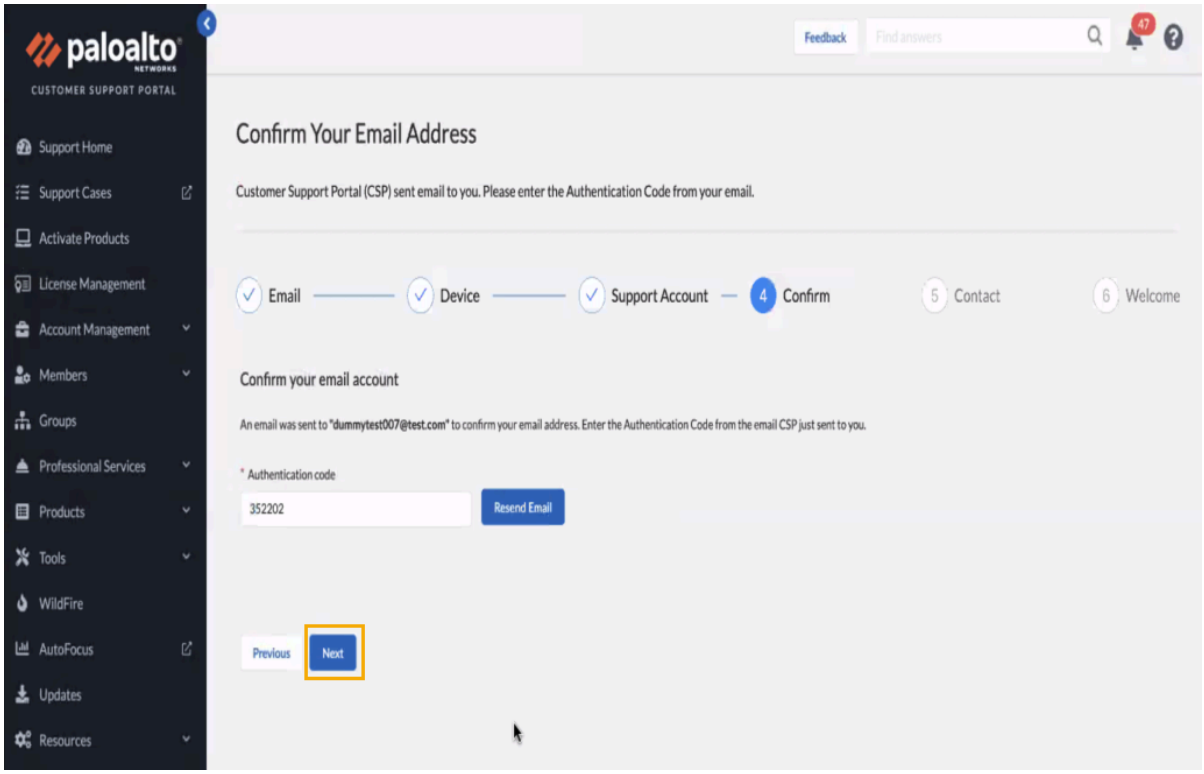


STEP 7 | Créez votre compte de support. Saisissez les **Account Details (Détails du compte)**, puis cliquez sur **Validate Address (Valider l'adresse).**



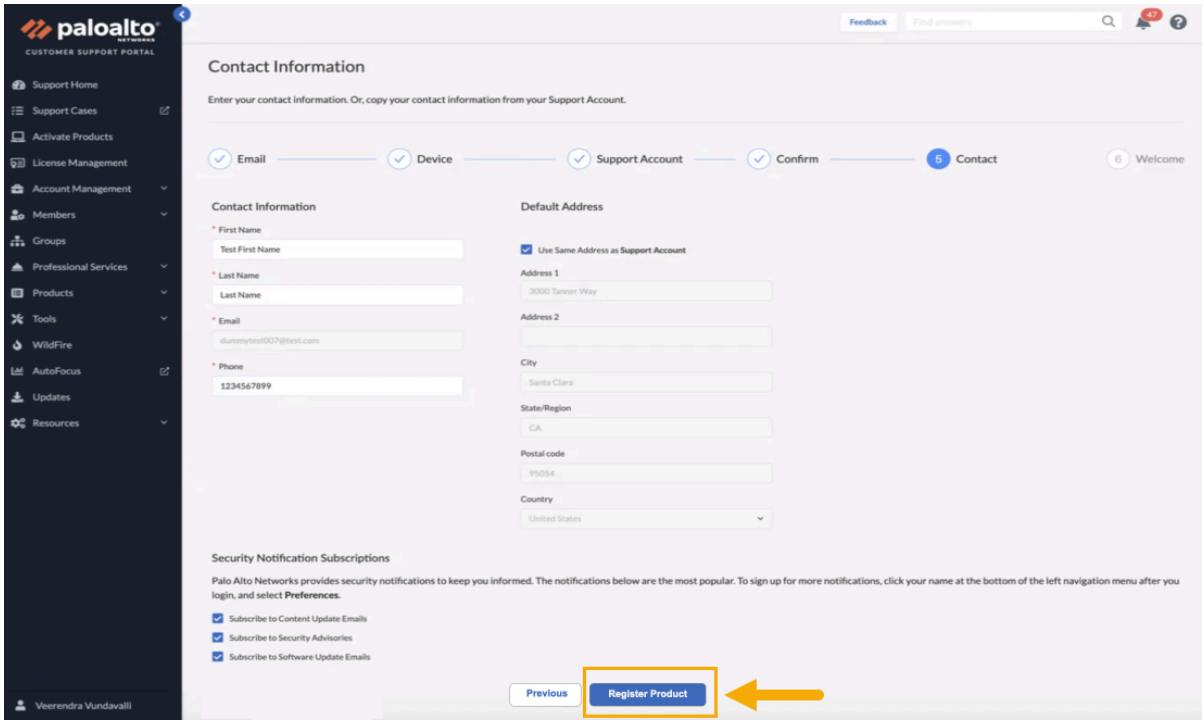
Vous serez peut-être invité à vérifier votre adresse pour le nouveau compte de support. Si nécessaire, vérifiez votre adresse et cliquez sur **OK** pour envoyer une requête d'authentification à l'adresse e-mail que vous avez indiquée.

STEP 8 | Vérifiez si vous avez un code d'authentification dans votre boîte de réception. Saisissez le **Authentification code (Code d'authentification)**, puis cliquez sur **Next (Suivant)**.

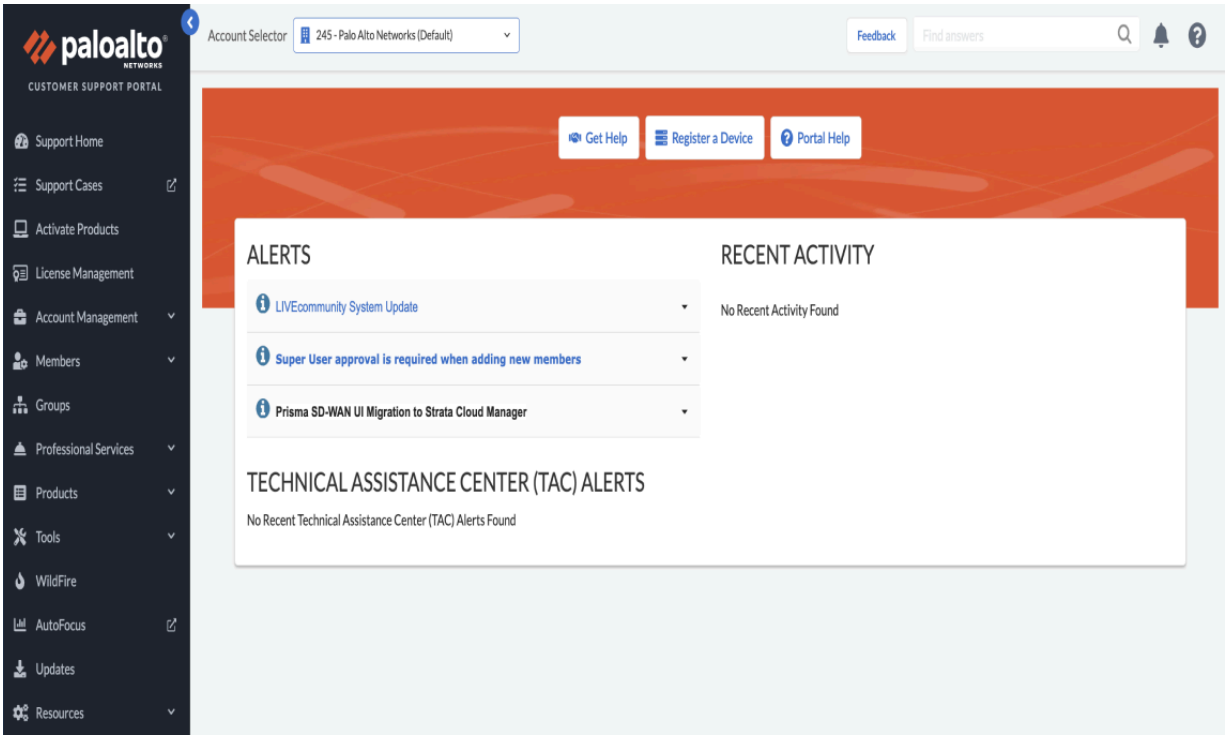


STEP 9 | Confirmez l'adresse e-mail de votre compte sur le portail de support client, puis cliquez sur **Next (Suivant)**.

STEP 10 | Vérifiez vos **Contact Information (Coordonnées)**. Sélectionnez **Security Notification Subscriptions (Abonnements aux notifications de sécurité)**, puis cliquez sur **Register Product (Enregistrer le produit)**

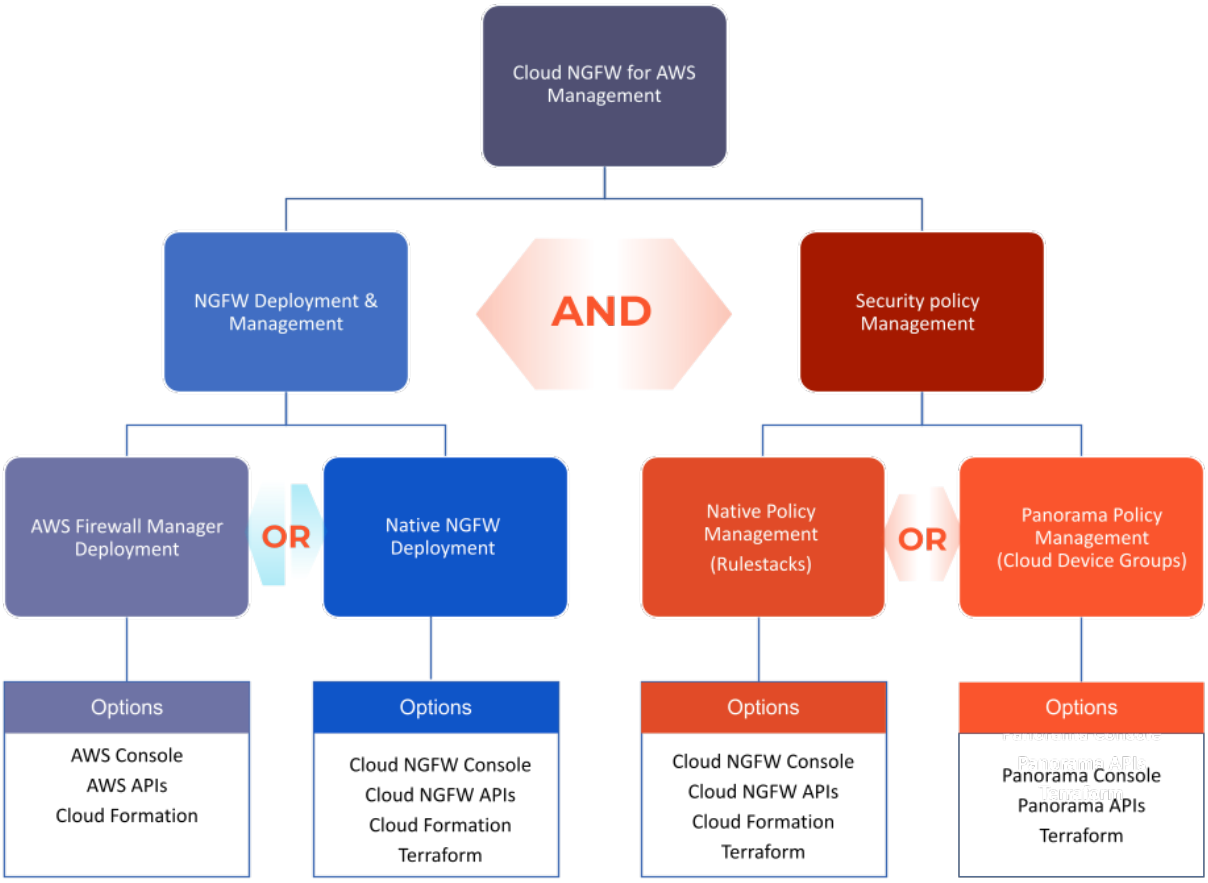


Une fois l’enregistrement terminé, une fenêtre de confirmation s’affiche, suivie de la page du portail de support client :



Travailler avec Cloud NGFW pour AWS

Cloud NGFW pour AWS propose plusieurs options de déploiement des ressources NGFW et de gestion des politiques de sécurité.



Déploiement et gestion de NGFW

- **Déploiement NGFW natif** : votre abonnement à Cloud NGFW via AWS Marketplace vous permet d'acquérir un locataire. Vous pouvez ensuite déployer des ressources Cloud NGFW pour vos VPC en quelques clics sur la console Cloud NGFW ou à l'aide des API. Ces ressources sont dotées d'une résilience, d'une capacité de mise à l'échelle et d'une gestion du cycle de vie intégrées. Vous pouvez également utiliser des outils d'infrastructure-as-code; notamment Cloud Formation ou Terraform, pour créer ces ressources. Une fois que ces ressources Cloud NGFW sont créées, vous pouvez leur créer des politiques de sécurité à l'aide de la gestion native des politiques (rulestacks) ou de la gestion des politiques Panorama (groupes d'appareils).
- **Déploiement d'AWS Firewall Manager** : si vous utilisez actuellement AWS Firewall Manager pour gérer des groupes de sécurité ou d'autres fonctionnalités de sécurité réseau dans votre organisation AWS, vous pouvez utiliser le même AWS Firewall Manager pour déployer des NGFW dans plusieurs comptes et VPC au sein d'une organisation AWS. Vous pouvez utiliser la console AWS, les API AWS ou Cloud Formation pour créer la configuration de politique de Firewall Manager qui déploie et gère tous les paramètres Cloud NGFW.

  AWS Firewall Manager gère également les sous-réseaux de terminaux, les tables de routage et les terminaux de l'équilibreur de charge de passerelle au sein du VPC où la ressource Cloud NGFW est déployée. Lorsque vous utilisez AWS Firewall Manager, la ressource Cloud NGFW utilise des rulestacks globales dans votre locataire Cloud NGFW pour les paramètres et règles de sécurité. Si vous n'avez pas encore configuré de rulestack globale dans votre locataire (à l'aide de la gestion des politiques Panorama), AWS Firewall Manager vous redirige vers la console Cloud NGFW pour créer et gérer la rulestack globale à l'aide de la gestion native des politiques.

Gestion des politiques de sécurité

- **Gestion native des politiques :**vous pouvez gérer des politiques de sécurité sur les ressources Cloud NGFW en créant des rulestacks de manière native à l'aide de la console Cloud NGFW ou des API. Vous pouvez également créer les rulestacks à l'aide d'outils d'infrastructure-as-code, notamment Cloud Formation ou Terraform. Une rulestack définit le contrôle d'accès avancé (App-ID, filtrage des URL) et le comportement de prévention des menaces du NGFW. Une rulestack inclut un ensemble de règles de sécurité ainsi que les objets et profils de sécurité associés.
- **Gestion des politiques Panorama** : vous pouvez lier votre locataire Cloud NGFW à un appareil Panorama pour créer et gérer des politiques pour vos ressources Cloud NGFW. Vous pouvez utiliser la console Panorama, les APIou Terraform pour créer ces politiques de sécurité sur les groupes d'appareils Cloud. La politique que vous créez dans le groupe d'appareils Panorama Cloud aura l'apparence d'une rulestack globale dans votre locataire Cloud NGFW.

Pour plus d'informations

- Gestion et déploiement de NGFW
- Fonctionnalités de sécurité
- Régions et zones prises en charge par Cloud NGFW pour AWS
- Déploiements Cloud NGFW pour AWS pris en charge

Gestion et déploiement de NGFW

Palo Alto Networks Cloud NGFW pour AWS prend en charge les fonctionnalités de gestion et de déploiement suivantes.

Déploiement et gestion de NGFW	Description	Déploiement natif NGFW	Déploiement d'AWS Firewall Manager
Outils	Vous disposez de plusieurs options de configuration pour déployer et gérer les ressources de Cloud NGFW.	• Console Cloud NGFW • API Cloud NGFW • Cloud Formation • Terraform	• Console AWS • API AWS • Cloud Formation
Régions AWS	Cloud NGFW pour AWS est un service AWS régional. Les Cloud NGFW que vous déployez protègent le trafic d'entrée et de sortie de votre VPC dans cette région AWS.	• 21	• 16
Architectures de déploiement	Plusieurs modèles de déploiement sont disponibles avec Cloud NGFW pour AWS. Le bon modèle dépend du cas d'utilisation et des exigences.	• Centralisé • Distribué • Combiné (ressource NGFW multi-VPC)	• Modèle centralisé • Modèle distribué

Fonctionnalités de sécurité

Palo Alto Networks Cloud NGFW pour AWS prend en charge les fonctionnalités de sécurité suivantes.

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Outils	Vous disposez de plusieurs options de configuration pour créer des politiques pour vos Cloud NGFW.	• Console Cloud NGFW • API Cloud NGFW • Cloud Formation • Terraform	• Console Panorama • API Panorama • Terraform
Types de journaux	Cloud NGFW génère des journaux horodatés qui constituent une piste d'audit pour les	• Journaux du trafic • Journaux des menaces	• Journaux du trafic • Journaux des menaces

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	événements de trafic réseau surveillé par le pare-feu. 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, Cloud NGFW génère un journal des menaces pour enregistrer le trafic correspondant à un logiciel espion, une vulnérabilité ou une signature de virus.	• Journaux de décryptage • Journaux d'audit	• Journaux de URL Filtering • Journaux de décryptage
Destinations des journaux	Cloud NGFW peut livrer les journaux générés à des destinations AWS et Cortex Data Lake.	• Compartiment Amazon Simple Storage Service (S3) • Groupe de journaux Amazon CloudWatch • Amazon Kinesis Data Firehose	• Compartiment Amazon Simple Storage Service (S3) • Groupe de journaux Amazon CloudWatch • Amazon Kinesis Data Firehose • Cortex Data Lake • Transférer les journaux de Cortex Data Lake vers un serveur Syslog • Transférer les journaux de Cortex Data Lake vers un serveur HTTPS

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Visualisation et analytique des journaux	Examinez les journaux Cloud NGFW pour vérifier un grand nombre d'informations sur votre trafic de VPC. Ces informations sont, notamment, la source, la destination, les URL, les protocoles de ports, l'App-ID, les menaces, les pays, les URL, etc.	• Explorer les journaux dans les Destinations Amazon	• Explorer les journaux dans les Destinations Amazon • Explorer tous les journaux dans Cortex Data Lake • Surveiller les journaux dans Panorama • Surveiller l'Application Command Center (Centre de commande des applications – ACC) dans Panorama
Rapports	Générez des rapports prédéfinis et personnalisés sur les applications, les menaces et les activités URL de votre trafic de VPC.	—	• Rapports planifiés et personnalisés
Capture de paquets	Pare-feu Palo Alto Networks pour effectuer une capture de paquets personnalisée ou une capture de paquets de menace.	—	—

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Politique de Sécurité	La politique de sécurité protège votre trafic de VPC contre les menaces et les	• Rulestack locale • Rulestack globale	• Politiques de sécurité • Pré-règles

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	perturbations. Les règles des politiques de sécurité individuelles déterminent si une session de trafic de VPC doit être bloquée ou autorisée en fonction des attributs du trafic, comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service.		• Post-règles • Règles par défaut
Adresse	Vous pouvez spécifier un objet d'adresse pour inclure des adresses IPv4, un FQDN ou une adresse générique (adresse IPv4 suivie d'une barre oblique et d'un masque générique).	• Listes des préfixes • Liste FQDN	• Masque réseau IPv4 • Plages IPv4 • Masquage générique IPv4 • FQDN
Groupes d'adresses	Vous pouvez regrouper des adresses sources ou de destination spécifiques qui nécessitent l'application d'une politique identique.	—	• Groupes d'adresses
Régions	Vous pouvez autoriser ou bloquer le trafic provenant (ou à destination) d'adresses IP en fonction de leur emplacement géographique tel qu'un comté. La région est disponible en option lors de la spécification de la source et de la	• Pays	• Régions prédéfinies • Régions personnalisées

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	destination de vos politiques. Vous pouvez choisir parmi une liste standard de pays ou spécifier une région/géolocalisation personnalisée avec ses adresses IP associées		
Service (port et protocole)	Vous pouvez contrôler de manière granulaire l'utilisation de sessions de trafic de VPC vers des ports spécifiques de votre réseau (en d'autres termes, vous pouvez définir le port par défaut pour l'application). Cloud NGFW contient deux services prédéfinis (service-http et service-https) qui utilisent les ports TCP 80 et 8080 pour HTTP et le port TCP 443 pour HTTPS. Vous pouvez cependant créer n'importe quel service personnalisé sur un quelconque port TCP/UDP de votre choix.	• Port et protocole	• Services
Groupes de services	Vous pouvez combiner des services ayant les mêmes paramètres de sécurité dans des groupes de services afin de réduire le nombre de règles dans la politique de sécurité.	—	• Groupes de services
Liste dynamique externe	Vous pouvez contrôler votre trafic de VPC de manière granulaire à l'aide d'une liste	• Flux de renseignement • Flux intégrés	• Listes dynamiques externes • EDL intégré

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	dynamique d'adresses IP, de domaines ou d'URL. Stocké dans un fichier hébergé sur un serveur Web externe. Palo Alto Networks propose également des EDL intégrés (adresse IP pare-balles, à risque élevé, réputée malveillante, de sortie Tor). En outre, Palo Alto Networks offre un service d'hébergement EDL gratuit qui maintient la liste toujours dynamique des adresses IP pour Microsoft 365, Azure, Amazon Web Services (AWS) et Google Cloud Platform (GCP). Vous pouvez utiliser ces EDL pour contrôler votre trafic d'entrée et de sortie de VPC.	• Flux de services d'hébergement EDL	• Listes de services d'hébergement EDL
Applications	Vous pouvez contrôler votre trafic de VPC de manière granulaire en utilisant le système de classification de trafic App-ID™ de Palo Alto Networks qui s'appuie sur les signatures d'applications pour identifier avec précision les applications de votre réseau.	• APP-ID	• APP-ID • Signatures d'applications propres à l'entreprise
Groupe d'applications	Vous pouvez regrouper un ensemble d'App-ID qui nécessitent la	—	• Groupes d'application

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	même application de politique.		
Filtres de l'application	Vous pouvez contrôler votre trafic de VPC de manière granulaire en définissant un filtre d'application qui regroupe les App-ID actuels et les App-ID futurs correspondant à certains attributs. Par exemple, vous pouvez procéder à la création d'un filtre d'application selon un ou plusieurs attributs (catégorie, sous-catégorie, technologie, risque, caractéristiques). Désormais, chaque fois qu'un nouvel App-ID est introduit dans Cloud NGFW sur la base d'une mise à jour de contenu, toutes les nouvelles applications correspondant aux critères du filtre sont automatiquement ajoutées à votre ensemble.	—	• Filtres de l'application
Contrôle prioritaire sur l'application	Vous pouvez configurer Cloud NGFW de manière à disposer d'un contrôle prioritaire sur l'identification d'application (App-ID) normale du trafic spécifique transitant par le pare-feu. Dès que la politique de contrôle prioritaire sur l'application	—	• Contrôle prioritaire sur l'application

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	entre en vigueur, toutes les inspections supplémentaires d'App-ID du trafic sont arrêtées et la session est identifiée avec les signatures d'application propre à l'entreprise que vous fournissez.		
Étiquettes	Les étiquettes vous permettent de regrouper des objets à l'aide de mots-clés ou d'expressions. Vous pouvez appliquer des étiquettes à des objets d'adresse, à des groupes d'adresses (statiques et dynamiques), à des applications, à des zones, à des services, à des groupes de services et à des règles de politique.	—	• Étiquettes
Groupe d'utilisateurs dynamiques	Vous permet de créer une liste d'utilisateurs à partir de la base de données locale ou d'une base de données externe et de les regrouper.	—	—
Périphériques	Egalement connu sous le nom de Dictionnaire des périphériques, cette page contient les métadonnées des objets de périphériques.	—	—

Certificats et décryptage	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d’appareils cloud)
Gestion des certificats	Cloud NGFW utilise des certificats pour accéder à un flux intelligent et pour activer le décryptage entrant et sortant. Chaque certificat contient une clé cryptographique pour crypter un texte brut ou décrypter un texte crypté. Chaque certificat contient également une signature numérique pour authentifier l'identité de l'émetteur.	• Certificats TLS/SSL dans AWS Secrets Manager	• Certificats CA racine auto-signés • Importation d'un certificat et d'une clé privée • Certificats TLS/SSL dans AWS Secrets Manager • Générer des certificats • Obtenir un certificat auprès d’une CA externe • Répondeur Online Certificate Status Protocol (protocole de vérification des certificats en ligne, OCSP) • CA de confiance par défaut • Profil du certificat
Déchiffrement	Cloud NGFW peut décrypter, inspecter et recrypter votre trafic d’entrée et de sortie de VPC en tant que décision basée sur une politique. Vous pouvez contrôler de manière granulaire le trafic de VPC à décrypter et celui à ne pas décrypter, ainsi que le type de décryptage SSL que vous souhaitez effectuer sur le trafic indiqué.. Pour activer le décryptage, vous configurez les certificats requis pour agir en tant que tiers	• Décryptage SSL sortant • Inspection SSL entrante	• Politique de décryptage • Profil de décryptage • Proxy de transfert SSL (décryptage sortant) • Inspection SSL entrante • Proxy SSH • Vérification des certificats du serveur • Exclusion du décryptage

Certificats et décryptage	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	de confiance d'une session.		• Désactivation temporaire du décryptage SSL

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Protection contre les vulnérabilités IPS	La protection contre les vulnérabilités protège contre les menaces entrantes, dans lesquelles un attaquant tente d'exploiter la vulnérabilité d'un système pour violer votre réseau, Les vulnérabilités du système peuvent être des dépassements de tampon, une exécution de code illégale, etc.	• Meilleures pratiques	• Profil par défaut • Profil strict • Profil personnalisé (exceptions de menaces) • Signatures personnalisées des vulnérabilités • Signatures Snort/ Suricata
Logiciel anti-espion	Le logiciel antispyware détecte et bloque les menaces sortantes, en particulier les activités de commande et de contrôle (C2), initiées par des charges de travail infectées par un logiciel malveillant (cyberattaque exploitée) dans votre VPC AWS. Vous pouvez également définir des modèles d'expressions régulières personnalisés pour identifier les communications des logiciels espions aux téléphones fixes.	• Meilleures pratiques	• Profil par défaut • Profil strict • Profil personnalisé (exceptions de menaces) • Signatures personnalisées de logiciels espions • Signatures Snort/ Suricata

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Blocage des fichiers	Le blocage de fichiers vous permet de contrôler de manière granulaire les types de fichiers de votre trafic de VPC dans une direction spécifiée (entrant/sortant/les deux). Vous pouvez bloquer de façon proactive les fichiers réputés porter des menaces ou qui n'ont pas de cas d'utilisation réel pour le chargement et le téléchargement.	• Meilleures pratiques et personnalisations	• Profil de base • Profil strict • Profil personnalisé
Antivirus	L'antivirus détecte et protège contre les logiciels malveillants dissimulés dans des fichiers compressés, des exécutables, des fichiers PDF et des virus HTML et JavaScript dans votre trafic de VPC	• Meilleures pratiques	• Profil # par défaut • Profil personnalisé (exceptions de menaces)
Analyse WildFire	Cloud NGFW détecte et transfère des fichiers et des exécutables de votre trafic de VPC vers le service cloud WildFire™ pour analyse, et effectue également une analyse ML en ligne de certains fichiers. Si une menace est détectée sur les fichiers, WildFire crée des protections pour bloquer les logiciels malveillants et distribue une protection contre cette menace à l'échelle	—	—

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	mondiale en moins de cinq minutes.		
Filtrage d'URL	Le filtrage des URL analyse le trafic de VPC et contrôle les URL accédées par vos charges de travail de VPC (trafic en clair et crypté) en effectuant une analyse en ligne et en comparant avec les catégories d'URL gérées par Palo Alto Networks ou les catégories personnalisées que vous fournissez.	• Contrôle d'accès pour les catégories d'URL gérées par Palo Alto Networks • Catégories d'URL personnalisées	• Contrôle d'accès pour les catégories d'URL gérées par Palo Alto Networks et les catégories d'URL personnalisées • Catégorisation en ligne dans le cloud
Sécurité DNS	La sécurité DNS protège les requêtes DNS sortantes de vos VPC contre les menaces telles que la tunnellisation DNS, la détection des algorithmes de génération de domaine (DGA), les domaines de logiciels malveillants, etc.	—	• Sécurisez votre déploiement contre les menaces basées sur DNS
Filtrage des données et DLP d'entreprise	Le filtrage des données détecte les informations sensibles dans votre trafic de VPC, telles que les numéros de carte de crédit ou de sécurité sociale ou les documents internes de l'entreprise, et empêche ces données de quitter votre environnement AWS.	—	• Modèles prédéfinis, expressions régulières et propriétés de fichiers DLP d'entreprise NON pris en charge à l'heure actuelle

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	Avec le DLP d'entreprise, vous bénéficiez d'un filtrage avancé des données sur votre trafic de VPC grâce à une liste prédéfinie de modèles de données avec une analytique basée sur le cloud.		
Groupes de profils de sécurité	Un groupe de profils de sécurité est un ensemble de profils de sécurité qui peut être traité comme une unité puis facilement ajouté à des politiques de sécurité.	—	• Groupes de profils de sécurité

Zones de sécurité et protection	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
Zones de sécurité	Les zones de sécurité représentent un moyen logique de regrouper des interfaces sur le pare-feu, et des terminaux Cloud NGFW pour contrôler et journaliser le trafic de VPC.	—	—
protection de zones	La protection de zones défend les zones de sécurité réseau contre les attaques par saturation, les tentatives de reconnaissance et les attaques basées sur les paquets.	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
XFF	Le trafic vers vos charges de travail de VPC peut être passé par plus d'un serveur proxy (tel que CDN ou ALB) avant d'atteindre le Cloud NGFW. S'il y a un en-tête XFF existant, ces proxys lui ajoutent son adresse IP ou l'ajoutent avec son adresse IP. Par conséquent, l'en-tête de requête XFF peut contenir plusieurs adresses IP séparées par des virgules. Le Cloud NGFW utilise le champ d'en-tête HTTP X-Forwarded-For (XFF) qui identifie l'adresse IP d'origine du client. Le Cloud NGFW utilise toujours la dernière adresse ajoutée dans l'en-tête XFF pour appliquer la politique.	• Support des en-têtes XFF dans les politiques • Afficher les valeurs XFF dans les journaux	• Utiliser les valeurs XFF dans la politique • Afficher les valeurs XFF dans les journaux • Afficher les valeurs XFF dans les rapports
NAT	Les pare-feu Palo Alto Networks peuvent imposer le NAT de destination sur votre trafic de VPC entrant et le NAT source sur votre trafic de VPC sortant.	—	—
Proxy DNS	Lorsque vous configurez Cloud NGFW en tant que proxy DNS, il agit comme un intermédiaire entre les clients et les	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	serveurs, et comme un serveur DNS en résolvant les requêtes du cache DNS ou en transférant les requêtes à d'autres serveurs DNS. Cette page vous permet de configurer les paramètres qui déterminent comment le pare-feu sert de proxy DNS.		
Gestion d'interface	Les pare-feu Palo Alto Networks vous permettent de configurer des VLAN, des câbles virtuels Link Layer Discovery Protocol (protocole de découverte de la couche de liaison – LLDP), Bidirectional Forwarding Detection (détection de transfert bidirectionnel – BFD) sur leurs interfaces	—	—
QoS	Les pare-feu Palo Alto Networks vous permettent de spécifier le trafic nécessitant un traitement préférentiel ou une limitation de bande passante. Les règles QoS vous permettent d'exécuter de manière fiable les applications et le trafic à priorité élevée avec une capacité réseau limitée.	—	—
Gestion du routage	Les pare-feu Palo Alto Networks vous permettent	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	de configurer un routage statique et des protocoles de routage (BGP, BFD, OSPF, OSPFv3, multicast, RIPv2 et des filtres).		
Gestion de tunnels IPSec	Les pare-feu Palo Alto Networks résilient les tunnels IPSec et inspectent le trafic tunnellisé	—	—
Gestion de GlobalProtect	Les firewalls Palo Alto Networks sécurisent les mains-d'œuvre mobiles en spécifiant des algorithmes d'authentification et de cryptage dans des tunnels VPN entre un module de passerelle GlobalProtect et le client.	—	—
Gestion de tunnel GRE	Les pare-feu Palo Alto Networks résilient les tunnels d'encapsulation générique de routage (Generic Routing Encapsulation – GRE) et inspectent le trafic tunnellisé.	—	—
Gestion des liens SD-WAN	Les pare-feu Palo Alto Networks lient plusieurs connexions WAN (ADSL/DSL, modem câble, Ethernet, fibre, LTE/3G/4G/5G, MPLS, micro-ondes/ radio, satellite, Wi-Fi) à une interface virtuelle et prennent en charge la sélection dynamique et intelligente des	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	chemins d'accès en fonction des applications et des services et des conditions des liaisons que chaque application ou service est autorisé à utiliser.		
Transfert basé sur une politique	Les règles de transfert basé sur les politiques des pare-feu Palo Alto Networks permettent au trafic d'emprunter un chemin alternatif pour des raisons de sécurité ou de performances. Supposons que votre entreprise dispose de deux liaisons entre le siège social et la succursale : une liaison Internet bon marché et une ligne louée plus coûteuse. Afin de renforcer la sécurité, vous pouvez utiliser le transfert basé sur une politique pour envoyer des applications qui ne sont pas du trafic crypté, notamment du trafic FTP, sur la ligne privée louée et tout autre trafic sur la liaison Internet. Sinon, afin d'améliorer les performances, vous pouvez choisir d'acheminer les applications essentielles sur la ligne louée et d'envoyer tout autre trafic, tel que la navigation Web,	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)
	sur la liaison meilleur marché.		

Régions et zones prises en charge par Cloud NGFW pour AWS

Palo Alto Networks Cloud NGFW pour AWS prend en charge les régions suivantes.

Nom de la région	Indicatif régional	ID de zone	AWS Firewall Mana	Registre AWS CloudFormation
USA Ouest (Californie du Nord)	us-west-1	usw1-az1 usw1-az3	✓	✓
USA Ouest (Oregon)	us-west-2	usw2-az1 usw2-az2 usw2-az3	✓	✓
USA Est (Virginie du Nord)	us-east-1	use1-az1 use1-az2 use1-az4 use1-az5 use1-az6	✓	✓
USA Est (Ohio)	us-east-2	use2-az1 use2-az2 use2-az3	✓	✓
Canada (Centre)	ca-central-1	cac1-az1 cac1-az2 cac1-az4	✓	✓
Europe (Irlande)	eu-west-1	euw1-az1 euw1-az2 euw1-az3	✓	✓
Europe (Londres)	eu-west-2	euw2-az1 euw2-az2	✓	✓

Nom de la région	Indicatif régional	ID de zone	AWS Firewall Mana	Registre AWS CloudFormation
		euw2-az3		
Europe (Paris)	eu-west-3	euw3-az1 euw3-az2 euw3-az3	✓	✓
Europe (Francfort)	eu-central-1	euc1-az1 euc1-az2 euc1-az3	✓	✓
Europe (Stockholm)	eu-north-1	eun1-az1 eun1-az2 eun1-az3	✓	✓
Europe (Milan)	eu-south-1	eus1-az1 eus1-az2 eus1-az3	—	—
Asie-Pacifique (Osaka)	ap-northeast-3	apse1-az1 apse1-az2 apse1-az3	✓	✓
Asie-Pacifique (Singapour)	ap-southeast-1	apse1-az1 apse1-az2 apse1-az3	✓	✓
Asie-Pacifique (Sydney)	ap-southeast-2	apse2-az1 apse2-az2 apse2-az3	✓	✓
Asie-Pacifique (Tokyo)	ap-northeast-1	apne1-az1 apne1-az2 apne1-az4	✓	✓
Asie-Pacifique (Séoul)	ap-northeast-2	apne2-az1 apne2-az2 apne2-az3	✓	✓

Nom de la région	Indicatif régional	ID de zone	AWS Firewall Mana	Registre AWS CloudFormation
Asie-Pacifique (Osaka)	ap-northeast-3	apne3-az1 apne3-az2 apne3-az3	—	—
Asie-Pacifique (Mumbai)	ap-south-1	aps1-az1 aps1-az2 aps1-az3	✓	✓
Asie-Pacifique (Hong Kong)	ap-east-1	ape1-az1 ape1-az2 ape1-az3	—	—
Amérique du Sud (São Paulo)	sa-east-1	sae1-az1 sae1-az2 sae1-az3	✓	✓
Moyen-Orient (Bahreïn)	me-south-1	mes-az1 mes-az2 mes-az3	—	—
Afrique (Le Cap)	af-south-1	afs-az1 afs-az2 afs-az3	—	—

Déploiements Cloud NGFW pour AWS pris en charge

Vous pouvez déployer Cloud NGFW dans un modèle centralisé derrière une passerelle de transit (TGW) avec une ressource Cloud NGFW déployée dans un VPC de sécurité dédié ou dans un modèle distribué, avec une ressource Cloud NGFW associée à chaque VPC.

Déploiement centralisé

Dans un déploiement centralisé, un VPC de sécurité dédié fournit une approche centralisée de la gestion du contrôle d'accès et de la prévention des menaces du trafic entrant, sortant et est-ouest de vos VPC. Vous devez spécifier le VPC de sécurité et le(s) sous-réseau(x) lors de la configuration de Cloud NGFW. Les terminaux NGFW sont créés et déployés dans le VPC et les sous-réseaux spécifiés. Vous devez ensuite configurer les règles de routage sur les VPC d'application et TGW pour rediriger le trafic vers le VPC de sécurité pour inspection, ainsi que les règles de routage pour le trafic de retour.

Pour plus d’informations et des exemples de déploiements centralisés, consultez Déploiements centralisés Cloud NGFW pour AWS.

Déploiement distribué

Le modèle de déploiement distribué permet la distribution de pare-feu Cloud NGFW sur plusieurs VPC, tout en maintenant un contrôle de sécurité centralisé. Dans ce modèle, il est recommandé d’utiliser AWS Firewall Manager pour créer une politique Firewall Manager qui facilite le déploiement des NGFW sur plusieurs comptes AWS d’une organisation AWS. Vous êtes ensuite dirigé vers la console Cloud NGFW pour créer des rulestacks globales et les associer à la politique Firewall Manager. Firewall Manager appelle ensuite les API Cloud NGFW pour créer la NGFW avec les rulestacks globales associées qui protègent vos VPC d’application. En outre, AWS Firewall Manager utilise les API AWS VPC pour créer des terminaux NGFW dans les VPC que vous spécifiez.

Pour plus d’informations et des exemples de déploiements centralisés, consultez Déploiements distribués Cloud NGFW pour AWS.

Tarification de Cloud NGFW pour AWS

Modèle de tarification à l’utilisation

Cloud NGFW est disponible sous la forme d'un abonnement à l’utilisation (PAYG) sur AWS Marketplace. Avec ce modèle, vous ne payez que ce que vous utilisez chaque mois, avec tous les frais regroupés sur la facture que vous recevez d'AWS. Vous pouvez également profiter des avantages d’AWS Marketplace tels que la facturation consolidée du programme de réduction d’entreprise (EDP) d’Amazon Web Services.

Pour plus d’informations, consultez Relier votre compte PAYG aux crédits Cloud NGFW.

Vous payez un tarif horaire pour chaque ressource Cloud NGFW. Vous payez également la quantité de trafic, facturée au gigaoctet, traitée par la ressource NGFW. De plus, vous payez un taux horaire et la quantité de trafic traité par votre ressource Cloud NGFW lorsque vous configurez des extensions de services de sécurité (notamment la prévention des menaces, le filtrage avancé des URL, la sécurité DNS ou WildFire) ou le module complémentaire de gestion centralisée. (Gestion de Panorama). Le tarif facturé pour le trafic dépend également du trafic agrégé traité par tous les NGFW du locataire au cours du mois (appelé *tarification du trafic par niveaux*).

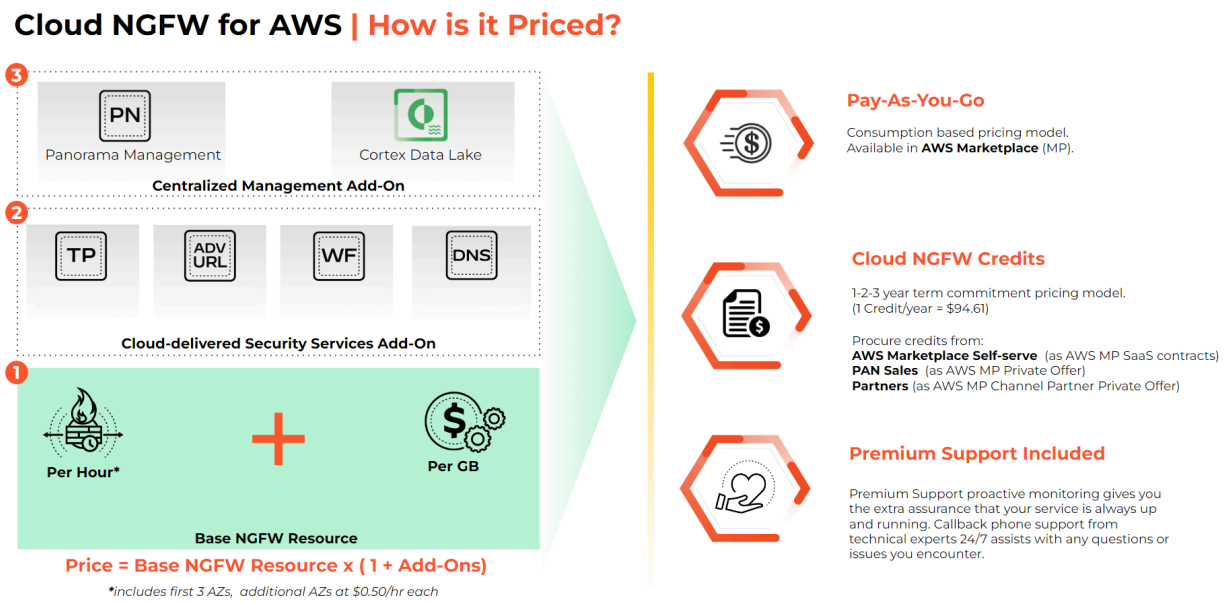
Modèle de tarification des crédits

Vous pouvez acquérir et associer des crédits Cloud NGFW pour AWS à votre locataire en payant un coût initial pour un contrat à long terme d’un, de deux ou de trois ans. Vous pouvez vous procurer ces crédits directement depuis AWS Marketplace (contrats SaaS AWS) ou à un prix privé auprès de Palo Alto Networks (offre privée AWS) ou de ses partenaires (offre privée de partenaire consultant AWS). Vous achetez ces crédits tout en profitant des avantages d’AWS Marketplace tels que la facturation consolidée, AWS EDP et les renouvellements automatisés ou configurables. Les crédits Cloud NGFW vous permettent de consommer des ressources Cloud NGFW dans votre locataire à moindre coût dans les limites d’une capacité spécifique jusqu’à l’expiration de votre contrat. Consulter S'abonner à Cloud NGFW pour AWS pour apprendre à ajouter des crédits de contrat.

Si votre consommation moyenne mensuelle dépasse les crédits achetés, les dépassements sont facturés aux tarifs PAYG.

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

*Utilisez l’*estimateur de tarification Cloud NGFW pour AWS *pour vous aider à déterminer la tarification AWS pour votre locataire Cloud NGFW.*



Mesure et facturation

La consommation de Cloud NGFW se traduit par une tarification horaire à l'utilisation ou par des crédits Cloud NGFW, comme décrit dans les tableaux ci-dessous.

Consommation de ressources de base NGFW

Vous payez un tarif horaire pour chaque ressource Cloud NGFW. Vous payez également la quantité de trafic, facturée au gigaoctet, traitée par la ressource NGFW.

Ressource de base NGFW		Prix (par heure)	Prix (par Go)	Crédits Cloud NGFW équivalents
Heure d'utilisation	Jusqu'à 3 AZ	1,50 $		125,0
	Chaque AZ supplémentaire	0,50 $		41,7
Trafic sécurisé	Premiers 15 To/mois		0,065 $	5,4
	15 To/mois suivants		0,045 $	3,7
	Au-dessus de 30 To/mois		0,030 $	2,5

Les heures d'utilisation sont mesurées sur chaque ressource NGFW que vous déployez. Le trafic est mesuré sur toutes les ressources NGFW déployées dans votre locataire Cloud NGFW.

Consommation de l'extension des services de sécurité fournis par le cloud (CDSS)

La consommation de l’extension de vos services de sécurité est mesurée sur chaque ressource NGFW pour chaque heure pendant laquelle vous avez activé le module complémentaire et pour la quantité de trafic traitée par ce NGFW, lorsque vous l’avez configuré. Le tarif facturé pour le trafic dépend également du trafic agrégé traité par tous les NGFW du locataire au cours du mois (appelé *tarification du trafic par niveaux*).

Extension de prévention des menaces		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heure d’utilisation*	Jusqu’à 3 AZ	0,300 $		25,0
	Chaque AZ supplémentaire	$ 0,100		8.3
Trafic sécurisé	Premiers 15 To/mois		0,013 $	1,1
	15 To/mois suivants		0,009 $	0,7
	Au-dessus de 30 To/mois		0,006 $	0,5

Extension de prévention avancée des menaces		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heure d’utilisation*	Jusqu’à 3 AZ	0,450 $		0,8
	Chaque AZ supplémentaire	0,150 $		0,3
Trafic sécurisé	15 premiers To/mois		0,020 $	1,7
	15 To/mois suivants		0,014 $	1,2
	Au-dessus de 30 To/mois		0,009 $	0,7

Module complémentaire de sécurité DNS		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heure d’utilisation*	Jusqu’à 3 AZ	0,300 $		25,0
	Chaque AZ supplémentaire	0,100 $		8,3

Trafic sécurisé	Premiers 15 To/mois		0,013 $	1,1
	15 To/mois suivants		0,009 $	0,7
	Au-dessus de 30 To/ mois		0,006 $	0,5

Extension WildFire		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heure d’utilisation*	Jusqu’à 3 AZ	0,300 $		25,0
	Chaque AZ supplémentaire	0,100 $		8.3
Trafic sécurisé	Premiers 15 To/mois		0,013 $	1,1
	15 To/mois suivants		0,009 $	0,7
	Au-dessus de 30 To/ mois		0,006 $	0,5

Extension de filtrage avancé des URL		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heure d’utilisation*	Jusqu’à 3 AZ	0,450 $		37,5
	Chaque AZ supplémentaire	0,150 $		12,5
Trafic sécurisé	Premiers 15 To/mois		0,020 $	1,7
	15 To/mois suivants		0,014 $	1,2
	Au-dessus de 30 To/ mois		0,009 $	0,7

Extension DLP		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heures d’utilisation*	Jusqu’à 3 AZ	0,600 $		50,0

	Chaque AZ supplémentaire	0,200 $		16,7
Trafic sécurisé	Premiers 15 To/mois		0,026 $	2,2
	15 To/mois suivants		0,018 $	1,5
	Au-dessus de 30 To/mois		0,012 $	1,0

**Les heures d'utilisation sont mesurées sur chaque ressource NGFW avec l'extension CDSS activée.*

Consommation de l'extension de gestion centralisée

Vous pouvez utiliser un appareil virtuel Panorama pour gérer les règles de politique dans votre locataire Cloud NGFW. Dans ce cas, la consommation de votre extension de gestion centralisée est mesurée sur chaque ressource NGFW pour chaque heure que vous avez associée à un appareil Panorama et pour la quantité de trafic traitée par ce NGFW, lorsque vous l'avez configuré. Le tarif qui vous est facturé pour le trafic dépend également du trafic agrégé traité par tous les NGFW du locataire au cours du mois (appelé *tarification du trafic par niveaux*).

Vous ne payez pour les licences de périphériques supplémentaires pour la gestion des règles de politique dans les ressources Cloud NGFW. Panorama ne compte pas ces ressources NGFW dans le nombre de ses licences de périphériques gérés.

Cloud NGFW envoie les journaux au même locataire de lac de données Cortex Data Lake actuellement associé à votre Panorama. Vous ne payez pas pour le stockage supplémentaire dans le lac de données Cortex Data Lake. Lorsqu'il est utilisé avec Cloud NGFW pour AWS, le lac de données Cortex Data Lake évolue automatiquement avec les ressources Cloud NGFW pour AWS. À mesure que le débit du trafic augmente sur ces ressources Cloud NGFW, votre stockage CDL disponible augmente également, de sorte que vous n'avez pas à vous préoccuper des ajustements manuels du stockage du lac de données Cortex Data Lake pour enregistrer vos données de journal.

Extension de gestion centralisée de Palo Alto Networks		**Prix (par heure)**	**Prix (par Go)**	**Crédits Cloud NGFW équivalents**
Heures d'utilisation	Jusqu'à 3 AZ	0,300 $		25,0
	Chaque AZ supplémentaire	0,100 $		8,3
Trafic sécurisé	Premiers 15 To/mois		0,013 $	1,1
	15 To/mois suivants		0,009 $	0,7

	Au-dessus de 30 To/ mois		0,006 $	0,5

Les heures d'utilisation sont mesurée sur chaque ressource NGFW associée à un appareil virtuel Panorama.

Mécanisme de mesure AWS Marketplace

Cloud NGFW utilise le modèle de tarification d'abonnement Saas AWS en traduisant la consommation du locataire en **unités** pour plusieurs dimensions **personnalisées** et en la signalant à AWS Marketplace comme indiqué dans le tableau ci-dessous. Ce mécanisme offre la flexibilité d'agréger toute la consommation de votre locataire en fonction de quelques dimensions. Ces dimensions incluent les heures de déploiement de tous les NGFW, la quantité de trafic qu'ils sécurisent et le nombre de fonctionnalités de sécurité qu'ils utilisent toutes les heures. Cloud NGFW traduit la consommation des services de sécurité et de la gestion centralisée en crédits Cloud NGFW et les rapporte sous forme d'unités d'extensions au service de mesure d'AWS.

AWS Marketplace	**Prix de l'abonnement Saas de Cloud NGFW**
Heures d'utilisation de base de NGFW	1,5 $/unité
(1 unité = 1 heure d'utilisation) jusqu'à 3 AZ	
(0,333 unité = 1 heure d'utilisation) pour les AZ supplémentaires	
Trafic sécurisé > Premiers 15 To/mois	0,065 $/unité
(1 unité = 1 Go sécurisé)	
Trafic sécurisé > 15 To/mois suivants	0,045 $/unité
(1 unité = 1 Go sécurisé)	
Trafic sécurisé > Au-dessus de 30 To/mois	0,030 $/unité
(1 unité = 1 Go sécurisé)	
Extensions	0,012 $/unité
(1 unité = 1 crédit Cloud NGFW)	
Reportez-vous aux tableaux des extensions ci-dessus.	

Relier votre compte PAYG aux crédits Cloud NGFW

Trois scénarios peuvent être envisagés pour l’intégration de crédits dans votre abonnement Cloud NGFW pour AWS :

- Vous avez accepté votre contrat, mais vous ne disposez pas d’un abonnement de paiement à l’utilisation (PAYG).
- Vous disposez d’un abonnement PAYG existant et avez accepté un nouveau contrat de crédit sur le même compte AWS Marketplace.
- Vous disposez d’un abonnement PAYG existant et avez accepté un nouveau contrat de crédit en utilisant un autre compte AWS. Dans ce scénario, vous devez relier vos comptes.

  Les informations contenues dans les sections suivantes décrivent les actions adaptées à chaque scénario.

Palo Alto Networks envoie un e-mail contenant les informations relatives au contrat de crédit Cloud NGFW que vous pouvez utiliser pour votre ressource Cloud NGFW. Cet e-mail contient des informations sur la création d’un locataire pour votre abonnement Cloud NGFW. Il fournit des informations sur votre abonnement, notamment le nombre de crédits alloués, le numéro de série de votre compte, des dates de début et de fin et l’ID de votre offre.

Dear Customer,

Please create your tenant by:

1. Going to AWS Marketplace
2. Following the steps in this documentation

Details are as follows:

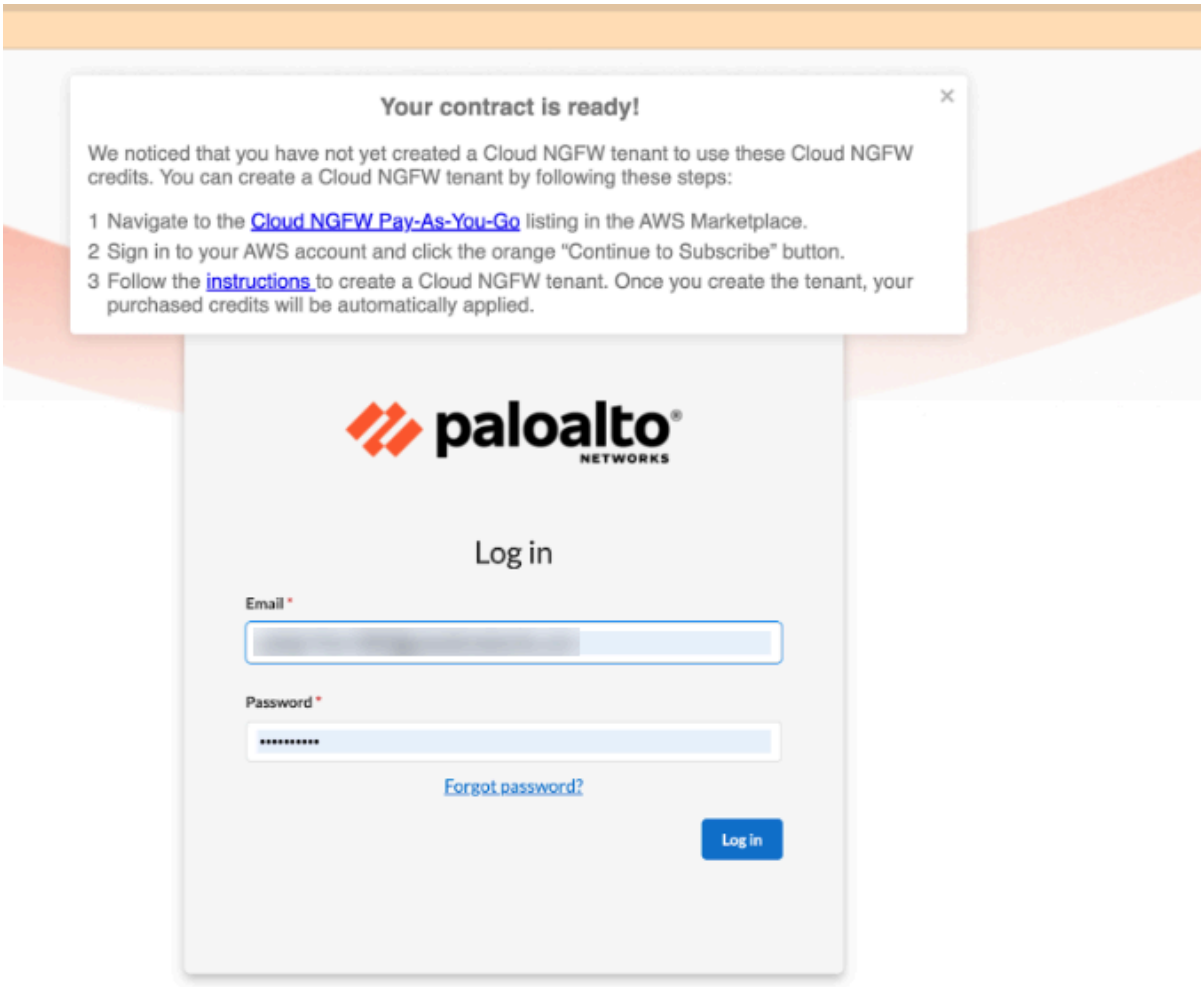
- Credits - {{CREDITS_NUM}}
- Serial Number - {{SERIAL_NUM}}
- Start Date - {{START_DATE}}
- End Date - {{END_DATE}}
- Offer ID - {{OFFER_ID}}

For further help, please navigate to the Cloud NGFW Live Community Page where you can search the documentation, knowledge base and community. Please do not hesitate to contact us if you need any assistance or have any questions.

Contrat de crédit accepté sans existence d’abonnement PAYG

Vous avez accepté votre contrat, mais vous n’avez pas d’abonnement PAYG.

STEP 1 | Si aucun abonnement PAYG n'existe, le message suivant s'affiche sur l'écran de connexion Cloud NGFW :



STEP 2 | Connectez-vous à la console AWS avec les informations d'identification de connexion que vous utilisez pour AWS Marketplace.

STEP 3 | Découvrez des produits en accédant à l'option **Cloud Next Generation Firewall (PAYG with 30-Day Free Trial) (Pare-feu Cloud nouvelle génération (PAYG avec essai gratuit de 30 jours))**.

STEP 4 | Cliquez sur **S'abonner**.

STEP 5 | Cliquez sur **Configurer le produit**.

STEP 6 | Suivez les étapes pour configurer PAYG pour votre compte.

Vos crédits sont automatiquement appliqués après la configuration de PAYG.

Un abonnement PAYG existe et vous avez accepté un contrat de crédit sur le même compte AWS

Vous disposez d'un abonnement PAYG existant et avez accepté un nouveau contrat de crédit sur le même compte AWS Marketplace.

STEP 1 | Connectez-vous à la console AWS avec les informations d'identification de connexion que vous utilisez pour AWS Marketplace.

STEP 2 | Accédez à **Cloud NGFW for AWS (Cloud NGFW pour AWS)** dans AWS Marketplace.

STEP 3 | Cliquez sur **S'abonner**.

STEP 4 | Cliquez sur **Set up product (Configurer le produit)** pour l'option **Palo Alto Networks Cloud NGFW for AWS Credits (Palo Alto Networks Cloud NGFW pour les crédits AWS)** ; utilisez les informations d'identification de connexion de votre compte AWS existantes.

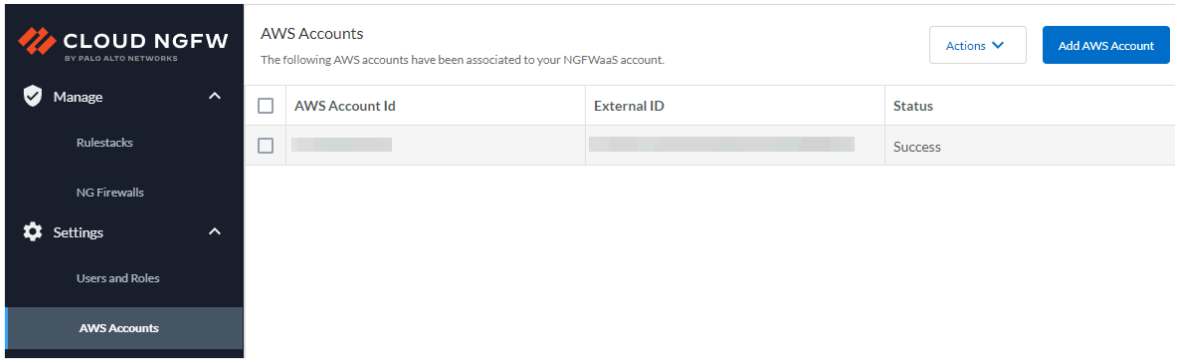
STEP 5 | Suivez les étapes pour configurer PAYG pour votre compte.

Vos crédits Cloud NGFW s'affichent après la connexion.

Un abonnement PAYG existe et vous avez accepté un contrat de crédit sur un autre compte AWS

Vous avez un abonnement PAYG existant et avez accepté un nouveau contrat de crédit en utilisant un autre compte AWS. Dans ce scénario, vous devez relier vos comptes.

STEP 1 | Dans la console Cloud NGFW, ajoutez un compte supplémentaire pour prendre en charge le nouveau contrat de crédit. Sélectionnez **Settings (Paramètres) > Accounts (Comptes) > Add AWS Account (Ajouter un compte AWS).**



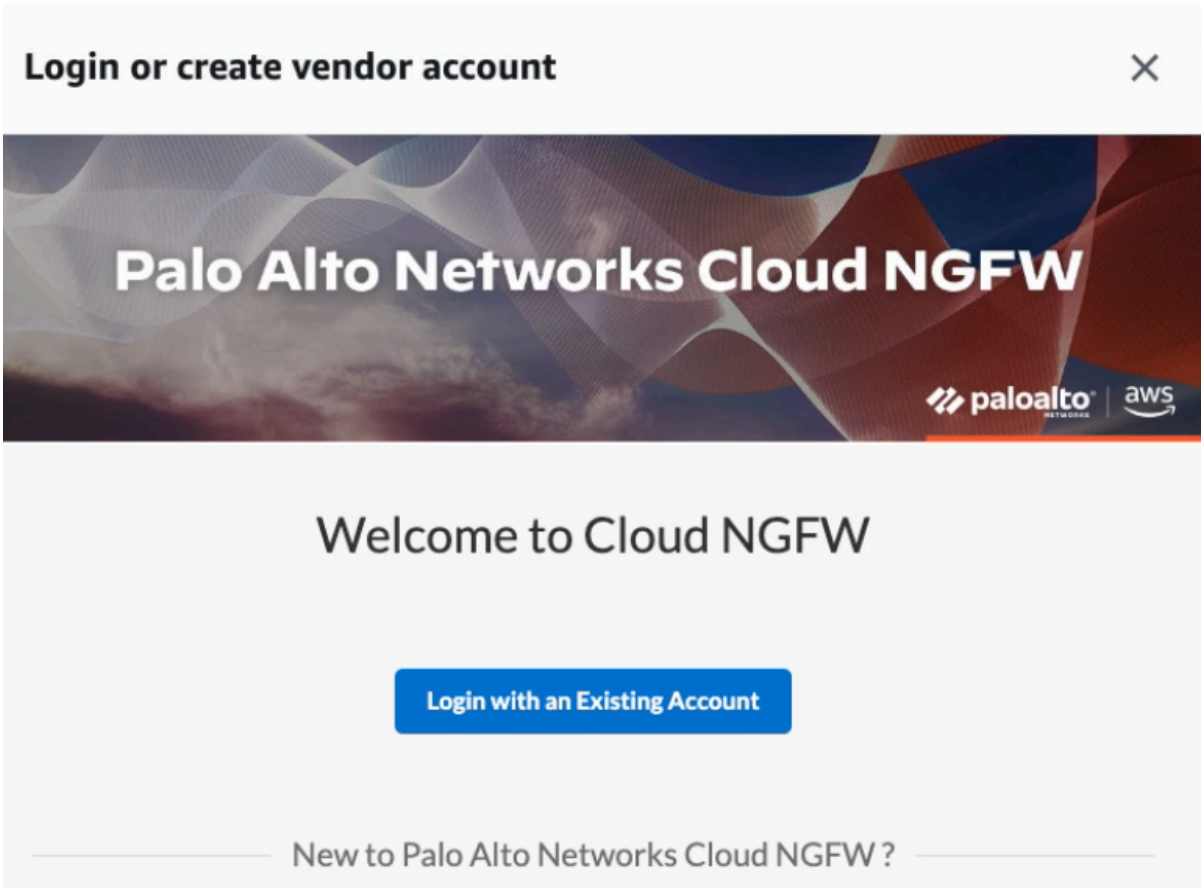
STEP 2 | Abonnez-vous à PAYG pour le nouveau compte que vous avez ajouté sur la console Cloud NGFW :

1. Connectez-vous à la console AWS.

STEP 3 | Accédez à **Cloud NGFW for AWS (Cloud NGFW pour AWS)** dans AWS Marketplace.

STEP 4 | Cliquez sur **Configurer le produit**.

STEP 5 | Sélectionnez **Login with Existing Account (Connexion avec un compte existant)**



Vos crédits Cloud NGFW s’affichent après la connexion.

*Ne créez pas de nouveaux locataires pendant la configuration du compte. Assurez-vous de sélectionner **Login with Existing Accounts (Connexion avec des comptes existants)**.*

Essai gratuit de Cloud NGFW pour AWS

Lorsque vous vous abonnez au Cloud NGFW via AWS Marketplace, vous êtes automatiquement inscrit pour un essai gratuit. Accédez à la page **Subscription Management (Gestion des abonnements)** pour valider que votre locataire Cloud NGFW est lié à la liste d'abonnement AWS Marketplace **Palo Alto Networks Cloud NGFW Pay-As-You-Go** et que votre essai gratuit est actif avec des crédits.

Pour activer cet essai gratuit, le Cloud NGFW associe les crédits d'essai gratuits à votre locataire nouvellement créé. Ces crédits vous permettent de créer jusqu'à deux pare-feu sécurisant jusqu'à 100 Go de trafic. Vous pouvez :

- intégrer vos comptes AWS à vos locataires ;
- créer jusqu'à deux ressources NGFW sur vos VPC AWS ;
- créer des rulestacks.

Lorsque la période d'essai gratuite se termine, vous commencez à payer pour la consommation. Vous pouvez accéder à la page **Subscription Management (Gestion des abonnements)** pour vérifier que votre locataire Cloud NGFW est toujours lié à la liste d'abonnement AWS Marketplace **Palo Alto Networks Cloud NGFW Pay-As-You-Go** et que votre période d'essai gratuite n'est plus active. Notez bien :

- Vous ne pouvez pas interrompre la période d'essai gratuite.
- À la fin de votre période d'essai gratuite, vous commencez à payer des frais lorsque vous utilisez le Cloud NGFW.

Limites et quotas de Cloud NGFW pour AWS

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

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

Gestion des politiques de rulestacks locales

Nom	Limites par défaut par client Cloud NGFW
Nombre de comptes Cloud (AWS) dans un locataire	200
Ressources Cloud NGFW dans un locataire	50 par compte et par région
Terminaux Cloud NGFW dans un locataire	50 par compte et par région
Terminaux Cloud NGFW pour chaque ressource NGFW	50
Rulestacks globales en suspens non associées aux ressources NGFW	10
Rulestacks locales en suspens non associées aux ressources NGFW	10

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

Attribut	Limite maximale par ressource Cloud NGFW
Flux intelligents (notamment les cinq flux prédéfinis)	30
Adresses IP dans tous les flux	50 000
Objets de certificats	100

Gestion des politiques de Panorama

Attribut	Limite maximale par ressource Cloud NGFW*
Politique	
Règles de sécurité	6 000
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 maximum 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

Attribut	Limite maximale par ressource Cloud NGFW*
Filtrage d'URL	
Total des 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.

S'abonner à Cloud NGFW pour AWS

Effectuez les étapes suivantes pour vous abonner au service Cloud NGFW. Vous pouvez souscrire à un abonnement Cloud NGFW de paiement à l'utilisation (PAYG) SaaS.

Cette procédure lance le processus de création de votre premier utilisateur, un administrateur de locataire. Un administrateur de locataire est le niveau d'utilisateur le plus élevé du service Cloud NGFW. Il offre la possibilité d'ajouter des comptes AWS au service Cloud NGFW et d'intégrer des utilisateurs supplémentaires.

Vous devez créer un abonnement Cloud NGFW PAYG SaaS avant de pouvoir souscrire à un contrat de crédits Cloud NGFW pour AWS.

- Abonnement Cloud NGFW PAYG SaaS
- Sécuriser votre accès actuel au Cloud NGFW à l'aide de SSO et de la MFA
- Ajouter des crédits Cloud NGFW pour AWS à votre locataire
- Utilisateur multilocataire d'un utilisateur unique pris en charge sur plusieurs locataires
- Ajouter plusieurs comptes AWS
- Ajouter un modèle CloudFormation manuellement

Abonnement Cloud NGFW PAYG SaaS

Avant de vous abonner à Cloud NGFW pour AWS et de déployer le service dans votre environnement AWS, vous devez prendre en compte et créer les éléments suivants. Au cours du processus d'abonnement, il vous sera demandé de définir les paramètres décrits ci-dessous dans un modèle CloudFormation (CFT) pour terminer la configuration initiale.

- **Configuration des terminaux** (obligatoire) : le rôle IAM entre comptes inclut des autorisations qui permettent à Cloud NGFW de lire les informations sur les ressources VPC, qui sont requises pour la configuration des terminaux NGFW.
- **Création des terminaux** (facultatif) : vous pouvez configurer Cloud NGFW pour créer et gérer des terminaux NGFW dans votre environnement AWS. En sélectionnant **Yes (Oui)**, vous accordez à Cloud NGFW les autorisations nécessaires pour créer et gérer les terminaux nécessaires dans vos VPC. Si vous sélectionnez **No (Non)**, vous devez Créer et afficher des terminaux NGFW manuellement.
- **Autorisations pour la journalisation** (facultatif) : Cloud NGFW vous permet d'envoyer des journaux de trafic, de menaces et de décryptage à un compartiment S3, un groupe de journaux Cloudwatch ou Kinesis Data Firehose. Pour que Cloud NGFW envoie ces journaux à la destination prévue, vous devez fournir les autorisations nécessaires.

  La console Cloud NGFW vous redirige vers la console AWS CloudFormation et vous invite à créer une pile. Cette pile configure les rôles IAM entre comptes, désigne (mais ne crée pas) les destinations de journalisation et permet à Cloud NGFW d'accéder aux certificats dans Secrets Manager de votre compte AWS pour le décryptage.

  La pile préremplit les destinations de journalisation pour le groupe de journaux CloudWatch et le flux de diffusion Kinesis Data Firehose avec une destination appelée **PaloAltoCloudNGFW**. Le champ de compartiment S3 n'est pas prérempli. Si vous souhaitez envoyer les journaux vers une autre destination,

vous devez créer cette destination et remplacer la valeur par défaut par le nom avant de terminer la création de la pile.

Pour une destination de journal de compartiment S3, vous devez fournir le nom du compartiment de destination.

Si vous utilisez un Kinesis Data Firehose, la source de ce flux de diffusion doit exécuter une instruction **PUT directe**.

- **Journalisation d'audit** (facultatif) : vous pouvez envoyer des journaux d'audit, qui suivent l'activité de l'administrateur, à un groupe de journaux Cloudwatch. La pile CFT inclut une destination de groupe de journaux Cloudwatch par défaut appelée **PaloAltoCloudNGFWAuditLog**. Vous pouvez créer un groupe Cloudwatch Log avec la valeur de nom par défaut ou remplacer la valeur par défaut par le nom d'un autre groupe Cloudwatch Log.
- **Autorisations de décryptage** (facultatif) : pour utiliser Cloud NGFW afin d'inspecter les flux de trafic cryptés, vous devez autoriser Cloud NGFW à récupérer le certificat nécessaire auprès d'AWS Secrets Manager. Vous devez activer Cloud NGFW pour utiliser le contrôle d'accès basé sur les attributs en spécifiant une étiquette lorsque vous lancez la pile CFT.

  Par défaut, le CFT inclut l’étiquette **PaloAltoCloudNGFW**. Vous pouvez modifier cette étiquette en configurant l'ARN dans le service et en remplaçant la valeur par défaut dans le CFT.

Suivez cette procédure pour vous abonner avec un abonnement Cloud NGFW PAYG SaaS.

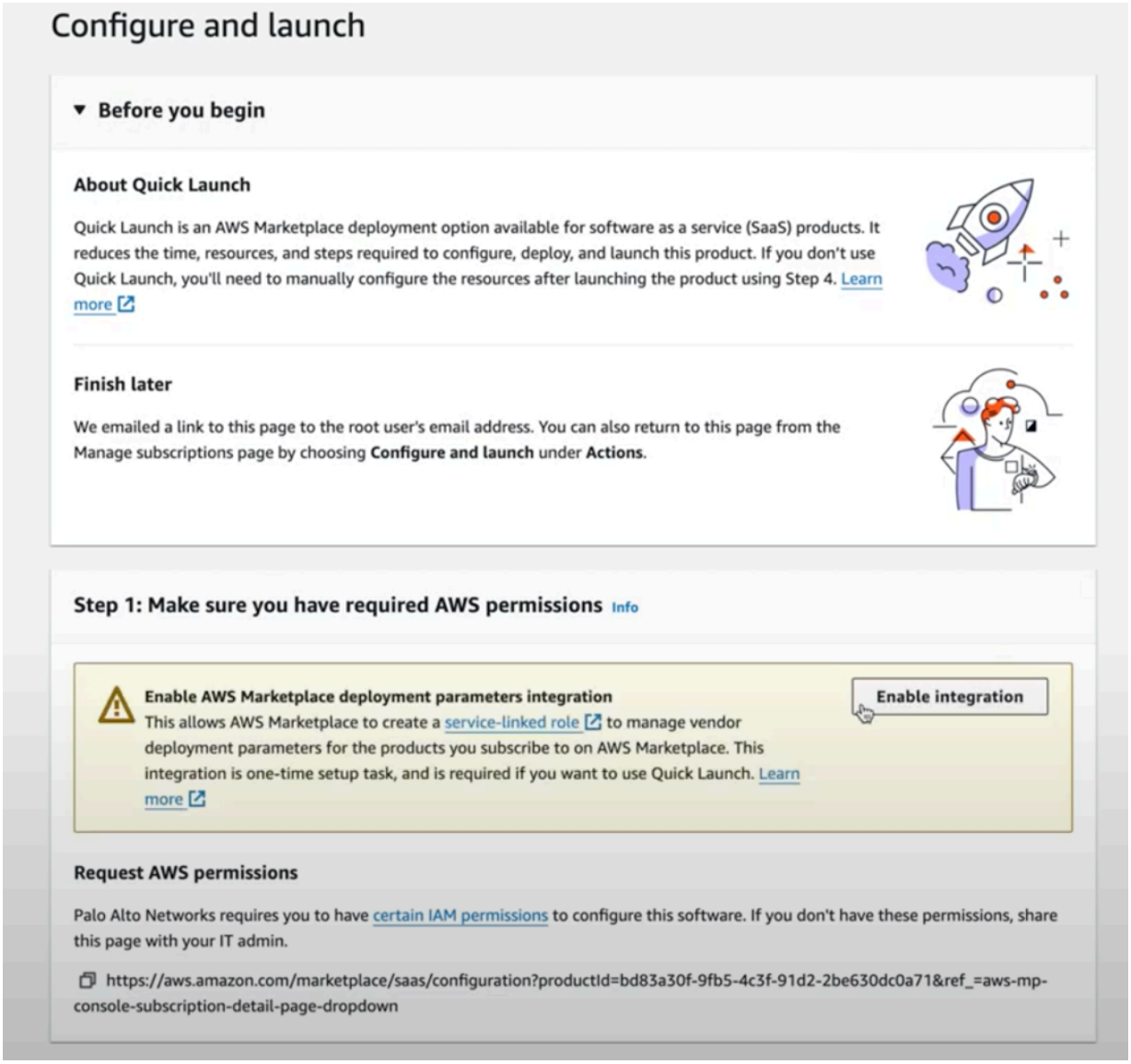
STEP 1 | Connectez-vous à la console AWS.

STEP 2 | Accédez à Cloud NGFW pour AWS dans AWS Marketplace.

STEP 3 | Cliquez sur **S'abonner**.

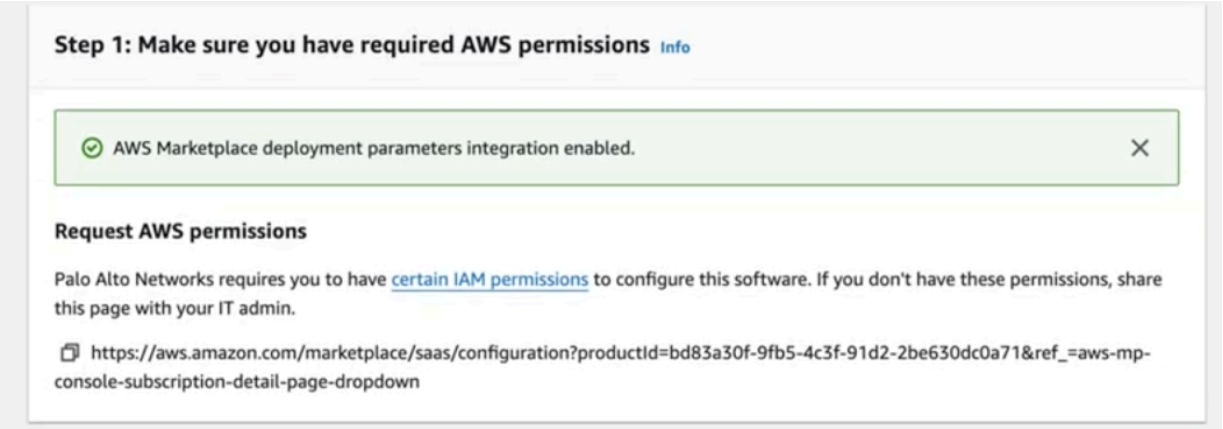
STEP 4 | Cliquez sur **Configurer le produit**. Cela lance la fonction la page Configurer et lancer (Lancement rapide de SaaS) sur AWS Marketplace. Palo Alto Networks a activé le lancement rapide sur ses

produits Cloud NGFW, et vous pouvez désormais créer et déployer un nouveau locataire à l’aide du lancement rapide.

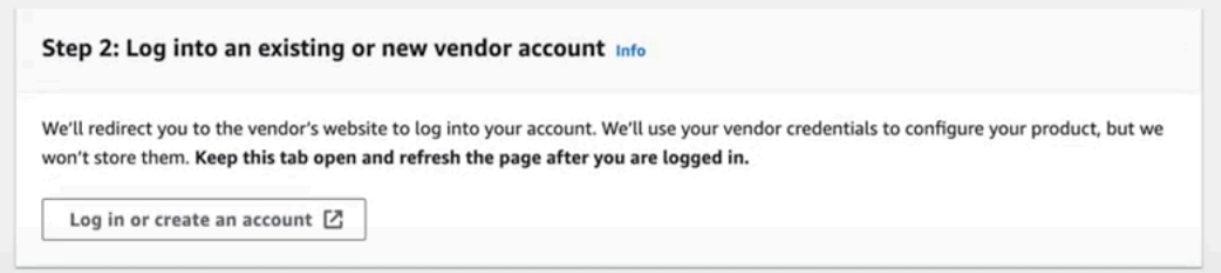


STEP 5 | Cliquez sur **Enable integration (Activer l’intégration)** sur la page Configurer et lancer du lancement rapide afin de vous assurer de disposer des autorisations IAM requises d’AWS.

Si vous êtes un nouvel utilisateur, le bouton Activer l’intégration s’affiche automatiquement à l’étape 1 de la page Configure and Launch (Configurer et lancer).



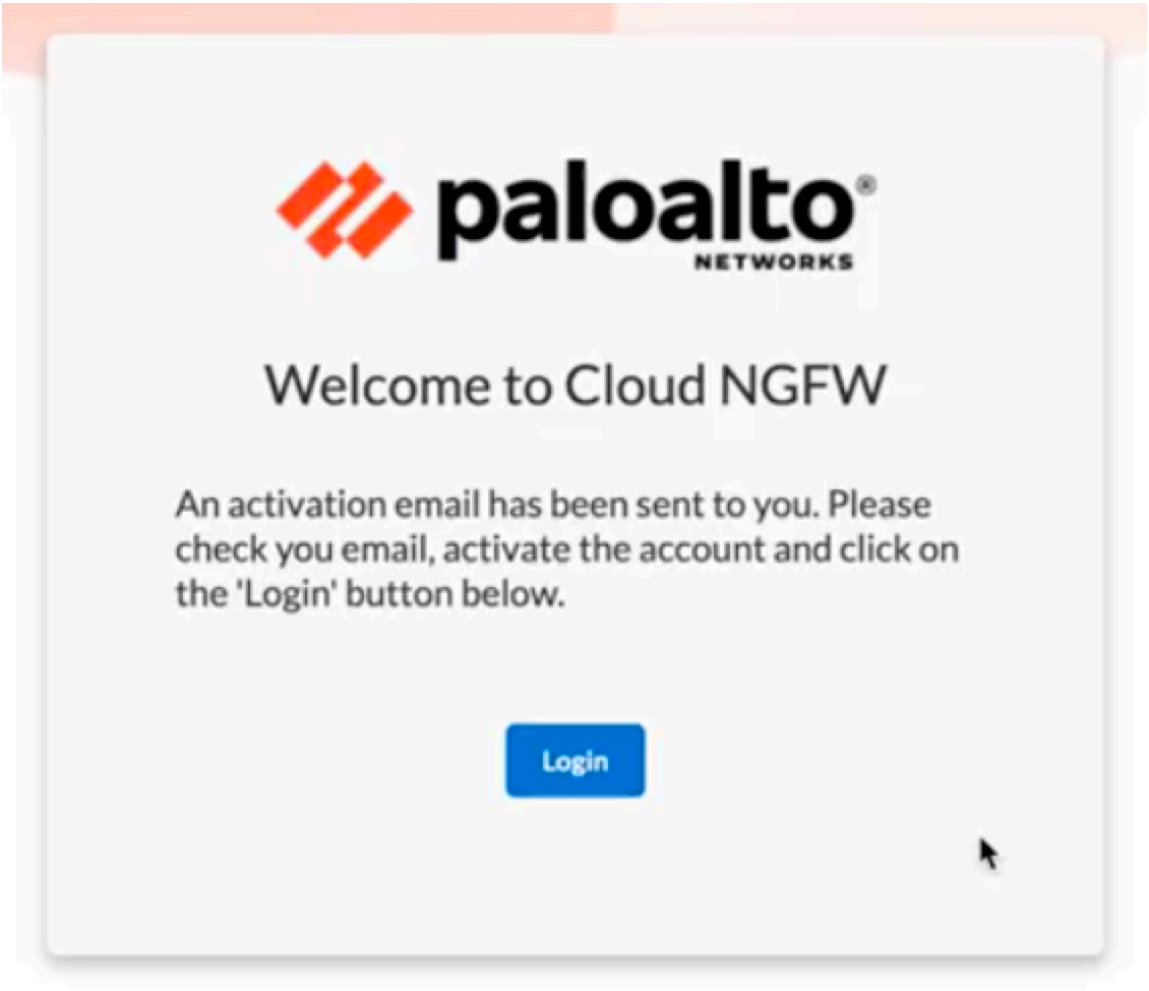
STEP 6 | Cliquez sur le bouton **Login or create an account (Se connecter ou créer un compte)** pour vous connecter à un compte existant ou en créer un nouveau sur le site Web du fournisseur. Cela vous amène à une page d'enregistrement de création de locataire du Cloud NGFW pour le locataire AWS.



1. Si vous êtes un ***nouvel utilisateur***, vous devrez créer un compte Cloud NGFW. Entrez votre adresse e-mail.

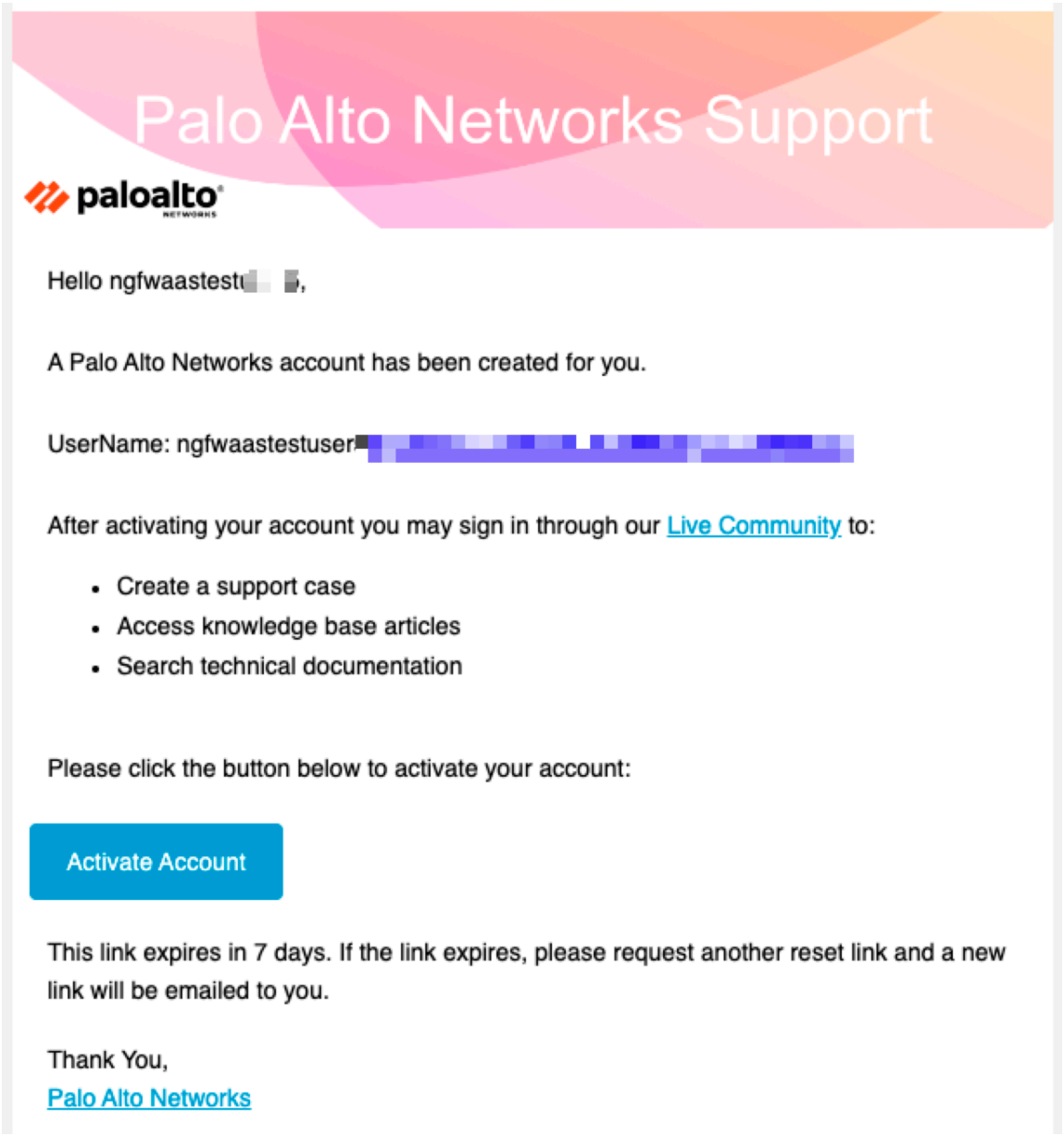
   Vous devez utiliser le même e-mail lorsque vous vous connectez au service Cloud NGFW pour la première fois. De plus, lors de la première connexion, cette adresse e-mail est utilisée pour créer le premier utilisateur, un admin locataire. En outre, le domaine de l'adresse e-mail des utilisateurs invités par l'admin du locataire doit correspondre au domaine de l'adresse e-mail des informations d'identification de connexion de l'admin du locataire.
2. Renseignez les champs **First Name (Prénom)** et **Last Name (Nom)**.
3. Cliquez sur **Create (Créer)**.

   Après avoir cliqué sur **Create (Créer)**, un e-mail contenant un bouton d'activation est envoyé à l'adresse e-mail que vous avez saisie ci-dessus.

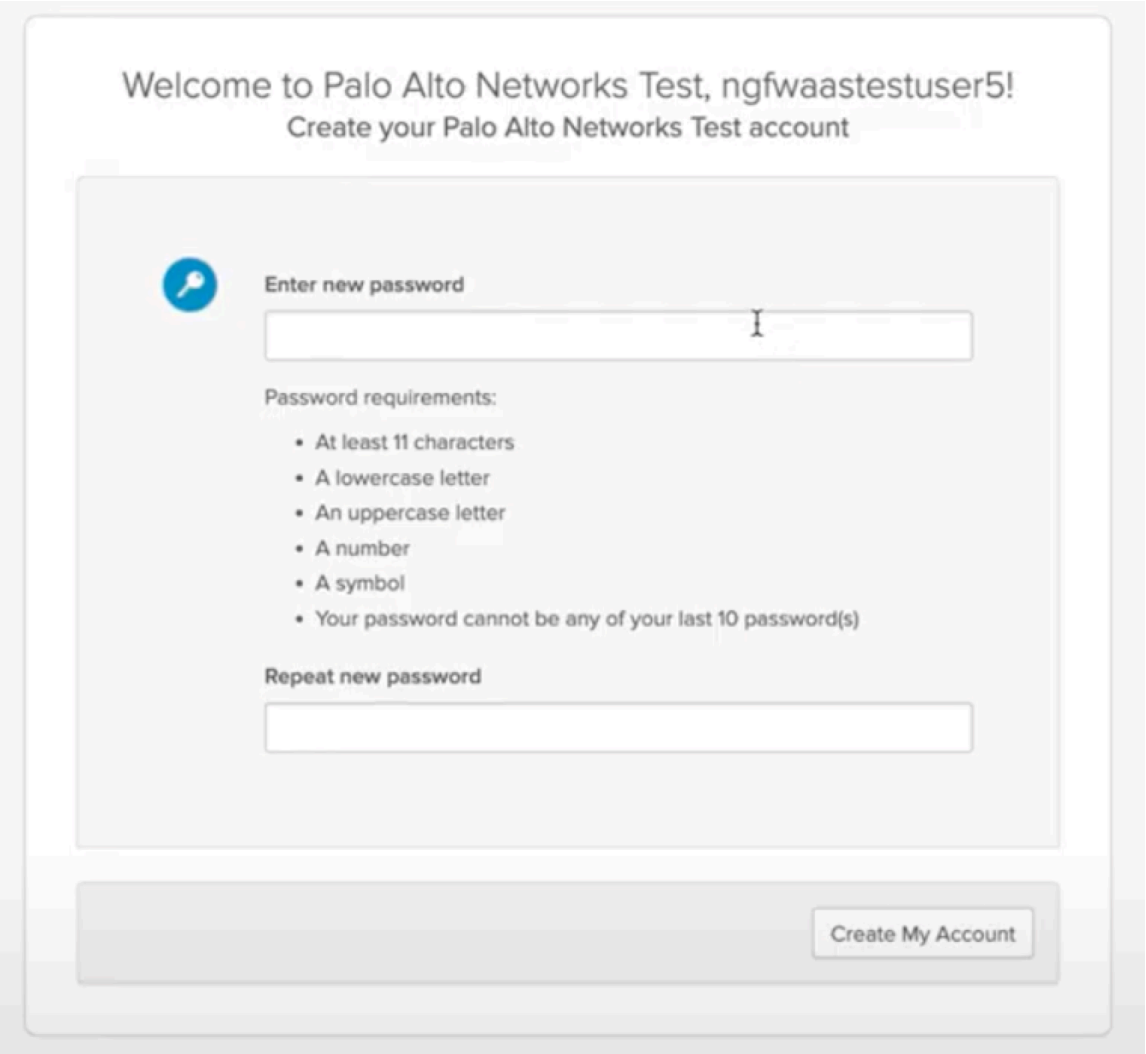


4. Cliquez sur le bouton **Activate Account (Activer le compte)** dans l’e-mail que vous avez reçu.

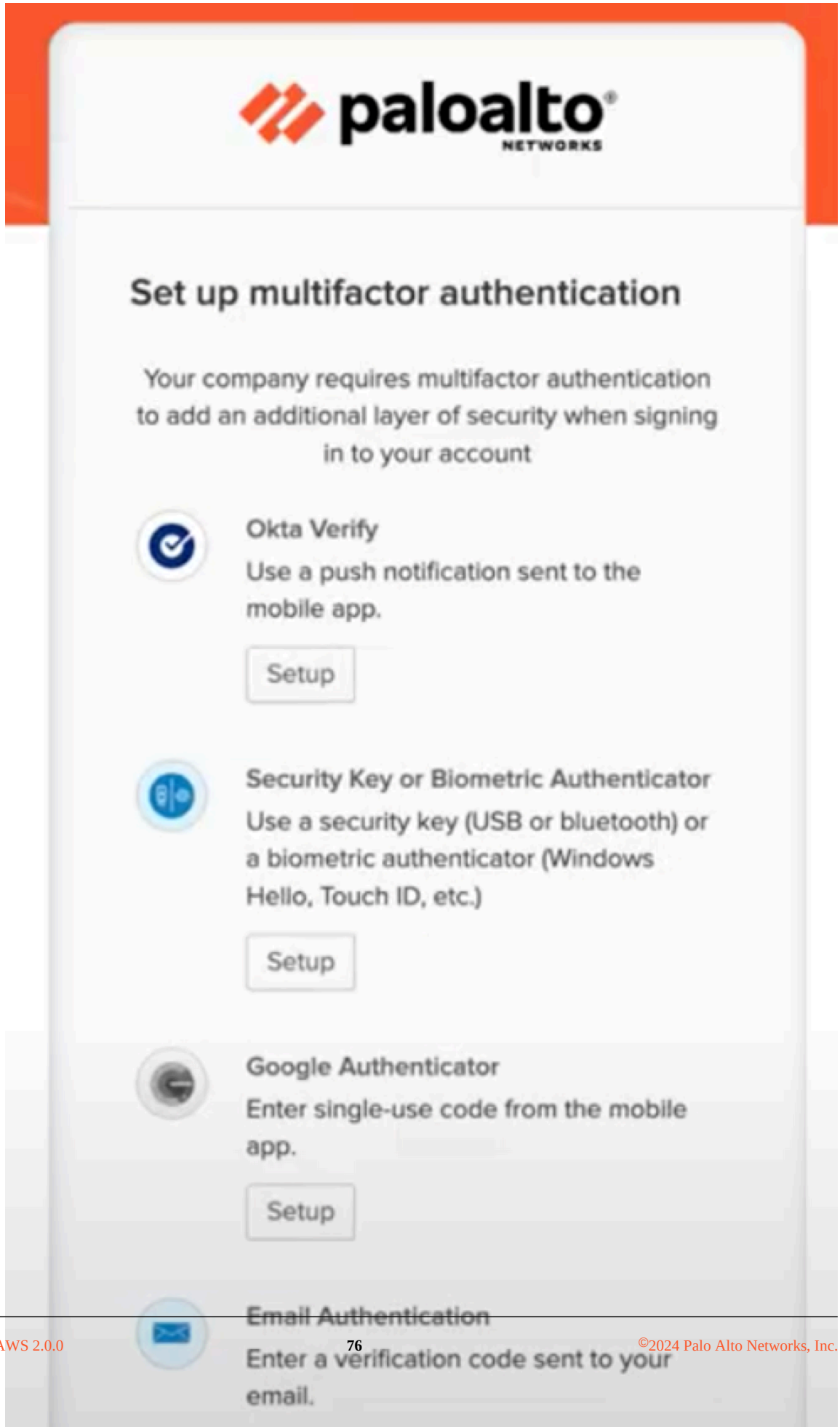
   Le lien reste actif pendant 7 jours. Si vous ne cliquez pas sur le lien dans les 7 jours, vous devrez demander l’envoi d’un e-mail d’activation.



5. Entrez et ressaisissez votre nouveau mot de passe.
6. Cliquez sur **Create My Account (Créer mon compte)**.



7. Configurez votre authentification multifactorielle (MFA).

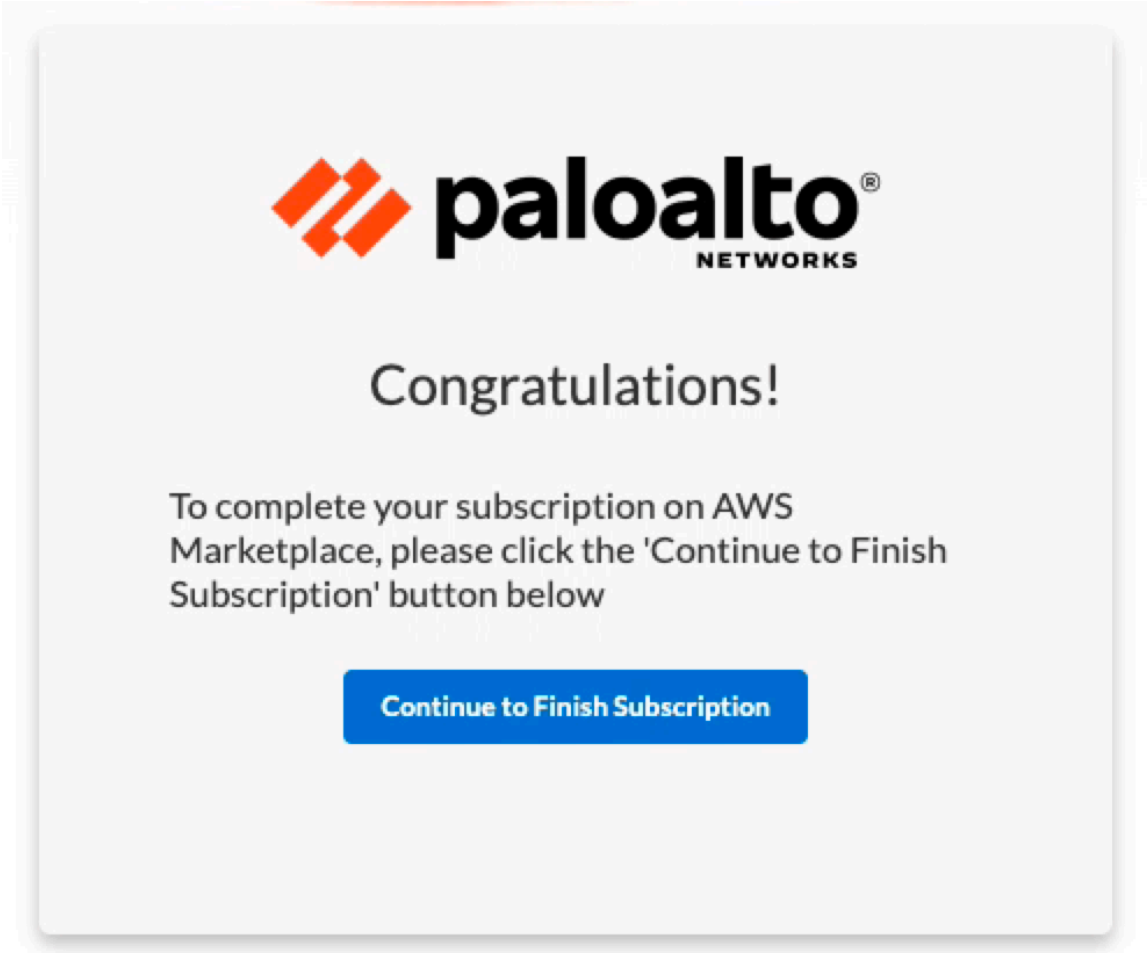


> *Si vous n'êtes pas encore enregistré à l'authentification multifactorielle, mais que vous connaissez votre mot de passe SSO, vous êtes invité à vous enregistrer à l'authentification multifactorielle lors de votre première connexion à l'une des applications. Créez un ticket d'assistance si vous souhaitez réinitialiser la MFA.*

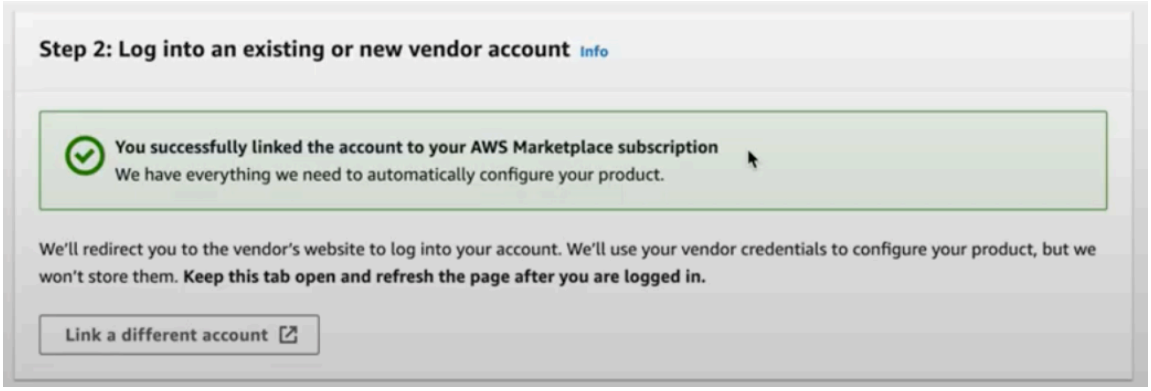
8. Choisissez l'une des méthodes MFA et cliquez sur **Setup (Configuration)**.
9. Terminez le processus de vérification MFA : par exemple, si vous cliquez sur le bouton Configuration pour l'authentification par e-mail, vous serez invité à cliquer sur **le bouton Send me the code (Envoyez-moi le code)**. Après avoir cliqué, vous recevrez un e-mail contenant le code de vérification. Saisissez le code de vérification et cliquez sur **Verify (Vérifier)**. Vous

pouvez également choisir d’effectuer le processus de vérification MFA à l’aide d’Okta Verify, d’une clé de sécurité, d’un authentificateur biométrique ou de Google Authenticator.

10. Connectez-vous au locataire à l’aide de votre adresse e-mail et votre mot de passe enregistrés, puis cliquez sur **Continue to Finish Subscription (Continuer pour finaliser l’abonnement)**.



11. La page de lancement rapide indique désormais que vous avez correctement lié votre compte à l’abonnement AWS Marketplace.



1. Si vous êtes un utilisateur existant non enregistré à SSO, mais que vous souhaitez créer un nouveau locataire utilisant le même identifiant de messagerie, vous recevrez un e-mail d'activation après votre connexion au locataire. Suivez les étapes 6d à 6k pour enregistrer votre locataire.

   Si vous êtes un utilisateur existant sur Cloud NGFW, mais que vous n'êtes pas un administrateur de locataire, la MFA n'est pas actuellement disponible. Vous continuerez à vous connecter sans être invité à vous inscrire à la MFA.

2. Si vous êtes un utilisateur existant qui s'est enregistré à SSO et que vous souhaitez créer un nouveau locataire à l'aide du même identifiant de messagerie, vous serez invité à sélectionner un locataire et à cliquer sur **Continue (Continuer)**.

STEP 7 | Cliquez sur **Launch Template (Lancer le modèle)**, sélectionnez la région CFT et créez des rôles et des autorisations pour votre locataire.

Cloud NGFW ouvre la console du modèle AWS CloudFormation (CFT) associée au compte AWS que vous avez spécifié dans un nouvel onglet de navigateur. Si vous avez installé un bloqueur de pop-up, le nouvel onglet peut être bloqué. Dans ce cas, dans la console Cloud NGFW, sélectionnez Comptes AWS et localisez le compte AWS que vous venez d'ajouter. Cliquez sur **Pending (En attente)** dans la colonne **Status (État)**.

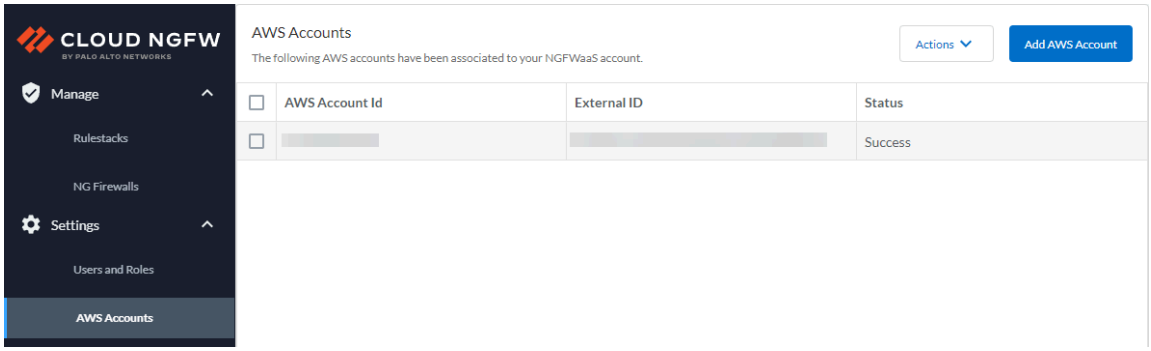
STEP 8 | Dans la section Capacités en bas de la console CFT, cochez **I acknowledge that AWS CloudFormation might create IAM resources (Je reconnais qu'AWS CloudFormation peut créer des ressources IAM)**.

STEP 9 | Cliquez sur **Create Stack (Créer une pile)**. Le CFT associé à l'abonnement (par exemple, PaloAltoNetworksCrossAccountRoleSetup) s'affiche.

STEP 10 | Cliquez sur **Launch your product (Lancer votre produit)**.

1. Saisissez votre e-mail et votre mot de passe, puis cliquez sur **Log In (Se connecter)**.
2. Sélectionnez **AWS Accounts (Comptes AWS)**.
3. Vérifiez que le **Status (État)** est passé à **Success (Réussi)**.

*L'état d'intégration reste à l'état **Pending (En attente)** jusqu'à ce qu'AWS ait fini de lancer le CFT.*

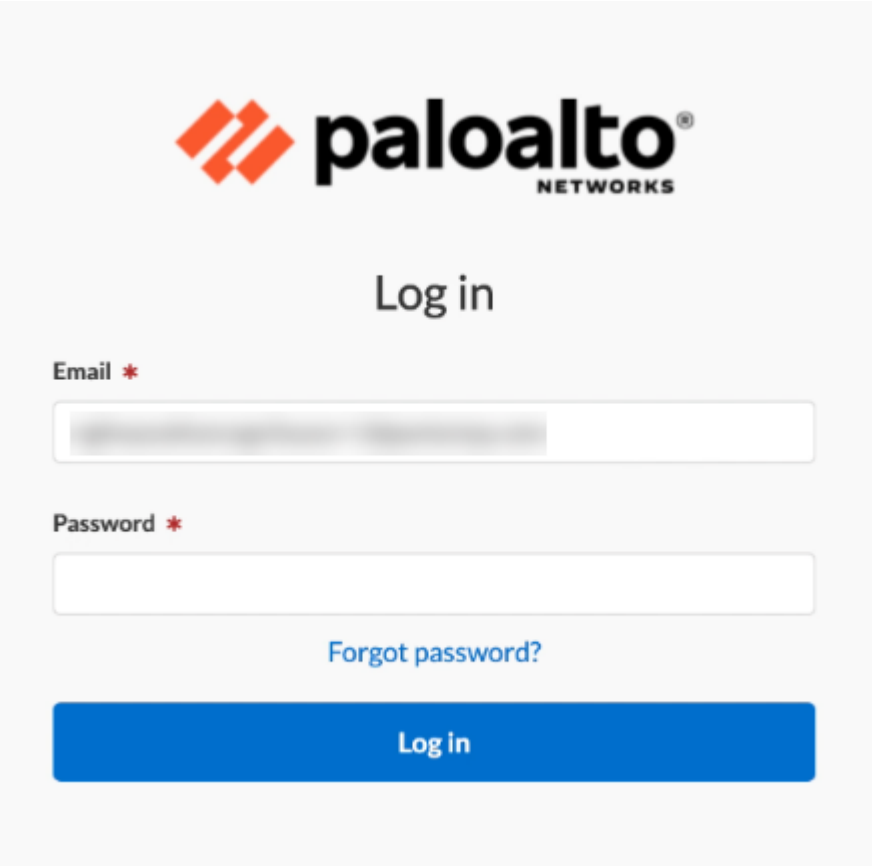


SAML 2.0 peut être utilisé comme fournisseur d'identité pour Cloud NGFW pour AWS. Pour plus d'informations, consultez Gérer les intégrations de fournisseurs d'identité tiers via les services communs *et* Comment activer un fournisseur d'identité tiers (IDP).

Sécuriser votre accès actuel au Cloud NGFW à l'aide de SSO et de la MFA

Utilisez les informations de cette section pour faire migrer un utilisateur cognito existant vers SSO. Si vous êtes un utilisateur existant de Cloud NGFW pour AWS, vous devez vous enregistrer à des mesures de sécurité supplémentaires, telles que SSO et MFA pour un locataire existant (en activant l'adresse e-mail de l'utilisateur avec SSO+MFA), afin de vous connecter et d'accéder aux locataires existants.

STEP 1 | Saisissez l’adresse **e-mail** avec laquelle vous vous êtes enregistré sur AWS Cloud NGFW et cliquez sur **Log in (Connexion).**



STEP 2 | Saisissez le mot de passe et cliquez sur **Log in (Connexion)**.

STEP 3 | Vous serez invité à vous enregistrer au Single Sign-On (ouverture de session unique – SSO) de Palo Alto Networks.

STEP 4 | Cliquez sur **Continue (Continuer)** pour poursuivre l'enregistrement à SSO. Vous pouvez également choisir de cliquer sur **Register Later (S'enregistrer ultérieurement)** pour continuer avec vos

informations d'identification de connexion précédentes. Cependant, vous serez invité à vous enregistrer à SSO chaque fois que vous tentez de vous connecter.

STEP 5 | Vous recevrez un e-mail contenant les instructions d'enregistrement à SSO. Suivez les instructions et terminez l'enregistrement à SSO et à MFA, comme décrit ci-dessus.

STEP 6 | Cliquez sur **Continue (Continuer)**.

STEP 7 | Lors de votre prochaine connexion, vous serez invité à cliquer sur le bouton **Enable and Log Out (Activer et Se déconnecter)** pour vous reconnecter à l'aide de SSO.

STEP 8 | Saisissez votre adresse **e-mail** et cliquez sur Log in (Connexion). Vous serez invité par l'affichage de la page SSO Sign In (Connexion SSO).

STEP 9 | Saisissez votre adresse e-mail et cliquez sur **Next (Suivant)**.

STEP 10 | Saisissez le mot de passe et cliquez sur **Log In (Connexion)**.

STEP 11 | Terminez le processus de vérification de MFA. Vous pourrez désormais accéder à la page du locataire Cloud NGFW après vous être connecté avec vos identifiants de connexion SSO.

Ajouter des crédits Cloud NGFW pour AWS à votre locataire

Après avoir configuré votre abonnement PAYG, vous pouvez éventuellement convertir votre abonnement Cloud NGFW en un contrat Cloud NGFW SaaS.

STEP 1 | Connectez-vous à la console AWS.

STEP 2 | Recherchez la liste des crédits de contrat Cloud NGFW sur AWS Marketplace.

STEP 3 | Après avoir examiné les informations de présentation du produit, cliquez sur **View purchase options (Visualiser les options d'achat)** pour continuer.

STEP 4 | Configurez votre contrat logiciel.

1. Définissez la durée de votre contrat : **12 months (12 mois)**, **24 months (24 mois)** ou **36 months (36 mois)**.
2. Configurer le renouvellement automatique : **Yes (Oui)** ou **No (Non)**.

   Vous pouvez configurer votre contrat SaaS pour qu'il se renouvelle automatiquement à la fin de la période de contrat que vous avez sélectionnée.

   Si vous choisissez de ne pas renouveler automatiquement votre contrat de crédits Cloud NGFW pour AWS lorsque celui-ci arrive à expiration, votre abonnement revient à un abonnement PAYG standard.

   Ne vous désabonnez pas de l'abonnement de crédits Cloud NGFW pour AWS pendant la durée du contrat.
3. Entrez le nombre de crédits. Pour plus d'informations, reportez-vous à la section Tarification de Cloud NGFW pour AWS.
4. Cliquez sur **Create contract (Créer un contrat)**.

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

How long do you want your contract to run?

○ 12 months ○ 24 months ◉ 36 months

Renewal Settings

Auto Renew when this contract ends on - Sun Aug 03 2025?

◉ Yes
○ No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Contract Options

Cloud NGFW Credits [redacted] / Units 1

Cloud NGFW Credits (1unit = 100 Credits)

You may increase your contract at any time. Changes will be billed on a pro-rated basis. If you have opted in for automatic renewal, your contracts will automatically renew at the end of each term until you change your automatic renewal selection. You may change your automatic renewal selection at any time.

Create contract

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services

Total Contract Price [redacted]

Due Today
Auto Renew -Yes

Cloud NGFW Credits [redacted]

Additional Usage Fees

Pay-as-you-go monthly for additional usage
usage Additional usage costs listed below will apply each month if your usage exceeds your contract. Please contact the seller of this product if you have any questions.

Cloud NGFW Overages [redacted]

Purchase order

Purchase order - *Optional* Learn more

Add purchase order number

STEP 5 | Passez en revue vos options de contrat de crédits Cloud NGFW pour AWS et cliquez sur **Pay Now (Payer maintenant)** pour finaliser l'achat de votre contrat.

STEP 6 | Cliquez sur **Set up your account (Configurer votre compte)** pour terminer votre contrat de crédits Cloud NGFW pour AWS.

STEP 7 | Après vous être connecté à la console Cloud NGFW, vous pouvez vérifier votre type d'abonnement et surveiller votre utilisation de crédit.

1. Connectez-vous à la console Cloud NGFW.
2. Sélectionnez **Settings (Paramètres)** > **Subscription Management (Gestion des abonnements)**.

Utilisateur multilocataire d’un utilisateur unique pris en charge sur plusieurs locataires

Le Cloud NGFW pour AWS prend en charge des informations d’identification de connexion uniques pour plusieurs locataires. Lorsque vous vous connectez à la console Cloud NGFW, les informations d’identification de connexion sont utilisées pour associer l’utilisateur au locataire approprié. Si les mêmes informations d’identification de connexion sont utilisées pour plusieurs locataires, la page de connexion vous invite à sélectionner le locataire que vous souhaitez configurer.

Après vous être connecté au Cloud NGFW, utilisez le menu déroulant pour sélectionner le locataire approprié, puis cliquez sur **Continue (Continuer)**.

Le tableau ci-dessous illustre les cas d’utilisation des scénarios à plusieurs locataires :

Cas d’utilisation	Étapes
L’utilisateur A s’est déjà enregistré auprès du locataire A et l’utilisateur A est invité sur le locataire B.	Vous ne recevrez pas un e-mail d’activation.
L’utilisateur A s’est déjà enregistré auprès du locataire A et s’abonne à un nouveau locataire via l’abonnement AWS Marketplace.	Vous ne recevrez pas un e-mail d’activation.

Ajouter plusieurs comptes AWS

Vous pouvez intégrer plusieurs comptes AWS auprès du même locataire. Une fois intégrés, vous pouvez créer des ressources de pare-feu dans plusieurs comptes. En outre, vous aurez la possibilité de déployer des terminaux Cloud NGFW sur les comptes intégrés pour la ressource de pare-feu dans n’importe quel compte AWS.

Votre abonnement au compte AWS s’intègre à une expérience d’abonnement améliorée à partir du service AWS Marketplace. Cette intégration se produit lorsque vous créez un locataire Cloud NGFW ; votre compte AWS est lié au locataire Cloud NGFW.

Plusieurs abonnements à un compte AWS peuvent être ajoutés au locataire. Cloud NGFW prend en charge jusqu’à 200 comptes.

Vous pouvez intégrer plusieurs comptes AWS (sans nouvelle exigence d’abonnement) au locataire à partir de la console Cloud NGFW, et vous créez des ressources de pare-feu dans tous les comptes AWS intégrés au locataire.

Pour faciliter l’utilisation, il n’existe qu’un seul compte de facturation dans le locataire. Si le compte de facturation est désabonné d’AWS Marketplace, le compte de facturation suivant du locataire est sélectionné de manière dynamique. Des modifications supplémentaires de l’état du compte sont introduites pour mieux gérer le cycle de vie du compte AWS dans le locataire. Lorsque le dernier compte AWS est désabonné du locataire, il déclenche un nettoyage des ressources du locataire s’il n’y a pas de contrat actif attaché au locataire.

Dix comptes en attente sont pris en charge par locataire.

Outre la prise en charge des locataires multicomptes, Cloud NGFW prend en charge un modèle de ressource de pare-feu multi-VPC. Grâce à la prise en charge de plusieurs VPC, vous pouvez activer votre Cloud NGFW pour sécuriser le trafic dans plusieurs VPC AWS. Vous payez pour l’utilisation du Cloud NGFW pour chaque zone de disponibilité AWS pour laquelle le NGFW est approvisionné pour sécuriser le trafic.

Utilisez la section **Endpoint Management (Gestion des terminaux)** de la page **Create Firewall (Créer un pare-feu)** pour gérer la création des terminaux pour le NGFW dans ces zones de disponibilité. Vous payez AWS pour chaque terminal VPC (équilibreur de charge de passerelle) que vous créez pour le NGFW.

Lorsque vous utilisez une ressource de pare-feu multi-VPC, tenez compte des points suivants :

- Les pare-feu multi-VPC sont uniquement pris en charge en mode géré par le client.
- Les terminaux d'une ressource de pare-feu multi-VPC peuvent exister dans n'importe quel VPC de l'un des comptes intégrés avec succès. 50 terminaux sont pris en charge pour une ressource de pare-feu multi-VPC.
- Lorsque vous désactivez la fonctionnalité multi-VPC pour une ressource de pare-feu, un terminal ne peut exister que dans le VPC d'ancrage (et le compte d'ancrage). L'ancrage représente une connexion résiliente à la zone de disponibilité. Le VPC d'ancrage et le compte d'ancrage font référence au VPC et au compte associé à la ressource de pare-feu au moment de la création. La communication avec le VPC échoue si un terminal existe en dehors du compte d'ancrage et du VPC.
- Lorsque vous supprimez un compte du locataire, tous les terminaux des pare-feu multi-VPC doivent être supprimés du compte. L'appel échoue si un terminal se trouve dans un compte qui a été supprimé du locataire.
- Lors de la création de terminaux entre comptes pour une ressource de pare-feu, les terminaux doivent être créés dans l'un des ID de zone mappés aux zones définies dans la configuration du pare-feu.
- Les noms des ID de zone sont traités différemment dans AWS. Pour les comptes distincts, utilisez le même ID de zone pour garantir l'affichage du terminal dans la zone correcte.
- Bien que l'ID de compte soit facultatif pour un seul compte, il doit être utilisé dans les comptes multiples.

Le nom de la zone (par exemple, us-east-la) aura un mappage différent sur l'ID de zone (par exemple, use1-az4) entre les différents comptes.

Vous pouvez ajouter des rôles entre comptes à partir de votre compte AWS au locataire Cloud NGFW à l'aide de l'expérience d'abonnement améliorée d'AWS Marketplace. Ce processus nécessite l'ajout d'autorisations IAM supplémentaires et le déploiement de ressources. Vous pouvez également utiliser la console Cloud NGFW pour ajouter les ARN de rôle manuellement. La gestion des rôles entre comptes est prise en charge pour les ajouts incrémentiels des rôles.

La mise à jour du modèle Cloudformation est prise en charge.

Par exemple, le certificat dans compte1 et le certificat dans compte2 peuvent être mappés à une rulestack dans compte3 qui pourrait être associée à une ressource de pare-feu dans compte4. Dans ce scénario, tous les comptes (1 à 4) doivent être intégrés avec succès.

Pour les comptes AWS déjà intégrés, vous pouvez ajouter des comptes supplémentaires à l'aide du locataire multicomptes. Commencez par accéder à la page d'abonnement d'AWS Marketplace pour votre abonnement Palo Alto Networks NGFW.

STEP 1 | Accédez à votre abonnement sur AWS Marketplace.

STEP 2 | À l'étape 1, vérifiez que votre abonnement dispose des autorisations d'administrateur AWS nécessaires.

STEP 3 | À l'étape 2, reliez un compte fournisseur nouveau ou existant. Cliquez sur **Login or create vendor account (Connectez-vous ou créez un compte fournisseur)** pour accéder à un compte Cloud NGFW existant afin de relier votre locataire et d'activer la communication avec le service AWS. La page de connexion de **Palo Alto Networks Cloud NGFW** s'affiche.

STEP 4 | Dans l'écran **Welcome (Bienvenue)** , cliquez sur **Login with an Existing Account (Se connecter avec un compte existant)**.

STEP 5 | Saisissez vos informations d'identification de connexion pour le locataire Cloud NGFW. Une fois connecté, AWS Marketplace indique que vous avez réussi à relier votre compte fournisseur.

S'il n'y a pas de modèle CloudFormation (CFT) pour votre compte, ou si vous devez configurer un CFT existant, consultez les informations figurant à la fin de cet article pour ajouter un modèle CloudFormation manuellement.

STEP 6 | Si un CFT existe, passez à l'étape 4 et lancez la console Cloud NGFW pour poursuivre la configuration. Cliquez sur **Launch product (Lancer le produit)**.

STEP 7 | Connectez-vous à la console Cloud NGFW.

STEP 8 | Sélectionnez **AWS Accounts (Comptes AWS)**.

STEP 9 | Sélectionnez l'**AWS Account ID (ID de compte AWS)** que vous souhaitez l'ajouter en tant que locataire multicomptes.

STEP 10 | Cliquez sur **Add AWS Account (Ajouter un compte AWS)**.

STEP 11 | Saisissez le nom de l'**AWS Account ID (ID de compte AWS)** du compte que vous souhaitez ajouter au compte existant.

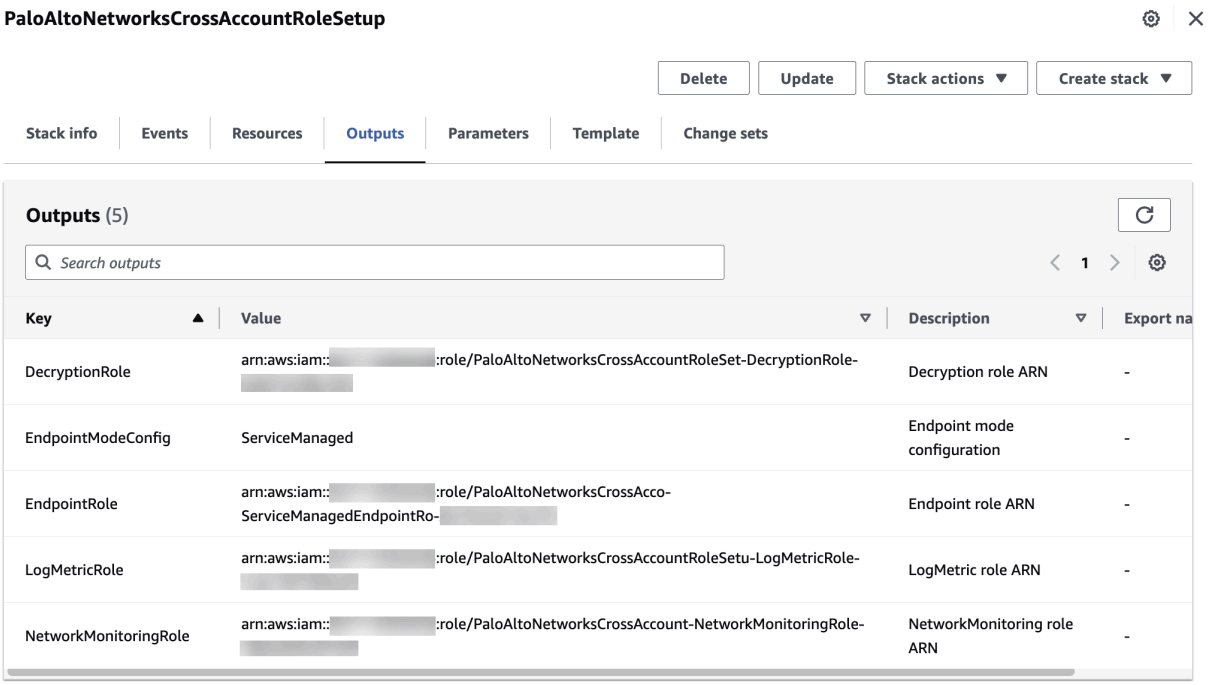
STEP 12 | Connectez-vous à votre compte AWS.

STEP 13 | Créez une pile à l'aide de la console AWS ; cliquez sur **Create Stack on AWS (Créer une pile sur AWS)**ou utilisez l'AWS CLI.

STEP 14 | Sélectionnez **Je reconnais qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés**.

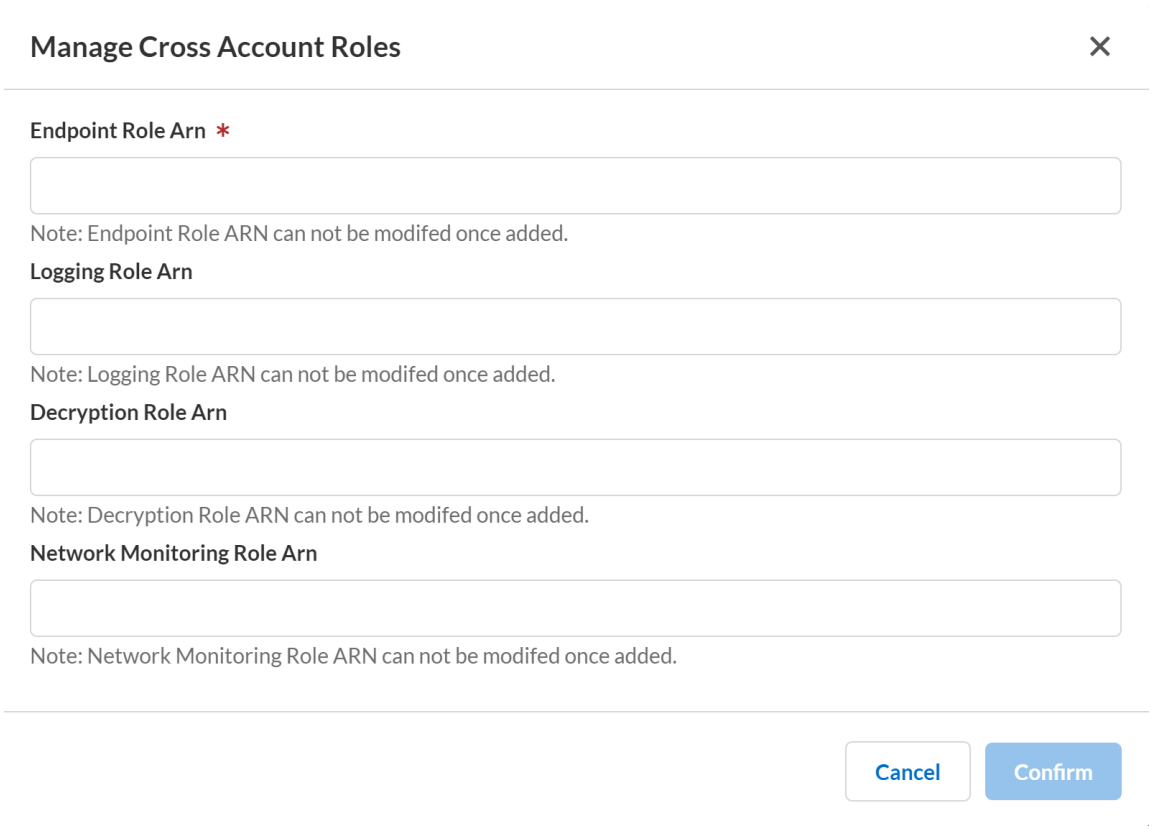
STEP 15 | Cliquez sur **Create Stack (Créer une pile)**.

STEP 16 | Une fois que l'état s'affiche **CREATE_COMPLETE**, copiez la **Value (Valeur)** ARN du rôle depuis l'onglet **Outputs (Sorties)** dans la console AWS.



STEP 17 | Ajoutez les valeurs ARN du rôle à la console de locataire Cloud NGFW.

1. Revenez à la console de locataire Cloud NGFW.
2. Dans la console de locataire Cloud NGFW, sélectionnez **Settings (Paramètres)** > **AWS Accounts (Comptes AWS)**.
3. Sélectionnez le bouton radio du compte AWS que vous ajoutez et sélectionnez **Manage Cross Account Roles (Gérer les rôles entre-comptes)** de la liste déroulante **Actions**.
4. Collez les valeurs ARN de rôle de l'étape précédente dans les champs correspondants.
5. Cliquez sur **Confirm (Confirmer)**.



Ajouter un modèle CloudFormation manuellement

Dans certains cas, vous devrez peut-être ajouter un modèle CloudFormation (CFT) manuellement à un compte.

STEP 1 | Dans la console Cloud NGFW, sélectionnez le compte AWS que vous souhaitez configurer.

STEP 2 | Sous **Account Property (Propriété du compte)**, cliquez sur **Check Details (Vérifier les détails)**. Cet écran fournit des détails que vous utiliserez pour le CFT.

STEP 3 | L'écran **Account Property Details (Détails sur la propriété du compte)** fournit les informations nécessaires à la création manuelle d'un nouveau CFT. Pour améliorer votre sécurité, générez un nouveau jeton pour le nouveau CFT. Cliquez sur **Generate Update Token (Générer un jeton de mise à jour)**.

STEP 4 | Utilisez les informations de jeton mises à jour, ainsi que les autres informations affichées sur l'écran **Account Property Details (Détails sur la propriété du compte)** (ID externe, ID de compte Cloud NGFW et ARN de la rubrique SNS) pour configurer manuellement le CFT dans la console AWS.

STEP 5 | Pour prendre en charge la fonctionnalité de locataire multicompte, certaines fonctionnalités ont été ajoutées à la page de la pile AWS CFT de votre abonnement. Localisez votre abonnement dans la console AWS et utilisez les informations de l'onglet **Events (Événements)** pour surveiller l'état de la pile CFT.

STEP 6 | Utilisez l'onglet **Outputs (Sorties)** pour afficher les informations que vous utiliserez (par exemple, les **EndpointRole** et **LogMetricRole** de la clé afin de configurer manuellement le locataire multicomptes d'un compte AWS existant dans la console Cloud NGFW. Copiez ces informations afin de pouvoir les utiliser ultérieurement.

STEP 7 | Dans la console Cloud NGFW, sélectionnez **AWS Accounts (Comptes AWS)**. Sélectionnez le compte que vous souhaitez configurer, puis sélectionnez l'option de gestion **Manage Cross Account Rules (Gérer les règles de compte croisé)** dans le menu déroulant.

STEP 8 | Dans l'écran **Account Property Details (Détails de la propriété du compte)**, saisissez les éléments **Endpoint Rules Arn (Règles de terminal arn)**, **Logging Rule Arn (Règle de journalisation Arn)**et **Network Monitoring Role Arn (Rôle de surveillance du réseau Arn)**. Vous trouverez ces informations dans le champ **Endpoint Rules (Règles de terminal)** situé dans l'onglet **Outputs (Sorties)** dans la console AWS (**CloudFormation > Stacks [Piles]**), puis cliquez sur **Create (Créer)**.

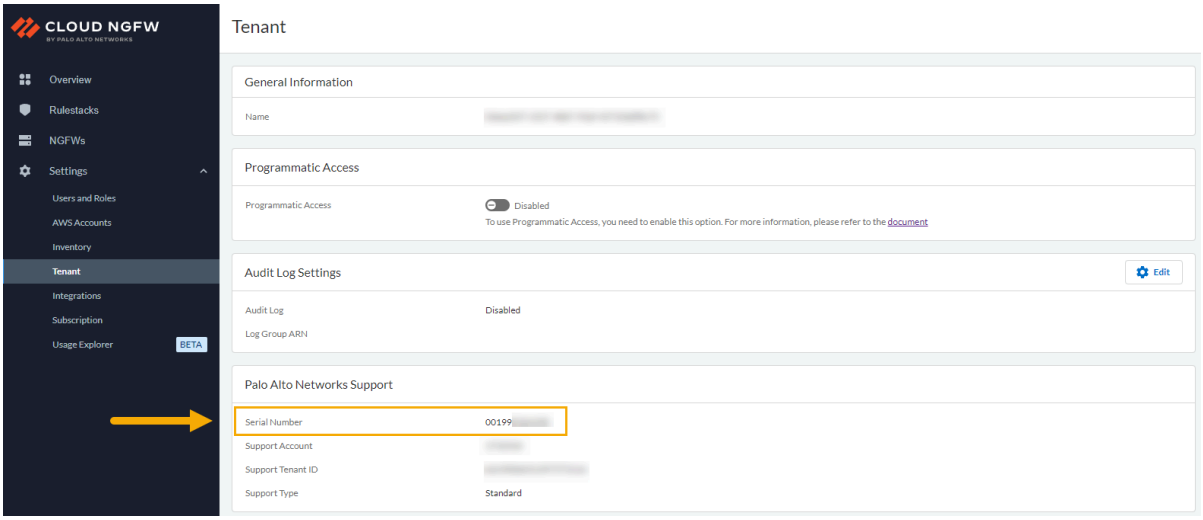
Après la mise à jour des informations ARN dans l'écran **Account Details (Détails du compte)**, la page **Cloud NGFW AWS Accounts (Comptes Cloud NGFW AWS)** indique que les informations du compte ont été mises à jour.

Rechercher le numéro de série de votre Cloud NGFW pour AWS

Pour rechercher le numéro de série de Cloud NGFW :

STEP 1 | Connectez-vous au locataire Cloud NGFW.

STEP 2 | Cliquez sur **Tenant (Locataire)**. La page Tenant (Locataire) affiche le **Serial Number (Numéro de série)** et des informations supplémentaires dans la section **Palo Alto Networks Support (Support Palo Alto Networks)**.



Autorisations CFT de rôle entre comptes pour Cloud NGFW

Cloud NGFW nécessite des autorisations pour accéder aux informations et aux ressources associées à vos comptes AWS. Lorsque vous intégrez un compte AWS, un modèle CloudFormation (CFT) est fourni pour vous aider à activer les autorisations. Lorsque vous déployez le CFT, il crée un rôle IAM entre comptes dans votre compte AWS. Ce rôle IAM fournit à Cloud NGFW les autorisations nécessaires pour lire les informations VPC requises pour créer et gérer des terminaux, envoyer des journaux aux destinations de journalisation et accéder aux certificats dans AWS Secrets Manager pour le décryptage du trafic.

Configuration du terminal

Le rôle IAM entre comptes nécessite des autorisations pour lire les informations sur vos ressources VPC, ce qui vous permet de configurer des terminaux NGFW dans votre environnement AWS.

```
{ "Sid": "Allow Cloud NGFW to read VPC resources", "Effect":
 "Allow", "Action": [ # Les quatre premières autorisations sont
 les quatre autorisations minimales nécessaires "ec2:DescribeVpcs",
 "ec2:DescribeSubnets", "ec2:DescribeAvailabilityZones
 "ec2:DescribeVpcEndpoints", ], "Resource": "*" }
```

Création de terminaux

(Facultatif) Vous pouvez configurer Cloud NGFW pour créer et gérer des terminaux NGFW dans votre compte AWS. Si vous choisissez de ne pas configurer ces autorisations, vous devez créer manuellement des terminaux NGFW après avoir déployé votre NGFW.

```
{ "Sid": "Allow Cloud NGFW to manage NGFW endpoints",
 "Effect": "Allow", "Action": [ "ec2:deleleVpcEndpoints"
 "ec2:CreateVpcEndpoints" ], "Resource": "*" }
```

Journalisation et gestion des métriques

(Facultatif) Le rôle entre comptes inclut les autorisations requises pour la journalisation et la gestion des métriques. Le modèle ne crée pas les destinations de journalisation ; au lieu de cela, il fournit les autorisations nécessaires pour accéder aux destinations de journalisation spécifiées. Vous devez créer les destinations de journalisation que vous spécifiez dans le modèle.

Le modèle fournit la valeur par défaut **PaloAltoCloudNGFW** pour un espace de noms Cloudwatch et Kinesis Data Firehose. Le modèle ne fournit pas de valeur par défaut pour un compartiment S3. Vous pouvez remplacer la valeur par défaut par la valeur d'une destination de journalisation correspondante dans votre compte AWS.

```
{ "Sid": "Allow Cloud NGFW access to one Cloudwatch
 Namespace", "Effect": "Allow", "Resource": "*", "Action":
 "cloudwatch:PutMetricData", "Condition": { "StringEquals":
 { "cloudwatch:namespace": "PaloAltoCloudNGFW" } } }{ "Sid":"Allow
 Cloud NGFW access to write logs in one LogGroup", "Action":
 [ "logs:CreateLogStream", "logs:DescribeLogStreams",
 "logs:PutLogEvents", ], "Effect": "Allow", "Resource":
 [ "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW"
 "arn:aws:logs:*:*:log-group:PaloAltoCloudNGFW:log-stream:*" ], }
{ "Sid": "Optionally, Allow Cloud NGFW to write logs to one
```



```
 S3 bucket", "Effect": "Allow", "Action": [ "s3:putObject" ],
 "Resource": [ # Ceci est la proposition n° 1 – le nom est codé
 en fonction d'externalid "arn:aws:s3:::<PaloAltoCloudNGFW-
ExternalD>/*" # Ceci est la proposition n° 2 – le nom est fourni
 par le client dans CFT. 'arn:aws:s3:::${S3Bucket}/*' ] }{ "Sid":
 " Optionally, Allow Cloud NGFW to write logs to Streams",
 "Effect": "Allow", "Action": [ "firehose:putRecordBatch" ],
 "Resource": [ "arn:aws:kinesis:region:account:deliveryStream/
PaloAltoCloudNGFW*" ], }
```

Déchiffrement

(Facultatif) Le rôle entre comptes inclut des autorisations permettant à Cloud NGFW de récupérer des certificats à partir de Secrets Manager dans votre compte AWS et de l'utiliser pour décrypter le trafic circulant via votre NGFW. Ces autorisations utilisent le mécanisme de contrôle d'accès basé sur les attributs (ABAC) en spécifiant une étiquette d'accès. Ces autorisations sont facultatives et vous pouvez choisir de ne pas les configurer lorsque vous déployez le modèle.

```
{ "Sid": "Allow Cloud NGFW to pick up certificates", "Effect":
 "Allow", "Action": [ "secretsmanager:GetSecretValue" ],
 "Resource": "*", "Condition": { "StringEquals": { "aws:ResourceTag/
PaloAltoCloudNGFW": "true" } } }
```

Surveillance des comptes

(Facultatif) Le modèle CloudFormation (CFT) existant de votre compte AWS intégré peut se voir ajouter des autorisations de surveillance de compte.

```
{ "Version": "2012-10-17", "Statement": [ { "Action":
 [ "ec2:DescribeVpcs", "ec2:DescribeNetworkInterfaces",
 "ec2:DescribeSecurityGroups", "ec2:DescribeInstances",
 "ec2:DescribeVpcEndpoints", "ec2:DescribeSubnets",
 "ec2:DescribeManagedPrefixLists",
 "elasticloadbalancing:DescribeLoadBalancers",
 "elasticloadbalancing:DescribeTags" ], "Resource": "*", "Effect":
 "Allow" }, { "Action": [ "ec2:GetManagedPrefixListAssociations",
 "ec2:GetManagedPrefixListEntries" ], "Resource":
 [ "arn:aws:ec2:*:*:prefix-list/*" ], "Effect": "Allow" } ] }
```


Inviter des utilisateurs sur Cloud NGFW pour AWS

En tant qu'admin locataire, vous pouvez inviter des utilisateurs supplémentaires à vous aider à gérer votre déploiement Cloud NGFW. Vous pouvez ensuite placer ces nouveaux utilisateurs dans les rôles nécessaires à leur niveau d'accès. Lorsque vous invitez un utilisateur au locataire Cloud NGFW, en spécifiant l'adresse e-mail de l'utilisateur et en attribuant un ou plusieurs rôles Cloud NGFW, le locataire Cloud NGFW envoie à l'utilisateur un e-mail contenant un lien d'inscription et un mot de passe temporaire. Après s'être connecté pour la première fois, le nouvel utilisateur sera invité à créer un nouveau mot de passe. Tant que l'utilisateur invité n'a pas accepté l'invitation et ne s'est pas connecté au locataire, l'invitation est considérée comme en attente.

Rôle Cloud NGFW	Autorisations
Admin	• Ajoutez des comptes AWS. • Invitez des utilisateurs et attribuez des rôles. • Créez NGFW. • Créez/gérez des rulestacks globales et locales.
Admin locataire	• Ajoutez des comptes AWS. • Invitez des utilisateurs et attribuez des rôles.
Lecteur locataire	• Lisez toutes les ressources du pare-feu et ses paramètres. • Lisez toutes les rulestacks globales et locales. • Lisez tous les utilisateurs locataires et les paramètres des locataires.
Admin de pare-feu global	• Créez NGFW. • Créez des rulestacks globales et locales.
Admin de la rulestack globale	Créez une rulestack globale.
Admin de pare-feu local	• Créez NGFW. • Associer une rulestack locale à des NGFW *Les administrateurs de pare-feu locaux peuvent uniquement créer des NGFW et associer des rulestacks au sein d'un compte AWS spécifié.*
Admin local de la rulestack	• Créez des rulestacks locales. • Associer des rulestacks locales à des NGFW

Rôle Cloud NGFW	Autorisations
	Chaque admin local de la rulestack est associé à un ID de compte. Cela autorise les rulestacks locales créées par cet administrateur avec des NGFW dans le même compte.

Le domaine de l'adresse e-mail des utilisateurs invités par l'admin du locataire doit correspondre au domaine de l'adresse e-mail des informations d'identification de connexion de l'admin du locataire.

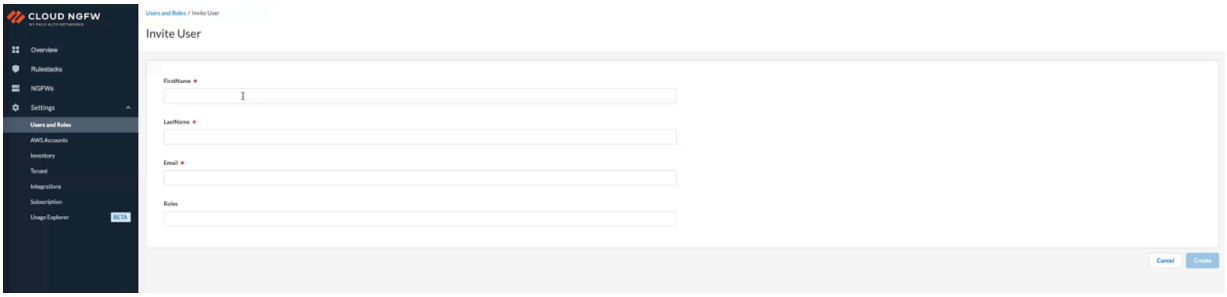
STEP 1 | Connectez-vous au locataire Cloud NGFW.

STEP 2 | Sélectionnez **Settings (Paramètres)** > **Users and Roles (Utilisateurs et rôles)** > **Invite User (Inviter l'utilisateur)**.

STEP 3 | Saisissez le **FirstName (Prénom)**, le **LastName (Nom)** et l'adresse **Email (E-mail)** de l'invité.

STEP 4 | Sélectionnez le ou les rôles du nouvel utilisateur dans la liste déroulante **Roles (Rôles)**. Vous pouvez désormais inviter un utilisateur existant chez un locataire Cloud NGFW.

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



*Après vous être connecté, vous serez invité à sélectionner un locataire et à cliquer sur **Continue (Continuer)**. Si vous êtes un nouvel utilisateur, vous recevrez un e-mail d'activation qui vous permettra de vous enregistrer à SSO et de vous connecter au locataire. Les utilisateurs existants peuvent se connecter directement au locataire à l'aide de votre SSO.*

Considérations relatives aux cas d'utilisation multicomptes

Si le compte d'un client AWS est déjà ajouté à un locataire à partir de la console CNGFW, l'utilisateur aura la possibilité durant le processus d'abonnement de se connecter au locataire sortant ou d'en créer un nouveau. Le tableau ci-dessous illustre ces cas d'utilisation :

Cas d'utilisation	Étapes
Si vous êtes déjà enregistré à SSO	Vous ne recevez pas un e-mail d'activation

Cas d’utilisation	Étapes
Si vous êtes un utilisateur existant qui n’est pas enregistré à SSO	Vous recevez un e-mail d’activation pour compléter l’enregistrement à SSO. Cependant, vous pouvez toujours choisir de vous connecter comme précédemment, jusqu’à ce que vous terminiez l’enregistrement

Utilisez un seul identifiant e-mail pour vous enregistrer à différents locataires à l’aide de l’option **Login with an Existing Tenant (Connexion avec un locataire existant)**.

Après vous être connecté, vous serez invité à sélectionner un locataire et à cliquer sur **Continue (Continuer)**. Si vous êtes un nouvel utilisateur, vous recevrez un e-mail d’activation qui vous permettra de vous enregistrer à SSO et de vous connecter au locataire. Les utilisateurs existants peuvent se connecter directement au locataire à l’aide de votre SSO.

Gérer les utilisateurs Cloud NGFW pour AWS

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.

Gérer les rôles des utilisateurs

STEP 1 | Sélectionnez **Settings (Paramètres)** > **User and Roles (Utilisateur et rôles)**.

STEP 2 | Cliquez sur le nom de l'utilisateur à modifier.

STEP 3 | Modifiez les valeurs **First Name (Prénom)** et **Last Name (Nom)** si nécessaire.

STEP 4 | Modifiez les paramètres **Roles & Scope (Rôles et portée)** de l'utilisateur.

- Pour ajouter un rôle :
  1. Cliquez sur **Add Role (Ajouter un rôle)**.
  2. Sélectionner les valeurs pour **Role (Rôle)** et **Scope (Étendue)** dans les listes déroulantes respectives.
- Pour supprimer un rôle :
  1. Cliquez sur l'icône de suppression ( ) située à droite de la règle à supprimer.

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

Supprimer un utilisateur

Si vous devez supprimer complètement l'accès et les autorisations d'un utilisateur, vous pouvez le supprimer.

STEP 1 | Sélectionnez **Settings (Paramètres)** > **User and Roles (Utilisateur et rôles)**.

STEP 2 | Cochez la case située à gauche du nom de l'utilisateur.

STEP 3 | Sélectionnez **Actions** > **Delete (Supprimer)**.

Modifiez les informations de l'utilisateur

Un administrateur non-client peut mettre à jour son nom ou modifier son mot de passe si nécessaire. Toutefois, ils ne peuvent pas modifier les rôles qui leur sont attribués.

STEP 1 | Sélectionnez **Settings (Paramètres)** > **User and Roles (Utilisateur et rôles)**.

STEP 2 | Cliquez sur le nom d'utilisateur.

STEP 3 | Modifiez les valeurs **First Name (Prénom)** et **Last Name (Nom)** si nécessaire.

STEP 4 | Pour modifier un mot de passe :

1. Cliquez sur **Change Password (Modifier le mot de passe)**.
2. Renseignez le champ **Current Password (Mot de passe actuel)**.
3. Renseignez le champ **New Password (Nouveau mot de passe)**, puis indiquez à nouveau le nouveau mot de passe.
4. Cliquez sur **Change (Modifier)**.

La modification du mot de passe vous déconnecte du locataire Cloud NGFW. Vous devez vous reconnecter à l'aide du nouveau mot de passe.

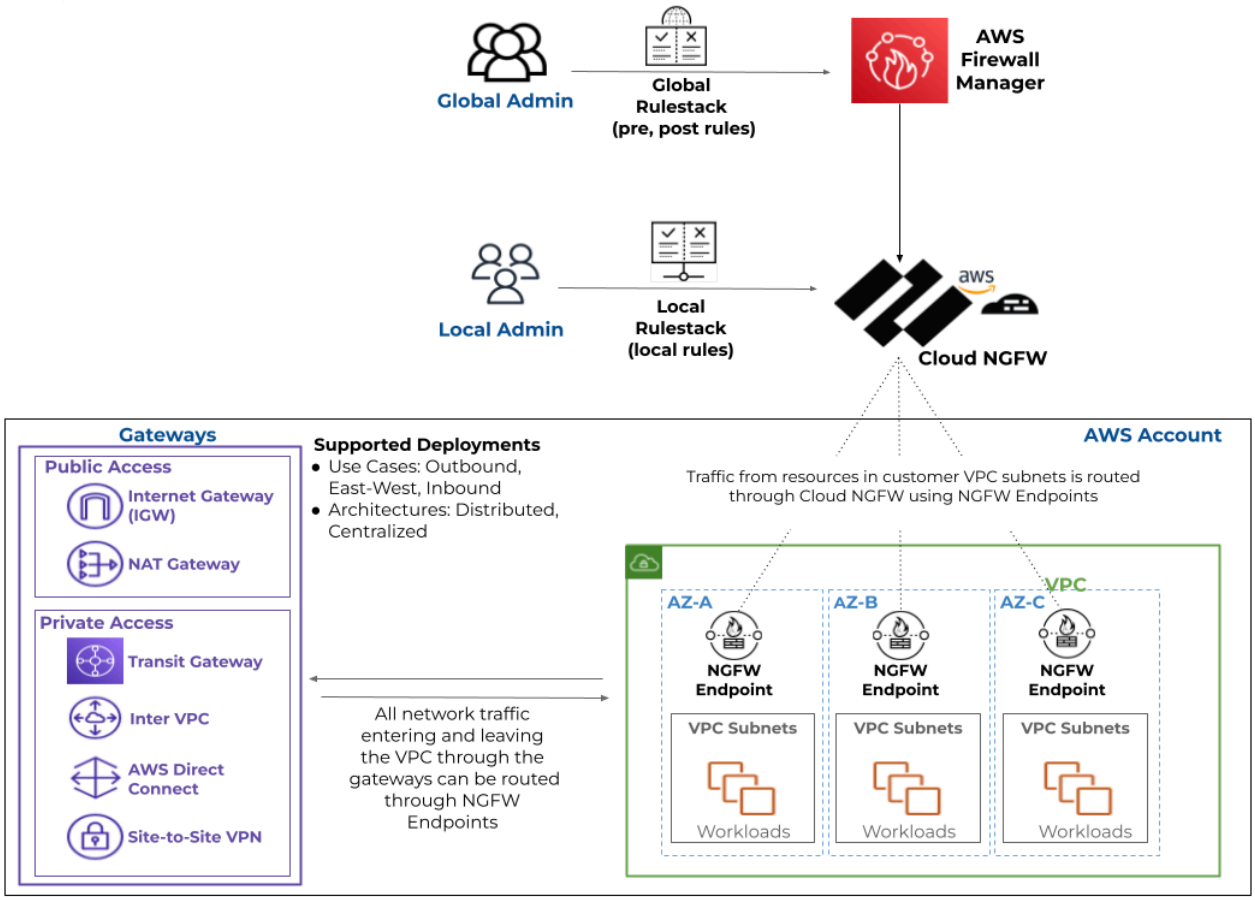
STEP 5 | Cliquez sur **Save (Enregistrer)**.

Déployer Cloud NGFW pour AWS avec AWS Firewall Manager

AWS Firewall Manager (FMS) est un service qui vous permet de gérer de manière centralisée les règles relatives aux pare-feu d'applications Web AWS, aux groupes de sécurité et aux pare-feu réseau AWS sur tous les comptes membres de l'organisation AWS. Vous pouvez désormais utiliser AWS Firewall Manager pour déployer de manière centralisée des ressources Cloud NGFW et gérer les règles entre les VPC de différents comptes AWS de votre organisation AWS. Le tableau de bord AWS Firewall Manager vous permet également d'afficher les notifications de conformité et d'y répondre.

AWS Firewall Manager fournit un flux de travail qui vous permet de déployer le Cloud NGFW en tant que politique FMS, de sélectionner une région et un mode de déploiement, de créer une pile de règles globale, de configurer des terminaux NGFW et de définir la portée du Cloud NGFW dans votre organisation.

Pour plus d'informations, consultez la documentation AWS Firewall Manager.



Cloud NGFW prend en charge les ressources VPC uniquement dans le cadre de la politique FMS.

STEP 1 | S'abonner à Cloud NGFW pour AWS. Le compte AWS que vous utilisez pour vous abonner au service Cloud NGFW doit être le même compte administrateur d'AWS Firewall Manager.

En tant qu'utilisateur IAM dans le compte AWS Firewall Manager, commencez par vous abonner au service Cloud NGFW via AWS Marketplace. Une fois la configuration initiale terminée, revenez au tableau de bord FMS dans la console AWS. Cette procédure crée un locataire Cloud NGFW et vous attribue automatiquement (l'administrateur FMS) les rôles TenantAdmin et GlobalFirewallAdmin.

STEP 2 | Associez le service Palo Alto Cloud NGFW à Firewall Manager.

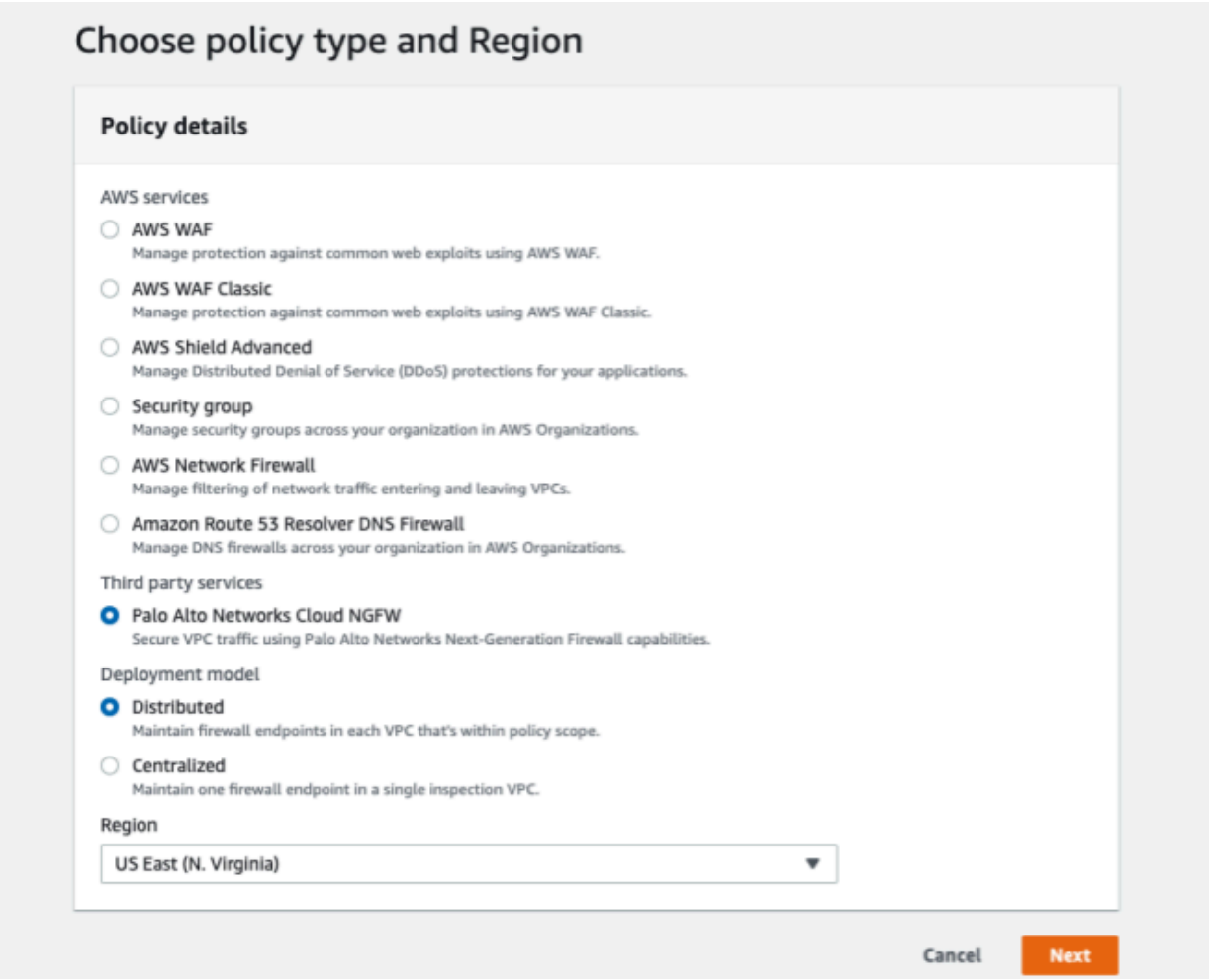
1. Connectez-vous à la console AWS et sélectionnez **Services** > **AWS Firewall Manager** > **Settings (Paramètres)**.
2. Sous Third Party Firewall Association Status (État de l'association de pare-feu tiers), sélectionnez Palo Alto Networks Cloud NGFW.
3. Cliquez sur **Associate (Associer)**.

STEP 3 | Sélectionnez **Security Policies (Politiques de sécurité)** > **Create Policy (Créer une politique)**.

STEP 4 | Choisissez le type de politique et la région.

1. Sous Third Party Services (Services tiers), sélectionnez **Palo Alto Networks Cloud NGFW.**
2. Sélectionnez votre **Deployment Mode (Mode de déploiement)** : distribué ou centralisé.
3. Sélectionnez la **Region (Région)**.

STEP 5 | Cliquez sur **Next (Suivant)**.



STEP 6 | Décrivez la politique FMS pour Cloud NGFW sur AWS.

Fournissez un nom descriptif pour votre politique FMS, configurez ou associez une rulestack globale à la politique FMS et configurez les paramètres des journaux. FMS affiche toutes les rulestacks globales existantes (si disponibles) et un lien qui mène à la console Cloud NGFW pour créer une rulestack

globale. Étant donné que l'utilisateur abonné (administrateur FMS) est un GlobalRulestackAdmin, vous n'avez aucune modification à apporter aux rôles d'utilisateur.

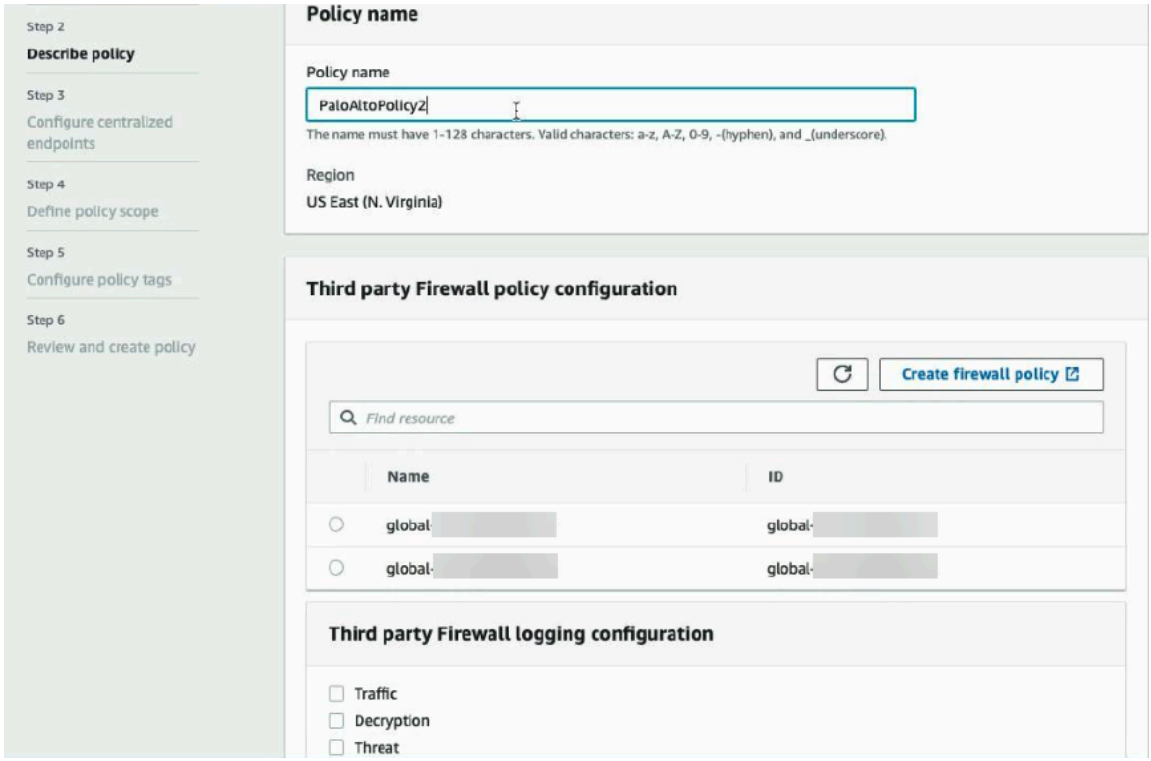
1. Entrez un **Policy Name (Nom de la politique)** descriptif.
2. Sélectionnez ou créez une **Third Party Firewall Policy Configuration (Configuration de politique de pare-feu tiers)**.

   Dans la console FMS, la configuration de la politique de pare-feu tiers fait référence à une rulestack globale dans le contexte du Cloud NGFW. Si vous avez déjà créé une ou plusieurs rulestacks globales, elles sont répertoriées ici. Si vous n'avez pas créé de pile de règles globale, vous pouvez en créer une en cliquant sur **Create Firewall Policy (Créer une politique de pare-feu)**. Cela vous redirige vers la console Cloud NGFW. Pour plus d'informations sur les rulestacks et la configuration des rulestacks, consultez À propos des rulestacks et des règles sur Cloud NGFW pour AWS.
3. Créez une rulestack globale.

   1. Saisissez un **Name (Nom)** descriptif pour votre rulestack.
   2. (facultatif) Entrez une **Description** pour votre rulestack.
   3. Cliquez sur **Save (Enregistrer)**.
   4. Revenez à la console FMS.
4. Configurez la journalisation.

   Vous pouvez sélectionner Journaux de trafic, de décryptage et/ou de menaces. Pour chaque type de journal, vous devez spécifier une destination (compartiment S3, groupe de journaux CloudWatch ou flux de diffusion Kinesis Firehose) dans la liste déroulante. La liste déroulante affiche les destinations précédemment configurées dans votre environnement AWS.

5. Cliquez sur **Next (Suivant)**.



STEP 7 | Configurez les terminaux NGFW.

Cloud NGFW crée des terminaux dans vos zones de disponibilité qui doivent être sécurisés. Ces terminaux NGFW interceptent et redirigent le trafic vers Cloud NGFW à des fins d'inspection et d'application. Le nombre et l'emplacement des terminaux NGFW diffèrent en fonction de votre mode de déploiement (distribué ou centralisé).

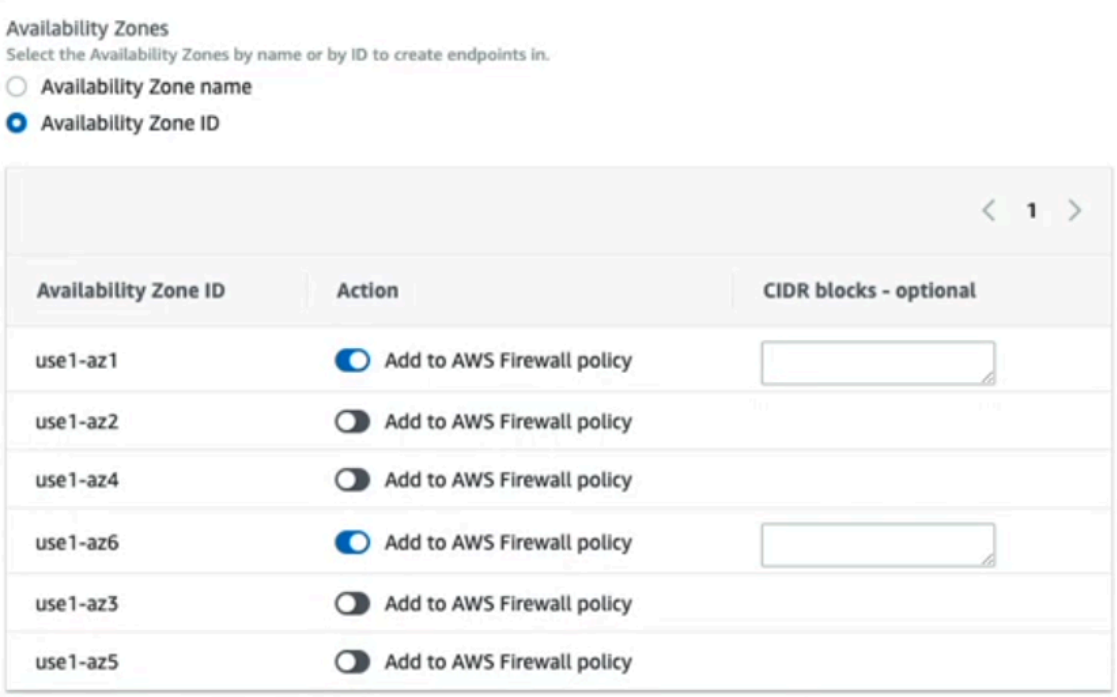
Vous sélectionnez les emplacements des terminaux NGFW en choisissant des noms de zone de disponibilité ou des ID de zone de disponibilité. Gardez à l'esprit que les noms des zones de

disponibilité peuvent différer d'un compte AWS à l'autre, mais que les ID de zone de disponibilité sont cohérents entre tous les comptes AWS.

1. Sélectionnez **Availability Zone Name (Nom de la zone de disponibilité)** ou **Availability Zone ID (ID de la zone de disponibilité)**. Cette sélection détermine les options (noms ou ID) répertoriées par la console FMS.
2. Dans la colonne Action, cliquez sur le curseur pour ajouter une zone de disponibilité à la politique FMS Cloud NFGW.
3. (facultatif) Ajoutez des blocs CIDR (Classless Inter-Domain Routing) pour spécifier les sous-réseaux utilisés par les terminaux NGFW.

   Vous pouvez spécifier un bloc d'adresse CIDR pour chaque zone de disponibilité sélectionnée ou créer une liste de blocs d'adresse CIDR que le FMS affectera aux zones de disponibilité sélectionnées. Chaque bloc CIDR doit être un bloc CIDR /28.

   Si vous ne spécifiez aucun bloc d'adresse CIDR, le FMS adoptera une approche optimale pour rechercher les blocs d'adresse CIDR non attribués dans votre VPC afin de créer des sous-réseaux pour les terminaux NGFW. Si aucun bloc d'adresse CIDR n'est disponible dans votre VPC, le FMS affiche une erreur non conforme.
4. Cliquez sur **Next (Suivant)**.



STEP 8 | Définissez la portée de la politique FMS Cloud NGFW.

La portée de la politique définit les comptes AWS ou les unités organisationnelles (UO) et les ressources qui sont couverts par la politique FMS Cloud NGFW. Vous pouvez appliquer les politiques

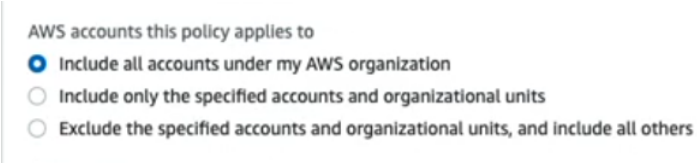
Cloud NGFW FMS à tous les comptes AWS et VPC de votre organisation ou spécifier un sous-ensemble de comptes et/ou de VPC.

Lorsque vous ajoutez un nouveau compte AWS ou VPC à votre organisation, le FMS détermine si votre politique Cloud NGFW doit être appliquée à ce compte ou à ce VPC. Par exemple, vous pouvez appliquer la politique Cloud NGFW à tous les comptes, à l'exception d'un petit sous-ensemble exclu. Lorsqu'un nouveau compte rejoint votre organisation, car il ne figure pas sur la liste des exclus, la politique Cloud NGFW est appliquée.

1. Spécifiez les comptes à inclure ou à exclure de la politique FMS Cloud NGFW.

   Vous pouvez choisir les options **Include all accounts under my AWS organization (Inclure tous les comptes de mon organisation AWS)**, **Include on the specified accounts and organizational units (Inclure sur les comptes et les unités organisationnelles spécifiés)** ou **Exclude specific accounts and organizational units, and include all others (Exclure des comptes et des unités organisationnelles spécifiques et inclure tous les autres)**.

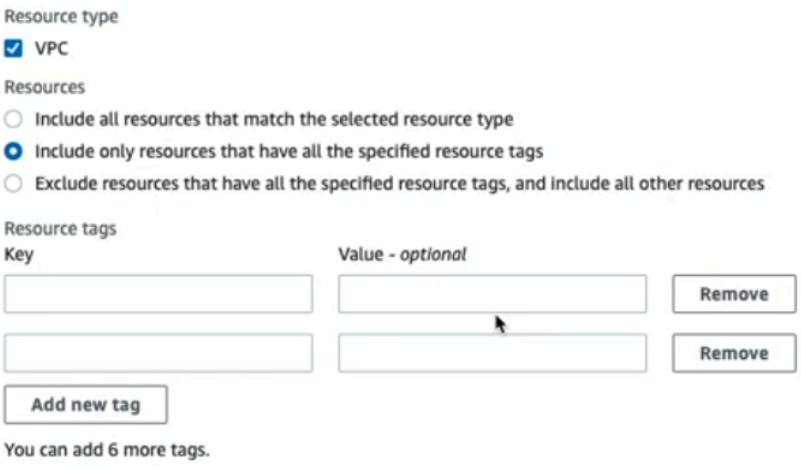
   Si vous choisissez d'inclure ou d'exclure un sous-ensemble de comptes et d'unités d'organisation, la console FMS affiche un champ qui vous permet de spécifier ces comptes et unités d'organisation. Cliquez sur **Edit List (Modifier la liste)** pour créer votre liste d'inclusion ou d'exclusion.

2. Spécifiez le VPC à inclure ou à exclure de la politique FMS Cloud NGFW.

   Comme pour les comptes et les unités d'organisation, vous pouvez sélectionner les options **Include all resources that match the selected type (Inclure toutes les ressources qui correspondent au type sélectionné)**, **Include only resources that have all the specified resource tags (Inclure uniquement les ressources qui ont toutes les étiquettes de ressource spécifiées)** ou **Exclude resources that have all the specified resource tags, and include all others (Exclure les ressources qui ont toutes les étiquettes de ressource spécifiées, et inclure toutes les autres)**.

   Si vous choisissez d'inclure ou d'exclure un sous-ensemble de VPC, la console FMS affiche des options pour fournir une liste de huit étiquettes et valeurs de ressource maximum.

3. Sous **Third Party Firewall Customer IAM Role (Rôle IAM client de pare-feu tiers)**, vous pouvez télécharger une copie du modèle CloudFormation (CFT) Cloud NGFW IAM Roles (Rôles IAM Cloud NGFW).
4. Cliquez sur **Next (Suivant)**.
5. (Facultatif) Configurez les étiquettes de la politique.

   Vous pouvez appliquer des étiquettes (composées d'une clé et d'une valeur facultative) pour vous aider à rechercher et à filtrer votre ressource Cloud NGFW créée via FMS.
6. Cliquez sur **Next (Suivant)**.
7. Vérifiez la configuration de votre politique Cloud NGFW.
8. Cliquez sur **Create Policy (Créer une politique)** pour déployer Cloud NGFW.

Activer l'accès par programmation

L’accès par programmation au Cloud NGFW vous permet de créer et de gérer des NGFW et des rulestacks à l’aide des REST API. À l’aide de ces API, vous pouvez appeler des actions sur les ressources Cloud NGFW (NGFW et rulestacks) via une application ou un outil tiers. Ces API vous permettent également d’utiliser des outils Infrastructure-as-Code (IAC) tels que les modèles CloudFormation (CFT) et les modèles Terraform. Vous pouvez installer et exécuter ces outils IaC dans des charges de travail à l’intérieur ou à l’extérieur de l’environnement AWS.

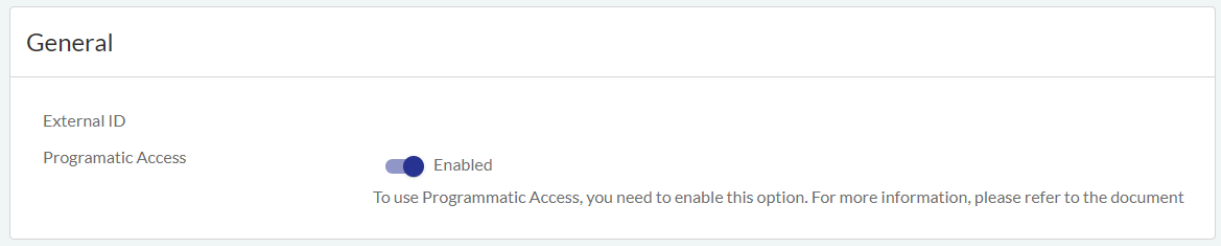
Étant donné que l’accès par programmation est puissant, Cloud NGFW ne fournit pas de clé d’accès ou de clé secrète pour signer les demandes d’autorisation. Au lieu de cela, vous pouvez utiliser le rôle IAM dans votre compte AWS pour accéder aux API Cloud NGFW, puis configurer les ressources IAM qui peuvent assumer ce rôle. Cette approche améliore la posture de sécurité générale en utilisant des informations d’identification temporaires et en les faisant pivoter automatiquement.

L’accès par programmation Cloud NGFW est désactivé par défaut.

Pour plus d’informations sur les documents de référence de l’API, consultez la documentation de l’API Cloud NGFW.

STEP 1 | Activez l’accès par programmation.

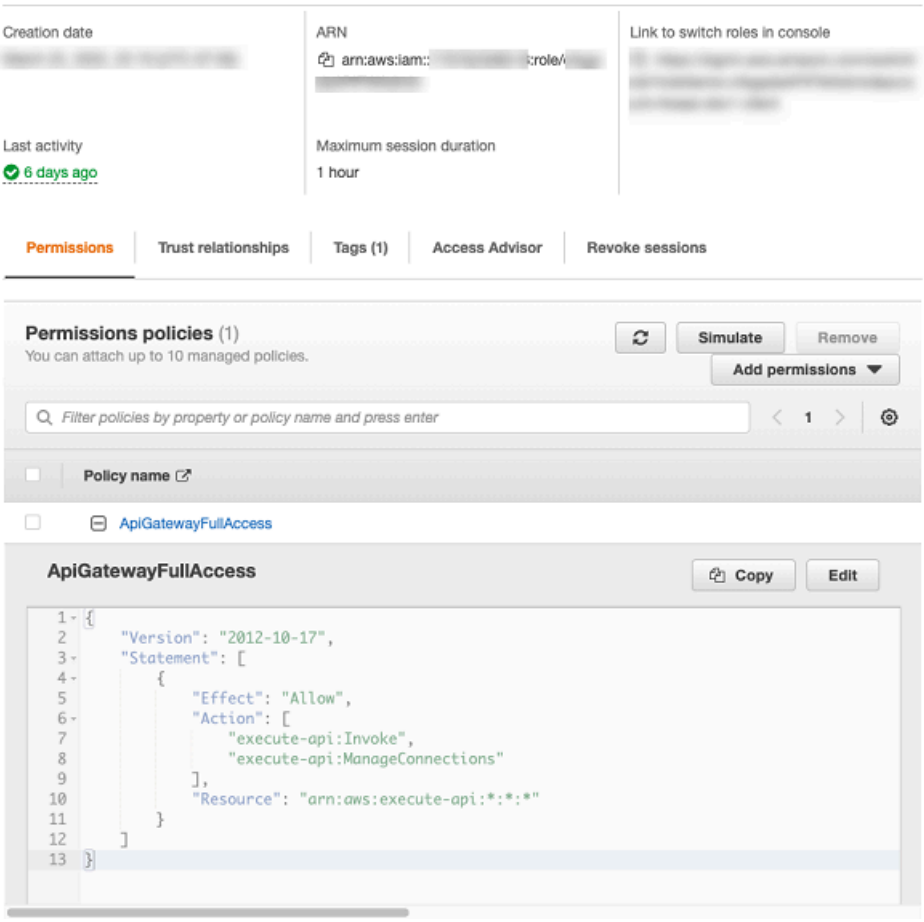
- Sélectionnez **Tenant (Locataire)** dans la console **Cloud NGFW Tenant (Locataire Cloud NGFW)**.
- Sous **General (Général)**, cliquez sur le curseur **Programmatic Access (Accès par programmation)**.
- Cliquez sur **Enable (Activer)** pour confirmer.



STEP 2 | Connectez-vous à la Console de gestion AWS et créez un rôle IAM.

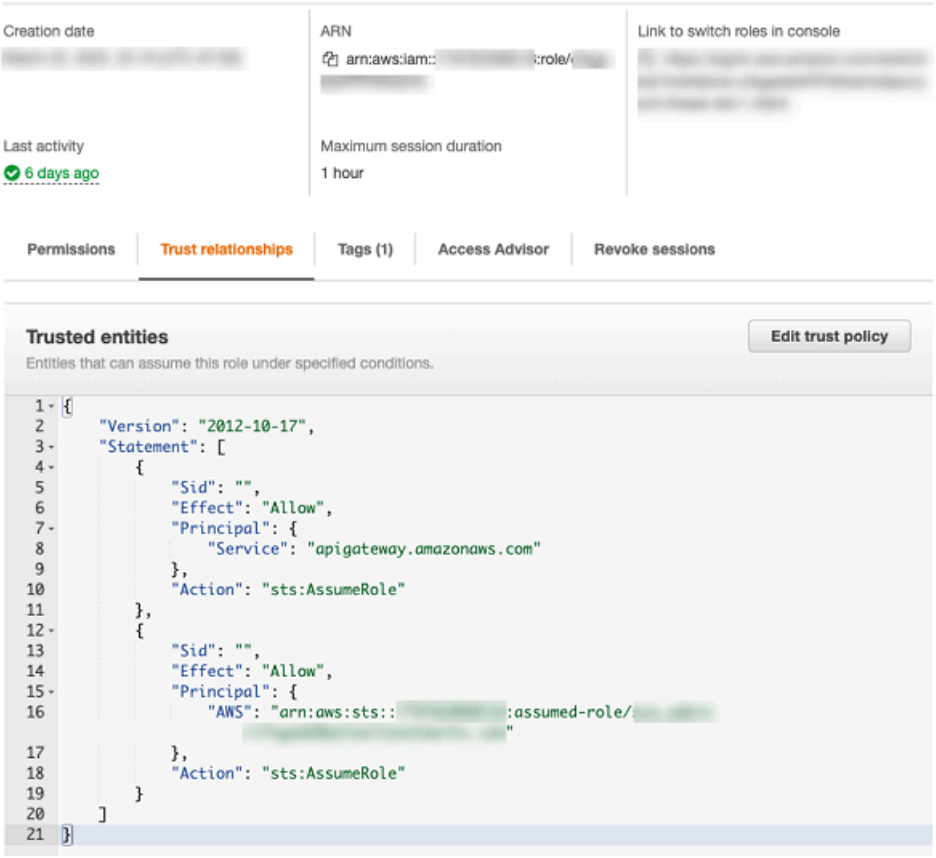
Voici la politique d'autorisation nécessaire pour activer l'accès complet à la passerelle API.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Action": "execute-api:Invoke", "Resource": "arn:aws:execute-
api:*:*:*" } ] }
```



STEP 3 | Activez l’autorisation de la passerelle API pour appeler des API.

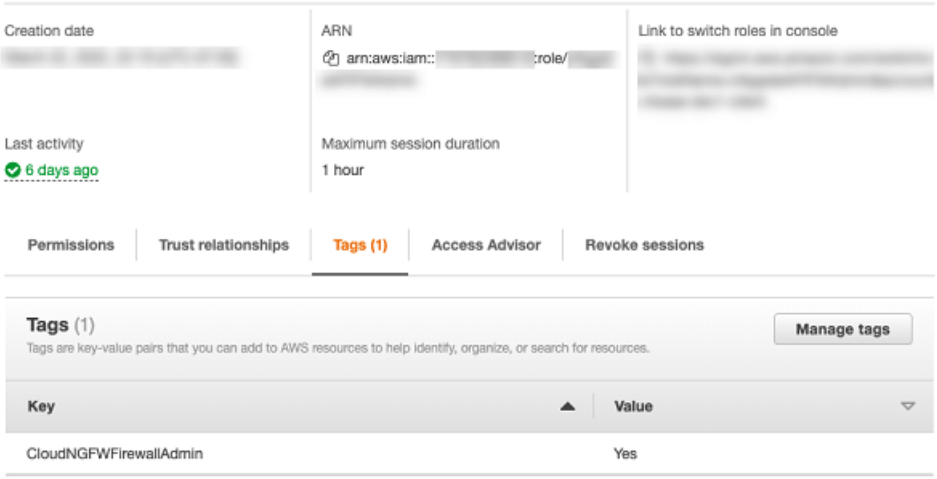
Assumez des rôles dans les conditions mentionnées dans Relations d’approbation.



STEP 4 | Ajoutez les étiquettes suivantes (composées d’une clé et d’une valeur) au rôle IAM pour fournir des politiques d’autorisation selon vos besoins.

Usage	TagKey	TagValue
Créer et gérer des pare-feu	**`CloudNGFWFirewallAdmin`**	Oui
Créer et gérer des rulestacks locales	**`CloudNGFWRulestackAdmin`**	Oui
Créer et gérer des rulestacks globales	**`CloudNGFWGlobalRulestackAdmin`**	Oui

Usage	TagKey	TagValue
Intégrer un compte AWS	`CloudNGFWGAccountAdmin`	Oui



Vous pouvez attribuer plusieurs étiquettes au même rôle. Ces étiquettes peuvent être utilisées pour accéder à différents jetons de rôle d'accès par programmation Cloud NGFW.

STEP 5 | (Ignorez les étapes 7 à 9 si vous choisissez d'utiliser les exemples d'accès par programmation Cloud NGFW) Utilisez les exemples des dossiers `API` et `CFT` sous le référentiel Git pour accéder respectivement à l'outil d'accès par programmation et aux CFT.

Téléchargez l'intégralité du répertoire `programmatic_access` pour exécuter des exemples fournis par Palo Alto Networks.

L'outil assume le rôle en interne et génère la clé d'accès et la clé secrète de votre rôle, et génère l'en-tête SigV4. Il appelle également le rôle du terminal spécifique pour obtenir un jeton d'accès par programmation pour Cloud NGFW.

STEP 6 | Assumez des rôles avec les valeurs de paire de clés d'étiquettes mentionnées à l'étape 5 selon vos besoins à l'aide de l'AWS CLI.

```
$ aws sts assume-role --role-arn arn:aws:iam::<AWS-ACCOUNT-
ID>:role/<ROLE-NAME> --profile <AWS-PROFILE-TO-ASSUME> --role-
session-name <SESSION-NAME> { "Credentials": { "AccessKeyId":
 "<ACCESS-KEY>", "SecretAccessKey": "<SECRET-ACCESS-KEY>",
 "SessionToken": "<SESSION-TOKEN>", "Expiration": "<CREDENTIALS-
EXPIRATION>" }, "AssumedRoleUser": { "AssumedRoleId": "<ROLE-
ID>:<SESSION-NAME>", "Arn": "arn:aws:iam::<AWS-ACCOUNT-ID>:role/
<ROLE-NAME>/<SESSION-NAME>" } }
```

Lorsque vous assumez le rôle, une clé d'accès et une clé secrète temporaires sont générées pour votre compte. Pour plus d'informations, voir assumer des rôles qui ont une étiquette spécifique.

STEP 7 | Générez l'en-tête SigV4 (signature version 4) à l'aide des informations d'identification temporaires obtenues à l'étape 7. Pour plus d'informations, consultez Signature de demandes AWS avec SigV4.

Voici un exemple d'en-tête signé AWS SigV4.

```
AWS4-HMAC-SHA256 Credential=<ACCESS-KEY>/20220421/<REGION>/execute-
api/aws4_request, SignedHeaders=host;x-amz-date;x-amz-security-
token, Signature=<SIGNATURE>
```

STEP 8 | Générez `SubcriptionKey` et `TokenID`.

Pour accéder à Cloud NGFW à l'aide de REST API, utilisez ce chemin avant l'appel d'API : `api.<region-name>.aws.cloudngfw.paloaltonetworks.com`. Pour plus d'informations, consultez la documentation API.

- Pour le rôle admin de pare-feu cloud : `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudfirewalladmin`
- Pour le rôle admin de la rulestack cloud : `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudrulestackadmin`
- Pour le rôle admin de la rulestack globale cloud : `GET https://api.<region-name>.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/cloudglobalrulestackadmin`

Obtenir un jeton

Voici un exemple de la commande cURL pour obtenir un jeton.

```
$ curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/mgmt/tokens/
cloudfirewalladmin' \ > --header 'X-Amz-Security-Token: <SESSION-
TOKEN>' \ > --header 'X-Amz-Date: <CREDENTIALS-EXPIRATION-AMZ-DATE-
FORMAT>' \ > --header 'Authorization: <AWS-V4-SIGNED-HEADER>'
```

Réponse

```
{"Response": {"TokenId": "<CLOUD-NGFW-PROGRAMMATIC-ACCESS-TOKEN>",
 "SubscriptionKey": "<SUBSCRIPTION-KEY>", "ExpiryTime": 30,
 "Enabled": true}, "ResponseStatus": {"ErrorCode": 0}}
```

STEP 9 | Ajoutez les données de réponse à la section **En-tête** console Cloud NGFW.

En-tête	Valeur
Autorisation	<TokenID>

En-tête	Valeur
x-api-key	<SubscriptionKey>

Voici un exemple d'appel d'API Cloud NGFW.

```
curl --location --request GET 'https://api.us-
east-1.aws.cloudngfw.paloaltonetworks.com/v1/config/rulestacks/
rs-1' \ > --header 'Authorization: <CLOUD-NGFW-PROGRAMMATIC-ACCESS-
TOKEN>' \ > --data-raw ''
```

Réponse

```
{"Response": {"RuleStackName": "rs-1", "RuleStackCandidate":
 {"Scope": "Local", "MinAppIdVersion": "8433-6838", "Profiles":
 {"AntiSpywareProfile": "BestPractice", "AntiVirusProfile":
 "BestPractice", "VulnerabilityProfile": "BestPractice",
 "URLFilteringProfile": "None", "FileBlockingProfile":
 "BestPractice"}, "UpdateToken": "1"}, "RuleStackState":
 "Uncommitted"}, "ResponseStatus": {"ErrorCode": 0}}
```

STEP 10 | Pour révoquer l'accès par programmation, utilisez la clé d'accès, la clé secrète et la clé d'abonnement pour appeler l'API de jeton : `DELETE https://:<region-name>.aws.cloudngfw.paloaltonetworks.comv1/mgmt/tokens/{TokenID}`.

La clé d'accès et la clé secrète sont temporaires. Générez une nouvelle clé d'accès et une nouvelle clé secrète si elles expirent.

Prise en charge de Terraform pour Cloud NGFW AWS

Hashicorp Terraform est un outil d'infrastructure en tant que code (IaC) open source pour les équipes gérant des environnements multi-cloud. Il vous permet de définir une configuration qui décrit l'état cible de votre infrastructure cloud et l'utilise pour calculer automatiquement les étapes nécessaires pour atteindre la cible définie tout en exécutant les modifications pertinentes pour provisionner et gérer l'infrastructure cloud. Ces configurations Terraform utilisent des plugins appelés *fournisseurs*. Les plugins interagissent avec les fournisseurs tels qu'AWS pour faciliter la réutilisation en créant des étapes reproductibles pour la construction et la maintenance de l'infrastructure cloud, garantissant des ajouts faciles à votre pipeline CI/CD.

Palo Alto Networks ajoute le fournisseur cloudngfwaws pour automatiser le processus de construction de l'infrastructure de sécurité et pour maintenir la posture de sécurité du réseau à l'aide des rulestacks NGFW. Ce fournisseur agit comme une couche de traduction qui facilite la communication entre le client (le périphérique exécutant Terraform) et les API proposées par le service Cloud NGFW pour AWS.

Visitez la documentation du développeur Palo Alto Networks pour en savoir plus sur le déploiement de Cloud NGFW sur AWS à l’aide de Terraform et consultez les informations de référence de Terraform.

Vous pouvez utiliser le fournisseur Terraform dans votre configuration pour :

- Lancez le Cloud NGFW.
- Configurez la rulestack utilisée par Cloud NGFW pour récupérer les informations de politique. La rulestack contient des informations de politique pertinentes, comme des règles de sécurité, des flux intelligents et divers objets.

Utilisez le fournisseur **cloudngfwaws** de Terraform pour accéder aux ressources de gestion du Cloud NGFW pour AWS. Le fournisseur **cloudngfwaws** s'authentifie auprès d'AWS à l'aide de la commande STS assume-role, qui génère des informations d'identification temporaires. Ces informations d'identification temporaires, utilisées brièvement lors de la séquence d'authentification initiale, incluent la clé d'accès, la clé secrète et un jeton de session. Au cours de cette séquence :

1. L’authentification exploite le rôle d’assumer AWS STS à l’aide de l’API AWS. Vous devez activer l'accès à l'API.
2. Les informations d'identification STS sont utilisées pour actualiser le jeton admin Cloud NGFW à l'aide de l'API Cloud NGFW pour AWS. Ces informations d'identification sont également utilisées pour actualiser le jeton admin de la rulestack.
3. Le jeton admin Cloud NGFW et le jeton admin de la rulestack sont utilisés pour la gestion de la configuration à l’aide de l’API Cloud NGFW pour AWS.

Notez bien :

- Une fois l’authentification réussie auprès d’AWS, le fournisseur récupère les JWT pour l’administration du pare-feu et de la rulestack.
- Vous pouvez spécifier de manière statique l’accès AWS et la clé secrète dans le bloc de fournisseur. Si vous ne spécifiez pas ces informations d'identification, elles sont automatiquement extraites du fichier d'informations d'identification partagé. Utilisez les paramètres access_key et secret_key pour fournir de manière statique les informations d’identification AWS.
- Lors de la configuration du fournisseur, le flux de travail d’authentification AWS utilise le kit SDK AWS Go pour contrôler les variables liées à l’authentification. Vous pouvez utiliser des variables

d’environnement AWS pour configurer les informations d’identification utilisées pour l’authentification AWS.

- Le fournisseur exige un accès à l’API.

Les paramètres du fournisseur sont priorisés de différentes manières. En présence de valeurs qui se chevauchent, ces paramètres sont traités dans l’ordre suivant :

1. Configurés de manière statique dans le bloc fournisseur.
2. Variables d'environnement.
3. Récupérés dans le fichier de configuration JSON.

Exemple de fournisseur Terraform pour Cloud NGFW

Terraform 0.13 et versions ultérieures :

```
terraform { required_providers { cloudngfwaws = { source =
 "paloaltonetworks/terraform-provider-cloudngfwaws" version
 = "1.0.0" } } } provider "cloudngfwaws" { json_config_file =
 "~/.cloudngfwaws_creds.json" }
```

Fichier de configuration JSON :

```
{ "host": "api.us-east-1.aws.cloudngfw.paloaltonetworks.com",
 "region": "us-east-1", "arn": "arn:aws:iam::123456789:role/MyRole" }
```


Provisionner des ressources Cloud NGFW sur votre AWS CFT

Le Cloud NGFW offre la flexibilité nécessaire pour allouer des ressources à votre modèle AWS CloudFormation (CFT) en vous permettant de créer vos propres ressources.

Vous devez activer l'accès par programmation avant d'utiliser CloudFormation Registry avec Cloud NGFW.

Utilisez les schémas **PaloAltoNetworks::CloudNGFW::RuleStack** et **PaloAltoNetworks::CloudNGFW::NGFW** pour intégrer le Cloud NGFW dans votre modèle AWS CloudFormation. Utilisez la syntaxe fournie dans ce document pour définir les paramètres de configuration du pare-feu Cloud NGFW que vous pouvez intégrer au registre d'AWS CloudFormation.

Schéma PaloAltoNetworks::CloudNGFW::RuleStack

- JSON

```
{ "Type" : "PaloAltoNetworks::CloudNGFW::RuleStack", "Properties" :
 { "RuleStackName" : String, "RuleStack" : RuleStack,
 "RuleList" : [ Rule, ... ], "SecurityObjects" : SecurityObjects,
 "CustomSecurityProfiles":CustomSecurityProfiles, } }
```

- YAML

```
Type:PaloAltoNetworks::CloudNGFW::RuleStack Properties:
 RuleStackName: String RuleStack: RuleStack RuleList: - Rule
 SecurityObjects: SecurityObjects CustomSecurityProfiles:
 CustomSecurityProfiles ProgrammaticAccessToken: Chaîne
```

Élément	Description

RuleStackName	Entrez un **nom** descriptif pour votre rulestack.
	JSON
	`“RuleStackName” : String,`
	YAML
	`RuleStackName: String`

RuleStack	Saisissez une **description** pour votre rulestack. La description comprend : **JSON** `{ "Scope" : String, "Profiles" : RuleStackProfiles, "Description" : String "Deploy" : String }`

Élément	Description
	YAML `Scope: String Profiles: RuleStackProfiles Description: String Deploy: String`

RuleStackProfiles	Identifiez les **profils** pour la rulestack spécifiée. Les profils comprennent :
	JSON
	`{ "AntiSpywareProfile" : String, "AntiVirusProfile" : String, "VulnerabilityProfile" : String, "URLFilteringProfile" : String, "FileBlockingProfile" : String, "OutboundTrustCertificate" : String, "OutboundUntrustCertificate" : String }`
	YAML
	`AntiSpywareProfile: String AntiVirusProfile: String VulnerabilityProfile: String URLFilteringProfile: String FileBlockingProfile: String OutboundTrustCertificate: String OutboundUntrustCertificate: String`

rule	Établissez des **règles** pour la rulestack. Les règles comprennent : **JSON** `{ "RuleName" : String, "Description" : String, "RuleListType" : String, "Priority" : Integer, "Enabled" : Boolean, "Source" : RuleSource, "NegateSource" : Boolean, "Destination" : RuleDestination, "NegateDestination" : Boolean, "Applications" : [String, ...], "Category" : UrlCategory, "Protocol" : String, "AuditComment" : String, "Action" : String, "Logging" : Boolean, "DecryptionRuleType" : String, "Tags" : [Tag, ...] }` **YAML** `RuleName: String Description: String RuleListType: String Priority: Integer Enabled: Boolean Source: RuleSource NegateSource: Boolean Destination: RuleDestination NegateDestination: Boolean Applications: - String Category: UrlCategory Protocol: String AuditComment: String Action: String Logging: Boolean DecryptionRuleType: String Tags: - Tag`

Élément	Description

RuleSource	Définissez la collection de règles à l'aide de **RuleSource**. RuleSource comprend :
	
	JSON
	`{ "Cidrs" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }`
	
	YAML
	`cidrs: - String PrefixLists: - String Countries: - String Feeds: - String`

RuleDestination	Définissez **RuleDestination** pour le service Web prenant en charge l'URL de confirmation et une ou plusieurs URL de collecte de données. RuleDestination comprend :
	
	JSON
	`{ "Cidrs" : [ String, ... ], "FqdnLists" : [ String, ... ], "PrefixLists" : [ String, ... ], "Countries" : [ String, ... ], "Feeds" : [ String, ... ] // RuleStackname? }`
	
	YAML
	`Cidrs: - String FqdnLists: - String PrefixLists: - String Countries: - String Feeds: - String`

Étiquette	Spécifiez une **étiquette** pour la rulestack. Une étiquette comprend :
	
	JSON
	`{ "Key" : String, "Value" : String }`
	
	YAML
	`Key: String Value: String`

UrlCategory	Utilisez **UrlCategory** pour faire correspondre les critères des règles d'authentification, de décryptage, de QoS et de politique de sécurité. UrlCategory comprend : **JSON** `{ "URLCategoryNames" : [ String, ... ], "Feeds" : [ String, ... ] }`

Élément	Description
	YAML `URLCategoryNames: - String Feeds: - String`

SecurityObjects	Définissez **SecurityObjects** pour la rulestack. Les SecurityObjects comprennent :
	JSON
	`{ "PrefixLists" : PrefixList, "FqdnLists" : FqdnList, "CustomUrlCategories" : CustomUrlCategory, "IntelligentFeeds" : IntelligentFeed, "CertificateLists" : CertificateList }`
	YAML
	`PrefixList: PrefixList FqdnList: FqdnList CustomUrlCategory: CustomUrlCategory IntelligentFeed: IntelligentFeed CertificateList: CertificateList`

CustomSecurityProfiles	Définissez **CustomSecurityProfiles** pour limiter les inspections antivirus sur le trafic entre des zones de sécurité de confiance ou au contraire les renforcer sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs. Les CustomSecurityProfiles comprennent :
	JSON
	`{ "FileBlocking" : FileBlocking }`
	YAML
	`FileBlocking: FileBlocking`

PrefixLists	Utilisez **PrefixList** pour filtrer les itinéraires en fonction des préfixes. En définissant un numéro de commande et des préfixes IP, une succursale ou un périphérique ION de centre de données peut autoriser ou refuser des itinéraires. La liste de préfixes dynamique générée automatiquement est basée sur ce que le périphérique ION annonce. Les préfixes peuvent être fractionnés ou non. Une PrefixList comprend : **JSON** `{ "Name" : String, "PrefixList" : [ String, ... ], "AuditComment" : String, "Description" : String }`

Élément	Description
	YAML `Name: String PrefixList: - String AuditComment: String Description: String`

FqdnLists	Avec l'objet **FqdnLists**, le DNS fournit la résolution FQDN aux adresses IP, éliminant ainsi le besoin de connaître les adresses IP et les mettant à jour manuellement chaque fois que le FQDN est résolu en une nouvelle adresse IP. Les FqdnLists incluent :
	JSON
	`{ "Name" : String, "Description" : String, "FqdnList" : [ String, ... ], "AuditComment" : String }`
	YAML
	`Name: String Description: String FqdnList : - String AuditComment: String`

CustomUrlCategories	Utilisez **CustomURLCategories** pour créer un objet de filtrage des URL personnalisé afin de spécifier des exceptions à l'application des catégories d'URL et pour créer une catégorie d'URL personnalisée basée sur plusieurs catégories d'URL : • Définir des exceptions à l'application de la catégorie d'URL : créez une liste personnalisée d'URL que vous souhaitez utiliser comme critères de correspondance dans une règle de politique de sécurité. C'est une bonne façon de spécifier des exceptions à des catégories d'URL, lorsque vous aimeriez appliquer des URL spécifiques différemment de la catégorie d'URL à laquelle elles appartiennent. • Définir une catégorie d'URL personnalisée en fonction de plusieurs catégories PAN-DB : cette option vous permet de cibler l'application pour des sites Web qui correspondent à un ensemble de catégories. Le site ou la page Web doivent faire correspondre l'ensemble des catégories définies dans le cadre de la catégorie personnalisée. Les CustomURLCategories incluent : **JSON** `{ "URLTargets" : [ String, ... ], "Name" : String, "Description" : String, "Action" : String, "AuditComment" : String }`

Élément	Description
	YAML `URLTargets: - String Name: String Description: String Action: String AuditComment: String`

IntelligentFeeds	Utilisez **IntelligentFeeds** pour alimenter en permanence les données de renseignement sur les menaces les plus récentes. Les IntelligentFeeds incluent :
	JSON
	`{ "Name" : String, "Description" : String, "Certificate" : String, "FeedURL" : String, "Type" : String, "Frequency" : String, "Time" : Integer, "AuditComment" : String }`
	YAML
	`Name: String Description: String Certificate: String FeedURL: String Type: String Frequency: String Time: Integer AuditComment: String`

CertificateObjects	Utilisez **CertificateObjects** pour définir les éléments du certificat. Les CertificateObjects incluent :
	JSON
	`{ "Name" : String, "Description" : String, "CertificateSignerArn" : String, "CertificateSelfSigned" : Boolean, "AuditComment" : String }`
	YAML
	`Name: String Description: String CertificateSignerArn: String CertificateSelfSigned: Boolean AuditCommentaire: String`

FileBlocking	Utilisez **FileBlocking** pour identifier les types de fichiers spécifiques que vous souhaitez bloquer ou surveiller. Pour la plupart du trafic (y compris le trafic sur votre réseau interne), vous devrez bloquer les fichiers qui comportent généralement des menaces ou qui n'ont pas besoin d'être chargés ou téléchargés. FileBlocking comprend :

Élément	Description

	JSON
	`{ "Direction" : String, "FileType" : String, "Description" : String, "Action" : String, "AuditComment" : String }`
	YAML
	`Direction: String FileType: String Description: String Action: String AuditComment: String`

Schéma PaloAltoNetworks::CloudNGFW::NGFW

- JSON

```
{ "Type": "PaloAltoNetworks::CloudNGFW::NGFW", "Properties" :
 { "Description" : String, "EndpointMode" : String,
 "FirewallName" : String, "RuleStackName" : String,
 "RuleStackName" : String, "SubnetMappings" : [ String, ... ],
 "Tags" : [ Map, ... ], "VpcId" : String, "UpdateToken" :
 String, "LogDestinationConfigs" : [ LogProfileConfig, ... ],
 "CloudWatchMetricNamespace" : String, }
```

- YAML

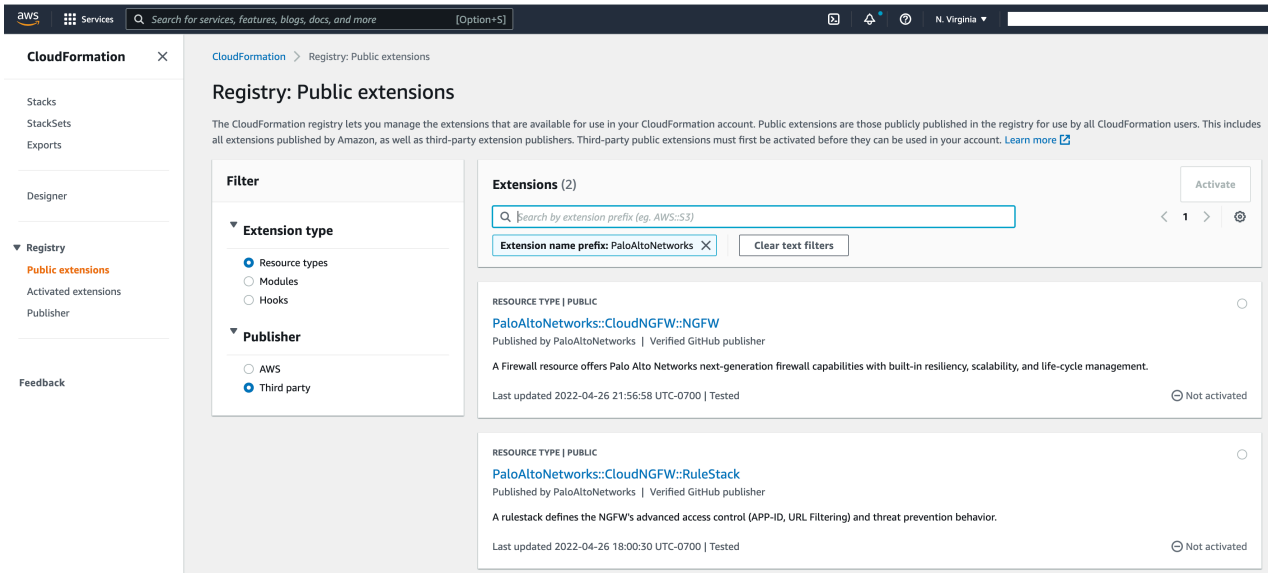
```
Type : PaloAltoNetworks::CloudNGFW::NGFWProperties: AppIdVersion:
 String AutomaticUpgradeAppIdVersion: Boolean Description:
 String EndpointMode: String FirewallName: String RuleStackName:
 String RuleStackName: String SubnetMappings: - String Tags: -
 Map VpcId: String UpdateToken: String LogDestinationConfigs:
 - LogProfileConfig CloudWatchMetricNamespace: String
 ProgrammaticAccessToken: Chaîne
```

Élément	Description

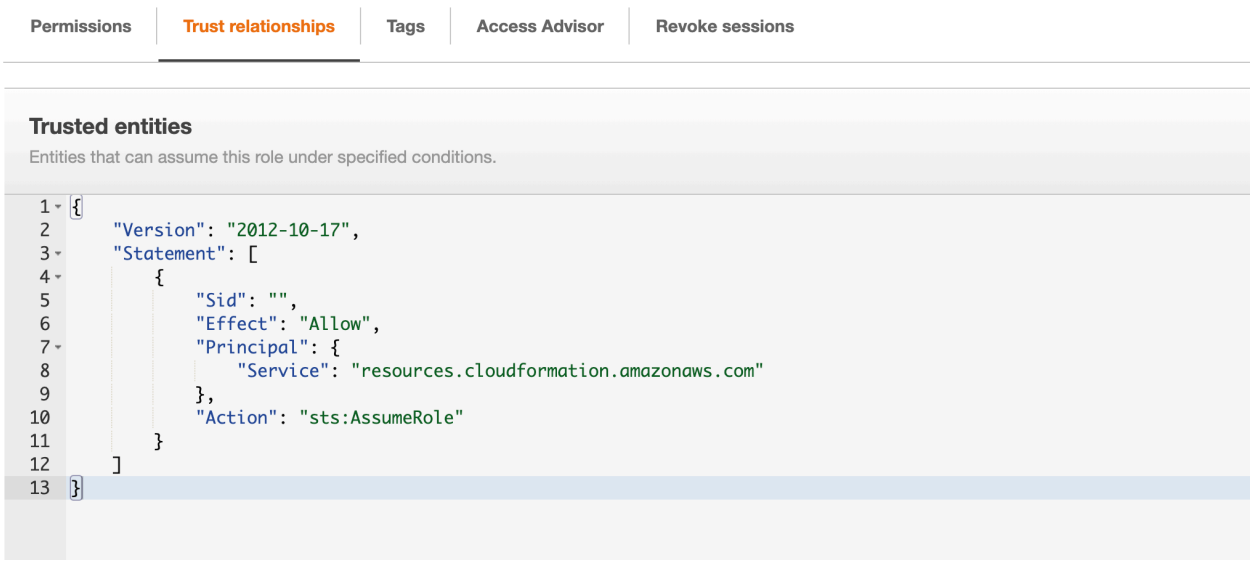
LogProfileConfig	Utilisez **LogProfileConfig** pour afficher les entrées permettant de modifier la configuration du pare-feu.
	JSON
	`{ "LogDestination" : String, "LogDestinationType" : String, "LogType" : String}`
	YAML
	`LogDestination: String LogDestinationType: String LogType: String`

Activer les extensions publiques

Activez les extensions publiques **PaloAltoNetworks::CloudNGFW::NGFW** et **PaloAltoNetworks::CloudNGFW::RuleStack** pour votre compte :



Créez un ARN de rôle d’exécution pour les extensions. Les deux extensions peuvent utiliser le même rôle. Établissez des relations d’approbation dans le rôle pour utiliser les modèles Cloud Formation :



Après avoir établi la relation d’approbation, activez les extensions :

Pour expédier des journaux dans AWS CloudWatch, consultez Configurer la journalisation pour Cloud NGFW sur AWS.

Sorties de pile

Vous pouvez accéder à ces attributs de ressources en tant que sorties de pile :

```
FirewallResource: "/properties/ReadFirewall", "/properties/
ReadFirewall/AccountId", "/properties/ReadFirewall/AppIdVersion",
 "/properties/ReadFirewall/AutomaticUpgradeAppIdVersion", "/
properties/ReadFirewall/EndpointMode", "/properties/ReadFirewall/
FirewallName", "/properties/ReadFirewall/MultiVpcEnable", "/
properties/ReadFirewall/Description", "/properties/ReadFirewall/
VpcId", "/properties/ReadFirewall/SubnetMappings", "/properties/
ReadFirewall/LinkId", "/properties/ReadFirewall/Attachments", "/
properties/ReadFirewall/LinkStatus", "/properties/ReadFirewall/
FirewallStatus", "/properties/ReadFirewall/RuleStackStatus",
 "/properties/ReadFirewall/FailureReason", "/properties/
```



```
ReadFirewall/EndpointServiceName", "/properties/ReadFirewall/
Tags", "/properties/ReadFirewall/RuleStackName", "/properties/
ReadFirewall/GlobalRuleStackName" RuleStackResource: "/properties/
RuleStackCandidate", "/properties/RuleStackRunning", "/properties/
RuleStackCandidate/AccountId", "/properties/RuleStackRunning/
AccountId", "/properties/RuleStackCandidate/Scope", "/properties/
RuleStackRunning/Scope", "/properties/RuleStackCandidate/
MinAppIdVersion", "/properties/RuleStackRunning/MinAppIdVersion",
 "/properties/RuleStackCandidate/Description", "/properties/
RuleStackRunning/Description", "/properties/RuleStackRunning/
Profiles/AntiSpywareProfile", "/properties/RuleStackCandidate/
Profiles/AntiSpywareProfile", "/properties/RuleStackRunning/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/
Profiles/AntiVirusProfile", "/properties/RuleStackCandidate/Profiles/
VulnerabilityProfile", "/properties/RuleStackRunning/Profiles/
VulnerabilityProfile", "/properties/RuleStackCandidate/Profiles/
URLFilteringProfile", "/properties/RuleStackRunning/Profiles/
URLFilteringProfile", "/properties/RuleStackCandidate/Profiles/
FileBlockingProfile", "/properties/RuleStackRunning/Profiles/
FileBlockingProfile
```

Rôle d’exécution

Utilisez le code suivant pour le rôle d’exécution :

Relation de confiance :

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "Service":
 "resources.cloudformation.amazonaws.com" }, "Action":
 "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": "{customer-account-id}" },
 "StringLike": { "aws:SourceArn": "arn:aws:cloudformation:*:
{customer-account-id}":type/resource/PaloAltoNetworks-
CloudNGFW-NGFW/*" } } }, { "Effect": "Allow", "Principal":
 { "Service": "resources.cloudformation.amazonaws.com" },
 "Action": "sts:AssumeRole", "Condition": { "StringEquals":
 { "aws:SourceAccount": {customer-account-id}" }, "StringLike":
 { "aws:SourceArn": "arn:aws:cloudformation:*:{customer-
account-id}":type/resource/PaloAltoNetworks-CloudNGFW-
RuleStack/*" } } } ] } Tags: CloudNGFWRulestackAdmin: Yes
 CloudNGFWFirewallAdmin: Yes CloudNGFWGlobalRulestackAdmin: Yes
 Permissions: AmazonAPIGatewayInvokeFullAccess
```

Créez un rôle, puis utilisez l’ARN du rôle pour configurer l’ARN du rôle d’exécution au cours de l’activation. Vous ne pouvez pas créer une ressource sans configurer le rôle d’exécution durant l’activation.

Exemple de schéma de ressources de pare-feu CloudFormation

Utilisez le code suivant comme exemple pour le schéma de la rulestack :

```
{ "typeName": "PaloAltoNetworks::CloudNGFW::NGFW", "description":
 "Une ressource de pare-feu offre des capacités de pare-feu
 nouvelle génération de Palo Alto Networks avec une résilience,
```



```
 une évolutivité et une gestion du cycle de vie intégrées.",
 "sourceUrl": "https://github.com/aws-cloudformation/aws-
cloudformation-rpdk.git", "definitions" : { "LogProfileConfig":
 { "title": "LogProfileConfig", "description": "Ajouter une
 configuration de profil de journal", "type": "object", "properties":
 { "LogDestination": { "title": "Logdestination", "minLength":
 1, "maxLength": 128, "type": "string" }, "LogDestinationType":
 { "title": "Logdestinationtype", "enum": ["S3", "CloudWatchLogs",
 "KinesisDataFirehose"], "type": "string" }, "LogType": { "title":
 "Logtype", "enum": ["TRAFFIC", "DECRYPTION", "THREAT"], "type":
 "string" } }, "required": ["LogDestination", "LogDestinationType",
 "LogType"], "additionalProperties": false }, "SubnetMappings":
 { "type": "array", "items": { "type": "object", "properties":
 { "AvailabilityZone": { "title": "availabilityZone", "type":
 "string" }, "SubnetId": { "title": "subnetId", "type": "string" } },
 "additionalProperties": false } } }, "properties": { "AccountId":
 { "title": "Accountid", "pattern": "^[0-9]+$", "type": "string",
 "minLength": 1 }, "AppIdVersion": { "title": "Appidversion",
 "minLength": 1, "maxLength": 64, "pattern": "^[0-9]+-[0-9]+
$", "type": "string" }, "AutomaticUpgradeAppIdVersion":
 { "title": "Automaticupgradeappidversion", "default": true,
 "type": "boolean" }, "Description": { "title": "Description",
 "type": "string", "minLength": 1 }, "EndpointMode": { "title":
 "Endpointmode: CustomerManaged Or ServiceManaged", "enum":
 ["ServiceManaged", "CustomerManaged"], "type": "string" },
 "FirewallName": { "title": "Firewallname", "minLength": 1,
 "maxLength": 128, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" },
 "MultiVpcEnable": { "title": "MultiVpcEnable", "type": "boolean" },
 "RuleStackName": { "title": "Rulestackname", "type": "string",
 "minLength": 1 }, "SubnetMappings": { "$ref": "#/definitions/
SubnetMappings" }, "AssociateSubnetMappings": { "$ref": "#/
definitions/SubnetMappings" }, "DisassociateSubnetMappings":
 { "$ref": "#/definitions/SubnetMappings" }, "Tags": { "title":
 "Tags", "type": "array", "items": { "type": "object" } },
 "VpcId": { "title": "Vpcid", "type": "string", "minLength": 1 },
 "LinkId": { "title": "LinkId", "type": "string", "minLength": 1 },
 "LogDestinationConfigs": { "title": "Logdestinationconfigs", "type":
 "array", "items": { "$ref": "#/definitions/LogProfileConfig" } },
 "CloudWatchMetricNamespace": { "title": "Cloudwatchmetricnamespace",
 "type": "string", "minLength": 1 } }, "additionalProperties":
 false, "required": [ "FirewallName" ], "createOnlyProperties": [ "/
properties/FirewallName" ], "primaryIdentifier": [ "/properties/
FirewallName" ], "handlers": { "create": { "permissions": [ "execute-
api:Invoke" ] }, "read": { "permissions": [ "execute-api:Invoke" ] },
 "update": { "permissions": [ "execute-api:Invoke" ] }, "delete":
 { "permissions": [ "execute-api:Invoke" ] } } }
```

Exemple de schéma de rulestack

Utilisez le code suivant comme exemple pour le schéma de rulestack :

```
{ "typeName": "PaloAltoNetworks::CloudNGFW::RuleStack",
 "description": "Une rulestack définit le contrôle d’accès
 avancé du NGFW (APP-ID, filtrage des URL) et le comportement
 de prévention des menaces.", "sourceUrl": "https://github.com/
aws-cloudformation/aws-cloudformation-rpdk.git", "definitions":
```



```
 { "RuleStack": { "title": "RuleStack", "type": "object",
 "properties": { "AccountId": { "title": "Accountid", "pattern":
 "^[0-9]+$", "type": "string", "minLength": 1 }, "Scope": { "title":
 "Scope", "default": "Local", "enum": ["Local", "Global"], "type":
 "string" }, "LookupXForwardedFor": { "title": "LookupXForwardedFor",
 "default": "None", "enum": ["SecurityPolicy", "None"], "type":
 "string" }, "MinAppIdVersion": { "title": "Minappidversion",
 "default": "8433-6838", "pattern": "8\\d\\d\\d\\-\\d\\d\\d\
\d", "type": "string" }, "Profiles": { "$ref": "#/definitions/
RuleStackProfiles" }, "Description": { "title": "Description",
 "maxLength": 512, "type": "string" }, "Deploy": { "title": "Deploy",
 "description": "Deploy RuleStack YES/NO", "default": "YES", "type":
 "string" } }, "additionalProperties": false }, "RuleStackProfiles":
 { "title": "RuleStackProfiles", "type": "object", "properties":
 { "AntiSpywareProfile": { "title": "Antispywareprofile", "default":
 "BestPractice", "enum": ["BestPractice", "None"], "type":
 "string" }, "AntiVirusProfile": { "title": "Antivirusprofile",
 "default": "BestPractice", "enum": ["BestPractice", "None"],
 "type": "string" }, "VulnerabilityProfile": { "title":
 "Vulnerabilityprofile", "default": "BestPractice", "enum":
 ["BestPractice", "None"], "type": "string" }, "URLFilteringProfile":
 { "title": "Urlfilteringprofile", "default": "None", "enum":
 ["BestPractice", "None"], "type": "string" }, "FileBlockingProfile":
 { "title": "Fileblockingprofile", "default": "BestPractice",
 "enum": ["Custom", "BestPractice", "None"], "type": "string" },
 "OutboundTrustCertificate": { "title": "Outboundtrustcertificate",
 "maxLength": 63, "type": "string" }, "OutboundUntrustCertificate":
 { "title": "Outbounduntrustcertificate", "maxLength": 63, "type":
 "string" } }, "additionalProperties": false }, "Tag": { "title":
 "Tag", "type": "object", "properties": { "Key": { "title": "Key",
 "minLength": 1, "maxLength": 128, "type": "string" }, "Value":
 { "title": "Value", "minLength": 1, "maxLength": 128, "type":
 "string" } }, "required": ["Key", "Value"], "additionalProperties":
 false }, "Rule" : { "title": "Rule", "type": "object", "properties":
 { "RuleName": { "title": "Rulename", "minLength": 1, "maxLength":
 48, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "Description":
 { "title": "Description", "maxLength": 512, "type": "string" },
 "RuleListType": { "title": "RuleListType", "description":
 "RuleList type: LocalRule, PreRule, PostRule", "type": "string" },
 "Priority": { "title": "Priority", "description": "Priority of
 the Rule", "type": "integer" }, "Enabled": { "title": "Enabled",
 "default": true, "type": "boolean" }, "Source": { "$ref": "#/
definitions/RuleSource" }, "NegateSource": { "title": "Negatesource",
 "default": false, "type": "boolean" }, "Destination": { "$ref":
 "#/definitions/RuleDestination" }, "NegateDestination": { "title":
 "Negatedestination", "default": false, "type": "boolean" },
 "Applications": { "title": "Applications", "default": ["any"],
 "type": "array", "items": { "type": "string", "maxLength":
 63 } }, "Category": { "$ref": "#/definitions/UrlCategory" },
 "Protocol": { "title": "Protocol", "default": "application-default",
 "maxLength": 63, "type": "string" }, "ProtPortList": { "title":
 "ProtPortList", "type": "array", "items": { "type": "string",
 "maxLength": 63 } }, "AuditComment": { "title": "Auditcomment",
 "maxLength": 512, "type": "string" }, "Action": { "title":
 "Action", "default": "Allow", "enum": ["Allow", "DenySilent",
 "DenyResetServer", "DenyResetBoth"], "type": "string" },
```



```
 "Logging": { "title": "Logging", "default": false, "type":
 "boolean" }, "DecryptionRuleType": { "title": "Decryptionruletype",
 "enum": ["SSLOutboundInspection", "SSLInboundInspection",
 "SSLOutboundNoInspection", "SSLInboundNoInspection"], "type":
 "string" }, "InboundInspectionCertificate": { "title":
 "InboundInspectionCertificate", "type": "string", "maxLength":
 63 }, "Tags": { "title": "Tags", "maxItems": 200, "type":
 "array", "items": { "$ref": "#/definitions/Tag" } } }, "required":
 ["RuleName", "RuleListType", "Priority"], "additionalProperties":
 false }, "RuleSource": { "title": "RuleSource", "type": "object",
 "properties": { "Cidrs": { "title": "Cidrs", "type": "array",
 "items": { "type": "string", "maxLength": 24 } }, "PrefixLists":
 { "title": "Prefixlists", "type": "array", "items": { "type":
 "string", "maxLength": 63 } }, "Countries": { "title": "Countries",
 "description": "Country code", "type": "array", "items": { "type":
 "string", "maxLength": 2 } }, "Feeds": { "title": "Feeds", "type":
 "array", "items": { "type": "string", "maxLength": 63 } } },
 "additionalProperties": false }, "RuleDestination": { "title":
 "RuleDestination", "type": "object", "properties": { "Cidrs":
 { "title": "Cidrs", "type": "array", "items": { "type": "string",
 "maxLength": 24 } }, "FqdnLists": { "title": "Fqdnlists", "type":
 "array", "items": { "type": "string", "maxLength": 63 } },
 "PrefixLists": { "title": "Prefixlists", "type": "array", "items":
 { "type": "string", "maxLength": 63 } }, "Countries": { "title":
 "Countries", "description": "Country code", "type": "array",
 "items": { "type": "string", "maxLength": 2 } }, "Feeds": { "title":
 "Feeds", "type": "array", "items": { "type": "string", "maxLength":
 63 } } }, "additionalProperties": false }, "UrlCategory": { "title":
 "UrlCategory", "type": "object", "properties": { "URLCategoryNames":
 { "title": "Urlcategorynames", "type": "array", "items": { "type":
 "string", "maxLength": 128 } }, "Feeds": { "title": "Feeds",
 "type": "array", "items": { "type": "string", "maxLength":
 63 } } }, "additionalProperties": false }, "CustomSecurityProfiles":
{ "description": "Objet Profils de sécurité personnalisés", "type":
 "object", "properties": { "FileBlocking": { "$ref": "#/definitions/
FileBlocking" } }, "additionalProperties": false }, "FileBlocking":
{ "title": "FileBlocking", "type": "object", "properties":
 { "Direction": { "title": "Direction", "default": "both", "enum":
 ["upload", "download", "both"], "type": "string" }, "FileType":
 { "title": "FileType", "type": "string" }, "Description": { "title":
 "Description", "minLength": 1, "maxLength": 255, "type": "string" },
 "Action": { "title": "Action", "default": "alert", "enum":
 ["alert", "block", "continue"], "type": "string" }, "AuditComment":
 { "title": "Auditcomment", "type": "string" } }, "required":
 ["FileType"], "additionalProperties": false }, "SecurityObjects":
 { "description": "Security objects", "type": "object", "properties":
 { "PrefixLists": { "type": "array", "uniqueItems": false,
 "items": { "$ref": "#/definitions/PrefixList" } }, "FqdnLists":
 { "type": "array", "uniqueItems": false, "items": { "$ref":
 "#/definitions/FqdnList" } }, "CustomUrlCategories": { "type":
 "array", "uniqueItems": false, "items": { "$ref": "#/definitions/
CustomUrlCategory" } }, "IntelligentFeeds": { "type": "array",
 "uniqueItems": false, "items": { "$ref": "#/definitions/
IntelligentFeed" } }, "CertificateObjects":{ "type": "array",
 "uniqueItems": false, "items": { "$ref": "#/definitions/
CertObject" } } }, "additionalProperties": false }, "PrefixList":
```



```
 { "title": "PrefixList", "description": "SecurityObjects
 PrefixList", "type": "object", "properties": { "Name": { "title":
 "Name", "minLength": 1, "maxLength": 58, "pattern": "^[a-
zA-Z0-9-]+$", "type": "string" }, "PrefixList": { "title":
 "Prefixlist", "type": "array", "items": { "type": "string" } },
 "AuditComment": { "title": "Auditcomment", "maxLength": 512,
 "type": "string" }, "Description": { "title": "Description",
 "maxLength": 512, "type": "string" } }, "required": ["Name",
 "PrefixList"], "additionalProperties": false }, "FqdnList":
{ "title": "FqdnList", "type": "object", "properties": { "Name":
 { "title": "Name", "minLength": 1, "maxLength": 58, "pattern":
 "^[a-zA-Z0-9-]+$", "type": "string" }, "Description": { "title":
 "Description", "maxLength": 512, "type": "string" }, "FqdnList":
 { "title": "Fqdnlist", "type": "array", "items": { "type": "string",
 "minLength": 1, "maxLength": 255, "pattern": "^[a-zA-Z0-9._-]+
$" } }, "AuditComment": { "title": "Auditcomment", "maxLength":
 512, "type": "string" } }, "required": ["Name", "FqdnList"],
 "additionalProperties": false }, "CustomUrlCategory":{ "title":
 "CustomURLCategory", "type": "object", "properties": { "URLTargets":
 { "title": "Urltargets", "type": "array", "items": { "type":
 "string", "minLength": 1, "maxLength": 255 } }, "Name": { "title":
 "Name", "minLength": 1, "maxLength": 58, "pattern": "^[a-zA-Z0-9-]+
$", "type": "string" }, "Description": { "title": "Description",
 "minLength": 1, "maxLength": 255, "type": "string" }, "Action":
 { "title": "Action", "type": "string", "default": "none", "enum":
 ["none", "allow", "alert", "block"] }, "AuditComment": { "title":
 "Auditcomment", "type": "string" } }, "required": ["URLTargets"],
 "additionalProperties": false }, "IntelligentFeed":{ "title":
 "IntelligentFeed", "type": "object", "properties": { "Name":
 { "title": "Name", "minLength": 1, "maxLength": 63, "pattern":
 "^[a-zA-Z0-9-]+$", "type": "string" }, "Description": { "title":
 "Description", "maxLength": 512, "type": "string" }, "Certificate":
 { "title": "Certificate", "type": "string" }, "FeedURL": { "title":
 "Feedurl", "minLength": 1, "maxLength": 255, "pattern": "^(http|
https)://.+$", "type": "string" }, "Type": { "title": "Type",
 "enum": ["IP_LIST", "URL_LIST"], "type": "string" }, "Frequency":
 { "title": "Frequency", "enum": ["HOURLY", "DAILY"], "type":
 "string" }, "Time": { "title": "Time", "default": 3, "minimum":
 0, "maximum": 23, "type": "integer" }, "AuditComment": { "title":
 "Auditcomment", "maxLength": 512, "type": "string" } }, "required":
 ["Name", "FeedURL", "Type", "Frequency"], "additionalProperties":
 false }, "CertObject":{ "title": "Certificate Object", "type":
 "object", "properties": { "Name": { "title": "Name", "minLength":
 1, "maxLength": 63, "pattern": "^[a-zA-Z0-9-]+$", "type":
 "string" }, "Description": { "title": "Description", "maxLength":
 512, "type": "string" }, "CertificateSignerArn": { "title":
 "Certificatesignerarn", "type": "string" }, "CertificateSelfSigned":
 { "title": "Certificateselfsigned", "default": false, "type":
 "boolean" }, "AuditComment": { "title": "Auditcomment",
 "maxLength": 512, "type": "string" } }, "required": ["Name"],
 "additionalProperties": false } }, "properties": { "RuleStackName":
 { "description": "Nom de la rulestack", "minLength": 1, "maxLength":
 128, "pattern": "^[a-zA-Z0-9-]+$", "type": "string" }, "RuleStack":
 { "$ref": "#/definitions/RuleStack" }, "RuleList": { "description":
 "list of rules", "type": "array", "uniqueItems": false, "items":
 { "$ref": "#/definitions/Rule" } }, "SecurityObjects": { "$ref": "#/
```



```
definitions/SecurityObjects" }, "CustomSecurityProfiles": { "$ref":
 "#/definitions/CustomSecurityProfiles" } }, "additionalProperties":
 false, "required": [ "RuleStackName" ], "createOnlyProperties":
 [ "/properties/RuleStackName" ], "primaryIdentifier": [ "/
properties/RuleStackName" ], "handlers": { "create": { "permissions":
 [ "execute-api:Invoke" ] }, "read": { "permissions": [ "execute-
api:Invoke" ] }, "update": { "permissions": [ "execute-
api:Invoke" ] }, "delete": { "permissions": [ "execute-
api:Invoke" ] } } }
```


Configurer l’intégration automatisée des comptes

Cloud NGFW pour AWS prend désormais en charge l’intégration automatisée des comptes pour les environnements desservant un grand nombre de comptes AWS. Grâce à cette fonctionnalité, vous n’avez plus besoin d’intégrer manuellement des comptes individuels. Lors de l’utilisation de l’intégration automatisée des comptes, tenez compte des éléments suivants :

- Il est possible d’intégrer jusqu’à 100 comptes à la fois. Pour intégrer plus de 100 comptes, vous devez définir plusieurs modules, chacun contenant 100 comptes. Consultez la Documentation Terraform pour en savoir plus.
- L’intégration automatisée des comptes peut prendre environ 10 minutes.
- Un compte doit être intégré manuellement afin d’utiliser la fonctionnalité d’intégration automatisée des comptes.

Vous devez créer un rôle à l’aide du modèle Cloud Formation (CFT) et appliquer des autorisations dans chacun des comptes que vous souhaitez intégrer.

Un modèle Terraform mis à jour est utilisé pour appeler l’API LinkAccount qui récupère les paramètres utilisés pour créer des ARN de rôle [pour vos comptes AWS intégrés]. Le modèle Terraform accède à l’API en étant exposé via l’accès par programmation, ce qui nécessite la création d’un nouveau rôle : **AccountAdmin (Administrateur de compte)**.

Pour accéder à la fonctionnalité d’intégration automatisée des comptes, vous devrez télécharger le dernier modèle Terraform et activer l’accès par programmation. Pour plus d’informations, consultez Activer l’accès par programmation.

Les aspects de la création de rôles fournis par le modèle sont les mêmes, cependant, elle a été modifiée pour inclure les ressources et les rôles afin de prendre en charge l’intégration automatisée des comptes.

Pour configurer l’intégration automatisée des comptes :

STEP 1 | Créez un rôle à accès par programmation **AccountAdmin (Administrateur de compte)** pour tout compte actuellement intégré.

STEP 2 | Créez un rôle pour exécuter le modèle Cloud Formation (CFT) de configuration des rôles entre comptes dans chaque compte que vous souhaitez intégrer. Le rôle doit avoir la relation de confiance suivante :

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Autoriser",

"Principal": {

"AWS": "arn:aws:iam::018147215560:user/sosrinath"

},

"Action": "sts:AssumeRole"

}

]

}

Le rôle doit avoir la **Permission Policy (Politique d'autorisation)** suivante définie à l'aide de l'option Créer une politique en ligne dans IAM

{

"Version": "2012-10-17",

"Statement": [

{

"Action": [

"lambda:CreateFunction",

"iam:GetRole",

"lambda:AddPermission",

"cloudformation:ListStacks",

"cloudformation:CreateStack",

"lambda:InvokeFunction",

"lambda:GetFunction",

"iam:CreateRole",

"iam:DeleteRole",

"lambda:GetFunctionConfiguration",

"lambda:GetPolicy",

"cloudformation:DescribeStacks",

"cloudformation:DescribeStackEvents",

"cloudformation:GetTemplate",

"cloudformation:DeleteStack",

"lambda:DeleteFunction",

"iam:DeleteRolePolicy",

"iam:DetachRolePolicy",

"iam:AttachRolePolicy",

"iam:PutRolePolicy",

"iam:PassRole"

],

"Resource": "*",

"Effect": "Autoriser",

"Sid": "VisualEditor1"

}

]

}

STEP 3 | Utilisez le fournisseur **cloudngfwaws** de Terraform pour accéder aux ressources de gestion du Cloud NGFW pour AWS. Le rôle CFT créé à l'étape précédente doit être spécifié comme valeur de la variable cft_role_name dans la définition du schéma du module **account_onboarding**.

STEP 4 | Exécutez Terraform Apply.

Après l'application des modifications au CFT, la ressource Cloud NGFW intègre chaque compte :

- Le module d'intégration des comptes exécute le CFT de configuration du rôle de compte dans le compte.
- Le CFT du rôle entre comptes envoie des ARN de rôle à la ressource Cloud NGFW.

Le module d'intégration des comptes attend un certain temps, qui peut prendre jusqu'à 10 minutes pour réussir l'intégration de tous les comptes.

Supprimer un compte intégré

Utilisez Terraform **destroy (détruire)**. Pour plus d'informations, consultez la Documentation Terraform.

Indiquez un compte non intégré

Utilisez Terraform **list (énumérer)**. Pour plus d'informations, consultez la Documentation Terraform.

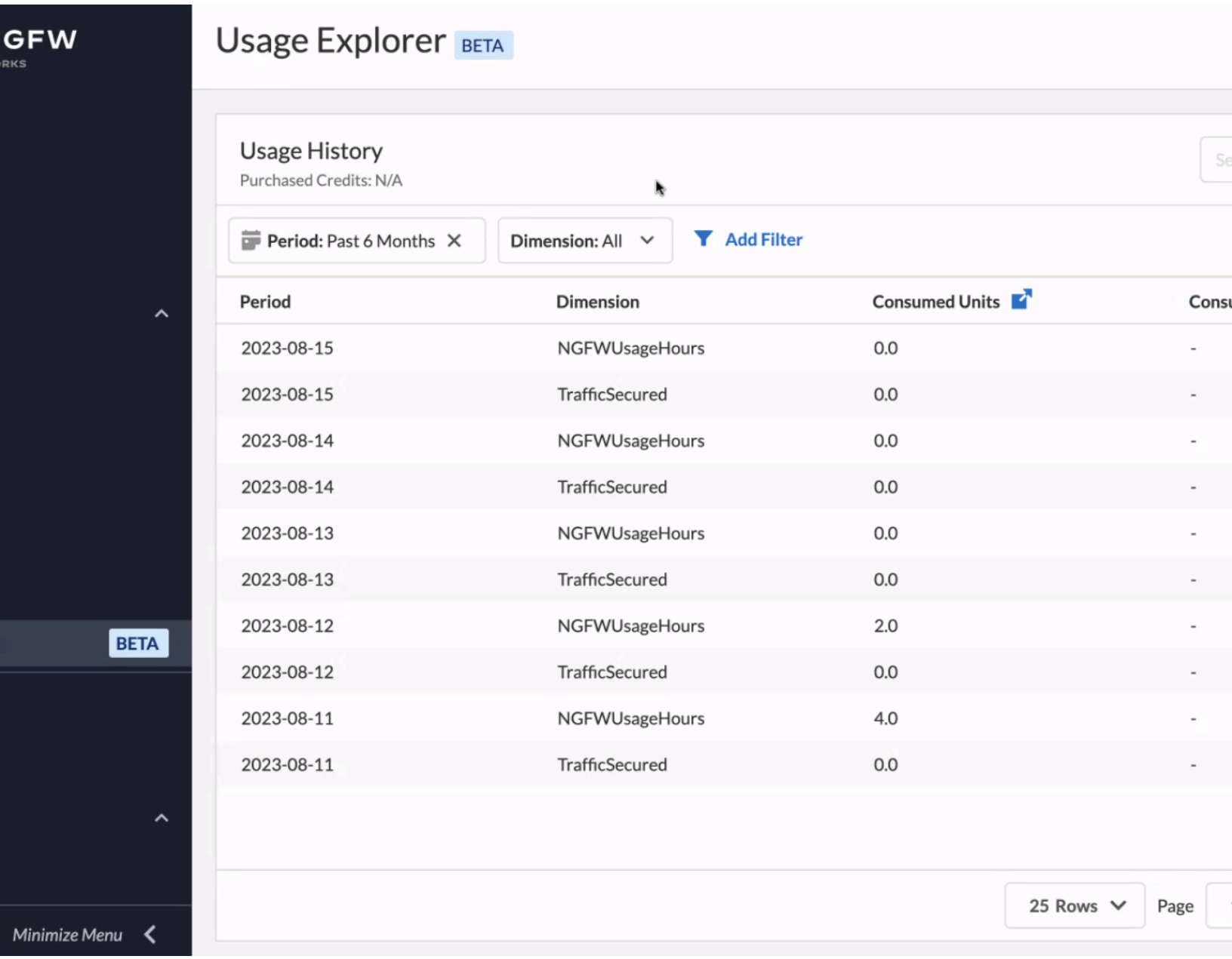
Explorateur de l’utilisation

Le tableau de bord de l’Explorateur de l’utilisation fournit un moyen rapide et pratique de déterminer la consommation Cloud NGFW d’un locataire pour les abonnements de paiement à l’utilisation (PAYG) et basés sur le crédit (achetés dans le cadre d’un contrat). Ces informations affichent une consommation quotidienne qui inclut des informations sur votre consommation moyenne et sa corrélation aux crédits Cloud NGFW associés au locataire.

La fonctionnalité Explorateur de l’utilisation est actuellement disponible en version préliminaire.

Pour accéder à l’Explorateur de l’utilisation :

1. Établissez une connexion à la console Cloud NGFW.
2. Dans la console, sélectionnez **Usage Explorer (Explorateur de l’utilisation)**.



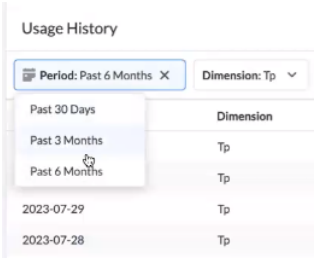
L'Explorateur de l'utilisation inclut des options permettant d'afficher la consommation sur une période donnée et vous permet de télécharger un fichier au format CSV afin de capturer des données pertinentes en vue d'une inspection future. L'historique de la consommation quotidienne est présenté dans un tableau comprenant les champs suivants :

- Period (Période) : représente la période de consommation du Cloud NGFW.
- Dimension : utilisée pour identifier la facturation d'un Cloud NGFW. Une dimension désigne une extension (par exemple, Prévention des menaces).
- Consumed Units (Unités consommées) : quantité de ressources consommée par le locataire pendant la période de facturation. Ce champ est pertinent pour le modèle d'abonnement PAYG.

- Consumed as Credits (Consommé sous forme de crédits) : quantité de ressources consommée par le locataire pendant la période de facturation. Ce champ est pertinent pour le modèle d'abonnement PAYG.

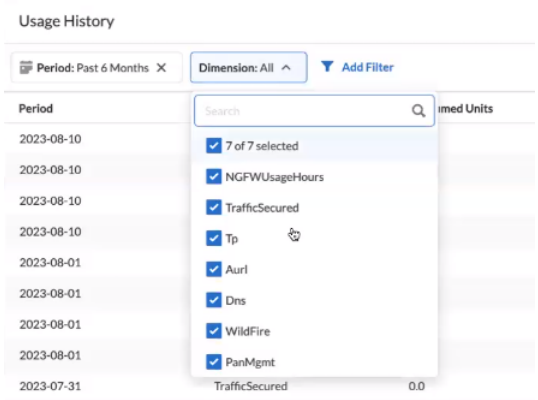
> *Vous ne pouvez appliquer un filtre que sur des dimensions prises en charge. L'option **Add filter (Ajouter un filtre)** ne fonctionne pas à l'heure actuelle dans cette version préliminaire.*

Utilisez le champ **Period (Période)** pour afficher la consommation sur une période donnée. Lorsque vous utilisez cette option, tenez compte du fait qu'un filtrage de la consommation sur des périodes plus longues peut entraîner des retards lors de l'affichage des données :



> *Par défaut, l'Explorateur de l'utilisation affiche les données de consommation des 30 derniers jours.*

Utilisez le champ **Dimensions** pour modifier l'affichage de l'Explorateur de l'utilisation de manière à n'afficher que les dimensions complémentaires qui font partie de votre abonnement. Vous pouvez appliquer un filtre sur toutes les dimensions ou sélectionner une dimension dans le menu déroulant :

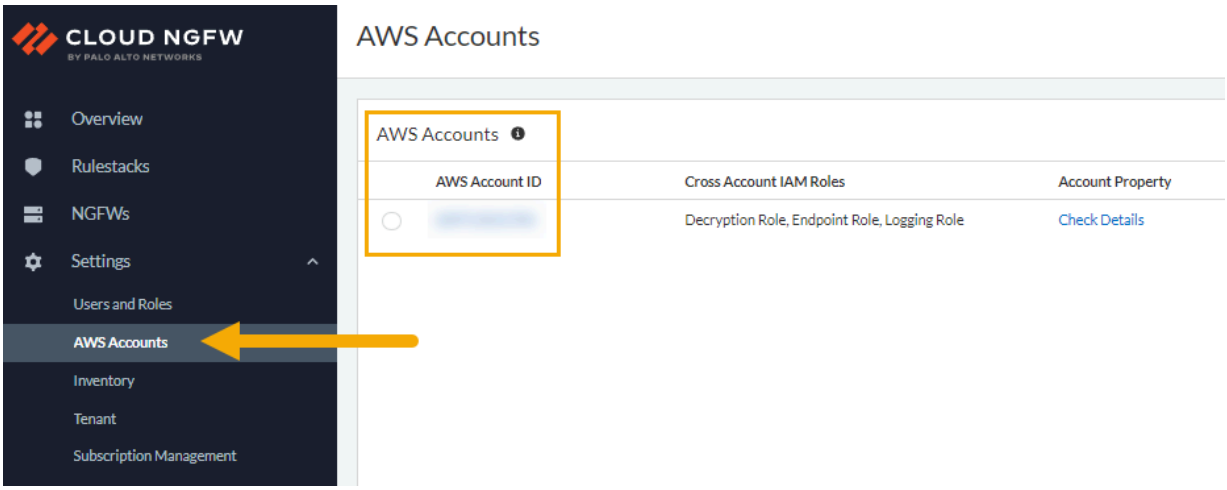


> *L'affichage de l'Explorateur de l'utilisation dépend du modèle d'abonnement du locataire Cloud NGFW, PAYG ou dans le cadre d'un contrat.*

Créer un dossier d’assistance

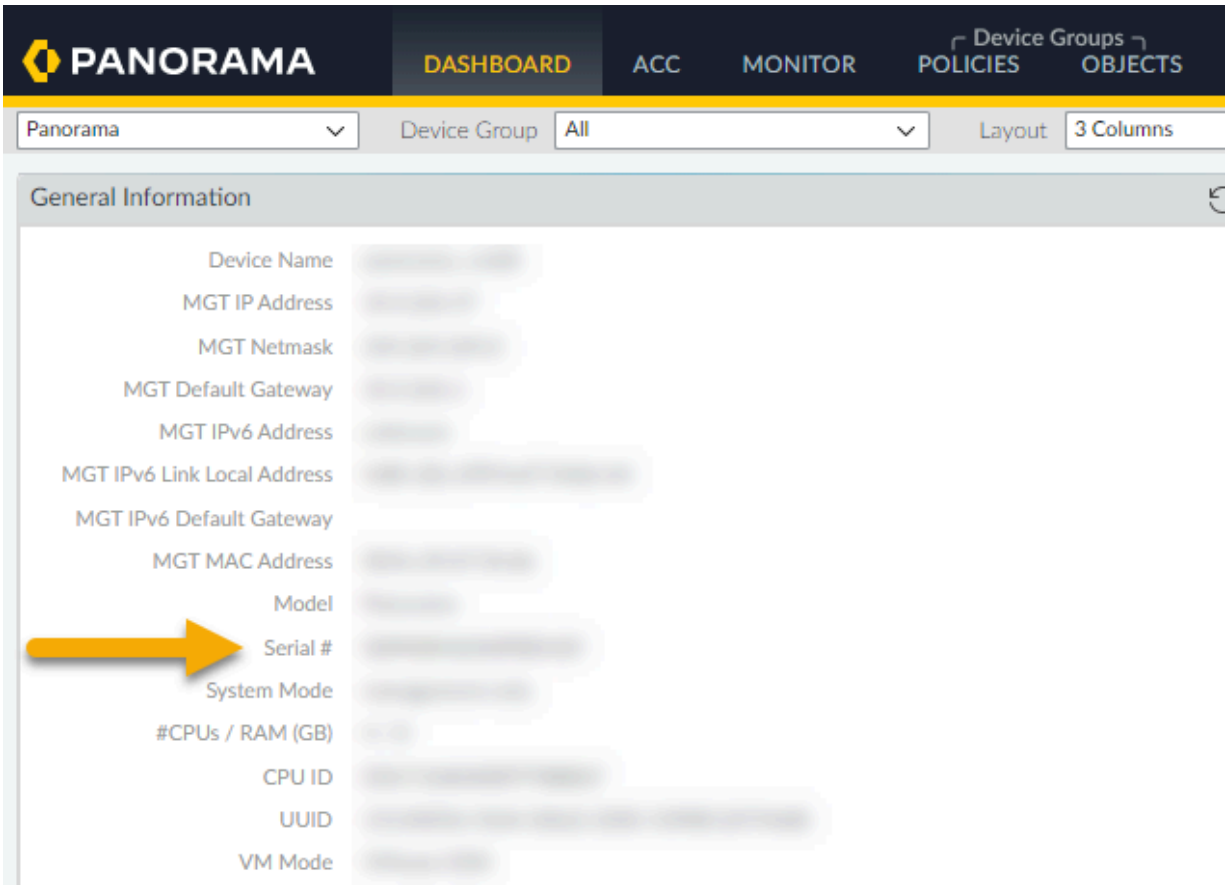
Pour créer une demande de support à l’aide de la console Cloud NGFW :

STEP 1 | Recherchez votre **AWS Account ID (ID de compte AWS)**. Sélectionnez **AWS Accounts (Comptes AWS)**.

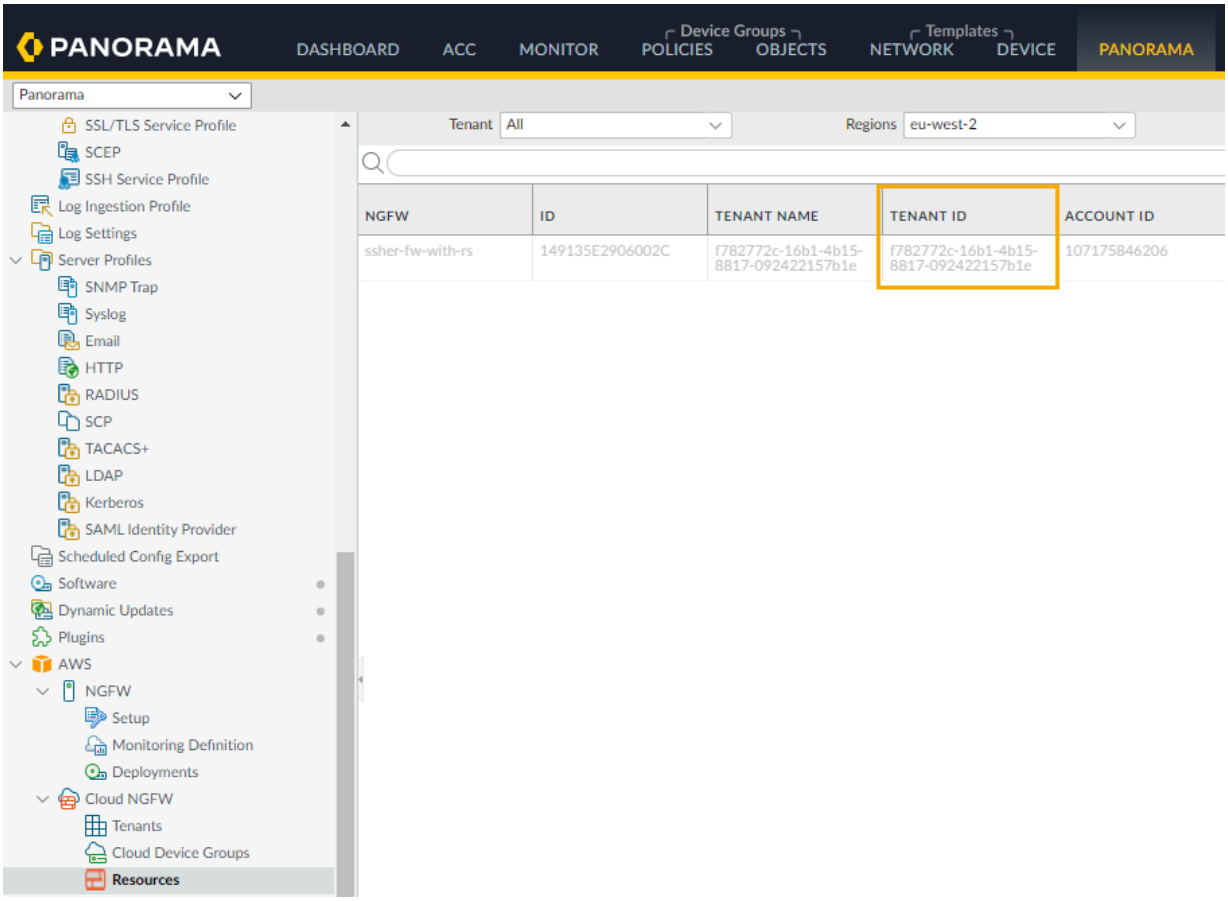


STEP 2 | Si nécessaire, utilisez la console Panorama pour déterminer des informations supplémentaires pour le dossier de support, telles que l'ID du locataire ou le numéro de série de Panorama.

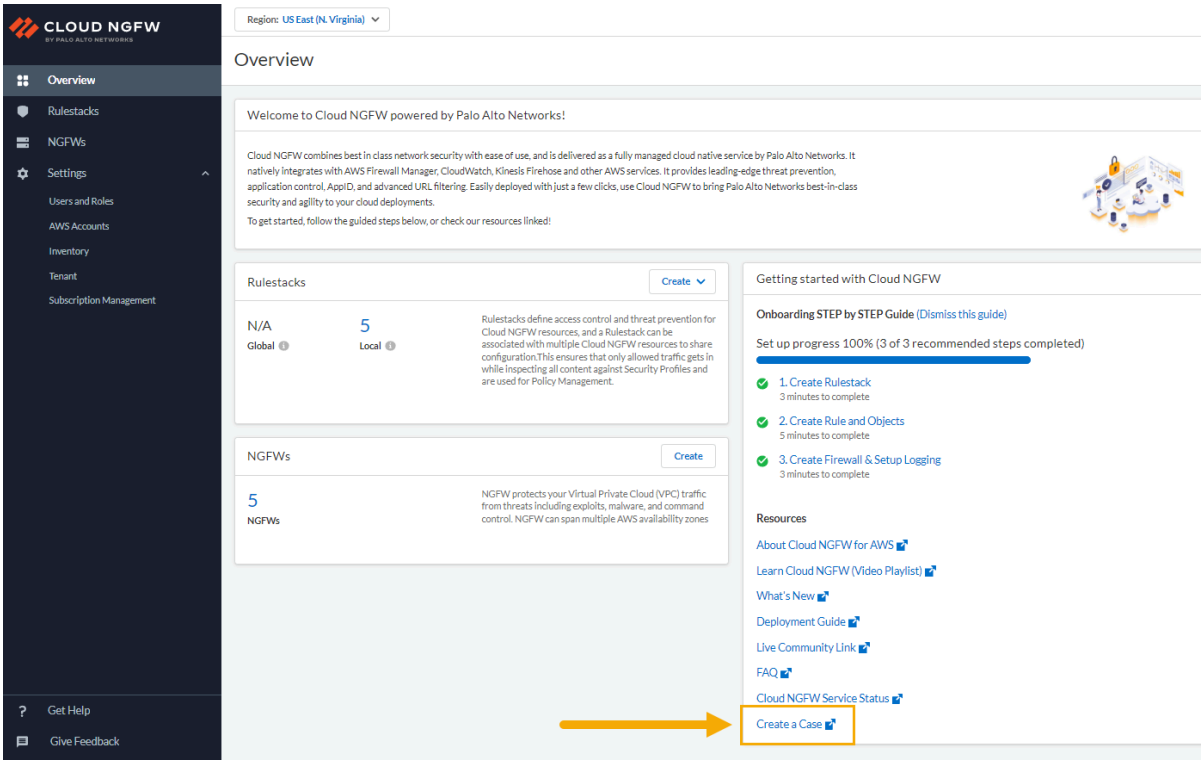
Recherchez le **Panorama serial number (numéro de série Panorama)** à l'aide du **Dashboard (Tableau de bord)** :



Recherchez le **Tenant ID (ID de locataire)** de la ressource Cloud NGFW :



STEP 3 | Sur la page **Overview (Présentation)** de la console Cloud NGFW, cliquez sur **Create a case (Créer un dossier)**.



Rulestacks et règles Cloud NGFW pour AWS

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

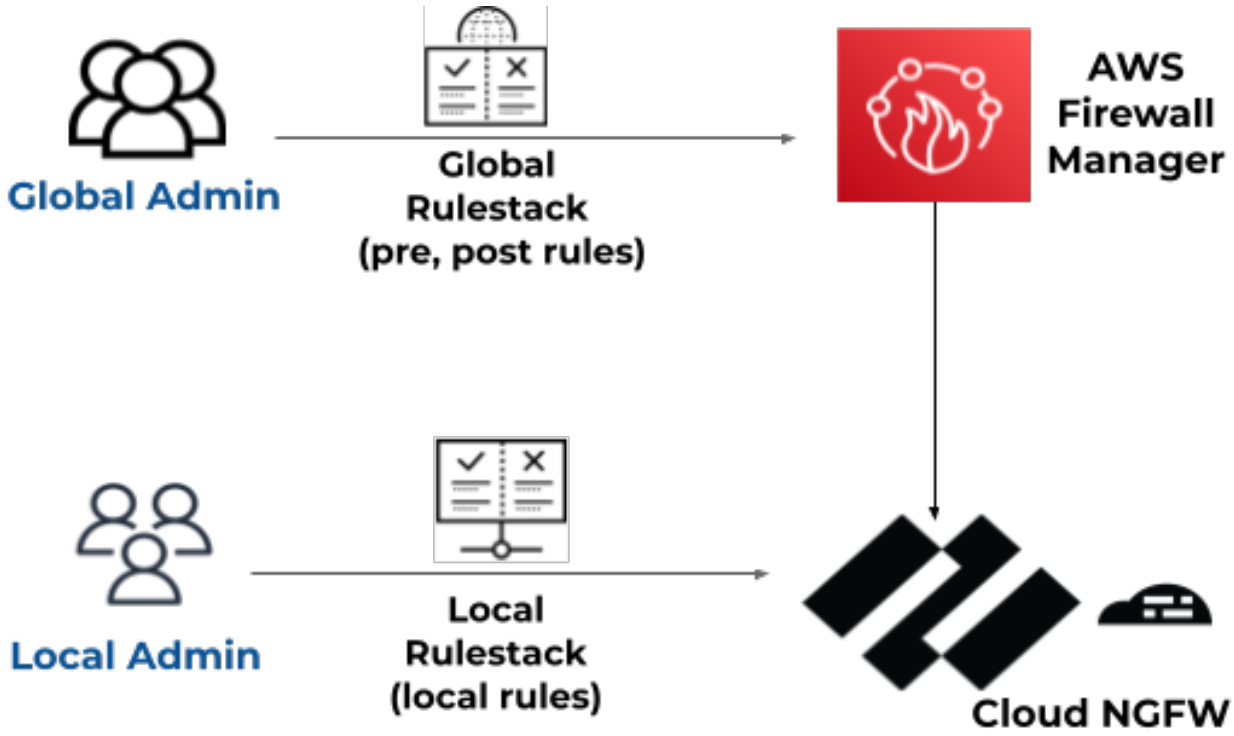
La console de locataire Cloud NGFW prend uniquement en charge la création de rulestacks locales.

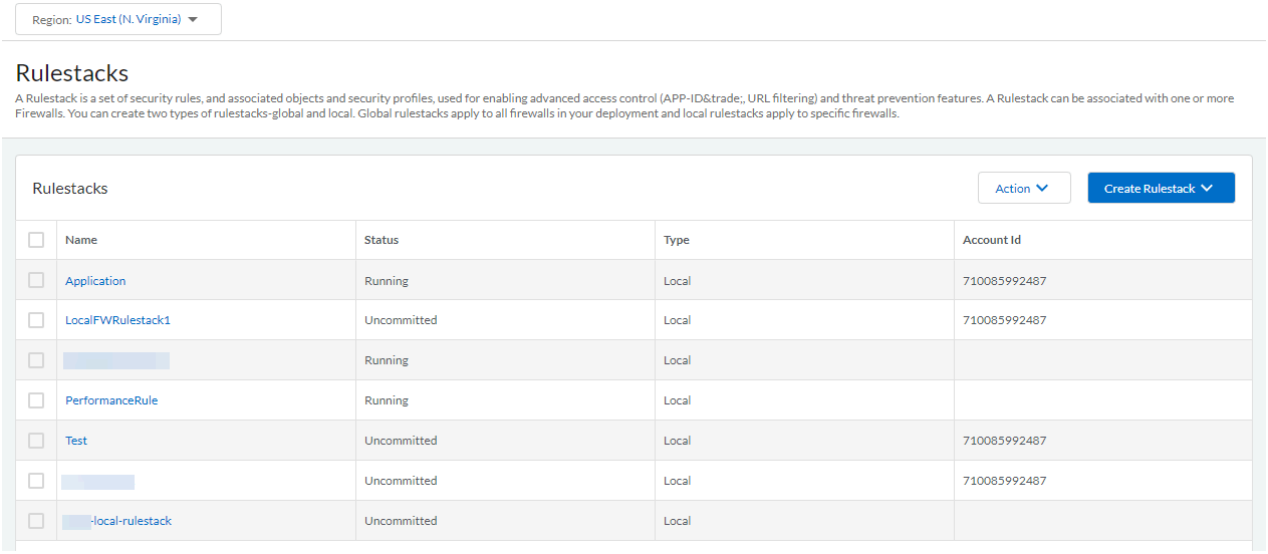
À propos des rulestacks et des règles sur Cloud NGFW pour AWS

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, elle applique vos règles sur le VPC 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 comprend un ensemble de règles de sécurité, des objets associés et des profils similaires aux groupes d'appareils sur Panorama. Il existe deux types de rulestacks.

- **Rulestack locale** – Une pile de règles locale se compose de règles locales et gère les règles locales. Un administrateur de compte local peut associer une rulestack locale à un NGFW dans son compte AWS. Pour créer et gérer des rulestacks locales, vous devez disposer du rôle Admin de la rulestack locale.
- **Rulestack globale** – L'administrateur d'AWS Firewall Manager peut créer une politique de service Firewall Manager (FMS) et y associer une rulestack globale. AWS Firewall Manager gère la rulestack globale sur tous ces NGFW dans différents comptes AWS d'une organisation AWS. Une rulestack globale configure les règles « avant » et règles « après » sur chaque NGFW. Pour créer et gérer des rulestacks globales, vous devez disposer du rôle Admin de la rulestack globale.
  - **Règles amont** – Règles ajoutées au début de la liste des règles et évaluées en premier.
  - **Règles « après »** – Règles ajoutées au bas de l'ordre des règles et évaluées après les règles « après » et les règles définies dans une rulestack locale appliquée à un NGFW individuel.

Lorsque vous utilisez Firewall Manager, une combinaison de rulestacks locales et globales vous permet de créer un modèle de règles hiérarchiques. Les règles « avant » d'une rulestack globale peuvent servir de règles globales par défaut pour tous les pare-feu associés. Vous pouvez ensuite utiliser une rulestack locale pour définir des règles pour des applications ou des utilisateurs spécifiques. Les règles de publication peuvent être utilisées pour autoriser ou refuser le trafic qui ne correspond à aucune règle « avant » ou aux règles définies dans la rulestack locale.





Une rulestack globale et une rulestack locale peuvent être appliquées à chaque NGFW.

Si vous utilisez un locataire multicomptes ou multi-VPC, tenez compte des modifications suivantes dans le comportement de la rulestack :

- lors de sa création, une rulestack est mappée à un compte spécifique.
- vous pouvez désormais associer une rulestack à une ressource de pare-feu dans n'importe quel compte intégré.
- les autorisations sont toujours mappées au compte associé à la rulestack ; toute modification de la rulestack doit être effectuée par un utilisateur disposant des autorisations LRA dans le compte de la rulestack.

Les certificats de n'importe quel compte intégré peuvent être mappés à une rulestack.

Par exemple, le certificat dans compte1 et le certificat dans compte2 peuvent être mappés à une rulestack dans compte3 qui pourrait être associée à une ressource de pare-feu dans compte4. Dans ce scénario, tous les comptes (1 à 4) doivent être intégrés avec succès.

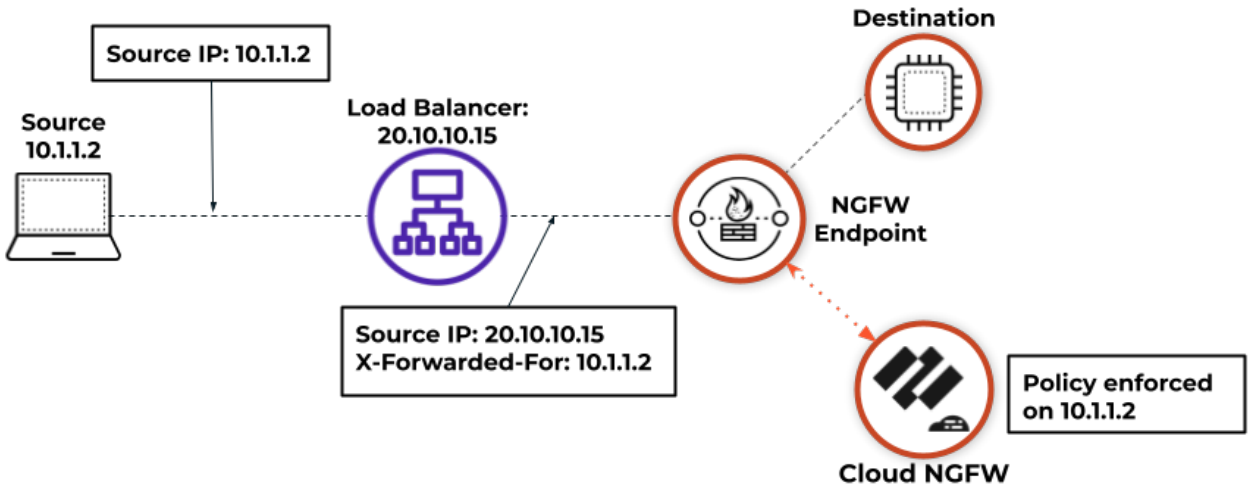
- Créer une rulestack sur Cloud NGFW pour AWS
- Profils de sécurité Cloud NGFW pour AWS
- Objets de règle de sécurité Cloud NGFW pour AWS
- Créer des règles de sécurité sur Cloud NGFW pour AWS

X-Forwarded-For sur Cloud NGFW pour AWS

Le trafic entrant vers vos applications peut passer par des équilibreurs de charge AWS ou des serveurs proxy avant d'atteindre le NGFW. Étant donné que ces périphériques interceptent le trafic entre la source et la destination, le NGFW voit l'adresse IP de l'équilibreur de charge ou du serveur proxy au lieu de l'adresse IP de la source. Ces périphériques ajoutent l'en-tête X-Forwarded-For (XFF) aux requêtes HTTP et ajoutent l'adresse IPv4 ou IPv6 réelle du client accédant à votre application.

Le trafic vers vos applications peut être passé par plusieurs serveurs proxy avant d'atteindre le NGFW. L'en-tête de requête XFF peut contenir plusieurs adresses IP séparées par des virgules. NGFW utilise toujours la dernière adresse ajoutée dans l'en-tête XFF pour appliquer la politique.

Lors de la configuration de votre rulestack, 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.



Créer une rulestack sur Cloud NGFW pour AWS

Dans le locataire Cloud NGFW, vous pouvez créer des rulestacks si le rôle LocalRuleStackAdmin ou GlobalRulestackAdmin vous est attribué. Pour créer une rulestack globale, vous devez avoir utilisé AWS Firewall Manager pour créer votre locataire Cloud NGFW.

Lorsque vous créez une rulestack locale, vous devez spécifier un compte AWS. La rulestack est appliquée aux NGFW associés à ce compte AWS uniquement. Effectuez la procédure suivante pour créer une rulestack.

STEP 1 | Sélectionnez **Rulestacks** > **Create Rulestack (Créer une rulestack)**.

STEP 2 | Sélectionnez **Local Rulestack (Rulestack locale)** ou **Global Rulestack (Rulestack globale)** (déploiement FMS uniquement) dans la liste déroulante.

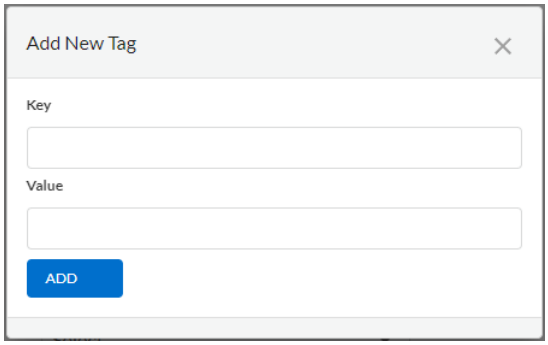
STEP 3 | Saisissez un **Name (Nom)** descriptif pour votre rulestack.

STEP 4 | (Facultatif) Saisissez une **Description** pour votre rulestack.

STEP 5 | (Rulestack locale uniquement) Sélectionnez un **AWS Account (Compte AWS)** dans la liste déroulante.

STEP 6 | (Facultatif) Appliquez des **Tags (Étiquettes)**.

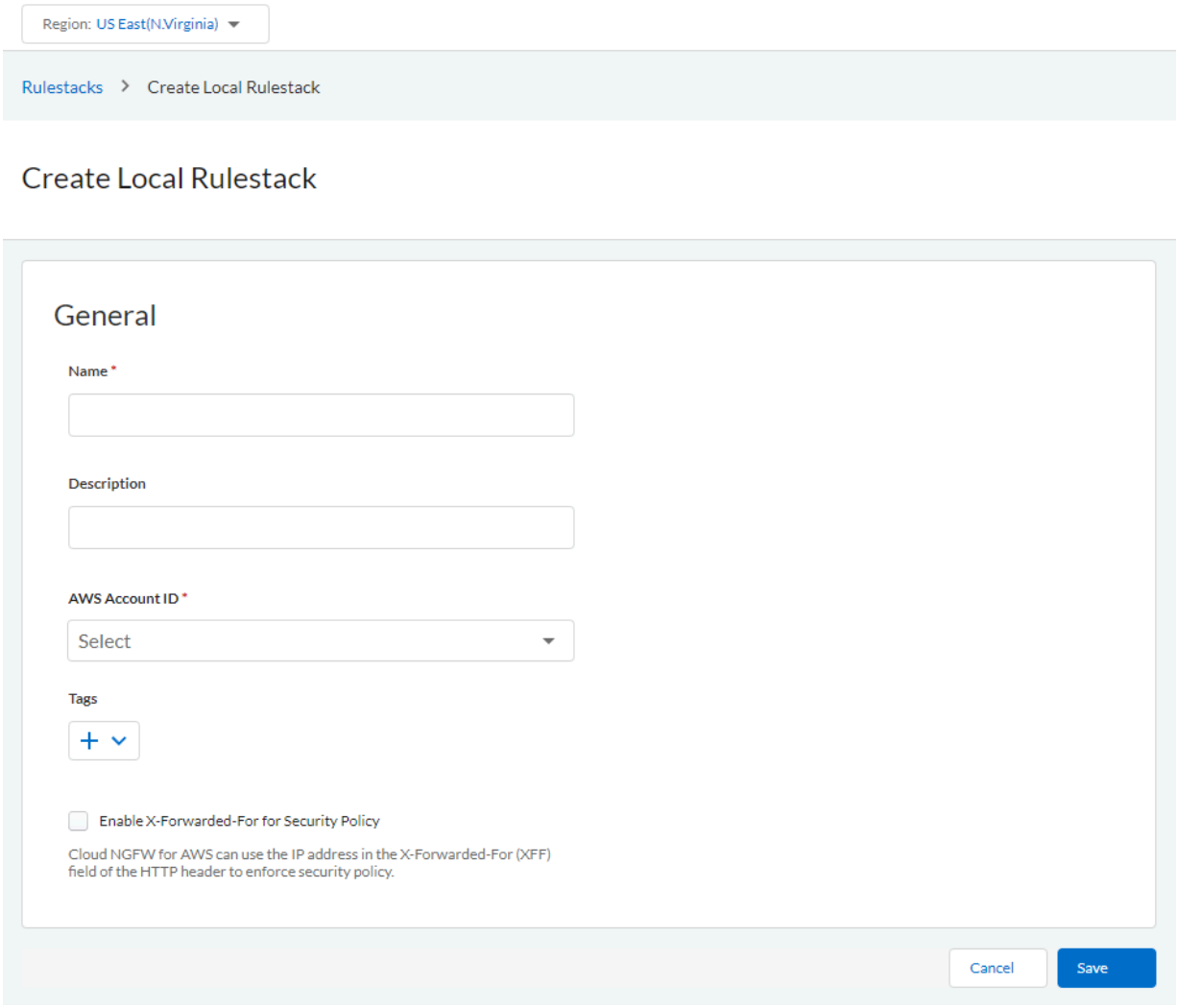
1. Cliquez sur l'icône + et sélectionnez **Add New (Ajouter nouveau)**.
2. Saisissez une **Key (Clé)** et une **Value (Valeur)**.
3. Cliquez sur **Add (Ajouter)**.



STEP 7 | (Facultatif) **Enable X-Forwarded-For for Security Policy (Activer X-Forwarded-For pour la politique de sécurité)**. Pour plus d'informations, reportez-vous à la section X-Forwarded-For sur Cloud NGFW pour AWS.

STEP 8 | Cliquez sur **Save (Enregistrer)**.

STEP 9 | Après avoir créé la rulestack, déployez-la sur le pare-feu.



Objets de règle de sécurité Cloud NGFW pour AWS

Un objet de règle de sécurité est un objet unique ou une unité collective qui regroupe des identités discrètes telles que des adresses IP, des noms de domaine complets (FQDN), des flux intelligents ou des certificats. En général, lors de la création d'un objet de politique, vous regroupez les objets nécessitant des autorisations similaires dans une politique. Par exemple, si votre organisation utilise un ensemble d'adresses IP de serveur pour authentifier les utilisateurs, vous pouvez regrouper l'ensemble d'adresses IP de serveur 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.
- **Catégorie d'URL personnalisée** : une catégorie d'URL personnalisée vous permet de spécifier des exceptions à une application de catégorie d'URL et de créer une catégorie d'URL personnalisée basée sur plusieurs catégories existantes.
- **Flux intelligent** : un flux intelligent, également appelé liste dynamique externe (EDL), est un flux continu de données liées aux menaces potentielles ou actuelles pour la sécurité d'une organisation. Un flux intelligent enregistre et suit les adresses IP et les URL associées à des menaces telles que les escroqueries par hameçonnage, les logiciels malveillants, les bots, les logiciels espions, les ransomwares, etc.

  Cloud NGFW comprend quatre flux intelligents intégrés.

  - **Adresses IP à toute épreuve de Palo Alto Networks** : contient des adresses IP fournies par des fournisseurs d'hébergement à toute épreuve. Comme les fournisseurs d'hébergement à toute épreuve ne placent que quelques (voire aucune) restrictions sur le contenu, les pirates utilisent souvent ces services pour héberger et distribuer du contenu malveillant, illégal et contraire à l'éthique.
  - **Adresses IP à risque élevé Palo Alto Networks)** : contient les adresses IP des informations sur les menaces émises par les organisations tierces de confiance. Palo Alto Networks compile la liste des informations sur les menaces, mais n'a pas de preuve directe du caractère malveillant des adresses IP.
  - **Adresses IP malveillantes connues de Palo Alto Networks** : contient les adresses IP qui sont malveillantes selon l'analyse effectuée par WildFire, la recherche de l'Unité 42 et les données recueillies de la télémétrie. Les pirates se servent de ces adresses IP presque exclusivement pour distribuer des logiciels malveillants, pour initier des activités de commande et contrôle et pour lancer des attaques.
  - **Palo Alto Networks Tor Exit IP Addresses (Adresses IP de sortie Tor de Palo Alto Networks)** : contient des adresses IP fournies par plusieurs fournisseurs et validées avec les données de renseignements sur les menaces de Palo Alto Networks en tant que nœuds de sortie Tor actifs. Le trafic provenant des nœuds de sortie Tor peut servir un objectif légitime, cependant, il est associé

de manière disproportionnée à des activités malveillantes, en particulier dans les environnements d'entreprise.

Vous pouvez connecter votre NGFW avec des flux d'intelligence intégrés de Palo Alto Networks et des flux intelligents tiers pour fournir des informations à jour sur les menaces pesant sur votre réseau. Si la connexion nécessite la spécification de certificats de décryptage, vous pouvez configurer Cloud NGFW pour utiliser un objet Cloud NGFW Certificate décrit ci-dessous.

- **Certificat** : un objet de certificat est une référence à un certificat TLS stocké dans AWS Secrets Manager de votre compte AWS.

Créer une liste de préfixes sur Cloud NGFW pour AWS

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 | Sélectionnez **Rulestacks** et sélectionnez une rulestack de règles créée précédemment sur laquelle configurer une liste de préfixes.

STEP 2 | Sélectionnez **Objects (Objets)** > **Prefix List (Liste de préfixes)** > **Create Prefix (Créer un préfixe)**.

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 **Save (Enregistrer)**.

Créer une liste FQDN pour Cloud NGFW sur AWS

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 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment sur laquelle configurer la liste FQDN.

STEP 2 | Sélectionnez **Objects (Objets)** > **FQDN List (Liste FQDN)** > **Create FQDN (Créer un FQDN)**.

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 **Save (Enregistrer)**.

Créer une catégorie d'URL personnalisée pour Cloud NGFW sur AWS

Palo Alto Networks fournit un ensemble de catégories prédéfinies de filtrage des URL. Vous pouvez également spécifier vos propres catégories de filtrage des URL à l'aide d'un objet de catégorie d'URL client. Par exemple, créez une liste personnalisée des URL que vous souhaitez utiliser comme critères de correspondance dans une règle de politique de sécurité. C'est une bonne façon de spécifier des exceptions à des catégories d'URL, lorsque vous aimeriez appliquer des URL spécifiques différemment de la catégorie d'URL à laquelle elles appartiennent.

Création d'une catégorie d'URL personnalisée

STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment sur laquelle configurer une catégorie d'URL personnalisée.

STEP 2 | Sélectionnez **Objects (Objets)** > **Custom URL Category (Catégorie d'URL personnalisée)** > **Create Custom URL Category (Créer une catégorie d'URL personnalisée)**.

STEP 3 | Entrez un **Name (Nom)** descriptif pour votre catégorie d'URL personnalisée.

STEP 4 | (facultatif) Saisissez une description pour votre catégorie d'URL personnalisée.

STEP 5 | Entrez une ou plusieurs **URL List (Liste des URL)**, une par ligne.

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

Directives de base pour les listes d'exceptions de catégories d'URL

- Saisissez les adresses IP ou les URL des sites Web que vous souhaitez appliquer distinctement de la catégorie des URL à laquelle elles sont associées.
- Les entrées de la liste doivent être exactes et sont sensibles à la casse.
- Entrez une chaîne qui est une correspondance exacte au site Web (et, éventuellement, un sous-domaine spécifique) auquel vous souhaitez contrôler l'accès ou utilisez des caractères génériques pour permettre à une entrée de correspondre à plusieurs sous-domaines d'un site Web. Pour plus de précisions sur l'utilisation des caractères génériques, passez en revue la section Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL.
- Omettez `http` et `https` des entrées d'URL.
- Chaque entrée d'URL peut contenir un maximum de 255 caractères.

Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL

Vous pouvez utiliser des caractères génériques dans les listes d'exceptions de catégories d'URL afin de facilement configurer une seule entrée qui doit correspondre à plusieurs sous-domaines de site Web et de pages, sans avoir à spécifier des sous-domaines et des pages exacts.

Suivez les directives suivantes lorsque vous créez des entrées qui possèdent des caractères génériques :

- Les caractères suivants sont considérés comme des séparateurs de jetons : . / ? & = ; +

  Chaque chaîne séparée par un ou deux de ces caractères est un jeton. Utilisez les caractères génériques en tant que marque substitutive d'un jeton, laquelle indique qu'un jeton spécifique peut contenir une valeur.

- À la place d’un jeton, utilisez un astérisque (*) ou un caret (^) pour indiquer une valeur d’un caractère générique.
- Les caractères génériques doivent être le seul caractère d’un jeton. Par exemple, www.gmail*.com ne serait pas valide, car l’astérisque suit d’autres caractères. Cependant, une entrée peut contenir plusieurs caractères génériques.

Utilisation des astérisques (*) et des carets (^)

*	À utiliser pour indiquer un ou plusieurs sous-domaines variables. Si vous utilisez *, l’entrée sera mise en correspondance avec les sous-domaines supplémentaires, qu’ils se trouvent au début ou à la fin de l’URL. Exemple : • ***.paloaltonetworks.com** correspond à www.paloaltonetworks.com et à www.paloaltonetworks.com.uk. • ***.paloaltonetworks.com** correspond à www.paloaltonetworks.com et à www.paloaltonetworks.com.uk.
^	À utiliser pour indiquer un sous-domaine variable. Exemple : **mail.^.com** correspond à mail.company.com, mais pas à mail.company.sso.com.

Ne créez pas d’entrée comportant des astérisques (*) consécutifs ou plus de neuf carets (^) consécutifs. De telles entrées peuvent compromettre la performance du pare-feu.

*Par exemple, n’ajoutez pas d’entrée comme **mail.*.*.com** ; selon la plage de sites Web auxquels vous souhaitez contrôler l’accès, entrez plutôt **mail.*.com** ou **mail.^.^.com**. Une entrée comme **mail.*.com** correspond à un plus grand nombre de sites que **mail.^.^.com** ; **mail.*.com** correspond à des sites qui comprennent un nombre indéfini de sous-domaines, tandis que **mail.^.^.com** correspond à des sites qui contiennent exactement deux sous-domaines.*

Listes d'exceptions de catégories d’URL : exemples de caractères génériques

Le tableau suivant présente des exemples d’entrées de liste des URL utilisant des caractères génériques et des sites correspondant à ces entrées.

Entrée de la liste d’exceptions d’URL	Sites correspondants
Ensemble d’exemples 1	
*.company.com	eng.tools.company.com support.tools.company.com tools.company.com docs.company.com
^.company.com	tools.company.com docs.company.com
^.^.company.com	eng.tools.company.com support.tools.company.com
Ensemble d’exemples 2	
mail.google.*	mail.google.com mail.google.co.uk mail.google.example.org
mail.google.^	mail.google.com mail.google.info
mail.google.^.^	mail.google.co.uk mail.google.example.info
Example Set 3 (Ensemble d’exemples 3)	
site.*.com	site.yourname.com site.abc.xyz.com
site.^.com	site.company.com site.example.com
site.^.^.com	site.a.b.com
site.com/*	site.com/photos site.com/blog/latest tout sous-répertoire site.com

Configurer un flux intelligent sur Cloud NGFW pour AWS

Un flux intelligent, également appelé liste dynamique externe, est une liste que vous ou des tiers pouvez héberger sur un serveur Web externe. Vous pouvez spécifier le flux intelligent comme source ou destination de votre règle de sécurité. Le NGFW vérifie la liste hébergée toutes les heures ou tous les jours et applique vos règles de sécurité en fonction des dernières entrées de votre liste, sans vous obliger à apporter des modifications à la configuration.

- **Liste IP** : appliquez la politique pour une liste d'adresses IP source ou de destination qui émergent ad hoc en utilisant un flux intelligent de type adresse IP comme objet d'adresse source ou de destination dans les règles de politique et configurez le NGFW pour refuser ou autoriser l'accès aux adresses IP incluses dans la liste. Le NGFW traite un flux intelligent de liste IP comme un objet d'adresse, et toutes les adresses IP incluses sont traitées comme un seul objet d'adresse.

  Le flux intelligent peut inclure des adresses IP individuelles, des adresses de sous-réseau (adresse/masque) ou une plage d'adresses IP. En outre, la liste d'interdiction peut contenir des commentaires et des caractères spéciaux, tels que * , : , ; , # ou /. La syntaxe de chaque ligne de la liste est **`[adresse IP, adresse IP/masque, ou début de la plage d'adresses IP et fin de la plage d'adresses IP] [espace] [commentaire]`**.

  Saisissez chaque adresse IP/plage d'adresses IP/sous-réseau IP sur une nouvelle ligne ; les URL ou domaines ne sont pas pris en charge dans cette liste. Un sous-réseau ou une plage d’adresses IP comme 92.168.20.0/24 ou 192.168.20.40-192.168.20.50, sont comptabilisés comme une entrée d’adresse IP et pas comme plusieurs adresses IP. Si vous ajoutez des commentaires, ils doivent être sur la même ligne que l'adresse IP/plage d'adresses IP/sous-réseau IP. L'espace à la fin de l'adresse IP est le délimiteur qui sépare un commentaire de l'adresse IP

  Une liste d'adresse IP type :

  ```
  192.168.20.10/32 2001:db8:123:1::1 #test IPv6 address
   192.168.20.0/24 ; test internal subnet 2001:db8:123:1::/64 test
   internal IPv6 range 192.168.20.40-192.168.20.50
  ```

- **Liste des URL** : protégez votre réseau contre les nouvelles sources de menaces ou de logiciels malveillants à l'aide des URL. Le NGFW gère un flux intelligent avec des URL comme une catégorie d'URL personnalisée. Pour plus d'informations sur le formatage de la liste des URL, voir Créer une catégorie d'URL personnalisée pour Cloud NGFW sur AWS.

Le NGFW nécessite un objet de certificat pour accéder au flux intelligent. Pour plus d’informations, consultez Ajouter un certificat à Cloud NGFW pour AWS.

STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment sur laquelle configurer le blocage de fichiers.

STEP 2 | Sélectionnez **Objects (Objets)** > **Intelligent Feed (Flux intelligent)** > **Create Intelligent Feed (Créer un flux intelligent)**.

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

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

STEP 5 | Sélectionnez le **Type** de flux intelligent.

STEP 6 | Saisissez la valeur **Source URL (URL source)**.

STEP 7 | Définissez le **Certificate Profile (Profil de certificat)**.

STEP 8 | Définissez le paramètre **Update Frequency (Fréquence de mise à jour)** : **Hourly (Toutes les heures)** ou **Daily (Tous les jours)**.

STEP 9 | Cliquez sur **Save (Enregistrer)**.

Ajouter un certificat à Cloud NGFW pour AWS

Cloud NGFW utilise des certificats pour accéder à un flux intelligent et pour activer le décryptage entrant et sortant. Ces certificats sont stockés dans AWS Secrets Manager.

Trois types de certificats sont utilisés dans un déploiement typique.

- **Certificat CA intermédiaire (certificat CA)** : une Certificate Authority (autorité de certification – CA) est une organisation de confiance qui émet des certificats SSL. Ces certificats numériques sont des fichiers qui permettent de lier une entité à une clé publique. Les navigateurs Web utilisent ces certificats pour authentifier le contenu envoyé depuis des serveurs Web. Les navigateurs Web sont généralement dotés de listes de CA auxquelles ils font implicitement confiance pour identifier les hôtes. Le but d'une CA est de vérifier l'authenticité du site Web, du domaine ou des organisations.
- **Certificat de serveur** : un certificat associé à un nom de domaine spécifique. Si un site Web possède un certificat valide, cela signifie qu'une autorité de certification a pris des mesures pour vérifier que l'adresse Web appartient réellement à cette organisation. Lorsque vous saisissez une URL, votre navigateur vérifie le certificat pour s'assurer que l'adresse du site Web correspond à l'adresse indiquée sur le certificat. Il vérifie également que le certificat est signé par une autorité de certification de confiance.

  Vous pouvez vous connecter de temps en temps à un serveur doté d'un certificat non approuvé. Cloud NGFW pour AWS bloquera la connexion comme si le serveur avait mis fin à la connexion.
- **Certificat CA racine** : une autorité de certification peut émettre plusieurs certificats sous la forme d'une arborescence. Un certificat racine est le certificat le plus haut de l'arborescence.

Lors de l'ajout d'un certificat à AWS Secrets Manager pour une utilisation avec Cloud NGFW, les conditions préalables suivantes doivent être remplies.

- Certificat ajouté sous forme de paire clé/valeur, avec deux clés : **private-key (clé privée)** et **public-key (clé publique)**. Pour la clé privée, la valeur doit être la clé réelle et, pour la clé publique, la valeur doit être le corps de certificat réel.
- Une étiquette avec la clé **PaloAltoCloudNGFW** et la valeur **true**.
- Vous devez importer le certificat CA racine et le ou les certificats CA intermédiaires dans le magasin de confiance du client.
- Si vous utilisez des certificats d'entité finale pour décrypter le trafic, seuls les certificats d'entité finale (clés privées et publiques) doivent être stockés dans AWS Secrets Manager.
- Le format de clé privée PKCS8 est pris en charge. Le format de clé privée PKCS1 n'est pas pris en charge.

Format PKCS pris en charge :

```
-----DÉBUT DE LA CLÉ PRIVÉE----- -----FIN DE LA CLÉ PRIVÉE-----
```

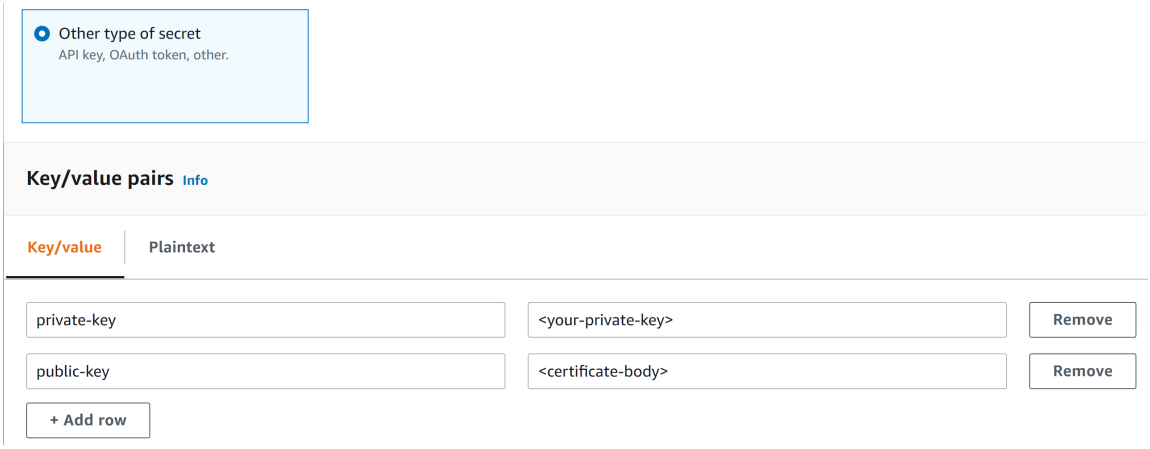

Format PKCS1 non pris en charge :

```
-----DÉBUT DE LA CLÉ PRIVÉE RSA----- -----FIN DE LA CLÉ PRIVÉE
 RSA-----
```

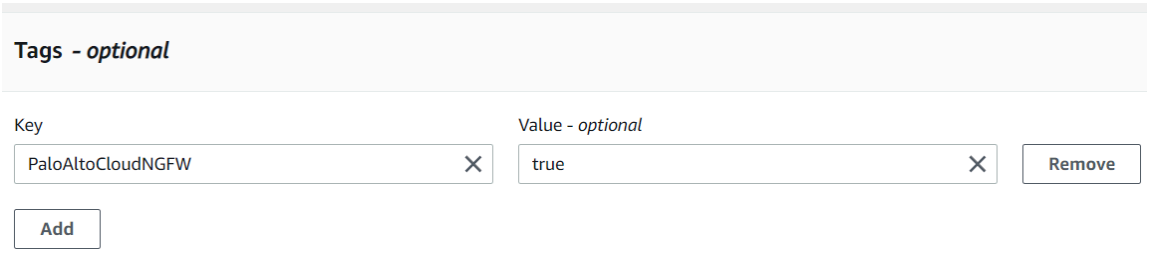
Effectuez la procédure suivante pour ajouter un certificat à utiliser avec Cloud NGFW pour AWS.

STEP 1 | Ajoutez votre certificat à AWS Secrets Manager.

1. Connectez-vous à la console AWS, accédez à AWS Secrets Manager, puis cliquez sur **Store a new secret (Stocker un nouveau secret)**.
2. Sélectionnez **Other type of secret (Autre type de secret)**.
3. Sous **Key/value pairs (Paires de clé/valeur)**, créez une clé appelée **clé privée** et une autre appelée **clé publique**.
4. Collez toute votre clé privée et votre clé publique entière dans le champ correspondant.



5. Cliquez sur **Next (Suivant)**.
6. Entrez un nom descriptif dans **Secret Name (Nom du secret)**.
7. Ajoutez une étiquette avec la clé **PaloAltoCloudNGFW** et la valeur **true**.



8. Cliquez sur **Next (Suivant)**, **Next (Suivant)** et **Store (Stocker)** pour terminer l'ajout de votre certificat.

STEP 2 | Sélectionnez **Rulestacks** et sélectionnez une rulestack précédemment créée sur laquelle configurer un certificat.

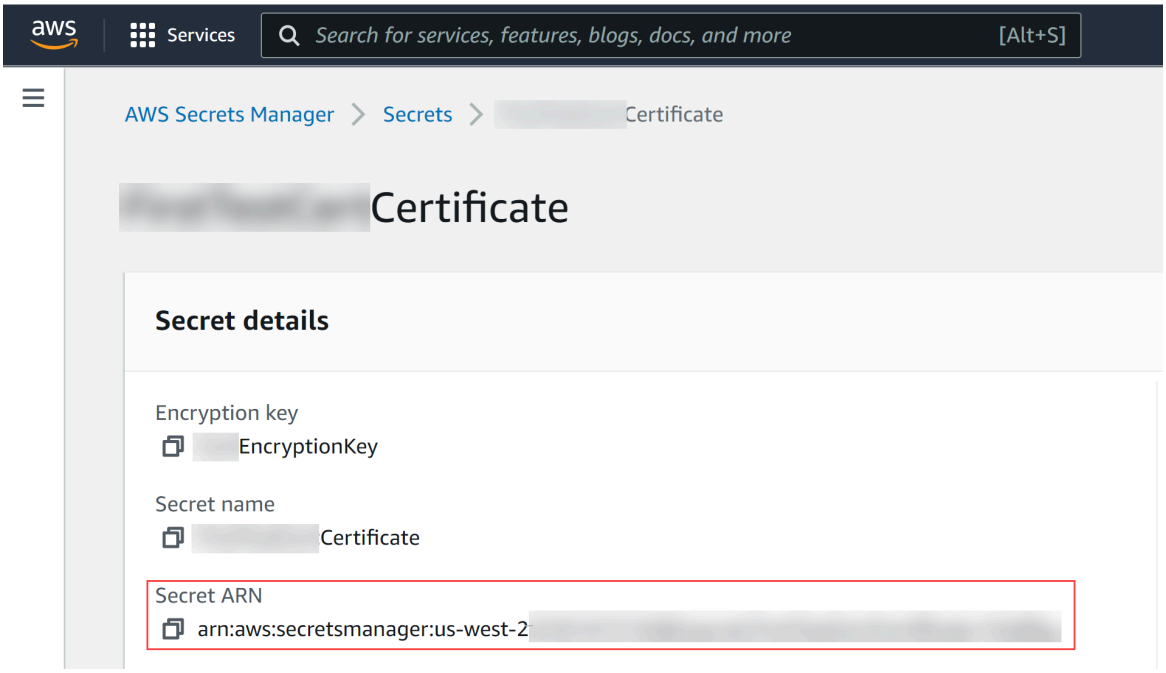
STEP 3 | Sélectionnez **Objects (Objets)** > **Certificate List (Liste des certificats)** > **Add Certificate (Ajouter un certificat)**.

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

STEP 5 | (facultatif) Entrez une description pour votre certificat.

STEP 6 | Sélectionnez le certificat.

- Entrez la valeur **Certificate ARN (ARN du certificat)** si vous souhaitez que Cloud NGFW télécharge le certificat à partir d'AWS Secrets Manager.



- Cochez **Self Signed Certificate (Certificat auto-signé)** si vous souhaitez que Cloud NGFW crée un certificat auto-signé.

STEP 7 | Cliquez sur **Save (Enregistrer)**.

Créer des règles de sécurité sur Cloud NGFW pour AWS

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 AWS, 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.

Vous pouvez afficher le nombre de fois où le trafic a atteint une règle spécifique en accédant à **Rulestacks** > **<rulestack-name>** > **Security Rules (Règles de sécurité)** > **<rule-name>** > **Usage (Utilisation)**. L'onglet Usage (Utilisation) affiche le nombre de fois que la règle suspecte a été déclenchée par du trafic passant par le NGFW. Le compteur de coups se rafraîchit toutes les 15 secondes.

De plus, vous pouvez afficher le compteur d'accès à la règle en sélectionnant **NGFWs (NGFW)** > **<firewall-name>** > **Rules (Règles)** > **<rule-name>**. Lorsque vous affichez le compteur d'accès à partir du menu NGFW, le compteur d'accès affiche le nombre de fois où la règle choisie a été déclenchée sur ce NGFW spécifique.

STEP 1 | Sélectionnez **Gérer les** > **Rulestacks** et sélectionnez la rulestack cible pour votre nouvelle règle.

STEP 2 | Cliquez sur **Create New (Créer nouveau)**. Lors de l'ajout d'une règle à une rulestack globale, vous devez choisir **Pre Rule (Règle « avant »)** ou **Post Rule (Règle « après »)**.

STEP 3 | 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)** ou **Match (Correspondance)**.

   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)**, cliquez sur l'icône d'ajout (+) et spécifiez au moins un objet source : adresse IP (CIDR), liste de préfixes, pays ou flux intelligent (type IP).

STEP 8 | Définissez la **Destination**.

1. Sélectionnez **Any (N'importe laquelle)** ou **Match (Correspondance)**.

   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)**, cliquez sur l'icône d'ajout (+) et spécifiez au moins un objet de destination : adresse IP (CIDR), liste de préfixes, liste FQDN, pays ou flux intelligent (type IP).

STEP 9 | Définissez le contrôle granulaire de l'**Application (App-ID)**.

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), cliquez sur l'icône d'ajout (+ −) et spécifiez l'application ou les applications.

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

1. Choisissez **Any (N'importe laquelle)** ou **Match (Correspondance)**.

   Lorsque vous choisissez **Any (N'importe laquelle)**, le trafic est évalué quelle que soit l'URL. Si vous spécifiez une ou plusieurs applications, le trafic est évalué par rapport à la règle si le trafic correspond à la catégorie d'URL spécifiée ou au flux intelligent (type d'URL).

2. Si vous choisissez **Match (Correspondance)**, sélectionnez **URLCategoryNames** ou **Feeds** et cliquez sur l'icône d'ajout (+ −). Dans la liste déroulante, sélectionnez une catégorie d'URL ou un flux intelligent.

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

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

   Si vous choisissez **Any (N'importe lequel)**, 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.

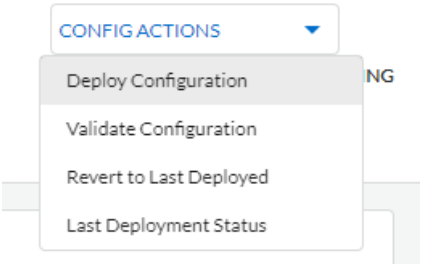
2. Si vous choisissez Select (Sélectionner), sélectionnez le protocole dans la liste déroulante et entrez le numéro de port. Vous pouvez spécifier un numéro de port unique ou utiliser des virgules pour spécifier plusieurs ports. Par exemple : 80, 8080

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)**, **Reset Server (Réinitialiser le serveur)**, ou **Reset Both (Réinitialiser les deux)** pour réinitialiser le client et le serveur.
2. Activez **Outbound TLS Decryption (Décryptage TLS sortant)**.
3. Activez **Logging (Journalisation)**.

STEP 13 | Cliquez sur **Create (Créer)**.

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



Utilisation des règles Cloud NGFW pour AWS

Utilisez Panorama pour gérer les règles sur votre ressource Cloud NGFW afin de suivre et surveiller l'utilisation des règles pour les opérations et les tâches de dépannage. Sur votre console Panorama, vous pouvez afficher l'utilisation des règles dans un groupe d'appareils cloud afin de déterminer si toutes les ressources Cloud NGFW, certaines d'entre elles ou aucune d'entre elles ont des correspondances de trafic.

Sur Panorama, vous pouvez afficher les détails de l'utilisation des règles pour les pare-feu gérés sur lesquels le nombre de correspondances d'utilisation des règles de politique est activé (par défaut) et sur lesquels vous avez défini des règles de politique et auxquels vous les avez transmis à l'aide de groupes d'appareils. Panorama ne peut récupérer les détails sur l'utilisation des règles pour les règles de politique configurées localement sur le pare-feu. Vous devez donc vous connecter au pare-feu pour afficher les informations sur l'utilisation des règles pour les règles configurées localement. Pour plus d'informations, consultez Surveiller l'utilisation des règles de politique.

Utilisation des règles – Nombre de correspondances et optimiseur de politique

Configuration système requise

Voici la configuration système minimale requise pour surveiller l'utilisation d'une règle de politique de sécurité :

- Panorama (PAN-OS) version 10.2.8 et supérieure
- Plug-in AWS version 5.2.0 et supérieure
- Plug-in services Cloud version 5.0.0 et supérieure
- Plug-in connecteur Cloud version 2.0.1 et supérieure

Afficher le nombre de correspondances de règle pour un groupe d'appareils Cloud

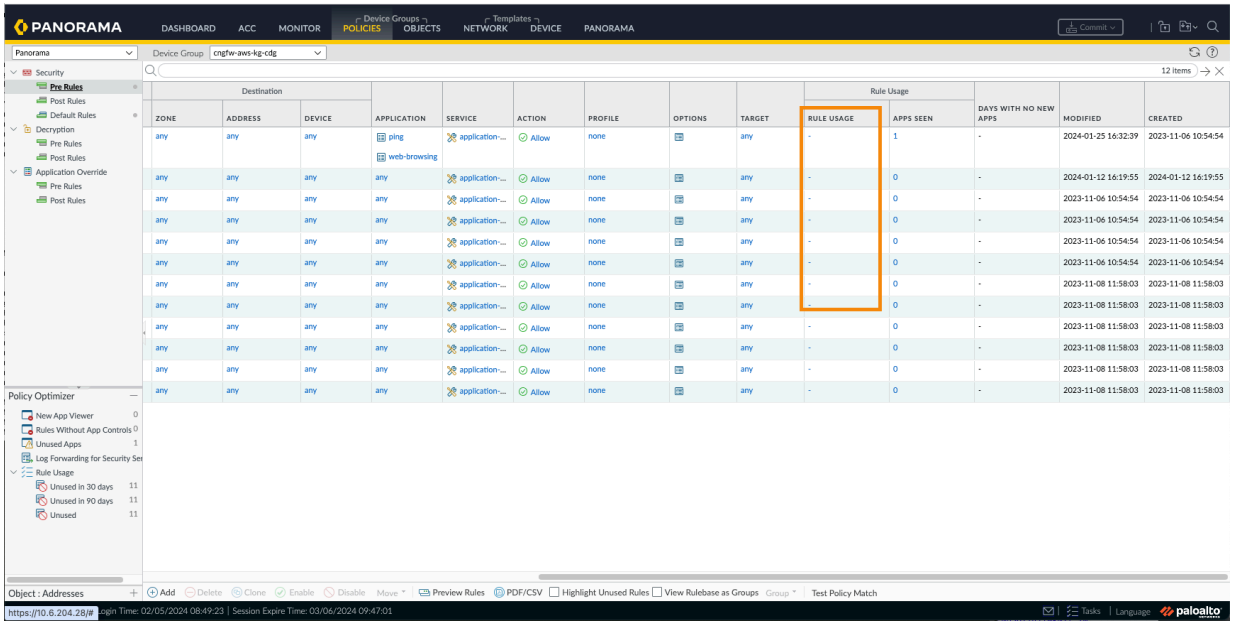
Dans la console Panorama, après avoir associé un groupe d'appareils cloud à une ressource Cloud NGFW et configuré des politiques pour le groupe d'appareils cloud, effectuez les étapes suivantes pour afficher le nombre de correspondances de règle pour un groupe d'appareils cloud dans Panorama :

Les ressources de pare-feu NGFW rapportent vos données de correspondance de règle toutes les deux minutes au service Cloud NGFW, et celui-ci dispose alors d'une latence de deux minutes maximum pour interroger les données des ressources de pare-feu. Cela crée une latence maximale de quatre minutes dans l'affichage des données du nombre de correspondances de règle sur la console Panorama.

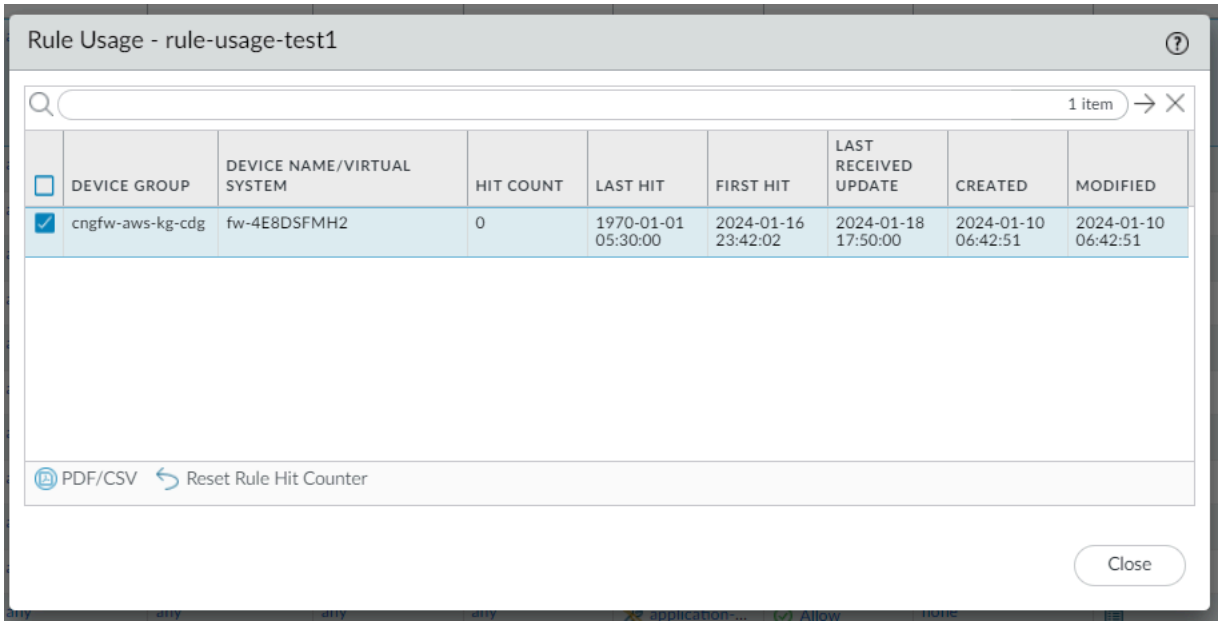
1. Sélectionnez **Policies (Politiques)**.
2. Dans la section **Device Group (Groupe d'appareils)**, utilisez la liste déroulante pour sélectionner le groupe d'appareils Cloud.

3. Sélectionnez une règle, puis cliquez sur **Rule Usage (Utilisation des règles)**.

   Vous pouvez surveiller l’état de l’utilisation des règles de vos types de politique pré, post et par défaut de sécurité, de décryptage et de contrôle prioritaire sur l’application.



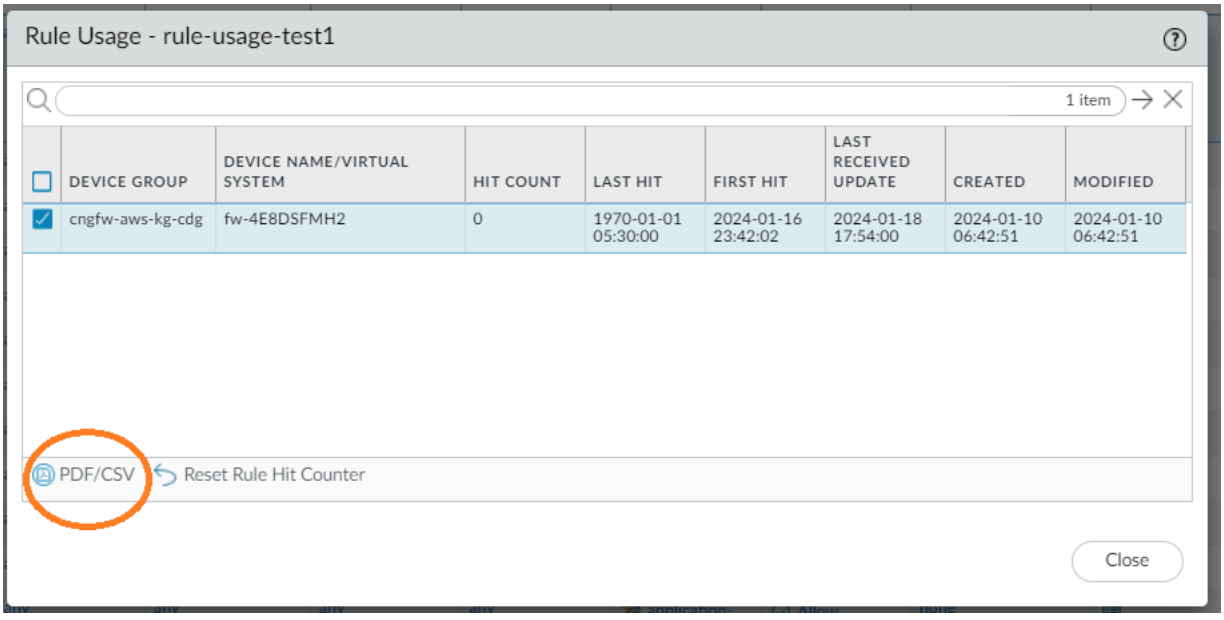
Vous pouvez maintenant voir le **Hit Count (Nombre de correspondances)** de la règle sélectionnée.



Dans la console Panorama, le nombre de correspondances de règle est actualisé pour chaque intervalle de quatre minutes, par défaut.

Cliquez sur **Reset Rule Hit Counter (Réinitialiser le compteur de correspondances de règle)** pour actualiser le nombre de correspondances de la règle sélectionnée.

Cliquez sur **PDF/CSV** pour exporter les détails de l'utilisation des règles pour une règle sélectionnée sous forme de fichier CSV ou PDF.

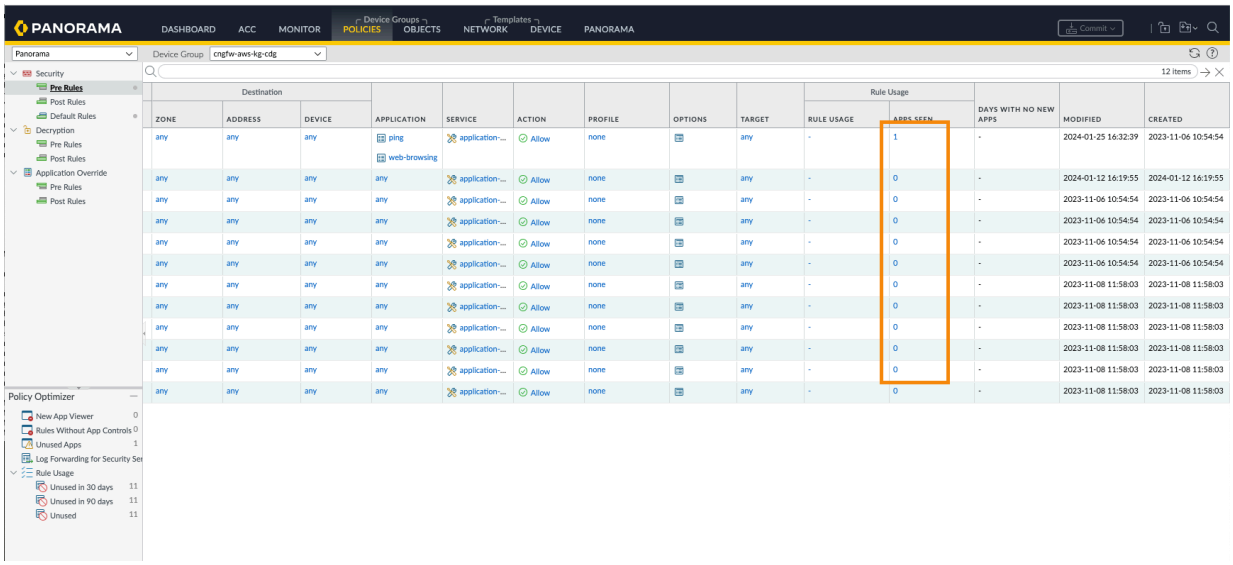


Utilisation des règles – Application vue et optimiseur de politique

Vous pouvez afficher toutes vos applications vues et autorisées sur le pare-feu qui correspondent à votre règle de politique de sécurité. Le chiffre de la colonne **Apps Seen (Applications vues)** indique le nombre d’applications vues dans la règle.

- Dans la console Panorama, accédez à l’onglet **Policies (Politiques)**.
- Dans la section **Device Group (Groupe d’appareils)**, utilisez la liste déroulante pour sélectionner le groupe d’appareils Cloud.

- Sélectionnez une règle, puis cliquez sur **Apps seen (Applications vues)**.



Vous pouvez désormais voir les applications configurées et affichées sur votre règle de politique de sécurité.

Pour plus d’informations sur les Applications d’une règle, Applications vues et Actions sur les applications vues, consultez Applications et utilisation.

Dans la section **Policy Optimizer (Optimisateur de politique)**, vous pouvez également afficher le nombre de correspondances de règle pour tous vos groupes d’appareils cloud configurés sur Panorama. L’optimiseur de politique offre un workflow simple pour migrer votre ancienne base de règles de politique de sécurité vers une base de règles basée sur App-ID, qui améliore la sécurité en réduisant la surface d'attaque et en vous procurant une visibilité des applications, ce qui vous permet de les activer en toute sécurité. Pour plus d’informations, consultez Optimisation de la règle de politique de sécurité et Applications et utilisation.

Profils de sécurité Cloud NGFW pour AWS

Cloud NGFW utilise vos définitions de rulestacks pour protéger votre trafic VPC 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.

  Le tableau suivant décrit la configuration par défaut de la vulnérabilité IPS selon les meilleures pratiques.

Gravité de la signature	Action
Critique	Réinitialiser les deux
Élevée	Réinitialiser les deux
Moyenne	Réinitialiser 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 communications phone-home ou de signalement sur les serveurs (C2) de commande et de contrôle externes par les logiciels espions sur les hôtes compromis. Ils vous permettent permet de détecter le trafic malveillant provenant de clients infectés et quittant le réseau

  Le tableau suivant décrit la configuration antispyware par défaut selon les meilleures pratiques.

Gravité de la signature	Action
Critique	Réinitialiser les deux
Élevée	Réinitialiser les deux

Gravité de la signature	Action
Moyenne	Réinitialiser les deux
Pour information	Par défaut
Faible	Par défaut

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 utiliser 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

Catégorie de menaces	Description
	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 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.

Catégorie de menaces	Description
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 tous des anomalies de protocole et peuvent 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 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).

Catégorie de menaces	Description
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 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 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.

Catégorie de menaces	Description
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.
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. Un acteur malveillant implante un shell Web 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

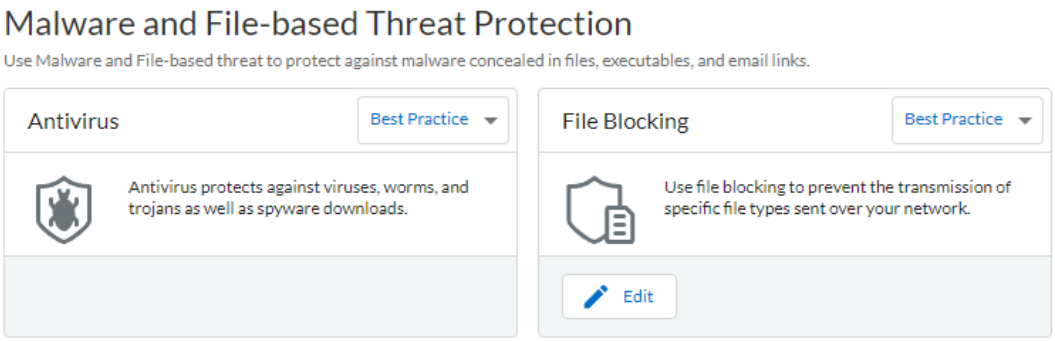
offrir aux clients une protection sans que les performances du pare-feu soient significativement altérées. Ce profil recherche une grande variété de logiciels malveillants dans les exécutables et les fichiers PDF, de virus HTML et JavaScript ; elle permet également l'analyse des fichiers compressés et des schémas de codage de données.

Le tableau suivant décrit la configuration antivirus par défaut selon les meilleures pratiques.

Protocole	Action
FTP	Réinitialiser les deux
HTTP	Réinitialiser les deux
HTTP2	Réinitialiser les deux
IMAP	Réinitialiser les deux
POP3	Alerter
SMB	Réinitialiser les deux
SMTP	Réinitialiser les deux

- **Blocage des fichiers** : un profil de blocage des fichiers vous permet d'identifier les 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. Pour plus d'informations sur la modification de votre profil de blocage des fichiers, consultez Configuration du blocage des fichiers.



Le tableau suivant décrit la configuration par défaut du blocage de fichiers selon les meilleures pratiques.

Types de fichier	Application	Direction	Action
Tous les types de fichiers à risque : • 7z • bat • cab • chm • class • cpl • dll • exe • flash • hip • hta • msi • Multi-Level-Encoding • ocx • PE • pif • rar • scr	indifférent	Les deux (charger et télécharger)	Bloquer

Types de fichier	Application	Direction	Action
• tar • torrent • vbe • wsf • encrypted-rar • encrypted-zip			
Tous les types de fichiers restants	indifférent	Les deux (charger et télécharger)	Alerter

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

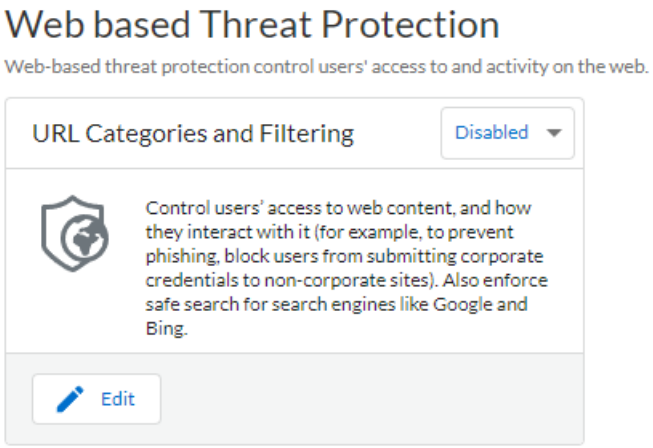
Catégorie de menaces	Description
Signatures antivirus	
apk	Fichiers malveillants d'application Android (APK).
MacOSX	Fichiers MacOSX malveillants, notamment : • Fichiers d’image disque Apple (DMG). • Les fichiers objet Mach (Mach-O) sont des exécutables, des bibliothèques et du code objet. • Packages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

Catégorie de menaces	Description
	• 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 des URL** : les profil 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



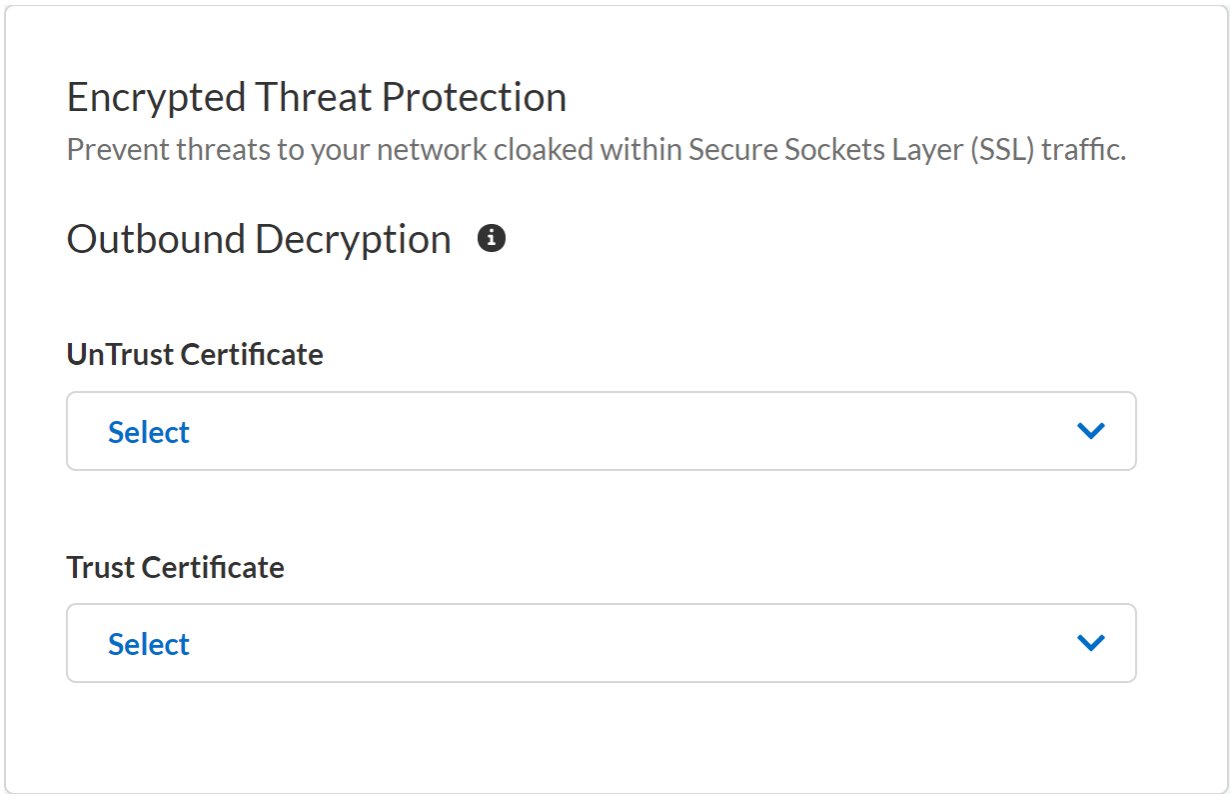
Le tableau suivant décrit la configuration par défaut du filtrage des URL selon les meilleures pratiques.

Catégories d'URL	Accès au site	Envoi des informations d’identification
Catégories malveillantes et exploitantes : • adulte • commande et contrôle • violation des droits d’auteur • DNS dynamique • extrémisme • logiciel malveillant • parqué • phishing • contournement de proxy et anonymiseurs • inconnue	Bloquer	Bloquer
Toutes les autres catégories d’URL	Alerter	Alerter

Protection contre les menaces cryptées

- **Décryptage sortant** : un profil de décryptage sortant vous permet de préciser le trafic selon la destination, la source, le service ou la catégorie d'URL et de bloquer, de restreindre ou de transmettre le trafic précisé selon les paramètres de sécurité du profil de décryptage associé. Un profil de décryptage sortant contrôle les protocoles SSL, la vérification des certificats et les vérifications des échecs pour empêcher le trafic qui utilise des algorithmes faibles ou des modes non pris en charge d’accéder au réseau. Les ressources Cloud NGFW utilisent des certificats pour déchiffrer le trafic en texte en clair. Il

applique ensuite les profils App-ID et de sécurité sur le trafic de texte en clair, notamment les profils de décryptage, d'antivirus, de vulnérabilité, d'antispyware, de filtrage des URL et de 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.



Catégories d'URL prédéfinies pour Cloud NGFW pour AWS

Le tableau suivant décrit les catégories d’URL prédéfinies disponibles sur Cloud NGFW sur AWS. 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.
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.

Catégorie d'URL	Description
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 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, tels que 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

Catégorie d'URL	Description
	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.
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

Catégorie d'URL	Description
	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 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,

Catégorie d'URL	Description
	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 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 tutoriels 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 soutiennent 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 (telles que 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.

Catégorie d'URL	Description
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 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,

Catégorie d'URL	Description
	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.
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 partagiciels 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.

Catégorie d'URL	Description
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 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.

Catégorie d'URL	Description
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.
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 continu.
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 de l'éducation et de la formation en ligne et du matériel connexe. Peut inclure des écoles de conduite / de circulation, une formation en milieu 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.

Catégorie d'URL	Description
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.

Configurer l'accès au site pour les URL sur Cloud NGFW pour AWS

Un profil de sécurité de filtrage des URL protège contre les menaces Web et vous permet de contrôler étroitement les ressources Web auxquelles vos charges de travail VPC peuvent accéder.

Lorsque le trafic passe par votre NGFW pour atteindre une URL, le NGFW autorise ce trafic en fonction de l'action que vous définissez pour la catégorie à laquelle cette URL appartient. Les actions d'accès au site que vous pouvez définir sont :

- **Alert (Alerter)** : sélectionnez alert (alerter) afin d'avoir une visibilité des sites auxquels vos utilisateurs accèdent. Le trafic correspondant est autorisé, mais un journal de URL filtering est généré pour journaliser les situations où un utilisateur accède à un site appartenant à cette catégorie.
- **Allow (Autoriser)** : le trafic destiné à cette catégorie est autorisé. En outre, le trafic autorisé n'est pas enregistré.
- **Block (Bloquer)** : refuse l'accès au trafic correspondant à cette catégorie et active la journalisation du trafic bloqué.

Pour tirer le meilleur parti de votre déploiement du filtrage des URL, vous devez commencer par créer des règles d'autorisation pour les applications desquelles vous dépendez pour exercer vos activités. Examinez ensuite les catégories d'URL qui classent le contenu malveillant et à risque. Nous vous recommandons ces types de catégories immédiatement.

Lorsque vous déployez le filtrage des URL pour la première fois, nous vous recommandons de commencer par une configuration de base qui nous donne une visibilité sur les modèles d'activité Web tout en bloquant le contenu malveillant confirmé. Vous pouvez commencer par bloquer les catégories connues pour être malveillantes : logiciel malveillant, commande et contrôle et hameçonnage. Pour les autres catégories, définissez-les sur alerte pour obtenir une visibilité sur les sites auxquels vos utilisateurs accèdent. Ensuite, vous pouvez décider ce que vous voulez autoriser, limiter et bloquer.

Les alertes sur toute l'activité Web génèrent un grand nombre de fichiers journaux, vous pouvez donc le faire dans un premier temps, puis modifier vos actions d'accès au site pour mieux répondre à vos besoins.

Procédez comme suit pour définir l'accès au site pour les catégories d'URL personnalisées et prédéfinies.

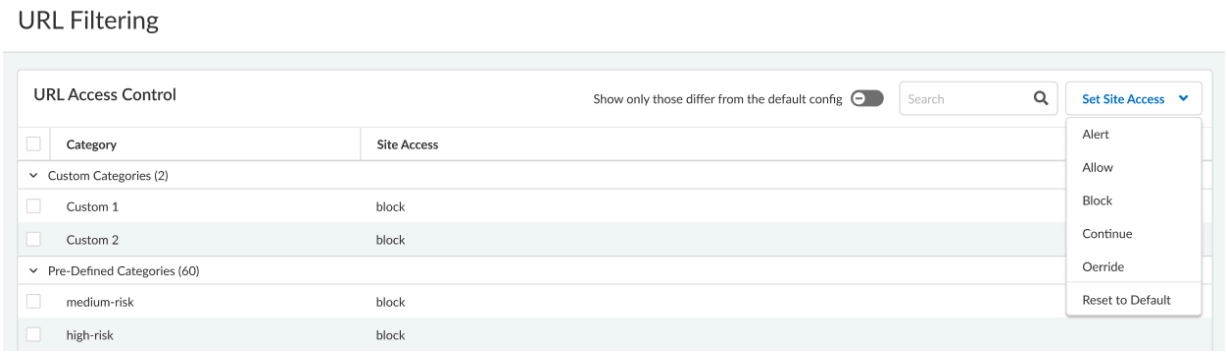
STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment sur laquelle configurer le filtrage des URL.

STEP 2 | Sélectionnez **Security Profiles (Profils de sécurité)** > **Web-based Threat Protection (Protection contre les menaces Web)** > **URL Categories & Filtering (Catégories et filtrage des URL)** > **Edit (Modifier)**.

STEP 3 | Sélectionnez la ou les catégories dans la liste affichée.

STEP 4 | Choisissez une option dans **Set Site Access (Définir l'accès au site)** pour les catégories sélectionnées dans la liste déroulante.

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



Configurer le blocage des fichiers sur Cloud NGFW pour AWS

Le blocage des fichiers vous permettent d'identifier les types de fichiers spécifiques que vous souhaitez bloquer ou surveiller. Pour la plupart du trafic (y compris le trafic sur votre réseau interne), bloquez les fichiers qui comportent généralement des menaces ou qui n'ont pas besoin d'être chargés ou téléchargés. Il s'agit de fichiers batch, de fichiers DLL, de fichiers de classe Java, de fichiers d'aide, de raccourcis Windows (.lnk) et de fichiers BitTorrent.

Cloud NGFW peut effectuer les actions suivantes sur les fichiers se déplaçant sur votre réseau.

- **Alerter** : lorsque le type de fichier donné est détecté, un journal est généré dans le journal de filtrage des données.
- **Block (Bloquer)** - Lorsque le type de fichier donné est détecté, le fichier est bloqué et une page de blocage est présentée à l'utilisateur. Une entrée est également générée dans le log de filtrage des données.
- **Continue (Continuer)** : lorsque le type de fichier donné est détecté, l'utilisateur voit une page de réponse s'afficher. L'utilisateur peut cliquer sur la page pour télécharger le fichier. Une entrée est également générée dans le log de filtrage des données. Comme ce type d'action de transfert nécessite l'intervention de l'utilisateur, il s'applique uniquement au trafic Web.

De plus, vous pouvez autoriser ou bloquer des types de fichiers en fonction de leur direction : Télécharger, Charger ou Charger et télécharger.

STEP 1 | Sélectionnez **Rulestacks** et sélectionnez une rulestack créée précédemment sur laquelle configurer le blocage de fichiers.

STEP 2 | Sélectionnez **Security Profiles (Profils de sécurité)** > **Malware and File-based Threat Protection (Protection contre les logiciels malveillants et les menaces basées sur les fichiers)** > **File Blocking (Blocage des fichiers)** > **Edit (Modifier)**.

STEP 3 | Sélectionnez le ou les types de fichiers dans la liste affichée.

STEP 4 | Définissez l'**Action** et la **Direction of traffic (Direction du trafic)** pour les types de fichiers sélectionnés dans les listes déroulantes.

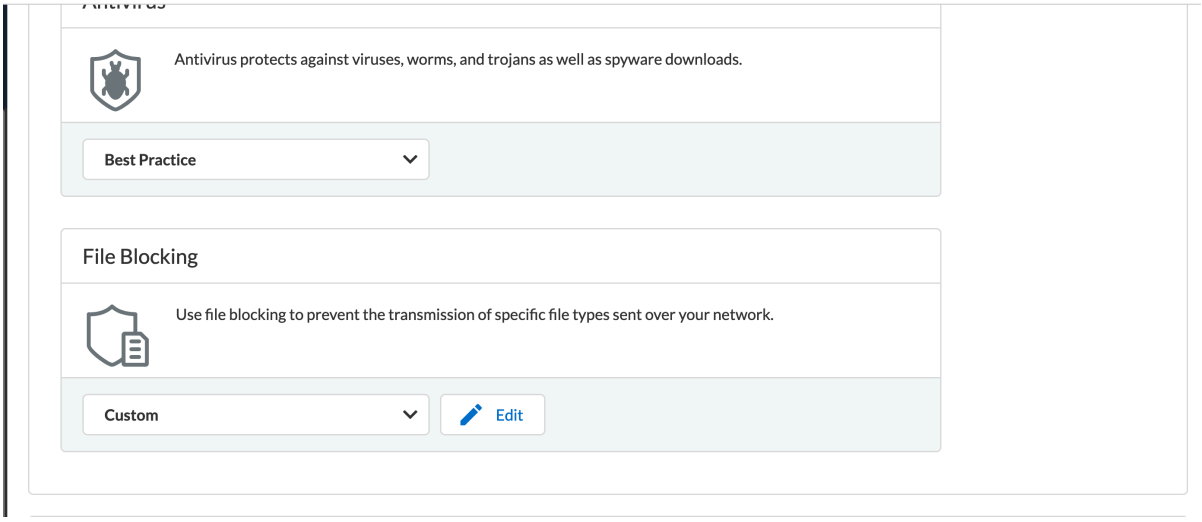
STEP 5 | Cliquez sur **Save (Enregistrer)**.

Modifier le profil de blocage de fichiers

Par défaut, le profil de blocage de fichiers est défini sur **best practice (meilleures pratiques)**. Pour modifier le profil de blocage de fichiers :

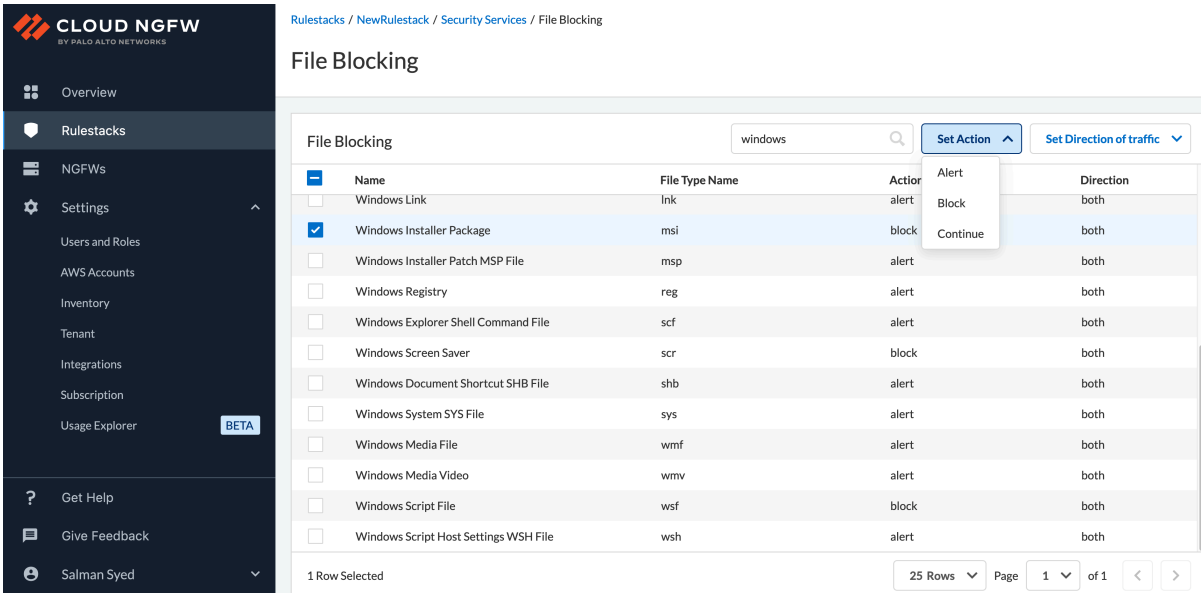
STEP 1 | Dans l'écran **Malware and File-based Threat Protection (Protection contre les logiciels malveillants et les menaces basées sur les fichiers)**, accédez à **File Blocking (Blocage des fichiers)**.

STEP 2 | Utilisez la liste déroulante pour sélectionner **Custom (Personnalisé)**.



STEP 3 | Ouvrez la console Cloud NGFW. Accédez à **Rulestacks > Rulestack name (Nom de la rulestack) > Security Services (Services de sécurité) > File Blocking (Blocage des fichiers)**.

STEP 4 | Dans la liste déroulante **Set Action (Définir l'action)**, modifiez l'action en **Alert (Alerte)** ou **Continue (Continuer)**.



Configurer le décryptage sortant sur Cloud NGFW pour AWS

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 intacts vos en-têtes et la charge utile de vos paquets de trafic, offrant une visibilité complète de l'identité de la source à vos destinations.

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 VPC 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 de la règle.

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

STEP 2 | Sélectionnez **Security Services (Services de sécurité)** > **Outbound Decryption (Décryptage sortant)**.

La valeur CA indiquée sous les contraintes de base dans le certificat CA doit être définie sur **true (vrai)**.

STEP 3 | Sélectionnez un certificat.

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

Créez un certificat *si vous ne l'avez pas déjà fait.*

Le certificat et la clé privée sont stockés dans AWS Secrets Manager (ASM) et la charge de travail utilise ces informations pour déchiffrer 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 le certificat est une chaîne, utilisez le certificat feuille et la clé. Importez le certificat CA racine et le certificat CA intermédiaire dans le magasin de confiance du client. Voici un exemple de la façon d'importer le certificat Root CA et le certificat Intermediate CA dans le magasin de confiance du système d'exploitation Ubuntu.

```
$ sudo apt-get install -y ca-certificates $ sudo cp root-ca.crt /
usr/local/share/ca-certificates $ sudo cp intermediate-ca.crt /usr/
local/share/ca-certificates $ sudo update-ca-certificates
```

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 l'ASM.

Le format de certificat pris en charge est PKCS8.

Le décryptage de confiance sortant ne prend pas en charge les certificats auto-signés.

STEP 4 | Cliquez sur **Save (Enregistrer)**.

Configurer le décryptage entrant sur Cloud NGFW pour AWS

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 VPC.

Votre certificat et votre clé de session sont stockés sur AWS Secrets Manager 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.

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.
- **Rule Priority (Priorité de la règle)** : 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 **Applications(App-ID™)** que vous souhaitez que la règle autorise ou bloque.

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

- Précisez une **URL Category (Catégorie d'URL)** en tant que critère de correspondance de la règle.
- Renseignez le champ **Protocol and Ports (Protocole et ports)** pour spécifier le protocole et les ports que vous souhaitez que la règle autorise ou bloque.

STEP 6 | Spécifiez l'**Action** que vous souhaitez que le pare-feu entreprenne lorsque le trafic correspond à l'une des règles que vous avez créées.

- **Allow (Autoriser)** : autoriser le trafic.
- **Deny (Refuser)** : bloque le trafic et applique l'*action Refuser* 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 7 | Sous **TLS Decryption (Décryptage TLS)**, sélectionnez **Inbound (Entrant)** et sélectionnez un **Inbound Inspection Certificate (Certificat d'inspection entrante)**.

Créez un certificat *si vous ne l'avez pas déjà fait. L'Amazon Resource Name (ARN) du secret doit être utilisé dans l'ARN du certificat lors de la création de l'objet de certificat.*

Le certificat et la clé privée sont stockés dans AWS Secrets Manager (ASM) et l'Application Load Balancer (ALB) utilise ces informations pour déchiffrer le trafic. Le certificat ne doit pas nécessairement être un certificat CA. Si le certificat est une chaîne, utilisez le certificat feuille et la clé.

Le format de certificat pris en charge est PKCS8.

Le décryptage entrant ne prend pas en charge les certificats auto-signés.

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.*

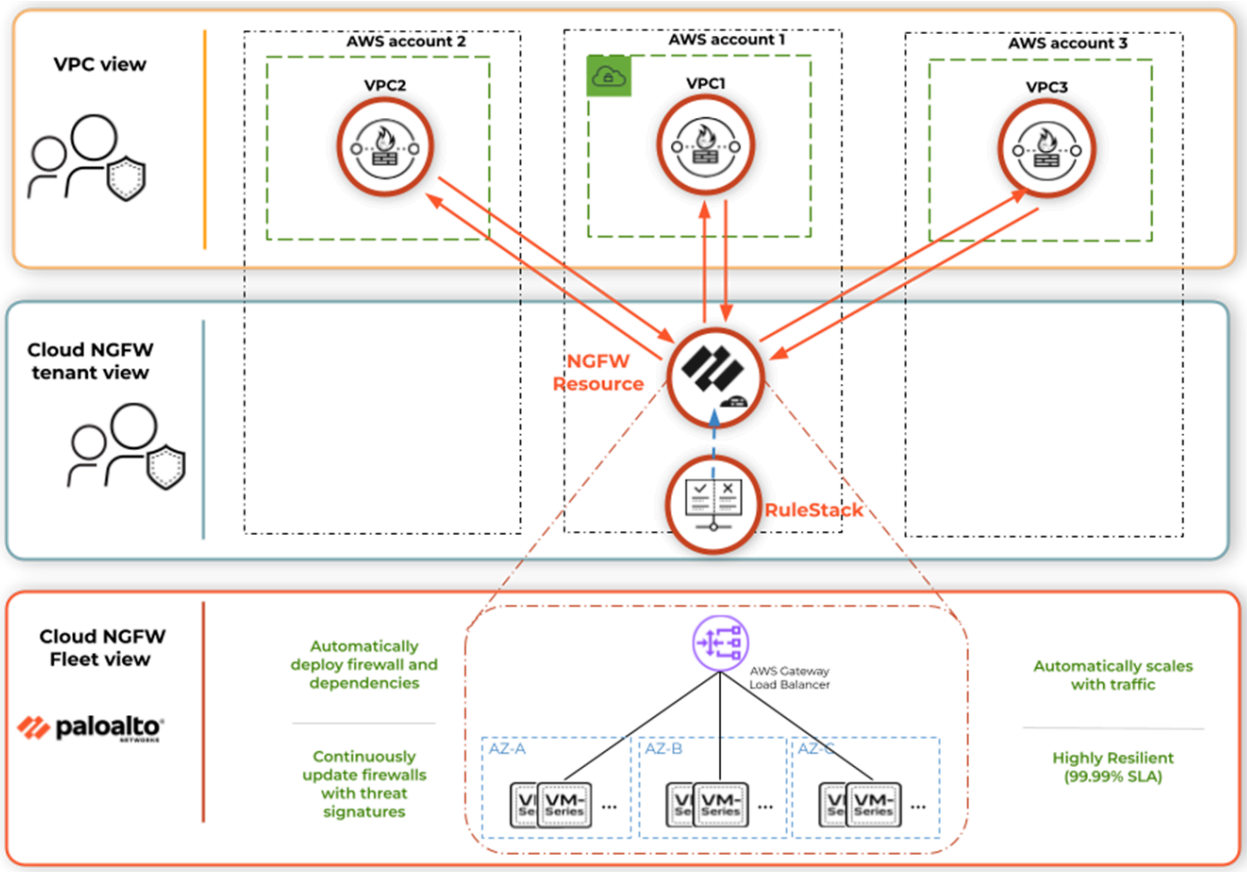
STEP 8 | Cliquez sur **Enabled (Activé)** pour activer la journalisation.

STEP 9 | Cliquez sur **Save (Enregistrer)**.

STEP 10 | Cliquez sur **Config Actions (Actions de configuration)** > **Deploy Configuration (Déployer la configuration)** > **Commit (Valider)** pour enregistrer la règle dans la configuration en cours d'exécution du pare-feu.

Ressource Cloud NGFW et terminaux NGFW

Le NGFW est une ressource de pare-feu, dédiée au VPC que vous spécifiez, qui fournit des fonctionnalités de pare-feu nouvelle génération. Lors de sa création, un NGFW est associé à un ou plusieurs VPC. Les terminaux NGFW sont des constructions créées manuellement ou automatiquement dans chaque zone de disponibilité des VPC que vous spécifiez. Le NGFW applique votre politique de sécurité au trafic reçu par les terminaux NGFW et applique cette politique. Lors de la création de votre NGFW, vous devez spécifier au moins un VPC et une rulestack locale. En outre, vous devez également spécifier comment et où les terminaux NGFW associés sont déployés.



Les terminaux des NGFW sont chargés de diriger le trafic vers le NGFW pour inspection et application. Les terminaux NGFW interceptent le trafic et l'acheminent vers le NGFW pour inspection et application des politiques. Il existe deux modes de gestion qui peuvent être utilisés pour créer des terminaux automatiquement ou manuellement.

- En **mode géré par le service**, le locataire Cloud NGFW crée un terminal dans chaque sous-réseau que vous spécifiez. Le service NGFW récupère une liste de sous-réseaux dans le VPC que vous avez spécifié et, dans cette liste, vous choisissez les sous-réseaux qui doivent avoir un terminal.
- En **mode géré par le client**, vous choisissez les zones de disponibilité existantes qui doivent être sécurisées dans votre VPC spécifié, puis créez manuellement les terminaux NGFW dans les sous-réseaux existants dans les zones de disponibilité choisies. Une fois le NGFW créé, vous devez accéder à la console AWS pour terminer le processus de création de terminal NGFW.

Après avoir créé un NGFW et des terminaux NGFW vous devez mettre à jour vos tables de routage AWS pour vous assurer que le trafic est envoyé au NGFW. Les tables de routage que vous mettez à jour et la façon dont vous les mettez à jour dépendent de votre déploiement spécifique. Pour obtenir des exemples de déploiement, consultez Diriger le trafic vers Cloud NGFW pour AWS avec des exemples de tables de routage pour vous guider.

- Créer une ressource NGFW sur AWS
- Créer et afficher des terminaux NGFW
- Diriger le trafic vers Cloud NGFW pour AWS
- Configurer la journalisation pour Cloud NGFW sur AWS
- Activer la journalisation d'audit sur Cloud NGFW pour AWS
- Supprimer une ressource Cloud NGFW

Créer une ressource NGFW sur AWS

Maintenant que vous avez créé des rulestacks et des règles, vous pouvez créer une ressource NGFW et associer une rulestack locale à ce NGFW. Lors de la configuration de votre NGFW, vous devez choisir comment les terminaux NGFW sont créés, automatiquement ou manuellement. Si vous décidez de créer manuellement des terminaux NGFW, vous devez créer des terminaux NGFW dans les zones de disponibilité que vous spécifiez.

Procédez comme suit pour créer un NGFW.

STEP 1 | Sélectionnez **NGFWs (NGFW)**.

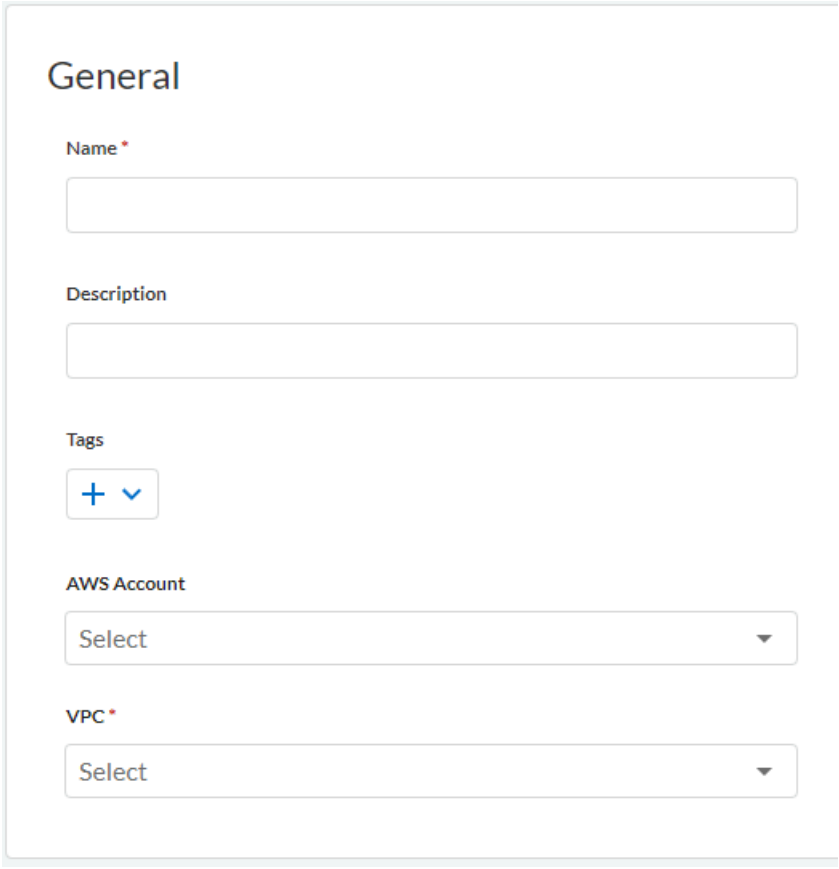
STEP 2 | Cliquez sur **Add Firewall (Ajouter un pare-feu)**.

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

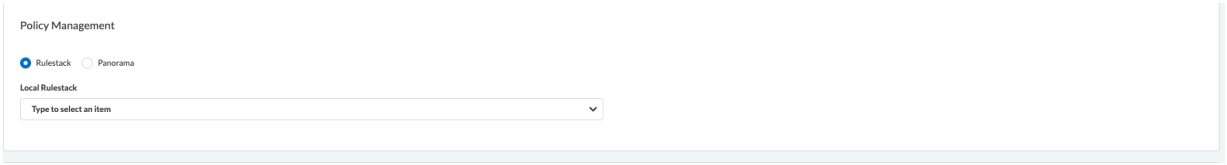
STEP 4 | (Facultatif) Saisissez une **Description (Description)**.

STEP 5 | Sélectionnez un **AWS Account (Compte AWS)** dans la liste déroulante à associer à ce NGFW.

STEP 6 | Sélectionnez un **VPC** dans la liste déroulante.



STEP 7 | Dans la section **Policy Management (Gestion des politiques)**, sélectionnez une **Local Rulestack (Rulestack locale)** dans la liste déroulante.

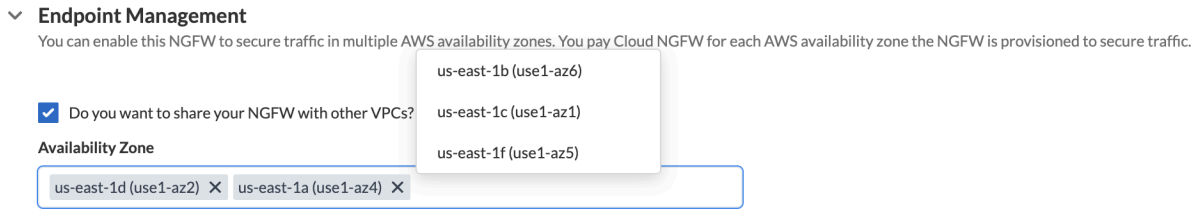


STEP 8 | Spécifiez des zones de disponibilité ou des sous-réseaux AWS. Vous devez spécifier si le locataire Cloud NGFW déploiera ou non (mode généré par le service) ou (mode géré par le client) ou les terminaux NGFW.

- **Yes (Oui)** (géré par le service) : en mode géré par le service, le locataire Cloud NGFW crée automatiquement des terminaux NGFW dans les sous-réseaux VPC que vous spécifiez. Effectuez la gestion de terminal pour le mode géré par le service via la console Cloud NGFW uniquement. La gestion des terminaux pour le mode géré par le service ne peut être réalisée qu'en associant ou en dissociant un sous-réseau. L'association d'un sous-réseau crée le terminal et la dissociation d'un sous-réseau le supprime.
- **No (Non)** (géré par le client) : en mode géré par le client, vous devez créer manuellement des terminaux NGFW dans chaque zone de disponibilité que vous spécifiez.

> *Dans la section **Endpoint Management (Gestion des terminaux)**, vous pouvez activer votre Cloud NGFW pour sécuriser le trafic dans plusieurs zones de disponibilité AWS. Vous payez pour chaque zone de disponibilité AWS dans laquelle votre NGFW est approvisionné pour sécuriser le trafic. Vous pouvez gérer la façon de créer les terminaux pour votre NGFW dans ces zones de disponibilité. Vous payez AWS pour chaque terminal VPC (équilibreur de charge de passerelle) que vous créez pour votre NGFW.*

L'**Availability Zone (Zone de disponibilité)** affiche le **Zone ID (ID de zone)** et le **Availability Zone Name (Nom de la zone de disponibilité)** correspondant dans votre compte Palo Alto Networks. Utilisez ces informations lors du mappage de vos zones de disponibilité sur vos comptes AWS.



STEP 9 | Cliquez sur **Create (Créer)**.

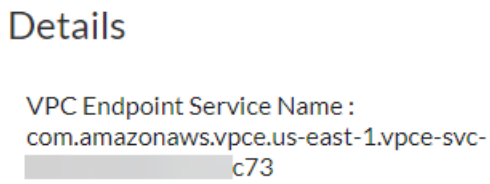
Créer et afficher des terminaux NGFW

Si vous avez sélectionné le mode géré par le client lors de la création d'un NGFW, vous devez créer manuellement les terminaux NGFW pour les sous-réseaux choisis. Dans la console AWS, les terminaux NGFW apparaissent en tant que terminaux d'équilibreur de charge de passerelle.

Les sous-réseaux auxquels vous attachez des terminaux NGFW doivent se trouver dans le VPC que vous avez spécifié lors de la création de NGFW.

STEP 1 | Dans le locataire Cloud NGFW, sélectionnez **NGFWs (NGFW)** et cliquez sur votre pare-feu.

STEP 2 | Sélectionnez **Endpoints (Terminaux)** et notez le nom du service des terminaux VPC.



STEP 3 | Connectez-vous à la console AWS.

STEP 4 | Sélectionnez **Services** > **Networking & Content Delivery (Mise en réseau et diffusion de contenu)** > **VPC**.

STEP 5 | Dans le tableau de bord VPC, sélectionnez **Endpoints (Terminaux)** > **Create Endpoint (Créer un terminal)**.

STEP 6 | Sélectionnez **Find service by name (Rechercher un service par nom)** et saisissez le nom qui correspond au service de terminaux VPC que vous avez noté ci-dessus.

STEP 7 | Sélectionnez le **VPC** que vous avez spécifié lors de la création du pare-feu dans la liste déroulante.

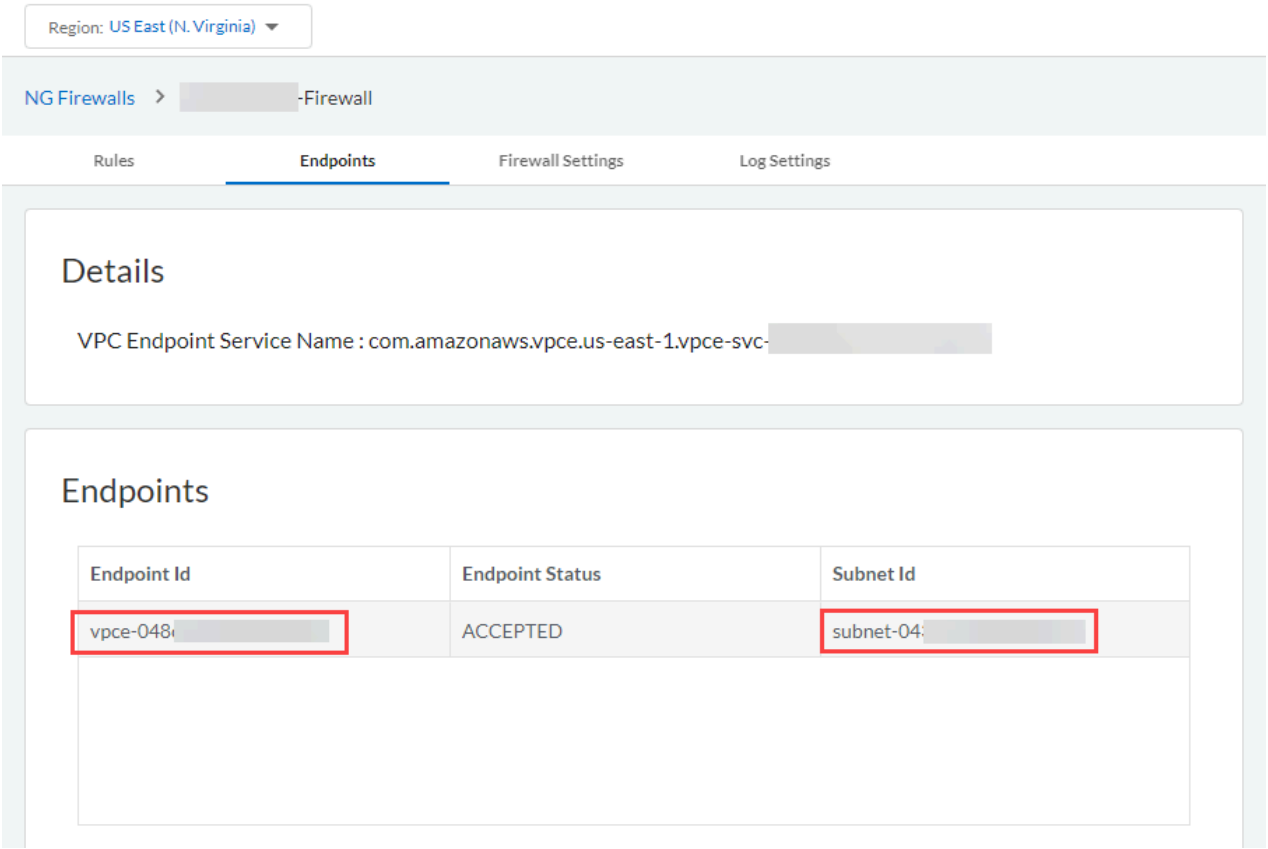
STEP 8 | Sélectionnez les sous-réseaux dans lesquels vous souhaitez créer des terminaux NGFW.

STEP 9 | Cliquez sur **Create endpoint (Créer terminal)**.

Diriger le trafic vers Cloud NGFW pour AWS

Une fois que vous avez déployé votre Cloud NGFW et créé des terminaux, vous devez mettre à jour vos tables de routage pour envoyer le trafic à votre pare-feu. Les tables de routage que vous mettez à jour et la façon dont elles sont mises à jour dépendent de votre déploiement spécifique.

Dans la console AWS, les terminaux NGFW sont affichés en tant que terminaux Gateway Load Balancer. Vous pouvez identifier les terminaux NGFW dans la console AWS par leur ID terminal. Vous pouvez trouver les ID terminaux pour un pare-feu spécifique dans la console Cloud NGFW sous **NGFWs (NGFW)** > **firewall-name** > **Endpoints (Terminaux)**.



Voici des exemples de flux de paquets dans différents modes de déploiement et incluent des exemples d'itinéraires mis à jour pour ces flux de paquets.

- Déploiements centralisés Cloud NGFW pour AWS
- Déploiements distribués Cloud NGFW pour AWS

Déploiements centralisés Cloud NGFW pour AWS

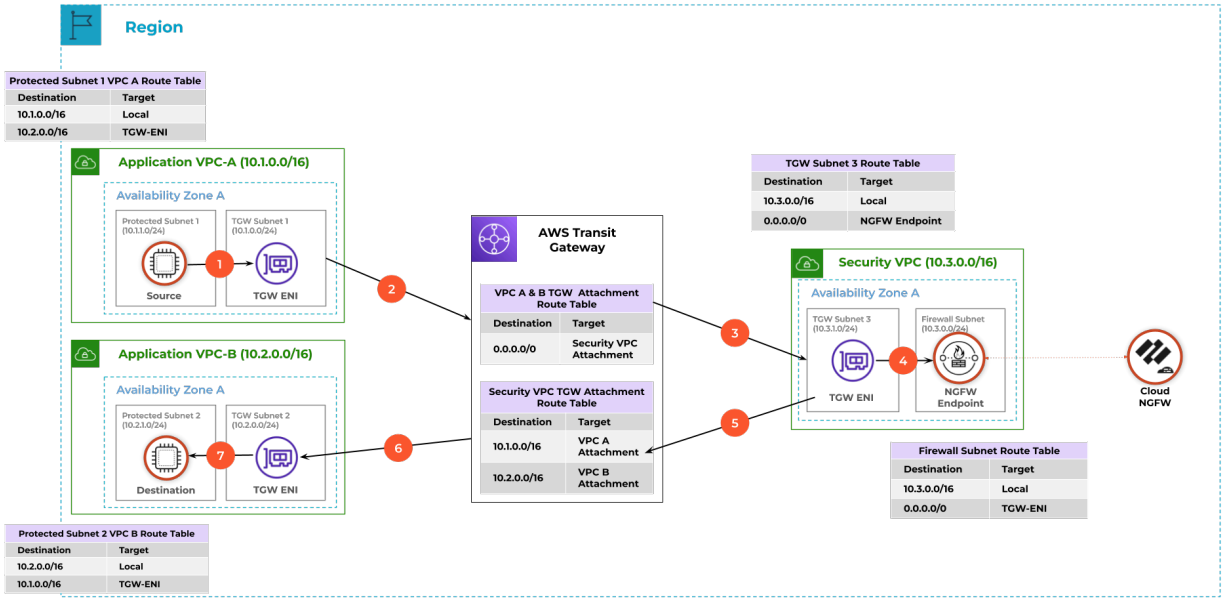
Dans un déploiement centralisé, vos composants Cloud NGFW sont déployés dans un VPC de sécurité centralisé. Le trafic doit toujours passer par une passerelle de transit AWS (TGW), qui agit comme un concentrateur réseau et simplifie la connectivité entre les VPC, ainsi que les réseaux sur site.

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 provenant de l'instance source est envoyé à l'ENI TGW.
2. L'ENI TGW dirige le trafic vers le TGW.
3. Le TGW achemine le trafic vers la sécurité VPC TGW ENI.
4. L'ENI TGW envoie le trafic au terminal NGFW et au NGFW pour 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. Le TGW transfère le trafic vers l'ENI TGW dans le VPC de destination.

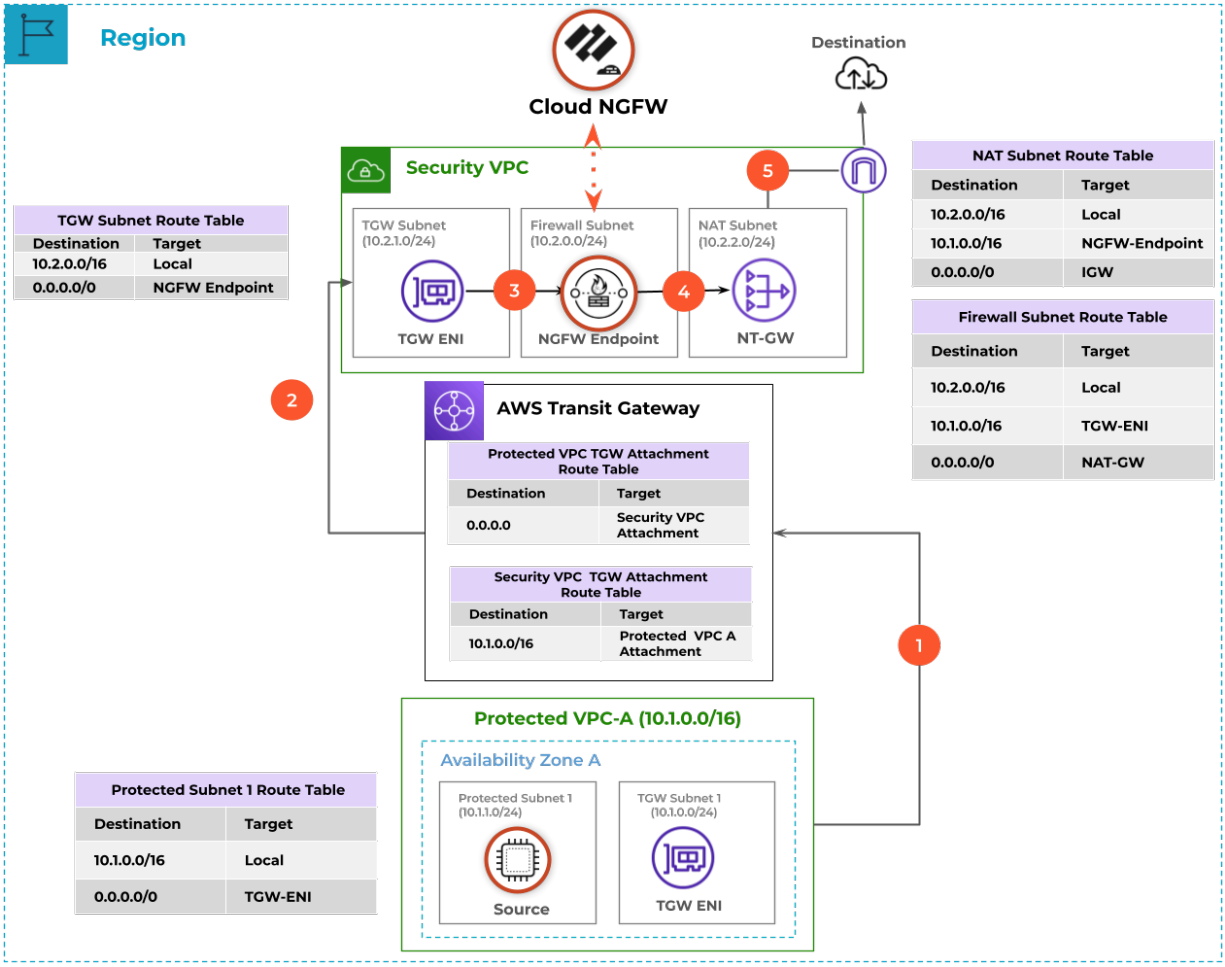
7. Ensuite, l’ENI TGW envoie le trafic vers la destination.



Sortie centralisée

1. Le trafic provenant de l’instance source est envoyé à l’ENI TGW et au TGW.
2. Le TGW achemine le trafic vers le VPC TGW ENI de sécurité.
3. L’ENI TGW envoie le trafic au terminal NGFW et au NGFW pour inspection.
4. Si le trafic est autorisé, le terminal NGFW achemine le trafic vers la passerelle NAT.

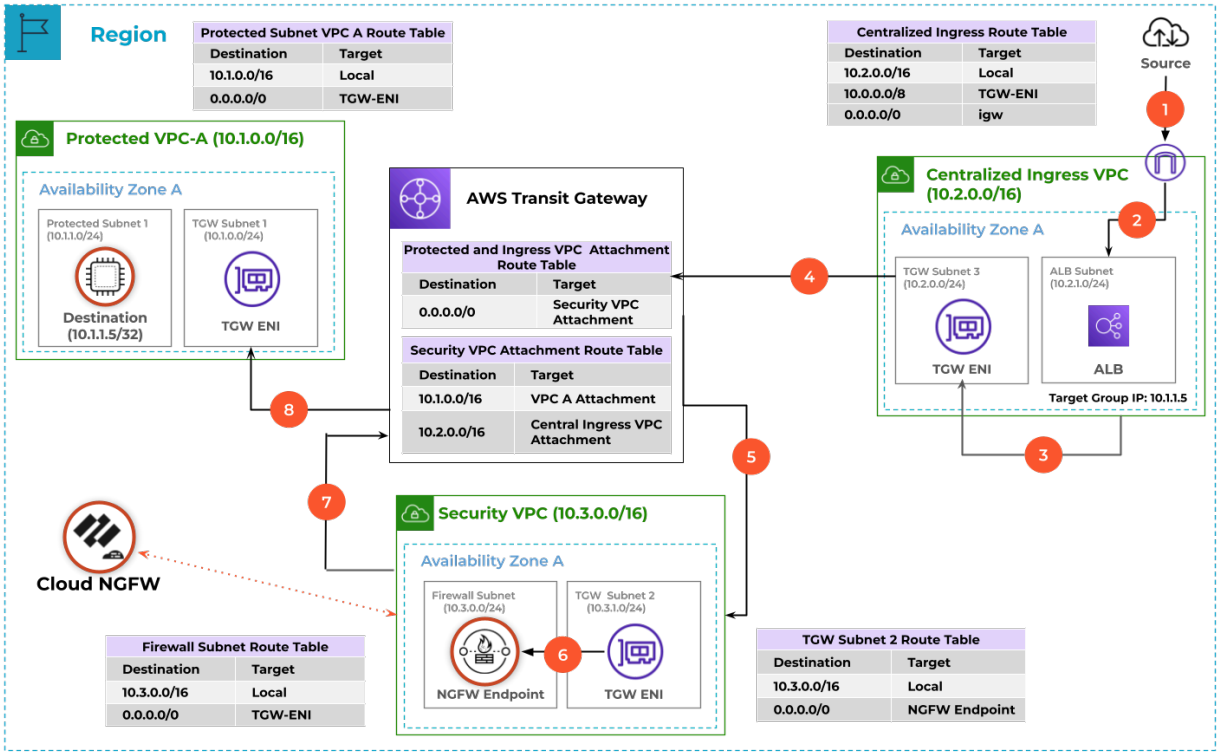
5. La passerelle NAT transmet le trafic à l’IGW et à la destination.



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 au VPC TGW ENI entrant.
4. L’ENI TGW envoie du trafic au TGW.
5. Le TGW achemine le trafic vers le VPC TGW ENI de sécurité.
6. L’ENI TGW envoie le trafic au terminal NGFW et au NGFW pour inspection.
7. Si le trafic est autorisé, le terminal NGFW envoie le trafic à TGW.

8. Le TGW achemine ensuite le trafic vers le VPC TGW ENI protégé, puis vers la destination.



Déploiements distribués Cloud NGFW pour AWS

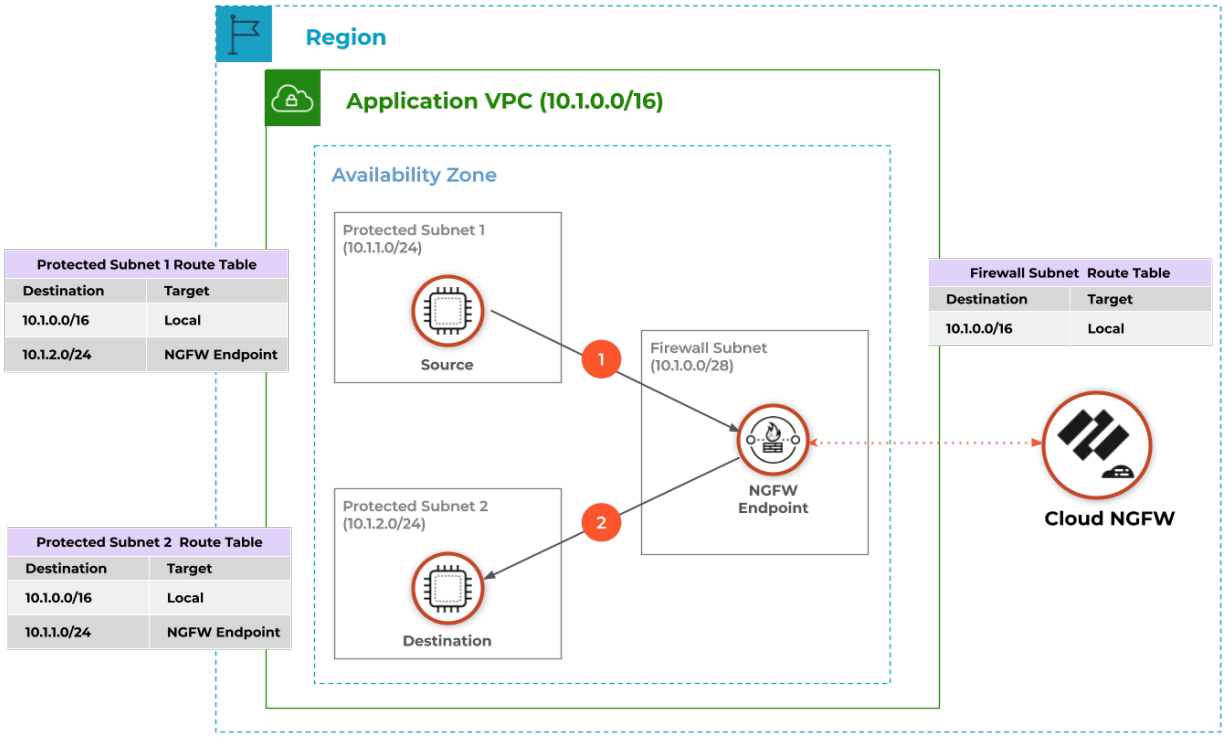
Dans un déploiement distribué, chaque VPC nécessitant une protection possède son propre NGFW. Cette méthode de déploiement est moins compliquée et, par conséquent, réduit les risques d’erreur de configuration.

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.

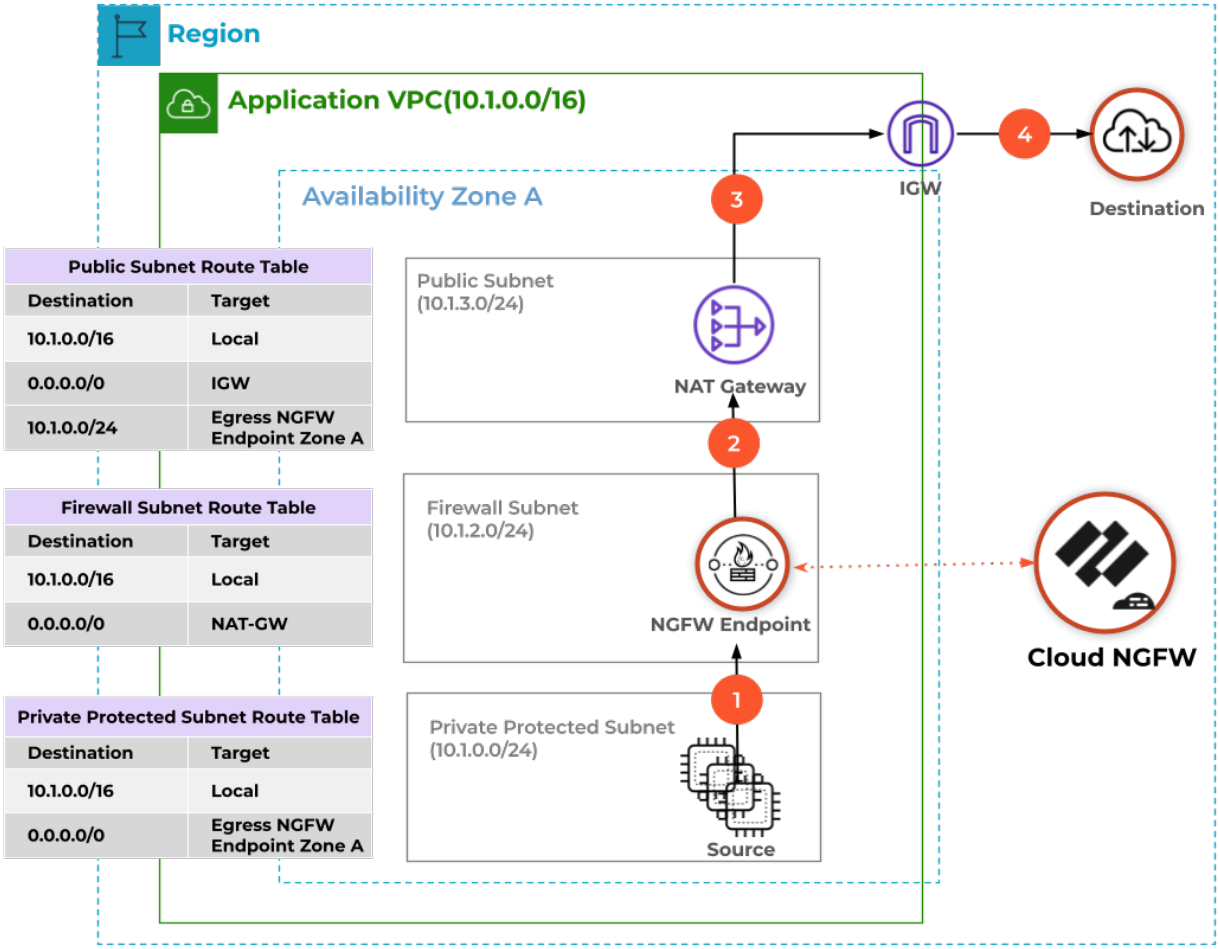
2. Si le trafic est autorisé, le terminal NGFW envoie le trafic vers la destination.



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.

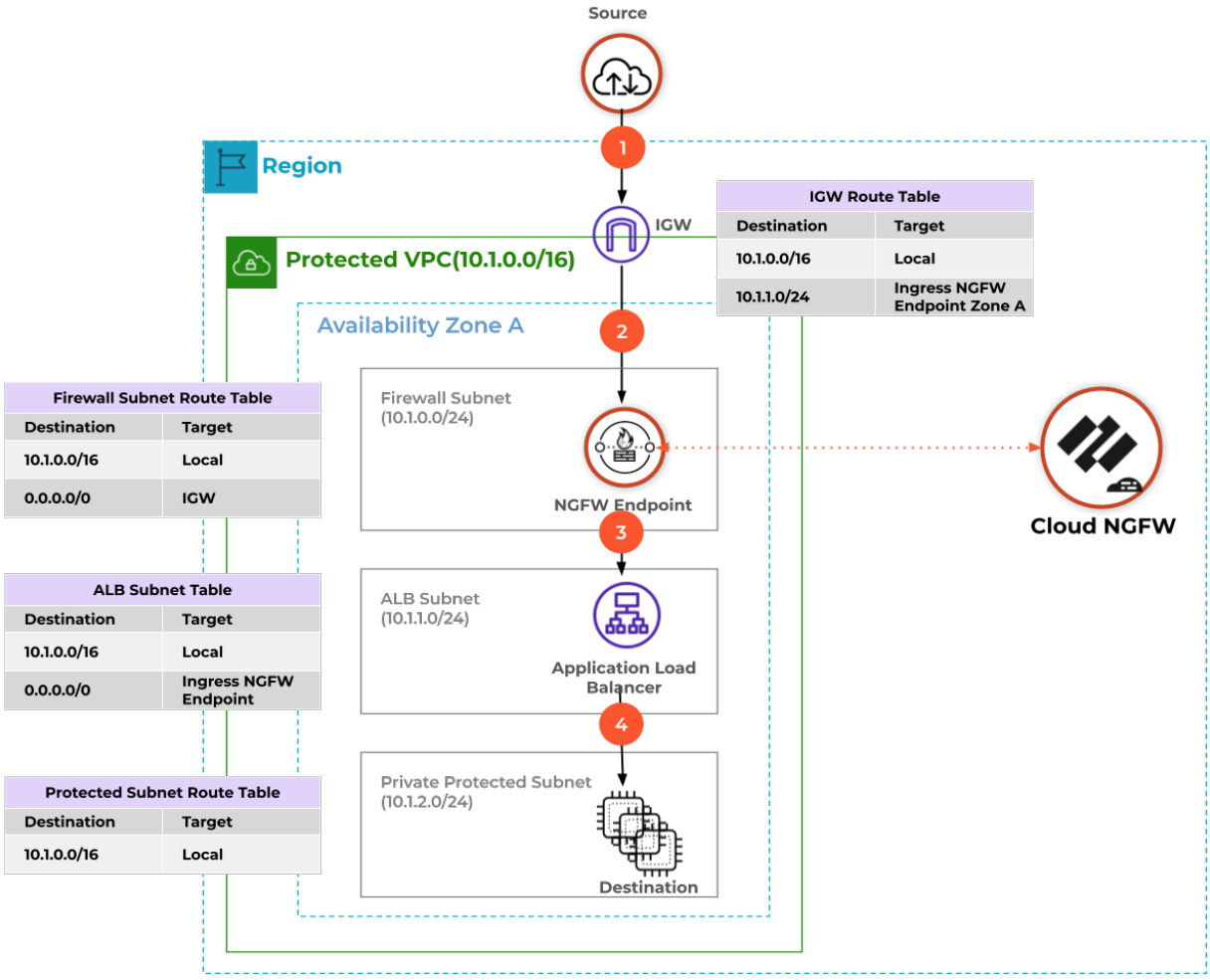
4. Le trafic continue vers Internet et la destination.



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.



Configurer la journalisation pour Cloud NGFW sur AWS

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.

Cloud NGFW vous permet d'envoyer des journaux de trafic, de menaces et de décryptage à un compartiment S3, à un groupe de journaux CloudWatch ou à Kinesis Data Firehose. Les noms de ces destinations de journal doivent être inclus dans le modèle Cloud NGFW CloudFormation lancé lorsque vous ajoutez votre compte AWS Tenet Admin au Cloud NGFW. CloudWatch Log Group et Kinesis Data Firehose ont une valeur par défaut **PaloAltoCloudNGFW** dans le CFT. Le compartiment S3 n'a pas de valeur par défaut. Cloud NGFW ne crée pas ces ressources dans votre environnement AWS. Le CFT donne au Cloud NGFW les autorisations d'écrire les journaux sur la destination. Une destination dont le nom a été fourni dans le CFT doit exister dans votre déploiement pour capturer correctement les journaux NGFW.

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 AWS.
- **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 AWS.

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

Sévérité	Description
	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 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 AWS.

Destination du journal

Vous avez trois choix de destination pour vos journaux Cloud NGFW. Ces destinations résident toutes en dehors du service Cloud NGFW, mais dans votre compte AWS : compartiment S3, groupe de journaux Cloudwatch ou Kinesis Data Firehose. Chaque fichier journal est généré sous forme de fichier JSON.

Lorsque vous vous abonnez à Cloud NGFW pour AWS (voir S'abonner à Cloud NGFW pour AWS), vous êtes invité à configurer votre pile de modèles AWS CloudFormation. La pile préremplit les destinations de journalisation pour le groupe de journaux CloudWatch et le flux de diffusion Kinesis Data Firehose avec une destination appelée **PaloAltoCloudNGFW**. Le champ de compartiment S3 n'est pas prérempli. Si vous souhaitez envoyer les journaux vers une autre destination, vous devez créer cette destination et remplacer la valeur par défaut par le nom avant de terminer la création de la pile.

Chaque ressource NGFW (affichée sous le nom NGFW dans le nom du flux de journaux) génère ses journaux dans plusieurs flux (distingués par la chaîne de caractères aléatoires dans le nom du flux de journaux). Par conséquent, les journaux d'une ressource Cloud NGFW particulière peuvent être répartis sur plusieurs flux.

Si vous envoyez les journaux à un groupe de journaux CloudWatch, vous pouvez afficher les entrées de journal directement dans la console AWS CloudWatch. Dans le groupe de journaux de configuration CloudWatch que vous spécifiez lors de la configuration de la journalisation, vous verrez une liste de flux de journaux. Le nom du flux de journal s'affiche comme suit :

```
/<aws-account-id>/<region>/<NGFW-name>/<random-string>/<log-type>.<year>.<month>.<day>.<hour>
```

Par exemple : /account123/us-west-1/firewall-1/qadd232312345dea/TRAFFIC.2022.02.10.23

<random string> fait référence à la ressource NGFW individuelle qui a généré le journal.

Vous pouvez cliquer sur le nom du flux pour afficher les entrées de journal, qui sont affichées comme indiqué dans l'exemple suivant.

Si vous envoyez les journaux à un compartiment S3, les fichiers journaux sont enregistrés en tant que fichier JSON. NGFW envoie un nouveau fichier journal lorsque l'un des critères suivants est rempli : le pare-feu a généré 256 Mo de journaux ou 10 minutes se sont écoulées depuis la génération du dernier fichier journal. Pour localiser les fichiers dans le compartiment S3 que vous spécifiez, accédez à la console S3 dans AWS et recherchez le compartiment que vous avez spécifié. Sélectionnez ensuite ***AWS-account-id*** > ***region*** > ***NGFW-name*** > ***log-type*** > ***year*** > ***month*** > ***day*** > ***hour***. Les noms des fichiers journaux de compartiment S3 adhèrent au format suivant :

```
<aws-account-id>-<region>-<NGFW-name>-<log-type>-<year>-<month>-<day>-<hour>-<random-string>
```


<random string> fait référence à la ressource NGFW individuelle qui a généré le journal.

Vous pouvez ensuite télécharger le fichier et utiliser un lecteur JSON pour afficher les journaux dans un format plus lisible. Outre les informations de journal, chaque entrée de journal contient également un en-tête qui enregistre la date, la priorité, l'heure, le nom d'hôte du pare-feu, le type de journal, l'année, le mois, le jour, l'heure, la minute et la seconde.

Si vous envoyez des fichiers journaux à Kinesis Firehose, les journaux sont envoyés au nom de flux que vous spécifiez, puis à la destination finale ; comme un compartiment S3, Datadog ou Splunk. La source de votre Kinesis Firehose doit être **une instruction PUT directe ou d'autres sources**. Outre les informations de journal, chaque entrée de journal contient également un en-tête qui enregistre la date, la priorité, l'heure, le nom d'hôte du pare-feu, le type de journal, l'année, le mois, le jour, l'heure, la minute, la seconde, la région, le nom du pare-feu et l'ID de compte AWS. Le NGFW ajoute la région, le nom du pare-feu et l'ID de compte AWS aux journaux pour aider à identifier l'endroit où le journal a été généré, car ces informations ne sont pas incluses dans le nom du fichier journal. Vous pouvez ensuite télécharger le fichier JSON pour le visualiser.

Les heures et dates enregistrées dans les entrées de journal et les noms de fichiers journaux sont affichées en heure UTC. Toutefois, les dates de journal affichées dans la console AWS sont affichées dans l'heure et la date locales.

STEP 1 | Dans la console Cloud NGFW, sélectionnez **NGFWs (NGFW)** et sélectionnez le pare-feu sur lequel configurer la journalisation.

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

STEP 3 | Sous **Log Type (Type de journal)**, sélectionnez un ou plusieurs types de journaux d'options à capturer.

Vous avez la possibilité d'envoyer tous les journaux vers la même destination ou de choisir une destination différente pour chaque type de journal.

STEP 4 | Sélectionnez la **Log Destination (Destination du journal)**. Si vous sélectionnez plusieurs types de journaux, vous devez sélectionner la destination individuellement pour chaque type de journal.

STEP 5 | Entrez le nom de la **Log Destination (Destination du journal)**. Le nom de destination du journal doit

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

Champs du journal du trafic Cloud NGFW pour AWS

Le tableau suivant décrit les champs du journal du trafic Cloud NGFW pour AWS :

Nom du champ	Description
Heure de génération (time_generated ou cef-formatted-time_generated)	Heure de génération du journal dans le plan de données.
Adresse source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
ID de session (sessionid)	Identificateur numérique interne appliqué à chaque session.
Adresse de destination (dst_ip)	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_recv)	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.

Nom du champ	Description
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_time)	Heure de début de la session et utilisation du disque.
Temps écoulé (elapsed_time)	Durée écoulée de la session.
Nombre de répétitions (repeat_count)	Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type sur une période de 5 secondes.
Catégorie (category)	Catégorie d'URL associée à la session (le cas échéant).
Pays source (pays src)	Pays ou région source pour les adresses privées ; 32 octets maximum.
Pays de destination (pays dst)	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

Nom du champ	Description
	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 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_ip)	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 AWS

Nom du champ	Description
Heure de génération (time_generated ou cef-formatted-time_generated)	Heure de génération du journal dans le plan de données.
Adresse source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
ID de session (sessionid)	Identificateur numérique interne appliqué à chaque session.
Adresse de destination (dst_ip)	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

Nom du champ	Description
	• 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 • 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

Nom du champ	Description
	(logiciel malveillant, hameçonnage, indésirable ou bénin, selon les informations que vous consignez) est consigné au journal des envois WildFire. • 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 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_ip)	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

Nom du champ	Description
	périphériques en amont, le pare-feu affiche l'adresse IP du périphérique le plus récent.
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 AWS

Nom du champ	Description
Heure de génération (time_generated ou cef-formatted-time_generated)	Heure de génération du journal dans le plan de données.
Adresse IP source (src_ip)	Adresse IP source de la session d'origine.
Port source (sport)	Port source utilisé par la session.
ID de session (sessionid)	Identificateur numérique interne appliqué à chaque session.
Adresse de destination (dst_ip)	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

Nom du champ	Description
	• 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 (key_exchange_algorithm)	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 (hash_algorithm)	L'algorithme d'authentification utilisé pour la session, par exemple, SHA, SHA256, SHA384, etc.
Courbe elliptique (elliptic_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

Métriques Cloud NGFW pour AWS CloudWatch

Cloud NGFW pour AWS publie des métriques personnalisées dans AWS CloudWatch pour vous aider à surveiller la santé, les performances et les modèles d’utilisation de votre Cloud NGFW. Grâce à ces métriques supplémentaires, vous pouvez évaluer la santé générale de vos ressources Cloud NGFW, identifier les bottlenecks de performance et détecter les anomalies. Ces métriques sont des valeurs

numériques qui décrivent des aspects d'un Cloud NGFW à un moment donné. Collectées toutes les cinq minutes, les métriques sont utiles aux alertes en raison de leur échantillonnage fréquent.

Les métriques sont collectées toutes les cinq minutes. Toutes les métriques sont publiées dans un espace de noms. CloudWatch stocke vos métriques, afin que vous puissiez accéder à des informations historiques pour une perspective supplémentaire sur les performances de vos ressources Cloud NGFW. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsqu'ils sont atteints. Pour plus d'informations, consultez la documentation Amazon CloudWatch.

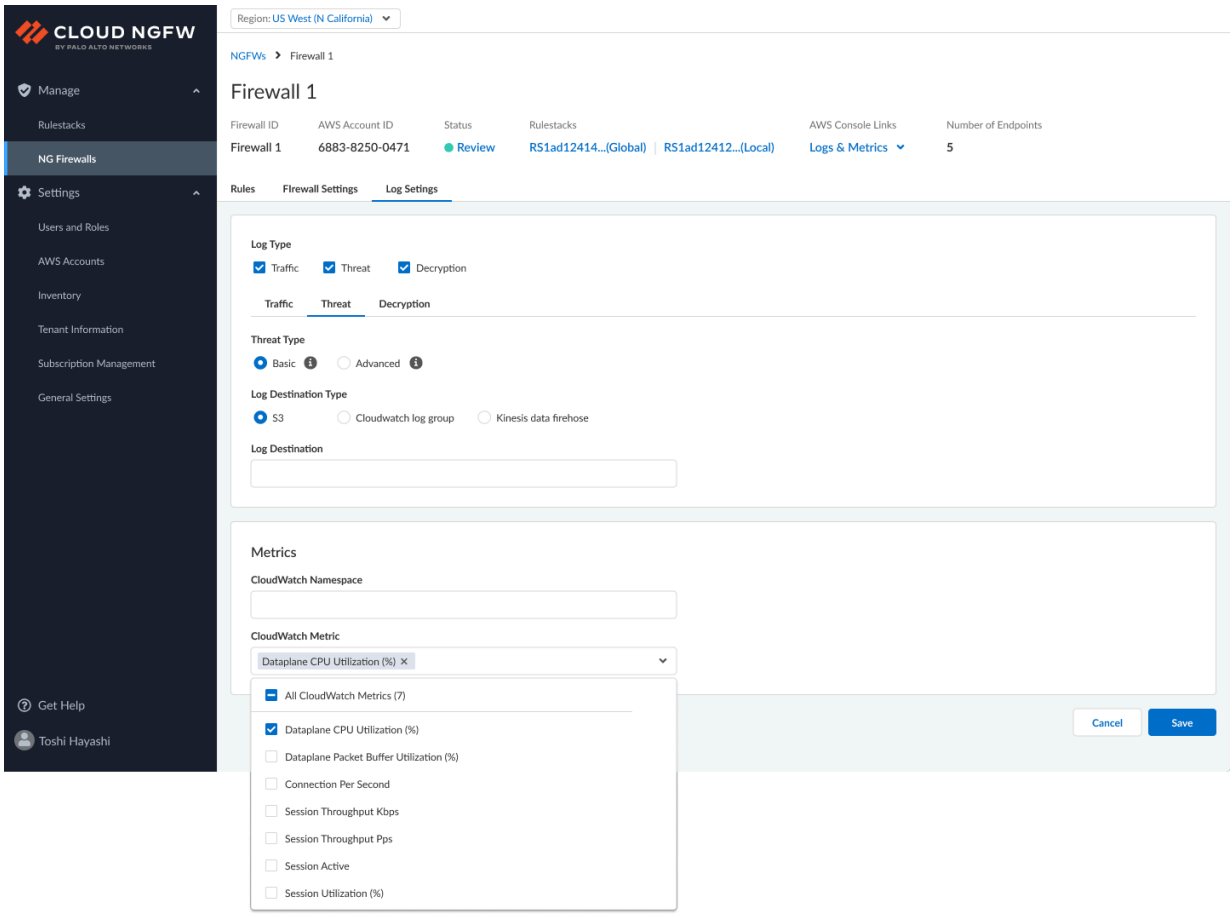
Les métriques CloudWatch suivantes sont prises en charge par la ressource Cloud NGFW :

Nom du champ	Description
Dataplane CPU Utilization (%) (Utilisation du processeur du dataplane)	Surveille l'utilisation du processeur du plan de données et mesure la charge de trafic sur la ressource Cloud NGFW.
Dataplane Packet Buffer Utilization (%) (Utilisation de la mémoire tampon des paquets du dataplane)	Surveille l'utilisation du tampon du dataplane et mesure l'utilisation du tampon. Si vous observez une rafale soudaine dans le trafic, la surveillance de l'utilisation de votre tampon vous permet de vous assurer que le pare-feu n'épuise pas le tampon du dataplane, ce qui entraîne la perte de paquets.
Connection per Second (Connexion par seconde)	Représente le nombre total de connexions TCP simultanées.
Session Throughput Kbps (Débit de session en Kbit/s)	Le débit de session, mesuré en Kbit/s.
Session Throughput Pps (Débit de session en pps)	Le débit de session, mesuré en pps.
Sessions actives	Surveille le nombre total de sessions actives sur la ressource Cloud NGFW. Une session active est une session qui se trouve dans la table de recherche de flux pour laquelle les paquets seront inspectés et transférés, comme requis par la politique.
Session Utilization (%) (Utilisation des sessions)	Surveille les sessions TCP, UDP, ICMP et SSL actuellement actives et le débit de paquets, le nouveau débit d'établissement de la connexion et le débit du pare-feu pour déterminer l'utilisation de la session.
BytesIn	Nombre d'octets dans le sens serveur/client de la session.
BytesOut	Nombre d'octets dans le sens client/serveur de la session.
PktsIn	Nombre de paquets serveur/client de la session.

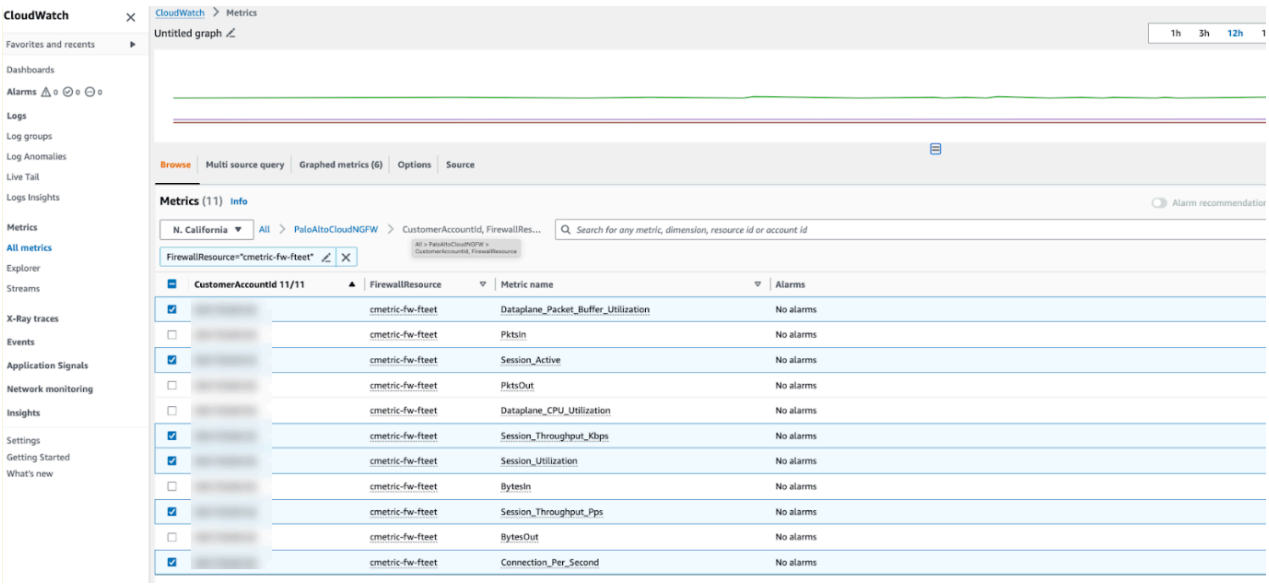
Nom du champ	Description
PktsOut	Nombre de paquets client/serveur de la session.

Pour publier les métriques CloudWatch :

1. Connectez-vous à votre ressource Cloud NGFW.
2. Sélectionnez **NG Firewalls (Pare-feu NG)**.
3. Sélectionnez **Log Settings (Paramètres du journal)**.
4. Sous **Metrics (Métriques)**, spécifier ce qui suit :
   1. **CloudWatch Namespace (Espace de noms CloudWatch)**. Ce champ représente l'emplacement sur AWS où les métriques sont collectées.
   2. **CloudWatch Metric (Métrique CloudWatch)**. Sélectionnez les métriques que vous souhaitez surveiller. Consulter le tableau ci-dessus pour les métriques prises en charge.
5. Cliquez sur **Save (Enregistrer).**



Un exemple de sortie de métriques affichées dans un compte ressemble à :



Activer la journalisation d’audit sur Cloud NGFW pour AWS

Suivez l’activité des administrateurs sur Cloud NGFW pour AWS 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’audit 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.

Si vous avez déjà déployé Cloud NGFW pour AWS, vous devrez peut-être mettre à jour votre CFT. Si votre CFT actuel n’inclut pas le champ Journal d’audit.

Le groupe de journaux doit être créé dans la console AWS de la même région que celle où le Cloud NGFW CFT a été déployé.

Lorsqu’un événement se produit, un journal d’audit est généré et transféré au groupe de journaux CloudWatch que vous spécifiez.

STEP 1 | Si nécessaire, mettez à jour votre CFT pour ajouter les autorisations nécessaires pour écrire dans le groupe de journaux CloudWatch du journal d’audit.

1. Connectez-vous à la console Cloud NGFW.
2. Sélectionnez **AWS Accounts (Comptes AWS)** > **Download CFT (Télécharger le CFT)** pour télécharger le CFT en tant que fichier yaml.
3. Chargez, modifiez et appliquez votre CFT à la console AWS.
    1. Connectez-vous à la console AWS et sélectionnez **CloudFormation** > **Stacks (Piles)**.
    2. Recherchez la pile Cloud NGFW :**PaloAltoNetworksCrossAccountRoleSetup**.
    3. Sélectionnez **Update (Mettre à jour)**.
    4. Sélectionnez **Replace current template (Remplacer le modèle actuel)** et **Upload a template file (Charger un fichier de modèle)**.
    5. Sélectionnez votre fichier CFT yaml et cliquez sur **Next (Suivant)**.
    6. Vérifiez le paramètre de pile CFT et cliquez sur **Next (Suivant)**.
    7. Vérifiez les options de la pile CFT et cliquez sur **Next (Suivant)**.
    8. Passez en revue la pile CFT et cliquez sur **Update (Mettre à jour)**.

STEP 2 | Connectez-vous à la console de locataire Cloud NGFW.

STEP 3 | Sélectionnez **Tenant (Locataire)**.

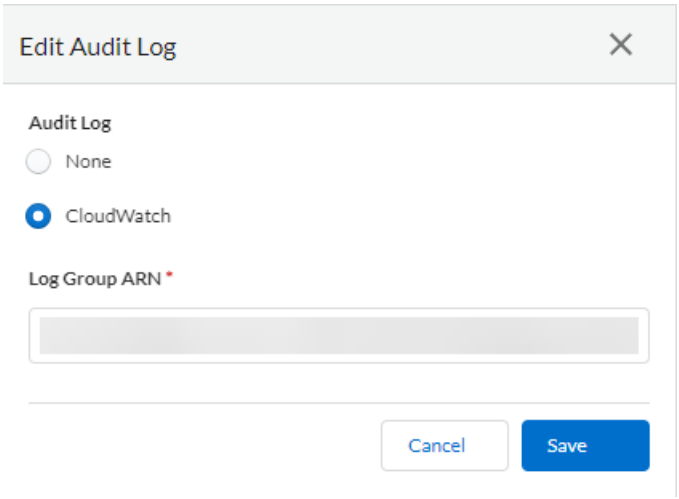
STEP 4 | Cliquez sur l’icône d’édition **Audit Log Settings (Paramètres du journal d’audit)** Edit.

STEP 5 | Sélectionnez la case d’option CloudWatch.

STEP 6 | Entrez le nom de ressource Amazon (ARN) de votre groupe de journaux CloudWatch cible.

Assurez-vous que l’ARN que vous entrez ici correspond au groupe de journaux CloudWatch que vous avez spécifié dans votre pile CFT.

STEP 7 | Cliquez sur **Save (Enregistrer)**.

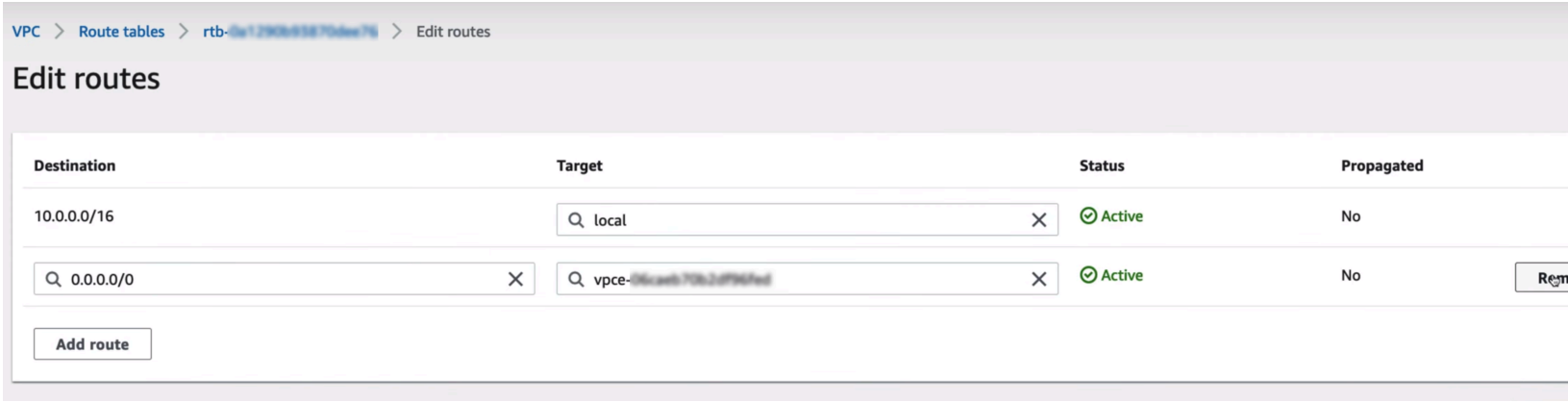


Supprimer une ressource Cloud NGFW

Si vous n'avez plus besoin d'une ressource Cloud NGFW, effectuez la procédure suivante pour la supprimer de votre déploiement AWS.

STEP 1 | Supprimez les terminaux Cloud NGFW associés de vos tables de routage.

1. Connectez-vous à la console AWS.
2. Sélectionnez **VPC** et recherchez le VPC contenant le terminal Cloud NGFW.
3. Sélectionnez **Route Tables (Tables de routage)**, puis sélectionnez la table de routage du terminal à supprimer.



4. Cliquez sur **Edit Routes (Modifier les itinéraires)**.
5. Cliquez sur **Remove (Supprimer)** pour supprimer l'itinéraire de la table de routage.
6. Cliquez sur **Save changes (Enregistrer les modifications)**.

STEP 2 | (Terminaux gérés par le client uniquement) Si vous avez déployé vos propres terminaux Cloud NGFW, vous devez les supprimer de la console AWS.

1. Dans la console AWS, sélectionnez **Endpoints (Terminaux)** et choisissez votre terminal Cloud NGFW.
2. Sélectionnez **Actions** > **Delete (Supprimer)** et confirmez la suppression.

STEP 3 | Supprimez la ressource Cloud NGFW du locataire Cloud NGFW.

1. Connectez-vous à la console Cloud NGFW et sélectionnez **NGFWs (NGFW)**.
2. Sélectionnez la ressource à supprimer.
3. Dans la liste déroulante **Actions**, cliquez sur **Delete (Supprimer)**.
4. **Confirm (Confirmer)** la suppression.

   Après quelques minutes, la ressource Cloud NGFW et tous ses terminaux sont supprimés de votre déploiement Cloud NGFW.

Intégration de Cloud NGFW avec AWS Cloud WAN

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 sites sur site, les sites de succursales, les centres de données et les VPC Amazon sur le réseau mondial AWS et même d'autres fournisseurs de cloud.

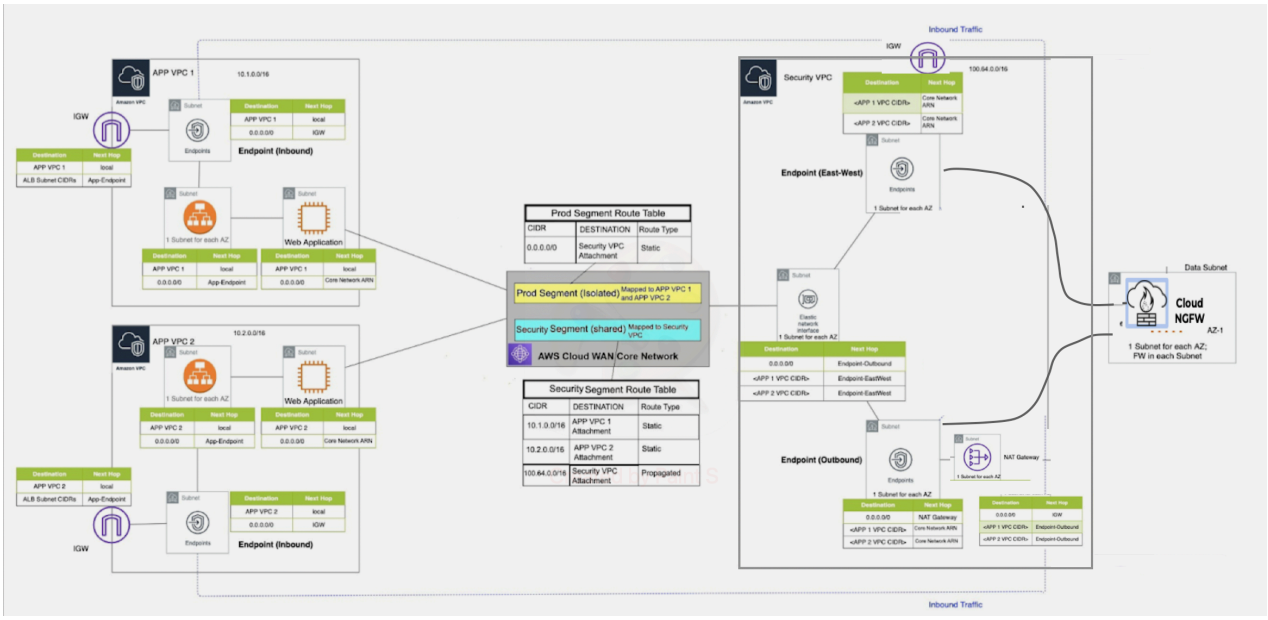
Cloud WAN facilite la connectivité au sein d'AWS via le gestionnaire de réseau AWS, une interface qui gère de manière centralisée votre réseau mondial. Un réseau mondial est un réseau privé unique qui agit comme un conteneur au niveau racine pour vos objets réseau et peut contenir à la fois des passerelles 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 la manière l'acheminement du trafic vers la ressource Cloud NGFW pour 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

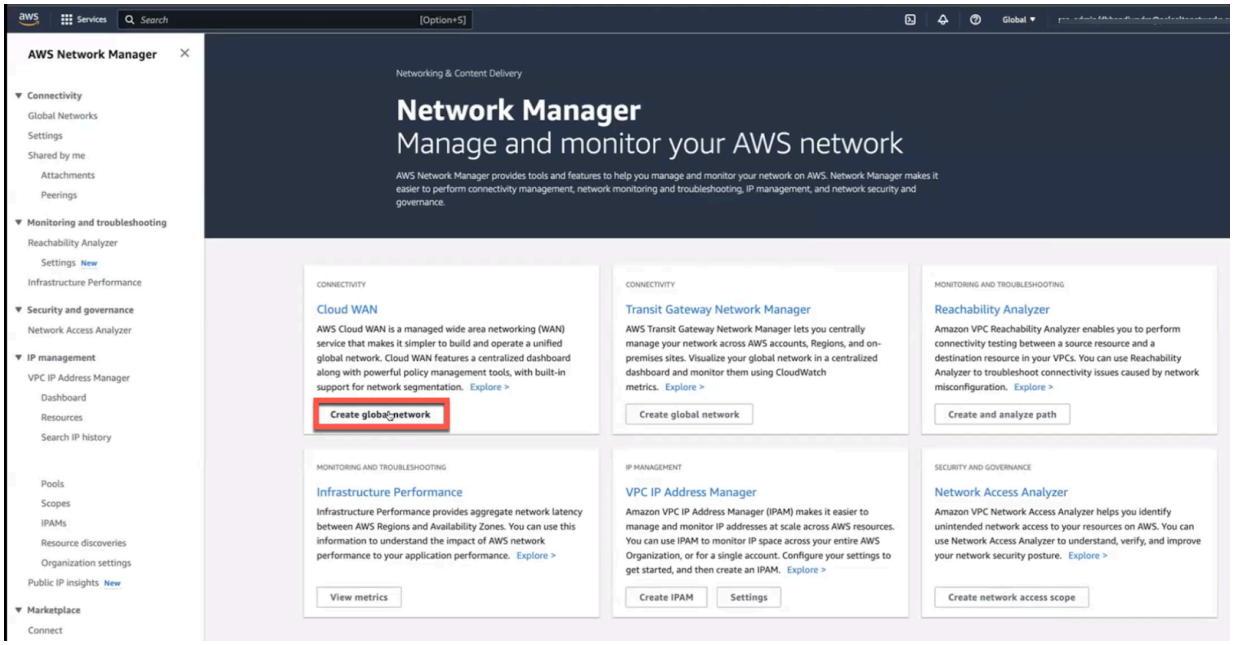
Examinons un cas d'utilisation où les VPC se trouvent dans la même région (attachements isolés). Pour réaliser cette configuration, déployez le pare-feu du Cloud NGFW dans le VPC de sécurité. Vous pouvez déployer le pare-feu du Cloud NGFW dans un VPC de sécurité, directement connecté à un Cloud WAN ou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

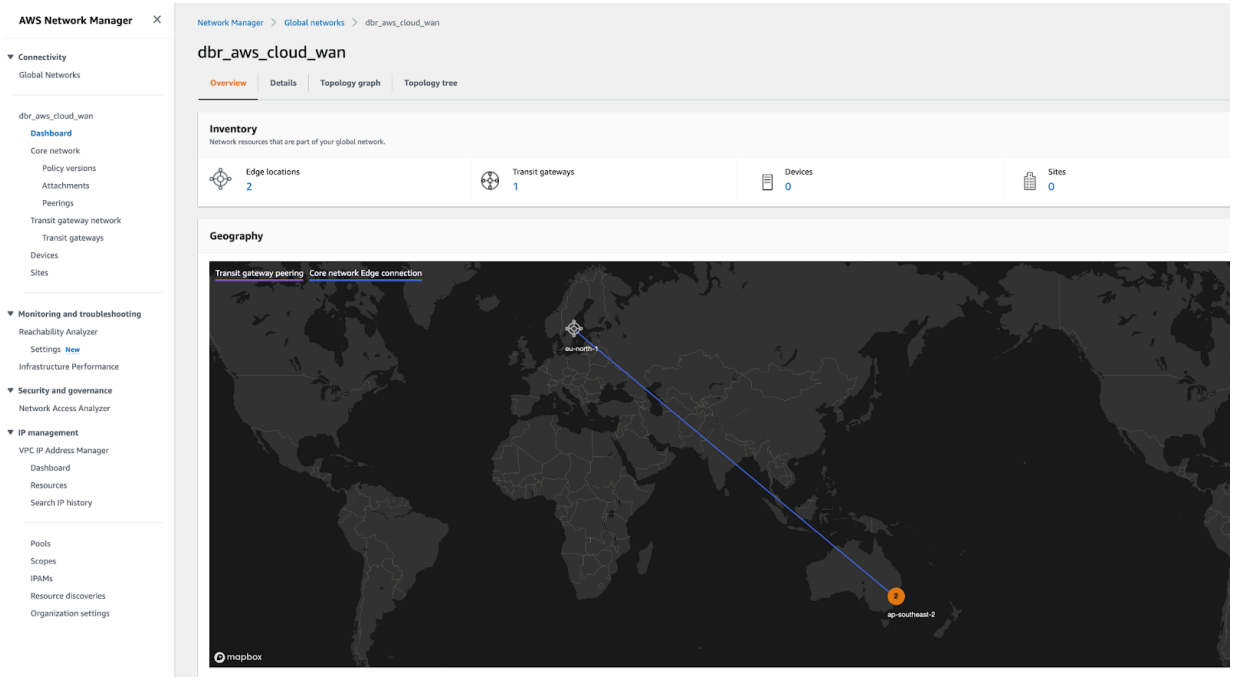
Pour migrer complètement en dehors de la passerelle de transit, vous devez connecter vos VPC directement au Cloud WAN.

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 **Create global network (créez un réseau mondial)**.

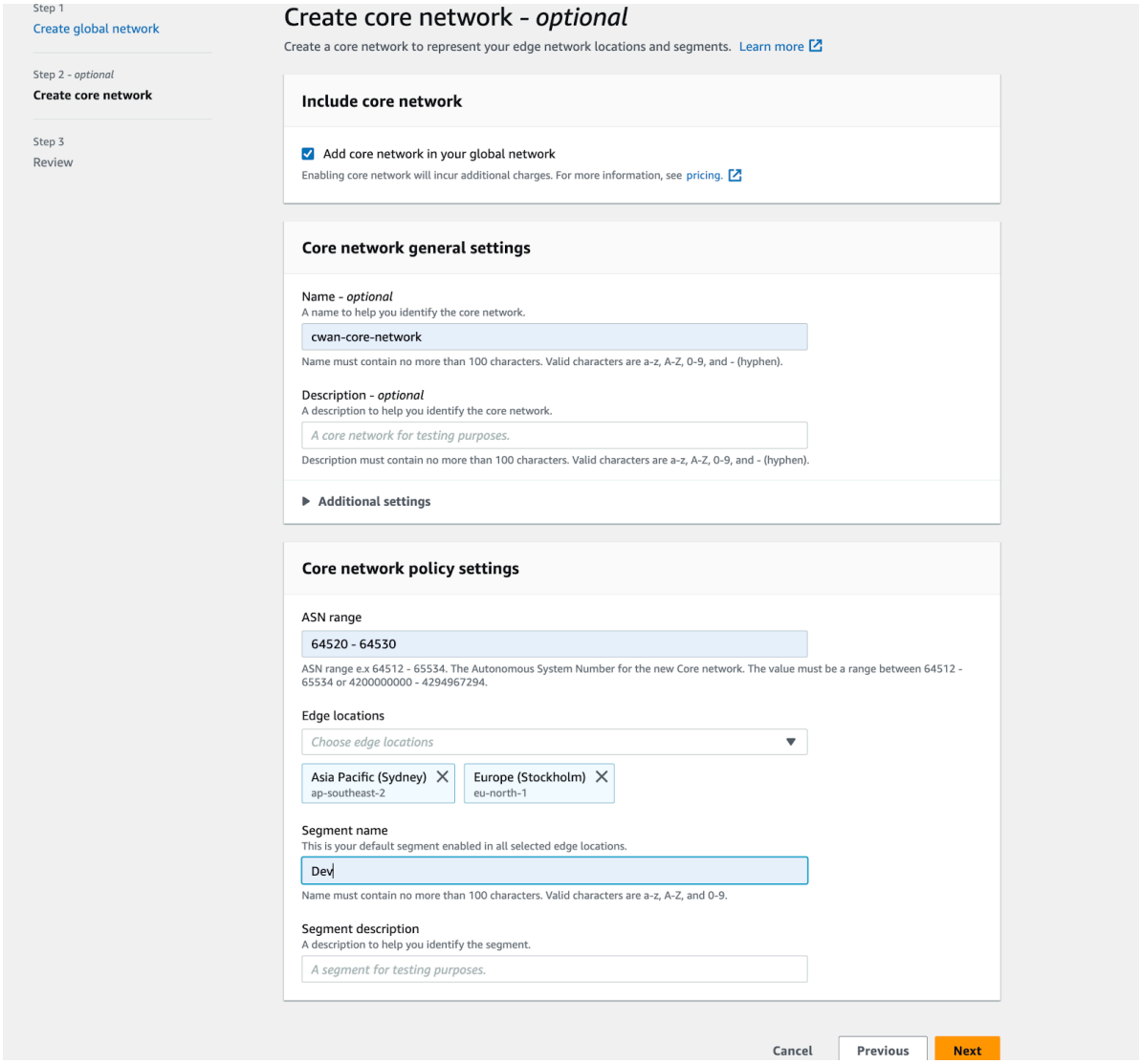




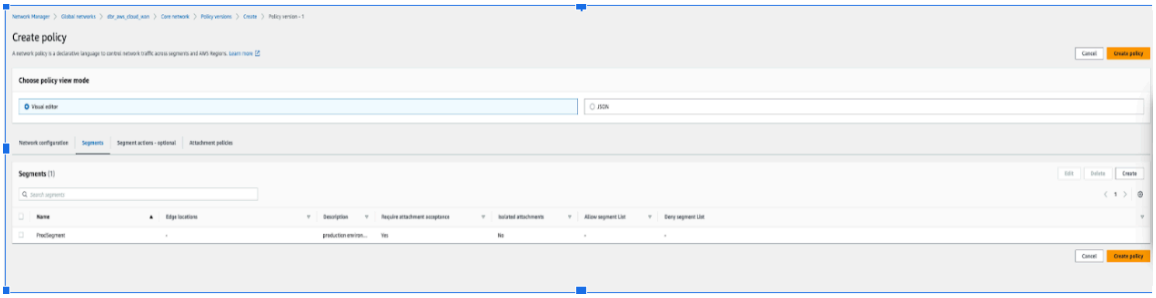
2. Créez un réseau principal et une politique de réseau principal.

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

   - Configurez les paramètres réseau.

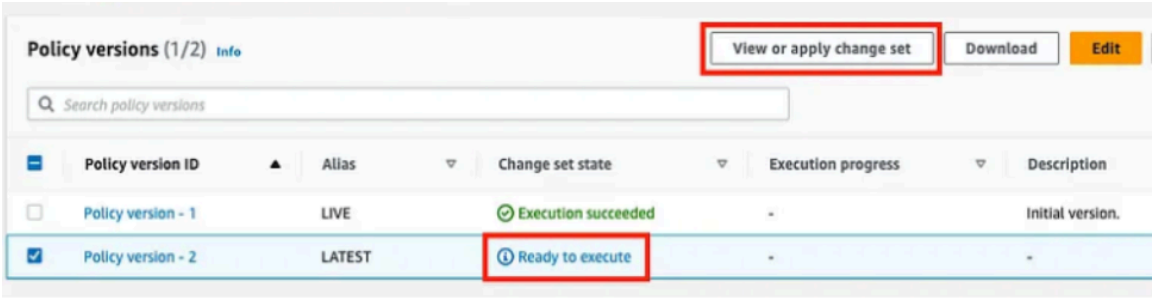


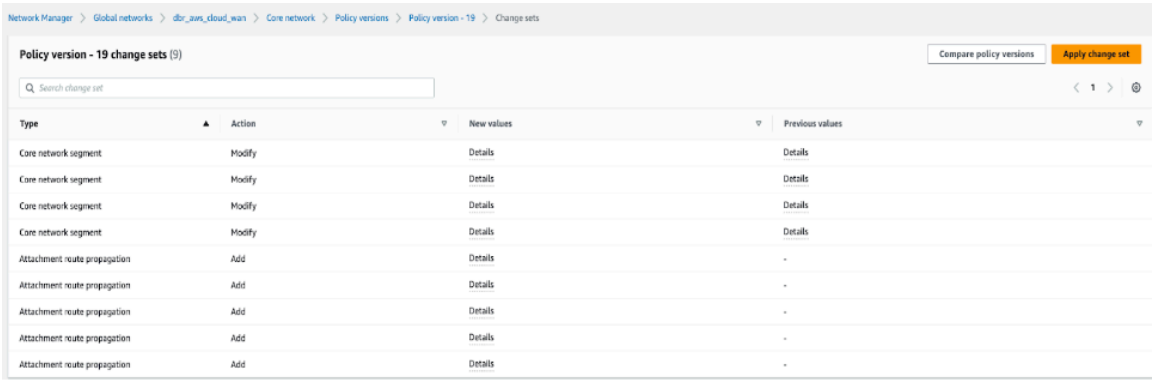
- Pour modifier une version de politique, cliquez sur **Policy versions (Versions de politique)**, sélectionnez la politique requise et cliquez sur **Edit (Modifier)**. Effectuez les modifications nécessaires et cliquez sur **Create Policy (Créer une politique)**.



- 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

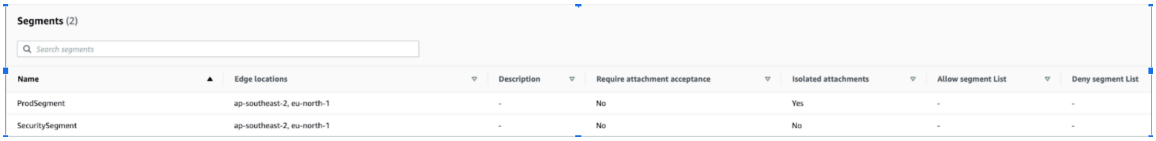
Compare policy version (Comparer la version de la politique) pour afficher le document JSON.



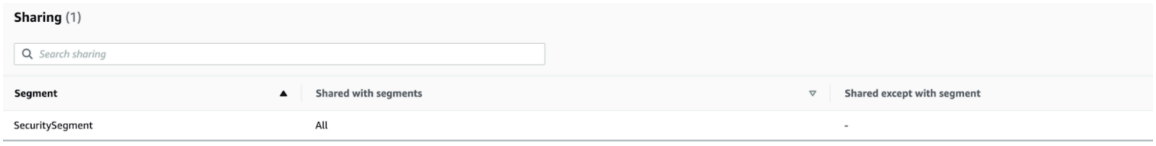


- • Créez des segments de politique de réseau au sein de votre réseau principal.

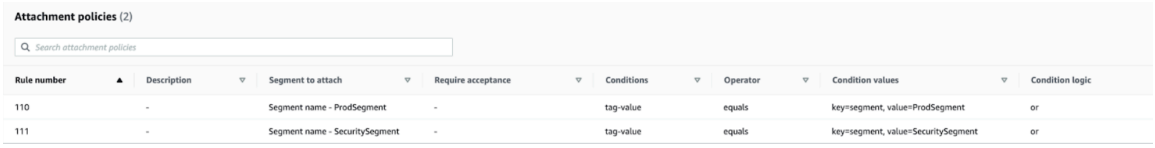
  Lors de la configuration des versions de politique, assurez-vous d'ajouter les applications – APP VPC 1 (10.1.0.0/16) et APP VPC 2 (10.2.0.0/16) dans le segment de production et le pare-feu, ainsi que le VPC de sécurité (100.64.0.0/16) dans le segment de sécurité.



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



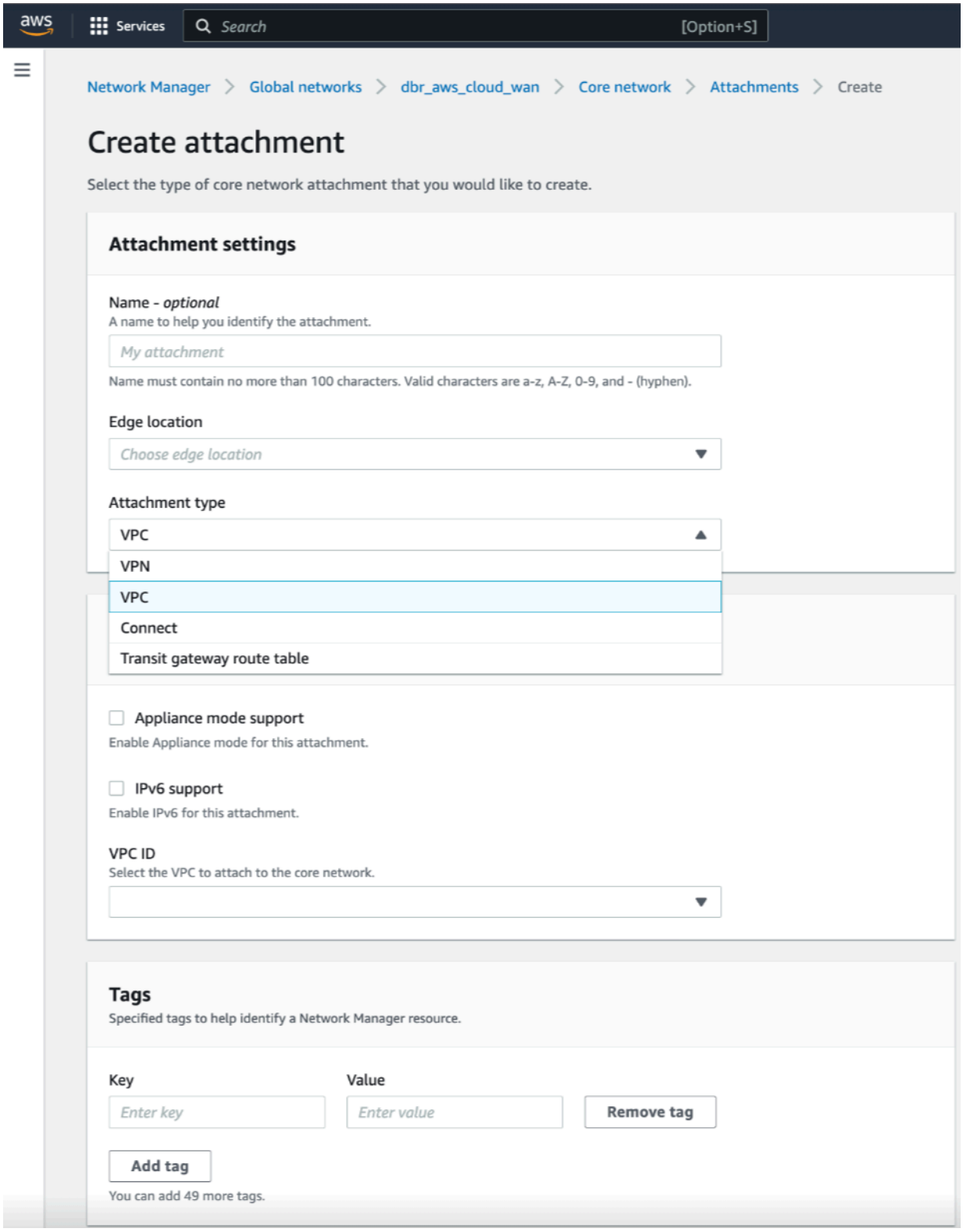
- Créez des attachements de politique.



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

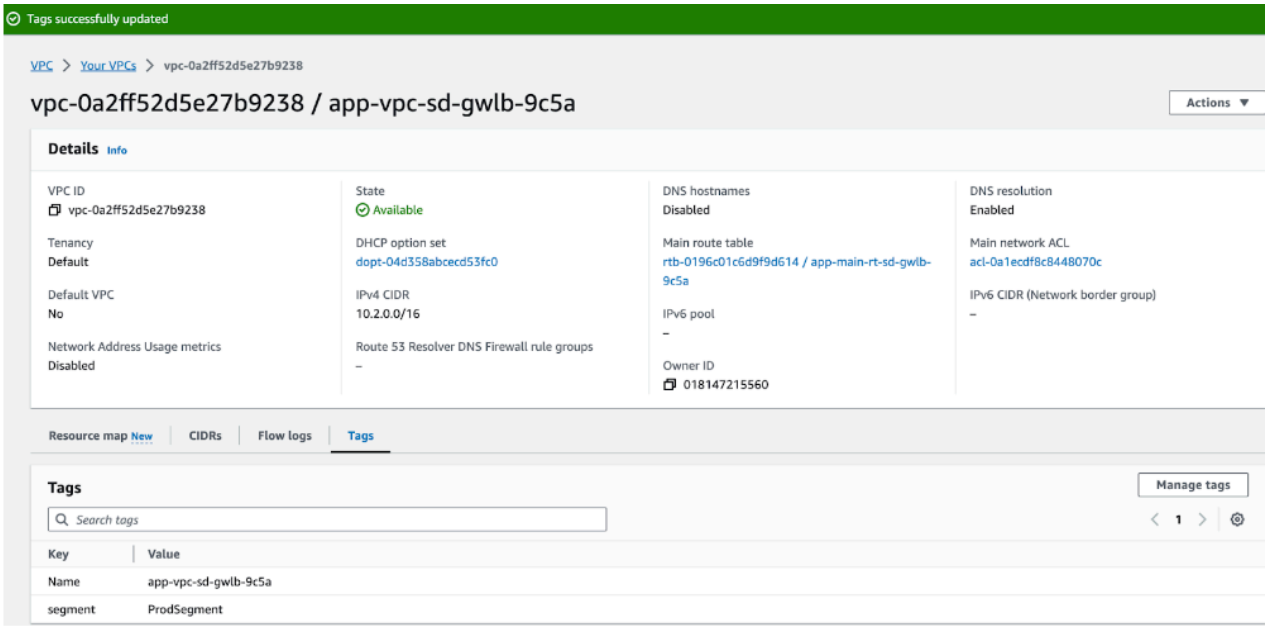
3. Créez un attachement.

- *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.*

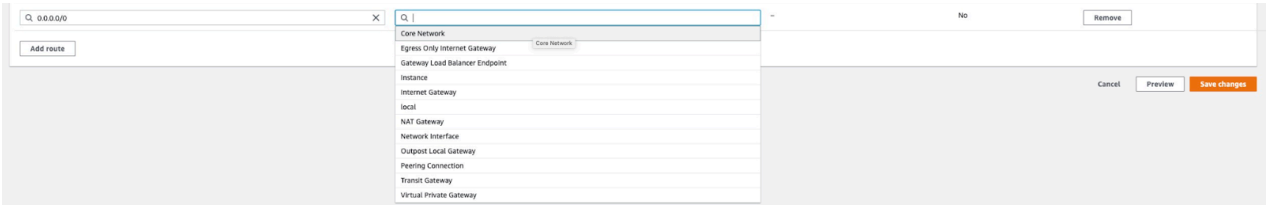


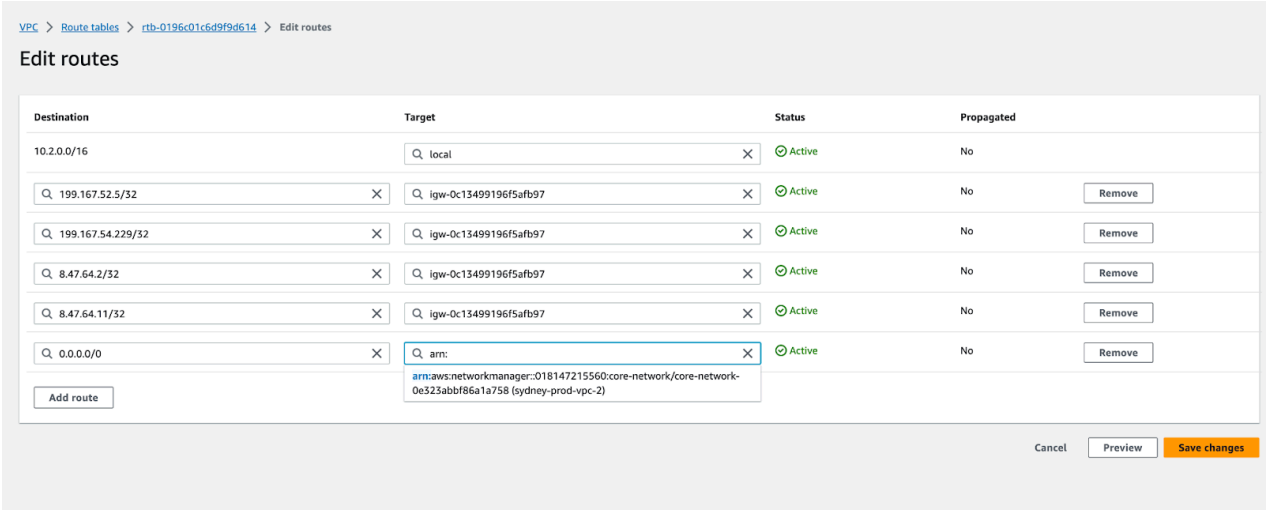
4. Mettez à jour les tables de routage de VPC.

   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.



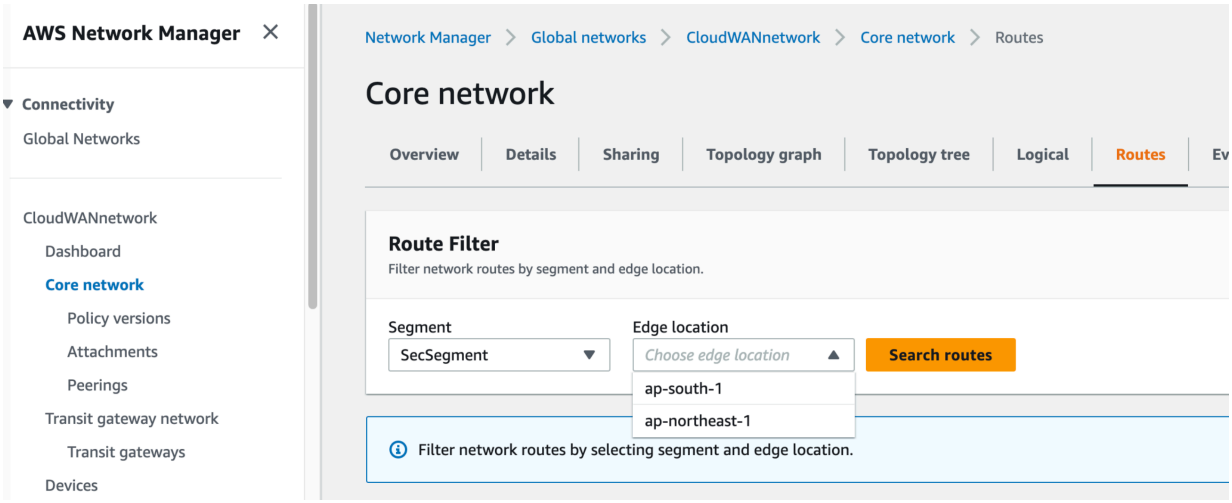


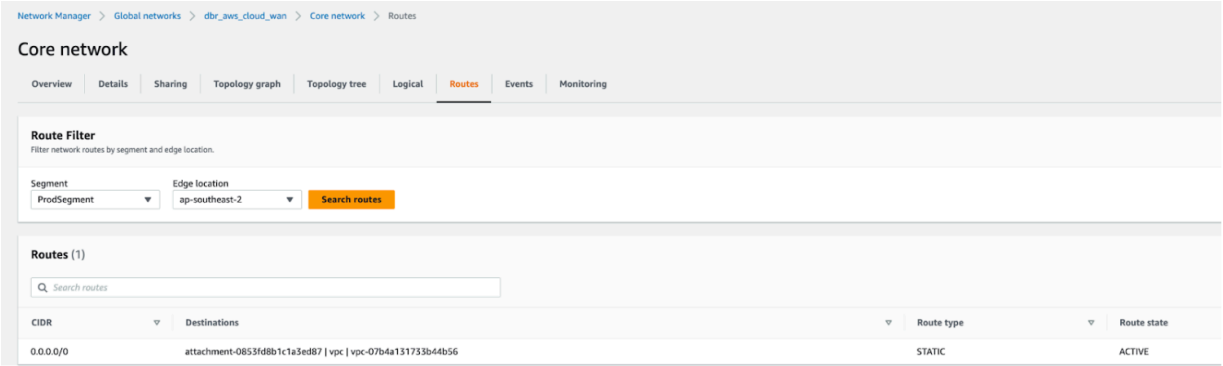
Procédure pas à pas relative aux paquets

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

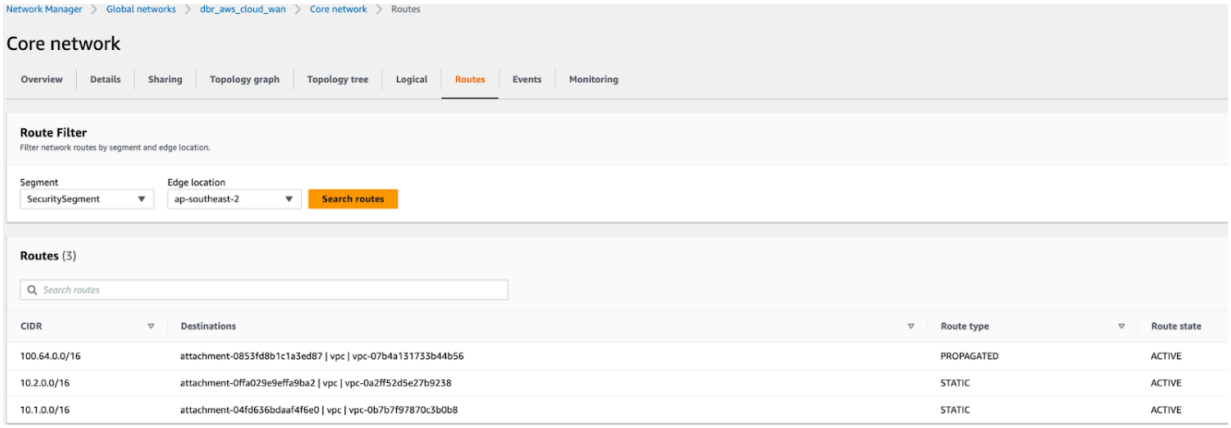
l’entrée par défaut avec l’attachement de sécurité comme cible et le paquet est acheminé vers le VPC de sécurité.





- 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.

Fonctionnalités de sécurité du Cloud NGFW pour AWS

Le Cloud NGFW pour AWS fournit des fonctionnalités de sécurité. Vous pouvez :

- Configuration de la sécurité DNS
- Configurer WildFire pour Cloud NGFW sur AWS

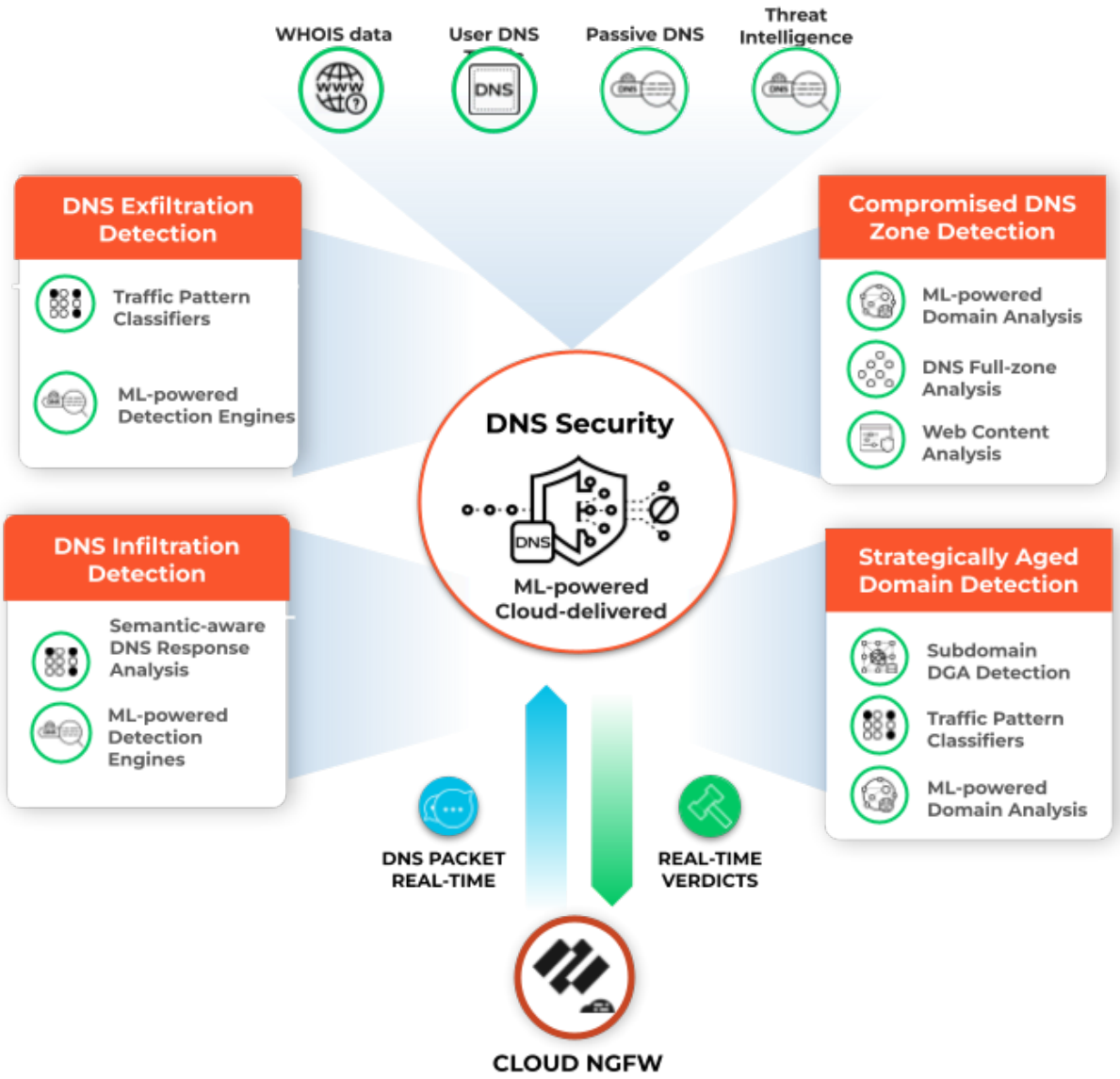
Configuration de la sécurité DNS

Le service de noms de domaine (DNS) est un protocole essentiel et fondamental d'Internet, comme 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 VPC, puis utilise la recherche DNS pour envoyer des données à l'extérieur du VPC vers un domaine qu'il contrôle. Des acteurs malveillants peuvent également infiltrer des données et des charges utiles malveillantes dans les charges de travail VPC via DNS. Les recherches de l'unité 42 de Palo Alto Networks ont décrit les différents types d'abus de DNS découverts.

Cloud NGFW pour AWS vous permet de protéger votre trafic de VPC contre les menaces avancées basées sur DNS, en surveillant et en contrôlant les domaines interrogés par vos ressources VPC. Avec Cloud NGFW pour AWS. Vous pouvez refuser l'accès aux domaines estimés mauvais ou suspects par Palo Alto Networks et autoriser toutes les autres requêtes.

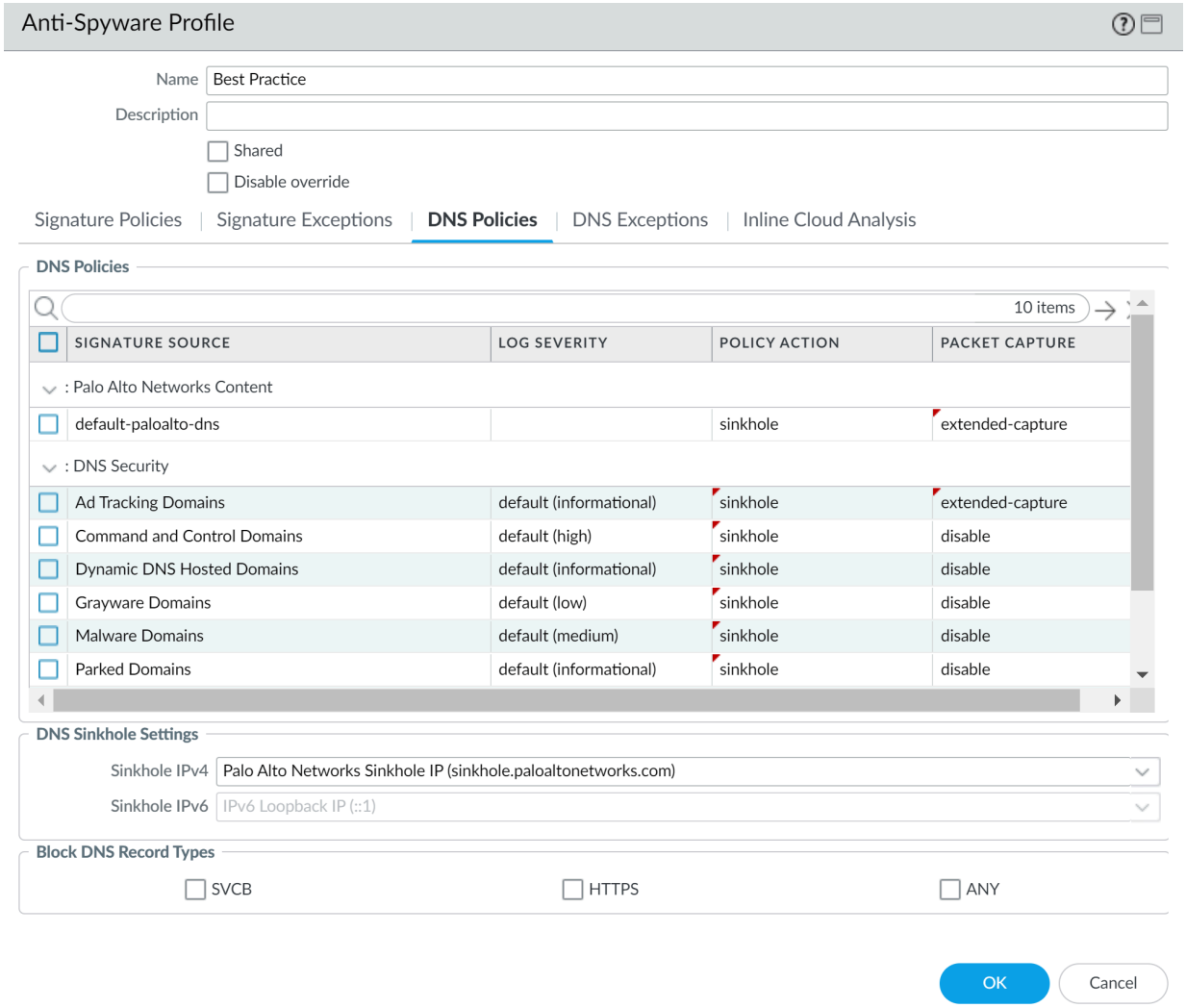
Cloud NGFW utilise le service de sécurité DNS de Palo Alto Networks qui détecte les domaines malveillants de manière proactive en générant des signatures DNS à l'aide d'une analyse prédictive avancée et de machine learning, avec des données provenant de plusieurs sources (telles que l'analyse du trafic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

La sécurité DNS pour le Cloud NGFW nécessite Panorama. Configurez toutes les règles de politique liées à la sécurité DNS sur Panorama et transférez-les vers les ressources Cloud NGFW dans le cadre d'un groupe d'appareils Cloud.



Pour activer la sécurité DNS dans les ressources Cloud NGFW :

1. Activez DNS Security (sécurité DNS) dans Panorama en créant un profil anti-spyware dans les groupes d'appareils cloud associés à vos ressources Cloud NGFW.



2. Redirigez votre trafic DNS dans votre VPC vers votre ressource Cloud NGFW. La configuration de la redirection du trafic dépend de la configuration de votre serveur DNS.
   - Serveur DNS privé
   - Service DNS Route 53
   - DNS de zone privée hébergée

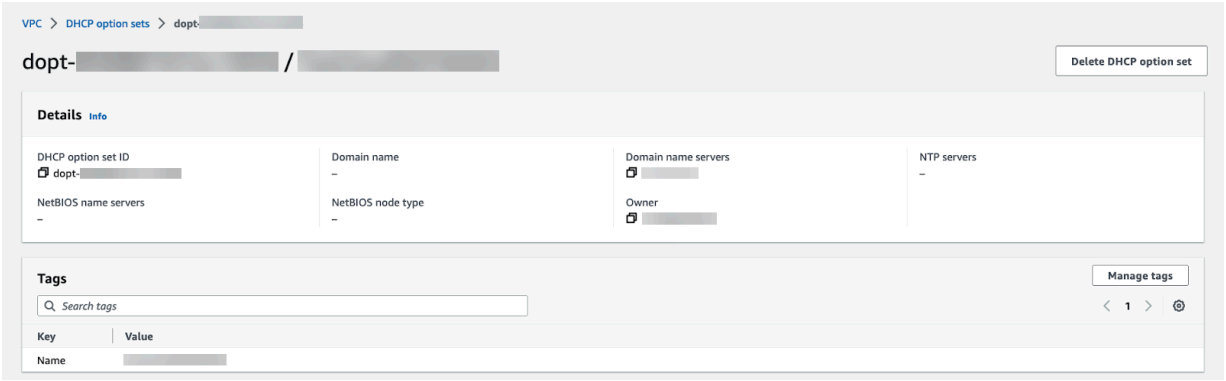
Serveur DNS privé

Lorsque vous utilisez un serveur DNS privé ou local, procédez comme suit pour diriger le trafic DNS vers vos terminaux Cloud NGFW.

STEP 1 | Connectez-vous à la console AWS.

STEP 2 | Sélectionnez votre VPC puis les **DHCP option sets (Ensembles d'options DHCP)**.

STEP 3 | Vous pouvez créer un nouvel ensemble d'options DHCP et ajouter l'adresse IP de votre serveur DNS. Dans cet exemple, l'adresse du serveur DNS privé est 172.18.10.1. Si vous disposez d'un ensemble d'options DHCP existant configuré sur votre serveur DNS, consultez les détails et notez l'adresse IP du serveur DNS.



STEP 4 | Sélectionnez **VPC** et choisissez le VPC à sécuriser.

STEP 5 | Dans le menu déroulant **Actions**, sélectionnez **Edit VPC settings (Modifier les paramètres du VPC)**.

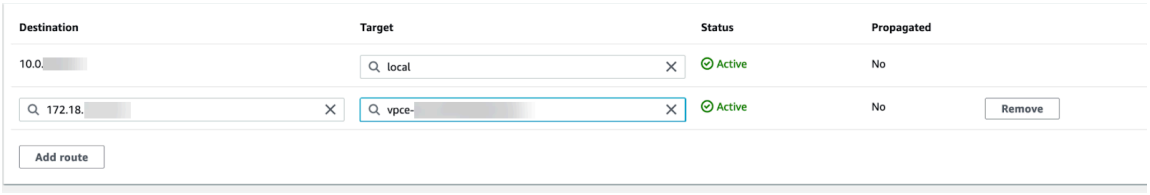
STEP 6 | Sous **DHCP settings (Paramètres DHCP)**, sélectionnez l'ensemble d'options DHCP configuré sur votre serveur DNS privé dans le menu déroulant **DHCP option set (Ensemble d'options DHCP)**.

STEP 7 | Cliquez sur **Save changes (Enregistrer les modifications)**.

Le VPC sélectionné dirige désormais toutes les requêtes DNS vers le serveur DNS configuré.

STEP 8 | Modifiez votre table de routage de sous-réseau.

1. Sélectionnez **VPC** > **Route Tables (Tables de routage)**.
2. Sélectionnez la table de routage du sous-réseau que vous souhaitez sécuriser.
3. Ajoutez un itinéraire et définissez la destination sur l'adresse IP de votre serveur DNS.



4. Cliquez sur **Save changes (Enregistrer les modifications).**

   Tout trafic DNS provenant du sous-réseau protégé est acheminé via le terminal Cloud NGFW et ensuite vers le Cloud NGFW pour inspection et application.

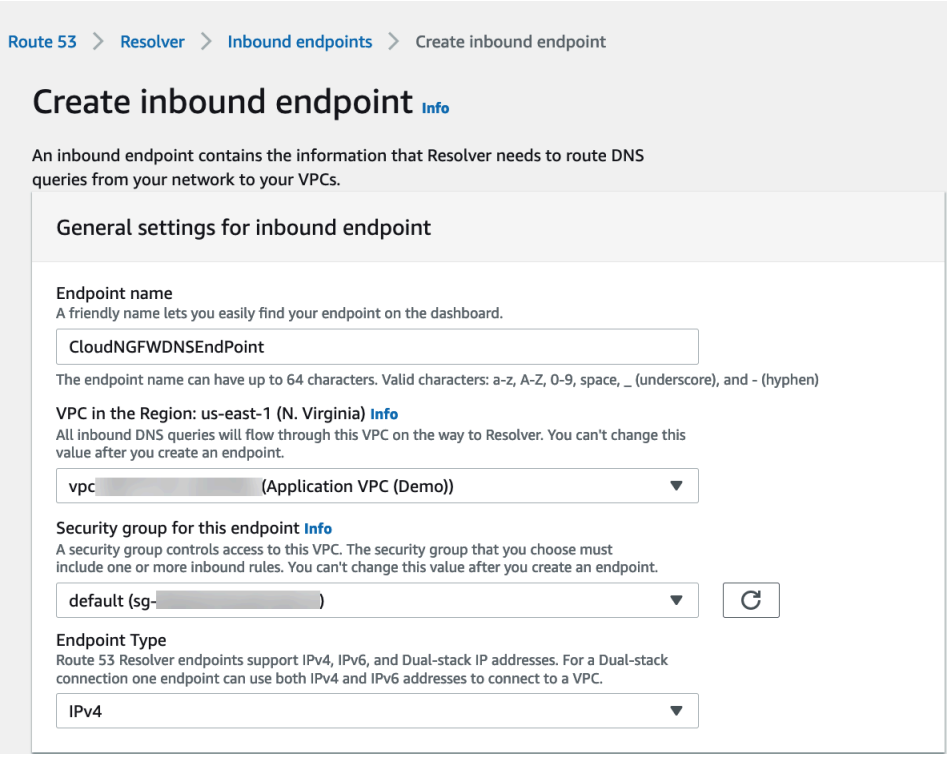
Service DNS Route 53

Procédez comme suit pour sécuriser le trafic DNS dans vos VPC lors de l'utilisation du service DNS Route 53 d'Amazon. Créez un sous-réseau dans chaque zone de disponibilité contenant des charges de travail afin de déployer les terminaux entrants du résolveur.

STEP 1 | Connectez-vous à la console AWS.

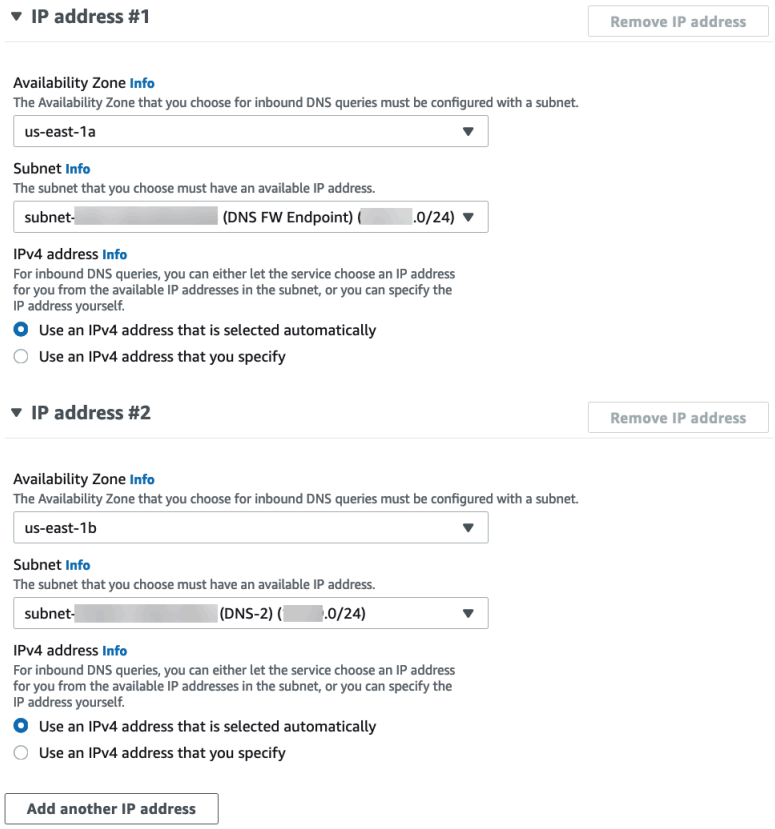
STEP 2 | Créez un terminal entrant.

1. Sélectionnez **Services** > **Route 53** > **Resolver (Résolveur)** > **Inbound Endpoints (Terminaux entrants)**.
2. Cliquez sur **Create inbound endpoint (Créer un terminal entrant)**.
3. Saisissez un **Name (Nom)** descriptif.
4. Sélectionnez le VPC pour le terminal.
5. Attachez un groupe de sécurité au terminal.
6. Définissez le **Endpoint Type (Type de terminal)** sur IPv4.



7. Sélectionnez la zone de disponibilité.
8. Sélectionnez le sous-réseau que vous avez créé ci-dessus.

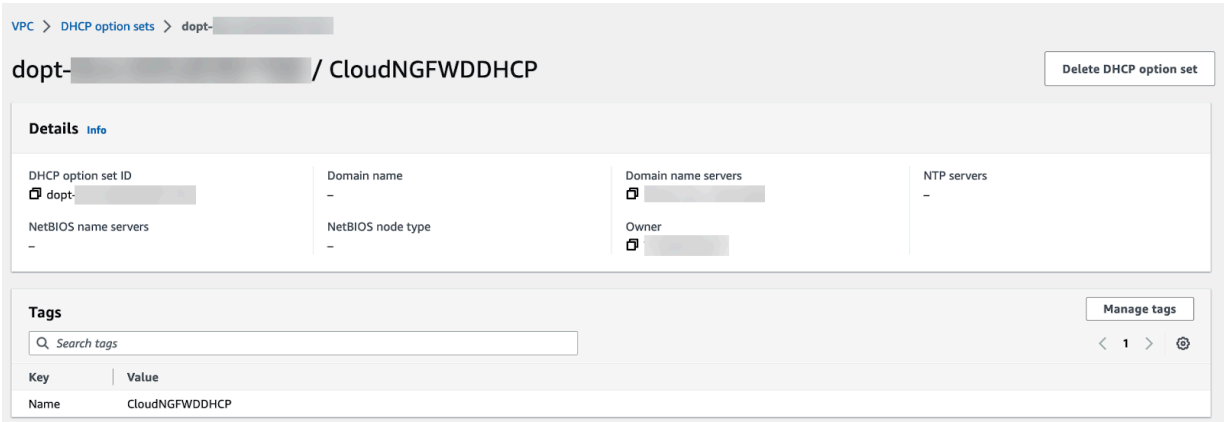
Si vous disposez de plusieurs zones de disponibilité, vous devez spécifier la zone de disponibilité et le sous-réseau de chacune.



9. Cliquez sur **Create inbound endpoint (Créer un terminal entrant)**.
10. Notez l'adresse IP associée à chaque sous-réseau attaché à votre terminal entrant. Utilisez ces adresses IP lors de la configuration de vos **DHCP option sets (Ensembles d'options DHCP)** dans les étapes suivantes.

STEP 3 | Sélectionnez **VPC** > **DHCP option sets (Ensembles d'options DHCP)**.

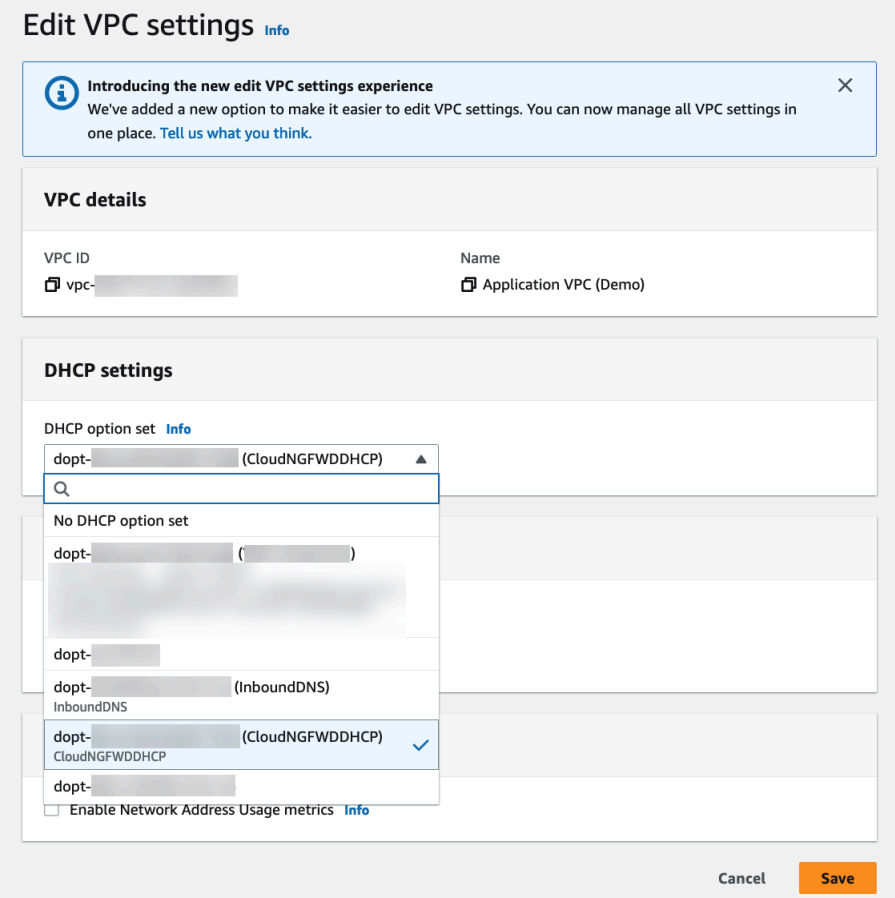
STEP 4 | Vous pouvez créer un nouvel ensemble d'options DHCP et ajouter l'adresse IP de chaque zone de disponibilité. Si vous disposez de plusieurs zones de disponibilité, saisissez chaque adresse IP dans une liste séparée par des virgules.



STEP 5 | Sélectionnez **VPC** et choisissez le VPC à sécuriser.

STEP 6 | Dans le menu déroulant **Actions**, sélectionnez **Edit VPC settings (Modifier les paramètres du VPC)**.

STEP 7 | Sous **DHCP settings (Paramètres DHCP)**, sélectionnez l'ensemble d'options DHCP que vous avez créé ci-dessus dans la liste déroulante **DHCP option set (Ensemble d'options DHCP)**.

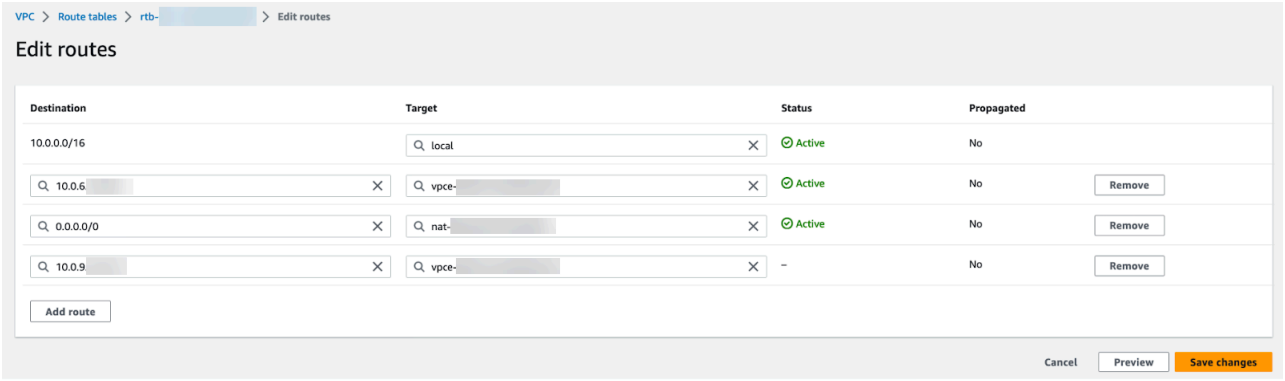


STEP 8 | Cliquez sur **Save changes (Enregistrer les modifications)**.

Le VPC sélectionné dirige désormais toutes les requêtes DNS vers le serveur DNS configuré.

STEP 9 | Modifiez votre table de routage de sous-réseau.

1. Sélectionnez **VPC** > **Route Tables (Tables de routage)**.
2. Sélectionnez la table de routage du sous-réseau que vous souhaitez sécuriser.
3. Ajoutez un itinéraire et définissez la destination sur l'adresse IP de votre serveur DNS et définissez la cible sur le terminal Cloud NGFW.



4. Cliquez sur **Save changes (Enregistrer les modifications)**.

   Tout trafic DNS provenant du sous-réseau protégé est acheminé via le terminal Cloud NGFW et ensuite vers le Cloud NGFW pour inspection et application.

DNS de zone privée hébergée

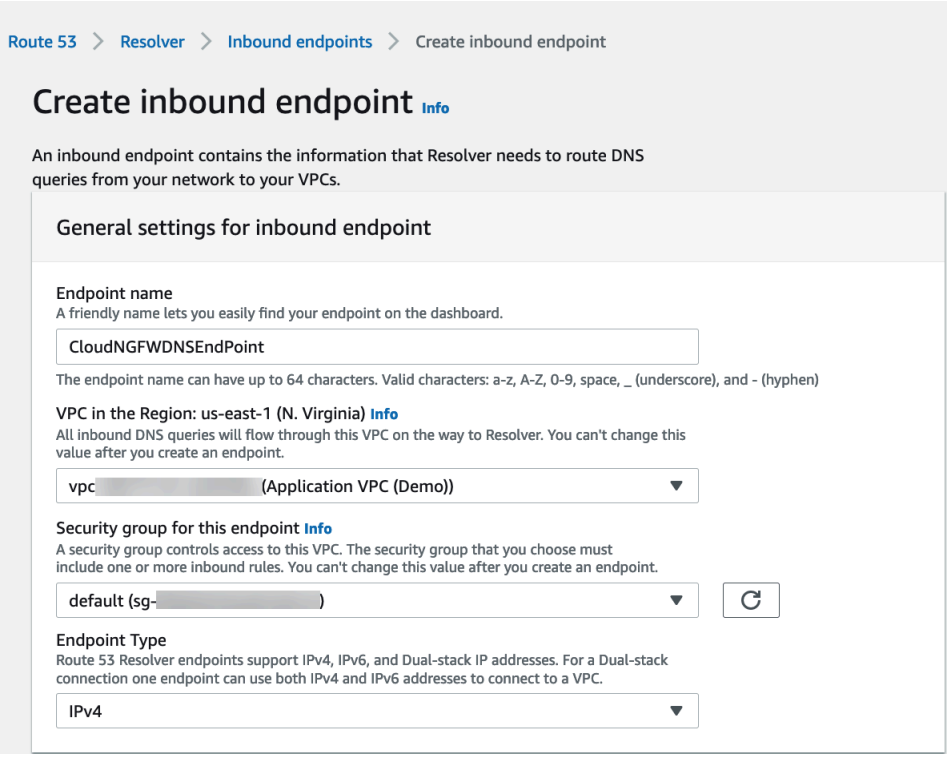
Pour créer une zone privée hébergée dans AWS, consultez Création d'une zone privée hébergée.

Pour permettre à votre ressource Cloud NGFW d'interroger le résolveur Route 53 pour toutes les zones DNS (p. ex., les zones privées) hébergées sur Route 53, vous créez un terminal entrant Route 53 comme indiqué précédemment. Le terminal entrant est un pont permettant à d'autres services d'interroger Route 53 pour la résolution de noms de domaine. Lorsque vous créez un terminal entrant, AWS crée une interface réseau élastique (ENI) dans chaque zone de disponibilité (AZ) que vous spécifiez pour recevoir des requêtes DNS entrantes.

STEP 1 | Ouvrez la console Amazon VPC.

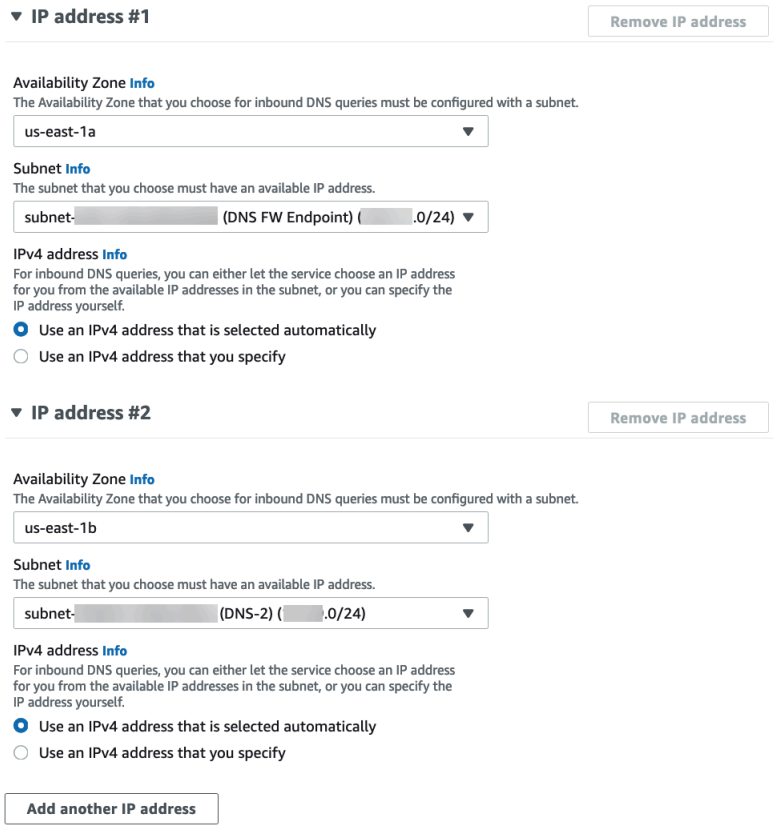
STEP 2 | Créez un terminal entrant.

1. Sélectionnez **Services** > **Route 53** > **Resolver (Résolveur)** > **Inbound Endpoints (Terminaux entrants)**.
2. Cliquez sur **Create inbound endpoint (Créer un terminal entrant)**.
3. Saisissez un **Name (Nom)** descriptif.
4. Sélectionnez le VPC pour le terminal.
5. Attachez un groupe de sécurité au terminal.
6. Définissez le **Endpoint Type (Type de terminal)** sur IPv4.



7. Sélectionnez la zone de disponibilité.
8. Sélectionnez le sous-réseau que vous avez créé ci-dessus.

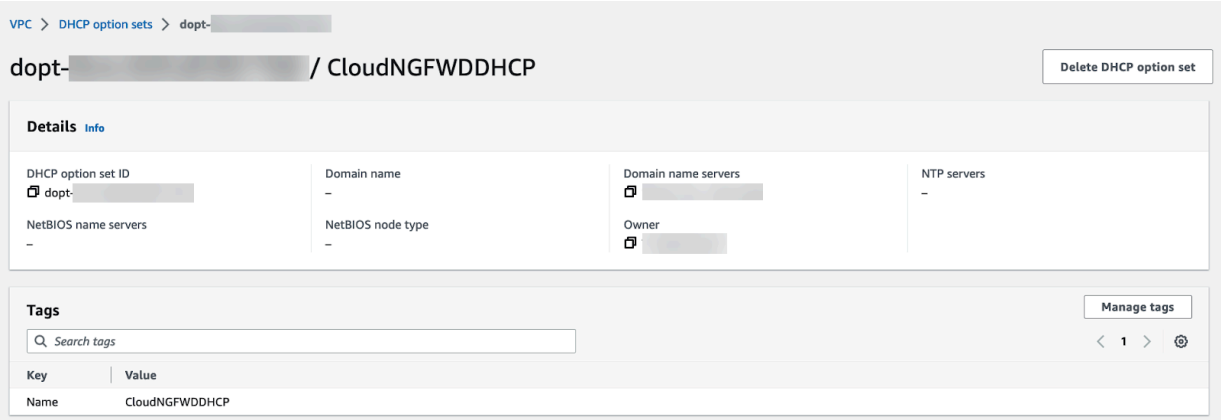
Si vous disposez de plusieurs zones de disponibilité, vous devez spécifier la zone de disponibilité et le sous-réseau de chacune.



9. Cliquez sur **Create inbound endpoint (Créer un terminal entrant)**.
10. Notez l'adresse IP associée à chaque sous-réseau attaché à votre terminal entrant. Utilisez ces adresses IP lors de la configuration de vos **DHCP option sets (Ensembles d'options DHCP)** dans les étapes suivantes.

STEP 3 | Sélectionnez **VPC** > **DHCP option sets (Ensembles d'options DHCP)**.

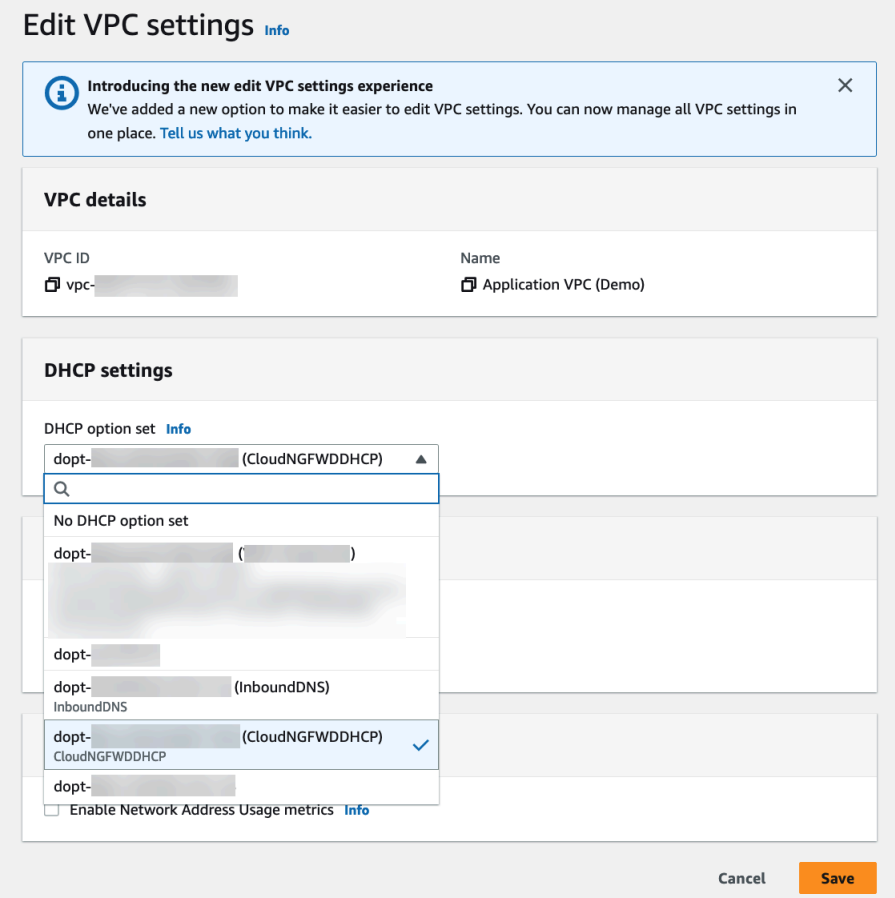
STEP 4 | Vous pouvez créer un nouvel ensemble d'options DHCP et ajouter l'adresse IP de chaque zone de disponibilité. Si vous disposez de plusieurs zones de disponibilité, saisissez chaque adresse IP dans une liste séparée par des virgules.



STEP 5 | Sélectionnez **VPC** et choisissez le VPC à sécuriser.

STEP 6 | Dans le menu déroulant **Actions**, sélectionnez **Edit VPC settings (Modifier les paramètres du VPC)**.

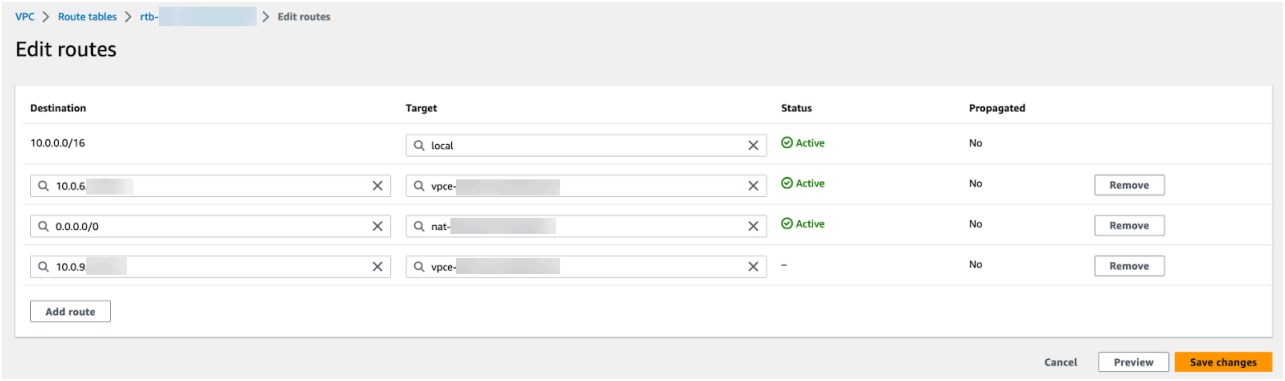
STEP 7 | Sous **DHCP settings (Paramètres DHCP)**, sélectionnez l'ensemble d'options DHCP que vous avez créé ci-dessus dans la liste déroulante **DHCP option set (Ensemble d'options DHCP)**.



STEP 8 | Cliquez sur **Save changes (Enregistrer les modifications)**.

STEP 9 | Modifiez votre table de routage de sous-réseau.

1. Sélectionnez **VPC** > **Route Tables (Tables de routage)**.
2. Sélectionnez la table de routage du sous-réseau que vous souhaitez sécuriser.
3. Ajoutez un itinéraire et définissez la destination sur l'adresse IP de votre serveur DNS et définissez la cible sur le terminal Cloud NGFW.



4. Cliquez sur **Save changes (Enregistrer les modifications)**.

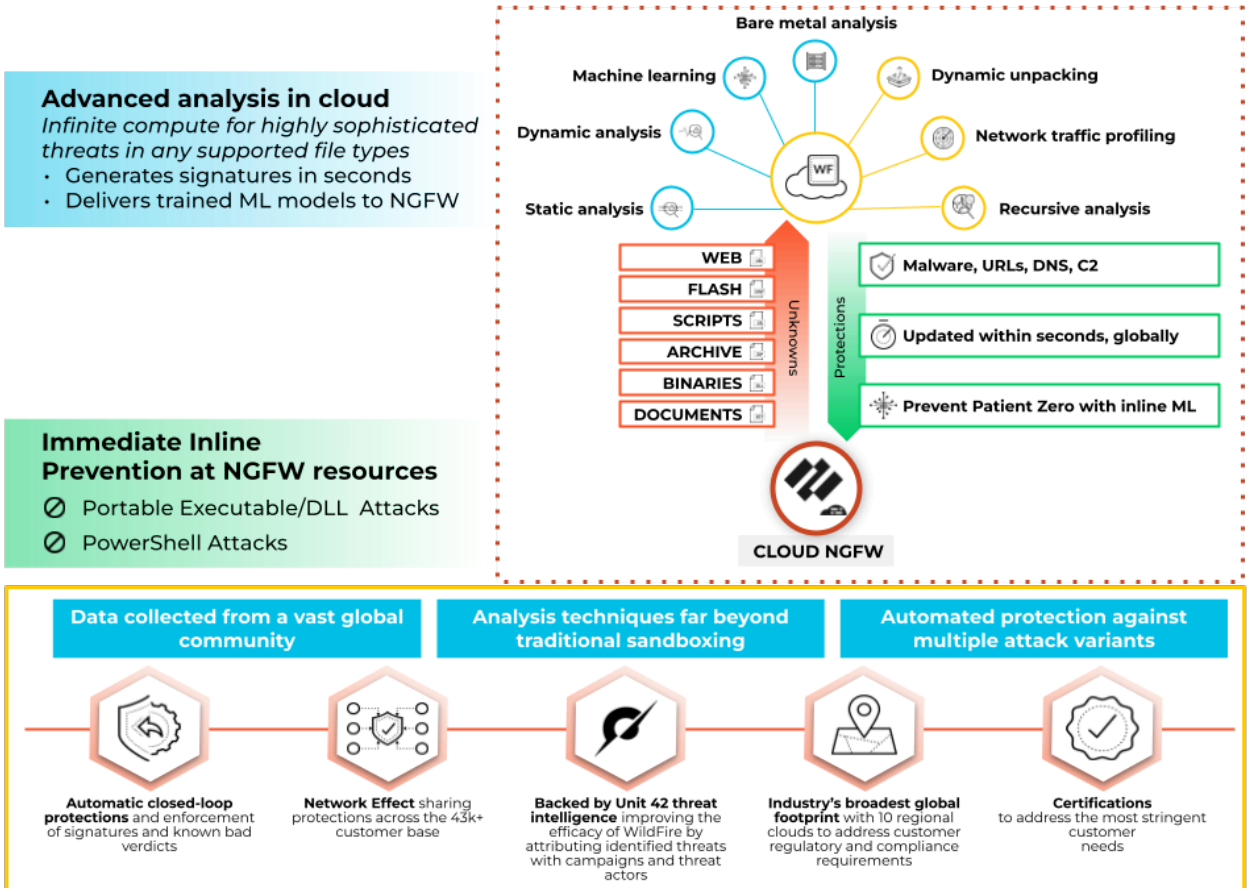
   Tout trafic DNS provenant du sous-réseau protégé est acheminé via le terminal Cloud NGFW et ensuite vers le Cloud NGFW pour inspection et application.

Configurer WildFire pour Cloud NGFW sur AWS

Cloud NGFW peut désormais détecter et transférer des fichiers, des exécutables et des scripts malveillants (tels que JScript et PowerShell) dans votre trafic de VPC vers le service cloud WildFire™ (WF) à des fins d'analyse. Wildfire applique ensuite des renseignements sur les menaces, l'analytique et des corrélations sur ces fichiers transférés (exécutables ou scripts) et délivre des verdicts basés sur l'analyse. Si une menace est détectée sur eux, WildFire crée des protections pour bloquer les logiciels malveillants, et distribue globalement ces protections contre cette menace en quelques minutes.

WildFire va au-delà des approches traditionnelles de sandbox et utilise plusieurs techniques pour identifier les fichiers présentant des comportements malveillants potentiels. Ces techniques comprennent :

- **Analyse dynamique** : observe les fichiers pendant leur exécution dans un environnement virtuel spécialement conçu et résistant aux invasions, permettant la détection de logiciels malveillants jusqu'alors inconnus à l'aide de centaines de caractéristiques comportementales.
- **Analyse statique** : complète l'analyse dynamique avec une détection efficace des logiciels malveillants, fournissant une identification instantanée des variantes de logiciels malveillants. L'analyse statique exploite davantage la décompression dynamique pour analyser les menaces qui tentent d'échapper à la détection grâce à l'utilisation d'ensembles d'outils de mise en paquets.
- **Profils de trafic réseau** : détecte les profils de trafic malveillants basés sur des variantes de logiciels malveillants telles que la création de backdoor, le téléchargement de logiciels malveillants d'étape suivante, l'accès à des domaines de faible réputation et la reconnaissance de réseau.
- **Machine learning** : extrait des milliers de fonctionnalités uniques de chaque fichier, en formant un modèle de machine learning prédictif pour identifier de nouveaux logiciels malveillants, ce qui n'est pas possible avec l'analyse statique ou dynamique seule.
- **Un hyperviseur créé sur mesure** : empêche les techniques d'évasion des attaquants grâce à un hyperviseur robuste et propriétaire qui ne dépend pas de projets open source ou de logiciels propriétaires auxquels les attaquants ont accès.



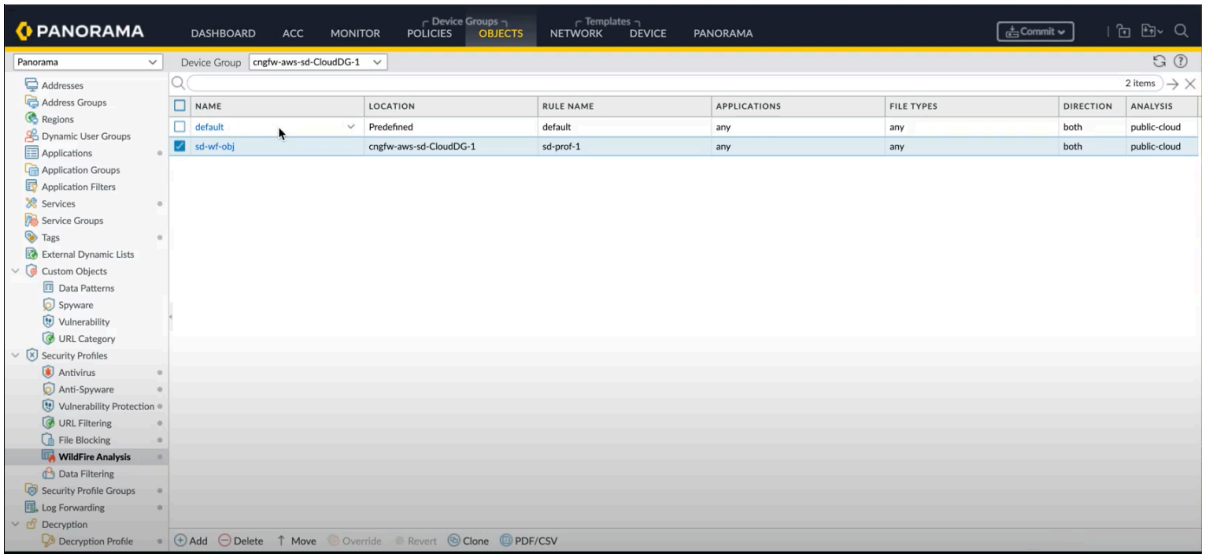
Pour configurer Wildfire sur votre ressource Cloud NGFW AWS, vous devez procéder comme suit :

- Configurez un profil Wildfire
- Définissez des règles de sécurité dans le groupe d’appareils Cloud que vous avez créé dans Panorama
- Afficher les journaux d’envois WildFire

Configurez un profil Wildfire

STEP 1 | Connectez-vous à **Panorama** et cliquez sur **Objects (Objets) > WildFire Analysis (Analyse WildFire)**. La fenêtre Profil d’analyse WildFire s’affiche.

STEP 2 | Sélectionnez le groupe d’appareils dans le menu déroulant où vous souhaitez créer le profil.



STEP 3 | Cliquez sur **Add (Ajouter)**.

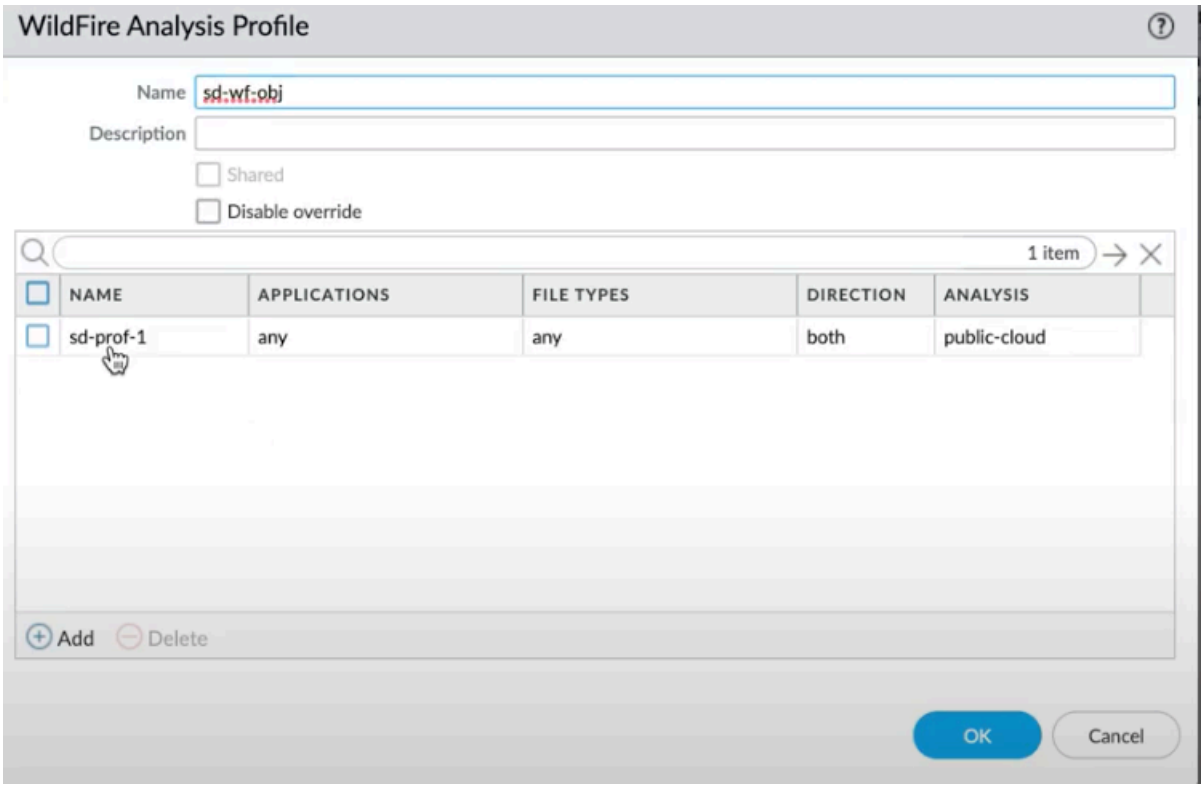
STEP 4 | Saisissez un **Name (Nom)** pour le profil WildFire et cliquez sur **Add (Ajouter)**.

STEP 5 | Saisissez un **Name (Nom)** descriptif à toute règle que vous ajoutez au profil

STEP 6 | Dans la section Application, cliquez sur **Add (Ajouter)** pour sélectionner l'application dans la liste des applications auxquelles vous souhaitez autoriser l'accès via votre profil Wildfire.

STEP 7 | Cliquez sur **FileTypes (Types de fichiers)** pour sélectionner les types de fichiers que vous souhaitez autoriser.

STEP 8 | Cliquez sur **Direction** pour autoriser le téléchargement/chargement ou les deux options.



STEP 9 | Sélectionnez la **Destination** du trafic à transférer pour analyse : Sélectionnez **public-cloud (cloud public)** si vous souhaitez que tout le trafic correspondant à la règle soit transféré vers le Cloud public WildFire à des fins d'analyse.

STEP 10 | Sélectionnez **private-cloud (cloud privé)** afin que l'ensemble du trafic correspondant à la règle soit transféré vers l'appareil WildFire à des fins d'analyse.

STEP 11 | Cliquez sur **OK**.

Définir des règles de sécurité

STEP 1 | Connectez-vous à Panorama, puis cliquez sur **Policies (Politiques)**.

STEP 2 | Choisissez le Device Group (Groupe d'appareils) requis et cliquez sur la règle de sécurité préconfigurée (règle « avant » ou règle « après ») ou créez une nouvelle règle.

STEP 3 | Cliquez sur **Actions**.

STEP 4 | Dans les paramètres du profil, sélectionnez **Profiles (Profils)** sous le type de profil.

STEP 5 | Sélectionnez le profil Wildfire que vous souhaitez choisir dans la liste déroulante **WildFire Analysis (Analyse WildFire)**.

STEP 6 | Cliquez sur **OK**.

Validez et transmettez le groupe d'appareils vers les ressources Cloud NGFW.

Pour plus d'informations, consultez Latest WildFire Cloud Features (Dernières fonctionnalités de WildFire Cloud).

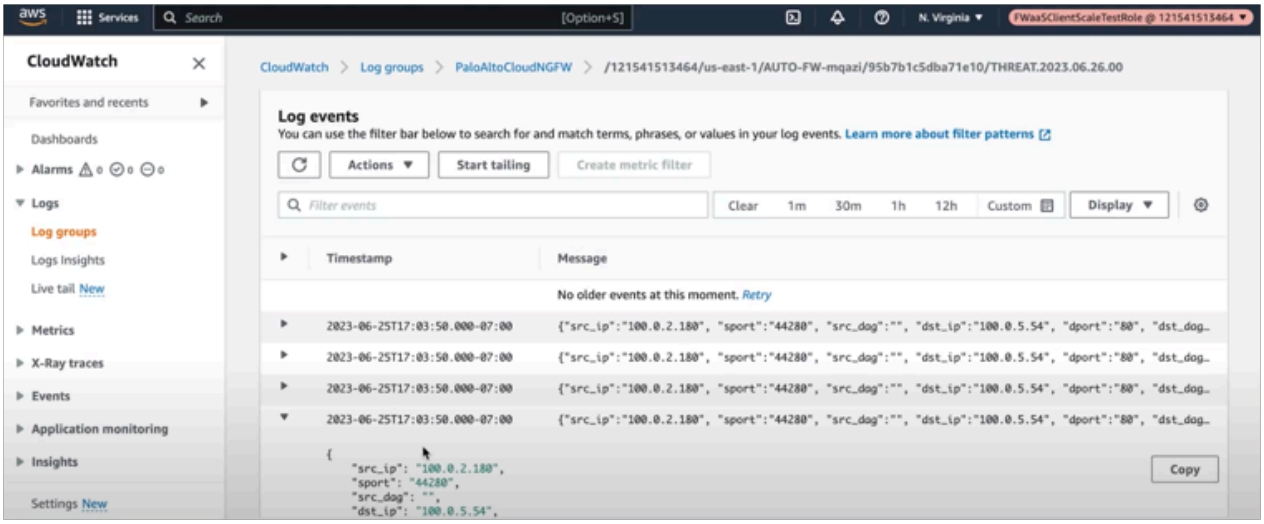
Afficher les journaux d'envois WildFire

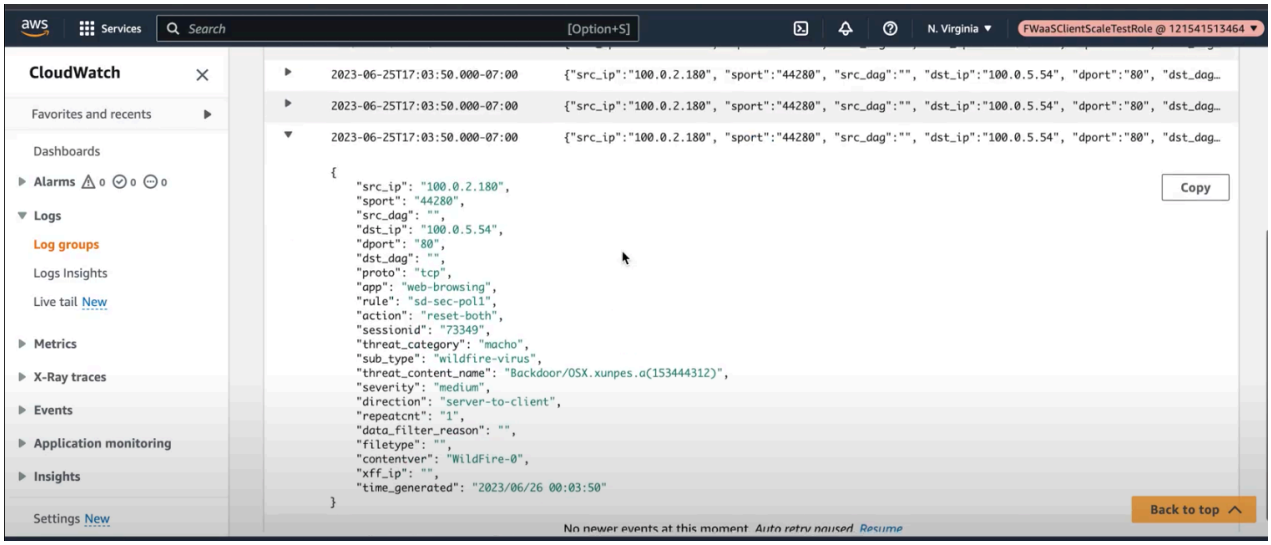
Vous pouvez afficher les journaux d'envois WildFire dans :

1. Destinations des journaux AWS
2. Panorama
3. Service de journalisation Strata

Afficher les journaux dans les destinations AWS

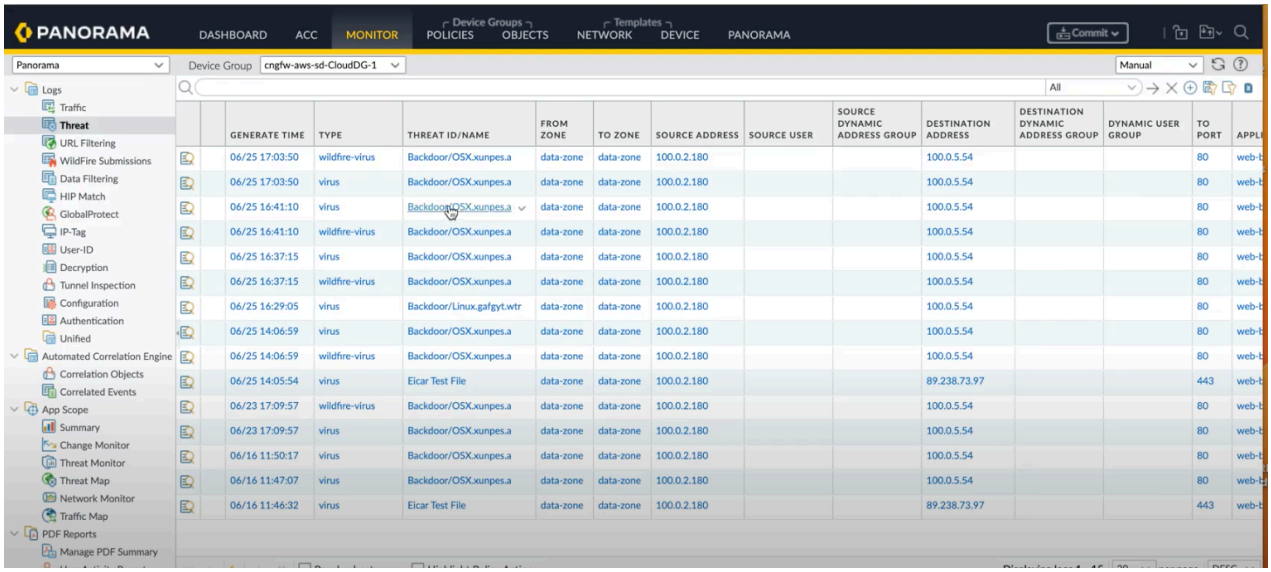
Si vous avez précédemment configuré Amazon Cloudwatch, Amazon S3 ou Amazon Kinesis comme destination de journal, vous pouvez les passer en revue à l'aide de Wildfire pour détecter les blocs de trafic malveillant.





Afficher les journaux dans Panorama

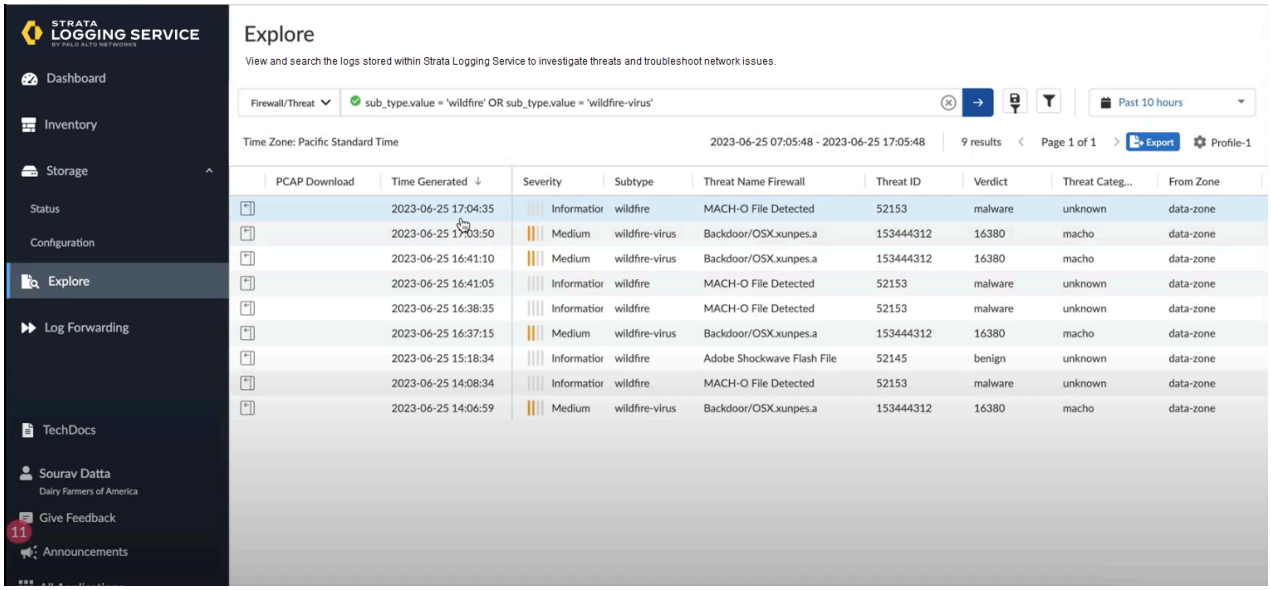
Sur Panorama, vous pouvez afficher les journaux sur le tableau de bord en cliquant sur **Monitor (Surveiller)** > **Threats (Menaces)**.



Afficher les journaux dans le service de journalisation Strata

Vous pouvez également afficher les journaux WildFire dans votre instance Strata Logging Service.

1. Cliquez sur **Explore (Explorer)** et sélectionnez **Firewall/Threat (Pare-feu/menace)** dans le menu déroulant Explorer.
2. Saisissez `sub_typevalue = wildfire` ou `wildfire-virus` et filtrez les journaux WildFire.

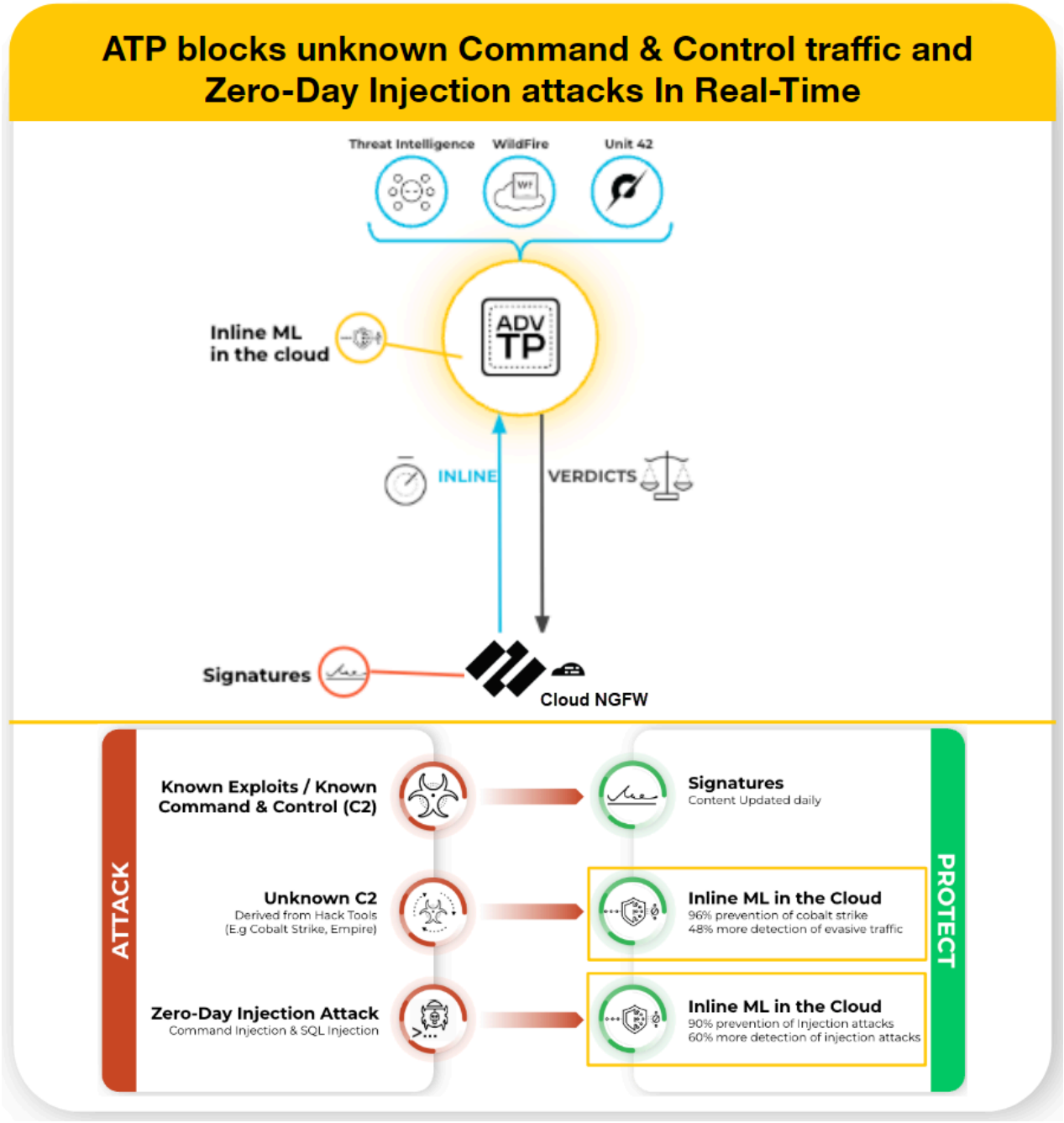


Protection avancée contre les menaces dans le Cloud NGFW

La prévention avancée des menaces (ATP) est une solution de système de prévention des intrusions (IPS) capable de détecter et de bloquer les logiciels malveillants, les exploits de vulnérabilité et la commande et le contrôle (C2) sur tous les ports et protocoles, à l'aide d'un système de prévention multicouche avec des composants fonctionnant sur Cloud NGFW pour AWS et dans le cloud. Le cloud de prévention des menaces exploite une multitude de services de détection en utilisant les données de menaces combinées des services Palo Alto Networks pour créer des signatures, chacune possédant des modèles identifiables spécifiques, et sont utilisées par le Cloud NGFW pour AWS pour appliquer des règles de politique de sécurité lors de la détection de menaces et de comportements malveillants correspondants. Ces signatures sont classées en fonction du type de menace et se voient attribuer des numéros d'identification uniques. Pour détecter les menaces qui correspondent à ces signatures, Cloud NGFW pour AWS exploite des moteurs d'analyse qui inspectent et classent le trafic réseau présentant des caractéristiques anormales.

Après avoir activé la Prévention avancée des menaces, utilisez Panorama pour configurer les politiques de prévention avancée des menaces associées.

En plus du mécanisme de détection basé sur les signatures, la prévention avancée des menaces fournit un système de détection en ligne afin de prévenir les menaces C2 inconnues et évasives, y compris celles produites via le framework Empire, ainsi que les vulnérabilités d'injection de commandes et d'injection SQL. Le cloud de prévention avancée des menaces exploite des modèles de deep learning extensibles qui permettent des capacités d'analyse en ligne sur le Cloud NGFW pour AWS, sur une base par requête, pour empêcher les menaces de type «zero-day» de pénétrer dans le réseau et pour distribuer des protections. Cela vous permet de prévenir les menaces inconnues à l'aide d'une inspection du trafic en temps réel avec des détecteurs en ligne. Ces moteurs de détection basés sur le ML et l'apprentissage profond dans le cloud de prévention avancée des menaces analysent le trafic à la recherche de C2 inconnus et de vulnérabilités qui utilisent l'injection SQL et l'injection de commandes pour protéger contre les menaces de type «zero-day». Pour fournir un contexte de menace et des détails de détection complets, des rapports sont générés et peuvent inclure les outils et techniques utilisés par l'attaquant, la portée et l'impact de la détection, ainsi que la classification de cyberattaque correspondante, telle que définie par le framework MITRE ATT&CK®.



Gestion native des politiques

La prévention avancée des menaces (ATP) est configurée automatiquement lorsque vous créez une rulestack locale. Pour les rulestacks précédemment créées avant mars 2024, activez ATP manuellement à l'aide de la console Cloud NGFW pour AWS.

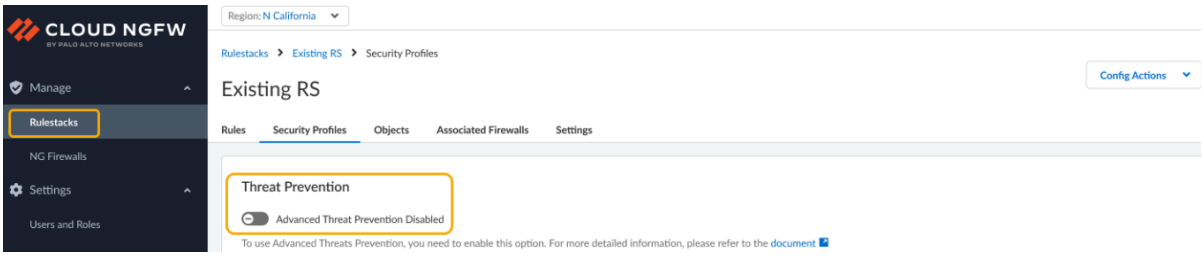
Pour activer ATP pour une rulestack :

STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sélectionnez **Rulestacks**.

STEP 3 | Sélectionnez **Security Profiles (Profils de sécurité)**.

STEP 4 | Dans la section **Threat Prevention (Prévention des menaces)**, utilisez le bouton d'activation/de désactivation pour activer **Advanced Threat Prevention (Prévention avancée des menaces)**.



STEP 5 | Une boîte de dialogue de confirmation s'affiche, indiquant que la fonctionnalité ATP peut entraîner des frais. Cliquez sur **Enable (Activer)**. Pour plus d'informations, consultez votre abonnement à la facturation AWS.

Utilisez Panorama pour configurer votre abonnement ATP dans le cadre de votre déploiement de sécurité réseau. Bien qu'il ne soit peut-être pas nécessaire de mettre en œuvre tous les processus qui composent l'ATP, Palo Alto Networks vous recommande de passer en revue toutes les tâches pour vous familiariser avec les options disponibles pour un déploiement réussi.

Gestion des politiques de Panorama

La prévention avancée des menaces (à l'instar des autres services de sécurité de Palo Alto Networks) est administrée par le biais de profils de sécurité, qui dépendent à leur tour de la configuration des politiques d'application du réseau telles que définies par les règles de politique de sécurité.

Vous utilisez Cloud NGFW pour AWS pour activer la prévention avancée des menaces pour la rulestack, mais vous devez utiliser Panorama pour configurer les politiques qui composent le service de sécurité.

Pour configurer les règles de politique de filtrage avancé des URL à l'aide de Panorama :

STEP 1 | Connectez-vous à Panorama.

STEP 2 | Vérifiez que vous disposez de l'abonnement de licence approprié pour le filtrage avancé des URL. Dans Panorama, sélectionnez **Device (Périphérique) > Licenses (Licences)**. Vérifiez que la date d'expiration de la licence se situe dans le futur.

STEP 3 | Configurez Advanced Threat Prevention (Prévention avancée des menaces) à l'aide de Panorama.

STEP 4 | Validez vos modifications.

Palo Alto Networks propose plusieurs options pour surveiller l'activité traitée par le service de sécurité de prévention avancée des menaces. Consulter Surveiller la prévention avancée des menaces pour plus d'informations.

Gestion des politiques de Panorama

Cloud NGFW est le seul NGFW alimenté par le machine learning (ML) du secteur fourni en tant que service cloud natif sur AWS. 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 AWS.

Cette page explique la manière de configurer et d'intégrer Cloud NGFW pour AWS 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 à partir d'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, les pare-feu virtuels et les pare-feu cloud, améliorant ainsi l'efficacité opérationnelle de la gestion et de la maintenance d'un réseau hybride de pare-feu.

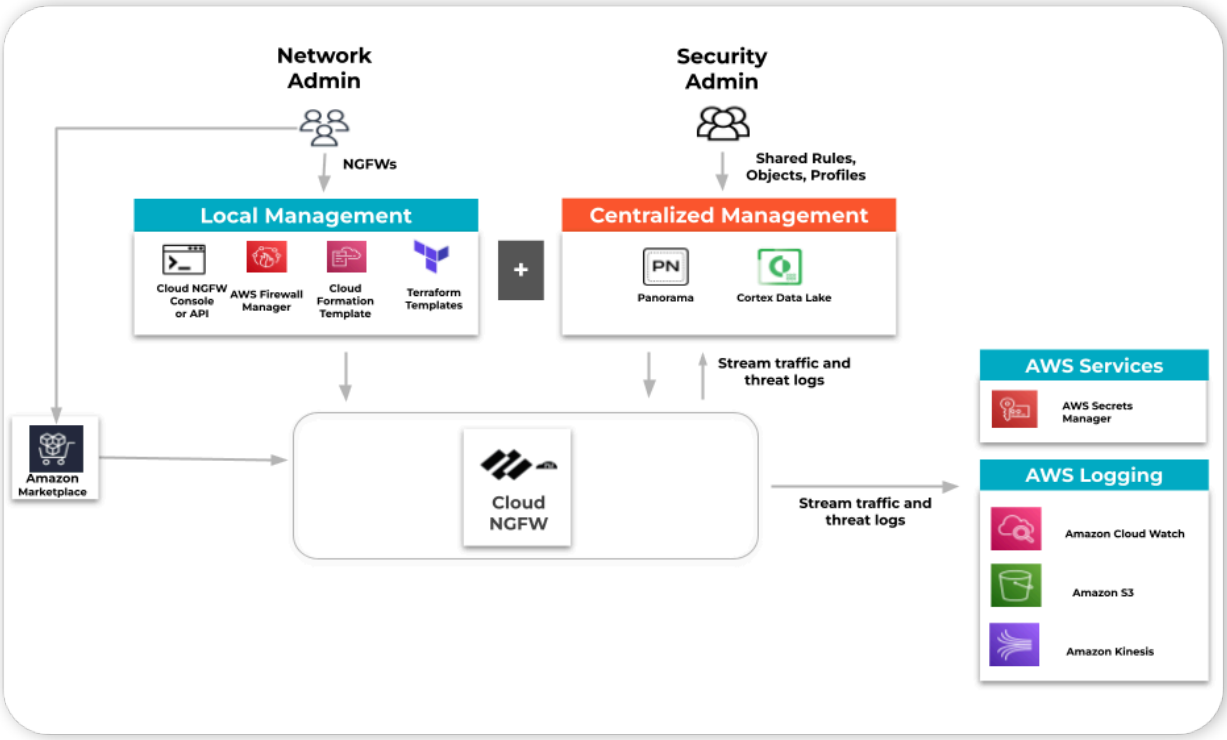
Comment fonctionne l'intégration ?

Vous continuerez votre abonnement au service Cloud NGFW à l'aide d'AWS Marketplace et vous créez un locataire. Ensuite, vous pouvez lier votre locataire Cloud NGFW à votre ou vos appareils Panorama. Vous pouvez ensuite gérer un ensemble partagé de règles de sécurité de manière centralisée sur les ressources Cloud NGFW que vous créez sur ce locataire 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 à partir d'une console Panorama.

Votre ou vos appareils Panorama peuvent résider dans n'importe quelle région Cloud ou dans un environnement sur site. Panorama utilise le plug-in AWS pour transmettre des politiques et des objets aux ressources NGFW dans les régions AWS.

L'intégration entre le Cloud NGFW et votre ou votre ou vos appareils Panorama permet éventuellement à vos ressources Cloud NGFW de diffuser les journaux vers un compte de Cortex Data Lake (CDL). Vous pouvez ensuite utiliser l'interface utilisateur CDL, la visionneuse de journaux Panorama ou le Application Command Center (Centre de commande des applications - ACC) pour afficher et analyser les journaux de CDL. Panorama utilise le plug-in Cloud Services pour interroger les journaux de votre compte CDL.

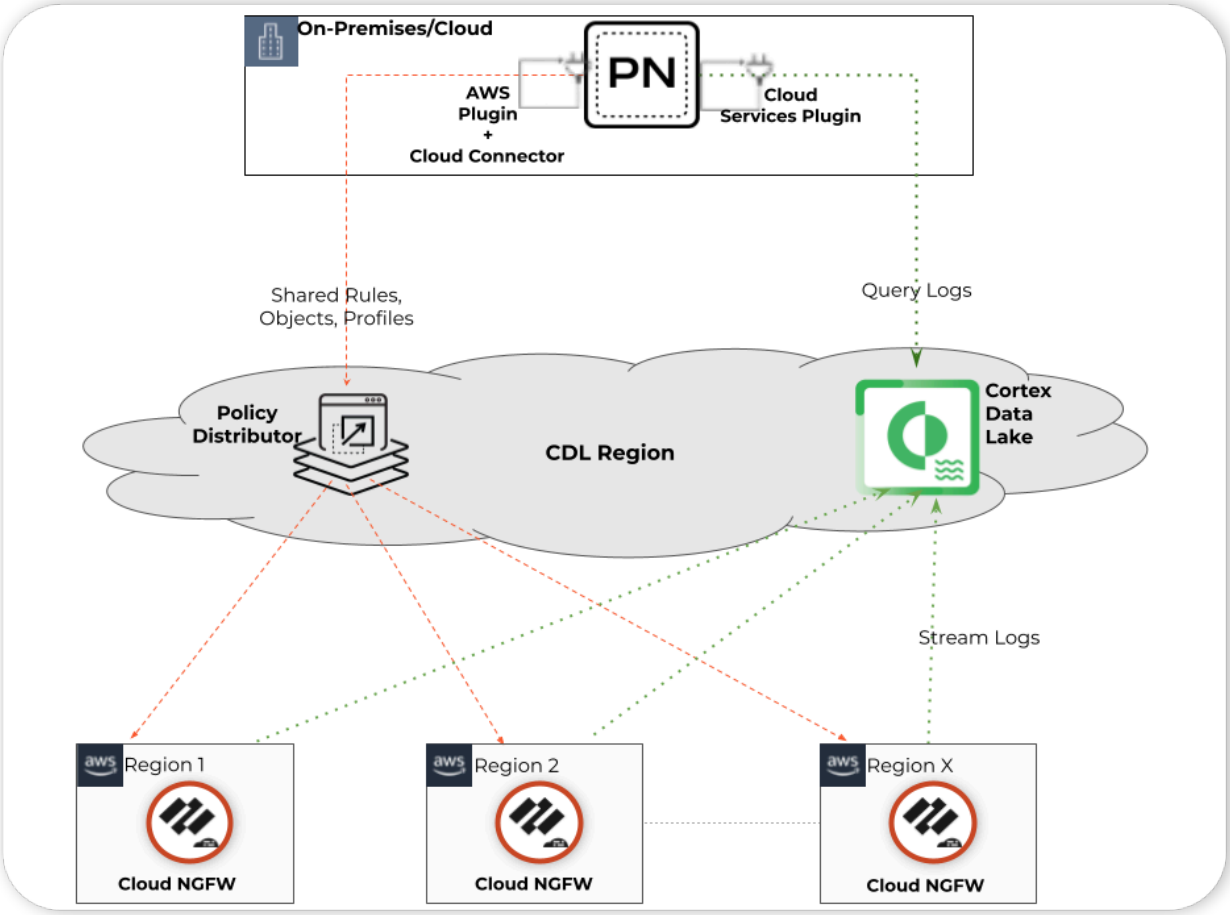
Vous pouvez également configurer les ressources Cloud NGFW pour diffuser les journaux vers des destinations de journaux AWS telles que les flux S3, Cloudwatch et Kinesis.



Vous pouvez lier plusieurs paires Panorama, CDL au locataire Cloud NGFW.

Composants de l’intégration

L’image ci-dessous illustre l’intégration de Cloud NGFW à Panorama. Tous ces composants sont décrits dans la section suivante.



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

La gestion des journaux de Palo Alto Networks n'est pas un composant obligatoire de cette solution. Vous utilisez Cortex Data Lake (CDL) si vous préférez afficher les journaux dans la console Panorama ou utilisez Application Command Center (Centre de commande des applications – ACC) dans la console Panorama pour obtenir des informations sur le trafic Cloud NGFW ou générer des rapports dans Panorama. Pour cela, vous devez relier votre Panorama à un compte Cortex Data Lake à l'aide du plug-in Cloud Services dans Panorama. Vous pouvez configurer les ressources Cloud NGFW pour envoyer simultanément les journaux au lac de données Cortex Data Lake et à l'une des destinations de journaux AWS (flux S3, Cloudwatch ou Kinesis).

1) Reliez votre Panorama au lac de données Cortex Data Lake avant de le relier à votre locataire Cloud NGFW, 2) Si vous utilisez plusieurs Panoramas avec le même locataire Cloud NGFW, assurez-vous que chaque Panorama soit lié à des instances individuelles du lac de données Cortex Data Lake.

Le plug-in AWS Panorama est un composant obligatoire de cette solution. Le plug-in AWS 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 du ou des locataires Cloud NGFW liés à Panorama. Le plug-in AWS Panorama utilise le plug-in Cloud Connector en interne pour communiquer avec les ressources Cloud NGFW.

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/des API du plug-in AWS Panorama en spécifiant le locataire Cloud NGFW et les informations de région AWS. Cloud DG se manifeste sous la forme d'une rulestack globale dans ce locataire/cette région.

- Le plug-in AWS 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 du locataire Cloud NGFW. Ce Cloud DG se manifestera sous la forme d'une rulestack globale dédiée dans chaque région AWS de votre locataire 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 AWS 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 Cloud DG en tant que pile de modèles de référence. À partir de ce moment, vous pouvez utiliser la page Template Stack (Pile de modèles) de l'interface utilisateur Panorama native pour configurer vos modèles et les ajouter à ces Cloud TS.

- Le service Palo Alto Networks Cloud NGFW 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 de 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.

Certaines étapes doivent être suivies pour intégrer Cloud NGFW à Panorama. Après avoir configuré votre appareil virtuel Panorama et installé des plug-ins, vous devrez vous abonner à Cloud NGFW à l'aide d'AWS Marketplace et créer un locataire. Après avoir créé le locataire Cloud NGFW, reliez-le à votre appareil virtuel Panorama. Une fois que vous avez lié Cloud NGFW, utilisez Panorama pour gérer les objets et les règles de sécurité, et surveiller les journaux et l'analytique.

Intégration de Panorama

Certaines étapes doivent être suivies pour intégrer Cloud NGFW à Panorama. Vous devez d'abord préparer votre appareil Panorama à cette intégration en installant les plug-ins. Vous devrez ensuite utiliser la console Cloud NGFW pour la lier à votre appareil Panorama. Une fois que la liaison au Cloud NGFW est réussie, utilisez Panorama pour gérer les objets et les règles de sécurité et pour surveiller les journaux et l'analytique.

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

- Préparer votre Panorama pour établir une liaison avec le ou les locataires du Cloud NGFW
- Relier le Cloud NGFW à la gestion centralisée de Palo Alto Networks
- Associer un Panorama lié à la ressource Cloud NGFW
- Dissocier le Cloud NGFW de Palo Alto Networks Management
- Utiliser Panorama pour la gestion des politiques Cloud NGFW
- Afficher les journaux et l'activité du Cloud NGFW dans Panorama
- Afficher les journaux et l'activité du Cloud NGFW dans le service de journalisation Strata

Répétez les étapes ci-dessus lors de la liaison de plusieurs Panoramas avec un locataire Cloud NGFW.

Préparation à l'intégration de Panorama

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

- Assurez-vous d'avoir installé un Panorama enregistré avec des licences, activé à l'aide de la licence de support sur le Portail de support client (CSP) et utilisant la version du logiciel 10.2.3 (ou supérieure).

  Vous devez installer le certificat de périphérique sur le serveur de gestion Panorama pour pouvoir authentifier Panorama auprès du Portail de support client (CSP) de Palo Alto Networks et exploiter un ou plusieurs services cloud.
- Si vous choisissez d'utiliser la gestion des journaux Palo Alto, assurez-vous de configurer Panorama pour Cortex Data Lake.
- Assurez-vous de vous être abonné à Cloud NGFW avec succès pour disposer d'un locataire Cloud NGFW. Vous devez utiliser l'abonnement Cloud NGFW pour réussir l'intégration à Panorama.
- Assurez-vous de disposer d'un rôle administrateur de locataire dans votre locataire Cloud NGFW.
- Assurez-vous de disposer d'un rôle administrateur Panorama sur votre Panorama.
- Assurez-vous que vous êtes membre du compte de Portail de support client (CSP) de Palo Alto Networks sur lequel votre organisation a enregistré l'appareil Panorama.

  Vous devez utiliser l'adresse e-mail utilisée pour s'enregistrer sur le compte CSP pour l'abonnement du locataire Cloud NGFW. Si cette adresse e-mail est différente, vous ne pourrez pas configurer Cloud NGFW et intégrer Panorama.
- Autorisez l'accès au domaine https://storage.googleapis.com. Ce domaine est utilisé pour accéder à l'application AIOps pour le Cloud NGFW, quelle que soit votre situation géographique.

Exigences supplémentaires

Pour préparer Panorama à établir un lien à Cloud NGFW :

- Installez le plug-in Cloud Connector version 2.0.1 ou ultérieure

  PAN-OS version 11.1.x est pré-emballé avec un plug-in Cloud Connector (version 2.1.0-c98). Cette version de plug-in cause des problèmes de gestion de la ressource Cloud NGFW liée à PAN-OS version 11.1.x. Si vous utilisez PAN-OS version 11.1.x, Palo Alto Networks vous recommande de ***rétrograder*** *le plug-in Cloud Connector vers la version 2.0.1.*

- Installez le plug-in AWS version 5.1.1 ou ultérieure.
- Après avoir installé les plug-ins Cloud Connector et AWS, utilisez la CLI Panorama pour exécuter la commande `request plugins cloudconnector enable cloudngfw`.
- Affichez les plug-ins installés dans Panorama à l'aide du **tableau de bord**.
- Utilisez la CLI de Panorama pour afficher l'état d'un plug-in Panorama. Par exemple, la commande `show plugins aws cngfw-status`

```
show plugins aws cngfw-status CloudConnector plugin is enabled.
 Cloud NGFW functionality is enabled.
```

Considérations importantes

Le plug-in AWS nécessite que vous validiez une modification de configuration afin de lancer la fonctionnalité Cloud NGFW avec Panorama. Cette validation n'est pas requise pour la mise à niveau du plug-in AWS.

Dans les déploiements Panorama HA, la transmission d'une modification de configuration (par exemple, la modification d'un groupe d'appareils Cloud) peut entraîner le blocage de l'appareil virtuel Panorama. Un message d'erreur semblable à *La transmission ne peut pas être traitée, le téléchargement de la configuration n'est pas terminé. Veuillez réessayer ultérieurement.* Pour résoudre ce problème, utilisez `commit-force`, puis `commit-all`.

Reliez le Cloud NGFW à Palo Alto Networks Management

Vous avez deux options pour créer un lien :

1. Créez un lien du Cloud NGFW à Palo Alto Networks uniquement à l'aide de Panorama pour la gestion des politiques.
2. Reliez le locataire Cloud NGFW à Panorama pour la gestion des politiques et à Cortex Data Lake pour la gestion des journaux.

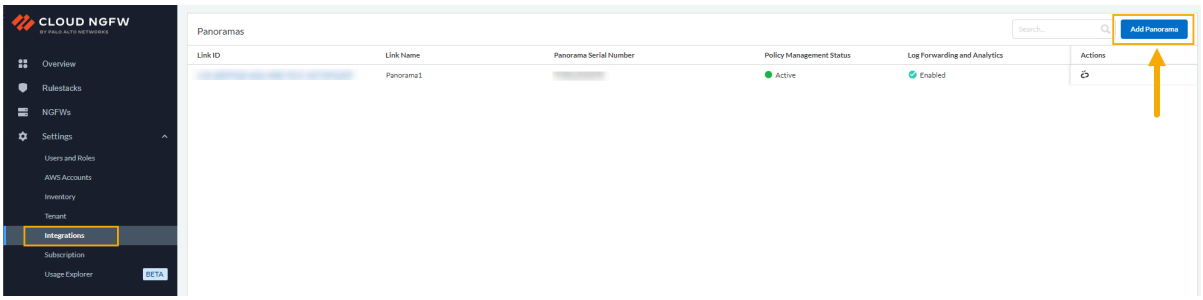
Vous devez être abonné au service Cloud NGFW à l'aide d'AWS Marketplace pour intégrer Cloud NGFW à Panorama. Après avoir lié votre locataire Cloud NGFW à Panorama, vous pouvez afficher les locataires et les ressources, ainsi que leur état, dans la console Panorama sous le plug-in AWS.

Consultez Dissocier le Cloud NGFW de Palo Alto Networks Management *pour supprimer un appareil virtuel Panorama existant de la ressource Cloud NGFW. Si vous utilisez AWS Firewall Manager, vous ne pouvez pas dissocier Panorama de votre ressource Cloud NGFW. Consultez* Créer un dossier de support pour dissocier le Cloud NGFW de Panorama lors de l'utilisation d'AWS Firewall Manager *pour en savoir plus.*

Pour relier votre locataire Cloud NGFW à Panorama à l'aide de Cloud NGFW :

STEP 1 | Sélectionnez **Integrations (Intégrations)**.

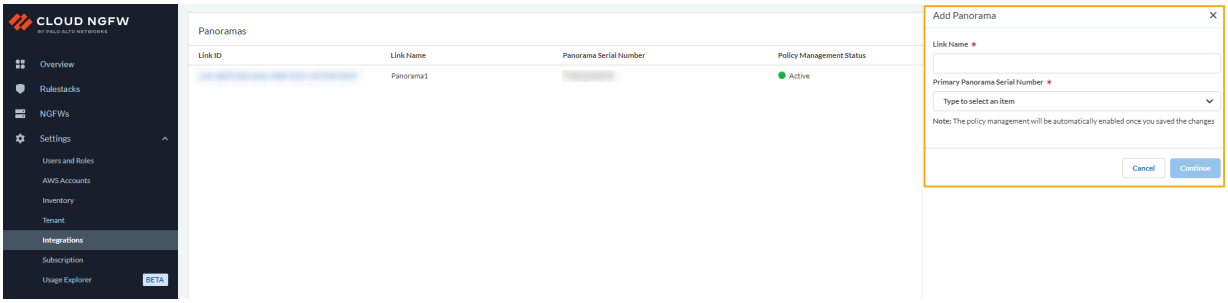
STEP 2 | Sur la page **Integrations (Intégrations)**, cliquez sur **Add Panorama (Ajouter Panorama)**.



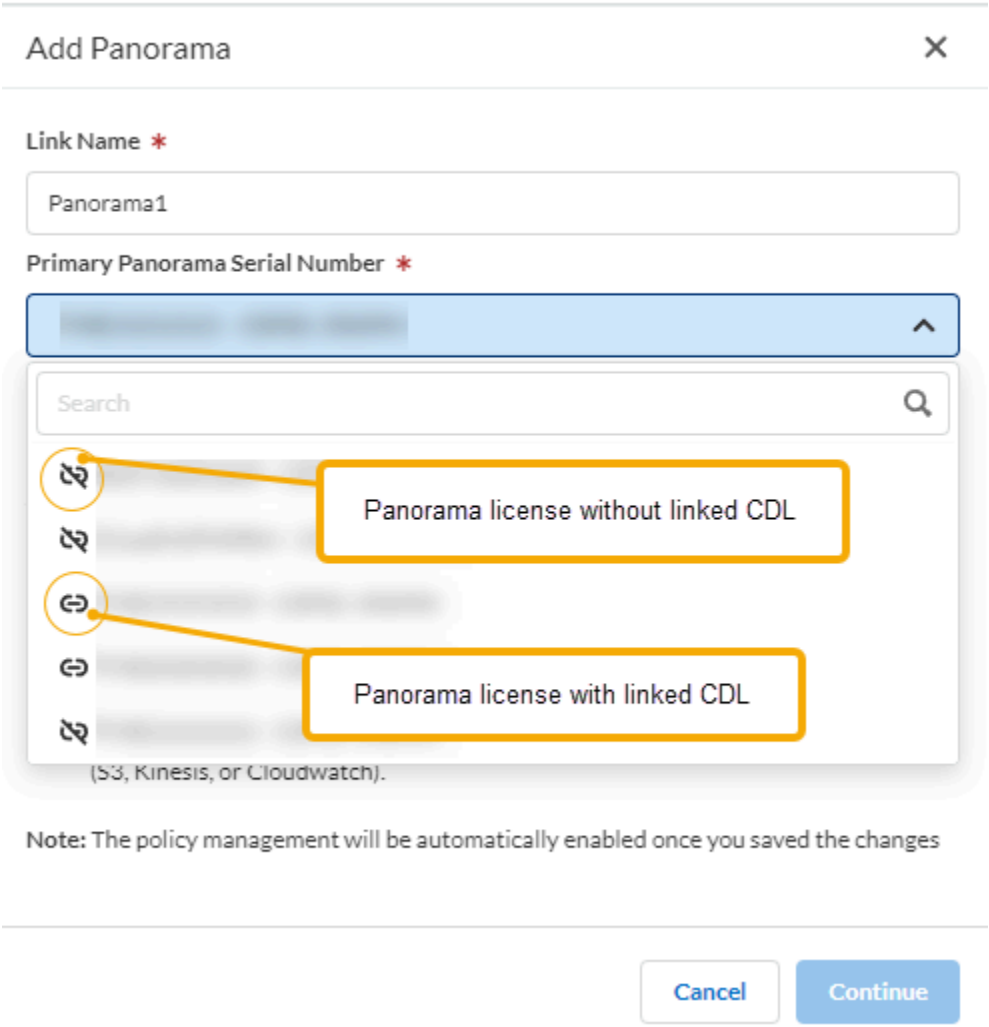
Si vous utilisez un locataire lié à Panorama qui avait été créé à l'aide d'AWS Firewall Manager, vous ne pouvez pas dissocier la ressource Cloud NGFW.

STEP 3 | Dans l'écran **Add Panorama (Ajouter un Panorama)**, saisissez un **Link Name (Nom de lien)**. Sélectionnez le **Primary Panorama Serial Number (Numéro de série Panorama principal)**

dans la liste déroulante. Pour les environnements HA, sélectionnez le **Secondary Panorama Serial Number (Numéro de série du Panorama secondaire)** dans la liste déroulante.



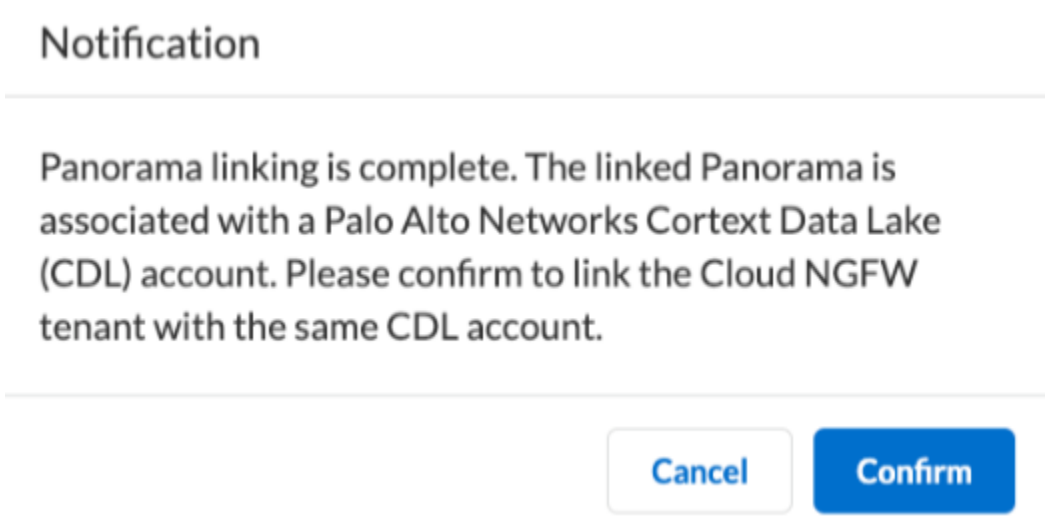
Cet écran affiche deux icônes différentes décrivant l'état de la licence Panorama ; un Panorama lié à CDL et un Panorama non lié à CDL. Ces icônes sont illustrées dans l'image ci-dessous :



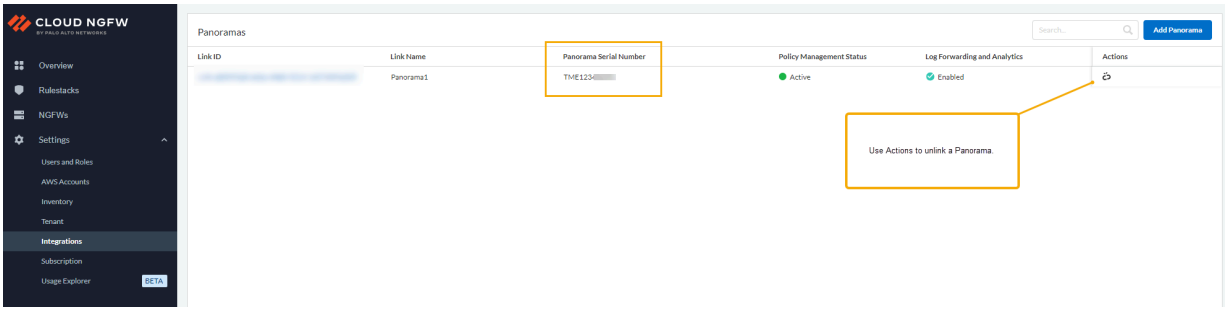
Si vous sélectionnez un numéro de série Panorama qui n'est pas lié à CDL, vous devez spécifier une option, soit pour annuler le processus de liaison, auquel cas vous acceptez d'acquérir une licence

CDL et de l’associer à votre appareil Panorama, soit vous acceptez de continuer à utiliser Panorama uniquement pour la gestion des politiques :

Si vous sélectionnez une licence Panorama déjà connectée à un CDL, vous êtes invité à **Confirm (Confirmer)** l’association avant de poursuivre le processus d’intégration :



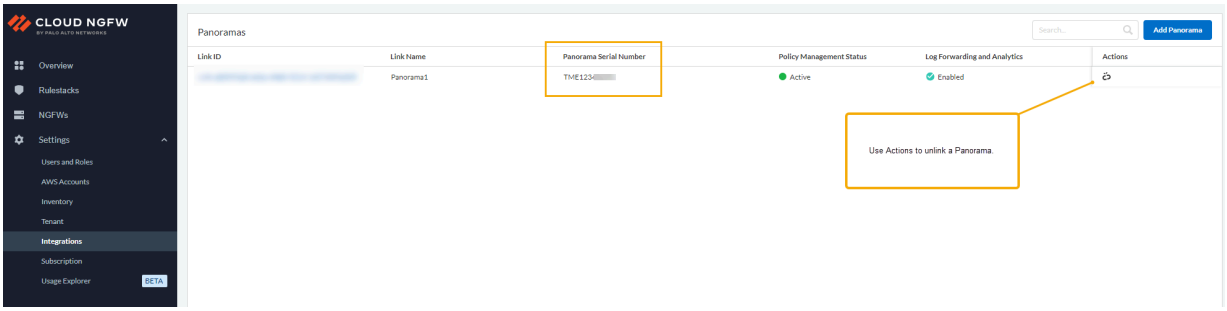
Après avoir sélectionné la licence Panorama, cliquez sur **Continue (Continuer)**. La page **Integrations (Intégrations)** affiche le **Link ID (ID du lien)** et le **Panorama Serial Number (Numéro de série Panorama)** lié :



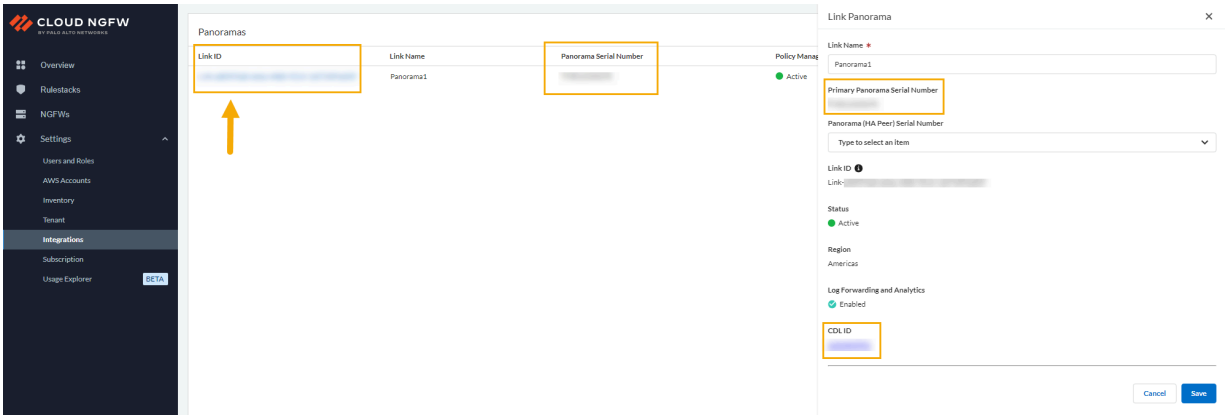
Le locataire Cloud NGFW extrait automatiquement les informations CDL de Panorama. Si vous ne prévoyez pas d’utiliser CDL pour la journalisation, vous pouvez envoyer des journaux à AWS.

Pour plus d’informations, consultez Configure Logging for Cloud NGFW on AWS (Configurer la journalisation pour Cloud NGFW sur AWS).

La page **Integrations (Intégrations)** affiche le **Link ID (ID du lien)** et le **Panorama Serial Number (Numéro de série Panorama)** lié. Pour plus d’informations, y compris l’ID de Cortex Data Lake, sélectionnez



Pour plus d’informations, y compris l’ID de Cortex Data Lake associé au Panorama lié, cliquez sur le **Link ID (ID de lien)** dans la page **Integrations (Intégrations)**. La fenêtre **Link Panorama (Lien Panorama)** apparaît :



Désabonnement d’un locataire Cloud NGFW d’AWS Marketplace

Pour désabonner un locataire Cloud NGFW d’AWS Marketplace :

STEP 1 | Connectez-vous à la Console de gestion AWS.

STEP 2 | Accédez à la page **My Subscriptions (Mes abonnements)**.

STEP 3 | Sélectionnez l’abonnement au produit que vous souhaitez annuler.

STEP 4 | Sélectionnez **Cancel subscription (Annuler l’abonnement)**. Après l’annulation de l’abonnement, vous ne pouvez pas lancer votre application.

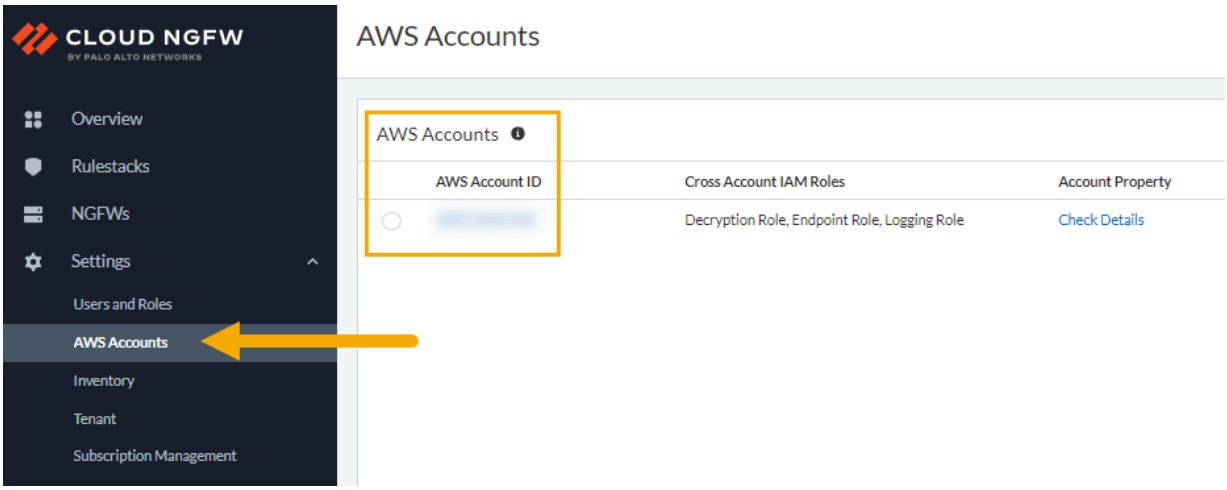
Pour plus d’informations, consultez Annuler votre abonnement.

Créer un dossier de support pour dissocier Panorama du Cloud NGFW lors de l’utilisation d’AWS Firewall Manager

Si vous utilisez AWS Firewall Manager et avez lié une ressource Cloud NGFW à Panorama, vous devez contacter le Support Palo Alto Networks pour dissocier la ressource Cloud NGFW de Panorama. Lors de la création du dossier de support, il peut vous être demandé de fournir des informations supplémentaires, telles que l’ID du compte AWS et l’ID du locataire de la ressource.

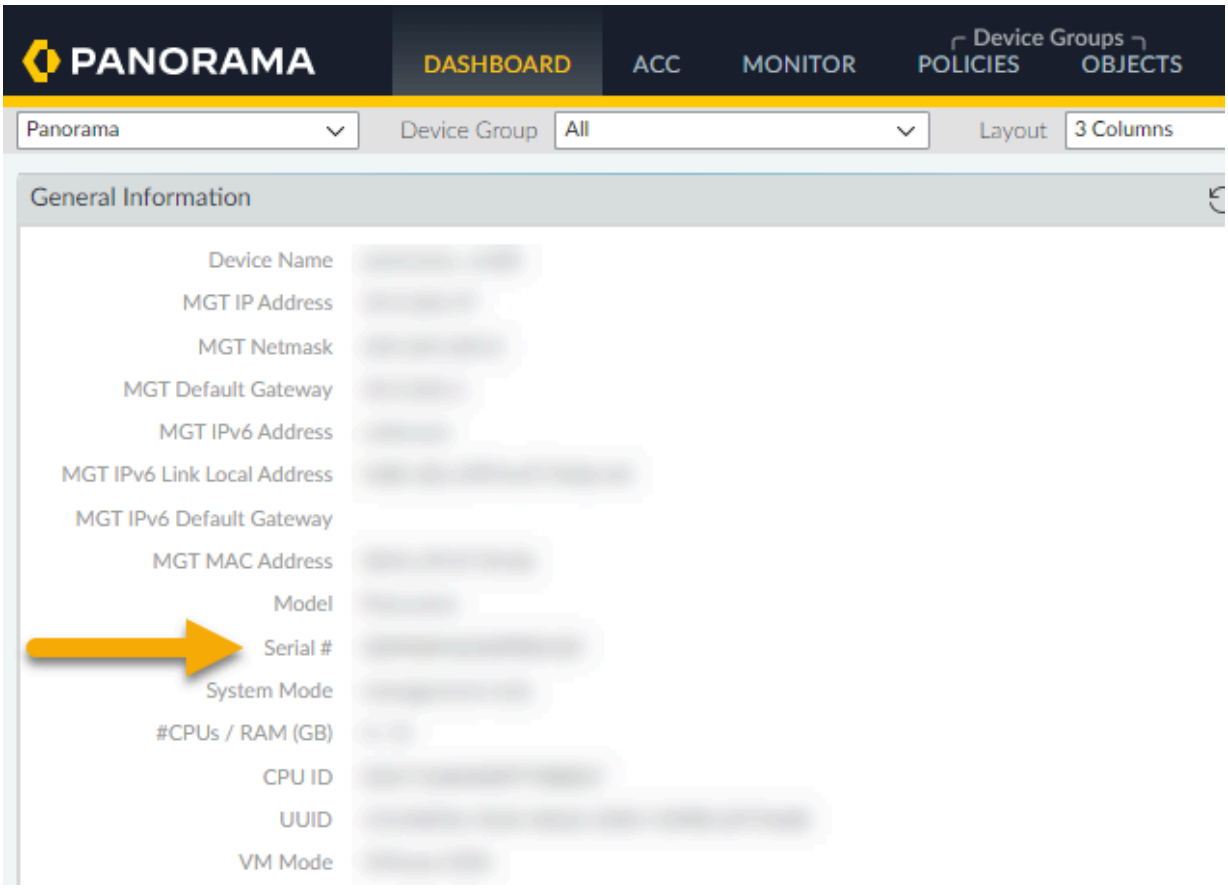
Pour créer une demande de support à l’aide de la console Cloud NGFW :

STEP 1 | Recherchez votre **AWS Account ID (ID de compte AWS)**. Sélectionnez **AWS Accounts (Comptes AWS)**.

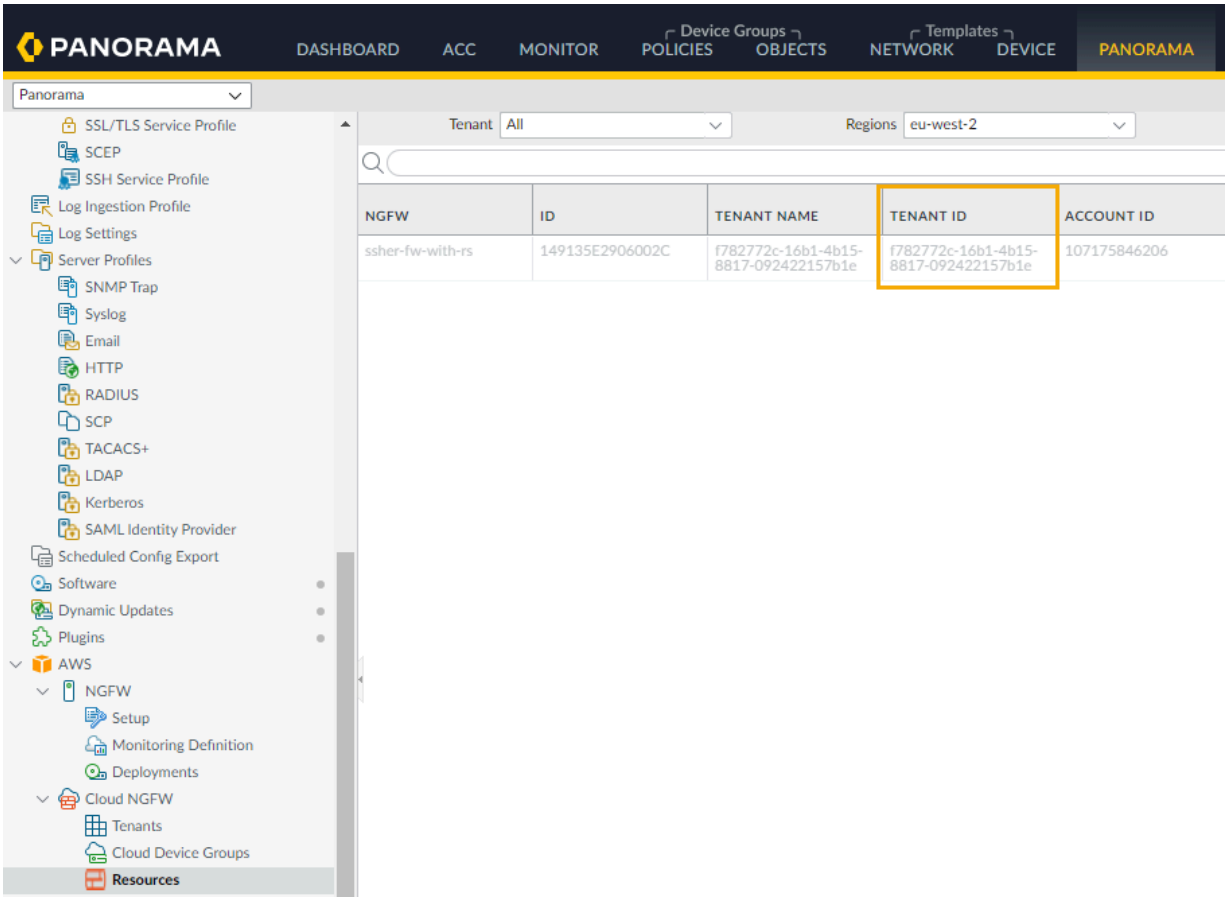


STEP 2 | Si nécessaire, utilisez la console Panorama pour déterminer des informations supplémentaires pour le dossier de support, telles que l'ID du locataire ou le numéro de série de Panorama.

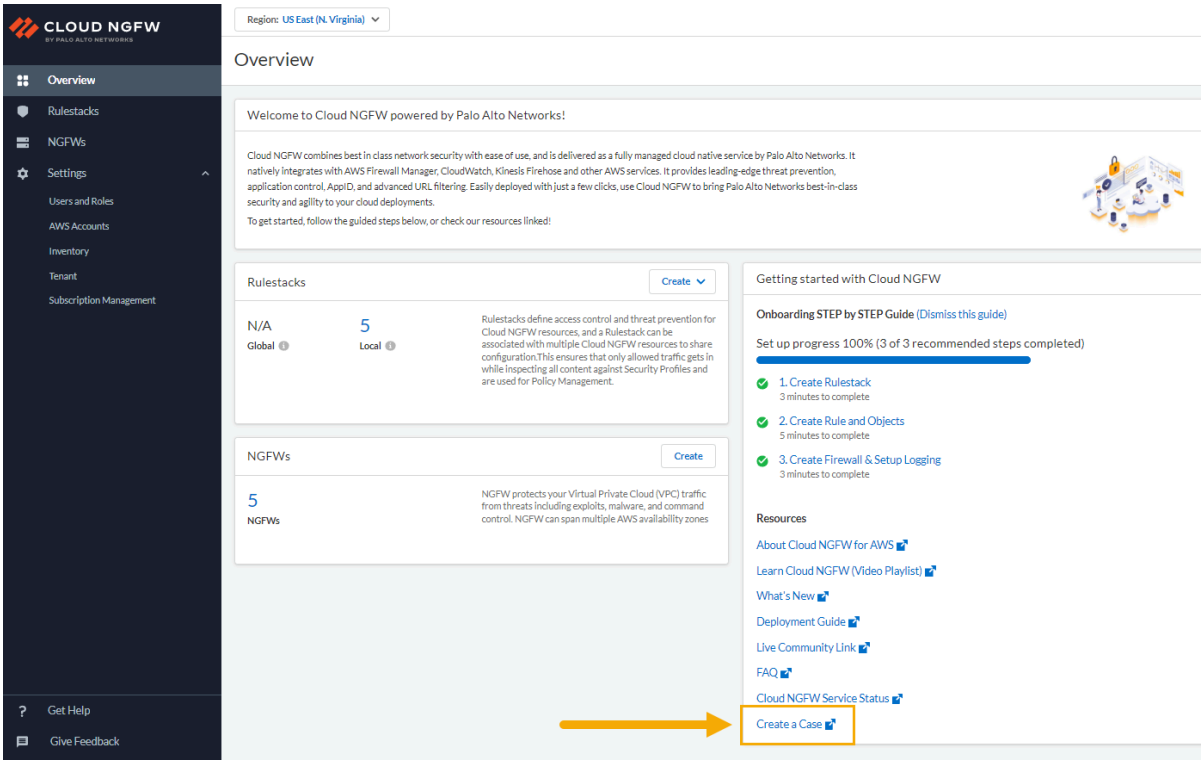
Recherchez le **Panorama serial number (numéro de série Panorama)** à l'aide du **Dashboard (Tableau de bord)** :



Recherchez le **Tenant ID (ID de locataire)** de la ressource Cloud NGFW :



STEP 3 | Sur la page **Overview (Présentation)** de la console Cloud NGFW, cliquez sur **Create a case (Créer un dossier)**.



Dissocier le Cloud NGFW de Palo Alto Networks Management

Avant de dissocier votre ressource Cloud NGFW de l'appareil virtuel Panorama, Palo Alto Networks vous recommande de supprimer ou de dissocier les *groupes d'appareils Cloud* associés à la ressource Cloud NGFW ou aux régions. Pour plus d'informations, consultez les sections Delete a Cloud Device Group (Supprimer un groupe d'appareils Cloud) ou Disassociate a Cloud Device Group from a Resource (Dissocier un groupe d'appareils Cloud d'une ressource).

Pour dissocier un appareil virtuel Panorama d'une ressource Cloud NGFW :

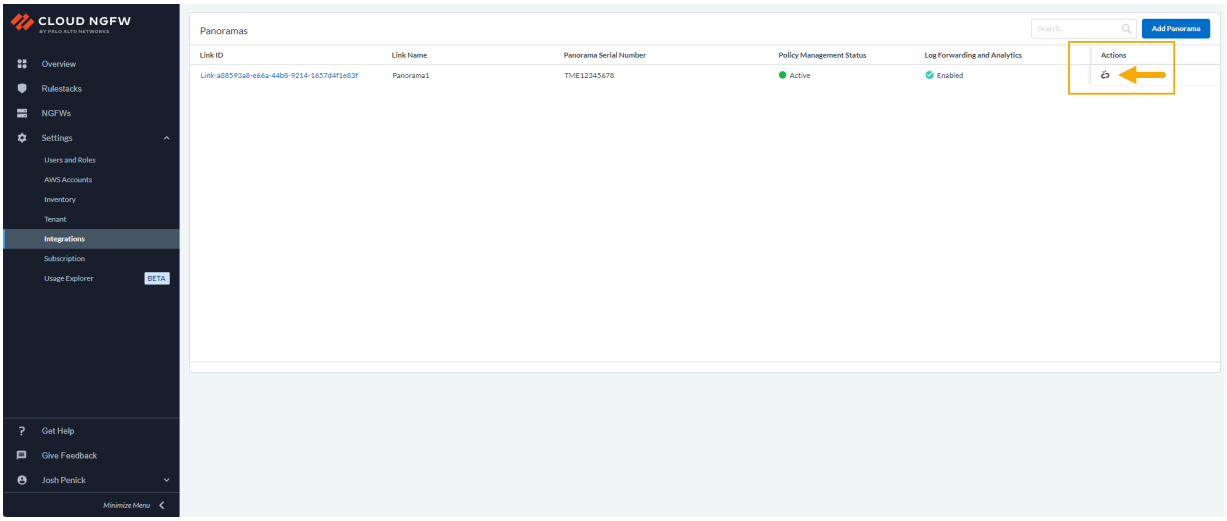
STEP 1 | Choisissez la région, par exemple, **us-east-1**, dans la page du pare-feu ou des rulestacks.

STEP 2 | Dans la console Cloud NGFW, sélectionnez **Integrations (Intégrations)**.

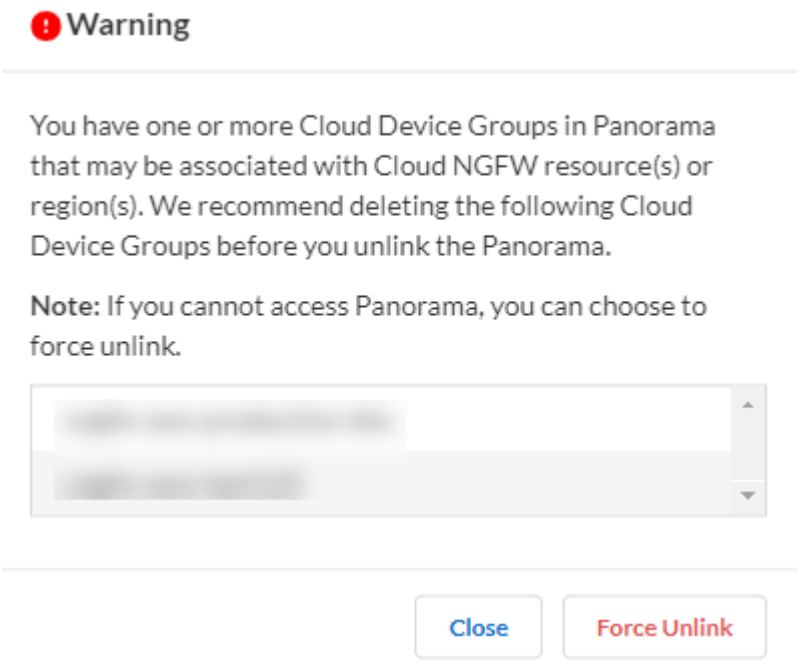
STEP 3 | Sur la page **Integrations (Intégrations)**, localisez la section **Actions**. Un Panorama précédemment lié apparaît grisé.

STEP 4 | Cliquez sur l'icône **Unlink (Dissocier)** pour commencer le processus de dissociation.

Si une paire HA est configurée, les deux paires sont dissociées.



STEP 5 | Lorsque vous dissociez un appareil virtuel Panorama de votre locataire Cloud NGFW, vous pouvez être invité à supprimer un ou plusieurs groupes d'appareils Cloud associés à la ressource Cloud NGFW ou à la région dont vous vous dissociez. Dans ces cas, un message d'erreur s'affiche, répertoriant les groupes d'appareils Cloud associés à la ressource Cloud NGFW liée à Panorama. Vous devez soit Supprimer un groupe d'appareils Cloud, soit Dissocier un groupe d'appareils Cloud d'une ressource avant de dissocier. Si vous n'avez pas accès à Panorama pour supprimer ces groupes d'appareils Cloud, cliquez sur **Force Unlink (Dissocier par la force)**.



STEP 6 | **Confirm (Confirmer)** le processus de dissociation. Si votre Panorama est associé à un compte de service de journalisation Strata, cette association est résiliée et les journaux sont supprimés après la période de conservation.

Après confirmation de la demande de dissociation, la page **Integrations (Intégrations)** change pour fournir l'état de la ressource Cloud NGFW.

Palo Alto Networks vous recommande de supprimer les **définitions de surveillance** configurées sur Panorama.

L'option **Dissocier par la force** ne supprimera pas automatiquement les **définitions de surveillance** de Panorama.

Vous pouvez consulter les définitions de surveillance des locataires et supprimer leur exécution des commandes suivantes uniquement sur CLI :

```
request plugins dau plugin-name cloud_services unblock-device-push
 yes request plugins dau plugin-name cloudconnector unblock-device-
push yes request plugins dau plugin-name vm_series unblock-device-
push yes request plugins dau plugin-name aws unblock-device-push
 yes
```


Associer un Panorama lié à la ressource Cloud NGFW

Avant de pouvoir établir des liaisons entre plusieurs Panorama à un locataire Cloud NGFW, vous devez intégrer votre ressource Cloud NGFW à l'appareil virtuel Panorama. Vous devez d'abord préparer votre appareil Panorama à cette intégration en installant les plug-ins. Vous devrez ensuite utiliser la console Cloud NGFW pour la lier à votre appareil Panorama. Une fois que la liaison au Cloud NGFW est réussie, utilisez Panorama pour gérer les objets et les règles de sécurité et pour surveiller les journaux et l'analytique.

STEP 1 | Préparez votre Panorama.

STEP 2 | Liez votre Panorama.

Après avoir lié votre Panorama à votre ressource Cloud NGFW, vous pouvez l'associer à un autre locataire Cloud NGFW.

Établir des liaisons entre plusieurs Panorama à un locataire Cloud NGFW

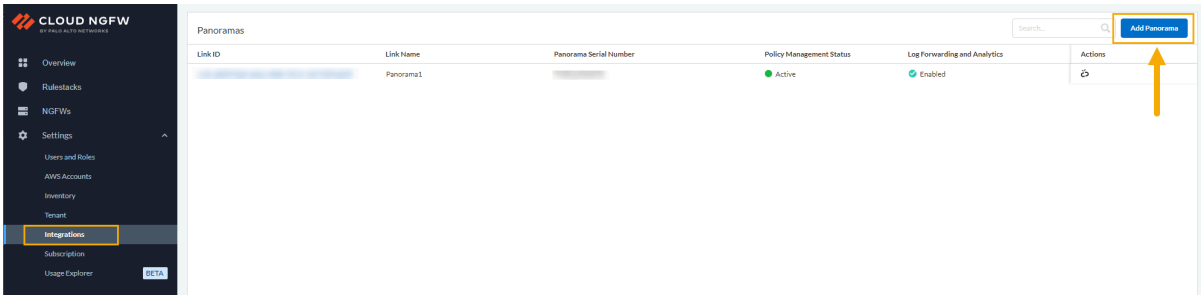
Pour établir des liaisons entre plusieurs Panorama au même locataire Cloud NGFW :

STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sélectionnez **Integrations (Intégrations)**.

La page **Integrations (Intégrations)** affiche des informations sur le Panorama actuellement lié. Si aucun Panorama n'est actuellement lié à un locataire Cloud NGFW, cette page est vide.

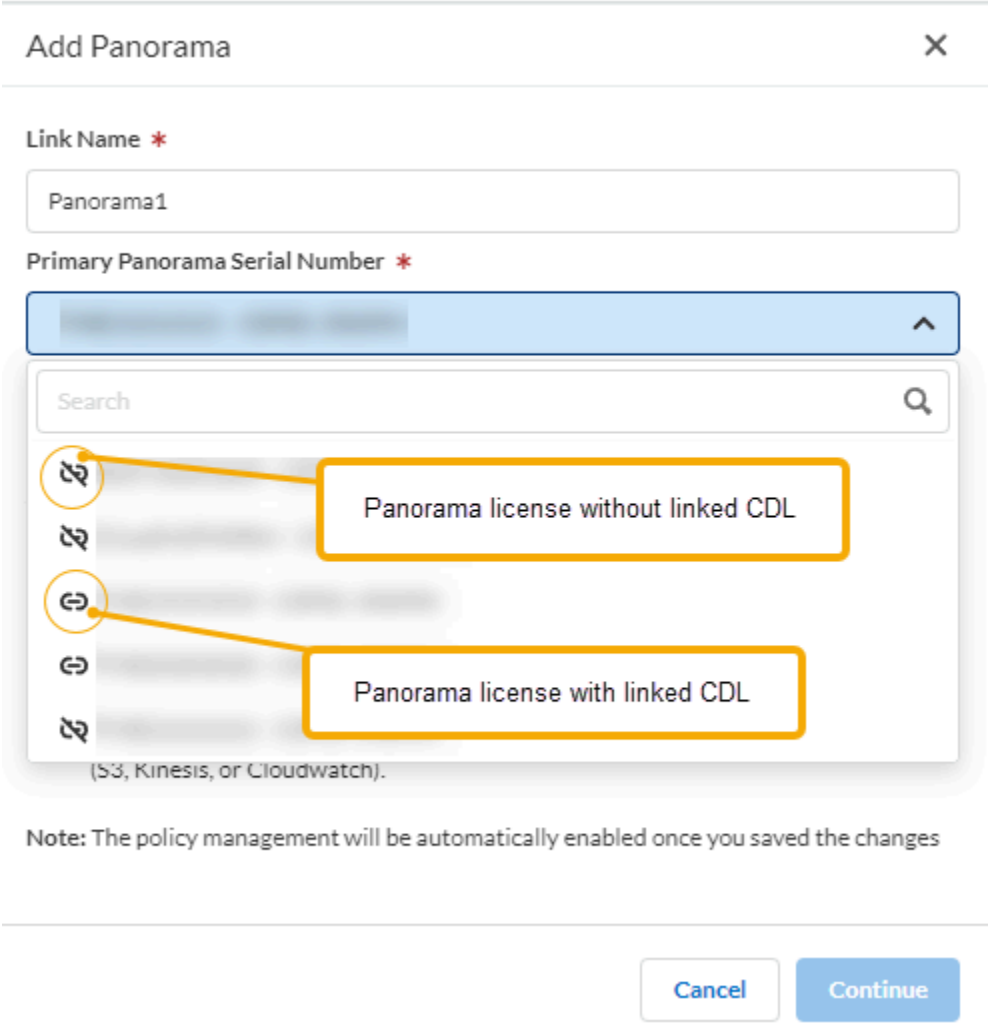
STEP 3 | Utilisez la page **Integrations (Intégrations)** pour ajouter un Panorama supplémentaire. Cliquez sur **Add Panorama (Ajouter un Panorama)**.



STEP 4 | Dans l'écran **Add Panorama (Ajouter un Panorama)**, saisissez un **Link Name (Nom de lien)**. Sélectionnez un Panorama actuellement lié dans la liste déroulante **Primary Panorama Serial Number (Numéro de série du Panorama principal)**. Pour les environnements HA, sélectionnez le

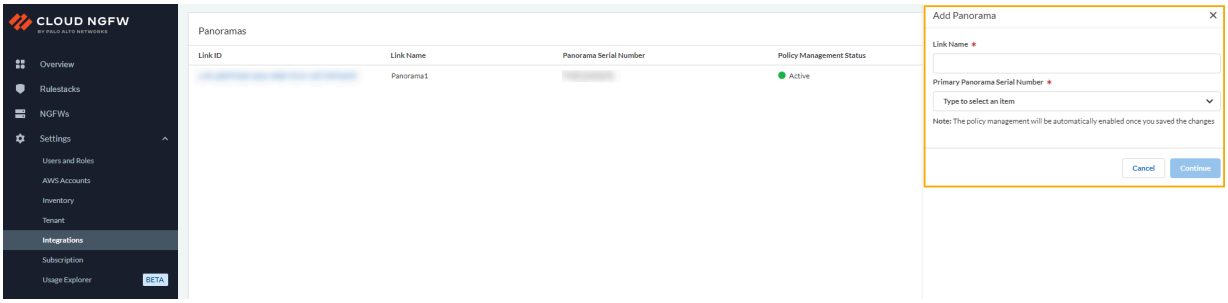
Secondary Panorama Serial Number (Numéro de série du Panorama secondaire) dans la liste déroulante.

Cet écran affiche deux icônes différentes décrivant l'état de la licence Panorama ; un Panorama lié à CDL et un Panorama non lié à CDL. Ces icônes sont illustrées dans l'image ci-dessous :

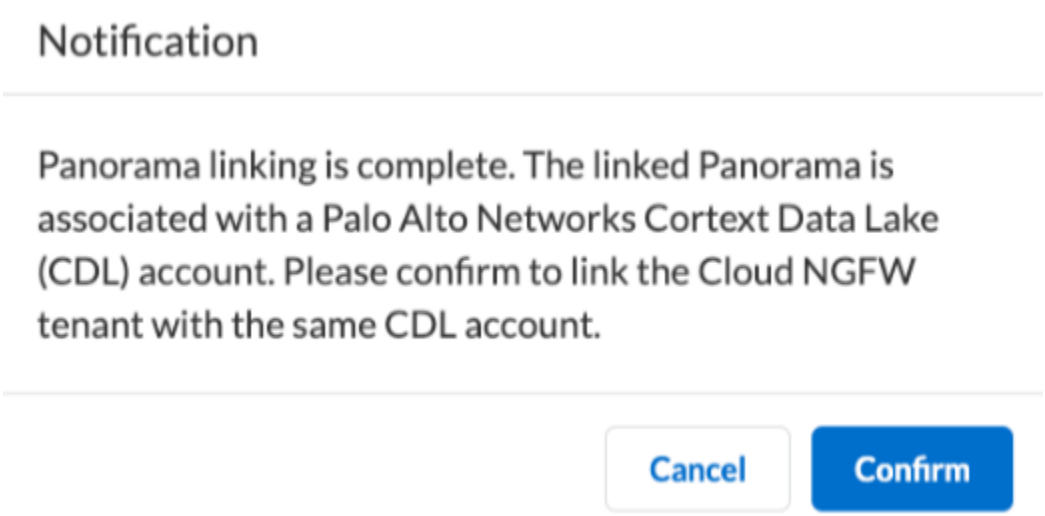


Si vous sélectionnez un numéro de série Panorama qui n'est pas lié à CDL, vous devez spécifier une option, soit pour annuler le processus de liaison, auquel cas vous acceptez d'acquérir une licence

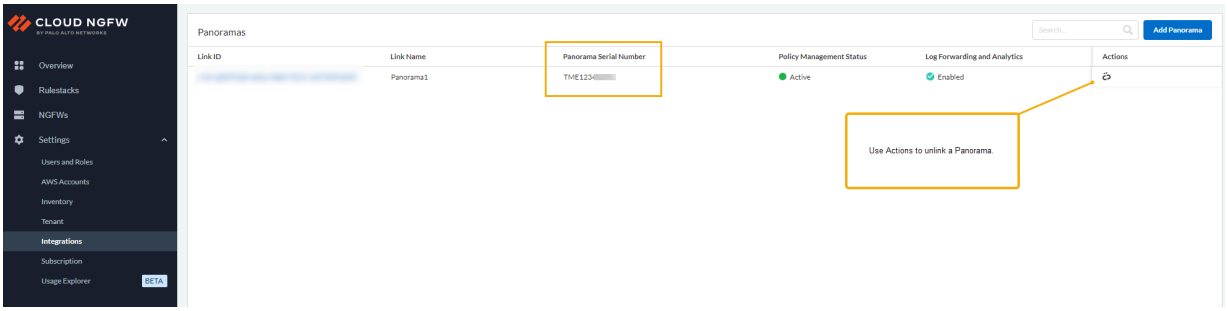
CDL et de l’associer à votre appareil Panorama, soit vous acceptez de continuer à utiliser Panorama uniquement pour la gestion des politiques :



Si vous sélectionnez une licence Panorama déjà connectée à un CDL, vous êtes invité à **Confirm (Confirmer)** l’association avant de poursuivre le processus d’intégration :



STEP 5 | Après avoir sélectionné la licence Panorama, cliquez sur **Continue (Continuer)**. La page **Integrations (Intégrations)** change pour afficher le **Link ID (ID de lien)** et le **Panorama Serial Number (Numéro de série Panorama)** lié :



STEP 6 | Après avoir ajouté un Panorama supplémentaire à votre Cloud NGFW, cliquez sur **NGFWs (les NGFW)** et sélectionnez le pare-feu que vous souhaitez associer à Panorama.

STEP 7 | Sélectionnez l'onglet **Firewall Settings (Paramètres du pare-feu)**.

STEP 8 | Faites défiler jusqu'à la section **Policy Management (Gestion des politiques)**. Sélectionnez **Panorama**.

STEP 9 | Utilisez le menu déroulant pour sélectionner **Linked Panorama (Panorama lié)** que vous souhaitez associer au pare-feu.

STEP 10 | Cliquez sur **Save (Enregistrer)**.

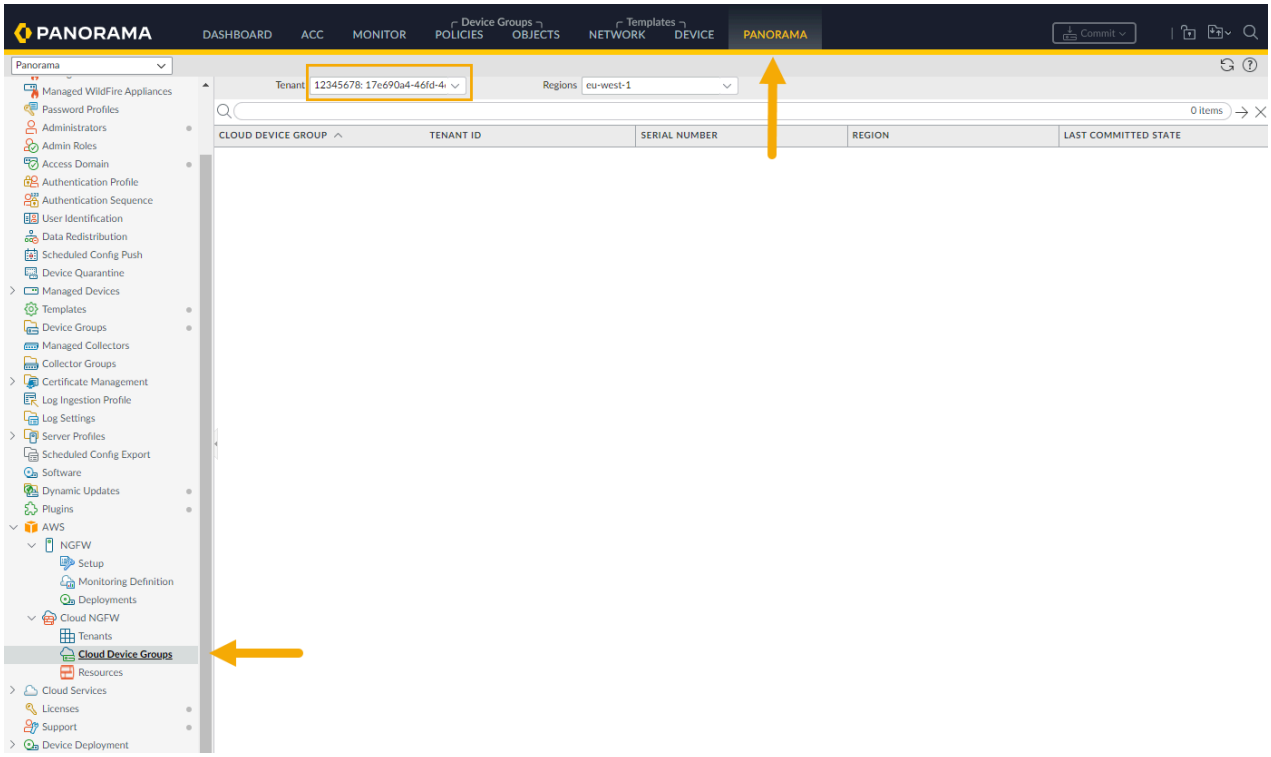
STEP 11 | Répétez les étapes 6 à 10 pour inclure un autre Panorama à la ressource.

Utiliser Panorama pour la gestion des politiques Cloud NGFW

Après avoir lié votre locataire 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 politiques au groupe d'appareils du locataire Cloud NGFW à l'aide de la console Panorama.

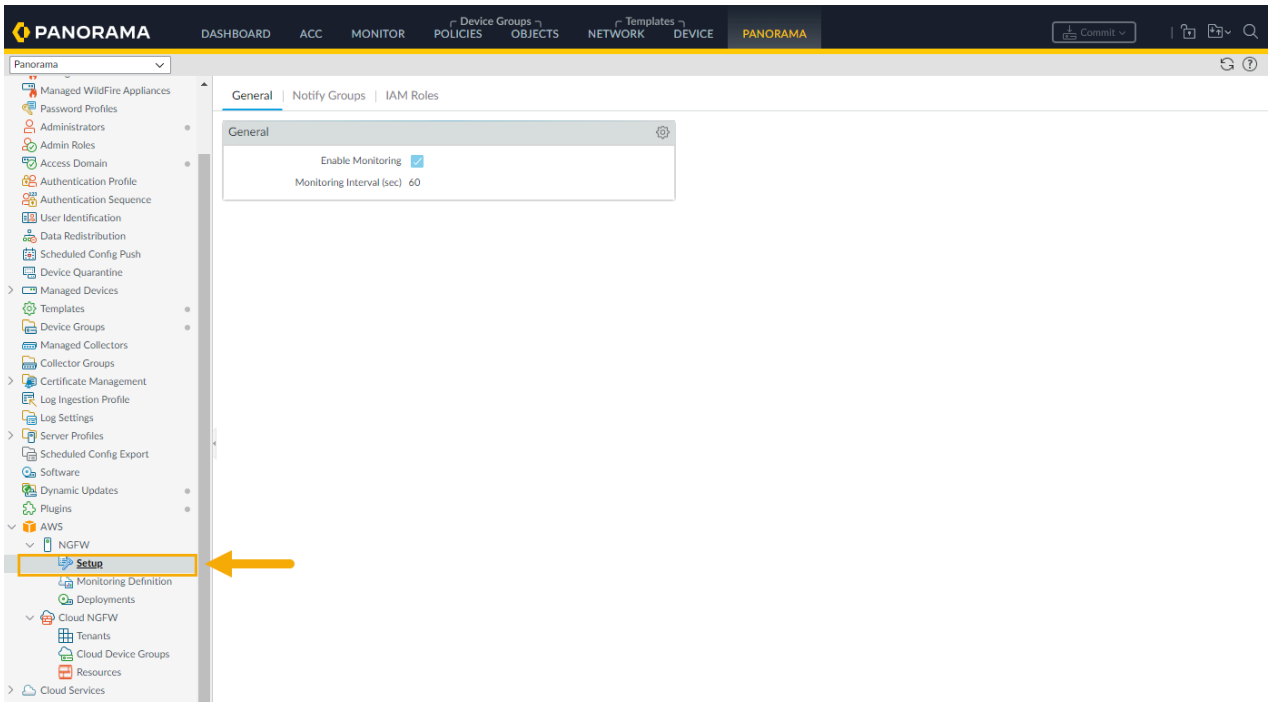
Lorsque vous utilisez la console Panorama pour configurer le Cloud NGFW, le navigateur met en cache les informations locales, telles que le groupe d'appareils Cloud, la pile de modèles et la région, de sorte que lorsque vous basculez entre les tâches Panorama, les informations Cloud NGFW en cache sont affichées dans la console Panorama.

Lorsque vous sélectionnez un locataire à partir du nœud **Cloud Device Groups (Groupes d'appareils Cloud)** et accédez à une autre option de configuration dans Panorama, le retour au nœud **Resources (Ressources)** conserve la vue du locataire que vous avez précédemment sélectionnée. Par exemple, la sélection d'un seul locataire dans une région affiche les groupes d'appareils cloud configurés pour ce locataire.

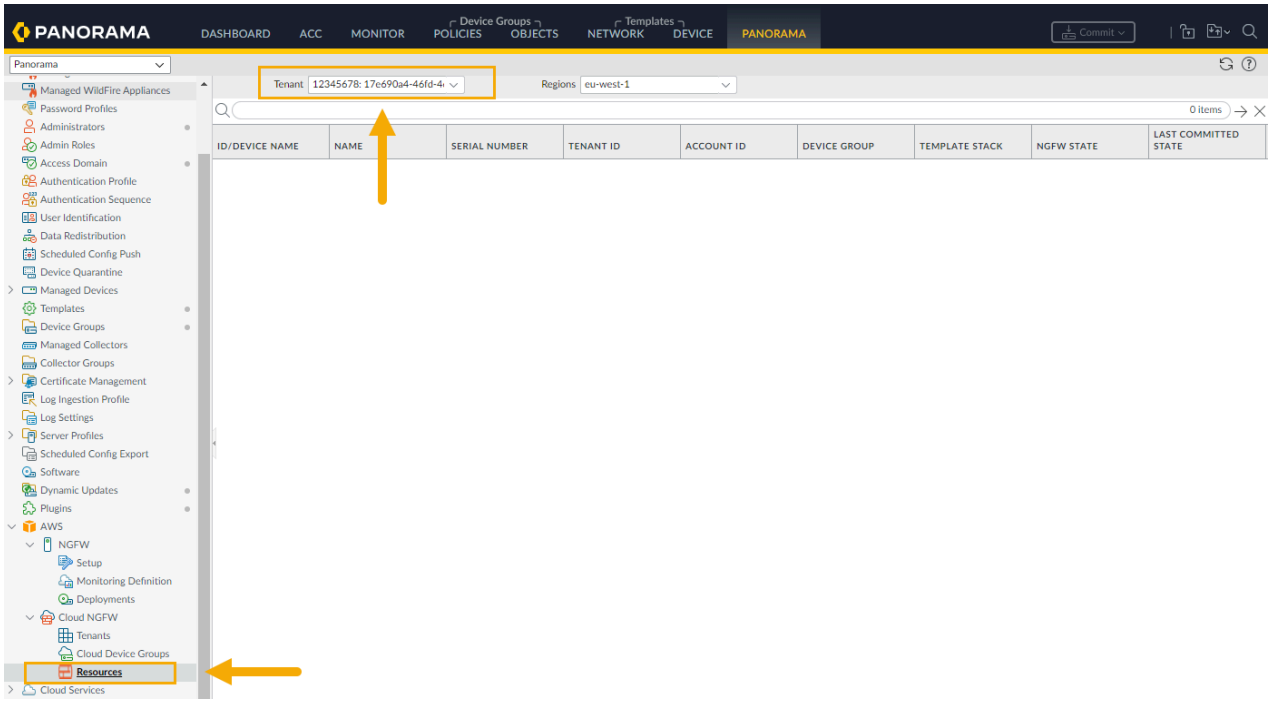


Lorsque vous accédez à une autre zone de la console Panorama, puis revenez à **Cloud NGFW > Groupes d’appareils Cloud**, la console affiche le locataire unique que vous avez précédemment sélectionné. Par

exemple, après avoir affiché les groupes d'appareils cloud pour un locataire, sélectionnez **AWS > Setup (Configuration)**.



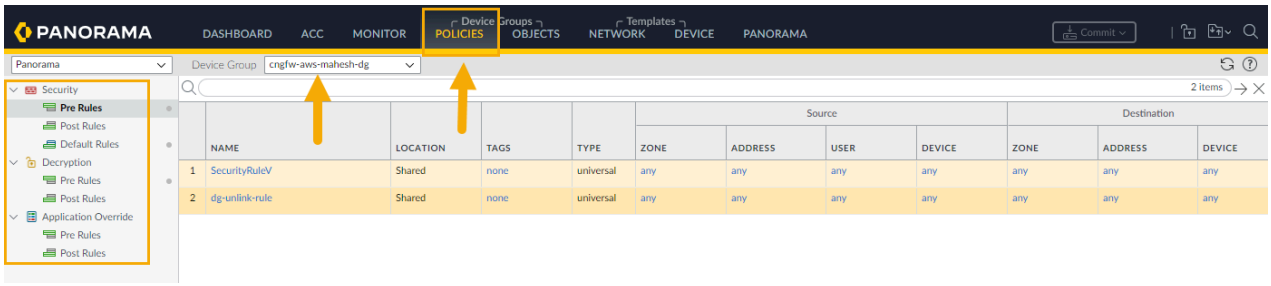
Lorsque vous revenez à l'écran **Cloud NGFW > Ressources**, la console Panorama se souvient du locataire précédemment sélectionné au lieu d'afficher tous les locataires associés à la ressource Cloud NGFW.



Actualisez le navigateur pour effectuer une mise à jour dynamique de l’affichage.

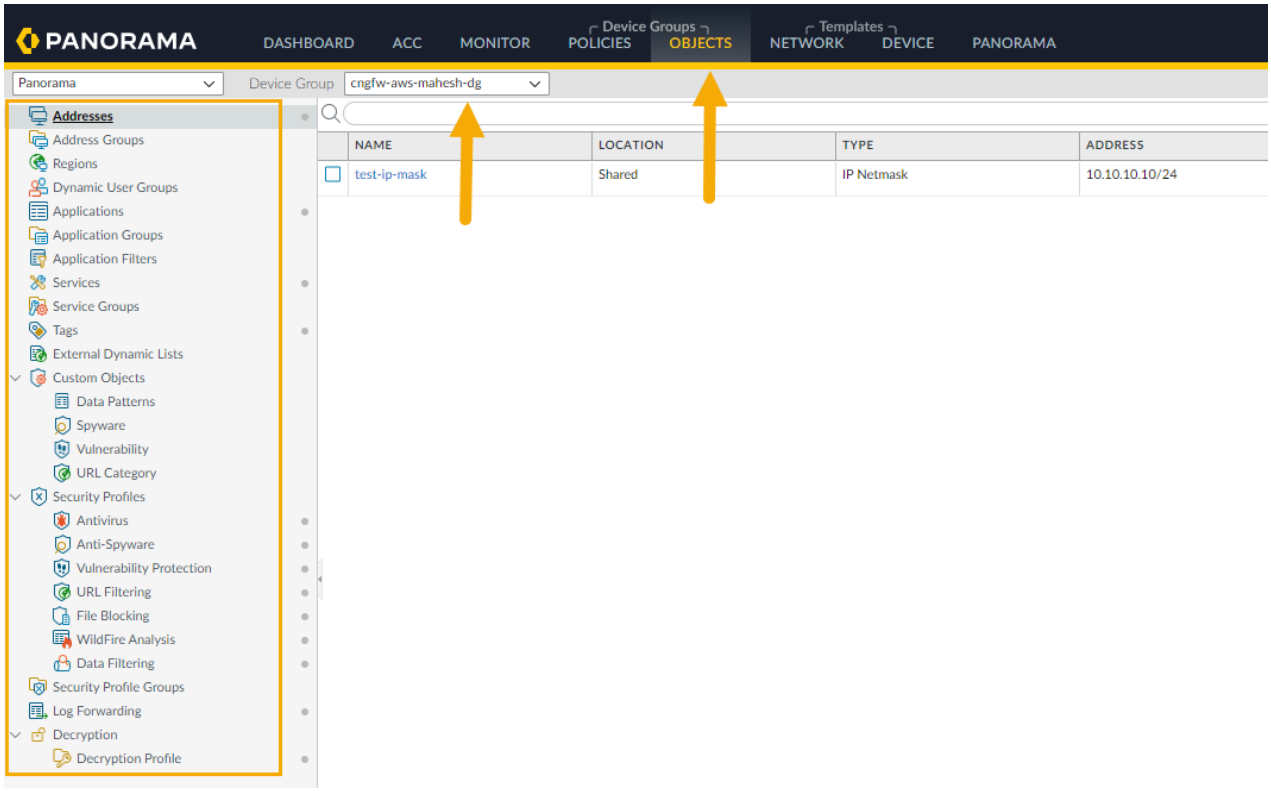
L’intégration Panorama affiche uniquement les options de configuration disponibles pour la ressource Cloud NGFW. Par exemple, pour afficher les options de politique disponibles pour la ressource Cloud

NGFW, sélectionnez **Policies (Politiques)**. La console Panorama n’affiche que les politiques disponibles pour le groupe d’appareils cloud du Cloud NGFW.

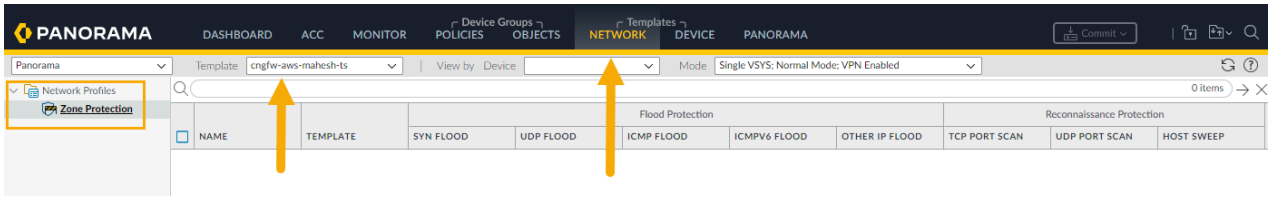


Le nom du groupe d’appareils est doté du préfixe `cngfw-aws`.

Pour afficher les objets du groupe d’appareils pris en charge par la ressource Cloud NGFW, sélectionnez **Objects (Objets)**. Seuls les objets pris en charge par Cloud NGFW s’affichent sur la console Panorama.



Pour afficher des modèles pris en charge par la ressource Cloud NGFW, sélectionnez **Network (Réseau)**. Seuls les modèles cloud pris en charge par le Cloud NGFW s’affichent.



Considérations relatives aux rulestacks

Lorsque vous approvisionnez une ressource Cloud NGFW avec une rulestack locale, vous ne pouvez pas l'associer à un groupe d'appareils cloud dans Panorama ; le pare-feu apparaît grisé dans la console Panorama. Pour résoudre ce problème, vous pouvez dissocier la rulestack locale à l'aide de la console Cloud NGFW ou approvisionner une nouvelle ressource de pare-feu sans rulestack locale et l'associer à un groupe d'appareils cloud dans Panorama. Sinon, utilisez une rulestack globale.

Pour les pare-feu créés à l'aide du Service AWS Firewall Manager (FMS), la rulestack ne peut pas être désélectionnée dans la console Panorama. Sélectionnez une rulestack globale transmise à Panorama depuis la console FMS. Ce processus supprime la rulestack associée et actualise le pare-feu avec une rulestack globale transmise depuis Panorama. Pour plus d'informations, consultez la documentation d'AWS FMS.

Ajouter un groupe d'appareils Cloud

Panorama vous permet de regrouper 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.

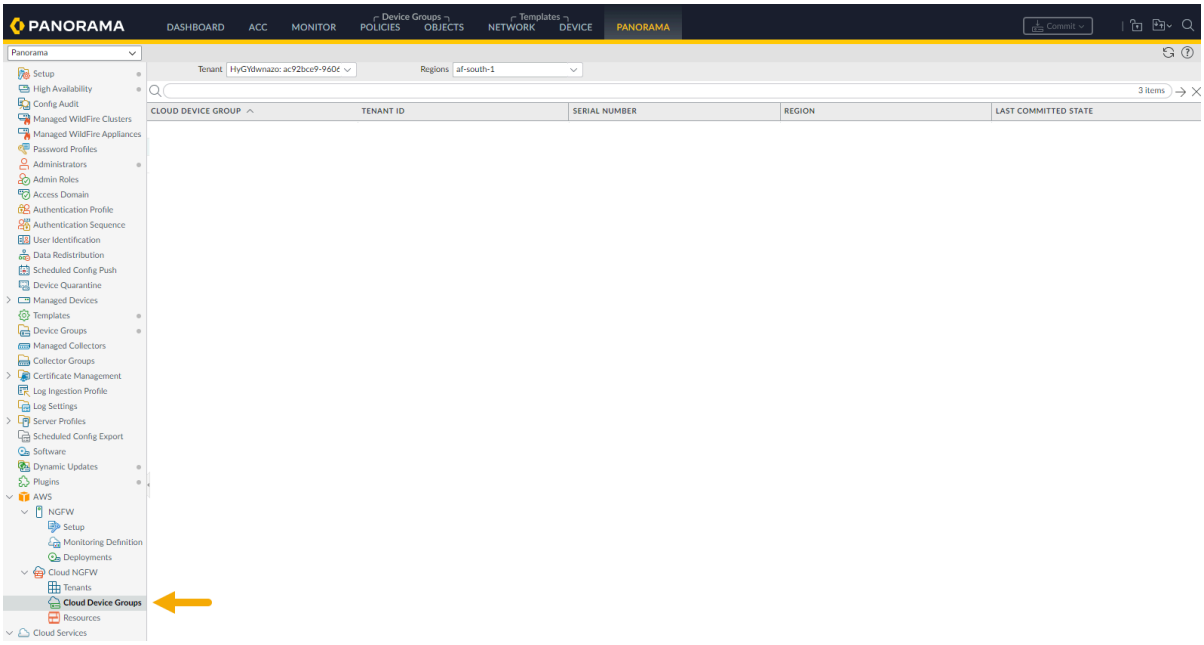
En utilisant des groupes de périphériques, vous pouvez configurer les règles de stratégie et les objets auxquels ils font référence. Vous pouvez organiser un groupe d'appareils hiérarchisé, avec des règles communes et des objets en haut, et des règles spécifiques au groupe d'appareils et des objets à 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 Manage Device Groups (Gérer les groupes d'appareils).

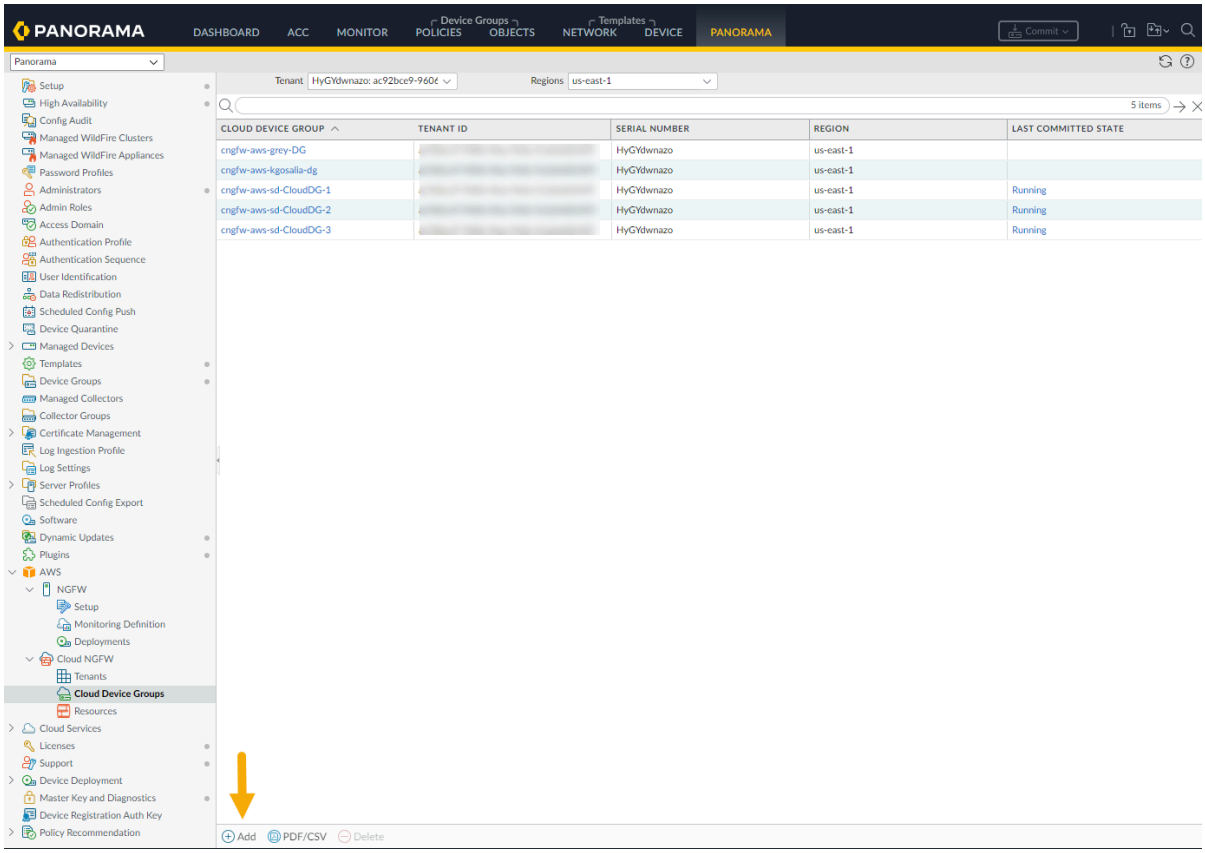
Pour ajouter un groupe d'appareils cloud à l'aide de la console Panorama :

STEP 1 | Dans le plug-in **AWS**, sélectionnez **Cloud Device Groups (Groupes d'appareils Cloud)**. La table Cloud Device Group (Groupe d'appareils Cloud) est vide lorsque vous la sélectionnez pour la

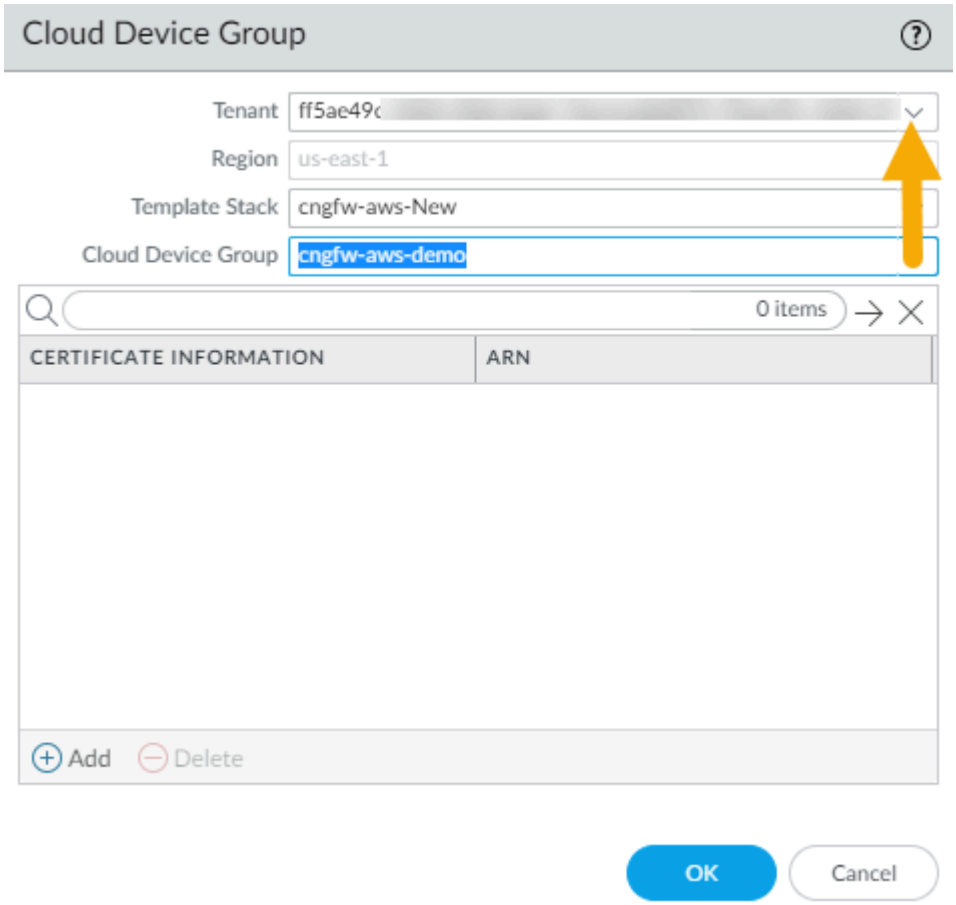
première fois. Les groupes d’appareils Cloud précédemment créés apparaissent s’ils ont été établis pour la ressource Cloud NGFW à l’aide d’AWS.



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



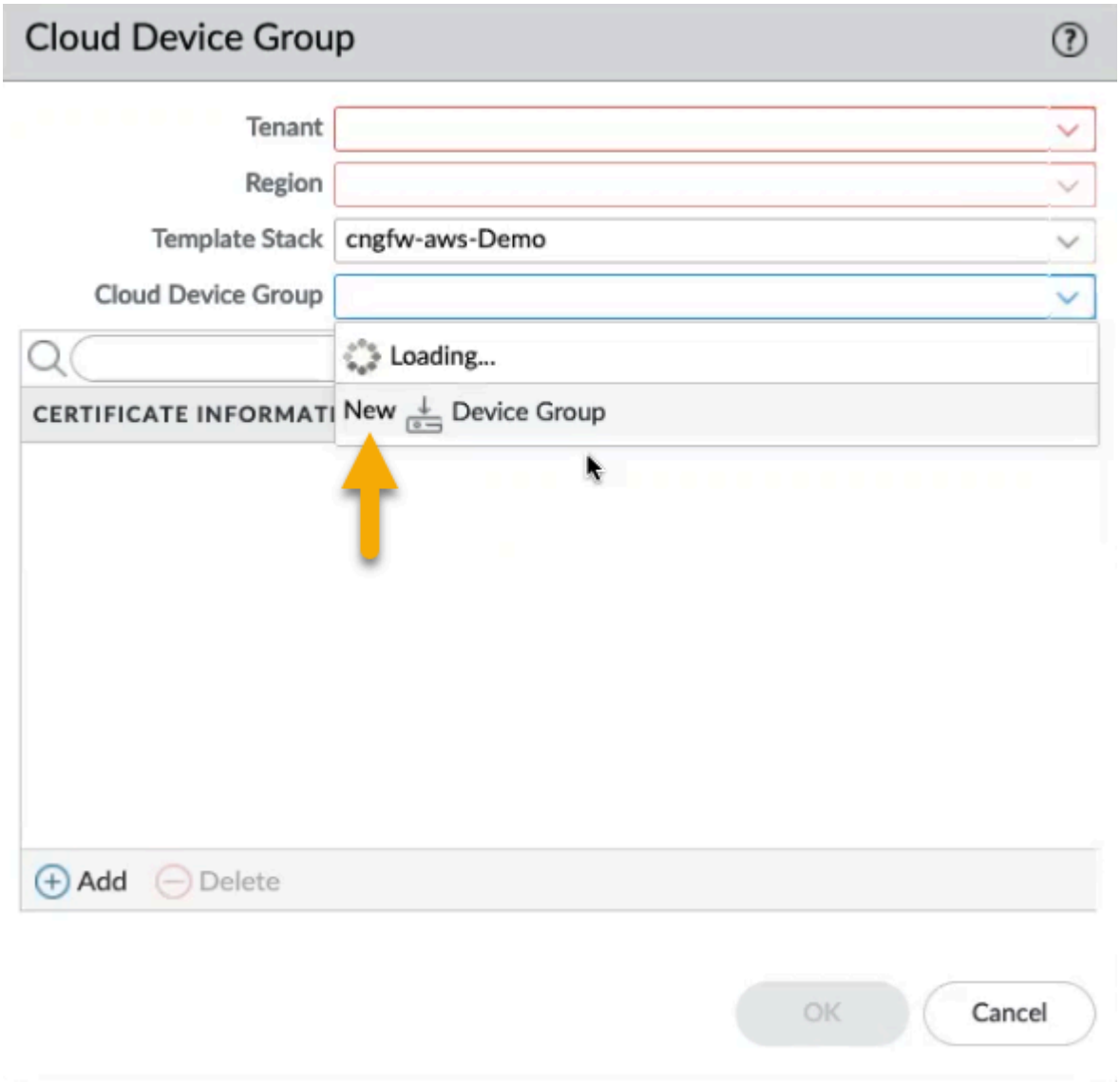
STEP 3 | Dans l'écran **Cloud Device Group (Groupe d'appareils Cloud)**, utilisez le menu déroulant pour sélectionner le **Tenant (Locataire)** que vous souhaitez utiliser.



La **Région** est automatiquement renseignée avec la région hébergeant le locataire.

STEP 4 | Créez une nouvelle **Template Stack (Pile de modèles)** ou utilisez le menu déroulant pour sélectionner une pile de modèles existante.

STEP 5 | Sélectionnez le menu déroulant **Cloud Device Group (Groupe d’appareils Cloud)** et cliquez sur **New (Nouveau)** :



STEP 6 | Saisissez un **Device Group Name (Nom de groupe d’appareils)** pour le groupe d’appareils, puis cliquez sur **Create (Créer)**.

STEP 7 | Cliquez sur **OK** pour appliquer le groupe d’appareils cloud au locataire.

STEP 8 | Vous pouvez associer un certificat natif Panorama, ou spécifier un mappage ARN. Après avoir ajouté un certificat au Cloud NGFW pour AWS, saisissez le nom du certificat, sinon spécifiez le mappage ARN.

STEP 9 | Validez la modification.

Supprimer un groupe d’appareils Cloud d’une ressource

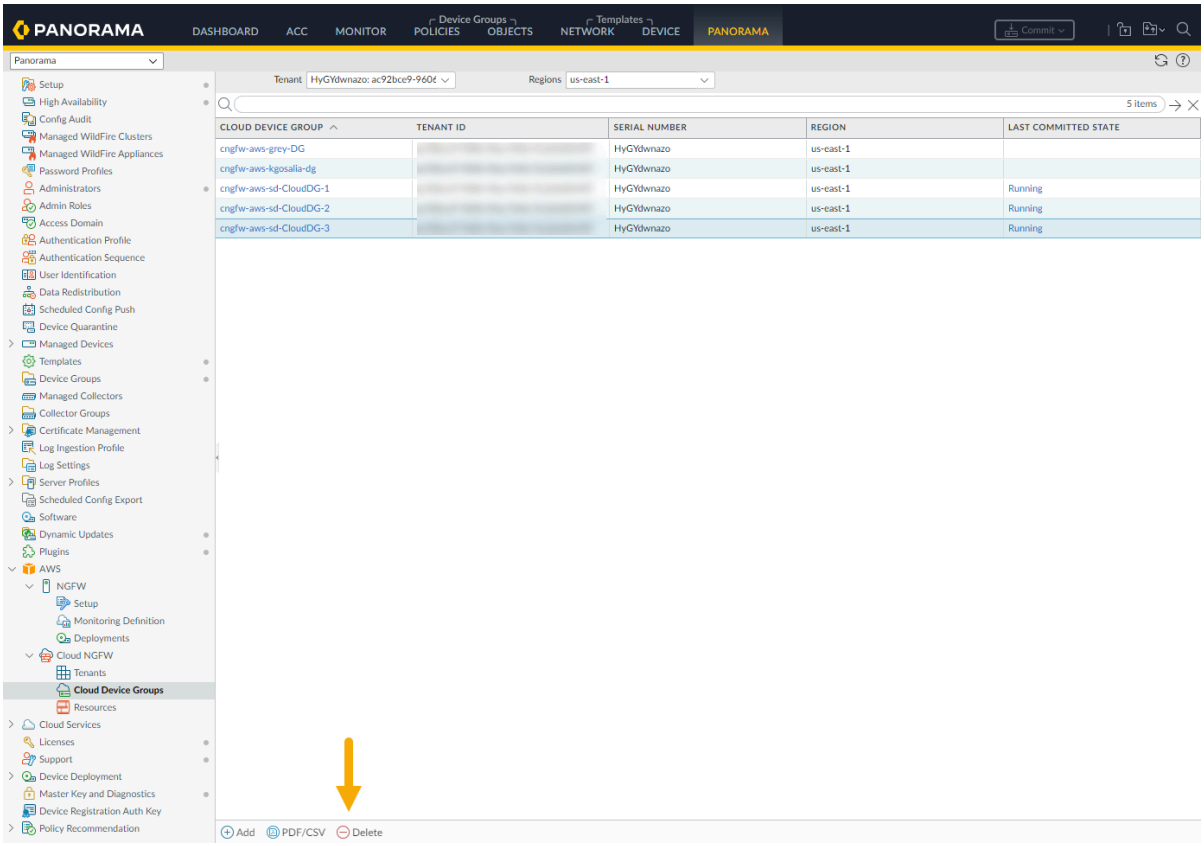
Utilisez la console Panorama pour supprimer un groupe d’appareils Cloud. Vous ne pouvez supprimer un groupe d’appareils Cloud que s’il n’est pas associé à un pare-feu.

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

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

STEP 2 | Sélectionnez le **Cloud Device Group (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.

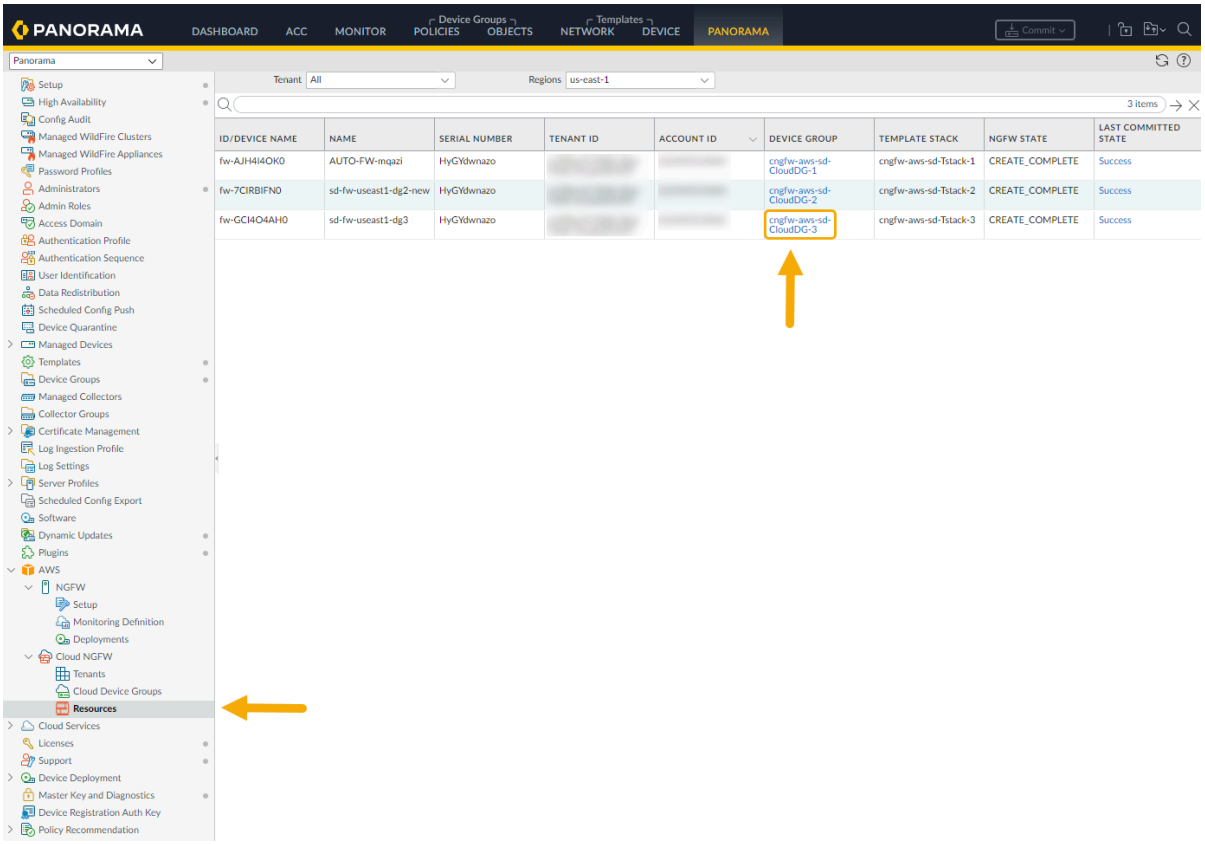
Associer un groupe d’appareils Cloud à une ressource

Utilisez la console Panorama pour associer un groupe d’appareils Cloud à une ressource Cloud NGFW. Vous pouvez transmettre un groupe d’appareils cloud sans l’associer à une ressource. Cependant, vous devrez l’associer si vous souhaitez que la ressource utilise la configuration du groupe d’appareils cloud

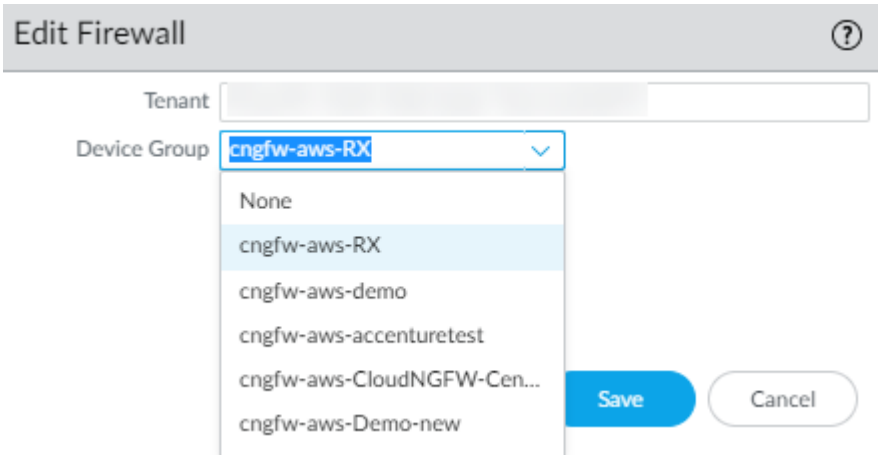
Pour associer un groupe d’appareils cloud à une ressource Cloud NGFW à l’aide de la console Panorama :

STEP 1 | Dans **Panorama**, sélectionnez **Resources (Ressources)**.

STEP 2 | Sélectionnez le **Device group (Groupe d’appareils)**.



STEP 3 | Dans l'écran **Edit Firewall (Modifier le pare-feu)**, utilisez le menu déroulant pour sélectionner le groupe d'appareils cloud que vous souhaitez associer à la ressource Cloud NGFW.



STEP 4 | Cliquez sur **Save (Enregistrer)**.

STEP 5 | **Commit (Validez)** les modifications.

STEP 6 | **Transmettez** la modification à votre appareil.

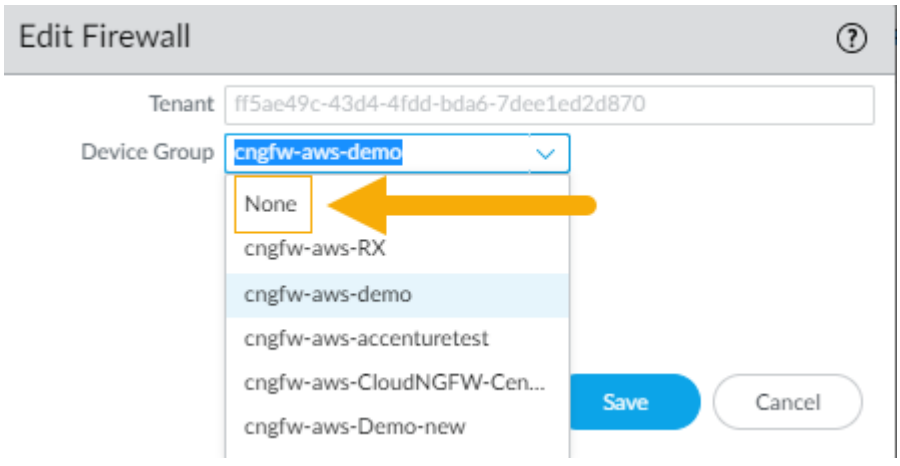
Dissocier un groupe d'appareils Cloud d'une ressource

Pour dissocier un groupe d'appareils cloud d'une ressource Cloud NGFW à l'aide de la console Panorama :

STEP 1 | Dans **Panorama**, sélectionnez **Resources (Ressources)**.

STEP 2 | Sélectionnez le **Device group (Groupe d'appareils)** de la ressource NGFW.

STEP 3 | Dans l'écran **Edit Firewall (Modifier le pare-feu)**, sélectionnez **None (Aucun)** dans la liste déroulante **Device group (Groupe d'appareils)**. Cliquez sur **Save (Enregistrer)**.



Appliquer la politique

Les groupes d'appareils Cloud sur Panorama vous permettent de gérer les règles de pare-feu de manière centralisée. Vous pouvez créer les politiques sur Panorama en tant que Règles avant ou que Règles après ; les Règles avant et les Règles après vous permettent de créer une approche progressive de la mise en œuvre

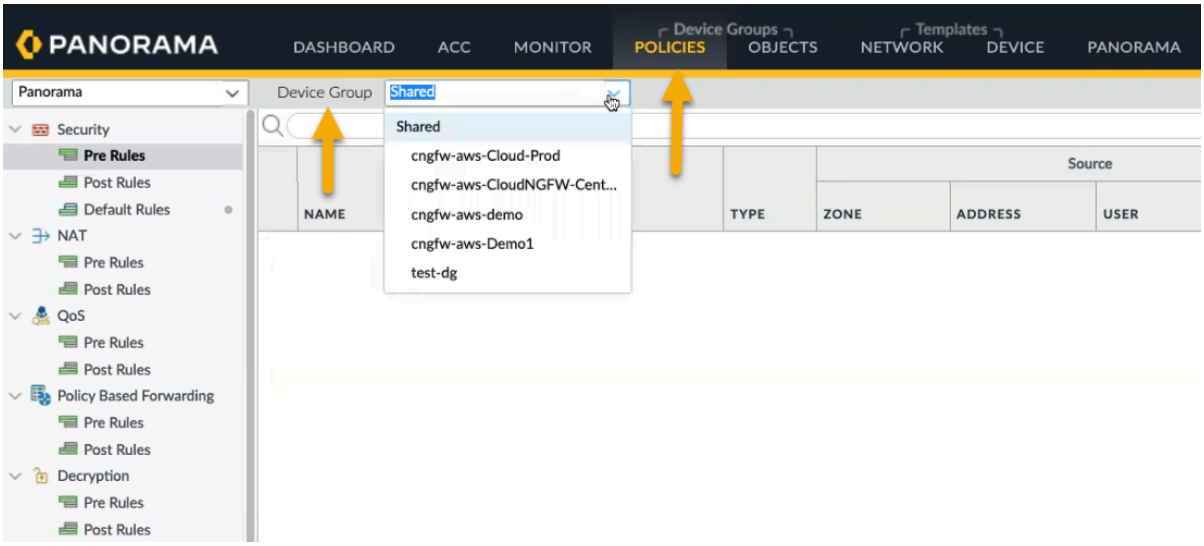
des politiques. Pour plus d'informations, consultez la section Defining Policies on Panorama (Définition des politiques sur Panorama).

Une politique créée sur Panorama crée une rulestack mondiale. Un pare-feu ne peut pas avoir de règles générées sur Panorama et de règles générées sur le locataire. Les règles doivent être créées soit dans Cloud NGFW soit dans Panorama.

Pour configurer les politiques du groupe d'appareils cloud dans Panorama :

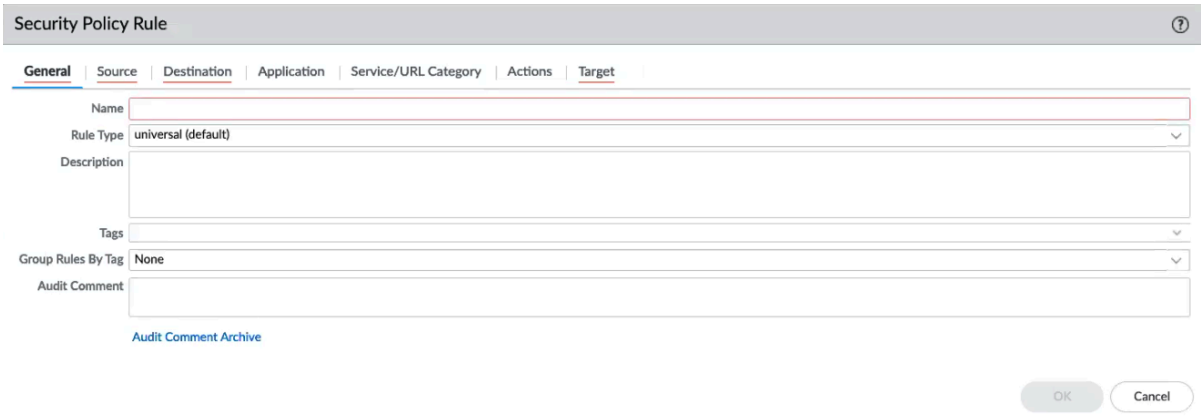
STEP 1 | Sélectionnez **Policies (Politiques)**.

STEP 2 | Dans la section **Device Group (Groupe d'appareils)**, utilisez le menu déroulant pour sélectionner le **Cloud Device Group (Groupe d'appareils Cloud)** précédemment créé. Lorsque vous créez un groupe d'appareils pour Cloud NGFW, le nom commence par *cngfw*. Par exemple, *cngfw-aws-demo*.



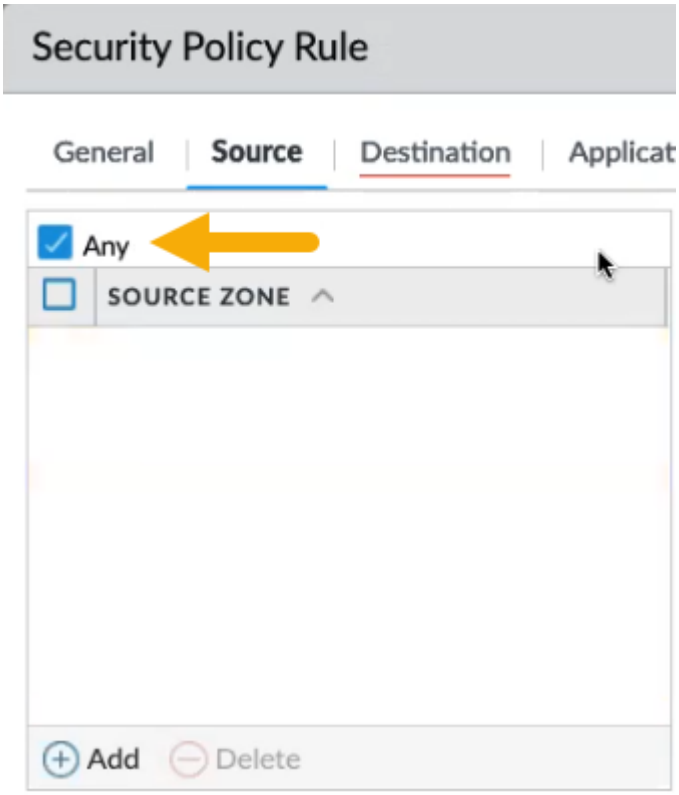
STEP 3 | Dans la partie inférieure gauche de la console, cliquez sur **Add (Ajouter)**.

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.

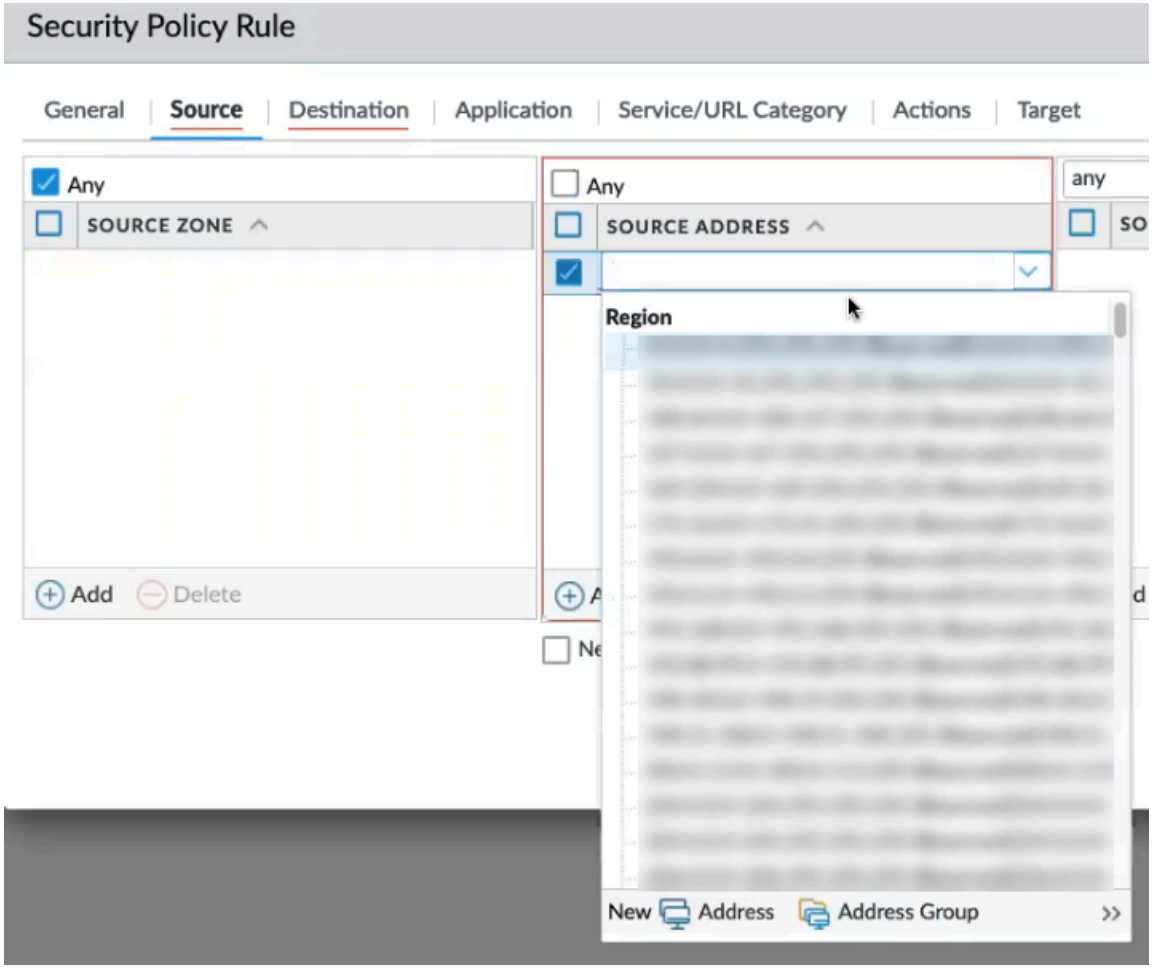


STEP 5 | Dans l’onglet **General (Général)**, saisissez un **nom** pour la politique.

STEP 6 | Configurer une politique **source**. La politique **source** définit la zone source ou l'adresse source qui génère le trafic. Pour **Source Zone (Zone source)**, cliquez sur **Any (Tout)**. Vous ne pouvez pas ajouter une adresse source spécifique.



1. Continuez à appliquer les politiques **Source** en incluant l'adresse **Source**. Cliquez sur **Any (Tout)**, ou utilisez le menu déroulant pour sélectionner une adresse existante, ou utilisez les options pour ajouter une nouvelle adresse ou un nouveau groupe d'adresses.

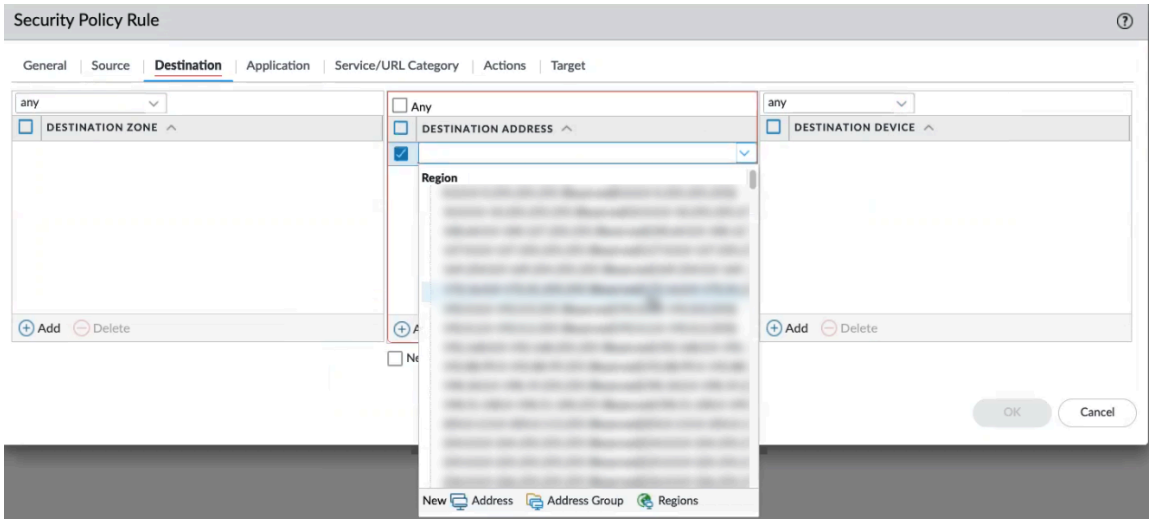


2. Pour la politique**Source User (Utilisateur source)** et **Source Device (Périphérique source)**, cliquez sur **Any (Tout)**. Cloud NGFW ne prend pas en charge la spécification d'utilisateurs ou de périphériques source spécifiques

STEP 7 | La politique de **destination** définit la zone de destination ou l'adresse de destination du trafic. Utilisez le menu déroulant pour sélectionner une adresse existante ou utilisez des options pour ajouter une nouvelle adresse ou un nouveau groupe d'adresses. La politique de Destination comprend des champs pour la zone, l'adresse et le périphérique.

1. Pour la **Destination Zone (Zone de destination)**, cliquez sur **Any (Tout)**. Cloud NGFW ne prend pas en charge l'ajout de zones de destination individuelles.
2. Pour la **Destination Address (Adresse de destination)**, cliquez sur **Any (Tout)**ou utilisez la liste déroulante pour sélectionner une zone existante. Cliquez sur **New (Nouveau)** pour ajouter une nouvelle adresse, un nouveau groupe d'adresses ou une nouvelle région.

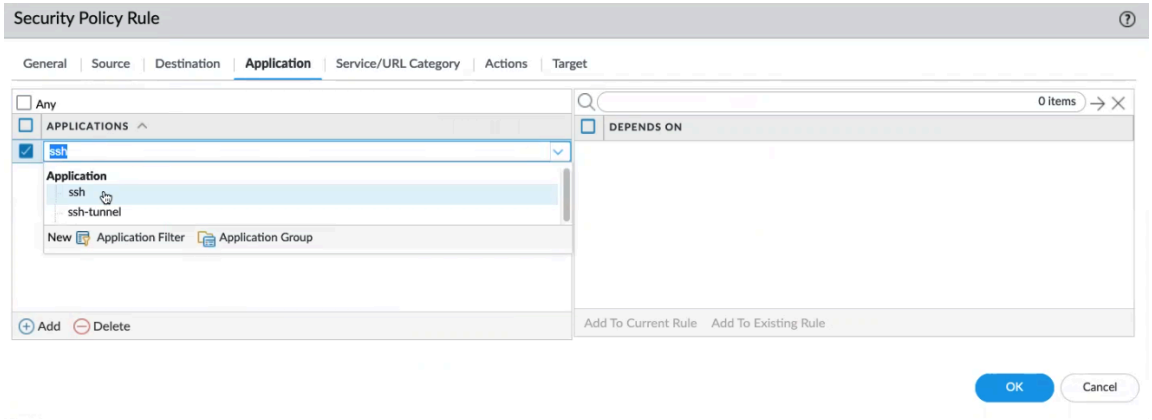
3. Pour le **Destination Device (Périphérique de destination)**, cliques sur **Any (Tout)**. Cloud NGFW ne prend pas en charge l'ajout de périphériques de destination individuels.



STEP 8 | Configurez la 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

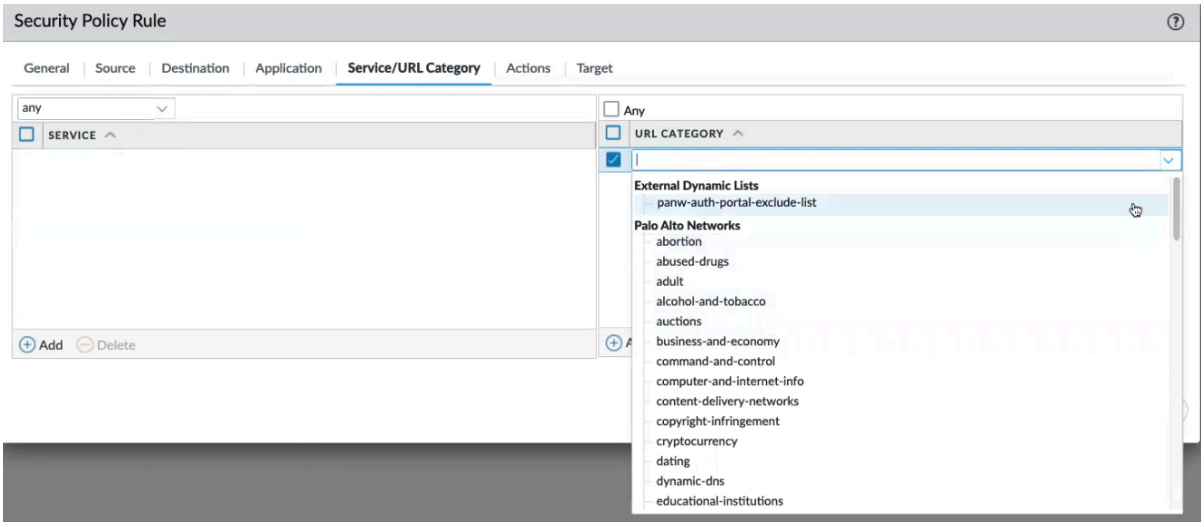
attributs d’une application existante. Les applications propres à l’entreprise sont définies dans **ObjectsApplications (Applications d’objets)**.

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



STEP 9 | Configurez des politiques **Service/URL Category (Catégorie de service/URL)** permettant au pare-feu d’indiquer un numéro de port TCP et/ou UDP spécifique ou une catégorie d’URL comme critères de correspondance dans la politique. Indiquez des politiques de niveau **Service** ou des politiques **URL Category (Catégorie d’URL)** en sélectionnant **Any (Tout)**,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 politiques pour le service ou la catégorie des URL.



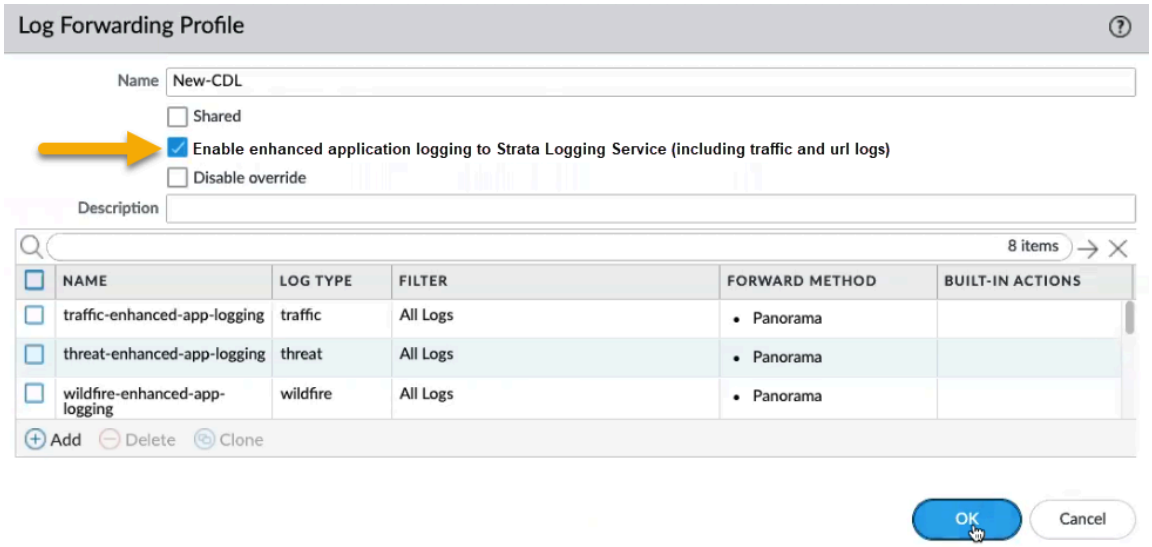
STEP 10 | Configurez une politique **Actions** pour déterminer l'action effectuée en fonction du trafic correspondant aux attributs de politique définis.

1. Dans l'écran **Actions**, sélectionnez l'action à effectuer (par exemple, autoriser ou refuser), déterminez le **Profile Setting (Paramètre de profil)**, configurez le **Log Setting (Paramètre de journal)** et d'autres paramètres.

   Pour plus d'informations sur l'utilisation des journaux Panorama, consultez la section Centralized Logging and Reporting (Journalisation et rapports centralisés) et View logs (Afficher les journaux)

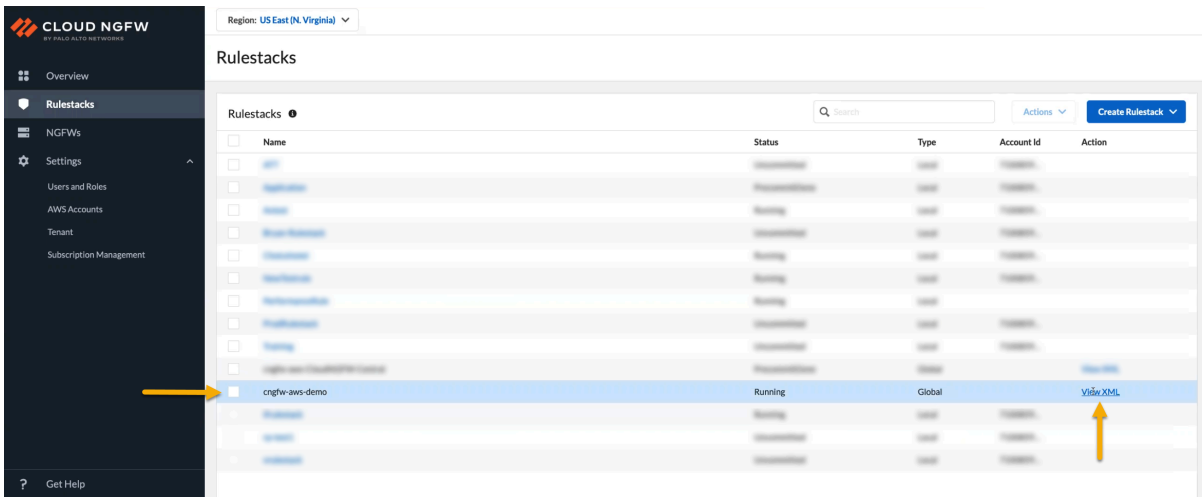
2. Vous pouvez également transférer les journaux au service de journalisation Strata depuis l'écran **Security Policy Rule (Règle de politique de sécurité)**. Dans le champ **Log Setting (Paramètre des journaux)**, sélectionnez la liste déroulante **Log Forwarding (Transfert des journaux)** et cliquez sur **New Profile (Nouveau profil).** Dans le profil de transfert des journaux, saisissez un **nom** pour le journal et sélectionnez **Activer la journalisation améliorée des applications vers**

le service de journalisation Strata (y compris les journaux du trafic et des url).Cliquez sur **OK**.

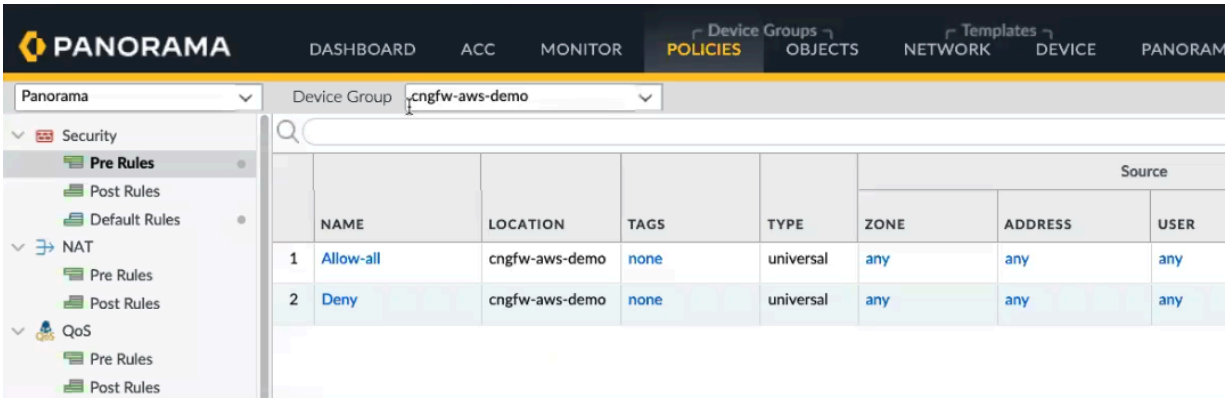


Pour plus d’informations sur le service de journalisation Strata, consultez la section Explore Logs (Explorer les journaux).

STEP 11 | Retournez à la console Cloud NGFW pour afficher les règles créées dans Panorama. Cliquez sur **View XML (Afficher XML)** pour afficher des informations sur les règles transférées de Panorama vers la rulestack globale appliquée au groupe d'appareils cloud :

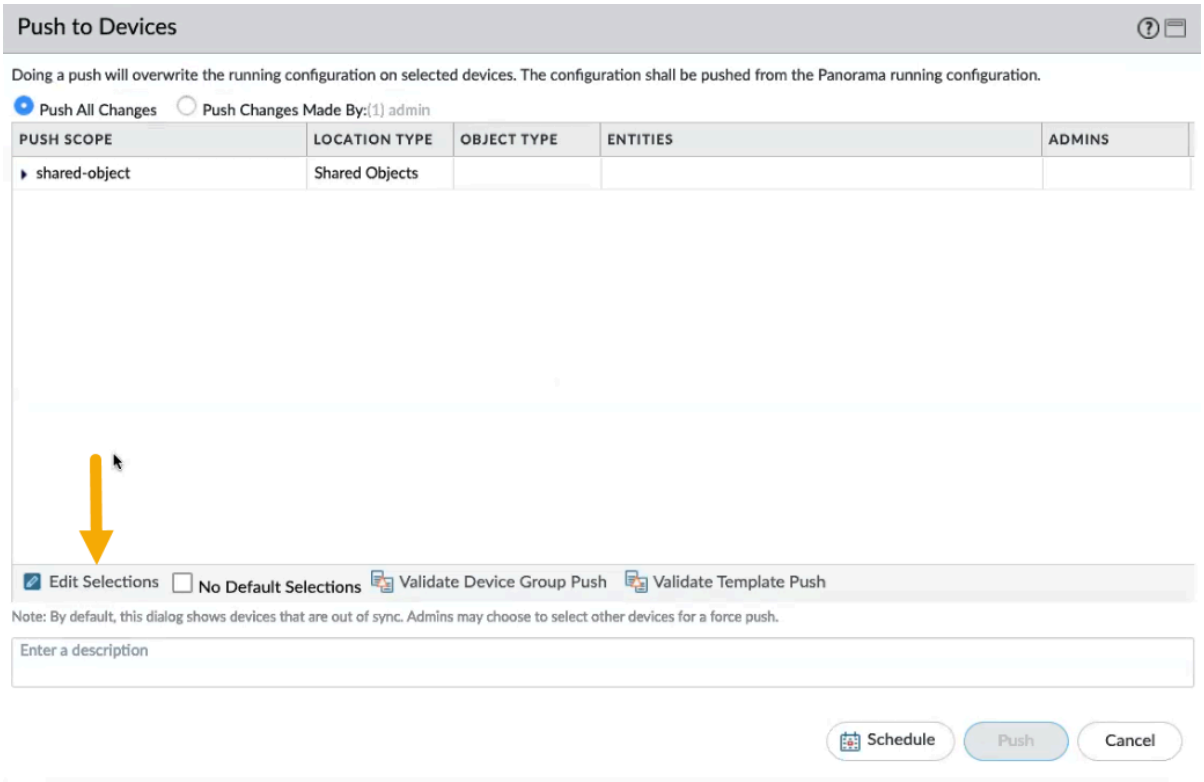


La rulestack est désormais associée aux politiques appliquées au groupe d’appareils Cloud créé dans Panorama :

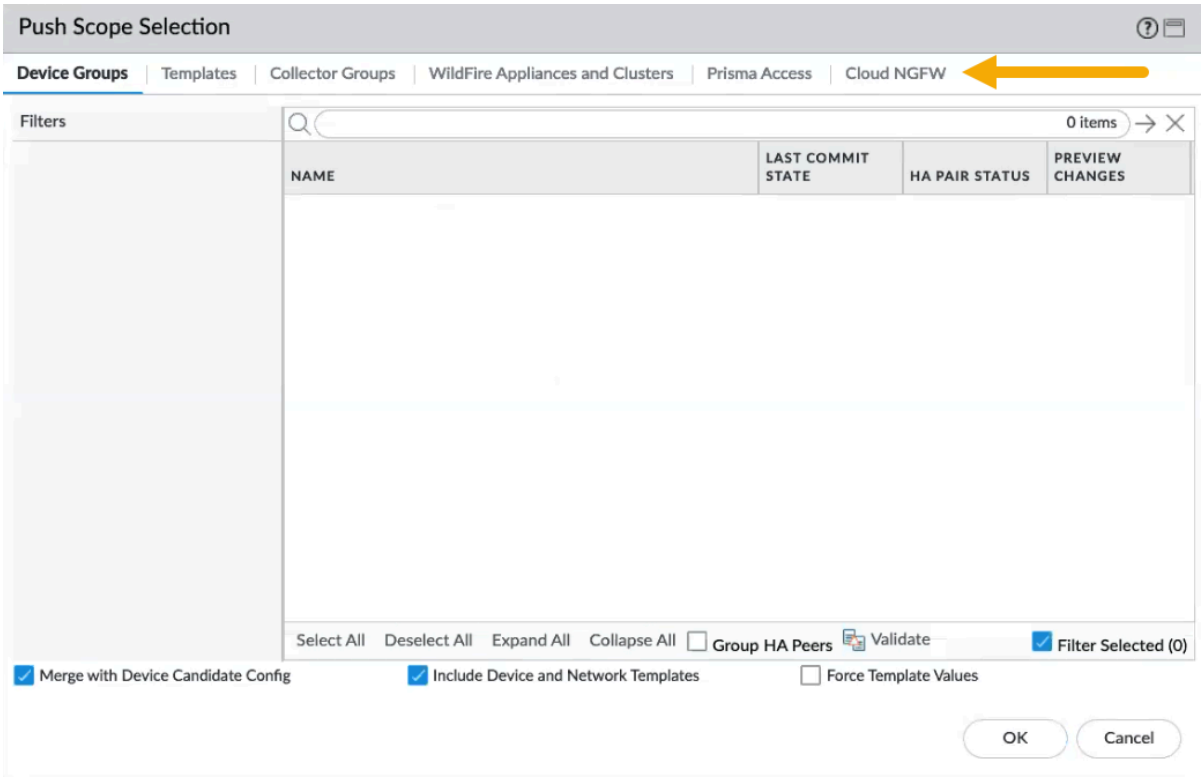


STEP 12 | Après avoir appliqué des politiques au groupe d’appareils cloud pour le locataire Cloud NGFW, transmettez les modifications à la console Panorama.

STEP 13 | Dans l'écran **Push to Devices (Transmettre aux appareils)**, cliquez sur **Edit Selections (Modifier les sélections)**.



STEP 14 | Dans l'écran de **Push Scope Selection (Transmettre la sélection de l'étendue)**, cliquez sur **Cloud NGFW**. Le nœud **Cloud NGFW** a été ajouté à l'écran **Push Scope Selection (Transmettre la sélection de l'étendue)** pour faciliter l'intégration Cloud NGFW et Panorama.



STEP 15 | Sélectionnez les groupes d'appareils Cloud que vous souhaitez transmettre aux ressources, puis cliquez sur **OK** et sur **Push (Transmettre)**.

Utiliser un groupe d'appareils transmis depuis Panorama

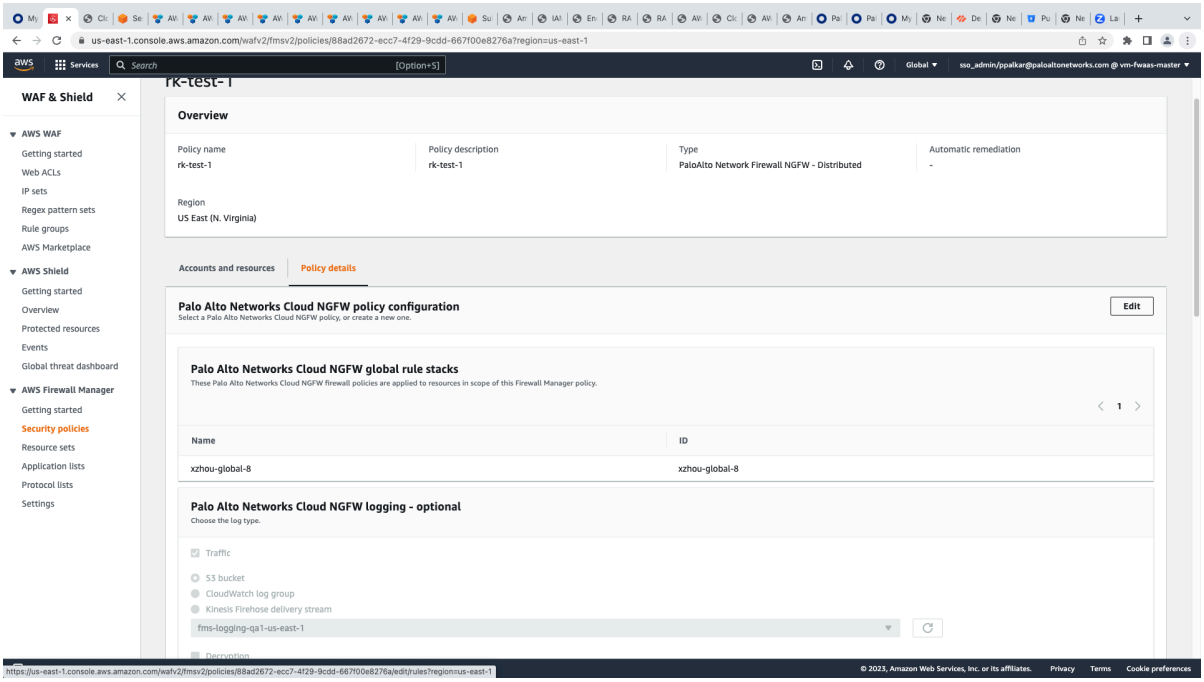
Les informations de cette section sont fournies aux utilisateurs qui utilisent le Service AWS Firewall Manager (FMS) pour configurer les groupes d'appareils transmis depuis Panorama.

Si vous utilisez FMS, vous ne pourrez pas associer un groupe d'appareils cloud au Cloud NGFW depuis Panorama ; cette option est grisée dans la console Panorama. Utilisez la console FMS AWS pour créer cette association.

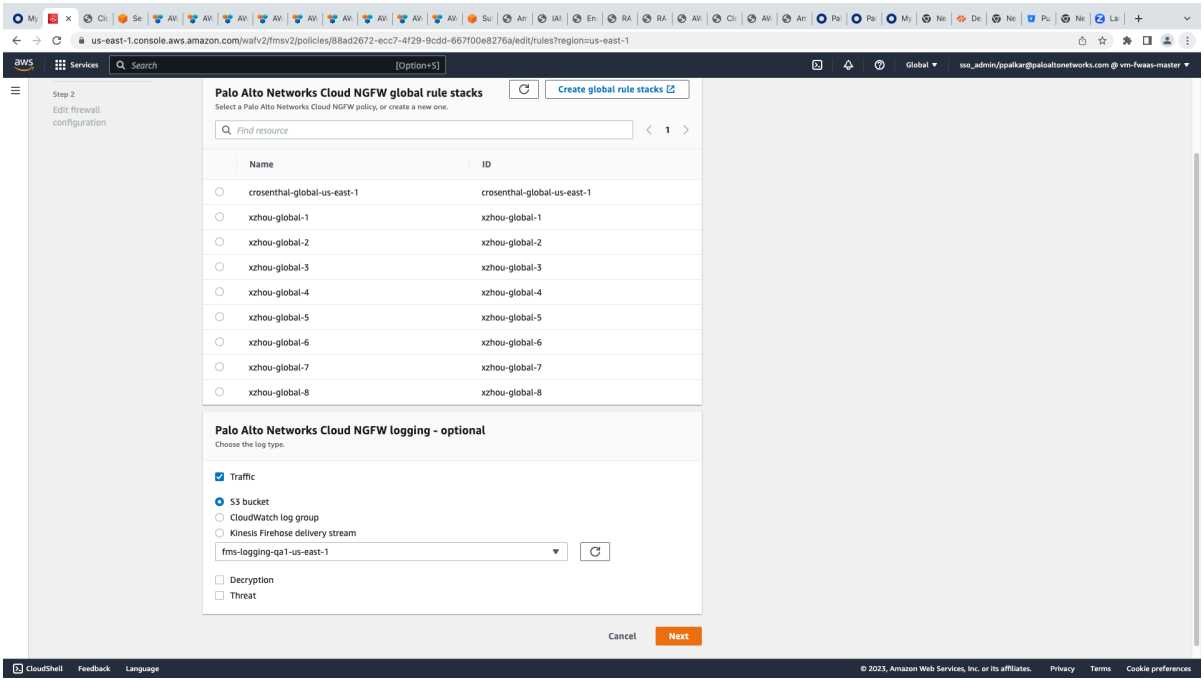
STEP 1 | Reliez un locataire à Panorama.

STEP 2 | Créez un groupe d'appareils cloud et transmettez-le au le Cloud NGFW. Cette procédure est identique pour les utilisateurs qui n'utilisent pas FMS.

STEP 3 | Accédez à la console FMS AWS et modifiez la politique.


us-east-1.console.aws.amazon.com/wafv2/fmsv2/policies/88ad2672-ecc7-4f29-9cdd-667f00e8276a?region=us-east-1
Services
Search
[Option+S]
Global
sso_admin/ppalkar@paloaltonetworks.com @ vm-fwaas-master
WAF & Shield
AWS WAF
Getting started
Web ACLs
IP sets
Regex pattern sets
Rule groups
AWS Marketplace
AWS Shield
Getting started
Overview
Protected resources
Events
Global threat dashboard
AWS Firewall Manager
Getting started
Security policies
Resource sets
Application lists
Protocol lists
Settings
rk-test-1
Overview
Policy name
rk-test-1
Policy description
rk-test-1
Type
PaloAlto Network Firewall NGFW - Distributed
Automatic remediation
-
Region
US East (N. Virginia)
Accounts and resources
Policy details
Palo Alto Networks Cloud NGFW policy configuration
Select a Palo Alto Networks Cloud NGFW policy, or create a new one.
Edit
Palo Alto Networks Cloud NGFW global rule stacks
These Palo Alto Networks Cloud NGFW firewall policies are applied to resources in scope of this Firewall Manager policy.
Name
ID
xzhou-global-8
xzhou-global-8
Palo Alto Networks Cloud NGFW logging - optional
Choose the log type.
Traffic
S3 bucket
CloudWatch log group
Kinesis Firehose delivery stream
fms-logging-qa1-us-east-1
Decryption
https://us-east-1.console.aws.amazon.com/wafv2/fmsv2/policies/88ad2672-ecc7-4f29-9cdd-667f00e8276a/edit/rules?region=us-east-1
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

STEP 4 | Sélectionnez la rulestack globale transmise depuis Panorama.



STEP 5 | Cliquez sur Save (Enregistrer) pour enregistrer vos modifications.

Utiliser plusieurs Panoramas avec votre ressource Cloud NGFW

Pour utiliser plusieurs Panorama avec la même ressource Cloud NGFW

STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sélectionnez **Integrations (Intégrations)**. La page **Integrations (Intégrations)** affiche des informations sur le Panorama actuellement lié. Si aucun Panorama n'est actuellement lié à un locataire Cloud NGFW, cette page est vide.

STEP 3 | Dans la page **Panoramas**, cliquez sur **Add Panorama (Ajouter un Panorama)**.

STEP 4 | Dans la fenêtre **Add Panorama (Ajouter un panorama)**, saisissez un **Link Name (Nom de lien)**. Sélectionnez le **Primary Panorama Serial Number (Numéro de série Panorama principal)** dans le menu déroulant.

La fenêtre **Add Panorama (Ajouter Panorama)** affiche des icônes à côté de chaque Panorama accessible à votre locataire Cloud NGFW. Ces icônes indiquent si la licence Panorama est liée au service de journalisation Strata. Pour plus d'informations, reportez-vous à la section Link the Cloud NGFW to Palo Alto Networks Management (Lier le Cloud NGFW à Palo Alto Networks Management).

STEP 5 | Sélectionnez le deuxième **Panorama serial number for the HA pair (Numéro de série Panorama pour la paire HA)**.

STEP 6 | Cliquez sur **Continue (Continuer)**.

STEP 7 | Une **Notification** s'affiche, indiquant que le processus de liaison est terminé. Cliquez sur **Confirm (Confirmer)**.

La page **Integrations (Intégrations)** affiche désormais le Panorama lié au locataire Cloud NGFW. Cliquez sur **Link ID (ID de lien)** pour afficher des informations ou pour modifier le nom du lien. Cliquez sur **Save (Enregistrer)** si vous modifiez le nom du lien.

STEP 8 | Dans la console Cloud NGFW, sélectionnez **NGFWs** pour afficher les pare-feu déployés.

Dans la partie supérieure gauche de la console Cloud NGFW, utilisez la liste déroulante pour sélectionner la **Region (Région)** hébergeant le pare-feu.

STEP 9 | Sélectionnez le pare-feu que vous souhaitez gérer avec Panorama.

STEP 10 | Cliquez sur l'onglet **Firewall Settings (Paramètres du pare-feu)**.

STEP 11 | Faites défiler jusqu'à la section **Policy Management (Gestion des politiques)**, puis sélectionnez **Panorama**.

STEP 12 | Utilisez le menu déroulant pour sélectionner le **Linked Panorama (Panorama lié)**.

STEP 13 | Cliquez sur **Save (Enregistrer)**.

STEP 14 | Répétez les étapes 8 à 13 pour gérer un autre Panorama sur un autre locataire NGFW.

STEP 15 | Cliquez sur **Integrations (Intégrations)** pour lier un autre Panorama.

STEP 16 | Dans la page **Panoramas**, cliquez sur **Add Panorama (Ajouter un Panorama)**.

STEP 17 | Dans la fenêtre **Add Panorama (Ajouter un panorama)**, saisissez un nouveau **Link Name (Nom de lien)**. Sélectionnez le **Primary Panorama Serial Number (Numéro de série Panorama principal)** dans le menu déroulant.

STEP 18 | Sélectionnez le deuxième **Panorama serial number for the HA pair (Numéro de série Panorama pour la paire HA)**.

STEP 19 | Cliquez sur **Continue (Continuer)**.

STEP 20 | Une **Notification** s'affiche, indiquant que le processus de liaison est terminé. Cliquez sur **Confirm (Confirmer)**.

Lorsque vous liez plusieurs Panorama à un locataire Cloud NGFW, aucune rulestack ne lui est associé. Lorsque vous utilisez Panorama pour transmettre les groupes d'appareils Cloud vers le pare-feu, la section **Rulestacks** de la page NGFWs change pour refléter la gestion des politiques associée au NGFW.

STEP 21 | Une **Notification** s'affiche, indiquant que le processus de liaison est terminé. Cliquez sur **Confirm (Confirmer)**.

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 et Cortex Data Lake (CDL), 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. Consultez la documentation de la journalisation Cloud NGFW pour obtenir des descriptions des champs de journal.

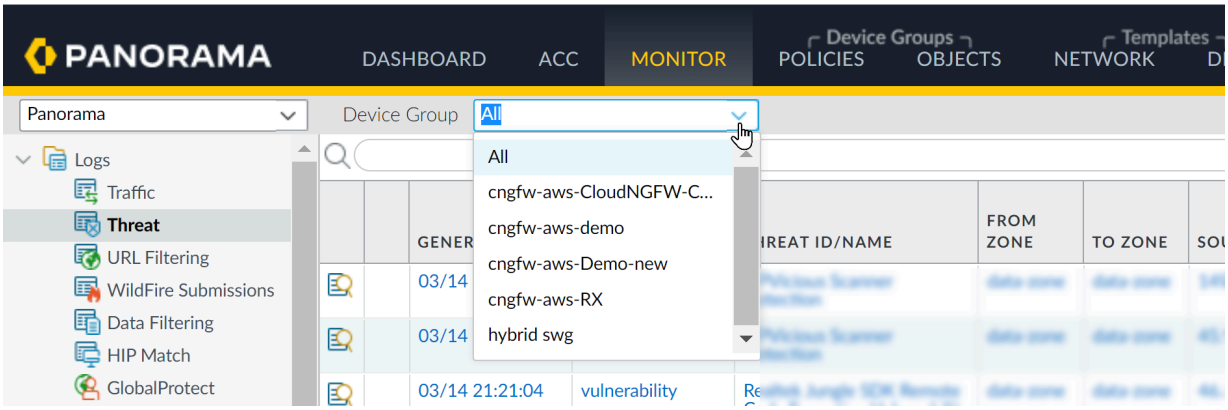
STEP 1 | Connectez-vous à Panorama.

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

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

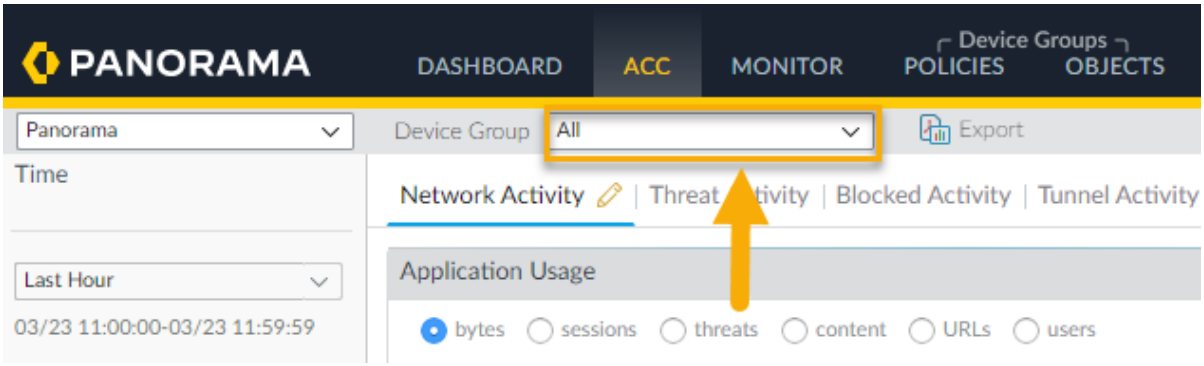
L'ACC est un outil analytique qui fournit des renseignements exploitables concernant l'activité sur votre réseau. L'ACC utilise les journaux du Cloud NGFW pour représenter graphiquement les tendances du trafic sur votre réseau. Cette représentation graphique vous permet d'interagir avec les données et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

Afficher les journaux de Cloud NGFW dans le service de journalisation Strata

Lorsque vous intégrez Cloud NGFW à Panorama et le service de journalisation Strata, vous transférez les journaux créés par vos ressources Cloud NGFW et les affichez dans le service de journalisation Strata. Dans l'interface Web Strata Logging Service, vous pouvez afficher les journaux de trafic, de menaces et de déchiffrement générés par vos ressources Cloud NGFW.

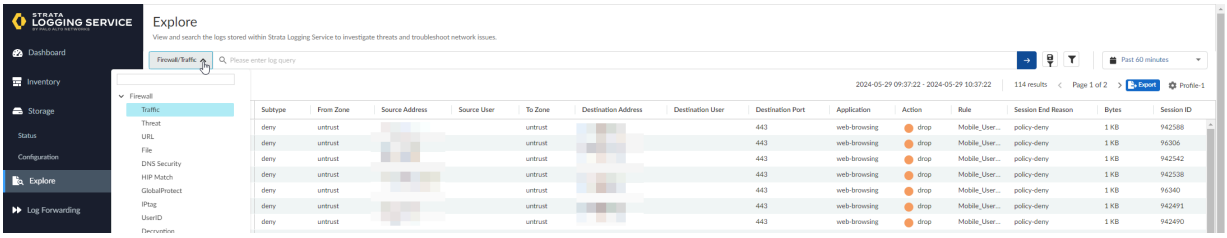
Si vous utilisez Panorama et n'utilisez pas le service de journalisation Strata pour la collecte de journaux, vous pouvez transférer les journaux à une autre entité, cependant, vous devez activer le service de journalisation Strata dans votre profil de journalisation.

Pour plus d'informations sur les champs de journalisation, consultez la référence du schéma du service de journalisation Strata : Trafic, menace et décryptage.

STEP 1 | Connectez-vous à votre instance du service de journalisation Strata.

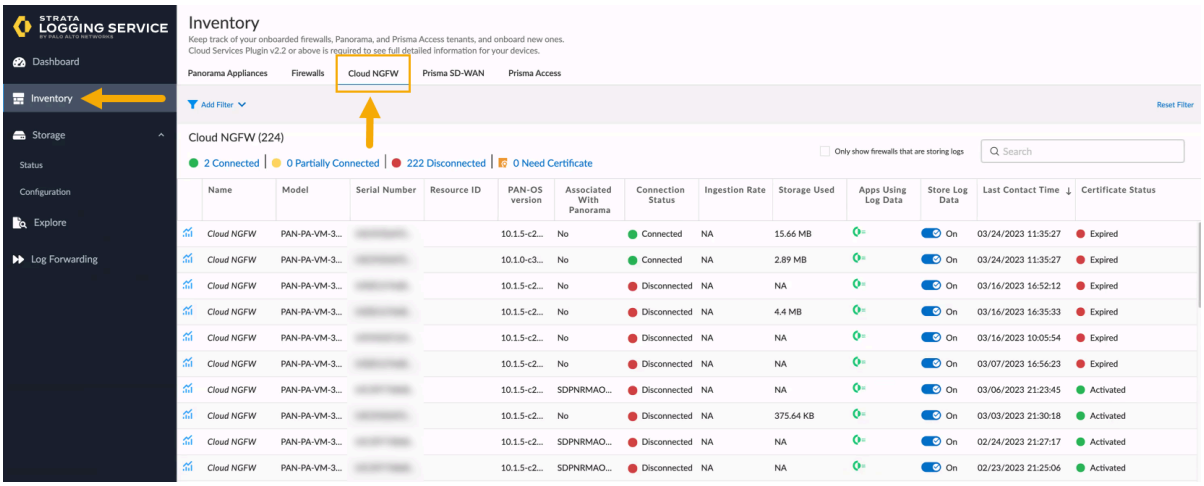
STEP 2 | Sélectionnez **Explore (Explorer)**.

STEP 3 | Dans le menu déroulant de la requête, vous pouvez sélectionner le type de journaux. Chaque page affiche 100 journaux. Cependant, vous pouvez utiliser les Requêtes du service de journalisation Strata pour affiner les informations affichées.



STEP 4 | Sélectionnez **Inventory (Inventaire)** pour afficher des informations sur les pare-feu embarqués.

STEP 5 | Dans la page **Inventory (Inventaire)**, sélectionnez **Cloud NGFW**.



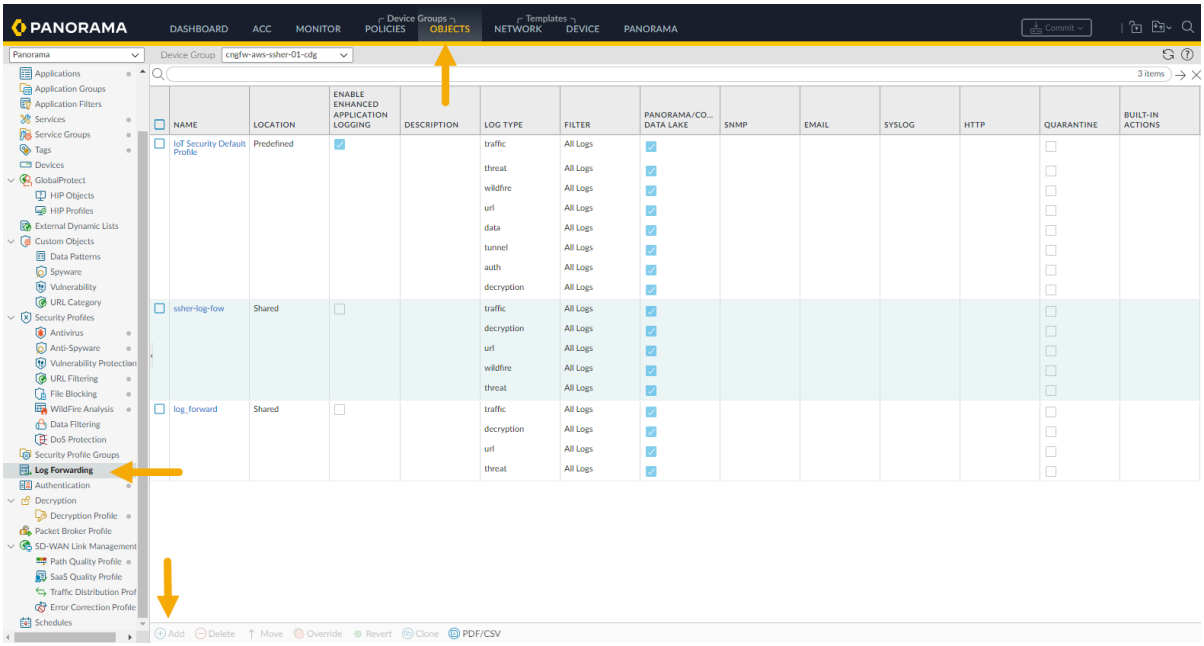
Transférer les journaux vers le service de journalisation Strata

Pour transférer les journaux au service de journalisation Strata :

STEP 1 | Dans la console Panorama, sélectionnez **Objects (Objets)** sous **Device Groups (Groupes d'appareils)**.

STEP 2 | Sélectionnez **Log Forwarding (Transfert des journaux)**.

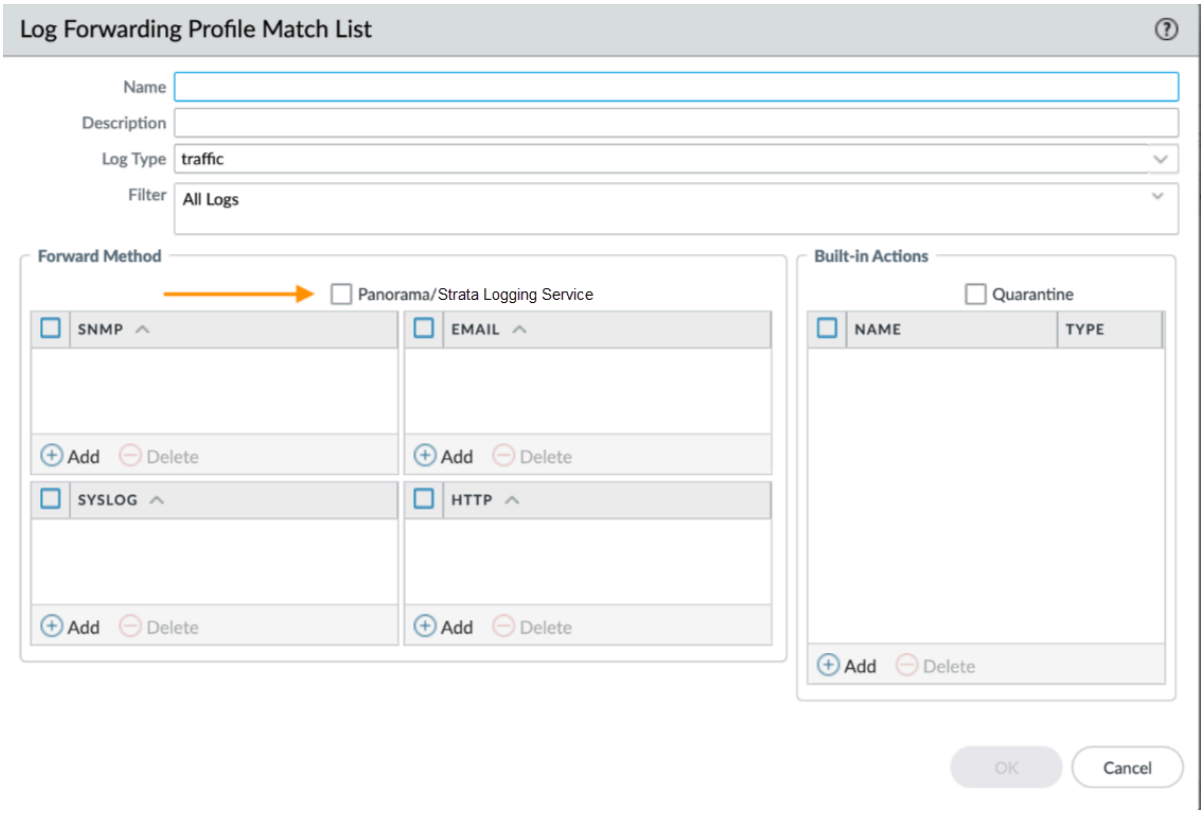
STEP 3 | Cliquez sur **Add (Ajouter)** pour créer un nouveau profil de liste de correspondance de transfert des journaux.



STEP 4 | Sur l'écran **Log Forwarding Profile Match List (Liste de correspondance des profils de transfert de journaux)**, spécifiez un nom pour le journal.

STEP 5 | Sélectionnez un **Log Type (Type de journal)** dans le menu déroulant.

STEP 6 | Sélectionnez **Panorama/Strata Logging Service (Service de journalisation Panorama/Strata)** comme **Forward Method (Méthode de transfert)**.



STEP 7 | Cliquez sur **OK**.

STEP 8 | Validez et appliquez votre modification.

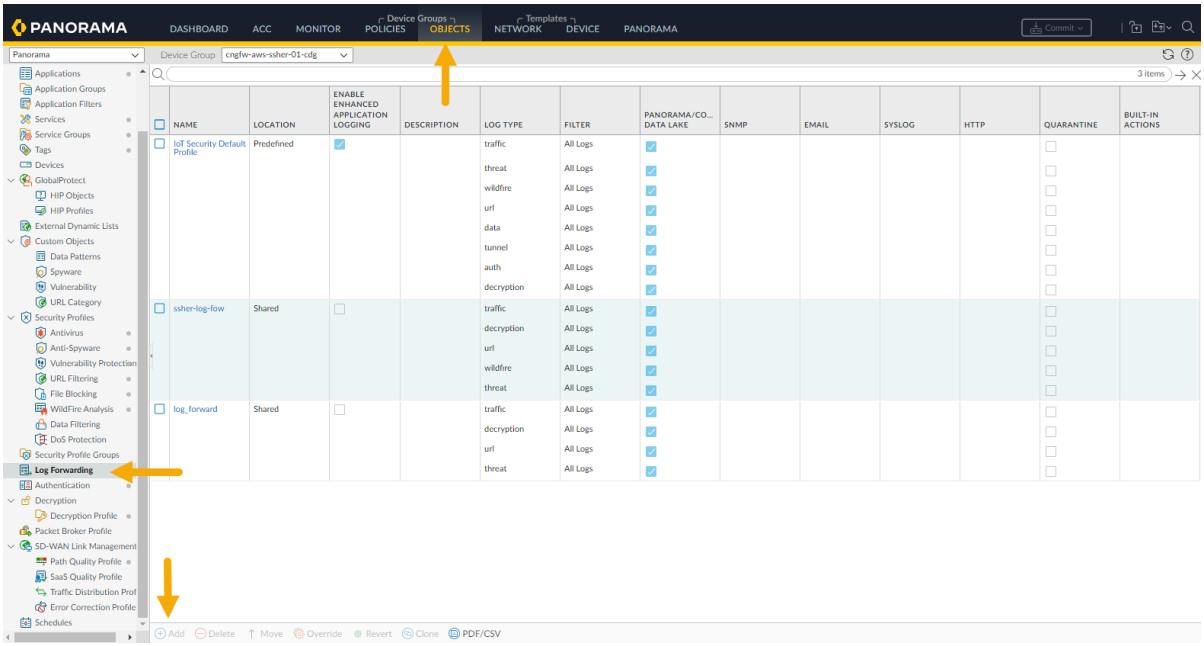
Transférer des journaux sans le service de journalisation Strata

Si vous utilisez Panorama et n'utilisez pas le service de journalisation Strata pour la collecte de journaux, vous pouvez transférer les journaux à une autre entité, comme AWS Cloudwatch, Amazon S3 ou Amazon Kinesis.

STEP 1 | Dans la console Panorama, sélectionnez **Objects (Objets)** sous **Device Groups (Groupes d'appareils)**.

STEP 2 | Sélectionnez **Log Forwarding (Transfert des journaux)**.

STEP 3 | Cliquez sur **Add (Ajouter)** pour créer un nouveau profil de liste de correspondance de transfert des journaux.



STEP 4 | Sur l'écran **Log Forwarding Profile Match List (Liste de correspondance des profils de transfert de journaux)**, spécifiez un nom pour le journal.

STEP 5 | Sélectionnez un **Log Type (Type de journal)** dans le menu déroulant.

Si Panorama n'est pas lié au service de journalisation Strata, les journaux ne sont pas transférés à la console Panorama. Ils peuvent être consultés dans une autre application comme CloudWatch, S3 ou Kinesis. Utilisez la console Cloud NGFW pour configurer les autres méthodes de journalisation.

Activez le service de journalisation Strata dans votre profil de journalisation même si vous n'avez pas l'intention d'y envoyer des journaux directement.

STEP 6 | Cliquez sur **OK**.

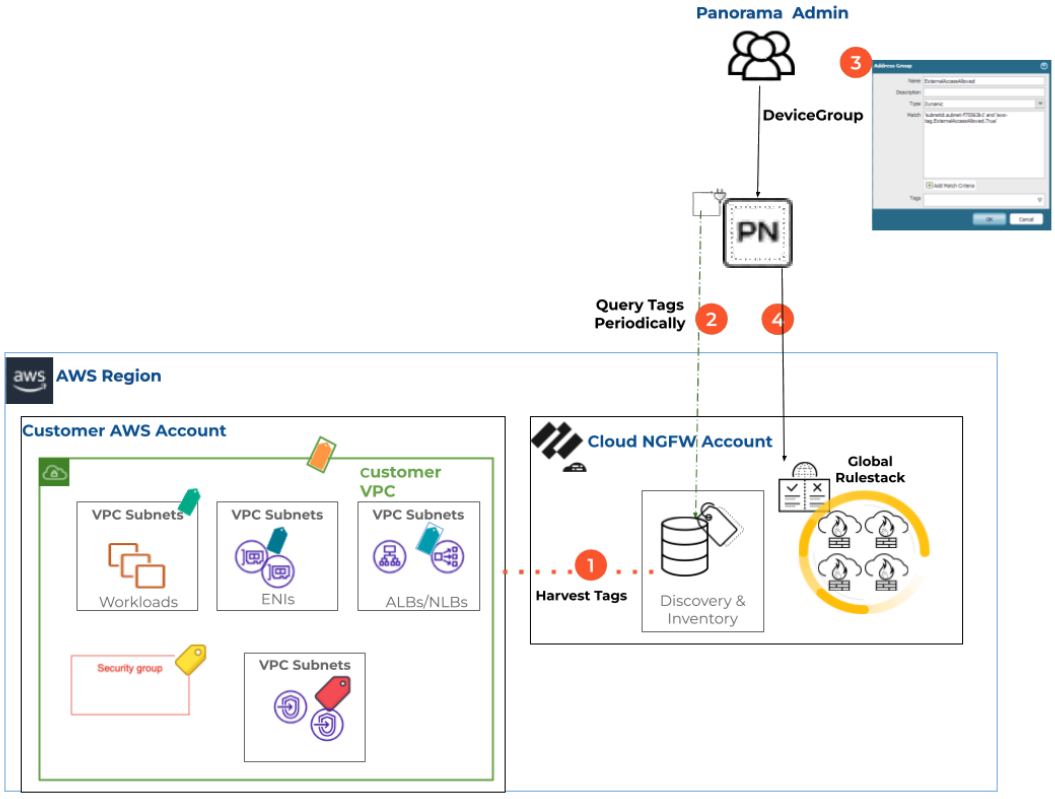
STEP 7 | Validez et appliquez votre modification.

Politiques basées sur des étiquettes

Vous pouvez mettre à jour automatiquement la politique de sécurité sur vos ressources Palo Alto Networks® Cloud NGFW afin de sécuriser le trafic vers ces ressources AWS pendant que vous déployez ou résiliez les ressources AWS (telles que des instances EC2) dans le cloud public AWS.

Pour activer cette fonctionnalité depuis Panorama, vous devez configurer le plug-in Panorama AWS pour récupérer les adresses IP/étiquettes que votre locataire Cloud NGFW collecte à partir des comptes AWS que vous avez ajoutés. Utilisez ensuite le plug-in AWS Panorama pour transmettre ces étiquettes aux ressources Cloud NGFW en configurant la définition de la surveillance et en les notifiant aux groupes d'appareils correspondants qui correspondent à ces pare-feu Palo Alto Networks.

Vous pouvez ensuite créer des objets Dynamic Address Group (groupe d'adresses dynamiques) Panorama dans ces groupes d'appareils à l'aide d'étiquettes de ressources AWS. Lorsque vous faites référence à ces étiquettes dans les groupes d'adresses dynamiques et que vous les faites correspondre à des règles de politique de sécurité, vous pouvez continuellement appliquer la politique sur l'ensemble des ressources déployées au sein de vos comptes AWS.



Prérequis

Pour activer les politiques basées sur des étiquettes pour les ressources Cloud NGFW pour AWS, voici la configuration système minimale requise :

- Installez le plug-in AWS version 5.1.0 ou supérieure sur votre Panorama. Pour plus d'informations, consultez la section Install or Upgrade the AWS Plugin (Installer ou mettre à niveau le plug-in AWS).
- Utilisation de la console Cloud NGFW Ajoutez des comptes AWS au locataire Cloud NGFW et collectez leurs étiquettes.
- Utiliser le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama.
- Configurer les objets Dynamic Address Group (groupe d'adresses dynamiques) avec des étiquettes dans les groupes d'appareils.

Concepts clés

Terme	Definition
Étiquettes de ressources cloud	Étiquettes AWS configurées sur des ressources AWS.
Groupe de VPC	Un ensemble de VPC AWS provenant d'un ou de plusieurs comptes AWS.
Définition de la surveillance	Associe un groupe de VPC à un groupe de notification.
Groupe de notification	Vous pouvez regrouper un ensemble de groupes d'appareils Panorama qui nécessitent le même ensemble d'étiquettes.

Pour activer les politiques basées sur des étiquettes pour les ressources Cloud NGFW pour AWS, vous devez préparer votre appareil Panorama pour cette intégration en installant le plug-in AWS version 5.1.0 ou supérieure. À l'aide de la console Cloud NGFW, ajoutez vos comptes AWS et collectez les étiquettes des ressources AWS. Utilisez ensuite le plug-in Panorama pour interroger régulièrement les étiquettes de votre locataire Cloud NGFW et ajoutez-le aux groupes d'appareils Panorama pour gérer les objets et les règles DAG.

Pour activer les politiques basées sur les étiquettes Cloud NGFW dans votre appareil Panorama :

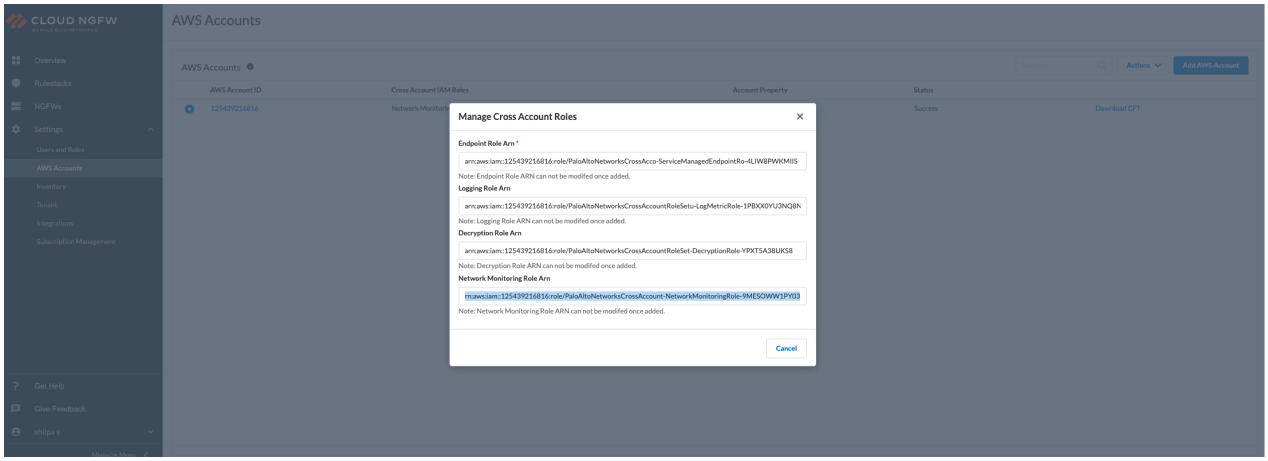
1. Ajoutez des comptes AWS au locataire Cloud NGFW et collectez leurs étiquettes
2. Utiliser le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama.
3. Configurer les objets Dynamic Address Group (groupe d'adresses dynamiques) avec des étiquettes dans les groupes d'appareils.

Ajoutez des comptes AWS au locataire Cloud NGFW et collectez leurs étiquettes

Intégrez votre compte AWS à votre locataire Cloud NGFW. Pour plus d'informations, consultez **l'étape 10** de la section Cloud NGFW PAYG SaaS Subscription (Abonnement Cloud NGFW PAYG SaaS).

Si vous avez déjà intégré votre compte AWS sur le locataire cloud NGFW, vous pouvez directement commencer la collecte des étiquettes.

Le modèle CloudFormation (CFT) existant de votre compte AWS intégré doit avoir un rôle `Network MonitoringRole Arn`. Le rôle de surveillance du réseau fournit une visibilité sur les performances du réseau connectant les applications hébergées sur AWS. Pour plus d'informations, consultez la section Manually add a CloudFormation template (Ajouter un modèle CloudFormation manuellement).



Activer la surveillance

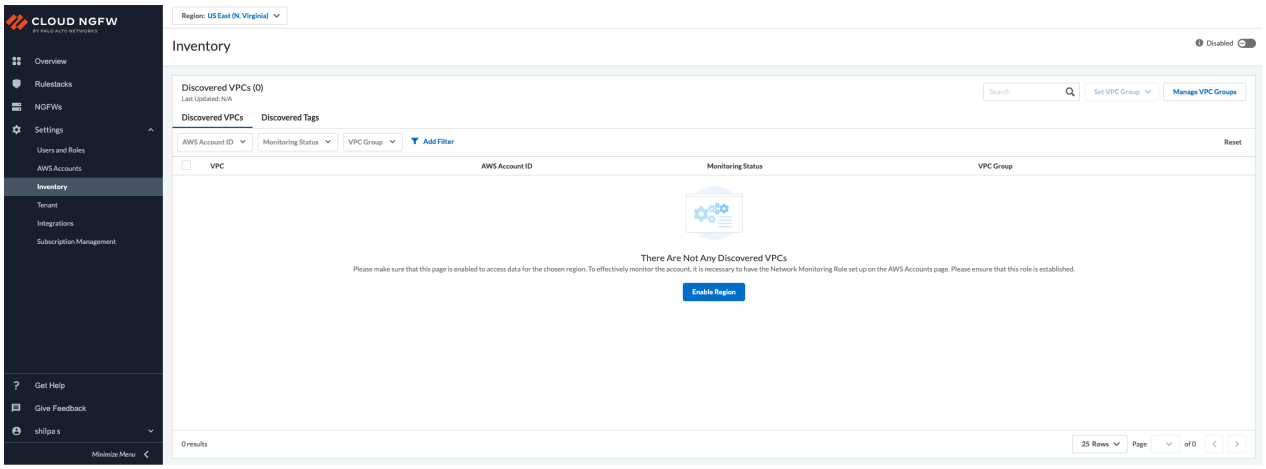
Dans la console Cloud NGFW, vous pouvez activer la découverte des étiquettes de ressources AWS pour les régions souhaitées. Cloud NGFW collectera périodiquement les étiquettes de vos ressources AWS (par

exemple : EC2, SG et LB) dans différents comptes AWS et enregistrera les informations sur votre locataire Cloud NGFW. Cloud NGFW affiche les étiquettes de ressources sur les ressources organisées par les VPC dans chaque compte AWS.

À cette fin, vous devez activer la surveillance dans la page **Inventory (Inventaire)** pour accéder aux données de chaque région AWS, afin de déclencher la découverte des étiquettes.

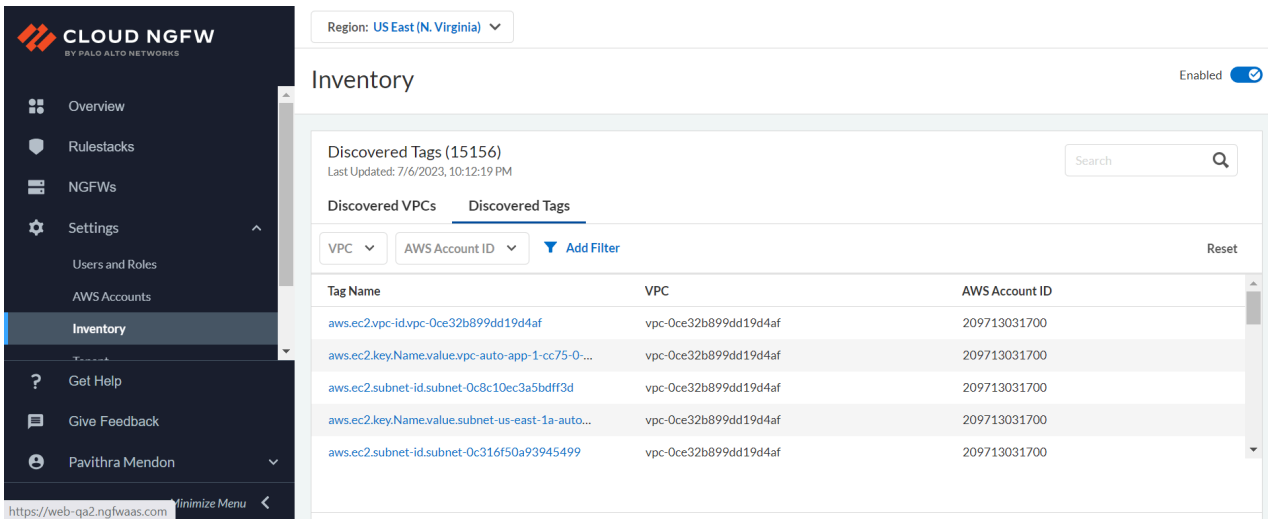
Le bouton **Enable Region (Activer la région)** sous l'onglet **Discovered VPCs (VPC découverts)** apparaît uniquement lors de l'intégration de votre compte AWS pour la première fois. Sélectionnez **Region (Région)** dans la liste déroulante et cliquez sur **Enable Region (Activer la région)** pour activer la surveillance des étiquettes.

Vous pouvez également sélectionner une **Region (Région)** dans la liste déroulante et cliquer sur le bouton **Enable (Activer)** pour activer la surveillance des étiquettes.

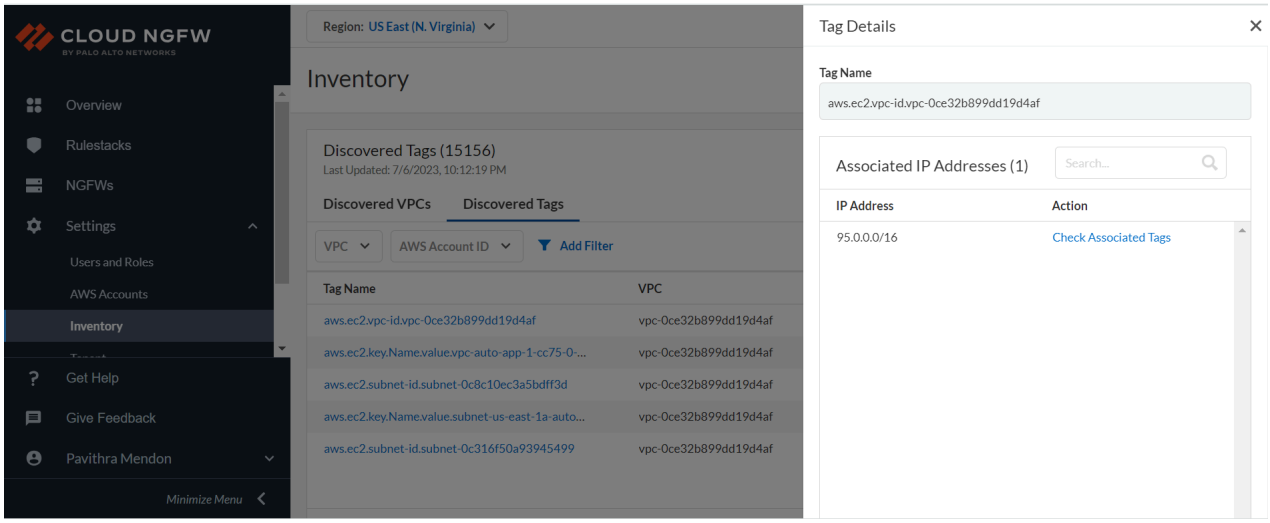


Afficher les étiquettes collectées dans la console Cloud NGFW

Vous pouvez voir le nombre total d'étiquettes découvertes sur la page **Inventory (Inventaire)** sous l'onglet **Discovered Tags (Étiquettes découvertes)**.



Cliquez sur **Tag Name (Nom de l'étiquette)** pour répertorier les adresses IP associées à chaque étiquette.



Cliquez sur **Check Associated Tags (Vérifier les étiquettes associées)** pour répertorier les différentes étiquettes associées à l'adresse IP.

Dans la console NGFW, la limite de caractères de l'étiquette est **de 127** caractères pour tous les types de ressource AWS (clé ou valeur combinée). Les étiquettes dont la clé/valeur est **supérieure à 127**ne sont pas ajoutées à la liste **DiscoveredTags (Étiquettes découvertes)**. Pour plus d'informations, consultez la section Tag Restrictions (Restrictions relatives aux étiquettes).

*Si vous ne disposez pas de l'**autorisation d'administrateur d'inventaire**, vous ne pouvez pas **définir un groupe de VPC** ni **créer un nouveau groupe de VPC**.*

Utiliser le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama

Utilisez le plug-in Panorama AWS pour effectuer les opérations suivantes :

1. Créer et gérer des groupes de VPC.
2. Ajouter des étiquettes aux groupes d'appareils à l'aide des définitions de surveillance et de groupes de notification.

Installer et configurer le plug-in AWS 5.1.0 sur Panorama pour interroger les étiquettes de ressources AWS collectées dans les locataires Cloud NGFW et les ajouter aux groupes d'appareils Cloud.

Créer et gérer des groupes de VPC

Lorsque vous activez la surveillance, un groupe de VPC **par défaut** est automatiquement créé. Vous ne pouvez pas **supprimer** le groupe de VPC **par défaut**. Un VPC nouvellement découvert est toujours placé dans le groupe de VPC **par défaut**. Si vous le souhaitez, vous pouvez ensuite le déplacer vers un autre groupe de VPC.

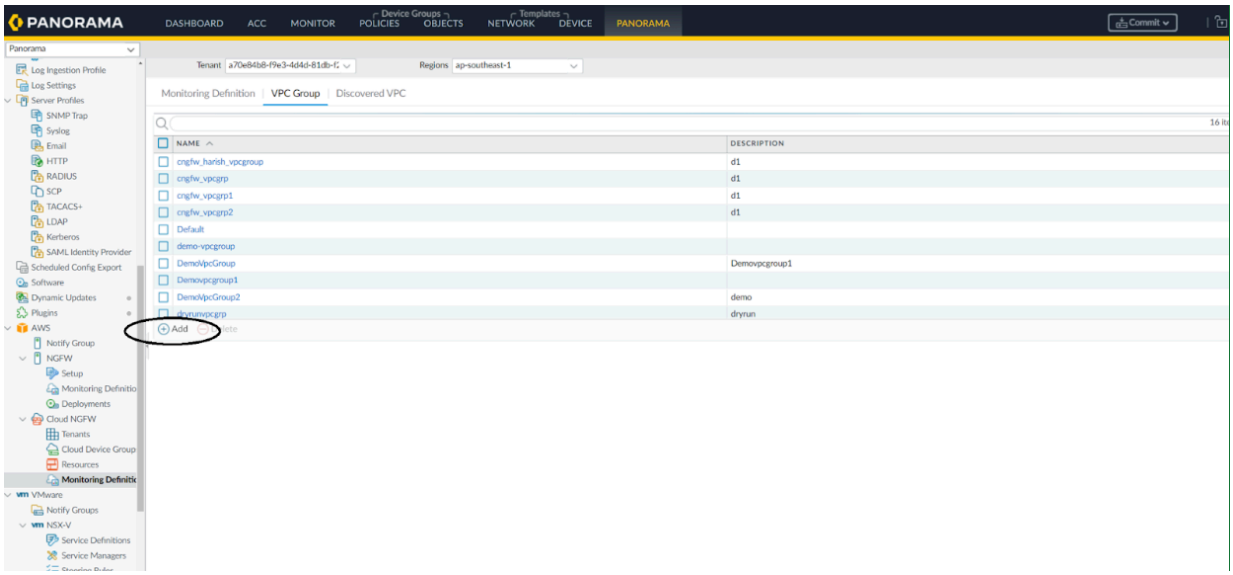
La portée d'un groupe de VPC créé dans une région s'applique uniquement à cette région. Par exemple, le groupe de VPC A créé dans la région X n'est pas accessible dans la région Y.

Vous pouvez également créer de nouveaux groupes de VPC et déplacer les VPC vers d'autres groupes de VPC en suivant les étapes ci-dessous :

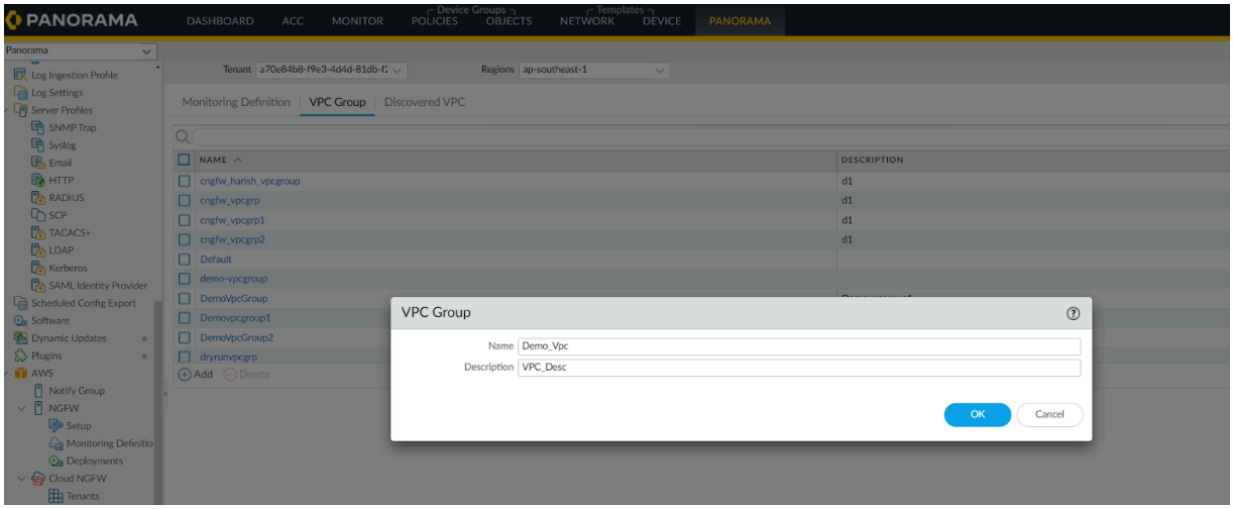
Si vous souhaitez créer un nouveau **groupe de VPC autre que par défaut** sur Panorama, suivez les étapes décrites dans la procédure ci-dessous :

1. Dans la console **Panorama**, accédez à l'onglet **Panorama** , puis cliquez sur **AWS**.
2. Sélectionnez **Tenant (Locataire)** et **Region (Région)**.

3. Accédez à **AWS** > **Cloud NGFW** > **Monitoring Definition (Définition de surveillance)** > **VPC Group (Groupe de VPC)** > **Add (Ajouter)**.

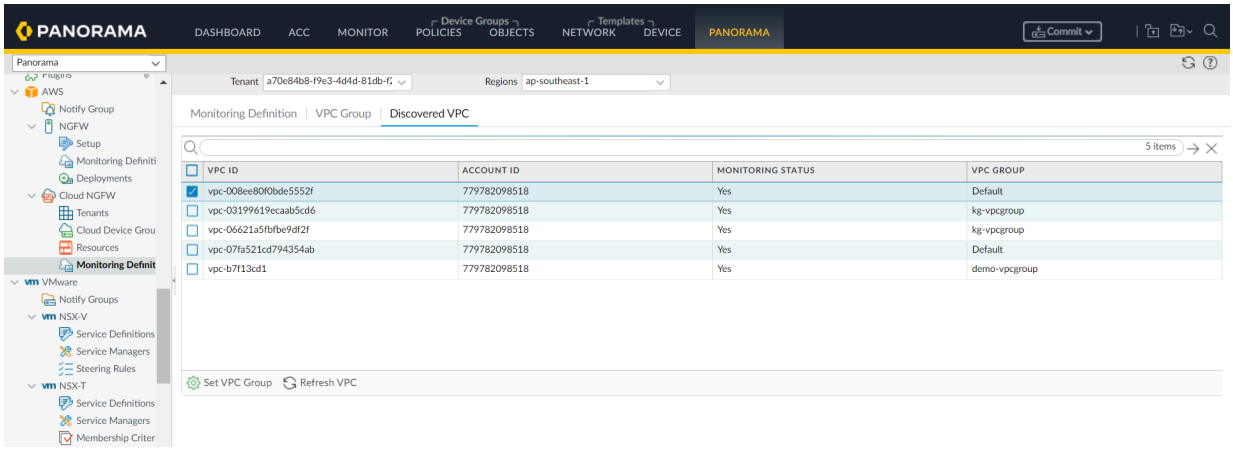


4. Saisissez le **Name (Nom)** et la **Description** du groupe de VPC.



5. Cliquez sur **OK**.

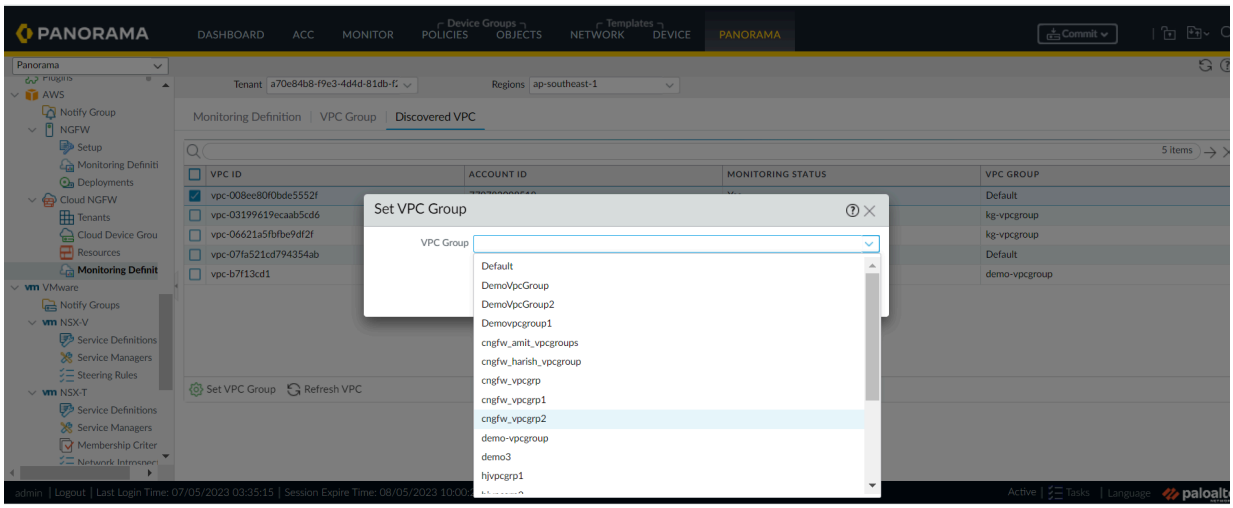
6. Accédez à **AWS** > **Cloud NGFW** > **Monitoring Definition (Définition de surveillance)** > **Discovered VPC (VPC découvert)**.



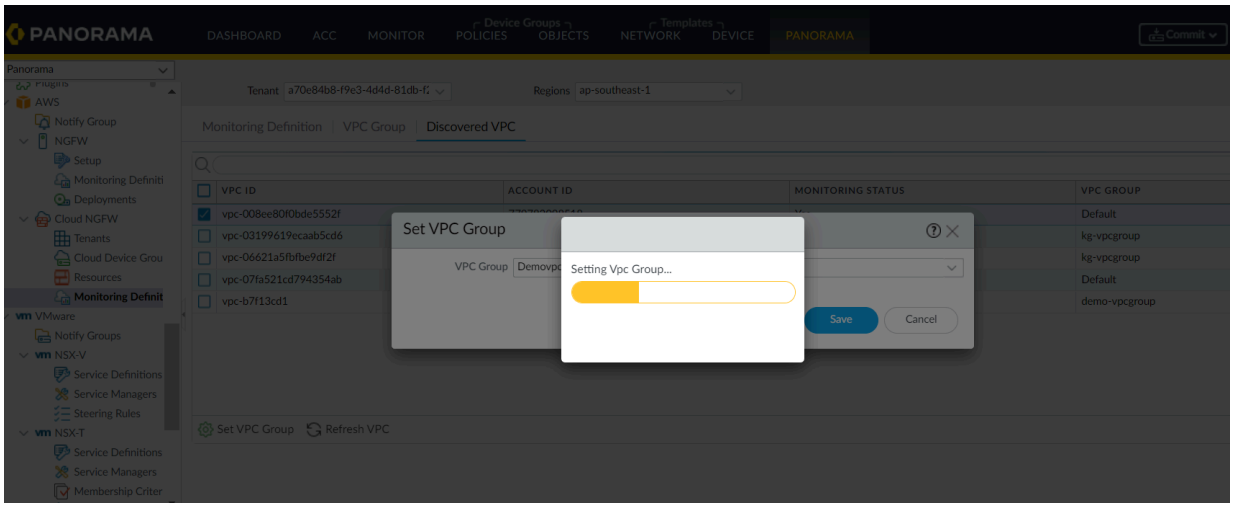
- *Vous ne pouvez pas mapper un **groupe de VPC** sur plus de 8 groupes d'appareils. Configurez les définitions de surveillance sur les groupes de VPC de telle sorte qu'un groupe de VPC donné n'ait que 8 groupes d'appareils mappés (via les groupes de notification) pour de meilleures performances.*
- *Le groupe de VPC **par défaut** est automatiquement créé. Vous ne pouvez pas **supprimer** le groupe de VPC **par défaut**. Un VPC nouvellement découvert est toujours placé dans le groupe de VPC **par défaut**. Si nécessaire, les VPC peuvent être déplacés sous un autre groupe de VPC.*

7. Cliquez sur **Set VPC Group (Définir le groupe de VPC)**.

8. Sélectionnez **VPC Group (Groupe de VPC)**.



9. Cliquez sur **Save (Enregistrer)**.



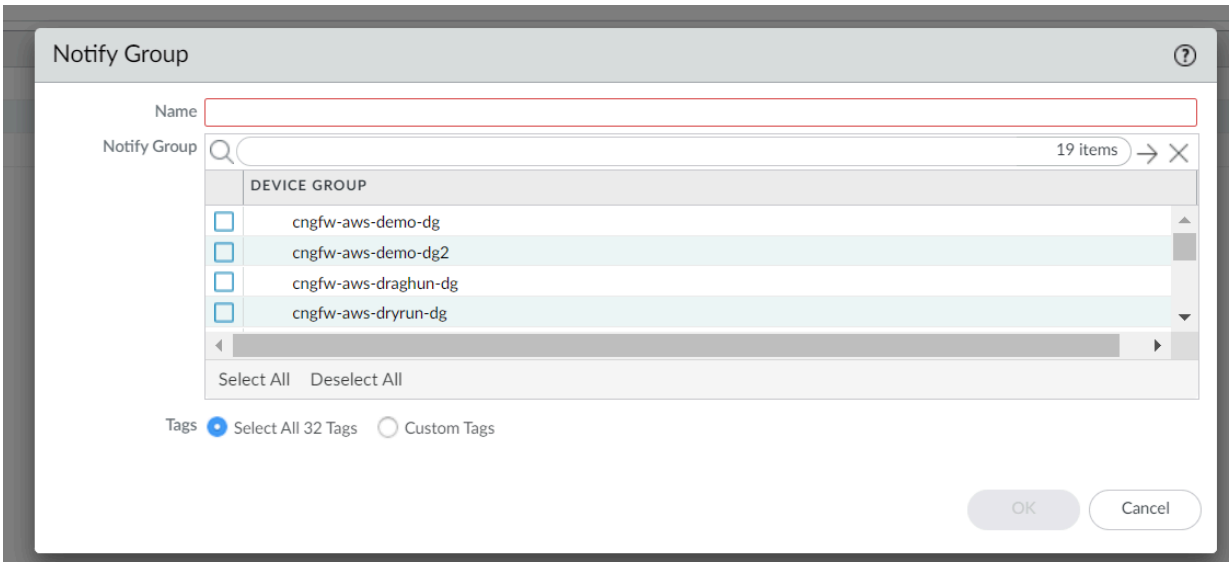
Ajouter des étiquettes aux groupes d’appareils à l’aide des définitions de surveillance et de groupes d’appareils

Pour transmettre les étiquettes acquises auprès du locataire Cloud NGFW vers des ressources Cloud NGFW, assurez-vous de configurer les **groupes de notification** et les **définitions de surveillance** sur les groupes d’appareils correspondants correspondant à ces pare-feu Palo Alto Networks. Vous pouvez ensuite afficher les étiquettes de comptes AWS collectées à partir du locataire Cloud NGFW dans Panorama.

Créez un **groupe de notification** pour votre groupe d’appareils cloud en suivant les étapes ci-dessous :

1. Dans la console du **plug-in Panorama** , accédez à **AWS** > **Notify Group (Groupe de notification)**.

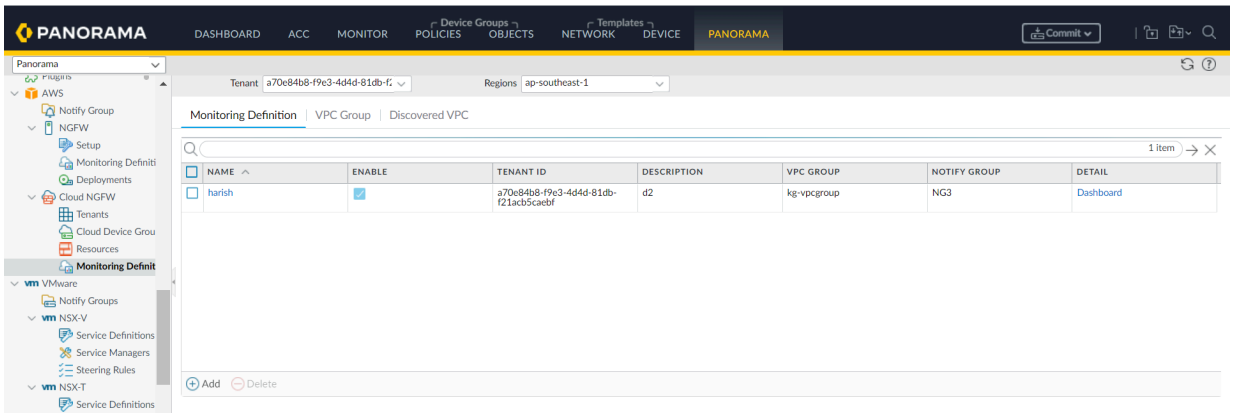
2. Cliquez sur **Add (Ajouter)**.



3. Saisissez le **Name (Nom)**.
4. Sélectionnez le **Device Group (Groupe d'appareils)** et les **Tags (Étiquettes)**.
5. Cliquez sur **OK**.

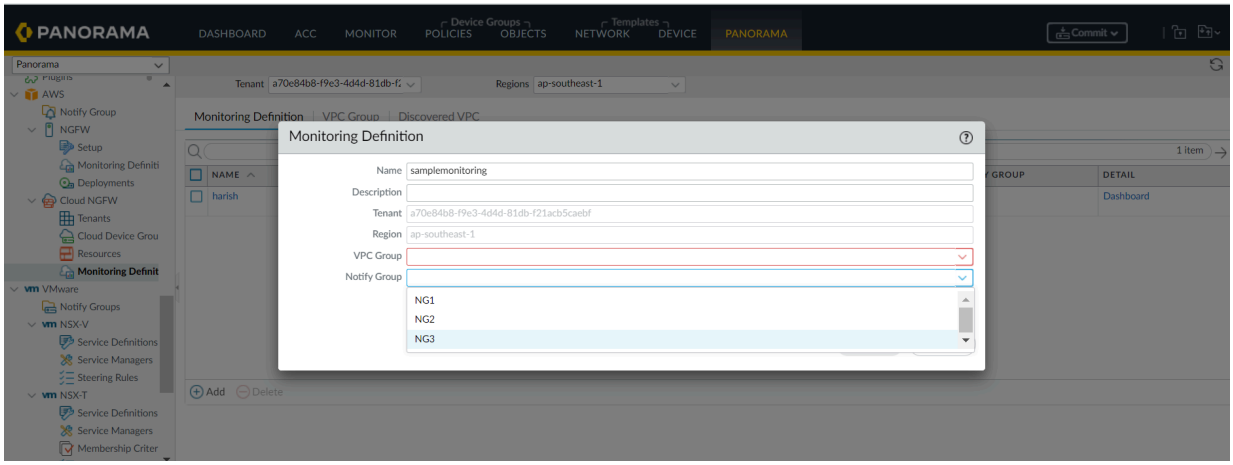
Créez une **définition de surveillance** cloud associant le **groupe de VPC** requis et le **groupe de notification** des étiquettes acquises auprès de Cloud NGFW.

1. Dans la console **Panorama** , accédez à **AWS** > **Cloud NGFW** > **Monitoring Definition (Définition de surveillance).**



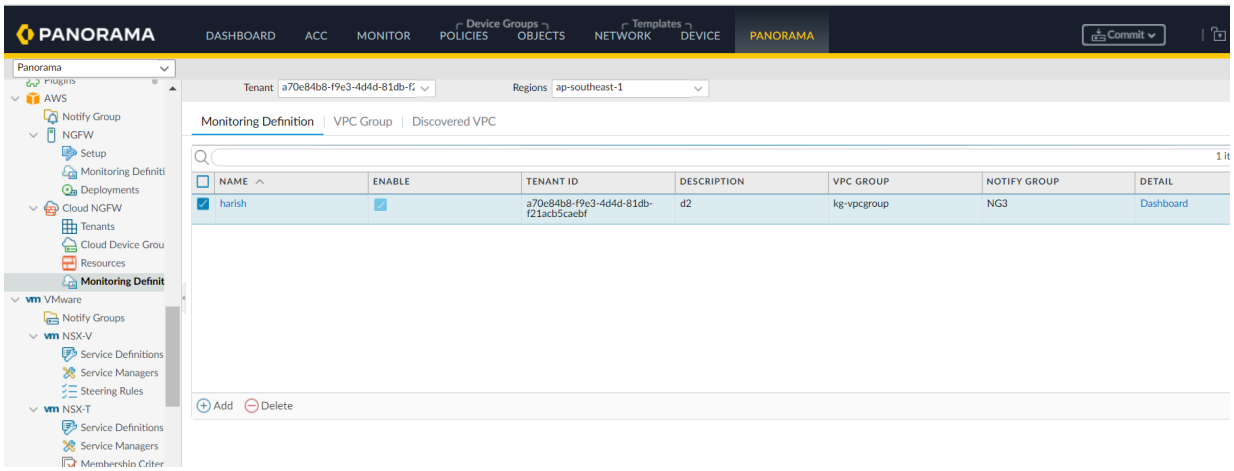
2. Cliquez sur **Add (Ajouter)**.
3. Saisissez votre **Name (Nom)** et la **Description**.
4. Sélectionnez le groupe de VPC requis dans le menu déroulant **VPC Group (Groupe de VPC)**.

5. Sélectionnez le groupe de notification requis dans le menu déroulant **Notify Group (Groupe de notification)**.

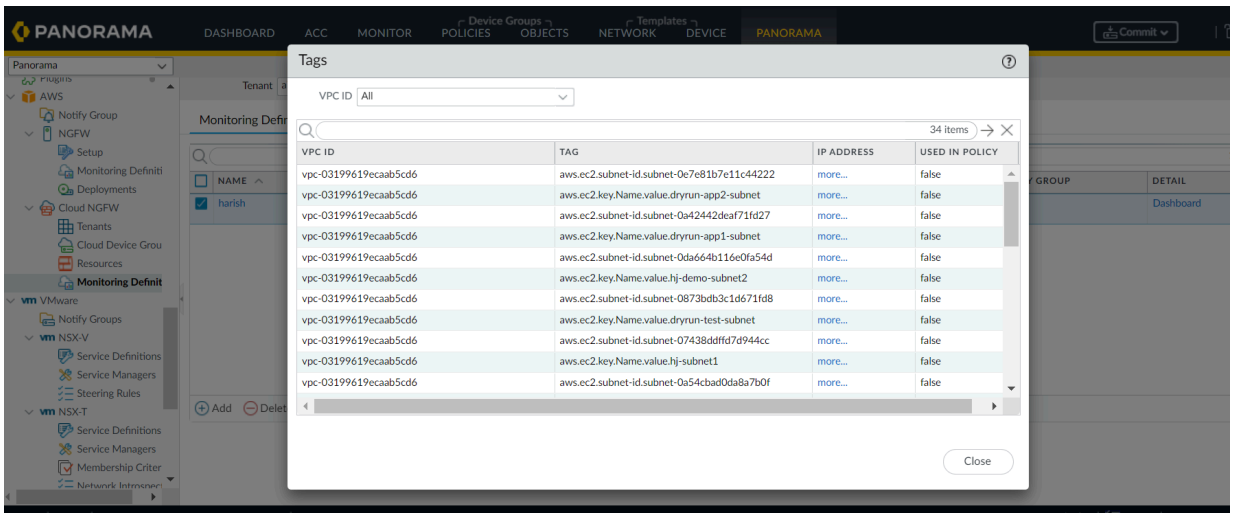


6. Cliquez sur **OK**.
7. **Validez** et **transmettez** vos modifications sur Panorama.

8. Sélectionnez une **Monitoring Definition (Définition de surveillance)** et cliquez sur le **Dashboard (Tableau de bord)** pour afficher les étiquettes collectées auprès du locataire Cloud NGFW.



Vous pouvez désormais afficher les étiquettes collectées auprès du locataire Cloud NGFW.



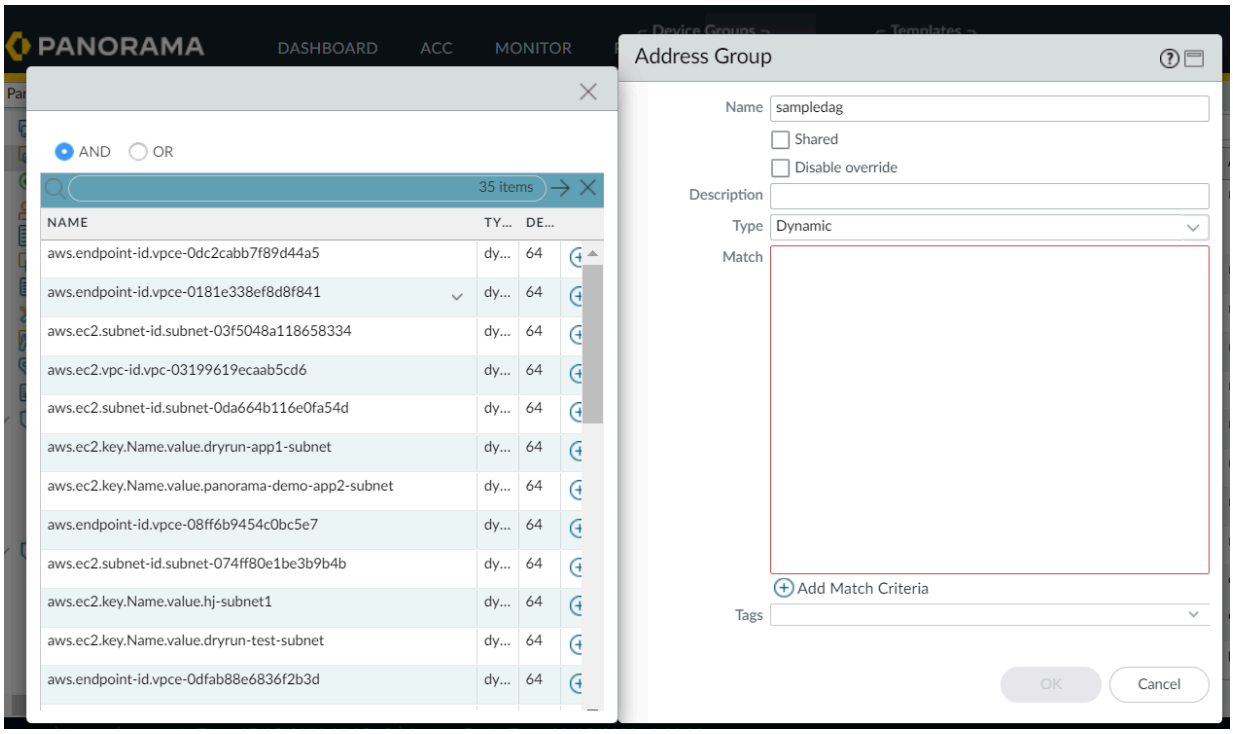
Configurer les objets Dynamic Address Group (groupe d’adresses dynamiques) avec des étiquettes dans les groupes d’appareils

Vous pouvez créer des Dynamic Address Groups (groupes d’adresses dynamiques) avec des étiquettes Cloud NGFW collectées pour votre groupe d’appareils cloud. Pour plus d’informations, consultez la section Create Dynamic Address Groups (Créer des groupes d’adresses dynamiques).

Voici les étapes à suivre pour ajouter des critères de correspondance à vos groupes d’adresses dynamiques :

1. Dans la console **Panorama** , accédez à l’onglet **Objects (Objets)**
2. Dans le volet de gauche, accédez à **Address Groups (Groupes d’adresses)**.
3. Cliquez sur **Add (Ajouter).**
4. Saisissez le **Name (Nom)** de votre groupe d’adresses et sélectionnez le type **Dynamic (Dynamique)**.

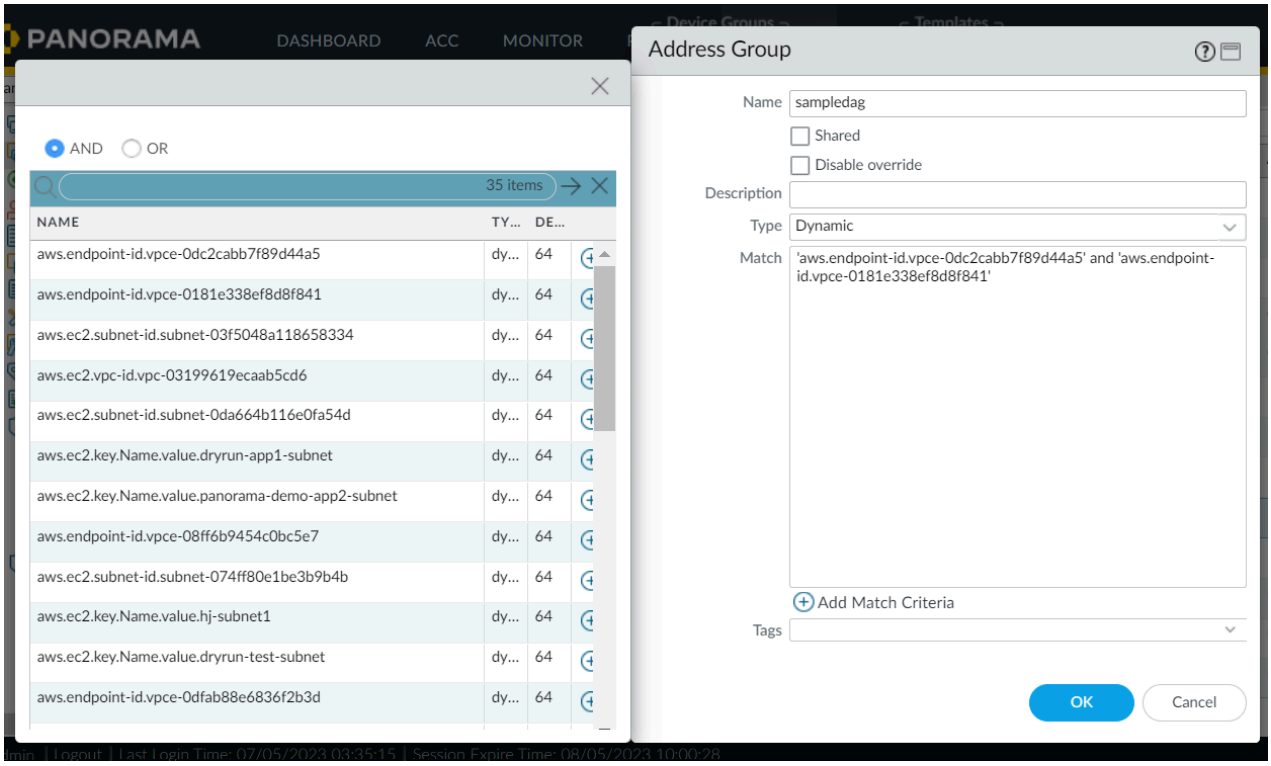
5. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)**.



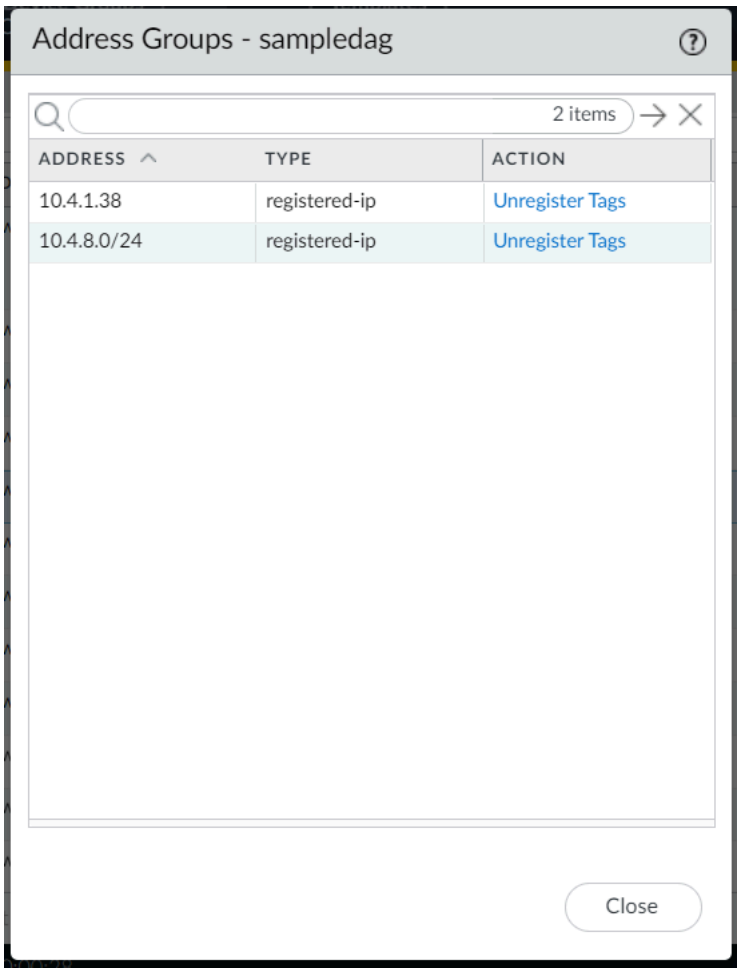
Vous pouvez désormais créer des **politiques de groupe d'adresses dynamiques** faisant référence aux DAG créés ci-dessus pour les groupes d'appareils cloud.

Vous pouvez ajouter des étiquettes à partir de différentes régions sur votre objet DAG. Pour utiliser des étiquettes de différentes régions, vous devez créer un groupe d'appareils cloud du même nom dans d'autres régions. En outre, vous devez créer une définition de surveillance dans d'autres régions mappant le groupe de notification au groupe au VPC de la région concernée. Pour plus d'informations, consultez Politiques basées sur des étiquettes inter-régions.

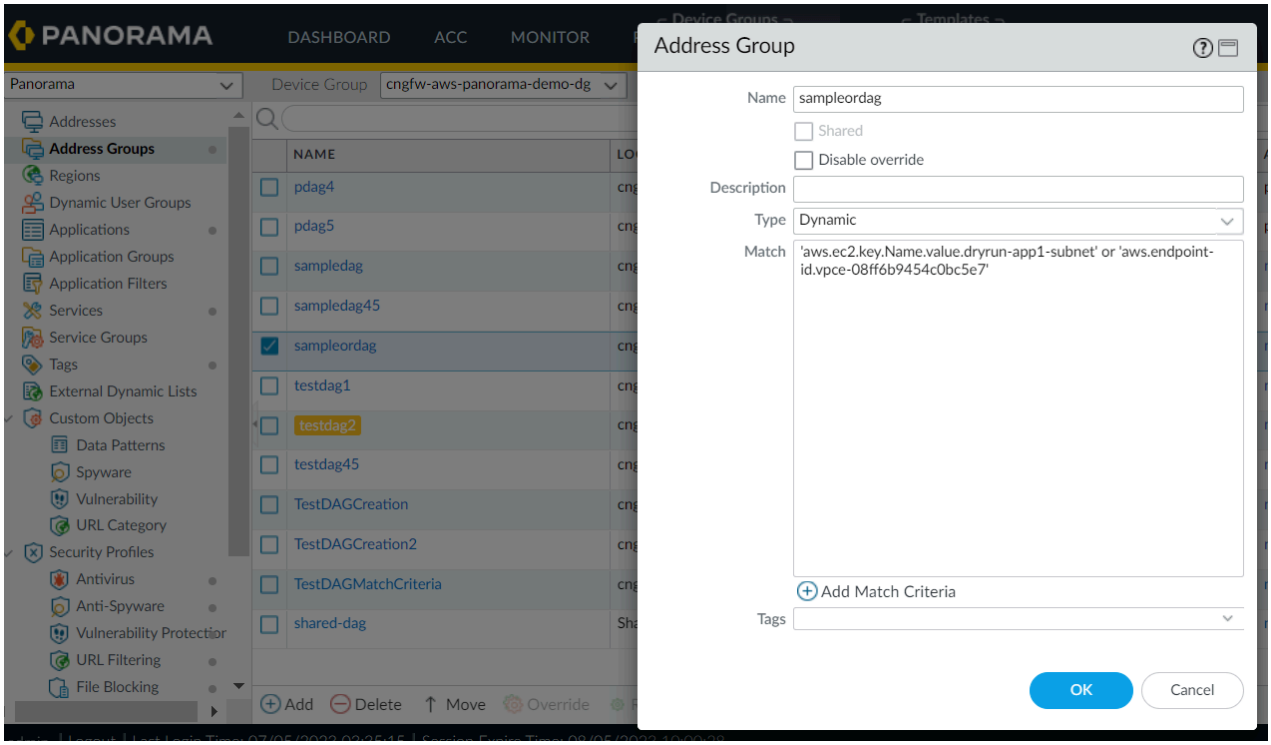
Voici un exemple de la création des DAG à l'aide de l'opérateur **AND** :



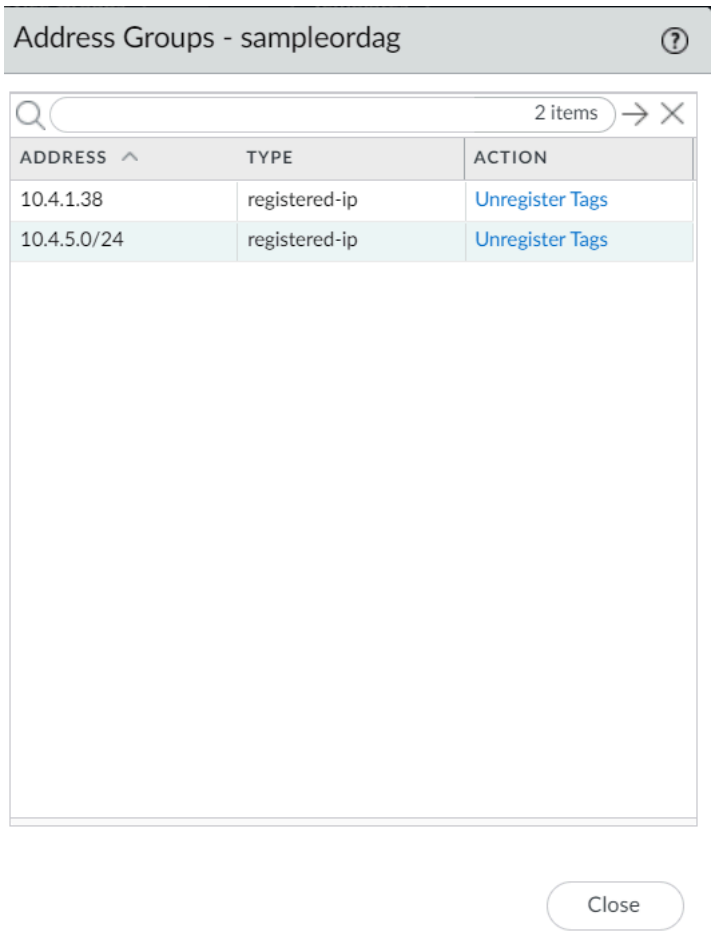
Le groupe d’adresses affiche la liste des adresses qui correspondent aux deux critères de correspondance.



Voici un exemple de la création des DAG à l'aide de l'opérateur **OR** :



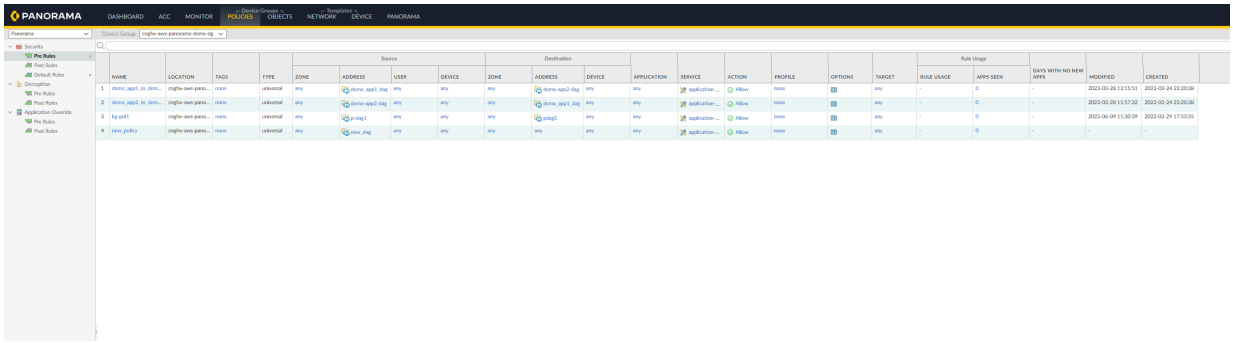
Le groupe d’adresses affiche la liste des adresses qui correspondent à l’un des critères de correspondance donnés.



Voici les étapes de création des politiques d’adresse dynamique faisant référence aux DAG pour les groupes d’appareils cloud :

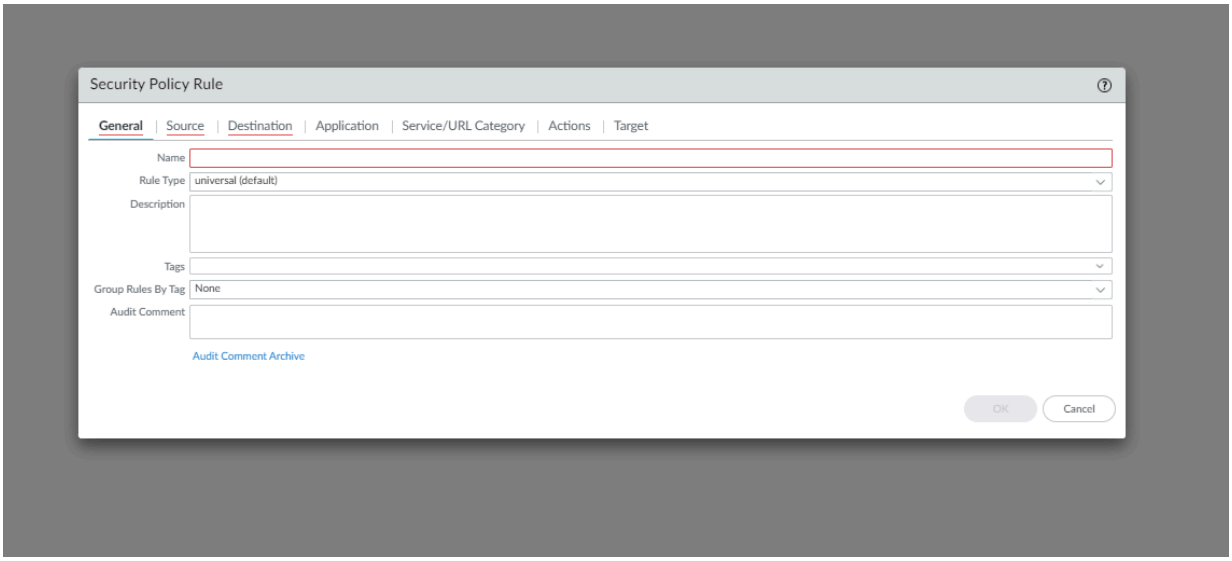
1. Dans la console **Panorama**, accédez à l’onglet **Policies (Politiques)**.

2. Accédez à **Security (Sécurité)** > **Pre/Post/Default Rules (Règles pré/post/par défaut)**.

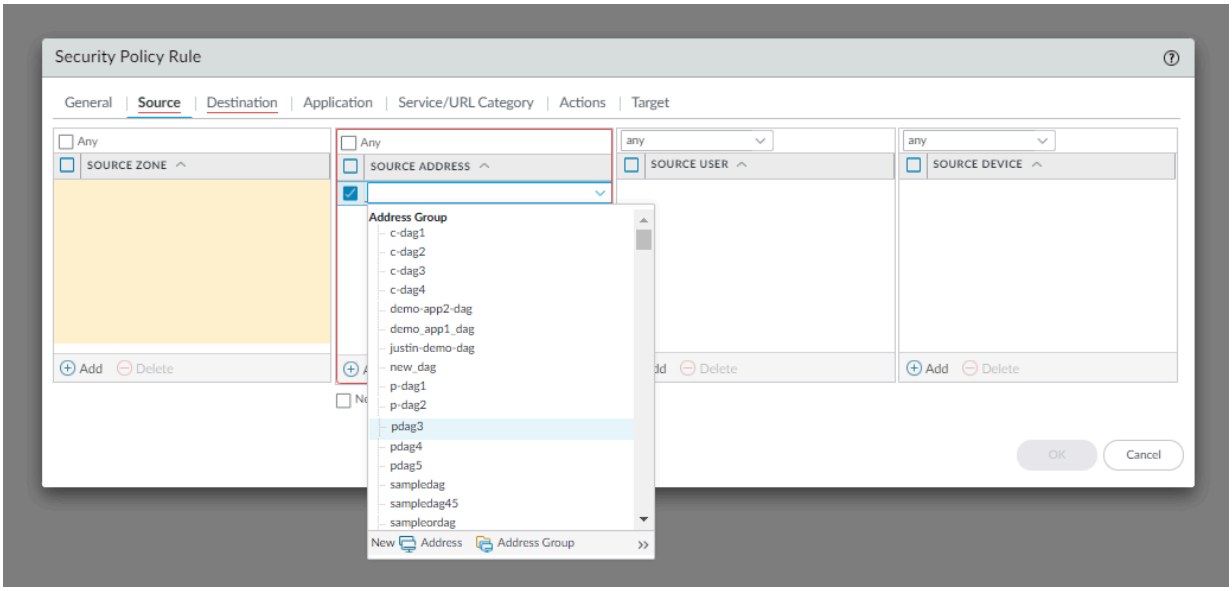


3. Cliquez sur **Add (Ajouter).**

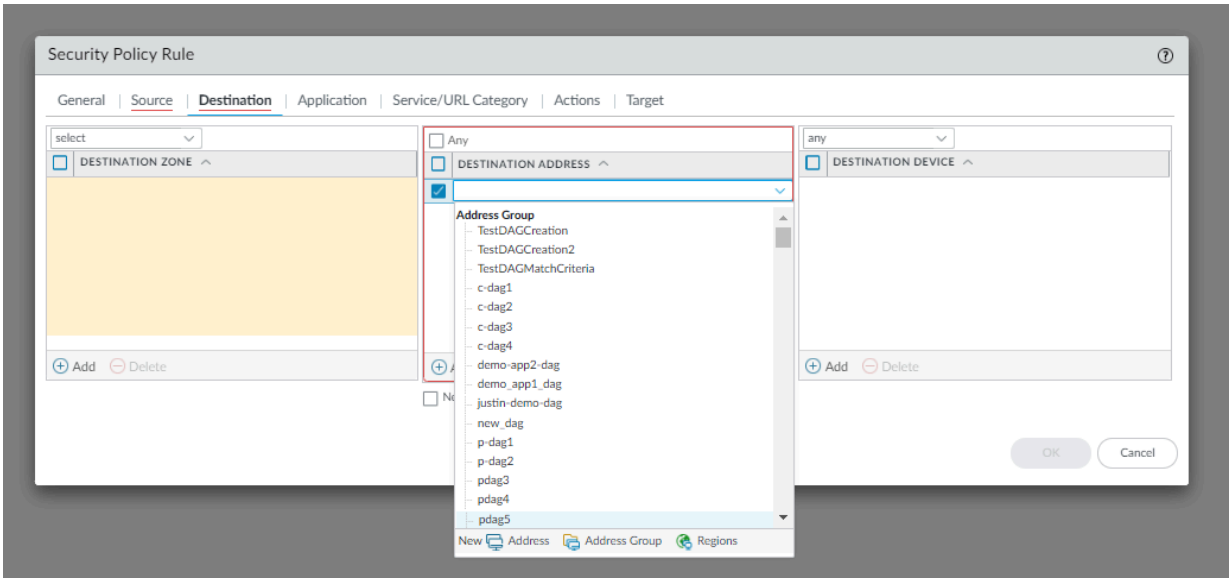
4. Dans la boîte de dialogue Règle de politique de sécurité, saisissez un **Name (Nom)** pour la règle de politique de sécurité.



5. Dans l'onglet **Source** , sélectionnez le DAG du champ **Source Address (Adresse source)** et cliquez sur **Add (Ajouter)**.



6. Dans l'onglet **Destination**, sélectionnez le DAG du **champ Destination Address (Adresse de destination)** et cliquez sur **Add (Ajouter).**

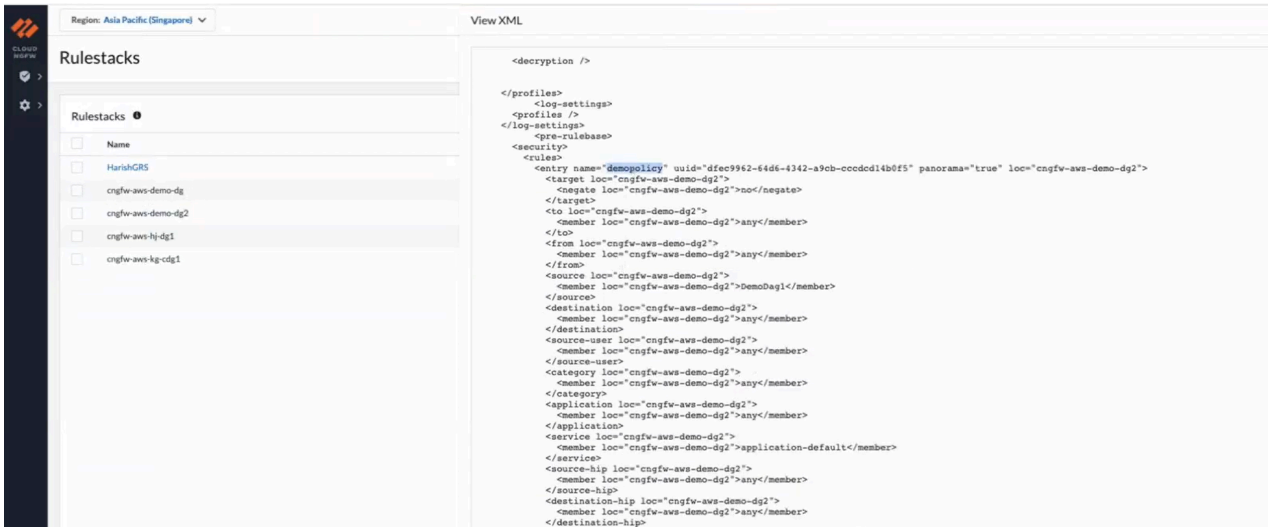


7. Cliquez sur **OK**.
8. **Validez** et **transmettez** vos modifications au groupe d'appareils Cloud NGFW.

Pour plus d'informations sur la **validation** et la **transmission** des modifications de configuration aux pare-feu, consultez la section Preview, Validate, or Commit Configuration Changes (Prévisualisation, validation ou confirmation des modifications de configuration).

Revenez à la console **Cloud NGFW** pour contrôler un fichier XML contenant des politiques d'adresse dynamique transmises de Panorama vers le groupe d'appareils cloud respectif. Cliquer

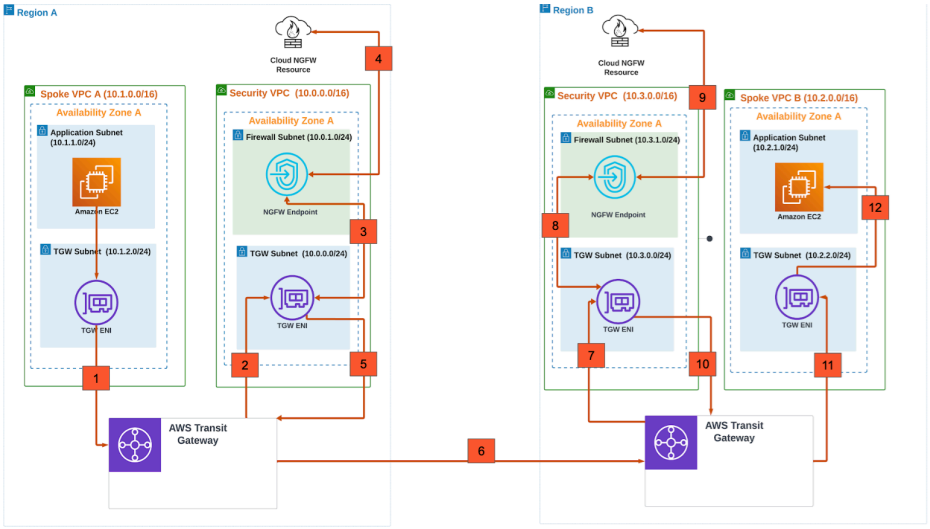
View XML (Afficher XML) pour afficher des informations sur les politiques d'adresses dynamiques récemment ajoutées au groupe d'appareils cloud.



Ajoutez un nouveau sous-réseau au compte client. Pour plus d’informations, consultez la section Create Subnet on AWS console (Créer un sous-réseau sur la console AWS).

Politiques basées sur des étiquettes inter-régions

Vous pouvez renseigner des étiquettes de deux régions différentes dans vos groupes d’appareils cloud.



Par exemple :

La région X et la région Y sont les régions que vous souhaitez activer pour la découverte des étiquettes de ressources AWS. Si la ressource CNGFW est présente dans la région X qui doit apprendre les étiquettes de la région Y, puis l'utiliser pour le cloud DG dans la région X, effectuez les étapes suivantes :

1. Ajoutez des comptes AWS au locataire Cloud NGFW et collectez les étiquettes à partir de ceux-ci.
2. Utilisez le plug-in Panorama pour interroger les étiquettes et ajoutez-les aux groupes d'appareils Panorama.
3. Configurez les objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans les groupes d'appareils.

   Vous ne pourrez voir que les étiquettes de la région X disponibles pour configurer vos objets DAG.
4. Dans la région Y, créez le groupe d'appareils cloud portant le même nom que dans la région X. Validez et transférez vos modifications sur Panorama. Si nécessaire, créez un groupe de VPC et attribuez les VPC appropriés ou utilisez le groupe de VPC par défaut de la région Y.
5. Créez une définition de surveillance dans la région Y, puis sélectionnez le groupe de VPC et le groupe de notification (où le Cloud DG est déjà mappé).
6. Configurez les objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans les groupes d'appareils.

   Vous pouvez maintenant voir que les étiquettes de la région X et de la région Y sont disponibles pour configurer vos objets DAG.
7. **Validez** la configuration dans Panorama.

Dans le groupe d'appareils cloud, vous pouvez désormais voir les étiquettes de la région Y à configurer et vous pouvez créer un groupe d'adresses dynamiques.

Intégration de la prévention des pertes de données d’entreprise (E-DLP) avec Cloud NGFW pour AWS

La prévention des pertes de données d’entreprise (E-DLP) est un ensemble d’outils et de processus qui vous permettent de protéger les informations sensibles de tout accès, mauvaise utilisation, extraction ou partage non autorisés. Pour plus d’informations, consultez À propos de la DLP d’entreprise.

Vous pouvez intégrer E-DLP à Cloud NGFW pour AWS et utiliser la console Panorama pour ajouter des profils de filtrage des données à vos règles de politique de sécurité.

Configuration minimale requise pour l’intégration E-DLP

Voici la combinaison des exigences de Panorama et de la version du plug-in Panorama pour l’intégration d’E-DLP à votre service Cloud NGFW :

Version Panorama (PAN-OS)	Plug-in DLP	Plug-in AWS
10.0.2 et supérieure	1.0.9	5.2.0
10.2.4 et supérieure	3.0.7	5.2.0
11.0.2 et supérieure	4.0.3	5.2.0
11.1.0 et supérieure	5.0.1	5.2.0

Approvisionnement d’un nouveau locataire E-DLP sur Cloud NGFW pour AWS

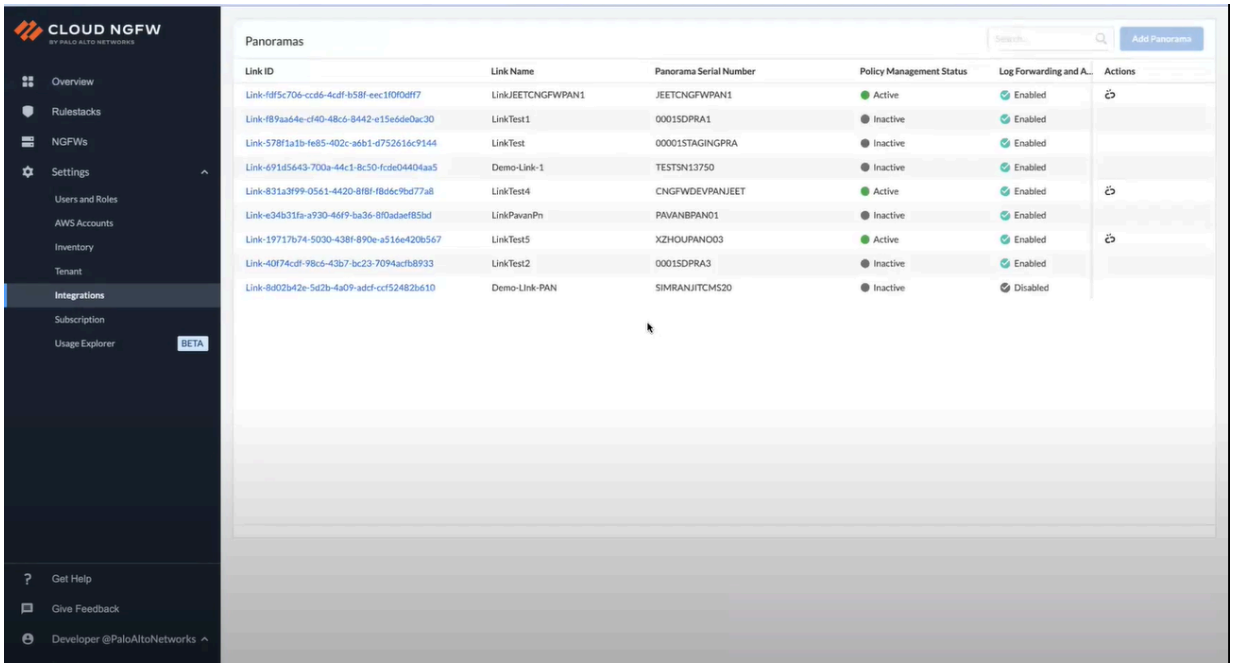
Si vous avez un locataire DLP existant sur votre compte du portail de support client (CSP) approvisionné dans Panorama, le service Cloud NGFW utilisera ce locataire DLP pour intégrer DLP à Cloud NGFW.

Si vous n’avez pas de locataire DLP sur votre compte du portail de support client, le service Cloud NGFW créera un nouveau locataire DLP.

Voici les étapes à suivre pour activer un nouveau locataire DLP sur la console Cloud NGFW :

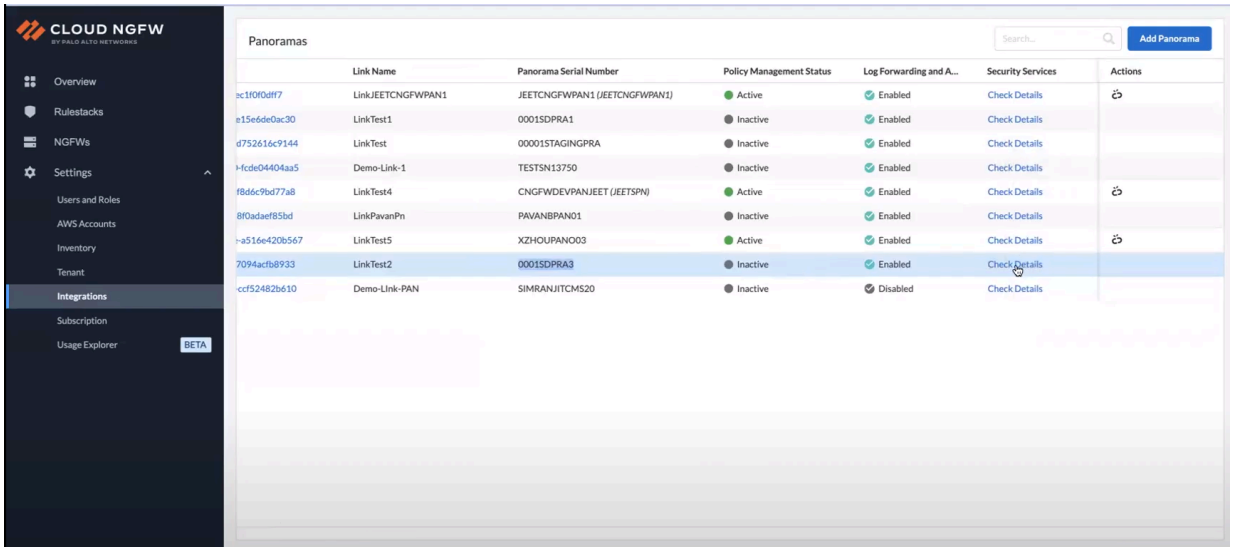
1. Connectez-vous à la console Cloud NGFW.

2. Sélectionnez **Integrations (Intégrations)**.



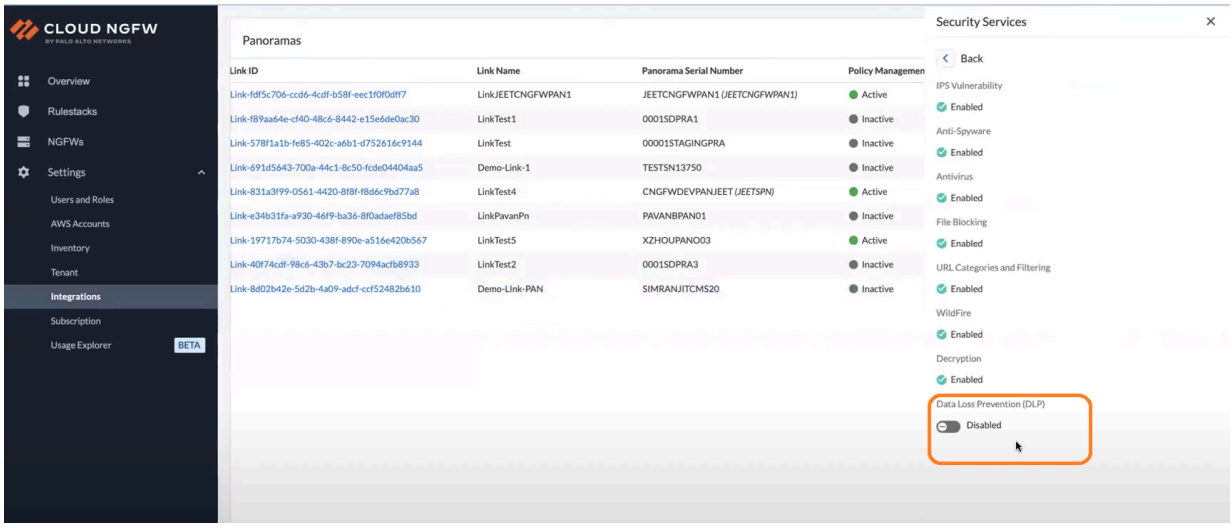
La page **Integrations (Intégrations)** affiche des informations sur le Panorama actuellement lié.

3. Dans la colonne Security Service (Service de sécurité), cliquez sur **Check Details (Vérifier les détails)**.

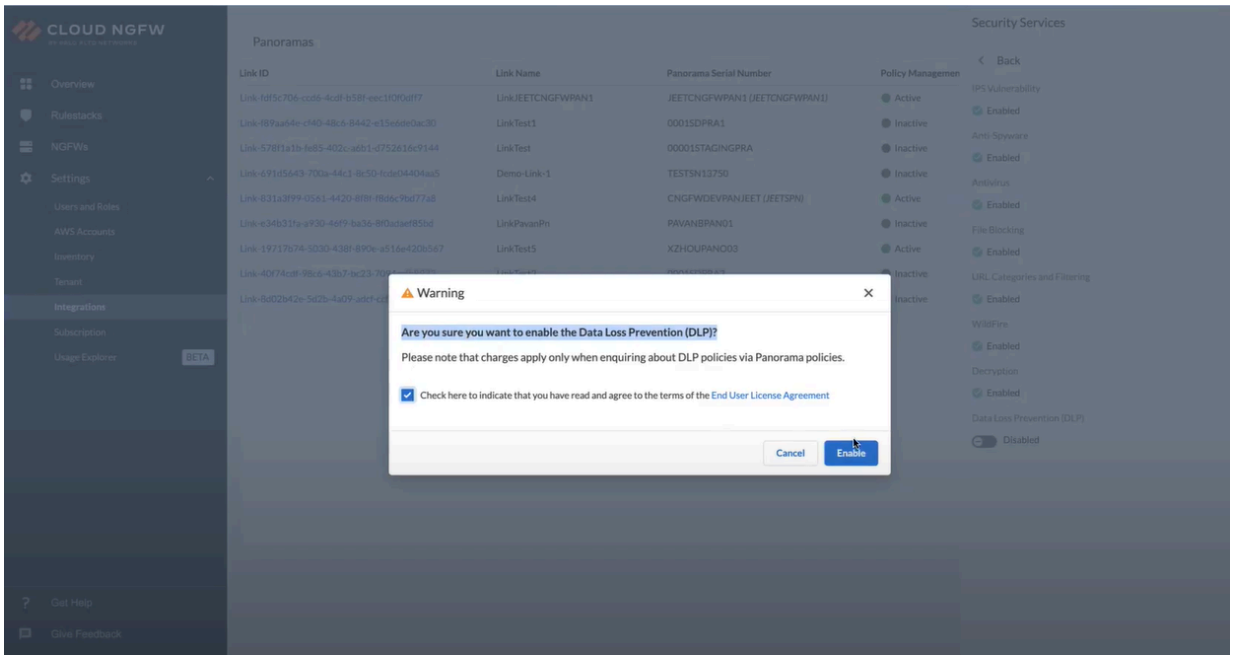


Vous pouvez également cliquer sur **Link ID (ID de lien)** d'un Panorama lié, puis cliquer sur **Check Details (Vérifier les détails)**.

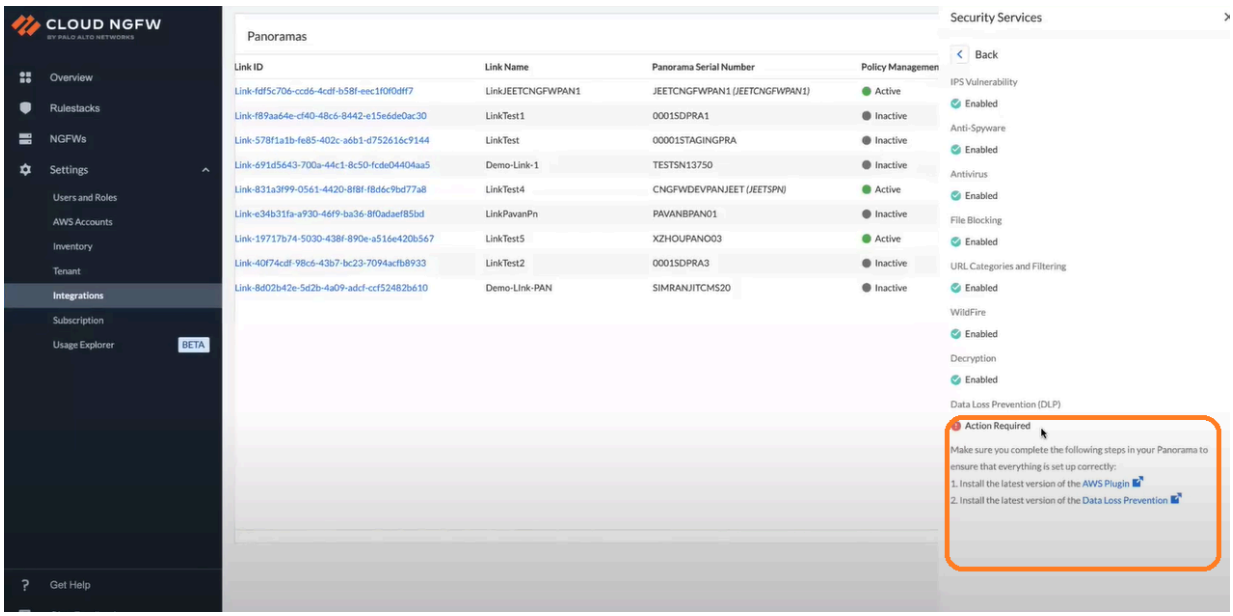
4. Dans le panneau **Security Services (Services de sécurité)**, cliquez sur la bascule **Data Loss Prevention (Prévention des pertes de données – DLP)**.



5. Sélectionnez la case à cocher pour accepter le **End User License Agreement (Contrat de licence utilisateur final)**, puis cliquez sur **Enable (Activer)**.



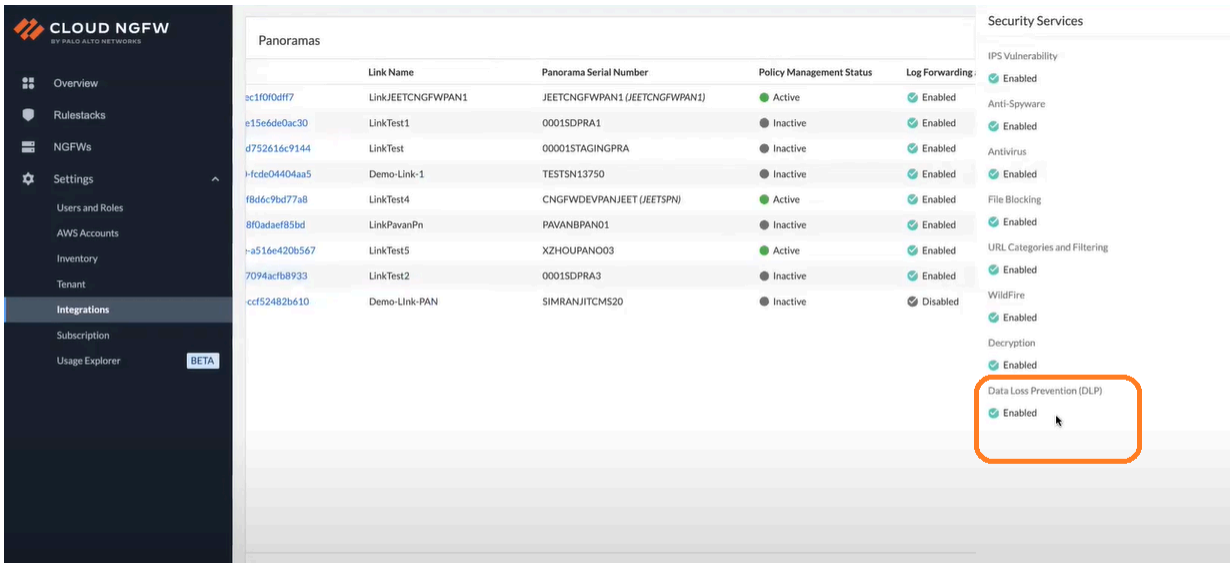
Passez en revue l'**Action Required (Action requise)** sur le panorama lié.



6. Vérifiez que le Panorama lié satisfait la configuration système minimale requise pour intégrer DLP à votre service Cloud NGFW**.**

   Après avoir installé le plug-in AWS et DLP requis sur votre Panorama, le locataire DLP sur une console Cloud NGFW est activé.

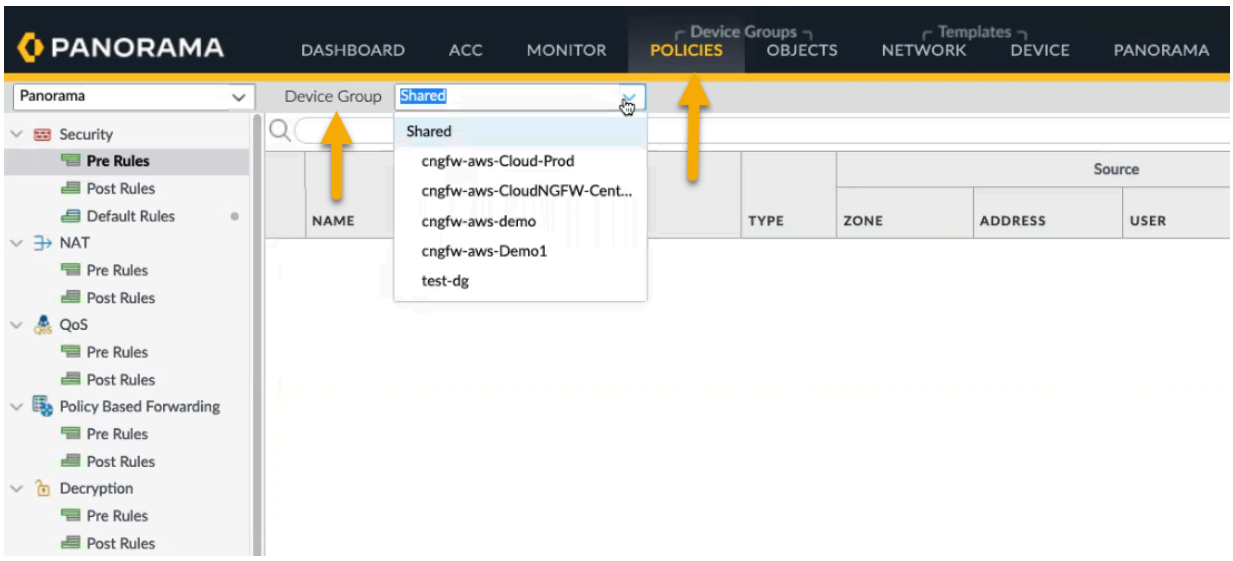
   Sur la console Cloud NGFW, accédez à la page **Integrations (Intégrations)**, sélectionnez Panorama lié, puis cliquez sur **Check Details (Vérifier les détails)** sous la colonne **Security Services (Services de sécurité)**.



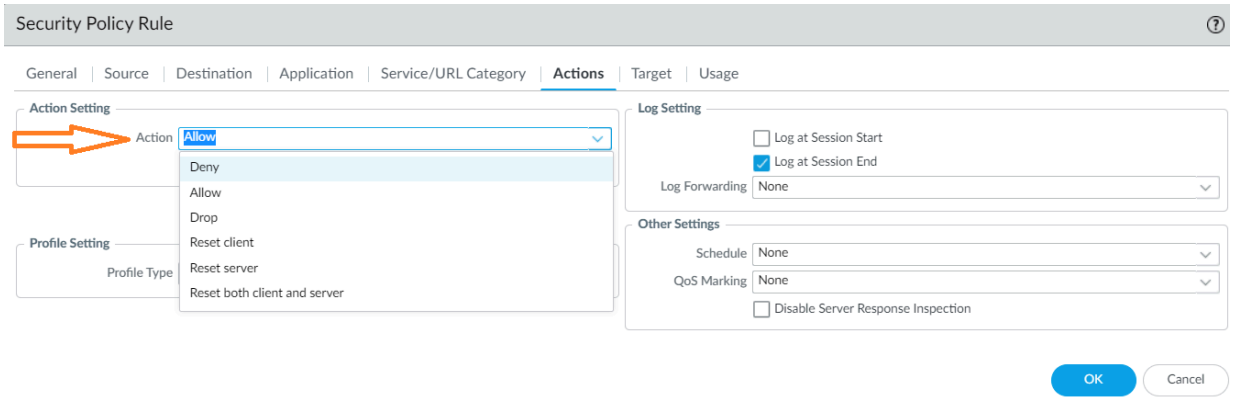
   Vous pouvez désormais voir que **Data Loss Prevention (prévention des pertes de données – DLP)** est activé.

   Une fois que vous avez activé le locataire DLP sur la console Cloud NGFW avec succès , les pare-feu associés au Panorama lié peuvent commencer à utiliser les services DLP.

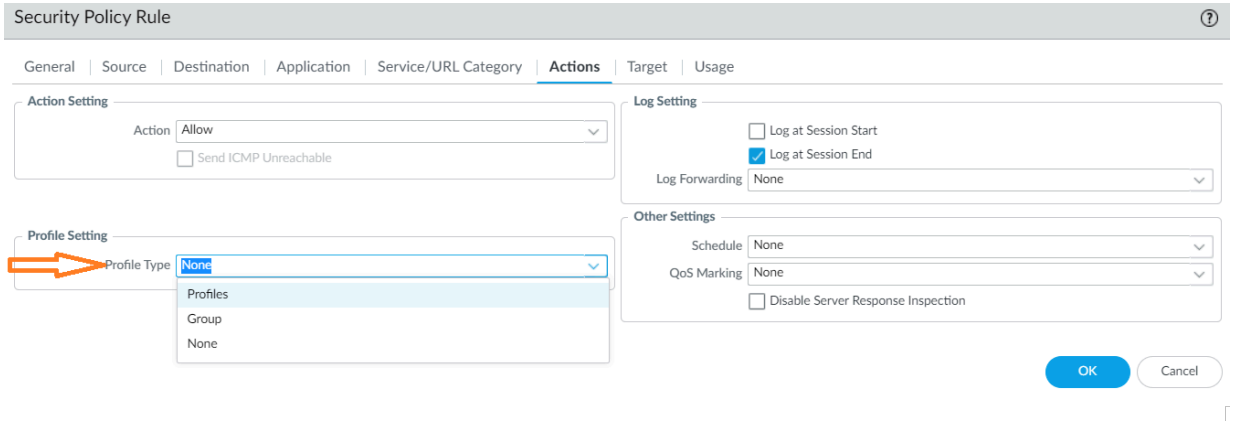
   Vous pouvez ajouter un profil de filtrage DLP à votre **Security Policy Rule (Règle de politique de sécurité)** pour votre pare-feu dans Panorama.



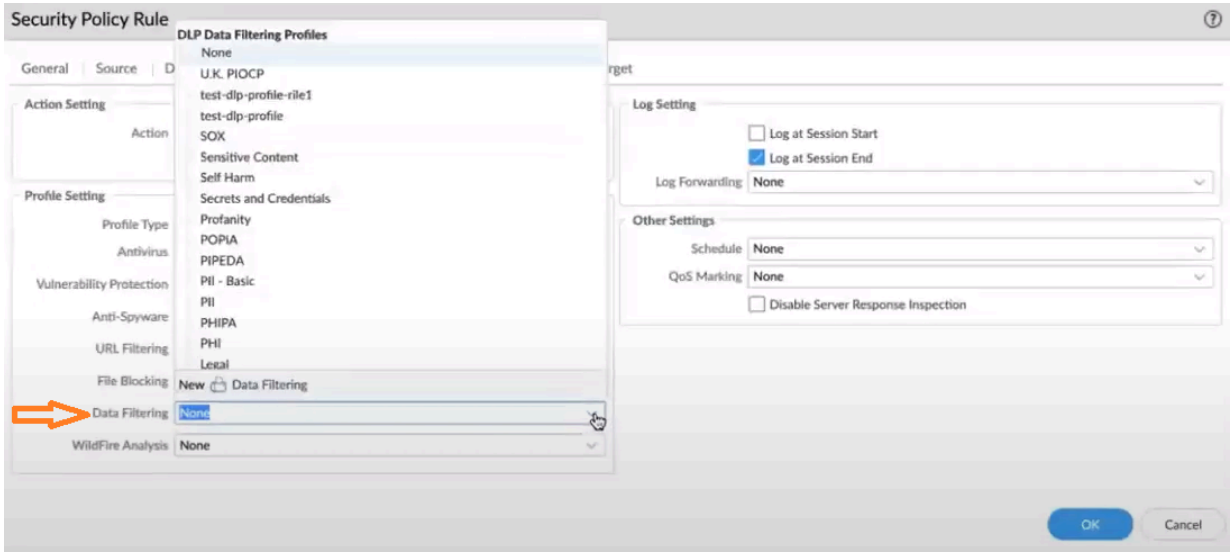
Surs l'écran **Security Policy Rule (Règle de politique de sécurité)**, accédez à l'onglet **Actions**, puis sélectionnez l'action à appliquer (par exemple, autoriser ou refuser).



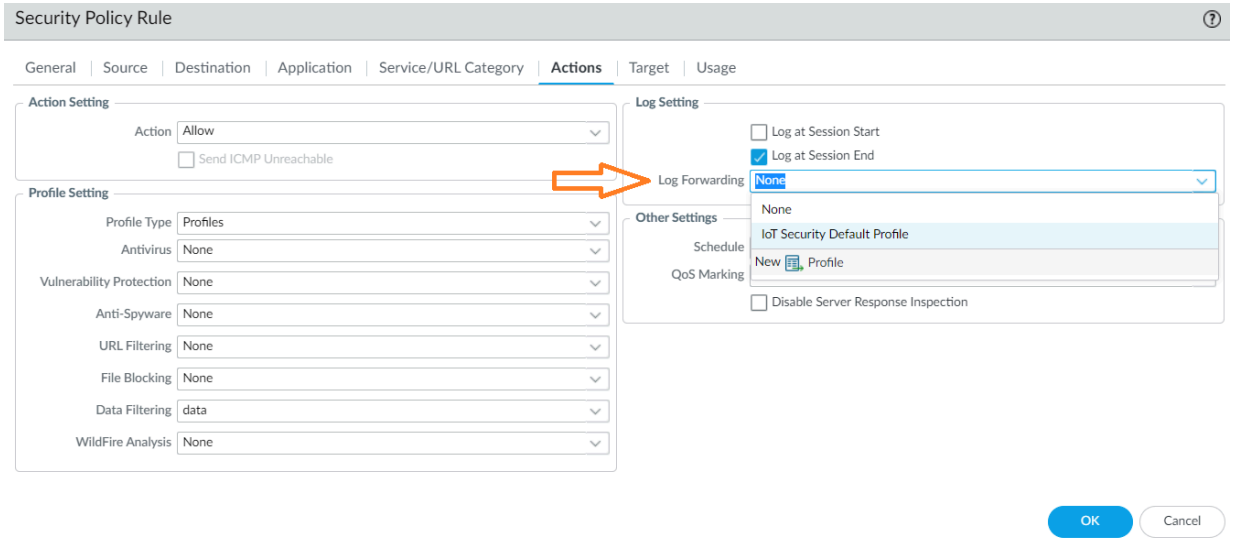
Déterminez les **Profile Setting (Paramètres du profil)**.



Sélectionnez un **Data Filtering profile (Profil de filtrage des données) DLP**.

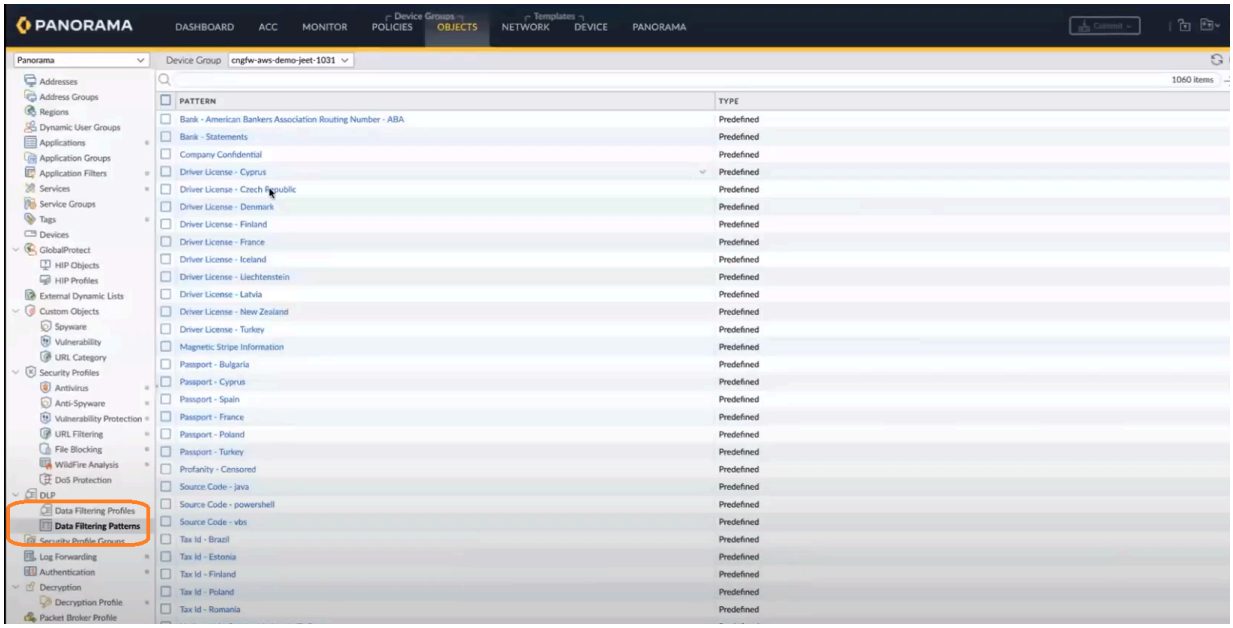


Configurez les **Log Setting (Paramètres des journaux)** et d’autres paramètres.



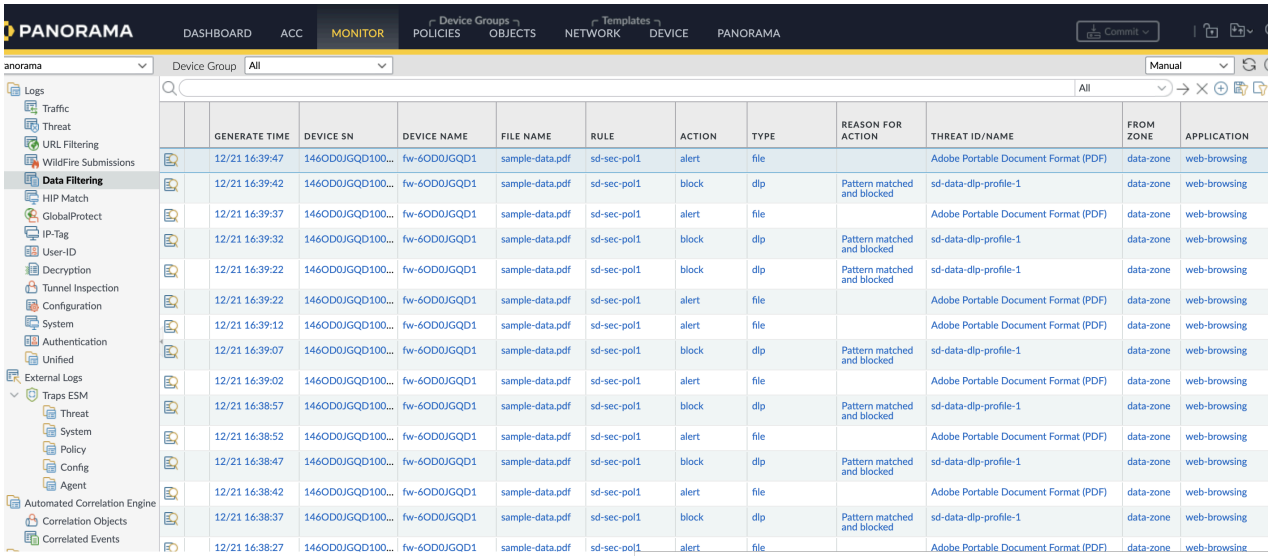
Pour plus d'informations, consultez Utiliser Panorama pour la gestion des politiques de Cloud NGFW.

Après avoir transmis la règle de politique de sécurité à votre pare-feu, vous pouvez afficher les profils de filtrage des données et les modèles de filtrage des données existants que vous pouvez utiliser pour votre locataire DLP.

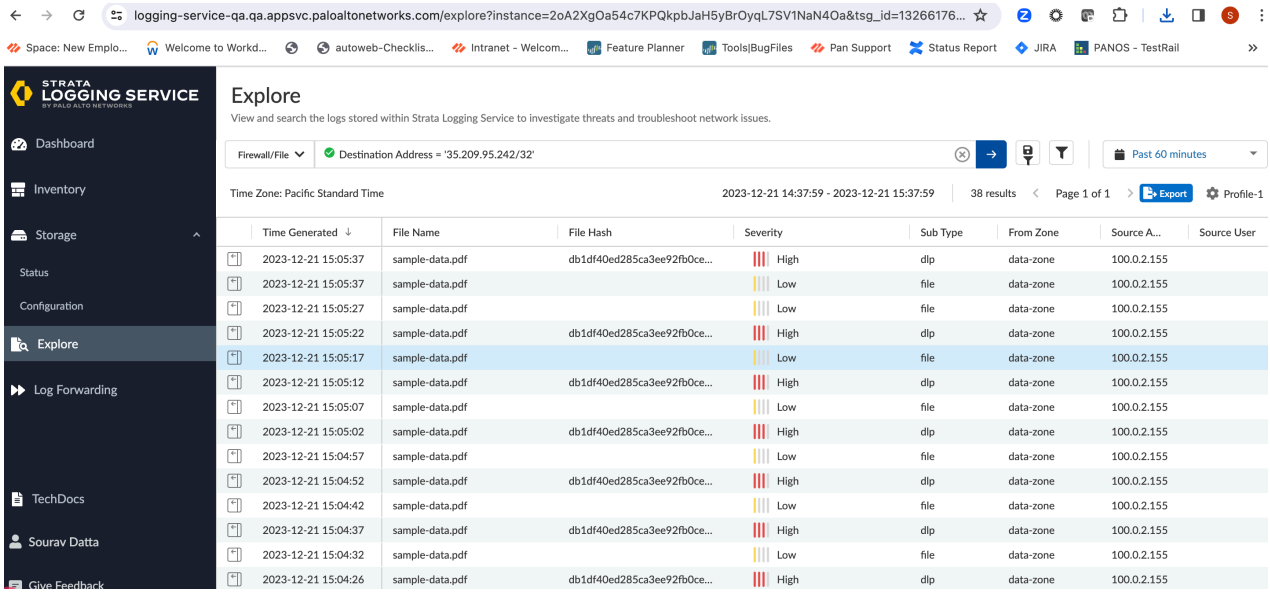


Surveillance des détails des journaux DLP

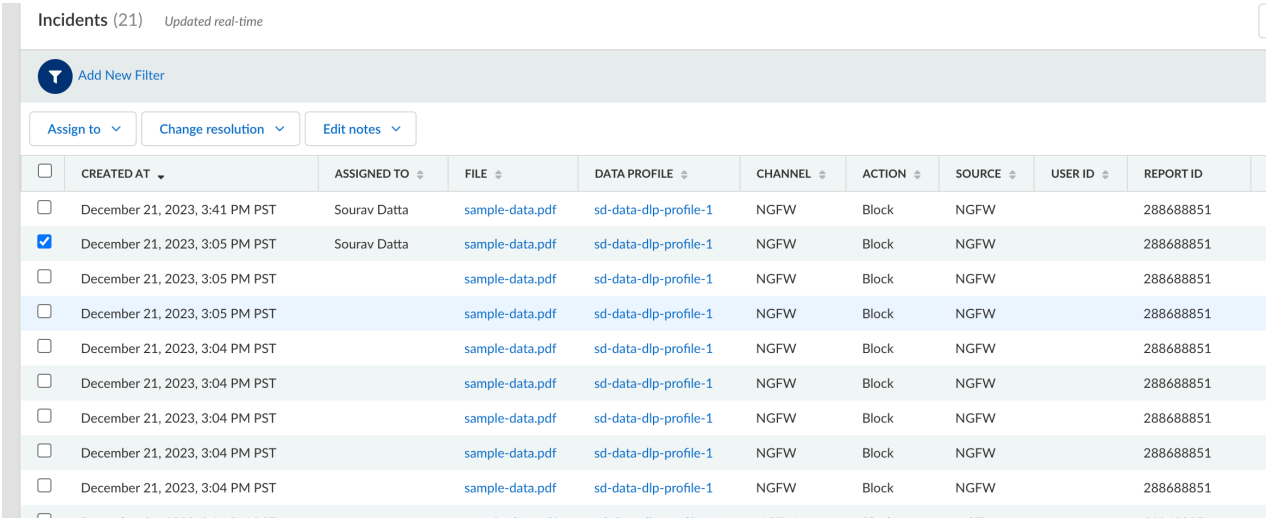
Pour afficher vos journaux DLP dans Panorama, cliquez sur l’onglet **Monitor (Surveiller)** , puis accédez à **Logs (Journaux)** > **Data Filtering (Filtrage des données)**. Pour plus d’informations, consultez Afficher les détails des journaux DLP d’entreprise sur Panorama.



Pour afficher vos journaux CDL pour DLP, accédez à l'onglet **Explore (Explorer)** et sélectionnez l'option **Firewall or File (Pare-feu ou Fichier)**. Pour plus d'informations, consultez Afficher les détails des journaux sur CDL.



Pour afficher les journaux des incidents de vos locataires DLP sur SCM, consultez Afficher les détails des journaux DLP d’entreprise sur Strata Cloud Manager.



Incidents (21) *Updated real-time*

Add New Filter

Assign to | Change resolution | Edit notes

	CREATED AT	ASSIGNED TO	FILE	DATA PROFILE	CHANNEL	ACTION	SOURCE	USER ID	REPORT ID
☐	December 21, 2023, 3:41 PM PST	Sourav Datta	sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☑	December 21, 2023, 3:05 PM PST	Sourav Datta	sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:05 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:05 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:04 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:04 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:04 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:04 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851
☐	December 21, 2023, 3:04 PM PST		sample-data.pdf	sd-data-dlp-profile-1	NGFW	Block	NGFW		288688851

Pour plus d’informations sur les destinations AWS sur les journaux DLP, consultez Journaux Amazon CloudWatch.

Gestion des politiques de Strata Cloud Manager

Vous pouvez relier votre ressource Cloud NGFW à Strata Cloud Manager (SCM) pour la gestion des politiques. Strata Cloud Manager offre une gestion unifiée pour l'ensemble de votre déploiement de sécurité réseau, ce qui vous permet de gérer facilement votre infrastructure de sécurité Palo Alto Networks à partir d'une interface utilisateur unique et simplifiée. Avec cette interface, vous bénéficiez d'une visibilité complète sur les utilisateurs, les sites de succursales, les applications et les menaces sur tous les points d'application de la sécurité du réseau. Cette fonctionnalité fournit des informations exploitables, une meilleure sécurité et une facilité de dépannage et de résolution des problèmes.

Lorsque vous utilisez SCM pour la gestion des politiques Cloud NGFW, tenez compte des éléments suivants :

- Lors de la première connexion à SCM, les ressources Cloud NGFW (par exemple, ID de la ressource) peuvent ne pas s'afficher. Ces ressources s'afficheront après quelques instants s'il n'y a pas de problèmes de connexion sous-jacents.
- Les bonnes pratiques pour la gestion des politiques Cloud NGFW SCM sont différentes de celles qui utilisent la gestion des politiques Panorama avec votre ressource Cloud NGFW. Par exemple, une partie du trafic transitant par un environnement géré par Panorama peut être supprimée dans une ressource Cloud NGFW gérée par SCM.
- La fonctionnalité X-transféré n'est pas prise en charge dans une gestion de politique SCM pour votre ressource Cloud NGFW.
- Le certificat cloud n'est pas pris en charge.
- DLP n'est pas pris en charge.
- Lors de la configuration des règles de sécurité pour votre ressource Cloud NGFW gérée par SCM, vous devez spécifier **ANY** pour la règle de sécurité. Cependant, la zone **from/to (de/à)** apparaît comme la **data zone (zone de données)** dans le service de journalisation de Strata.

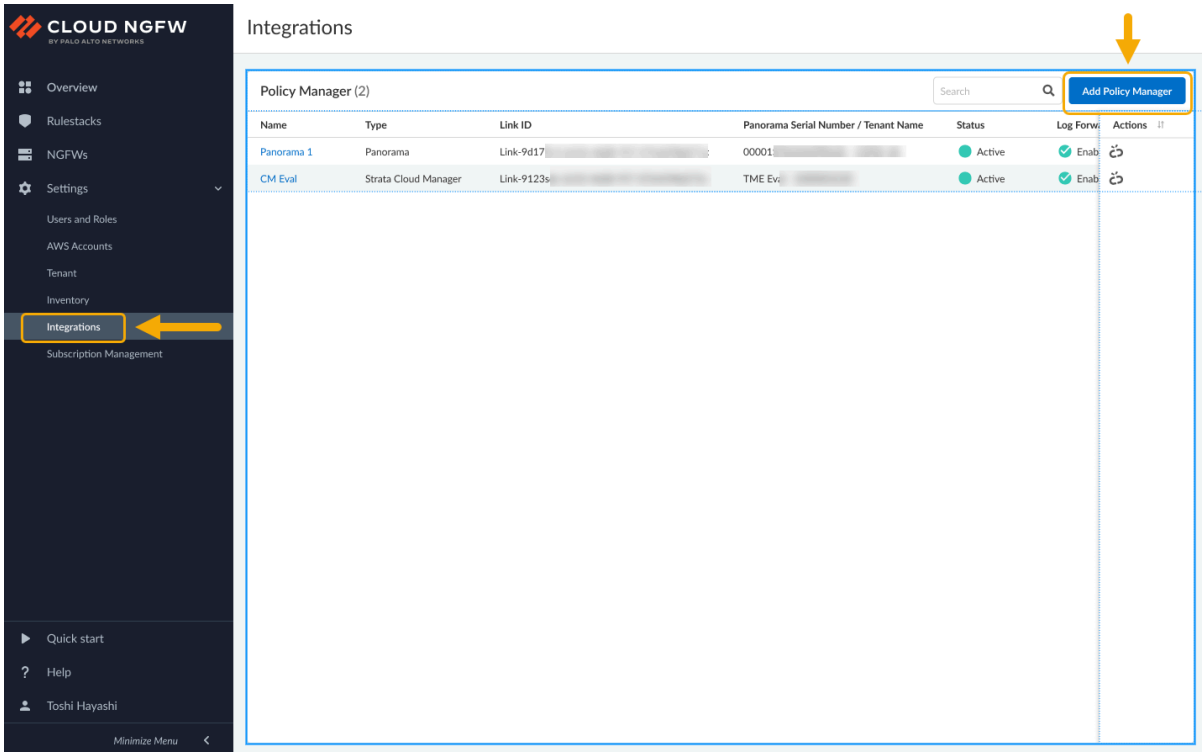
Lier votre ressource Cloud NGFW à la gestion des politiques de Strata Cloud Manager

Pour intégrer votre ressource Cloud NGFW à la gestion des politiques de Strata Cloud Manager :

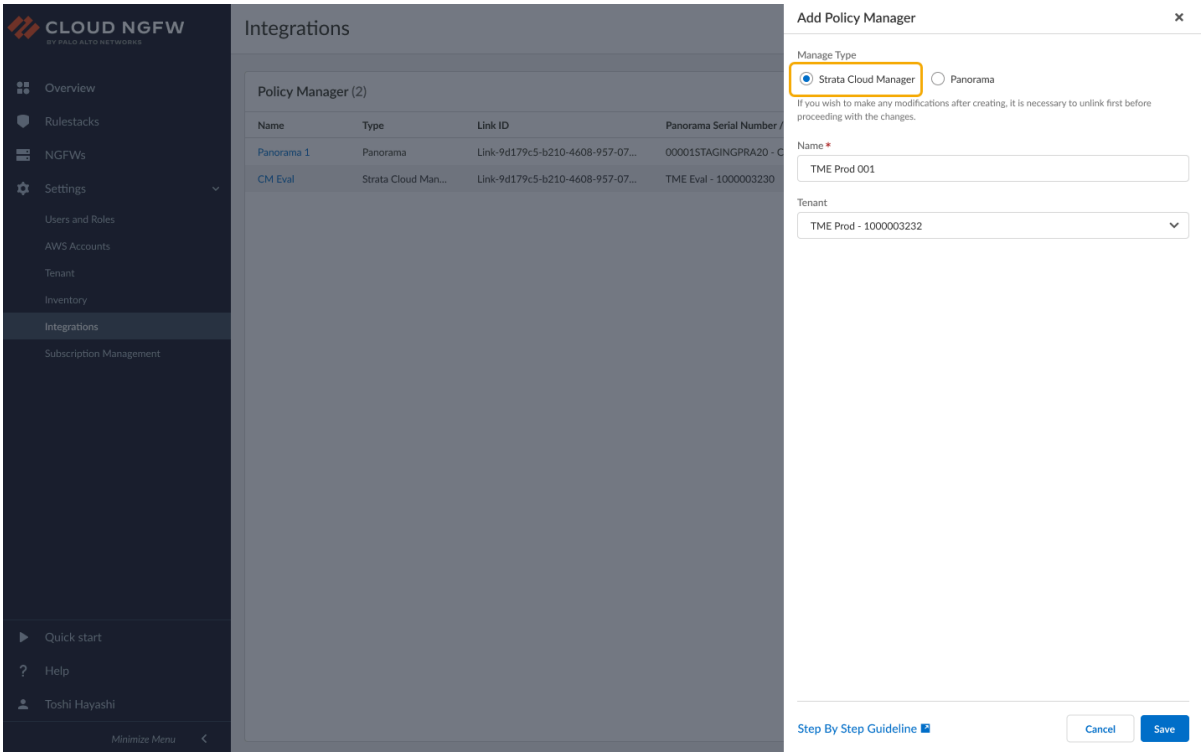
STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sélectionnez **Integrations (Intégrations)**.

STEP 3 | Dans l’écran **Policy Manager (Gestionnaire de politique)**, cliquez sur **Add Policy Manager (Ajouter un gestionnaire de politiques)**.



STEP 4 | Dans la section **Add Policy Manager (Ajouter un gestionnaire de politiques)**, sélectionnez **Strata Cloud Manager** pour le **Manage Type (Type de gestion)**.



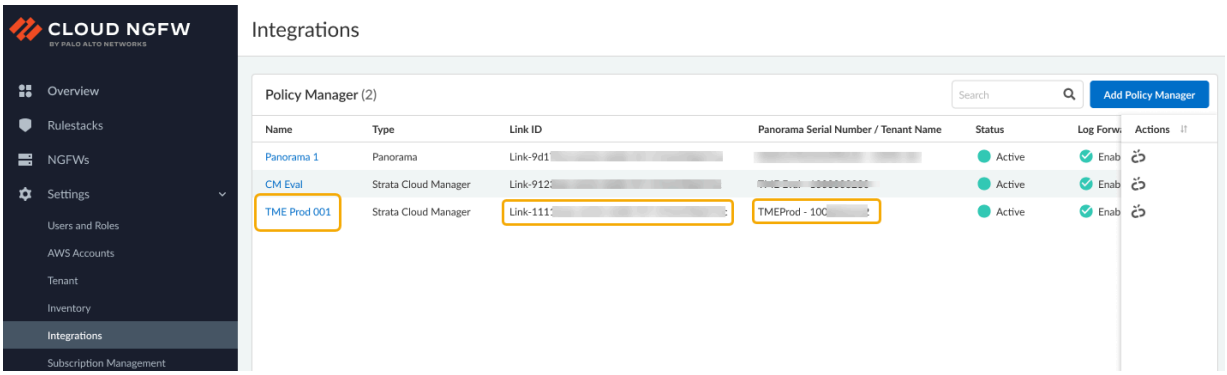
STEP 5 | Saisissez un nom descriptif.

STEP 6 | Utilisez le menu déroulant pour sélectionner le **Tenant (Locataire)** SCM que vous souhaitez associer à la ressource.

Le compte du portail de support client (CSP) doit être le même pour SCM et CNGFW.

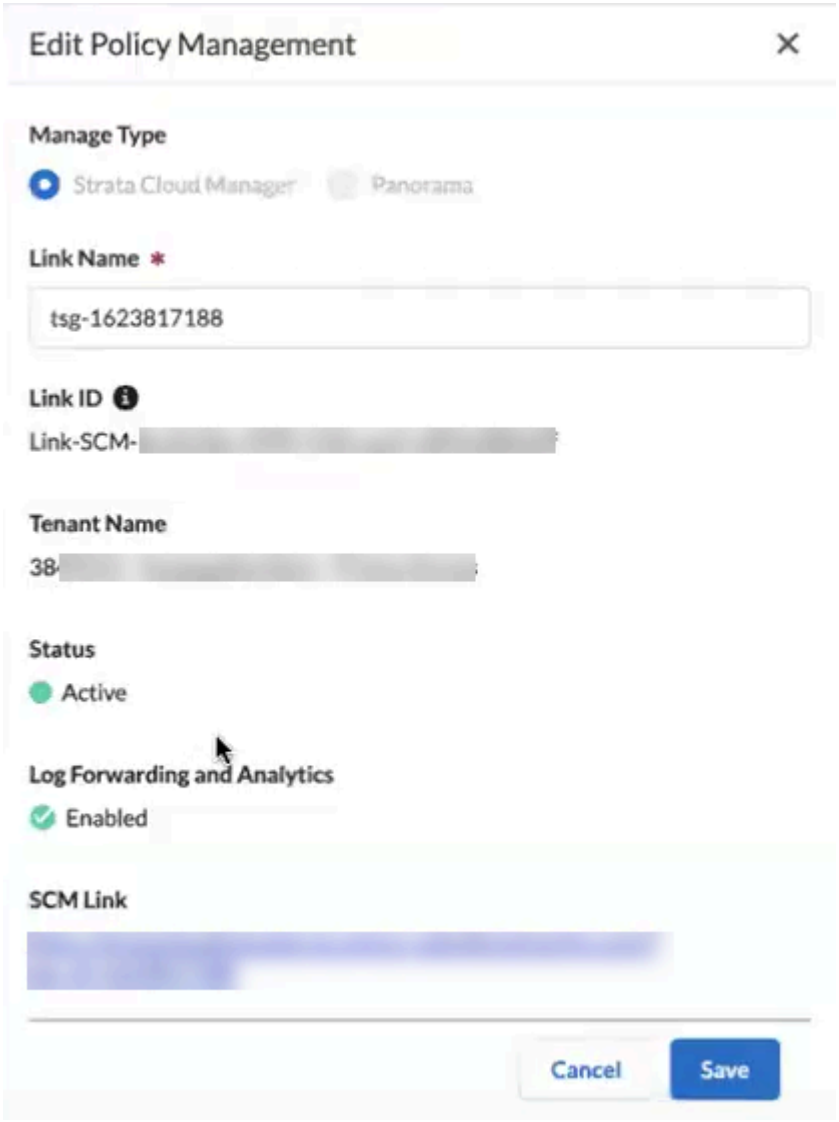
STEP 7 | Cliquez sur **Save (Enregistrer)**. Cela permet de relier efficacement votre ressource Cloud NGFW au locataire SCM.

Après l'enregistrement de la configuration, la page **Integrations (Intégrations)** est mise à jour pour refléter le nouveau paradigme de gestion des politiques, ainsi que l'ID de lien et le numéro de série/ nom du locataire SCM associés :



Pour afficher des informations sur un locataire SCM lié individuel, cliquez sur **Link ID (ID de lien)** dans l'écran **Policy Manager (Gestionnaire de politiques)**. Vous pouvez utiliser l'écran **Edit Policy**

Management (Modifier la gestion des politiques) pour modifier le **Link Name (Nom du lien)** et afficher les informations :



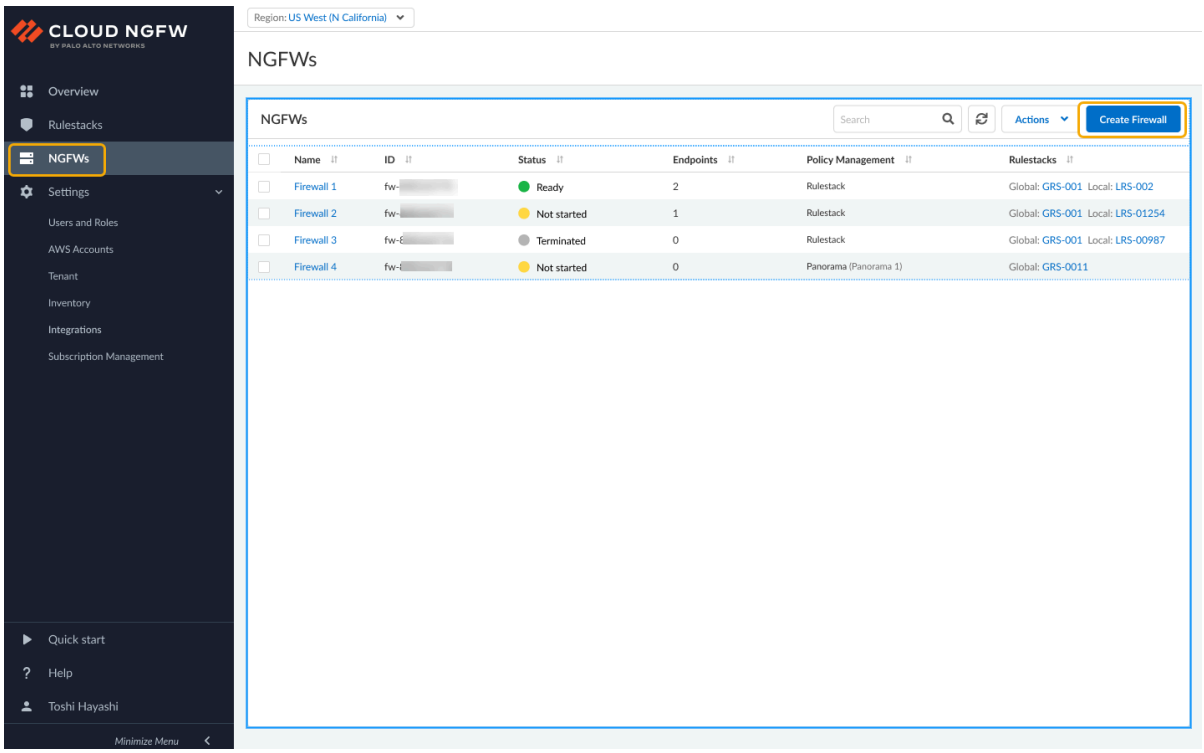
Associer un pare-feu à la gestion des politiques de Strata Cloud Manager

Après avoir établi un lien vers la gestion des politiques Strata Cloud, vous pouvez associer un nouveau pare-feu avec le locataire SCM lié :

STEP 1 | Connectez-vous à la console Cloud NGFW.

STEP 2 | Sélectionnez **NGFWs (NGFW)**.

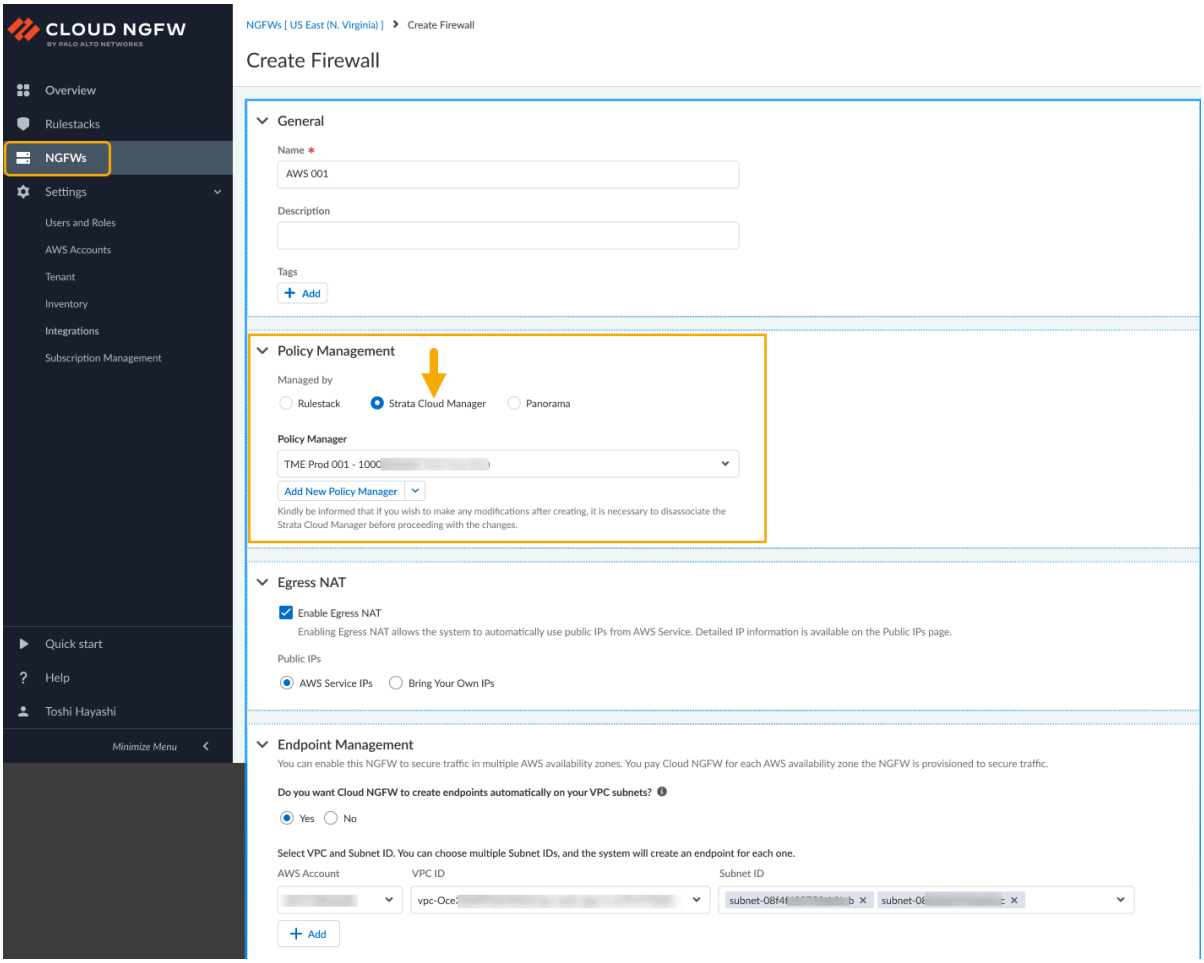
STEP 3 | Cliquez sur **Create Firewall (Créer un pare-feu)**.



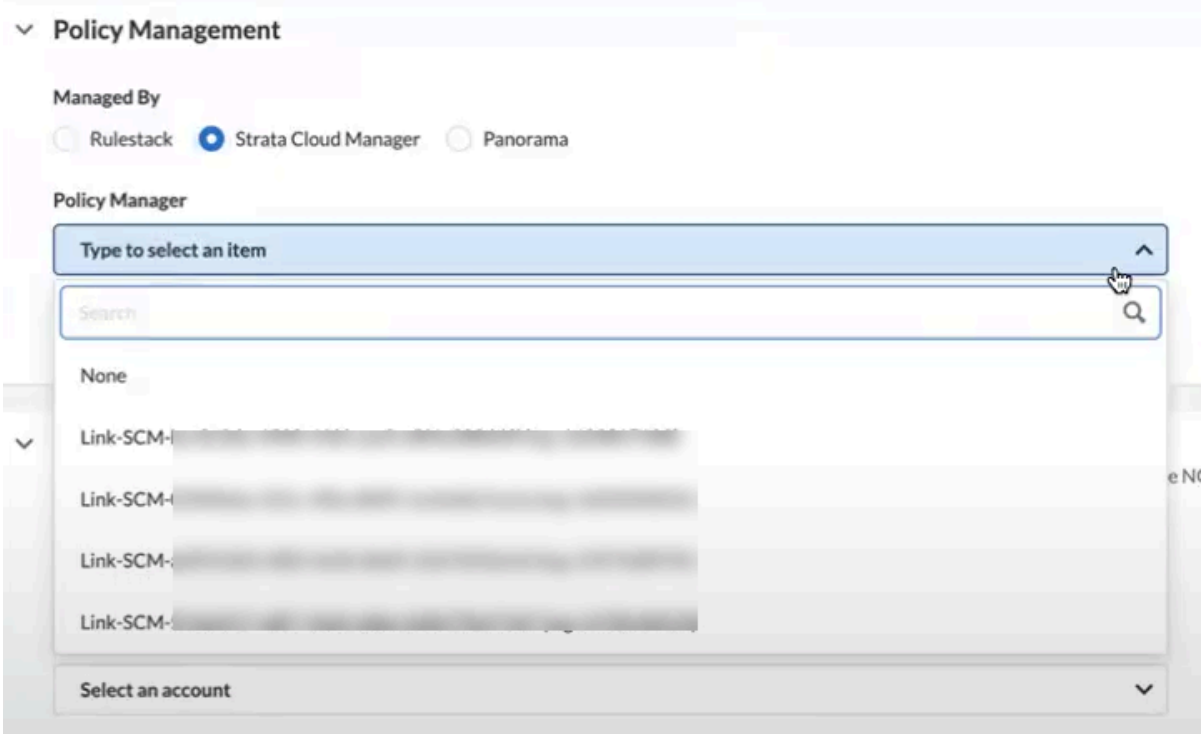
STEP 4 | Dans l’écran **Create Firewall (Créer un pare-feu)**, saisissez un nom pour le pare-feu.

STEP 5 | Vous pouvez également inclure une description.

STEP 6 | Dans la section **Policy Management (Gestion des politiques)**, sélectionnez **Strata Cloud Manager**.



STEP 7 | Dans le menu déroulant **Policy Manager (Gestionnaire de politiques)**, sélectionnez le locataire SCM lié que vous souhaitez associer au pare-feu.



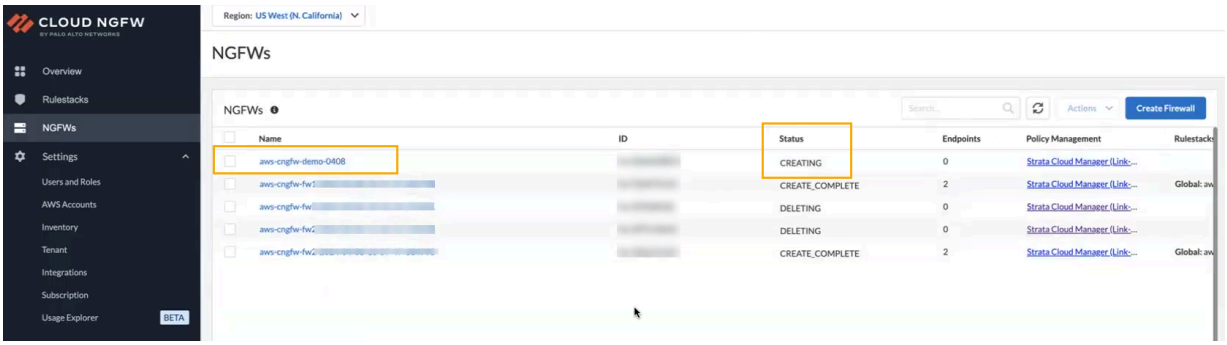
STEP 8 | Configurez **Endpoint Management (Gestion des terminaux)** pour sécuriser le trafic dans plusieurs zones de disponibilité AWS.

1. Déterminez si vous souhaitez que Cloud NGFW crée automatiquement des terminaux sur vos sous-réseaux VPC. Sélectionnez **Yes (Oui)** *pour les terminaux gérés par le service*.

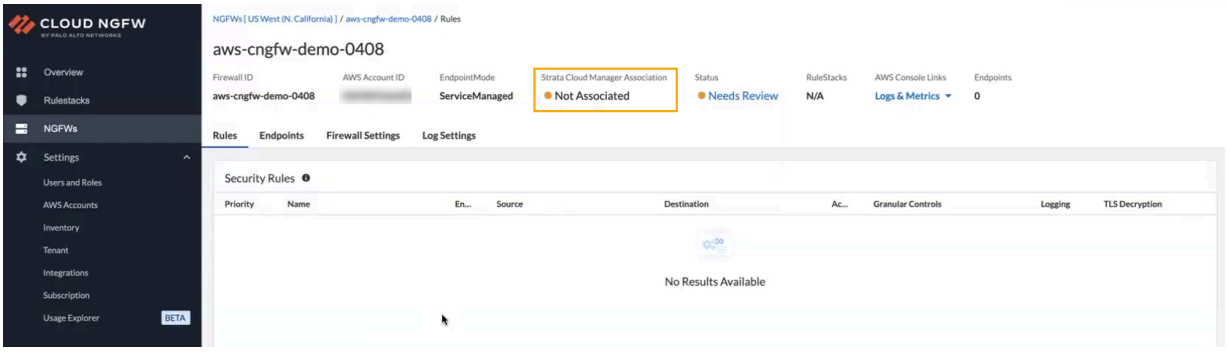
   Par défaut, la ressource Cloud NGFW ne crée pas ces terminaux automatiquement ; le bouton radio est réglé sur ***No (Non).***

2. Utilisez la liste déroulante pour sélectionner **AWS Account ID (ID de compte AWS)**.
3. Utilisez la liste déroulante pour sélectionner le **VPC**.
4. Utilisez le champ **Subnet (Sous-réseau)** pour sélectionner un sous-réseau disponible.
5. Cliquez sur **Save (Enregistrer)**.

L'écran NGFW change pour refléter le pare-feu nouvellement créé. Le processus de création d'un nouveau pare-feu prend environ 6 à 10 minutes ; le **Status (État)** indique **CREATING (EN COURS DE CRÉATION)** :



Cliquez sur le **NGFW Name (Nom NGFW)** pour afficher des informations détaillées sur le pare-feu. Il convient de noter que les informations qui s'affichent lors de la création du pare-feu sont limitées :



Afficher le pare-feu dans Strata Cloud Manager

Après avoir lié votre ressource Cloud NGFW à un locataire SCM et créé un pare-feu, vous pouvez utiliser SCM pour la gestion des politiques.

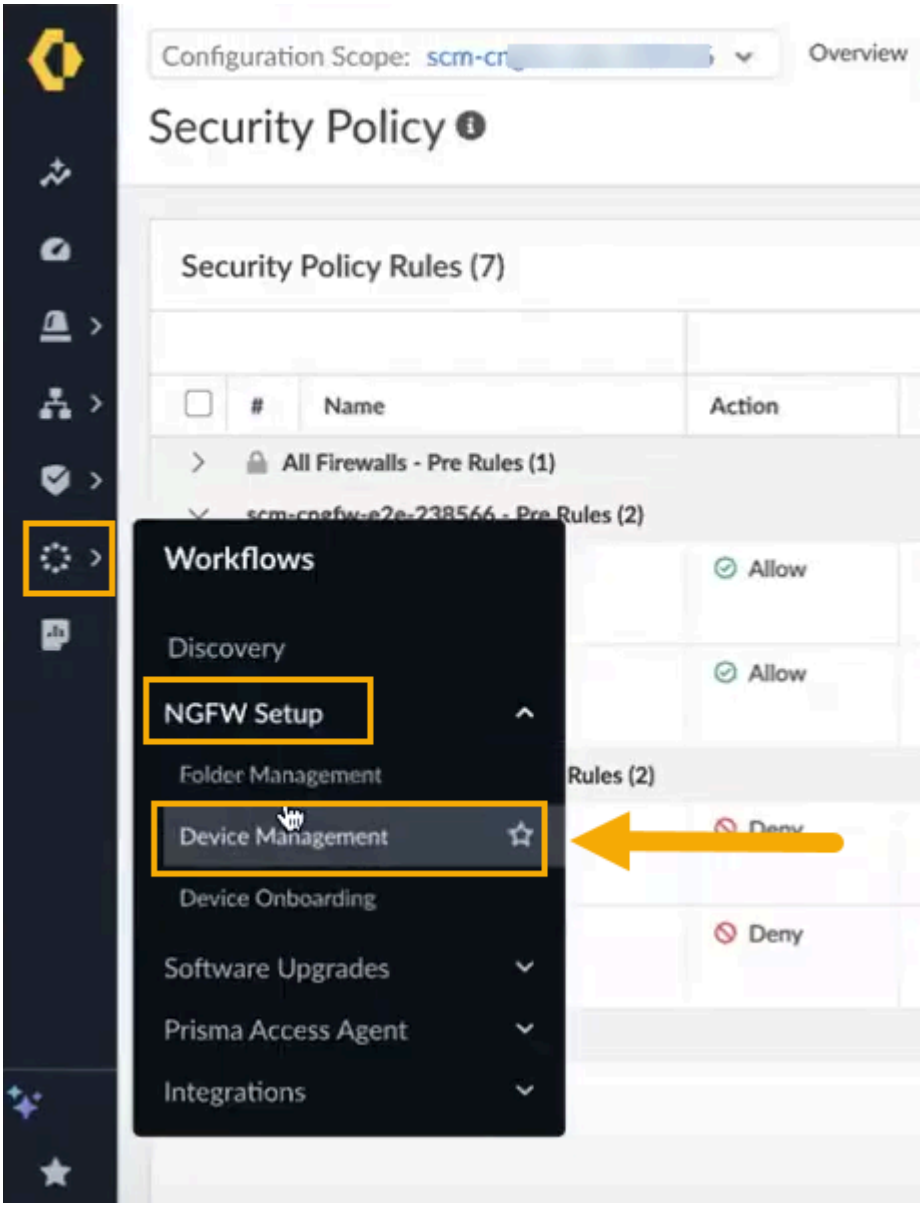
Quand vous vous connectez à Strata Cloud Manager, le tableau de bord ne parvient pas à afficher le nombre de Cloud NGFW sous ***NGFW > Software (Logiciel)***.

STEP 1 | Connectez-vous à l'application Strata Cloud Manager depuis le hub Palo Alto Networks directement sur le site stratacloudmanager.paloaltonetworks.com.

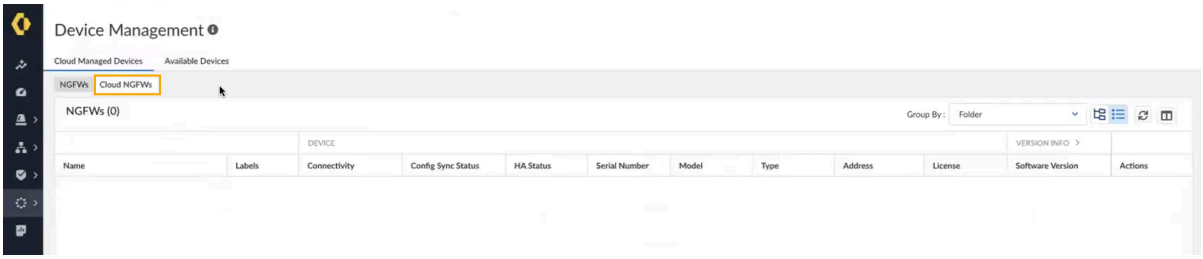
STEP 2 | Dans l’interface Strata Cloud Manager, recherchez votre locataire Cloud NGFW en utilisant l’option de navigation de gauche :

Les locataires disponibles liés à votre ressource Cloud NGFW s'affichent. Vous pouvez également rechercher le locataire à l'aide du *nom du locataire* ou son *identifiant*.

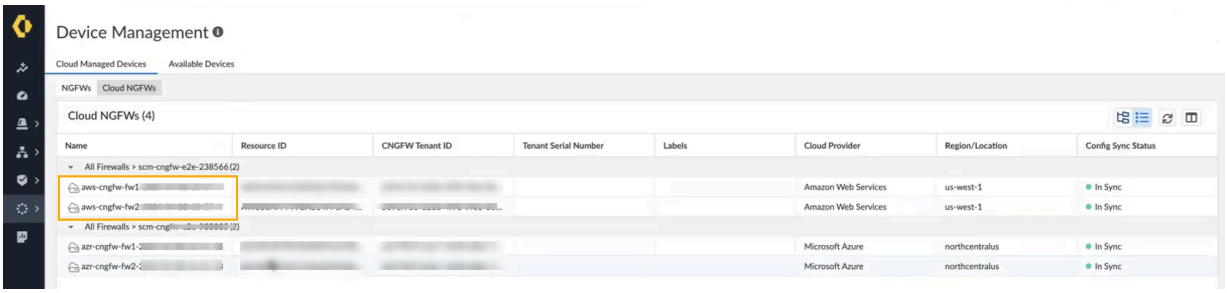
STEP 3 | Sélectionnez **Workflows (Flux de travail) > NGFW Setup (Configuration NGFW) > Device Management (Gestion des périphériques)** :



STEP 4 | L’écran Gestion des périphériques affiche les **NGFW** et les **Cloud NGFW**. Cliquez sur les **Cloud NGFW** pour afficher les pare-feu associés au locataire SCM :



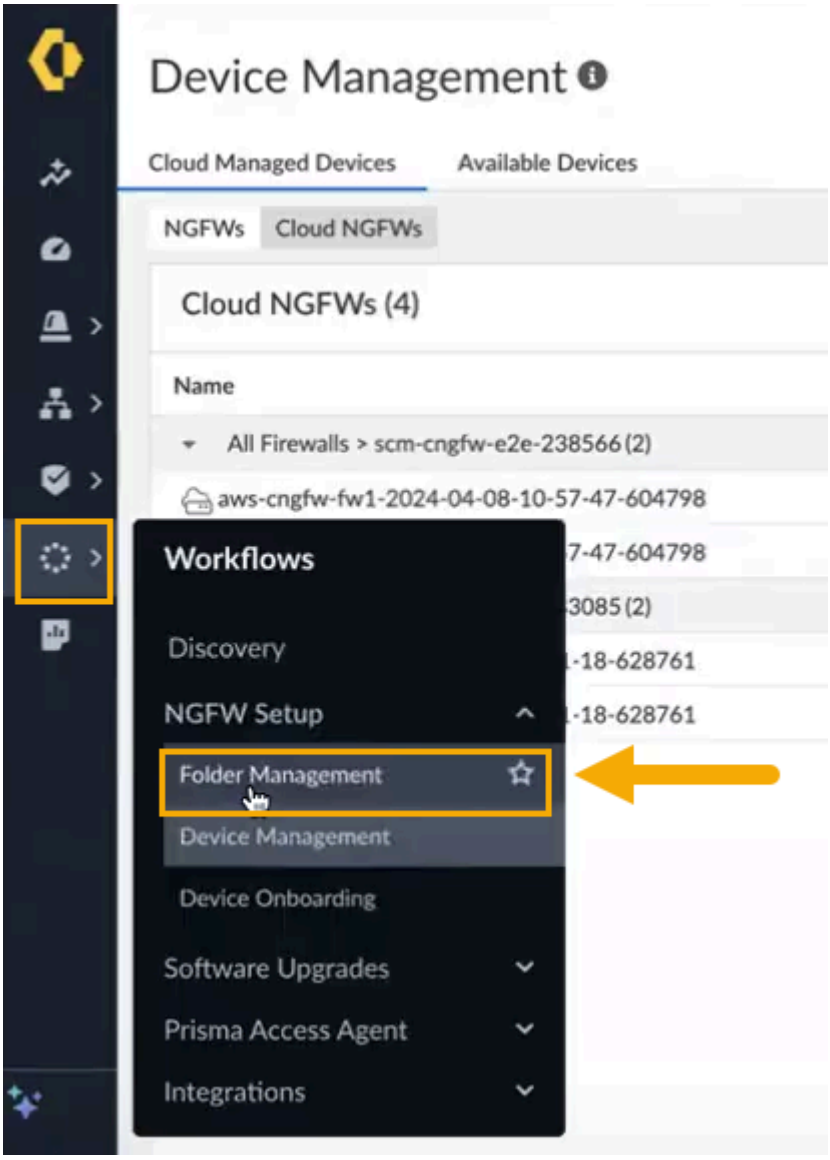
L’écran **Device Management (Gestion des périphériques)** affiche les ressources Cloud NGFW actuellement gérées par SCM :



L’écran Gestion des périphériques affiche les champs suivants :

- Nom. Représente le nom de la ressource Cloud NGFW.
- ID de la ressource. Indique l’ID de la ressource associé à la ressource NGFW.
- ID du locataire CNGFW. L’ID associé au locataire Cloud NGFW lié à SCM.
- Numéro de série du locataire CNGFW. Le numéro de série associé au locataire Cloud NGFW.
- Étiquettes. Une étiquette arbitraire attribuée au Cloud NGFW.
- Fournisseur cloud. Indique le fournisseur cloud associé à la ressource Cloud NGFW.
- Région/Emplacement. Région où se trouve la ressource Cloud NGFW.
- État de la synchronisation de la configuration. L’état de la ressource Cloud NGFW.

STEP 5 | L’écran **Device Management (Gestion des périphériques)** regroupe vos ressources Cloud NGFW dans des *dossiers*. Pour visualiser la structure de ces dossiers, sélectionnez **Workflows (Flux de travail) > Folder Management (Gestion des dossiers)** :



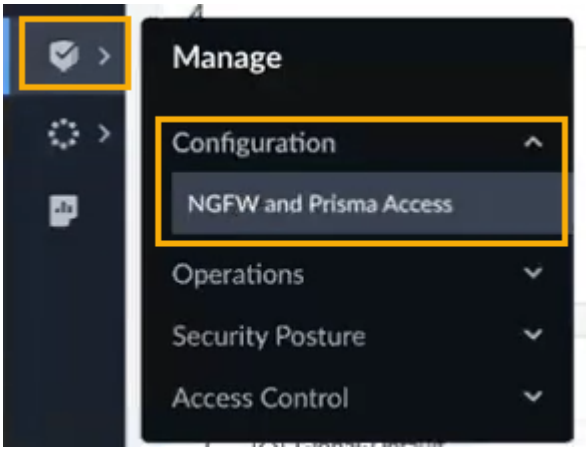
L’écran **Folder Management (Gestion des dossiers)** affiche les ressources Cloud NGFW associées au locataire SCM :

Pour plus d'informations sur la création de dossiers, consultez Créer un dossier pour votre ressource Cloud NGFW à l'aide de Strata Cloud Manager.

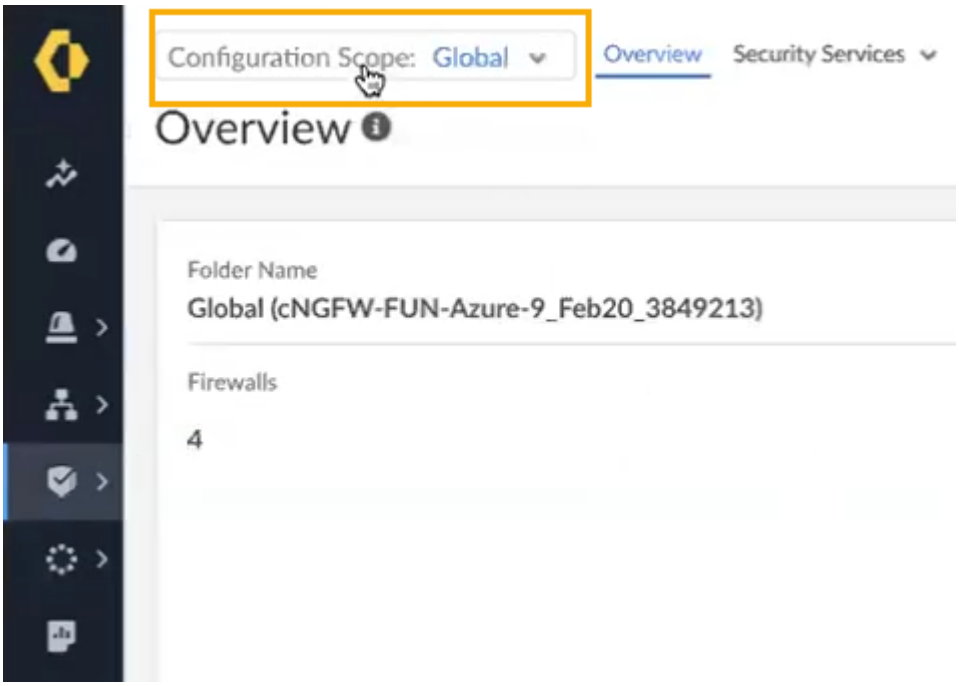
Utiliser Strata Cloud Manager pour la gestion des politiques Cloud NGFW

Vous pouvez utiliser Strata Cloud Manager pour appliquer globalement des politiques de sécurité aux ressources Cloud NGFW comportant un dossier.

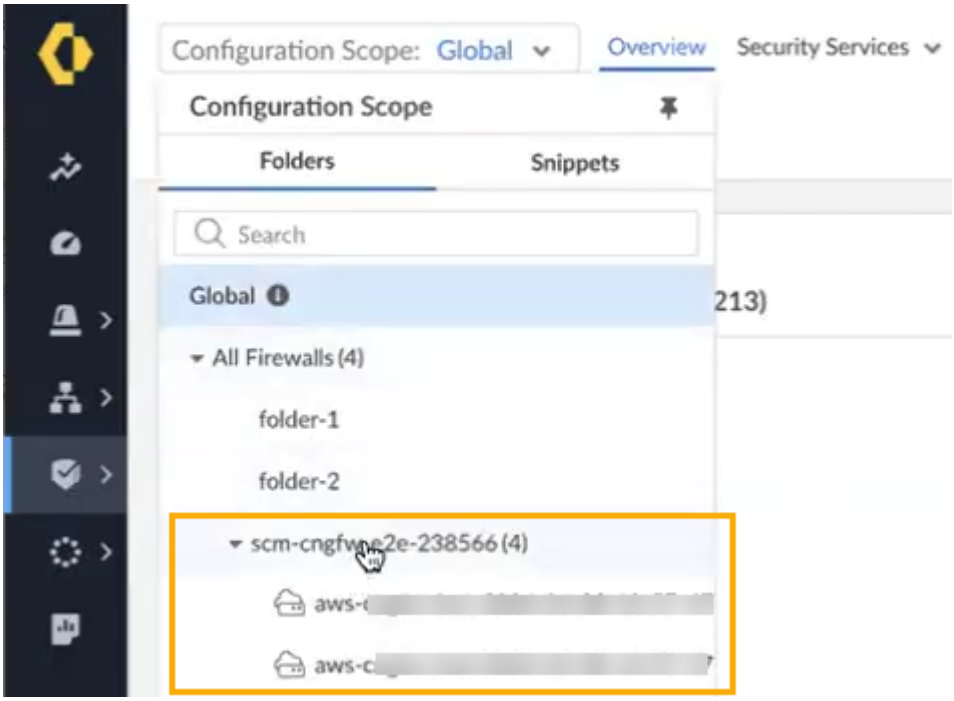
STEP 1 | Dans Strata Cloud Manager, sélectionnez **Manage (Gérer) > Configuration > NGFW and Prisma Access (NGFW et Prisma Access)**.



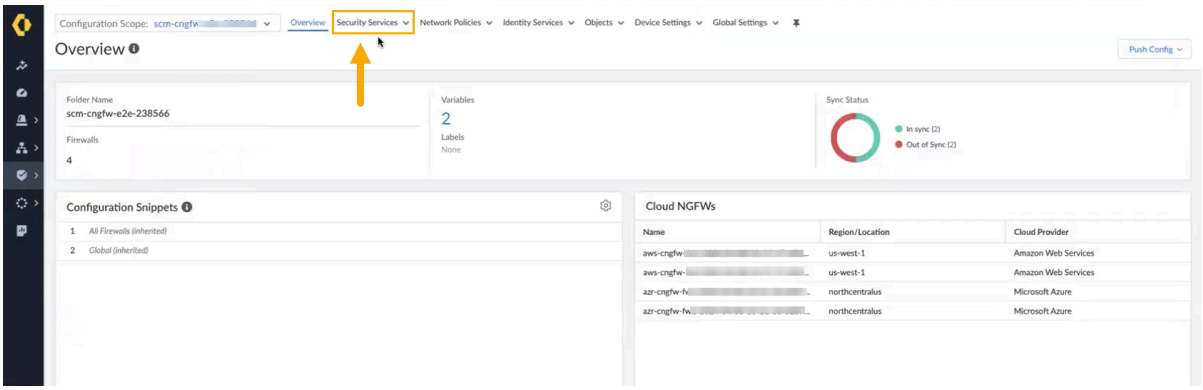
STEP 2 | Sélectionnez **Configuration Scope (Portée de la configuration)**.



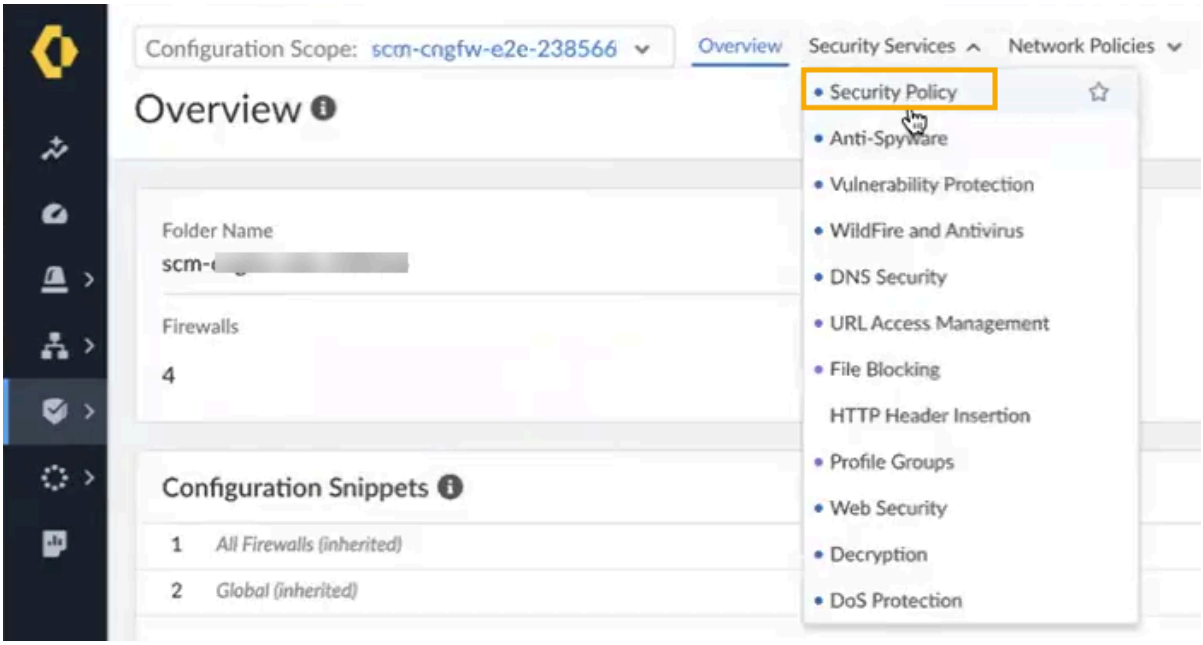
STEP 3 | Dans la liste déroulante, recherchez le dossier contenant les **Cloud NGFW AWS resources (Ressources Cloud NGFW AWS)** :



STEP 4 | Dans la page **Overview (Présentation)** , sélectionnez **Security Services (Services de sécurité)** :



STEP 5 | Dans la liste déroulante **Security Services (Services de sécurité)**, sélectionnez **Security Policy (Politique de sécurité)** :



Pour plus d'informations sur la configuration de la politique de sécurité à l'aide de Strata Cloud Manager, consultez Gérer la politique de sécurité.

Créer un dossier pour votre ressource Cloud NGFW à l’aide de Strata Cloud Manager

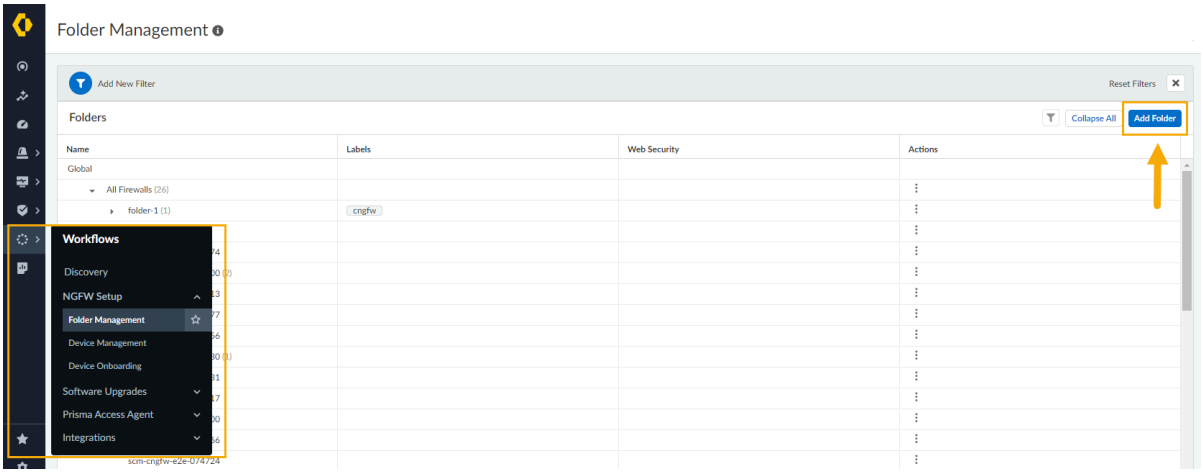
Après avoir configuré l’abonnement approprié pour utiliser le service Strata Cloud Manager pour votre ressource Cloud NGFW, créez un dossier pour afficher les données associées à votre pare-feu. Les dossiers sont utilisés pour effectuer un regroupement logique de vos pare-feu ou types de déploiement (par exemple, une connexion de service pour votre ressource Cloud NGFW) pour simplifier la gestion de la configuration. Vous pouvez créer un dossier contenant plusieurs dossiers imbriqués afin de regrouper les pare-feu et les déploiements nécessitant des configurations similaires. Les dossiers déjà imbriqués peuvent également contenir plusieurs dossiers imbriqués.

Les dossiers d’autres applications Palo Alto Networks, comme Prisma Access, et vos NGFW sont séparés ; vous ne pouvez pas regrouper des NGFW dans un dossier avec des déploiements Prisma Access. Cependant, vous pouvez facilement appliquer des paramètres partagés globalement à tous les dossiers ou utiliser Gérer : Extraits pour appliquer facilement des paramètres et des exigences de politique standard sur plusieurs dossiers.

Pour créer un dossier pour votre ressource Cloud NGFW :

STEP 1 | Connectez-vous à l’application Strata Cloud Manager depuis le hub Palo Alto Networks directement sur le site stratacloudmanager.paloaltonetworks.com.

STEP 2 | Dans l'interface Strata Cloud Manager, sélectionnez **Workflows (Flux de travail) > NGFW Setup (Configuration NGFW) > Folder Management (Gestion des dossiers)** et cliquez sur **Add Folder (Ajouter un dossier)**.



STEP 3 | Dans l’écran **Create Folder (Créer un dossier)** :

1. Saisissez un nom descriptif pour le dossier.
2. Vous pouvez également fournir une description du dossier.
3. Vous pouvez éventuellement attribuer une ou plusieurs étiquettes. Vous pouvez sélectionner une étiquette existante ou en créer une nouvelle en tapant l’étiquette que vous souhaitez créer. Par exemple, utilisez la liste déroulante **Labels (Étiquettes)** pour sélectionner **cngfw**.
4. Spécifiez l’emplacement du dossier à créer à l’aide du menu déroulant. Vous pouvez sélectionner **All Firewalls (Tous les pare-feu)** ou sélectionner un dossier existant pour y imbriquer le dossier. Ce champ est obligatoire.
5. Cliquez sur **Create (Créer)**.

Saisissez un nom descriptif pour le dossier.

Surveiller et dépanner à l’aide de Strata Cloud Manager

Vous pouvez utiliser Strata Cloud Manager pour connaître l’état de votre ressource Cloud NGFW. Utilisez la fonctionnalité **Monitor (Surveiller)** fournie par SCM pour en savoir plus sur :

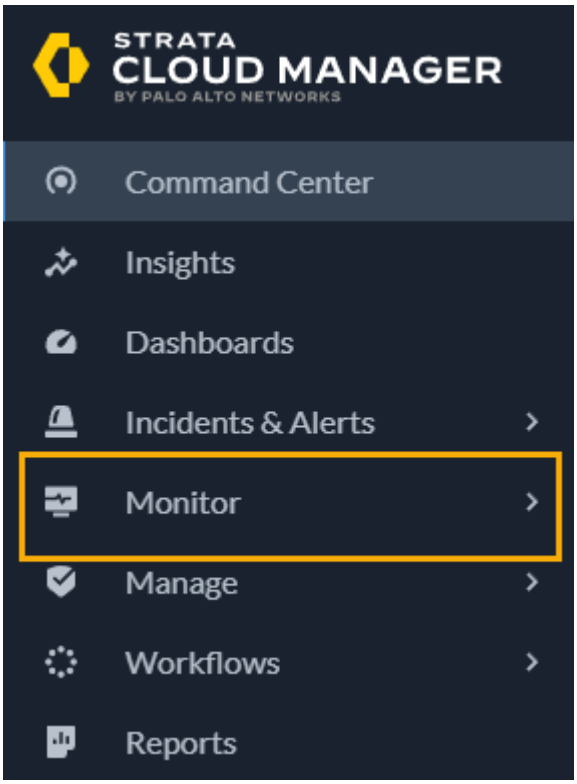
- les produits et abonnements que vous gérez à l’aide de Strata Cloud Manager.
- L’état de santé et de connectivité de vos périphériques Cloud NGFW.

Pour plus d’informations, consultez la section Monitor in Strata Cloud Manager (Surveiller dans Strata Cloud Manager).

Pour utiliser Strata Cloud Manager afin de surveiller votre ressource Cloud NGFW :

STEP 1 | Connectez-vous à l’application Strata Cloud Manager depuis le hub Palo Alto Networks directement sur le site stratacloudmanager.paloaltonetworks.com.

STEP 2 | Dans l’interface, sélectionnez **Monitor (Surveiller)** :



Mises à jour de la version Cloud NGFW pour AWS

Voici où vous pouvez en savoir plus sur les dernières fonctionnalités liées à Cloud NGFW pour AWS et les problèmes connus sur lesquels l’équipe travaille pour améliorer votre expérience :

Nouveautés

Voici les nouveautés de Cloud NGFW for AWS.

Quoi de neuf en juin 2024

Intégration du portail de support client	Cette version du Cloud NGFW pour AWS améliore l'expérience d'intégration en intégrant l'enregistrement de votre locataire Cloud NGFW au portail de support client de Palo Alto Networks. Pour plus d'informations, consultez Enregistrer votre locataire Cloud NGFW sur un compte de support Palo Alto Networks.

Intégration automatisée des comptes	Cloud NGFW pour AWS prend désormais en charge l'intégration automatisée des comptes pour les environnements desservant un grand nombre de comptes AWS. Grâce à cette fonctionnalité, vous n'avez plus besoin d'intégrer manuellement des comptes individuels. Pour plus d'informations, consultez Configurer l'intégration automatisée des comptes.

Quoi de neuf en mai 2024

Gestion des politiques Cloud NGFW à l'aide de Strata Cloud Manager	Vous pouvez désormais lier votre ressource Cloud NGFW au Strata Cloud Manager (SCM) pour la gestion des politiques. Strata Cloud Manager offre une gestion unifiée pour l'ensemble de votre déploiement de sécurité réseau, ce qui vous permet de gérer facilement votre infrastructure de sécurité Palo Alto Networks à partir d'une interface utilisateur unique et simplifiée. Avec cette interface, vous bénéficiez d'une visibilité complète sur les utilisateurs, les sites de succursales, les applications et les menaces sur tous les points d'application de la sécurité du réseau. Cette fonctionnalité fournit des informations exploitables, une meilleure sécurité et une facilité de dépannage et de résolution des problèmes. Cette version initiale vous permet de créer des ressources à l'aide de la console Cloud NGFW, puis de les enregistrer auprès de Strata Cloud Manager pour une gestion centralisée des politiques. Vous utilisez Strata Cloud Manager pour la surveillance et le dépannage. Pour plus d'informations, consultez Lier votre ressource Cloud NGFW à Strata Cloud Manager. Pour plus d'informations, consultez Gestion des politiques de Strata Cloud Manager.
Métriques Cloud NGFW	Vous disposez désormais d'une meilleure visibilité opérationnelle de vos ressources Cloud NGFW à l'aide des métriques Cloud NGFW. Cloud NGFW publie désormais des métriques dans AWS CloudWatch pour vous aider à surveiller la santé, les performances et les modèles d'utilisation de votre Cloud NGFW. Grâce à ces métriques supplémentaires, vous pouvez évaluer la santé générale de vos ressources Cloud NGFW, identifier les bottlenecks de performance et détecter les anomalies. Pour plus d'informations, consultez Champs du journal du trafic AWS.
Afficher l'ID de la zone	Cloud NGFW pour AWS améliore la fonctionnalité multi-VPC en vous permettant de spécifier des noms de zone de disponibilité lors de la création des ressources de pare-feu. AWS mappe l'ID physique des zones de disponibilité *de manière aléatoire* aux noms de zones de disponibilité de chaque compte AWS. Précédemment, vous deviez déterminer manuellement le nom de la zone de disponibilité en fonction d'un ID de zone de disponibilité particulier dans votre ou vos comptes AWS dans la console Cloud NGFW, puis utiliser ces informations pour créer des ressources Cloud NGFW. Grâce à cette

	amélioration, Cloud NGFW vous permet de spécifier l'ID ou le nom de la zone de disponibilité lors de la création d'une nouvelle ressource de pare-feu. Pour plus d'informations, consultez Créer une ressource NGFW sur AWS.
Améliorations de l'abonnement	Cloud NGFW pour AWS améliore les informations affichées sur la page **Subscription (Abonnement)** en affichant l'état de votre abonnement à crédit. Cette page indique désormais si votre abonnement est *périmé*, *actif*, ou *inactif*.
Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes : • Asie-Pacifique (Osaka) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.

Quoi de neuf en mars 2024

Prévention avancée des menaces	Cloud NGFW pour AWS utilise désormais la prévention avancée des menaces pour bloquer le trafic de commande et de contrôle inconnu et les attaques par injection de type « zero-day ». Pour plus d'informations, consultez Prévention avancée des menaces.
Améliorations de Single Sign-On (ouverture de session unique – SSO) et de l'authentification multifactorielle (MFA)	L'accès à la console Cloud NGFW est intégré au Single Sign-On (ouverture de session unique – SSO) et à l'authentification multifactorielle (MFA) pour offrir commodité et sécurité. Vous pouvez également utiliser la même adresse e-mail pour vous enregistrer auprès de plusieurs locataires Cloud NGFW. La page de connexion de Cloud NGFW vous permet désormais de sélectionner l'un des nombreux comptes/locataires Cloud NGFW que vous utilisez. Pour plus d'informations, consultez S'abonner au Cloud NGFW pour AWS et Inviter des utilisateurs sur Cloud NGFW pour AWS.
Prise en charge du lancement rapide du SaaS d'AWS Marketplace	Cloud NGFW est désormais intégré au lancement rapide SaaS d'AWS Marketplace pour faciliter, accélérer et sécuriser l'abonnement AWS Marketplace en proposant des instructions étape par étape à l'aide d'un modèle AWS CloudFormation préconfiguré. Pour plus d'informations, consultez S'abonner à Cloud NGFW pour AWS.
Améliorations au registre d'AWS CloudFormation	Le registre Cloud Formation de Cloud NGFW st désormais mis à jour avec les dernières fonctionnalités en matière de ressources de pare-feu et de rulestacks, ainsi que la récupération intégrée des jetons d'accès par programmation. Pour plus d'informations, consultez Provisionner des ressources Cloud NGFW sur votre AWS CFT.
Prévention des pertes de données d'entreprise	La prévention des pertes de données d'entreprise (E-DLP) vous permet de protéger les informations sensibles contre l'accès non

	autorisé, l'utilisation abusive, l'extraction ou le partage. Vous pouvez désormais intégrer E-DLP à Cloud NGFW pour AWS et utiliser l'interface Panorama pour ajouter des profils de filtrage de données à vos règles de politique de sécurité. Pour plus d'informations, consultez Intégration E-DLP avec CNGFW pour AWS.
Améliorations des politiques basées sur les étiquettes	Vous pouvez désormais renseigner des étiquettes IP de deux régions différentes dans vos groupes d'appareils cloud. Collectez vos étiquettes dans une région AWS, puis appliquez des politiques de sécurité sur votre pare-feu dans l'autre région. Pour plus d'informations, consultez Politiques basées sur les étiquettes.
Métriques d'utilisation des règles Cloud NGFW	Vous pouvez désormais utiliser la console Panorama pour suivre et surveiller l'utilisation des règles pour les opérations et les tâches de dépannage, y compris le nombre d'accès à la règle et les applications vues sur les ressources Cloud NGFW. Pour plus d'informations, consultez Utilisation des règles Cloud NGFW pour AWS. *Pour utiliser cette fonctionnalité, vous devez effectuer une mise à niveau du plug-in AWS vers la version 5.2.0.*
Intégration de Cloud NGFW avec AWS Cloud WAN	AWS Cloud WAN vous permet désormais de créer un réseau unifié qui interconnecte les environnements cloud et sur site et 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 dans la même région ; • des VPC dans le même segment dans différentes régions (attachements isolés) ; • des VPC dans différents segments dans différentes régions. Pour plus d'informations, consultez Intégration de Cloud NGFW avec AWS Cloud WAN.

Quoi de neuf en décembre 2023

Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Directives relatives à l'estimation de la tarification de Cloud NGFW pour AWS

Quoi de neuf en novembre 2023

Vidéos Cloud NGFW pour AWS	AWS Reinvent 2023 – Comment les organisations sécurisent les applications avec AWS et Palo Alto Networks (HYB205) Octets de sécurité réseau – Cloud NGFW pour AWS

Quoi de neuf en octobre 2023

Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Architectures de déploiement Cloud NGFW pour AWS

Quoi de neuf en septembre 2023

Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Cloud NGFW pour AWS s’intègre à Panorama Guide de résilience de Cloud NGFW pour AWS

Quoi de neuf en août 2023

Plusieurs Panoramas pour le locataire Cloud NGFW	Vous pouvez désormais lier plusieurs appareils Panorama avec leur instance du service de journalisation Strata à votre locataire Cloud NGFW. Vous pouvez ensuite associer la ressource NGFW d’un locataire à l’un de ces liens pour la gestion des politiques et des journaux. Pour plus d’informations, consultez Utiliser plusieurs panoramas avec votre locataire Cloud NGFW.
Support Premium ajouté au Cloud NGFW pour AWS	Le support Premium est désormais inclus avec Cloud NGFW pour AWS sans frais supplémentaires. Le support Premium de Palo Alto Networks améliore les ressources internes grâce à la disponibilité d’experts techniques qui prennent en charge votre infrastructure de sécurité Palo Alto Networks. Ce niveau de support permet d’accéder à l’assurance de sécurité afin de vous aider lorsque les incidents de sécurité nécessitent un accès à des experts en sécurité. Pour plus d’informations, consultez Support Premium.
Dimensionnement du service de journalisation Strata dynamique de Cloud NGFW pour AWS	Vous pouvez désormais utiliser le service de journalisation Strata pour effectuer des requêtes Explorer/visionneuse de journaux afin d’afficher les journaux générés par une ressource Cloud NGFW pour AWS spécifique. Le service de journalisation Strata affiche également les indicateurs clés de vos Cloud NGFW dans une **Page d’inventaire du Cloud NGFW pour le service de journalisation Strata** pour mieux surveiller le taux d’ingestion, l’utilisation du stockage et l’état de la

	connexion. Lors de son utilisation avec Cloud NGFW pour AWS, le service de journalisation Strata se met désormais automatiquement l'échelle avec les ressources Cloud NGFW pour AWS. À mesure que le débit du trafic augmente sur ces ressources Cloud NGFW, votre stockage du service de journalisation Strata disponible augmente également, de sorte que vous n'avez pas à vous préoccuper des ajustements manuels du stockage du lac de données Cortex Data Lake pour enregistrer vos données de journal.
Explorateur de l'utilisation (préversion)	Cette version introduit l'Explorateur de l'utilisation de la console Cloud NGFW pour AWS. Le tableau de bord de l'Explorateur de l'utilisation vous permet d'afficher la consommation du Cloud NGFW et sa corrélation avec les crédits associés au locataire. Pour plus d'informations, consultez Explorateur de l'utilisateur de Cloud NGFW pour AWS.
Modifications de la tarification et de la facturation	Cloud NGFW pour AWS modifie le modèle de tarification pour fournir plus de flexibilité à l'utilisation globale des locataires Cloud NGFW en fonction des heures de déploiement de tous les NGFW, de la quantité de trafic qu'ils ont sécurisée et du nombre de fonctionnalités de sécurité qu'ils utilisent chaque heure. Consultez la page Tarification pour en savoir plus.

Quoi de neuf en juillet 2023

Filtrer les journaux et l'activité du Cloud NGFW dans Panorama	Dans l'onglet **Monitor (Moniteur)** de Panorama, vous pouvez désormais filtrer pour afficher le journal d'un groupe d'appareils cloud individuel ou afficher les journaux et l'activité de tous les groupes d'appareils cloud. Consultez la section View Cloud NGFW Logs and Activity (Afficher les journaux et l'activité de Cloud NGFW) pour obtenir des informations plus détaillées.
Politiques basées sur des étiquettes	Lors du déploiement ou de la résiliation de ressources AWS (telles que des instances EC2) dans le cloud public AWS, vous pouvez mettre à jour automatiquement la politique de sécurité sur vos ressources Palo Alto Networks Cloud NGFW afin de sécuriser le trafic vers ces ressources AWS. Consultez la section Tag based policies (Politiques basées sur des étiquettes) pour en savoir plus.
WildFire	Cloud NGFW peut désormais protéger votre trafic de VPC contre les menaces basées sur les fichiers en détectant et transférant des fichiers, exécutables et scripts malveillants (tels que JScript et PowerShell) dans votre trafic de VPC vers le service cloud WildFire™ (WF) pour l'analyse des logiciels malveillants.

Quoi de neuf en juin 2023

Dissociation de la prise en charge de l'intégration Panorama	Vous pouvez désormais dissocier automatiquement l'appareil Panorama d'une ressource Cloud NGFW sans ouvrir un ticket de support. Reportez-vous à la section Unlink the Cloud NGFW from Palo Alto Networks Management (Dissocier le Cloud NGFW de Palo Alto Networks Management) pour en savoir plus.
Vidéo Cloud NGFW pour AWS	Comment supprimer une ressource Cloud NGFW

Quoi de neuf en mai 2023

Support Panorama	Vous pouvez désormais intégrer un locataire Cloud NGFW pour AWS à l'appareil Palo Alto Networks pour gérer de manière centralisée un ensemble partagé de règles de sécurité sur les ressources Cloud NGFW aux côtés de vos appareils de pare-feu physiques et virtuels. Consultez la section Panorama Integration (Intégration Panorama) pour en savoir plus.
Vidéo Cloud NGFW pour AWS	Intégration de Cloud NGFW pour AWS avec Panorama

Quoi de neuf en avril 2023

Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • af-south-1 (Le Cap) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.

Quoi de neuf en mars 2023

Rôle lecteur locataire	En tant qu'administrateur de locataire de Cloud NGFW, vous pouvez désormais inviter d'autres utilisateurs dans le rôle Lecteur locataire. Un utilisateur assumant ce rôle peut afficher et décrire tous les aspects du locataire Cloud NGFW, tels que • Ressources et paramètres NGFW • Rulestacks globales et locales • Tous les paramètres des utilisateurs et des locataires

Vidéo Cloud NGFW pour AWS	Flux de trafic des ressources NGFW multi-VPC

Quoi de neuf en février 2023

Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • ap-south-1 (Hong Kong) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.
Vidéo Cloud NGFW pour AWS	Flux intelligents de l'hôte sur le compartiment S3

Quoi de neuf en janvier 2023

Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • me-south-1 (Bahreïn) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.

Quoi de neuf en décembre 2022

Ressource Cloud NGFW pour plusieurs VPC	Vous pouvez partager la même ressource Cloud NGFW entre plusieurs clouds privés virtuels (VPC) dans les comptes AWS intégrés de vos locataires. Vous pouvez créer des terminaux pour une ressource NGFW dans différents VPC et acheminer le trafic vers la ressource NGFW à des fins d'inspection. Consultez la documentation et une page blog détaillée pour en savoir plus sur cette fonctionnalité.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Nouveau : Meilleure évolutivité Cloud NGFW sur plusieurs VPC AWS
Vidéo Cloud NGFW pour AWS	Ressource Cloud NGFW pour plusieurs VPC

Quoi de neuf en novembre 2022

Plusieurs comptes AWS dans le locataire Cloud NGFW	Vous pouvez intégrer plusieurs comptes AWS dans le même locataire Cloud NGFW et créer des ressources Cloud NGFW dans ces comptes. Consultez la section Add Multiple AWS Accounts (Ajouter plusieurs comptes AWS) pour en savoir plus.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Cloud NGFW pour AWS – FAQ (Mis à jour)
Vidéo Cloud NGFW pour AWS	AWS re:Invent 2022 – Avalon Healthcare Solutions sécurise son déploiement avec Palo Alto Networks (PRT241)

Quoi de neuf en octobre 2022

Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Grâce à un estimateur de tarification interactif, Cloud NGFW pour AWS devient encore plus facile
Vidéo Cloud NGFW pour AWS	Support AWS Firewall Manager pour Palo Alto Networks Cloud NGFW | Amazon Web Services

Quoi de neuf en septembre 2022

Vidéos Cloud NGFW pour AWS	AWS Summit SF 2022 – Gestion centralisée de Palo Alto Networks Cloud NGFW grâce à AWS Firewall Manager

Quoi de neuf en août 2022

Abonnement Cloud NGFW simplifié et intégration de compte	Vous pouvez vous abonner à Cloud NGFW pour AWS et intégrer vos comptes AWS en quelques clics avec le moins de changements de contexte entre la console AWS Marketplace et Cloud NGFW. Veuillez consulter la page de documentation et visionnez les Vidéos AWS pour en savoir plus sur cette fonctionnalité.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	La meilleure sécurité réseau pour AWS de sa catégorie est désormais plus facile à obtenir partout dans le monde

Vidéo Cloud NGFW pour AWS	Étape 1 du déploiement de Cloud NGFW pour AWS : Abonnez-vous à Cloud NGFW (Mis à jour)

Quoi de neuf en juillet 2022

Crédits Cloud NGFW pour AWS	Vous pouvez désormais passer à un contrat d'un an, de deux ans ou de trois ans en souscrivant à la liste des contrats de **Crédits Palo Alto Networks Cloud NGFW pour AWS** SaaS pour un nombre spécifié de crédits. Cet abonnement associe les Crédits Cloud NGFW pour AWS avec votre locataire Cloud NGFW existant. Les crédits Cloud NGFW pour AWS vous permettent de consommer des ressources Cloud NGFW dans votre locataire à moindre coût jusqu'à une capacité spécifique jusqu'à l'expiration de votre contrat, tout en conservant la possibilité d'étendre votre consommation Cloud NGFW à tout moment.
Décryptage entrant	Vous pouvez désormais utiliser Cloud NGFW pour AWS pour décrypter, inspecter et protéger les sessions SSL/TLS entrantes de votre trafic d'entrée VPC. Pour plus d'informations, reportez-vous à la section Configurer le décryptage entrant sur Cloud NGFW pour AWS.
Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • ap-northeast-1 (Tokyo) • ap-northeast-2 (Séoul) • ap-northeast-3 (Osaka) • ap-south-1 (Bombay) • sa-east-1 (São Paulo) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.
Vidéos Cloud NGFW pour AWS	AWS re:Inforce 2022 – Création d'une infrastructure réseau mondiale évolutive et sécurisée avec AWS (NIS205) AWS re:Inforce 2022 – Intégré et automatisé : Sécurisation de chaque étape de l'adoption du cloud (GRC306)

Quoi de neuf en juin 2022

Journaux d'audit dans Cloud NGFW	Vous pouvez désormais visualiser les journaux d'audit Cloud NGFW dans votre compte Cloudwatch. Consultez la documentation pour en savoir plus sur cette fonctionnalité.

Prise en charge de XFF dans la politique Cloud NGFW	Vous pouvez désormais activer les ressources Cloud NGFW pour utiliser l'adresse IP source dans le champ d'en-tête HTTP X-Forwarded-For (XFF) pour appliquer la politique. Consultez la documentation pour en savoir plus.
Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • eu-ouest-3 (Paris) • eu-north-1 (Stockholm) • eu-south-1 (Milan) • ap-southeast-1 (Singapour) • ap-southeast-2 (Sydney) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	Quelle est la prochaine étape avec Cloud NGFW – Questions-réponses en direct
Vidéo Cloud NGFW pour AWS	Cloud NGFW pour AWS – Intégration à Splunk

Quoi de neuf en mai 2022

Prise en charge de Terraform pour Cloud NGFW pour AWS	Avec le nouveau fournisseur cloudngfwaws vous pouvez automatiser le processus de création de votre infrastructure de sécurité et maintenir la posture de sécurité réseau de vos VPC AWS à l'aide des rulestacks Cloud NGFW. Consultez Prise en charge de Terraform pour Cloud NGFW pour AWS et le blog détaillé pour en savoir plus sur le fournisseur Terraform.
Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans les régions AWS suivantes. • us-east-2 (Ohio) • ca-central-1 (Canada) • eu-west-1 (Irlande) • eu-west-2 (Londres) • eu-central-1 (Francfort) Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.
Prise en charge de CloudFormation pour	Nous avons publié les types de ressources CloudFormation en tant qu'extension publique dans le Registre AWS CloudFormation.

Cloud NGFW pour AWS	Vous pouvez désormais ajouter ces ressources Cloud NGFW directement à vos modèles Cloud Formation de la même manière que vous utilisez les ressources fournies par AWS. Ces types de ressources vous permettent de déployer et de gérer des composants Cloud NGFW à l'aide de flux de travail IaC (Infrastructure as Code). Consultez Provisionner des ressources Cloud NGFW sur votre AWS CFT pour en savoir plus sur la prise en charge d'AWS CloudFormation pour Cloud NGFW.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	• Guide du développeur de Cloud NGFW pour AWS • Mise à jour : Cloud NGFW pour AWS – FAQ
Vidéos Cloud NGFW pour AWS	• Visite interactive du produit • Boucle de routage AWS – Équilibreur de charge de passerelle et FWaaS • Intégration de Cloud NGFW à AWS Firewall Manager • Cloud NGFW pour AWS – Découvrez ce qu'il y a sous le capot

Quoi de neuf en avril 2022

Présentation de l'essai gratuit du Cloud NGFW pour AWS	Vous pouvez désormais essayer et acheter Cloud NGFW pour AWS directement depuis AWS Marketplace. L'essai gratuit vous permet d'utiliser deux ressources NGFW avec toutes les fonctionnalités pour sécuriser 100 Go de trafic pendant sept jours sans frais. Commencez dès aujourd'hui ! Pour acquérir une expérience pratique avec le Cloud NGFW, abonnez-vous via AWS Marketplace. Pour en savoir plus sur la version d'évaluation gratuite de Cloud NGFW, consultez Essai gratuit de Cloud NGFW pour AWS.
Prise en charge supplémentaire des régions AWS	Cloud NGFW pour AWS est désormais disponible dans la région AWS us-west-2 (Oregon). Pour obtenir la liste complète des régions prises en charge, consultez Régions et zones prises en charge par Cloud NGFW pour AWS.
Accès par programmation Cloud NGFW pour AWS	Vous pouvez désormais créer et gérer par programmation des ressources Cloud NGFW à l'aide des REST API. Vous pouvez utiliser le rôle IAM dans votre compte AWS pour accéder aux API Cloud NGFW, puis configurer les ressources IAM qui peuvent assumer ce rôle. Pour en savoir plus sur l'accès par programmation Cloud NGFW pour AWS, consultez Activer l'accès par programmation et le Guide de la REST API Cloud NGFW pour AWS.
Blogs, articles et autres ressources sur	Cloud NGFW pour AWS – Cours numérique

Cloud NGFW pour AWS	
Vidéos Cloud NGFW pour AWS	Événement de lancement Cloud NGFW pour AWS (à la demande)

Quoi de neuf en mars 2022

Présentation de Cloud NGFW pour AWS	Cloud NGFW pour AWS est un service entièrement géré sur la plateforme AWS, alimenté par les pare-feu logiciels Palo Alto Networks. Avec Cloud NGFW pour AWS, vous disposez désormais d'une expérience de déploiement NGFW qui gère la fourniture des capacités et de l'infrastructure du pare-feu nouvelle génération de Palo Alto en un seul mouvement. Cloud NGFW pour AWS est un service régional. Actuellement, il est disponible dans les régions USA Est (Virginie du Nord) et USA Ouest (Californie). Consultez l'annonce de Cloud NGFW pour AWS sur le blog Palo Alto Networks et le blog technique sur la page de la communauté Live pour plus d'informations. Abonnez-vous via la page AWS Marketplace pour acquérir une expérience pratique de ce service. Pour en savoir plus sur Cloud NGFW, ses fonctionnalités et ses tarifs, consultez la documentation technique, la liste de lecture vidéo et les pages de la FAQ.
AWS Firewall Manager prend en charge Cloud NGFW	Vous pouvez utiliser AWS Firewall Manager pour orchestrer le déploiement des pare-feu Cloud NGFW Palo Alto Networks et obtenir une visibilité centralisée. AWS Firewall Manager ajoute automatiquement et systématiquement des pare-feu Cloud NGFW Palo Alto Networks aux nouveaux comptes et VPC sans intervention manuelle. Cette intégration réduit les tâches opérationnelles lourdes requises pour surveiller les nouveaux comptes, ajoute des protections par pare-feu et offre une visibilité sur les configurations non conformes entre les comptes de votre organisation. Consultez l'annonce d'AWS Firewall Manager, la page de documentation AWS Firewall Manager et le blog de Jeff Barr sur l'intégration.
Blogs, articles et autres ressources sur Cloud NGFW pour AWS	• Blog d'annonce Cloud NGFW pour AWS • Blog technique Cloud NGFW pour AWS • Cloud NGFW et AWS Firewall Manager – Blog de Jeff Barr • Cloud NGFW pour AWS - FAQ • Architectures de déploiement Cloud NGFW pour AWS • Cloud NGFW pour AWS – ebook

Vidéos Cloud NGFW pour AWS	• Présentation de Cloud NGFW pour AWS • Étape de déploiement 1 : Abonnez-vous à Cloud NGFW • Étape de déploiement 2 : Définir la politique de sécurité • Étape de déploiement 3 : Créer une ressource Cloud NGFW • Modèle de déploiement centralisé (protection du trafic est-ouest) • Modèle de déploiement distribué (protection du trafic sortant) • Modèle de déploiement distribué (protection du trafic entrant) • Modèle de déploiement distribué (protection du trafic inter-sous-réseau) • App-ID dans Cloud NGFW • Flux d’intelligence (EDL) dans Cloud NGFW • Rôles et autorisations dans Cloud NGFW • Profils de sécurité dans Cloud NGFW • Décryptage TLS sortant dans Cloud NGFW

Problèmes connus de Cloud NGFW pour AWS

Les problèmes connus suivants ont été identifiés dans Cloud NGFW pour AWS.

ID	Description
DIT-40616	Dans certains cas, la confirmation d'une modification de rulestack, puis sa validation peuvent amener votre ressource Cloud NGFW à appliquer une configuration incorrecte. Ce problème peut également amener un pare-feu automatiquement mis à l'échelle à appliquer un fichier de configuration incorrect lors du démarrage. Pour résoudre ce problème, Palo Alto Networks vous recommande de ne pas cliquer sur **Validate (Confirmer)** lors de la modification de votre rulestack. Vous devez plutôt valider la modification sans confirmation.
FWAAS-1501	Cloud NGFW utilise le résolveur AWS Route 53 natif pour résoudre les FQDN que vous configurez dans vos règles. Lorsqu'il est utilisé, le résolveur AWS Route 53 peut résoudre un FQDN en une adresse IP, différente de ce que vous pouvez voir lorsque vous utilisez le résolveur Route 53 dans vos VPC.
FWAAS-2589	Lorsque vous intégrez un compte AWS à votre locataire Cloud NGFW, vous choisissez l'un de ces deux modes de création de terminal : géré par le client ou géré par le service. Cloud NGFW ne vous permettra pas de changer de mode après avoir terminé le processus d'intégration du compte.
FWAAS-3009	Cloud NGFW vous permet d'utiliser un compartiment S3 comme destination de journalisation pour les ressources NGFW. Dans les régions AWS en dehors des États-Unis, Cloud NGFW s'attend à ce que vous utilisiez les compartiments S3 créés dans la même région AWS, où vous déployez les ressources NGFW.
FWAAS-5817	L'interface utilisateur de Panorama n'affiche pas de message d'erreur lors de l'échec du gestionnaire de cloud ou du service cloud NGFW. Vous ne serez informé de l'échec de la transmission que lorsque la **validation** du pare-feu échoue.
FWAAS-5823	Lors de la création d'un nouveau groupe d'appareils cloud, vous ne pouvez pas sélectionner les certificats à utiliser pour *l'approbation de transfert* ou *la non-approbation de transfert*.
FWAAS-6380	Un message d'erreur peut s'afficher lors de la transmission d'une modification non validée à un groupe d'appareils cloud. Validez vos modifications avant de les transmettre.
FWAAS-6540	Un groupe d'appareils existant vous permet par erreur d'appliquer une pile de modèles différente après l'avoir créée. Vous ne pouvez pas associer une pile de modèles différente pour le même groupe d'appareils entre les locataires.
FWAAS-6542	La mise à jour d'une pile de modèles échoue lors de son application à un autre groupe d'appareils.

ID	Description
FWAAS-6961	Sur le plug-in Panorama AWS Plugin pour le service Cloud NGFW, le premier locataire lié à Panorama ne pourra voir aucun VPC sous l'onglet VPC découvert. Solution alternative : Le premier locataire doit cliquer sur le bouton **Refresh Vpc (Actualiser le VPC)** sous l'onglet **Discover VPC (Découvrir un VPC)** pour obtenir une liste des VPC.
FWAAS-7721	Dans un environnement mis à l'échelle, l'interface utilisateur du plug-in AWS plante lors de l'affichage de la charge utile des étiquettes/adresse IP sur le tableau de bord **Monitoring Definition (Définition de surveillance)**. **Solution alternative** : Utilisez la CLI de Panorama pour exécuter la commande : `show plugins aws details-dashboard`.
FWAAS-7766	La page **Discovered VPC (VPC découvert)** sur l'interface utilisateur du Cloud NGFW n'affiche pas la raison de l'échec si l'état de surveillance d'un VPC découvert est Échec.
FWAAS-10971	L'émission de la commande **reset (réinitialisation)** avec des ID de ressource de pare-feu non valides ne réinitialise pas les compteurs d'utilisation des règles. Ce comportement est attendu.

Problèmes résolus de Cloud NGFW pour AWS

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

ID	Description
FWAAS-3009	Cloud NGFW vous permet d'utiliser un compartiment S3 comme destination de journalisation pour les ressources NGFW. Dans les régions AWS en dehors des États-Unis, Cloud NGFW s'attend à ce que vous utilisiez les compartiments S3 créés dans la même région AWS, où vous déployez les ressources NGFW.
FWAAS-5842	Vous ne pouvez pas afficher les journaux de groupes d'appareils cloud individuels envoyés à CDL à l'aide de l'onglet **Monitor (Surveiller)** dans Panorama. Les journaux de tous les groupes d'appareils cloud sont affichés.
FWAAS-6536	Cloud NGFW ne parvient pas à afficher tous les groupes d'appareils cloud lorsque vous sélectionnez **All (Tous)** sur la page **Tenants (Locataires)**. Si vous sélectionnez un locataire individuel, tous les groupes d'appareils cloud affichés dans la liste.
FWAAS-6633	Une validation de pare-feu peut ne pas être déclenchée après la première transmission de configuration du groupe d'appareils cloud depuis Panorama. **Solution alternative** : Réessayez la transmission de configuration du groupe d'appareils cloud depuis Panorama.
FWAAS-8622	La rulestack Cloud NGFW pour AWS peut rester bloquée dans l'état de pré-validation lorsque le bouton **Validate (Valider)** est utilisé avant la première validation. **Solution alternative** : Ne validez pas les modifications de configuration de votre rulestack ; effectuez plutôt le **Commit (Validation)** sans validation.

