paloalto TECHDOCS

Administration de Cloud NGFW pour AWS

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 5, 2024

Table of Contents

Gestion

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
•	❑

Cloud NGFW pour AWS prend en charge des services qui simplifient et facilitent la configuration et l’intégration. Des services numériques complets, une assistance technique et des services de formation soulignent notre engagement envers le succès continu de votre déploiement Palo Alto Networks. Vous pouvez accéder à de l’aide via la communauté LIVE et le portail de support client.

Cloud NGFW pour AWS est conçu pour vous permettre d’être opérationnel rapidement. Vous évitez le long processus de déploiement en configurant des rulestacks indispensables et des profils de sécurité automatisés tout en tirant parti des avantages d’AWS : intégration complète à AWS, surveillance, journalisation, etc. Invitez facilement des utilisateurs supplémentaires pour vous aider à gérer votre déploiement Cloud NGFW ou gérez les rôles des utilisateurs existants.

Inviter des utilisateurs sur Cloud NGFW pour AWS

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

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 à rejoindre le locataire Cloud NGFW, vous devez spécifier l’adresse e-mail de l’utilisateur et lui attribuer 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 crée 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 et 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 rulestack globale	Créez une rulestack globale.
Admin de pare-feu local	• Créez NGFW. • Associer une rulestack locale à des NGFW.

Rôle Cloud NGFW	Autorisations
	Les administrateurs de pare-feu locaux peuvent uniquement créer des NGFW et associer des rulestacks au sein d'un compte AWS spécifié.
Admin de rulestack locale	• Créez des rulestacks locales. • Associer des rulestacks locales à des NGFW. Chaque admin de rulestack locale 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.

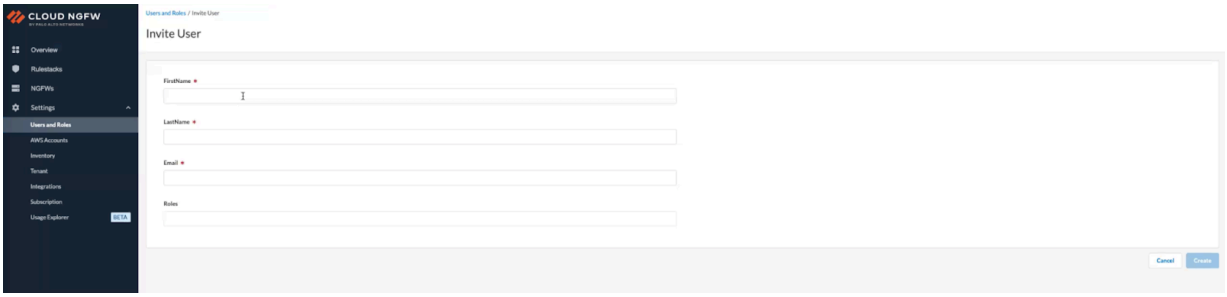
STEP 1 | Connectez-vous au locataire Cloud NGFW.

STEP 2 | Sélectionnez **Settings (Paramètres)** > **Users and Roles (Utilisateurs et rôles)** > **Invite User (Inviter un 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 au 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 au SSO.	Vous ne recevez pas d'e-mail d'activation.

Cas d’utilisation	Étapes
Si vous êtes un utilisateur existant qui n’est pas enregistré au 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 au 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

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

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 (Utilisateurs et rôles)**.

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

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.

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 (Utilisateurs 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-locataire peut modifier son nom ou 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 (Utilisateurs 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. Reconnectez-vous à l’aide du nouveau mot de passe.

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

Obtenir de l’aide

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

Utilisez ces informations pour intégrer votre ressource Cloud NGFW. Vous trouverez également des informations sur la façon de localiser votre numéro de série Cloud NGFW et sur la création d’un dossier d’assistance.

Enregistrer le locataire Cloud NGFW lors de la connexion initiale

Cloud NGFW vous invitera à enregistrer un compte de support pour votre locataire Cloud NGFW après que vous aurez 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 auprès de l’un de ces comptes lors de la connexion initiale.

Il se peut que l’adresse e-mail utilisée pour vous abonner à Cloud NGFW soit différente de celle utilisée pour accéder au compte de support 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**.

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

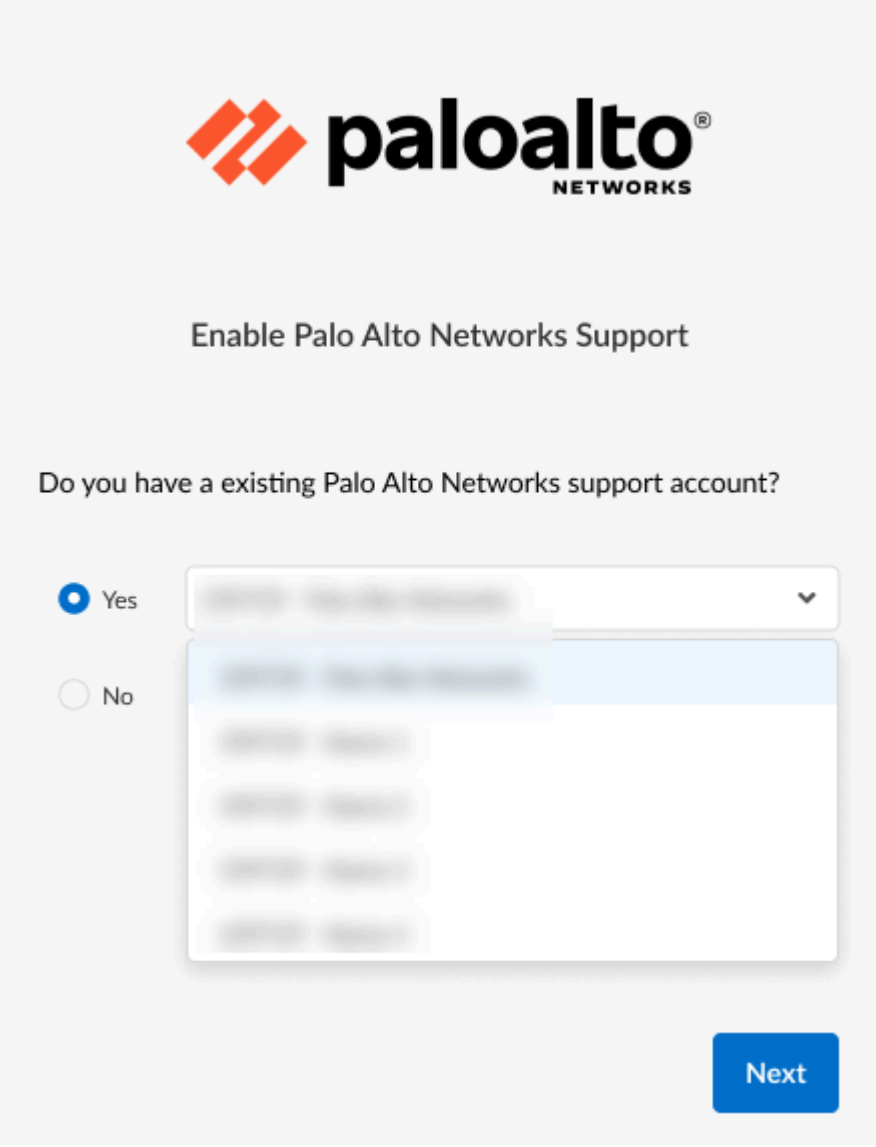
STEP 1 | Connectez-vous à la console Cloud NGFW.

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 devrez utiliser le portail de support client (CSP) pour enregistrer votre locataire Cloud NGFW, ou utiliser la console Cloud NGFW pour vous enregistrer sur le CSP.*

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

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



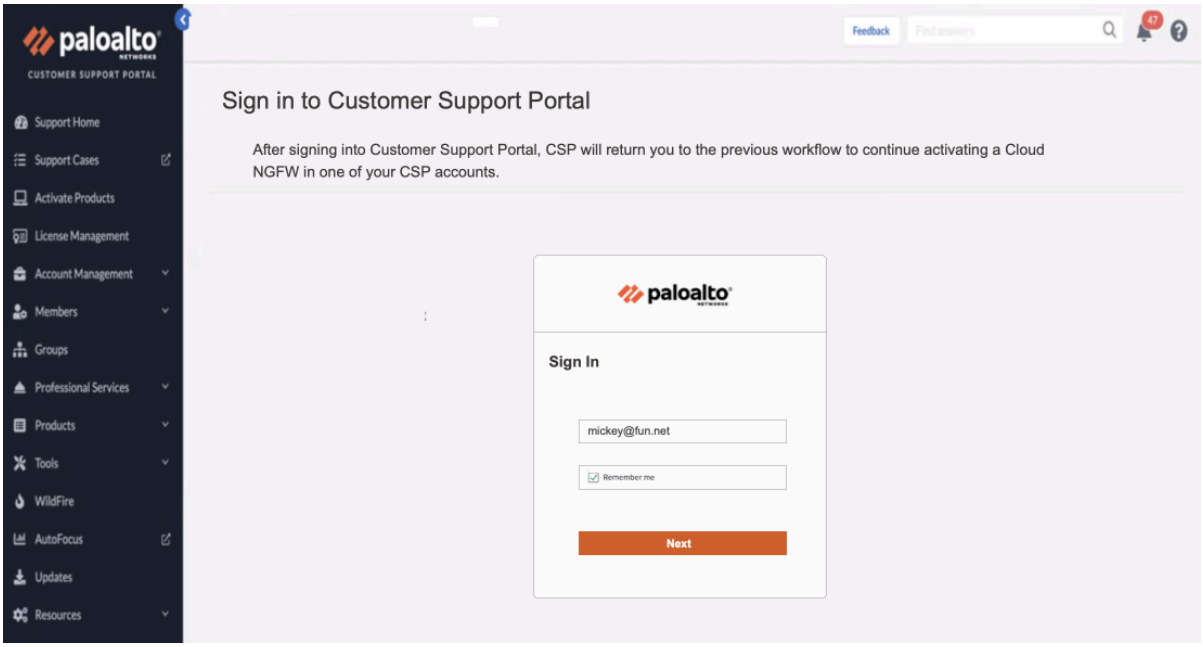
Si vous avez déjà enregistré votre compte de support client (CSP), la liste déroulante comporte les comptes existants. Toutefois, si vous êtes un nouvel utilisateur et que vous n'avez pas encore de compte, utilisez la page CSP pour créer un compte. Consultez Enregistrer votre locataire Cloud NGFW à l'aide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

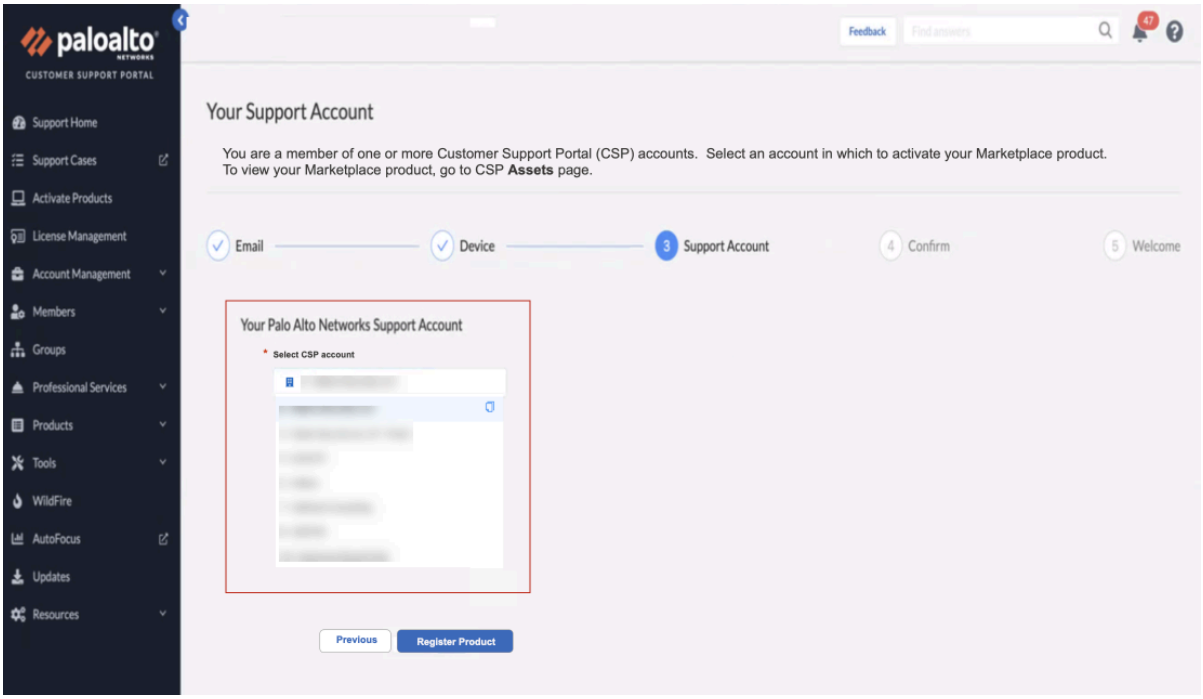
Vous pouvez utiliser le Customer Support Portal (portail de support client) pour enregistrer votre locataire Cloud NGFW.

Vous aurez besoin d'un compte pour vous connecter au CSP. Consultez Créer un compte de support client *pour en savoir plus.*

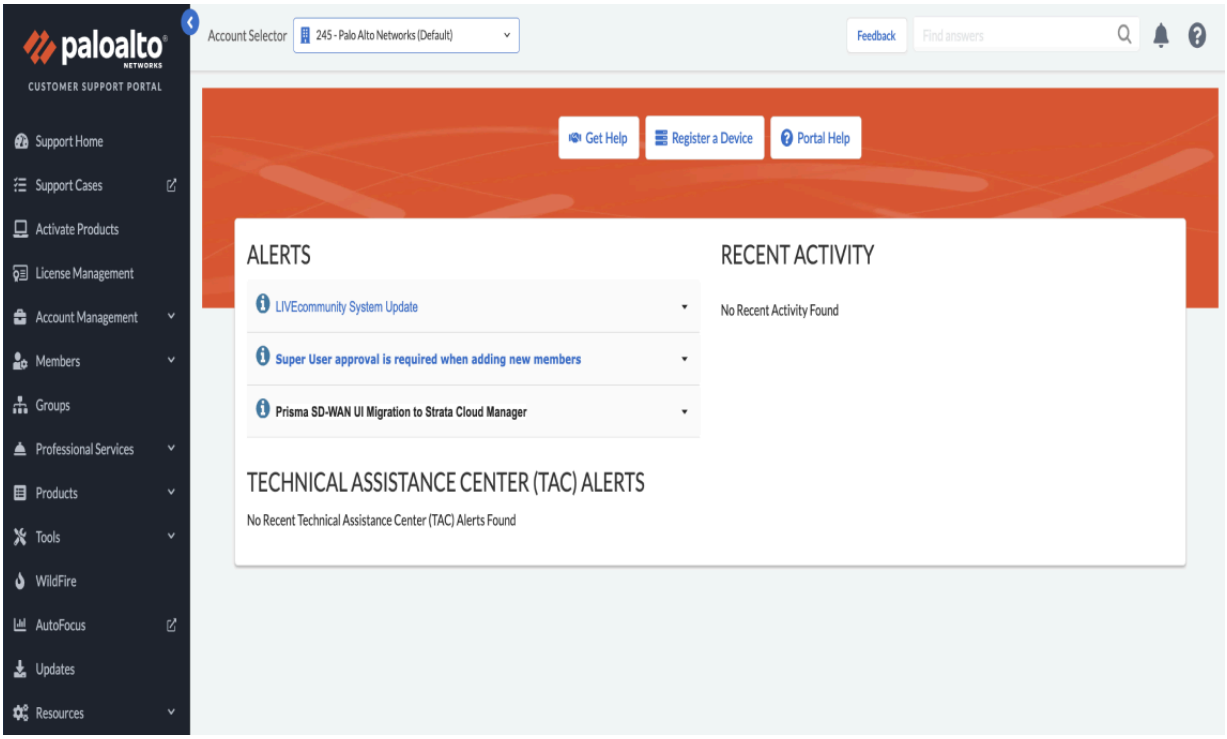
STEP 1 | Dans le Customer Support Portal (Portail de support client), saisissez vos informations d'identification de connexion, puis cliquez sur **Next (Suivant)**.



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 :



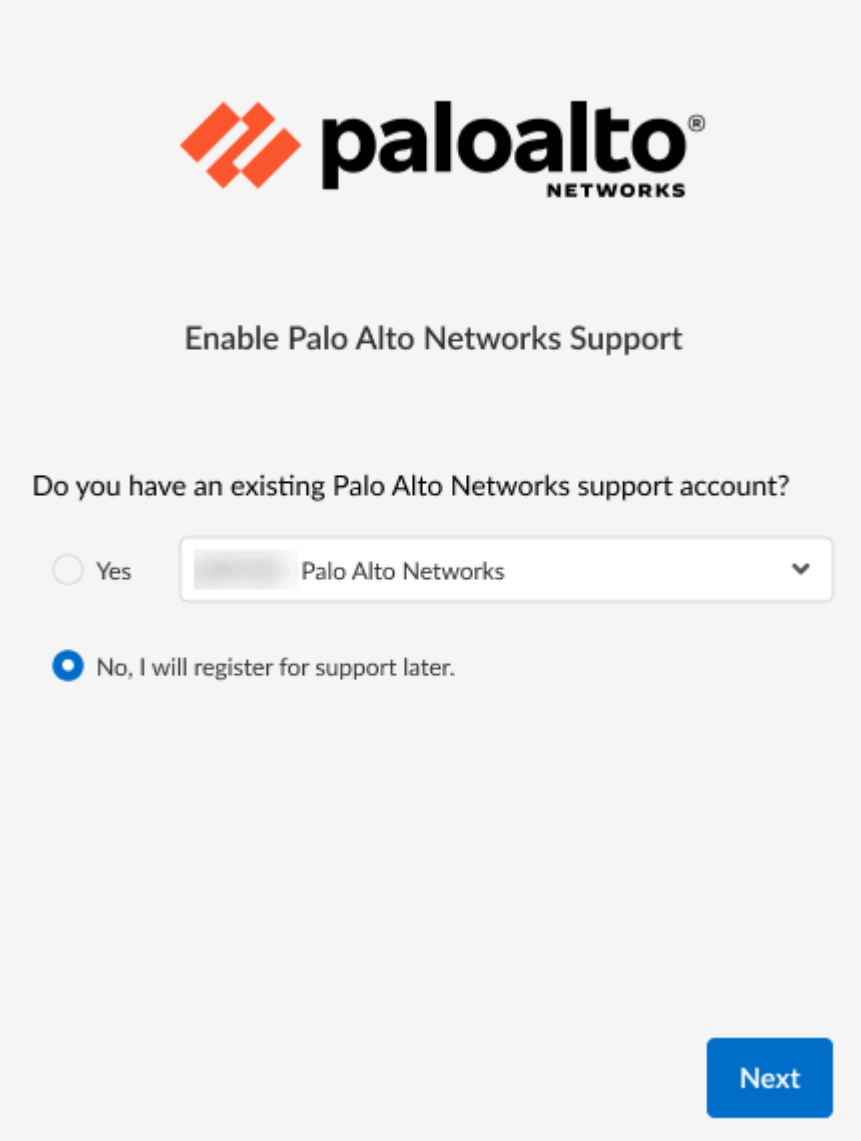
Enregistrer votre locataire Cloud NGFW sur le portail de support client à l’aide de la console Cloud NGFW

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.

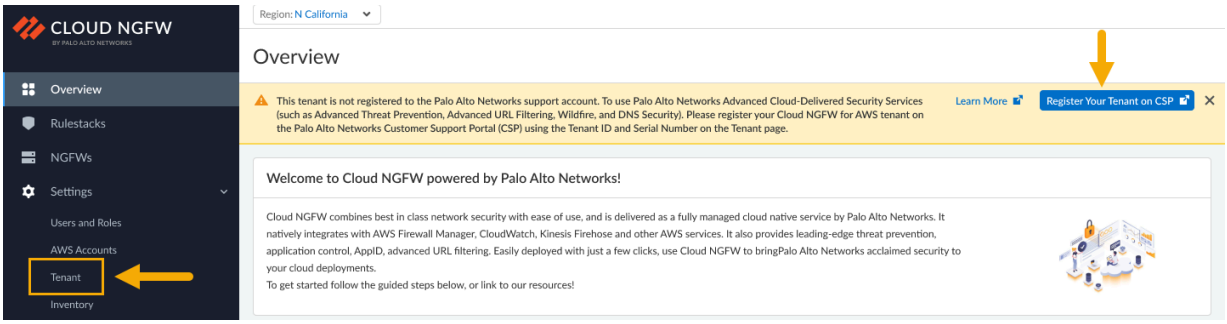
STEP 2 | Sur la page **Enable Palo Alto Networks Support (Activer le support Palo Alto Networks)**, sélectionnez **No (Non)**.

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)**.

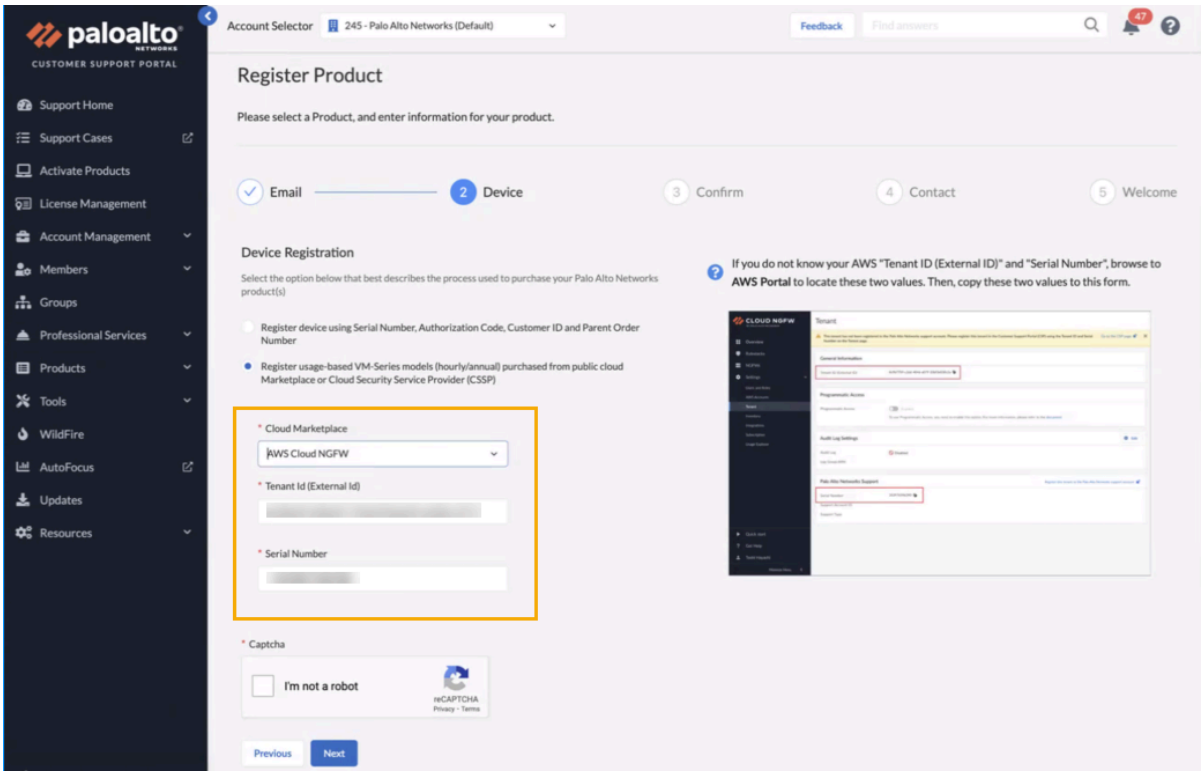
*Pour associer votre locataire Cloud NGFW à un compte sur le portail de support client, vous aurez besoin des informations d'enregistrement de votre périphérique, notamment le **Tenant ID (ID de locataire)** et le **Serial Number (Numéro de série)** de votre ressource Cloud NGFW. Ces informations sont 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).



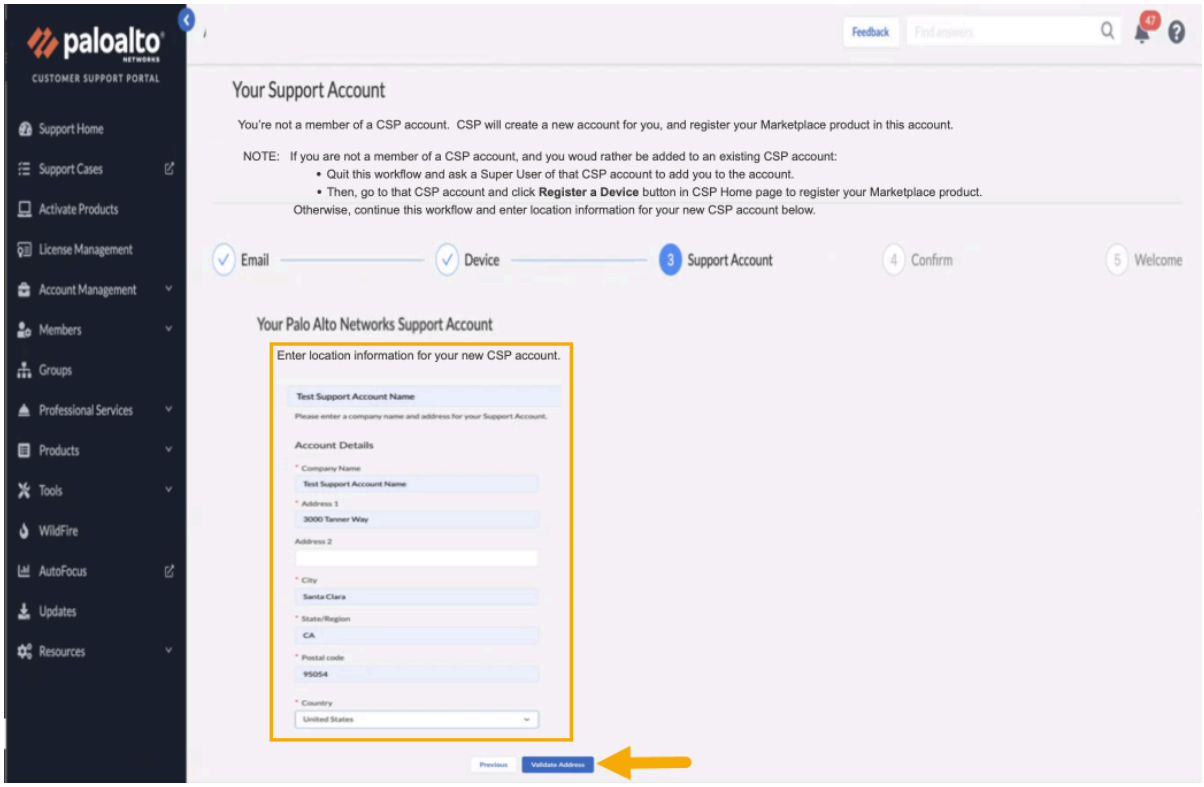
STEP 5 | Sur la page **Register Product (Enregistrer un produit)** du portail de support client, utilisez le menu déroulant pour sélectionner **AWS Cloud NGFW** pour le **Cloud Marketplace (Marketplace du cloud)**. Saisissez le **Tenant ID (ID de locataire)** et le **Serial Number (Numéro de série)**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

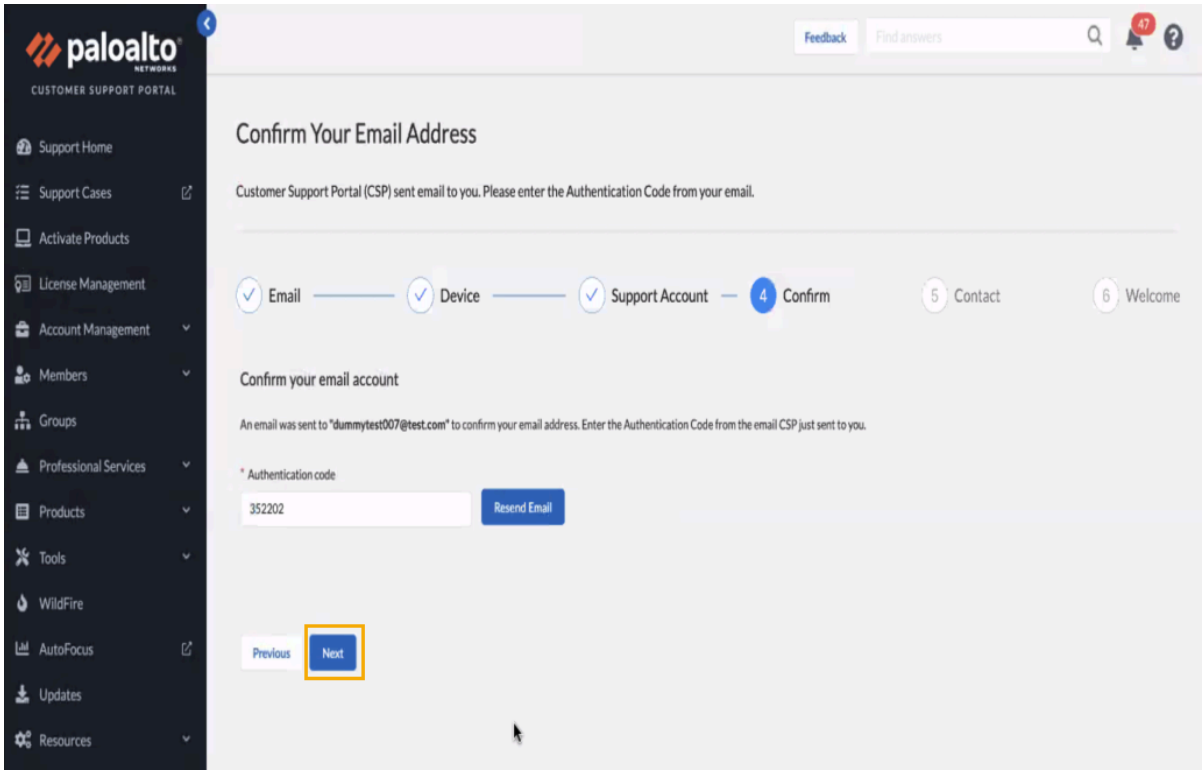


STEP 7 | Créez votre compte de support. Saisissez les **Account Details (Détails du compte)**, puis cliquez sur **Validate Address (Valider l’adresse).**



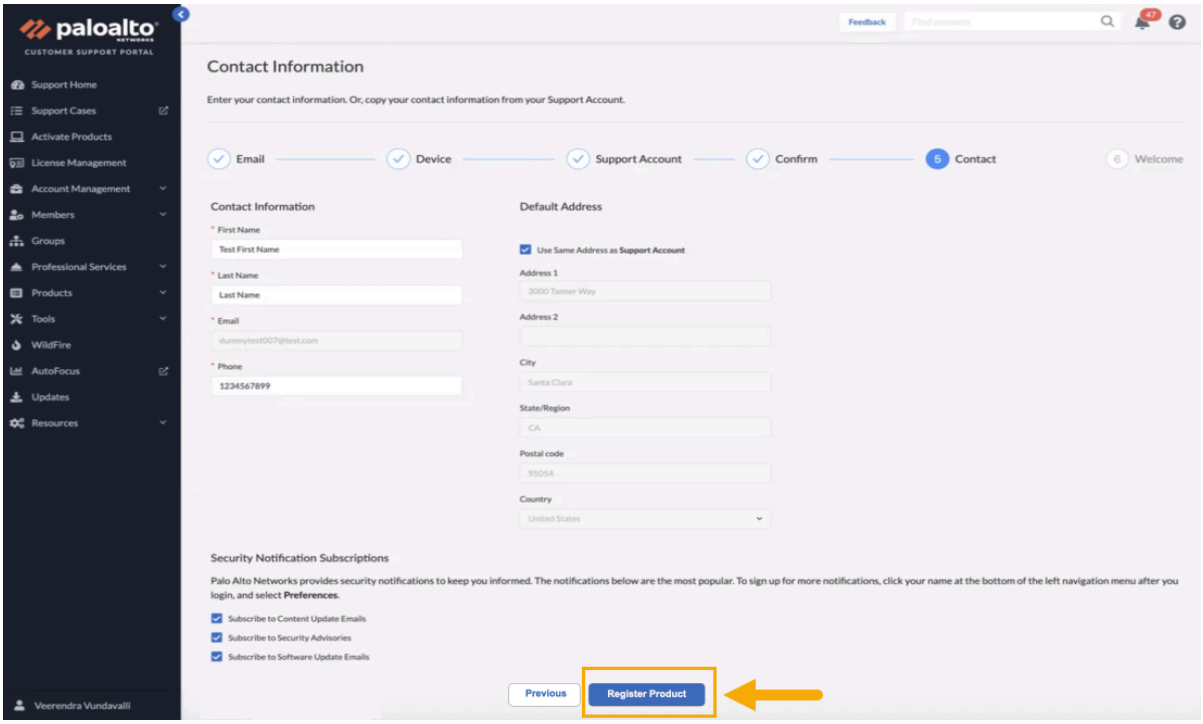
Vous serez peut-être invité à vérifier votre adresse pour le nouveau compte de support. Si nécessaire, vérifiez votre adresse et cliquez sur **OK** pour envoyer une requête d’authentification à l’adresse e-mail que vous avez indiquée.

STEP 8 | Consultez votre messagerie pour récupérer le code d'authentification. Saisissez le **Authentification code (Code d'authentification)**, puis cliquez sur **Next (Suivant)**.

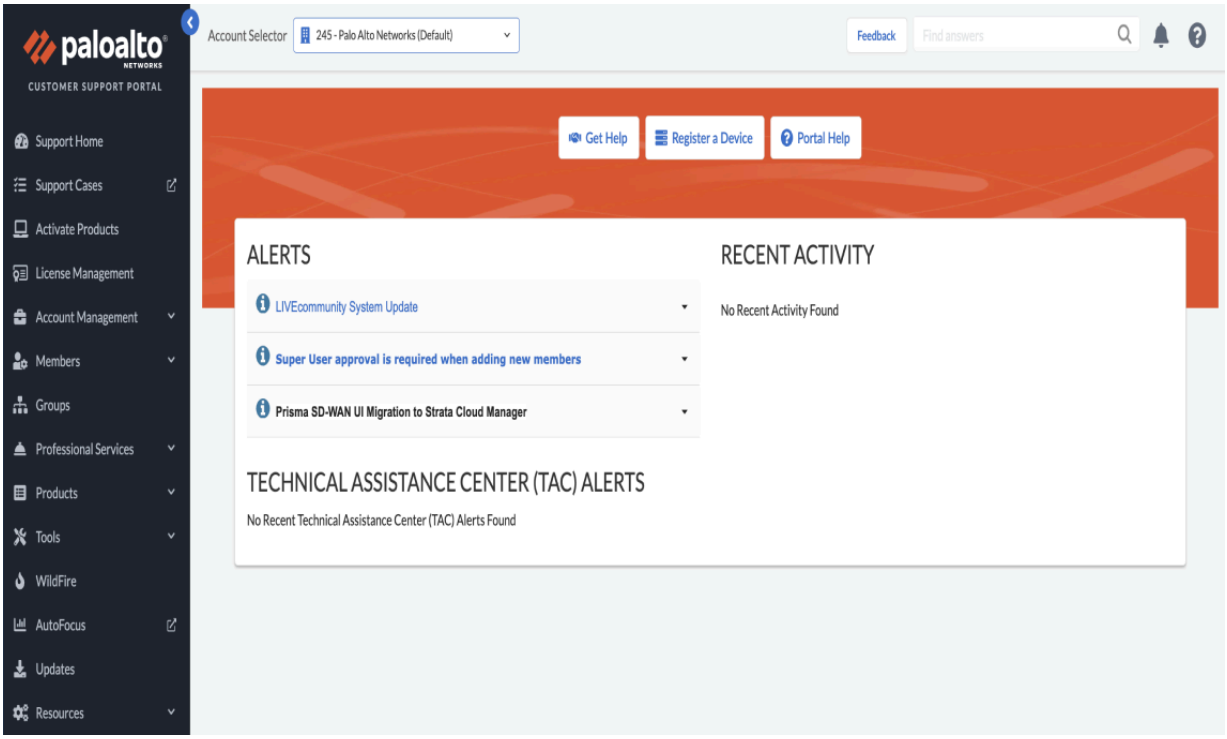


STEP 9 | Confirmez l'adresse e-mail de votre compte sur le portail de support client, puis cliquez sur **Next (Suivant)**.

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 :

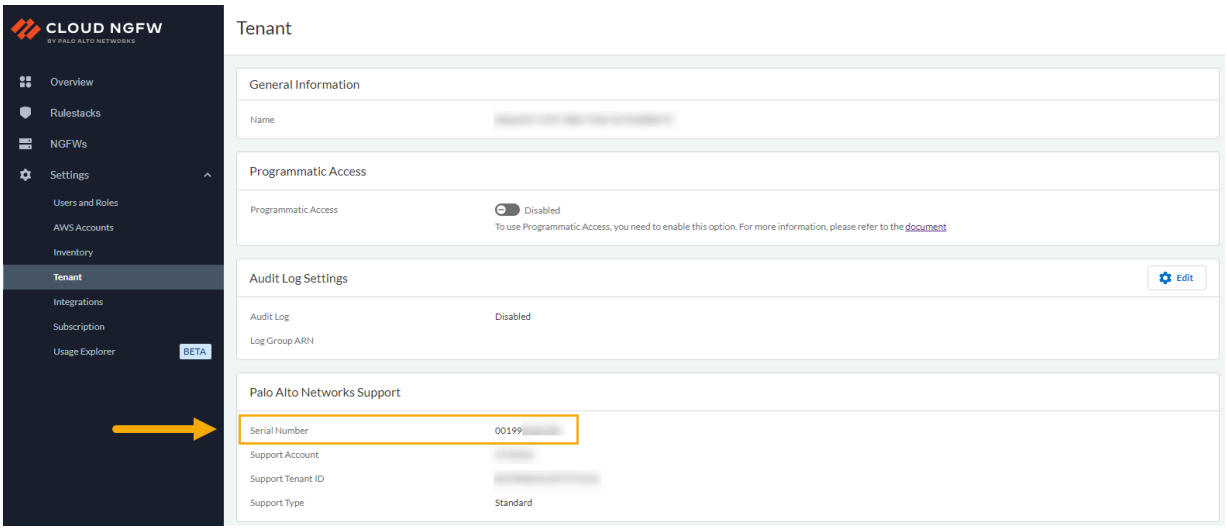


Rechercher le numéro de série de votre Cloud NGFW pour AWS

Pour rechercher le numéro de série de Cloud NGFW :

STEP 1 | Connectez-vous au locataire Cloud NGFW.

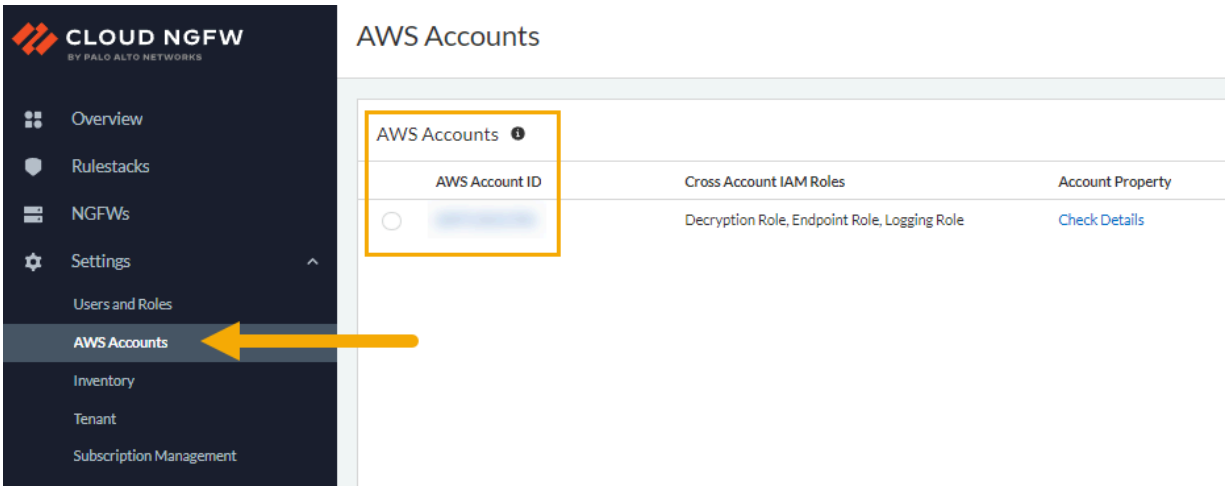
STEP 2 | Cliquez sur **Tenant (Locataire)**. La page Tenant (Locataire) affiche le **Serial Number (Numéro de série)** et des informations supplémentaires dans la section **Palo Alto Networks Support (Support Palo Alto Networks)**.



Créer un dossier d’assistance

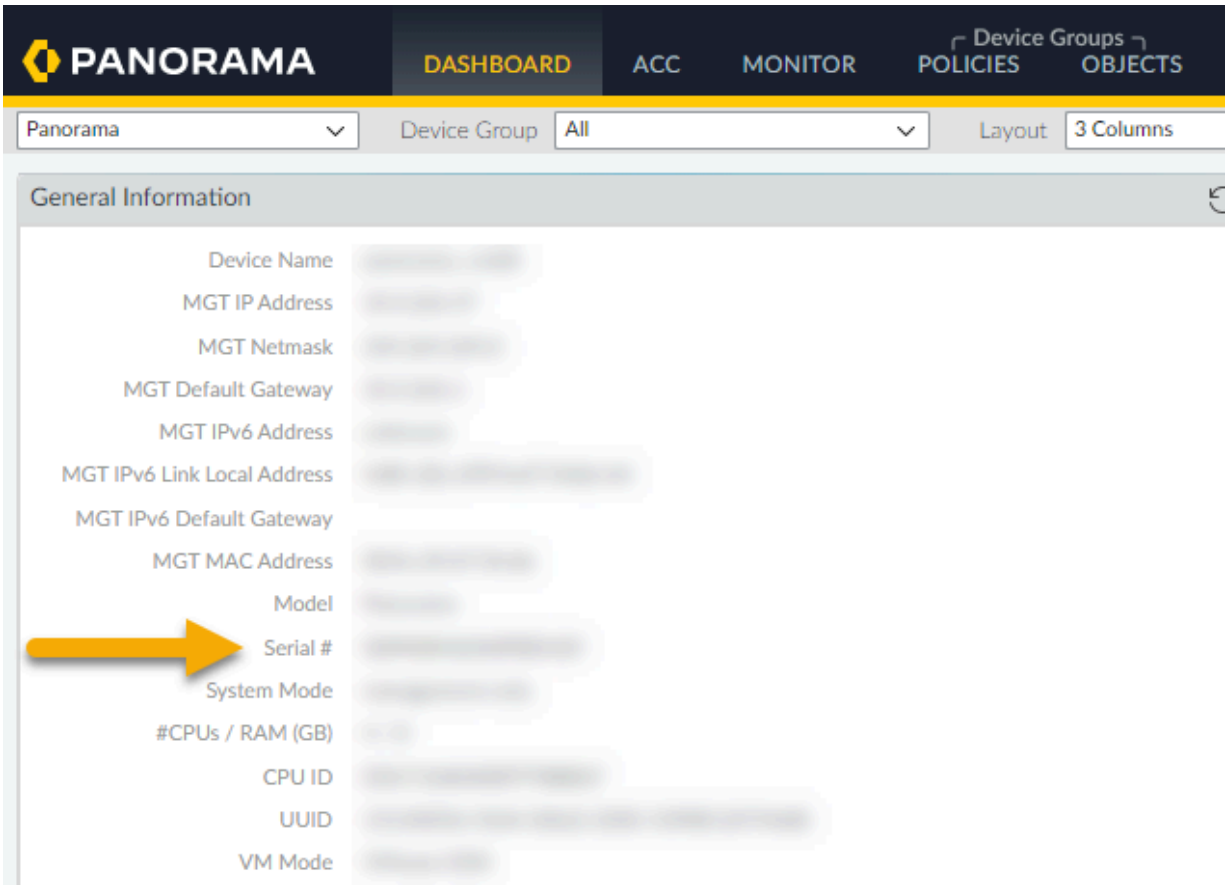
Pour créer une demande de support à l’aide de la console Cloud NGFW :

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

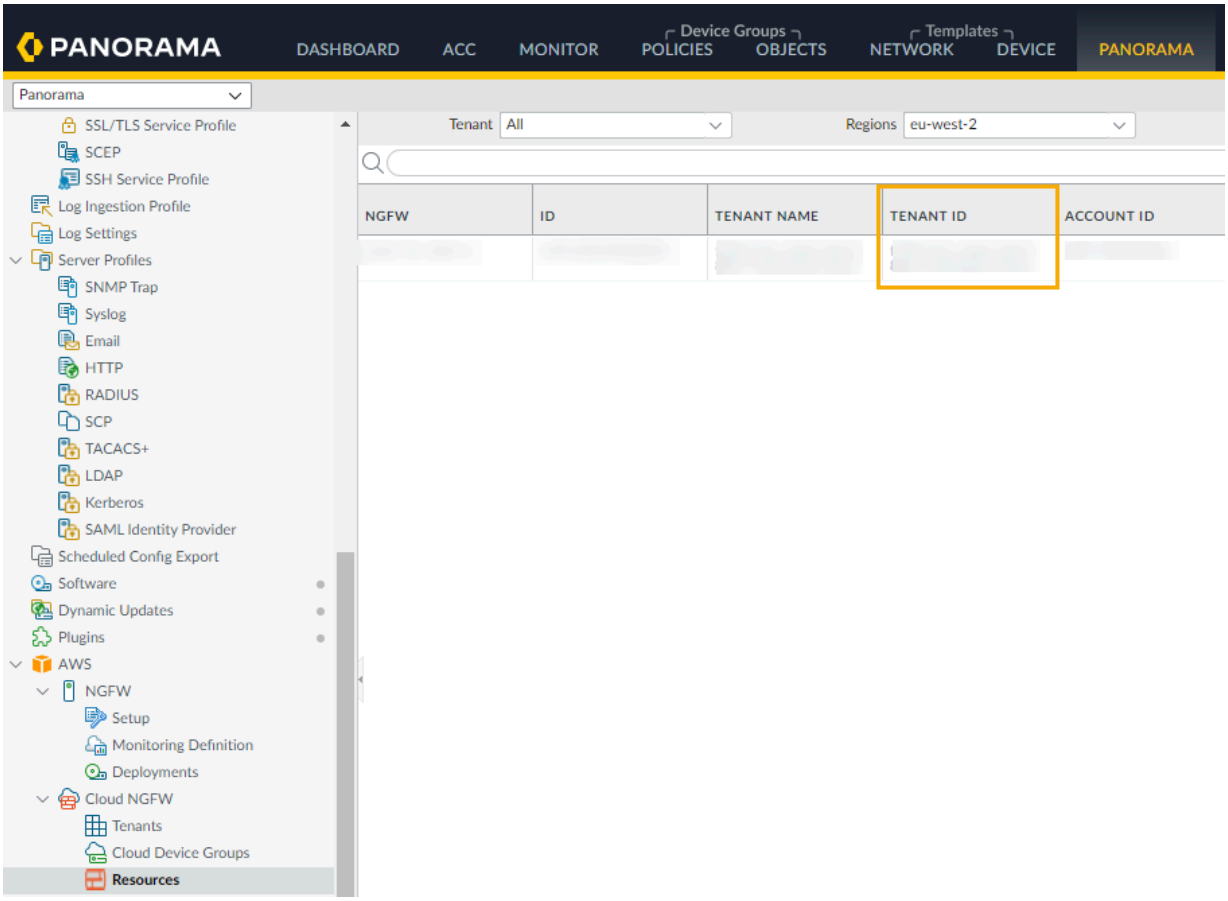


STEP 2 | Si nécessaire, utilisez la console Panorama pour déterminer des informations supplémentaires pour le dossier de support, telles que l'ID du locataire ou le numéro de série de Panorama.

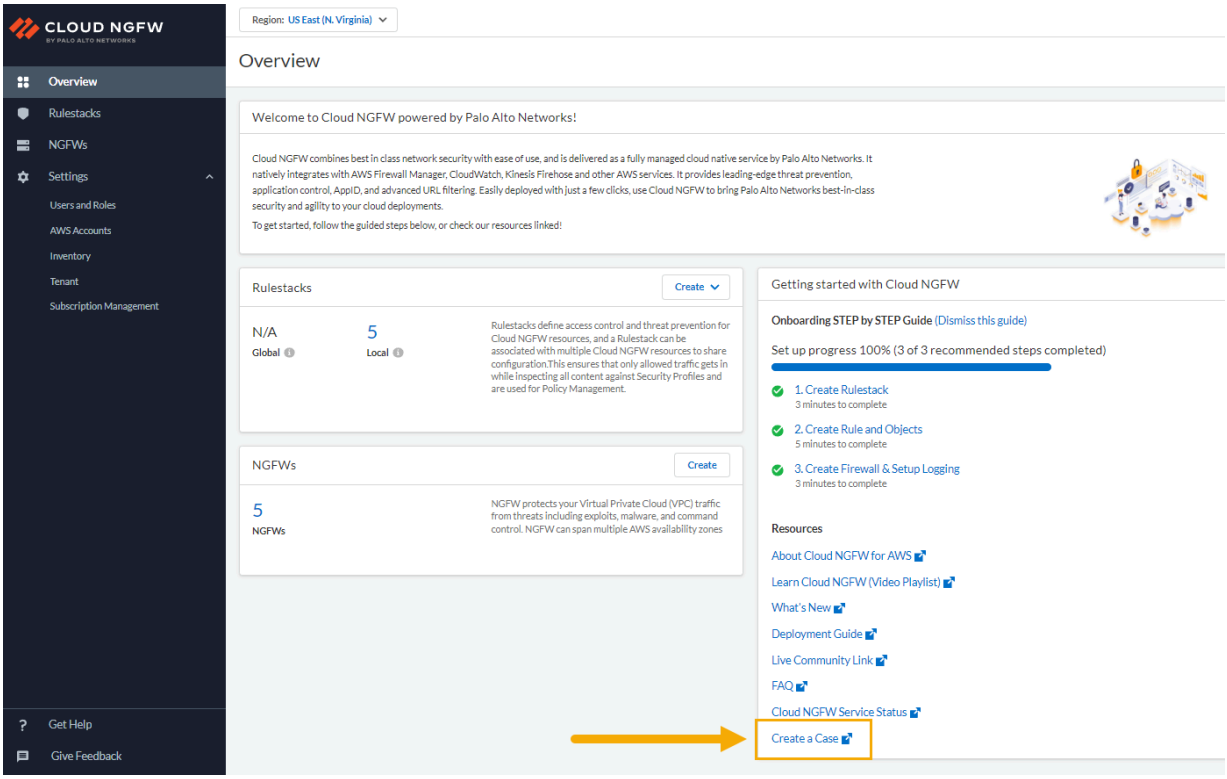
Recherchez le **Panorama serial number (numéro de série Panorama)** à l'aide du **Dashboard (Tableau de bord)** :



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)**.



Explorateur de l’utilisation

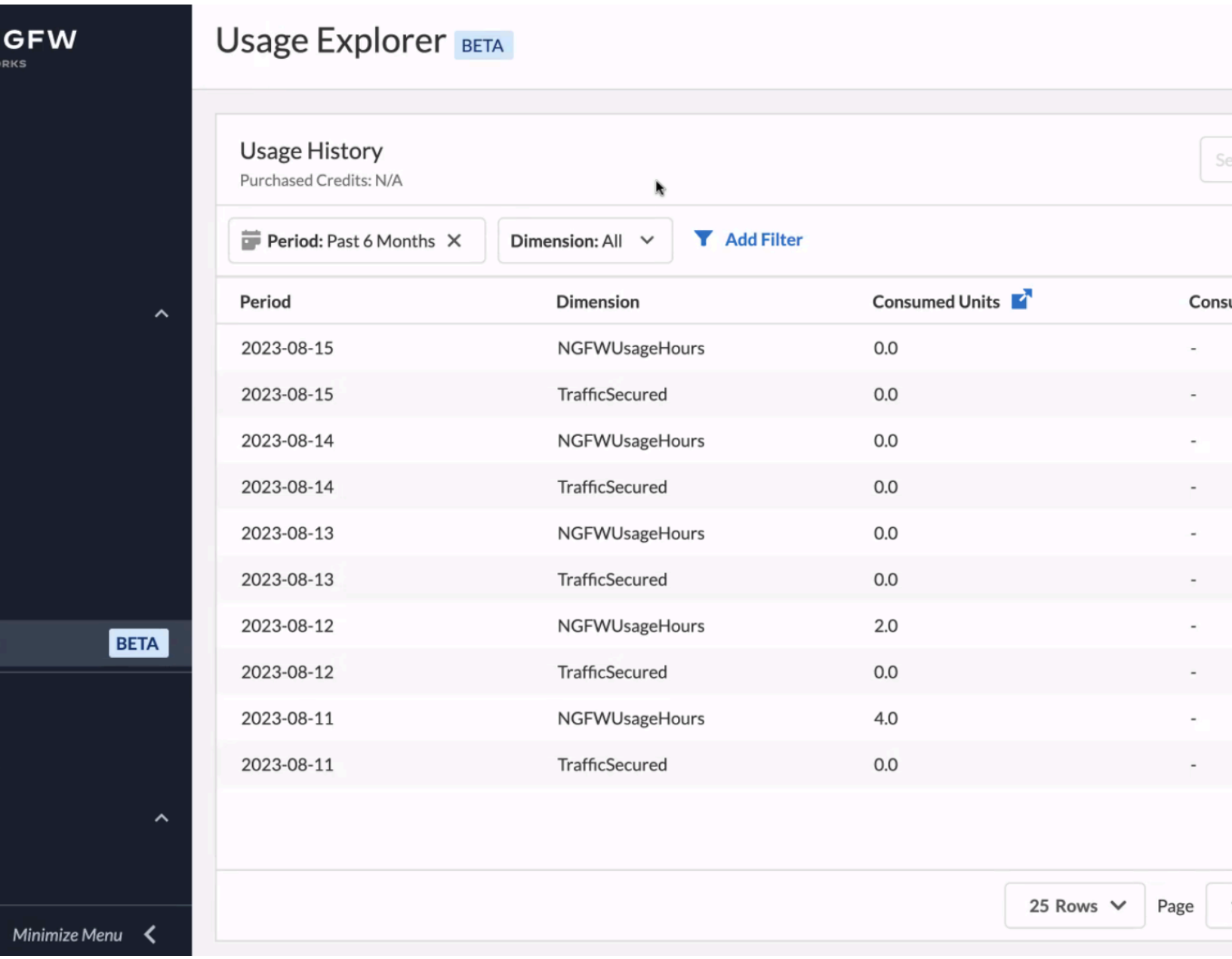
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d’utilisateur (locataire ou administrateur)

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)**.



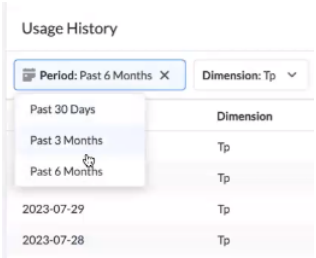
L’Explorateur de l’utilisation inclut des options permettant d’afficher la consommation sur une période donnée et vous permet de télécharger un fichier au format CSV afin de capturer des données pertinentes en vue d’une inspection future. L’historique de la consommation quotidienne est présenté dans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

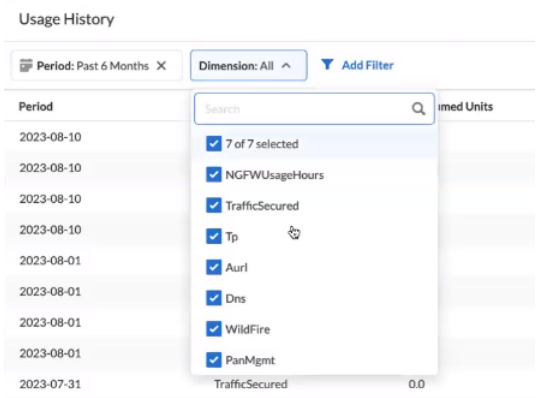
> *Vous ne pouvez appliquer un filtre que sur des dimensions prises en charge. L'option **Add filter (Ajouter un filtre)** ne fonctionne pas à l'heure actuelle dans cette version préliminaire.*

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 :

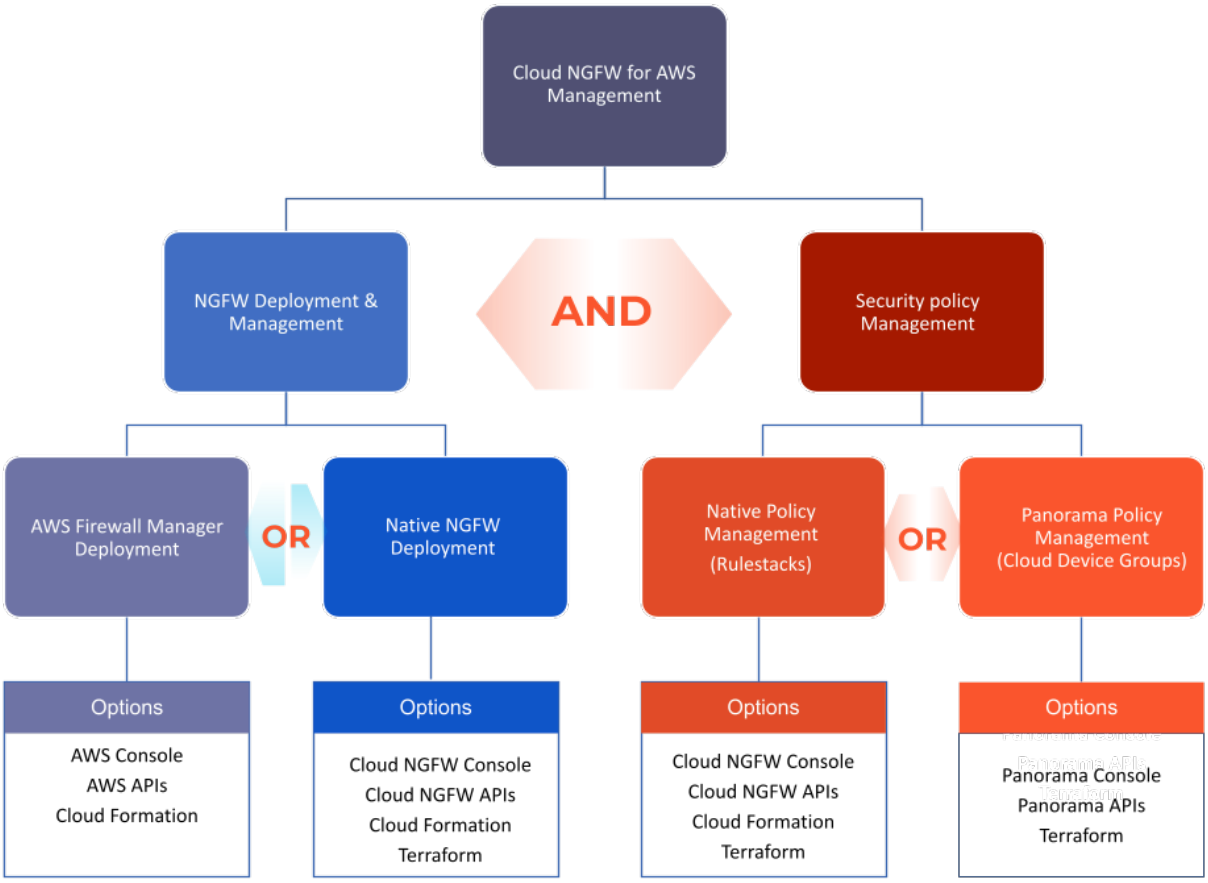


> *L'affichage de l'Explorateur de l'utilisation dépend du modèle d'abonnement du locataire Cloud NGFW, PAYG ou dans le cadre d'un contrat.*

Déployer

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

Cloud NGFW pour AWS propose plusieurs options pour le déploiement de ressources NGFW et la 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, comme Cloud Formation ou Terraform, pour créer ces ressources. Une fois les ressources Cloud NGFW créées, vous pouvez créer des politiques de sécurité pour ces ressources à l'aide de la gestion native des politiques (rulestacks) ou de la gestion des politiques de 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 de Panorama), AWS Firewall Manager vous redirige vers la console Cloud NGFW pour vous permettre de créer et de 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 d'API. Vous pouvez également créer les rulestacks à l'aide d'outils d'infrastructure as code, comme 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 de Panorama** : vous pouvez associer le locataire Cloud NGFW à un appareil Panorama pour créer et gérer des règles de politique pour vos ressources Cloud NGFW. Vous pouvez utiliser la console Panorama, des API ou Terraform pour créer ces règles de politique de sécurité sur les groupes d'appareils cloud. La politique que vous créez dans le groupe d'appareils cloud Panorama aura l'apparence d'une rulestack globale dans votre locataire Cloud NGFW.
- **Gestion des politiques de Strata Cloud Manager** : vous pouvez associer 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 web 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.

Création d’une ressource NGFW sur AWS

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

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 la façon de créer des terminaux NGFW : 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)**.

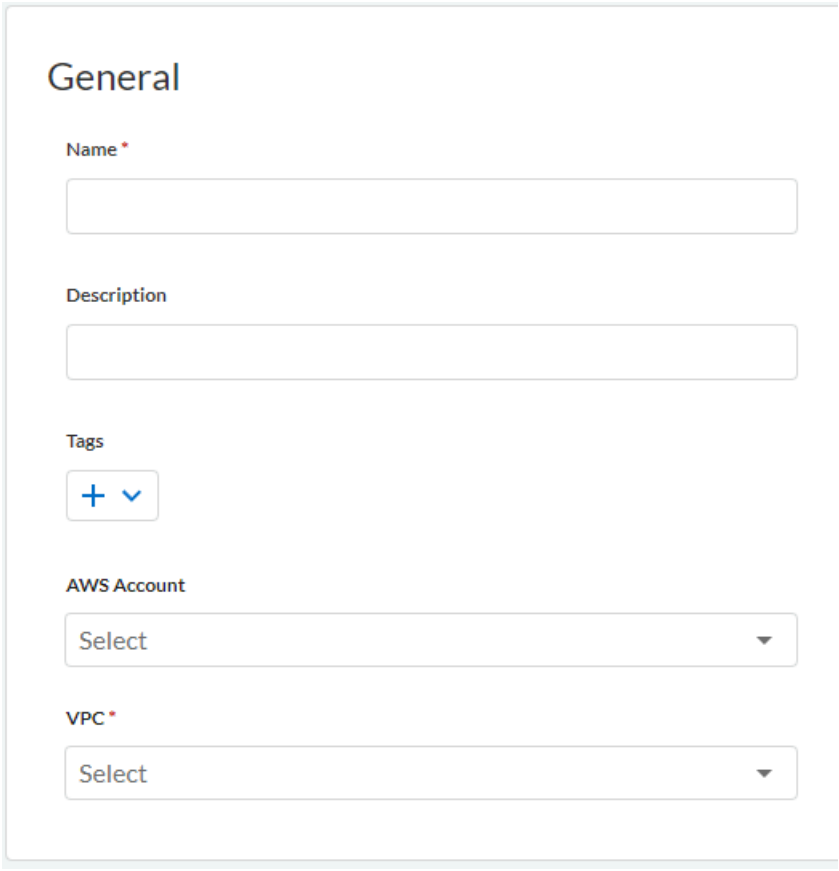
STEP 2 | Cliquez sur **Add Firewall (Ajouter un pare-feu)**.

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

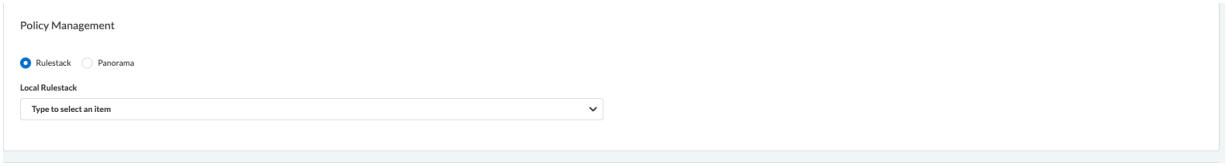
STEP 4 | (Facultatif) Saisissez une **Description (Description)**.

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 (mode généré par le service) ou non (mode géré par le client) ou des terminaux NGFW.

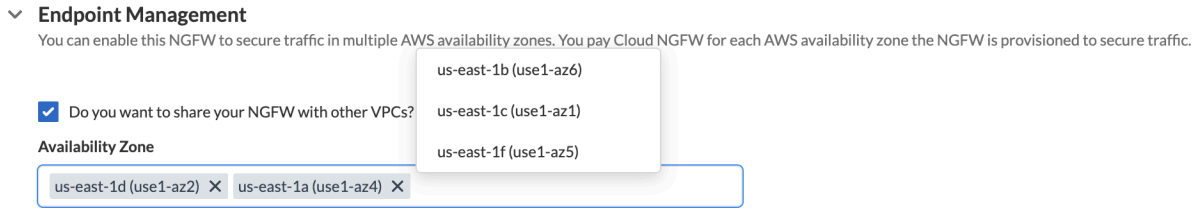
- **Yes (Oui)** (géré par le service) : en mode géré par le service, le locataire Cloud NGFW crée automatiquement des terminaux NGFW dans les sous-réseaux VPC que vous spécifiez. Effectuez la gestion de terminal pour le mode géré par le service via la console Cloud NGFW uniquement.

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 des terminaux Cloud NGFW pour AWS

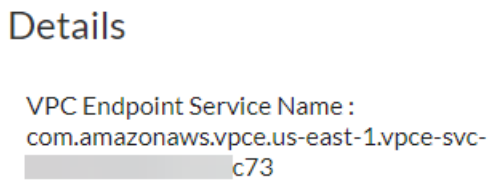
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d'utilisateur (locataire ou administrateur)

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 Virtual Private Cloud (cloud privé virtuel – VPC) que vous avez spécifié lors de la création du 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)**.

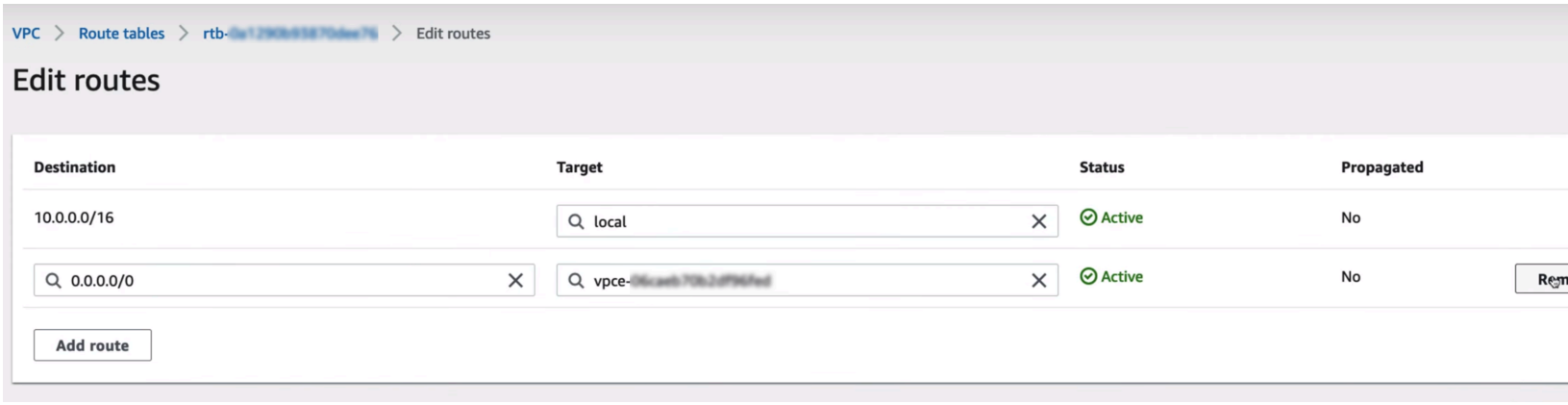
Supprimer une ressource Cloud NGFW

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

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.

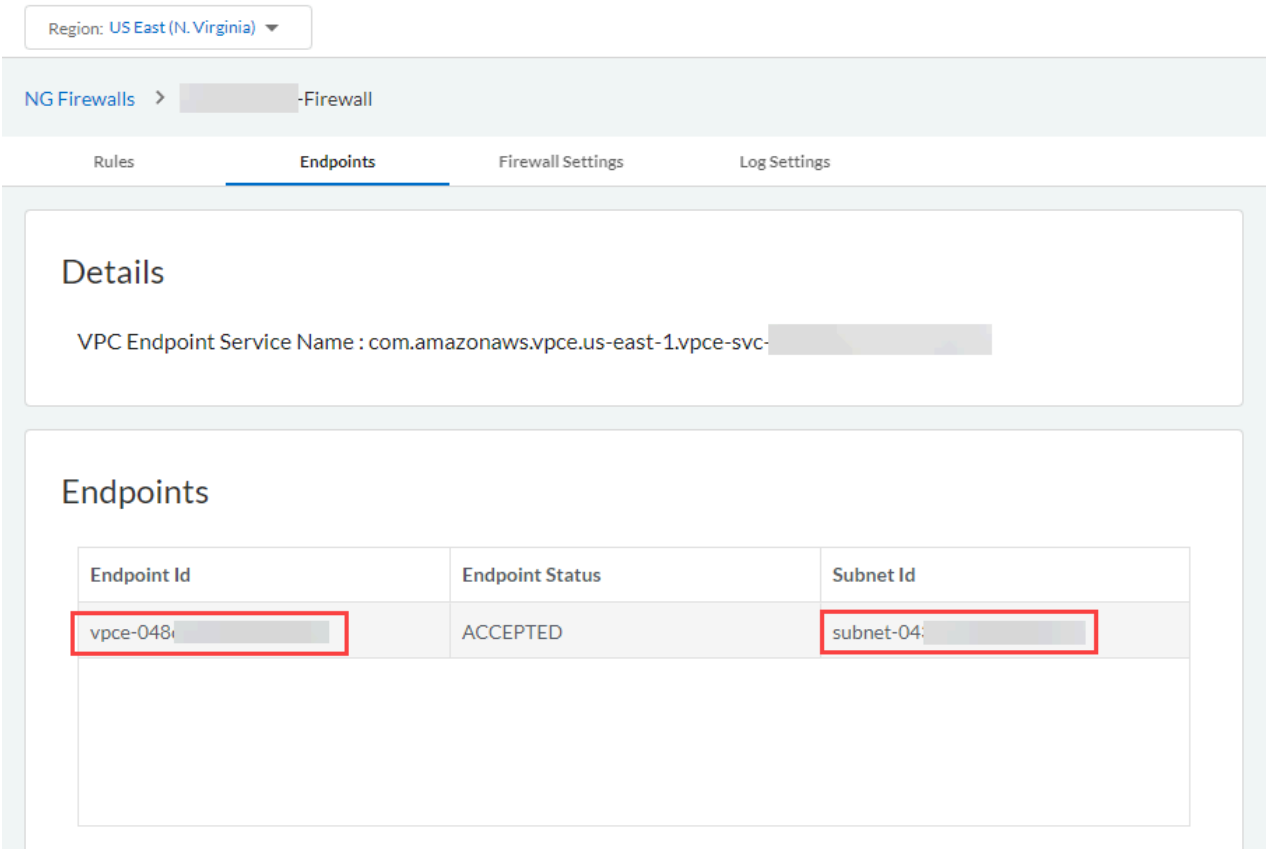
   Après quelques minutes, la ressource Cloud NGFW et tous ses terminaux sont supprimés de votre déploiement Cloud NGFW.

Diriger le trafic vers Cloud NGFW pour AWS

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

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 des terminaux d'un pare-feu spécifique dans la console Cloud NGFW sous **NGFWs (NGFW)** > **firewall-name (nom-du-pare-feu)** > **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

Configurer la plage de trafic privé

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

Cloud NGFW vous permet de spécifier la plage de trafic privé pour chaque terminal. Par défaut, les préfixes de plage de trafic privé incluent les plages d'adresses IP autorisées par le VPC, comme spécifié dans la RFC 1918 de l'IANA. Toutefois, votre réseau cloud hybride peut également inclure l'espace d'adressage partagé comme indiqué dans la RFC 6598 de l'IANA ou un certain ensemble de blocs CIDR publiquement acheminables dans les préfixes de plage de trafic privé.

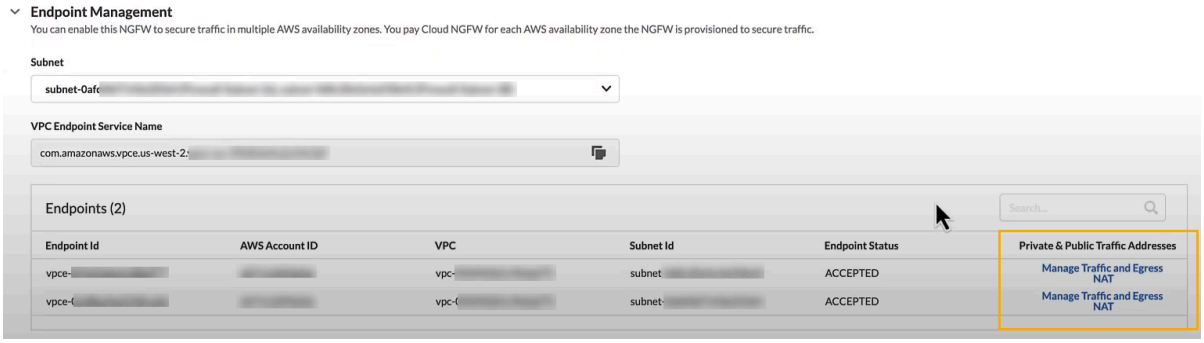
Pour configurer des plages de trafic privé :

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

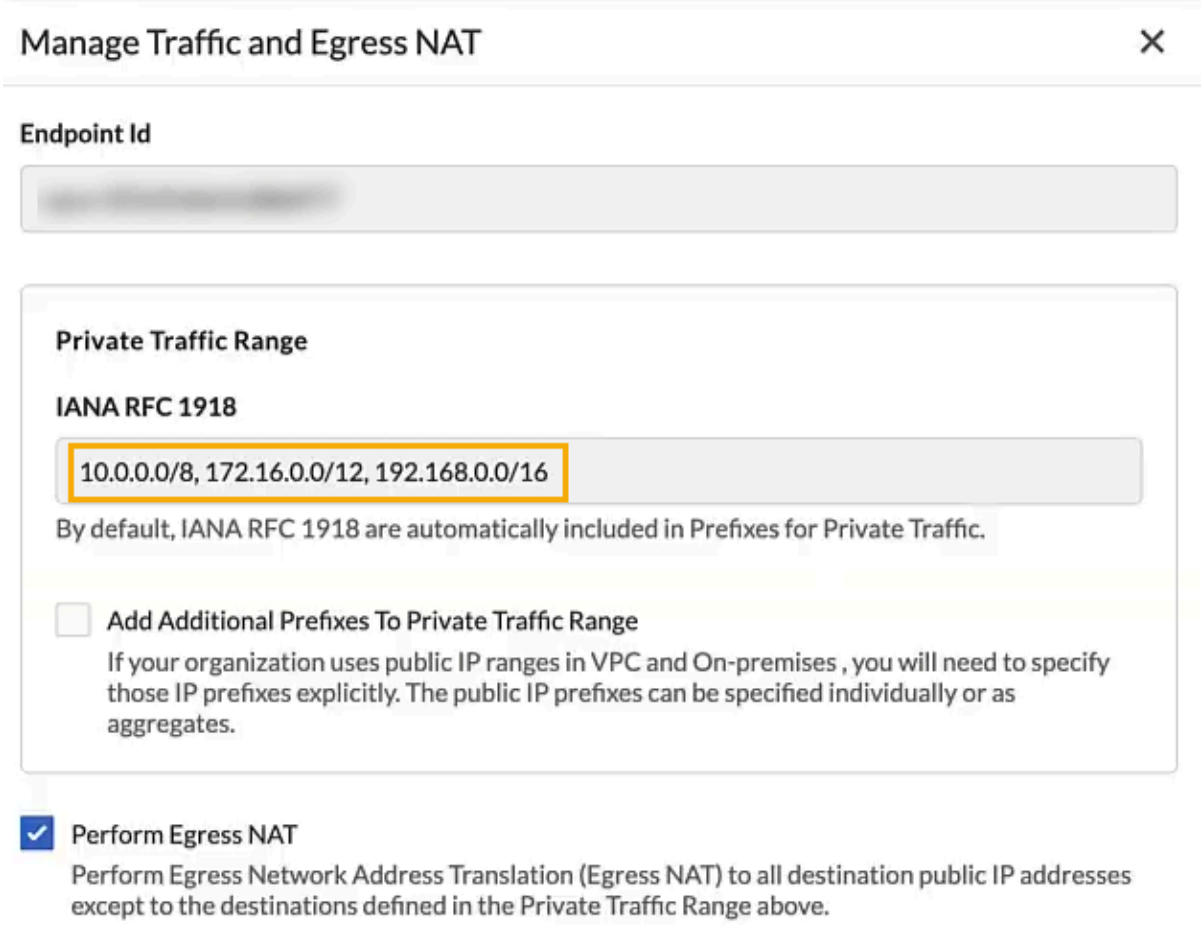
STEP 2 | Cliquez sur **NGFWs (NGFW)**.

STEP 3 | Dans la section Endpoint Management (Gestion des terminaux), sélectionnez le sous-réseau dans le menu déroulant.

STEP 4 | Sélectionnez **Manage Traffic and Egress NAT (Gérer le trafic et la NAT de sortie)** pour le terminal approprié dans la table **Endpoints (Terminaux)** :



STEP 5 | Sur l'écran **Manage Traffic and Egress NAT (Gérer le trafic et la NAT de sortie)**, spécifiez l'adresse IP (ou les adresses IP) que vous souhaitez inclure explicitement :



STEP 6 | Cochez la case **Add Additional Prefixes to Private Traffic Range (Ajouter des préfixes supplémentaires à la plage de trafic privé)**.

STEP 7 | Cochez la case **Perform Egress NAT (Effectuer la NAT de sortie)** pour faire en sorte que la traduction d'adresse ait lieu vers toutes les destinations d'adresses IP publiques, à l'exception de celles notées dans la plage de trafic privé.

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

Configurer le NAT de sortie

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

Cloud NGFW offre deux façons d'effectuer la NAT source sur le trafic sortant vers des destinations sur l'Internet public : la passerelle NAT AWS et la NAT de sortie Cloud NGFW.

La fonctionnalité NAT de sortie n'est pas prise en charge sur les pare-feu existants (ceux créés avant cette version de Cloud NGFW pour AWS). Créez-en un nouveau pour utiliser la NAT de sortie.

Passerelle NAT AWS

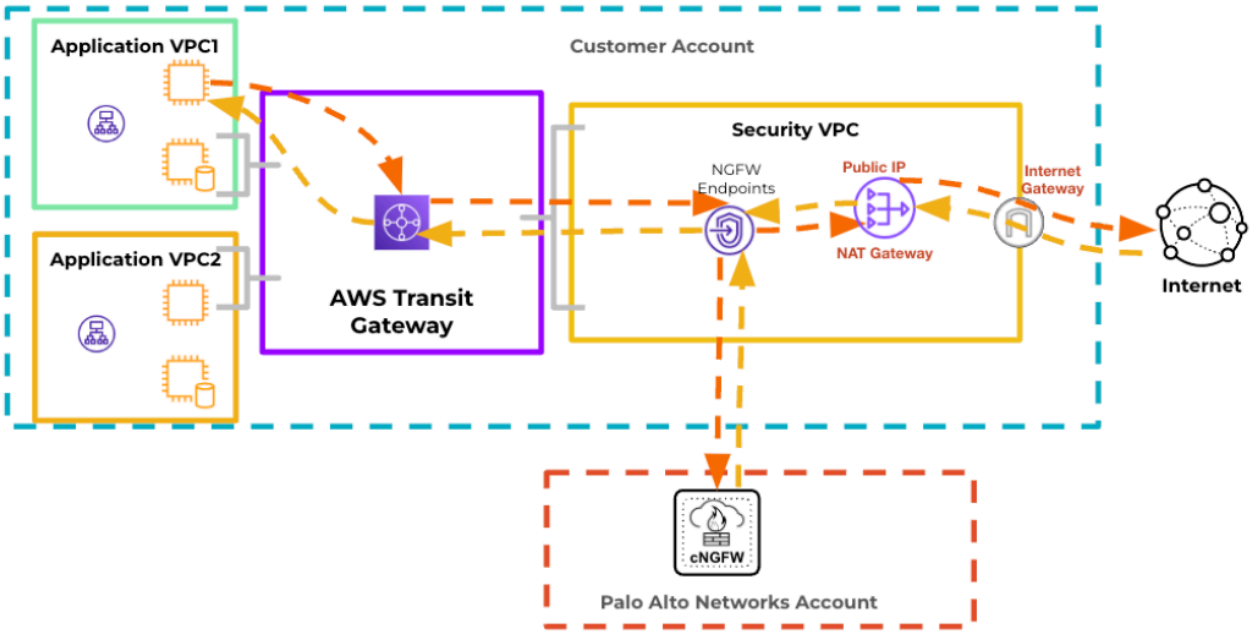
La passerelle NAT Amazon permet aux ressources VPC dans vos sous-réseaux privés d'accéder en toute sécurité à des services en dehors du sous-réseau, y compris sur l'Internet public, tout en gardant les ressources privées accessibles au trafic non sollicité.

Vous pouvez continuer à utiliser la passerelle NAT AWS dans votre VPC. Dans ce scénario, Cloud NGFW agit comme un dispositif de sécurité « bump-in-the-wire », dirigeant tout le trafic inspecté vers son terminal.

AWS vous facture la passerelle NAT et les coûts de transfert de données de sortie associés.

La NAT de sortie n'est pas prise en charge sur les pare-feu Strata Cloud Manager (SCM).

L'image ci-dessous illustre la NAT source sur le trafic Internet avec la passerelle NAT AWS :



Consultez Work with NAT gateways (Utilisation de passerelles NAT) *pour en savoir plus sur l'utilisation d'AWS pour configurer la NAT.*

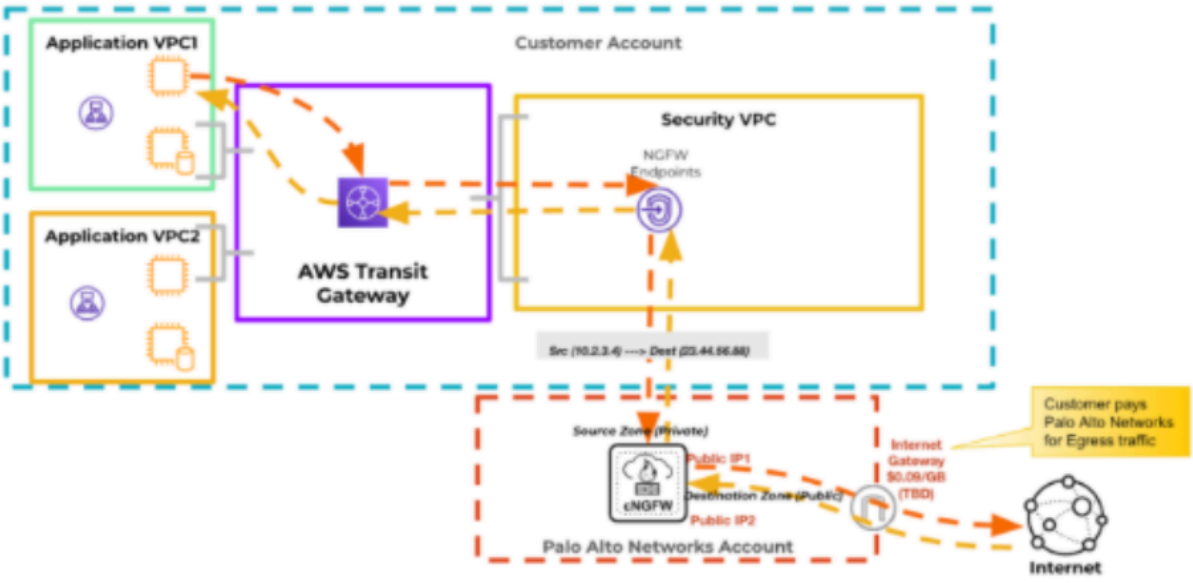
NAT de sortie Cloud NGFW

Une autre option consiste à configurer la fonctionnalité NAT de sortie. Dans ce cas, Cloud NGFW effectuera la NAT source sur tout le trafic sortant, sauf pour les sessions avec des adresses IP de destination comprises dans les préfixes de plage de trafic privé définis pour le terminal sur lequel le trafic entre dans la ressource Cloud NGFW. Le cas échéant, la ressource Cloud NGFW ne redirige pas le trafic inspecté vers le terminal. À la place, le trafic de sortie inspecté est envoyé directement sur Internet. Vous ne devez plus payer de coûts de passerelle NAT AWS, mais Palo Alto Networks vous facture le transfert de données du trafic de sortie. Cependant, vous associerez des adresses IP publiques à la ressource Cloud NGFW de l'une des deux manières suivantes :

1. Configurez la ressource Cloud NGFW pour qu'elle utilise des adresses IP élastiques (EIP) gérées par Palo Alto Networks afin d'effectuer la NAT source pour votre VPC. Dans ce cas, vous devrez payer des coûts de gestion d'EIP horaires.

2. Transférez vos adresses BYOIP vers Cloud NGFW depuis votre compte AWS pour éviter les coûts de gestion d'EIP horaires. Pour en savoir plus, consultez BYOIPs with AWS IPAM (Adresses BYOIP avec AWS IPAM).

L'image ci-dessous illustre le fonctionnement de la NAT source sur le trafic Internet avec la NAT de sortie Cloud NGFW ; NAT source sur le trafic Internet avec la NAT de sortie de Cloud NGFW :

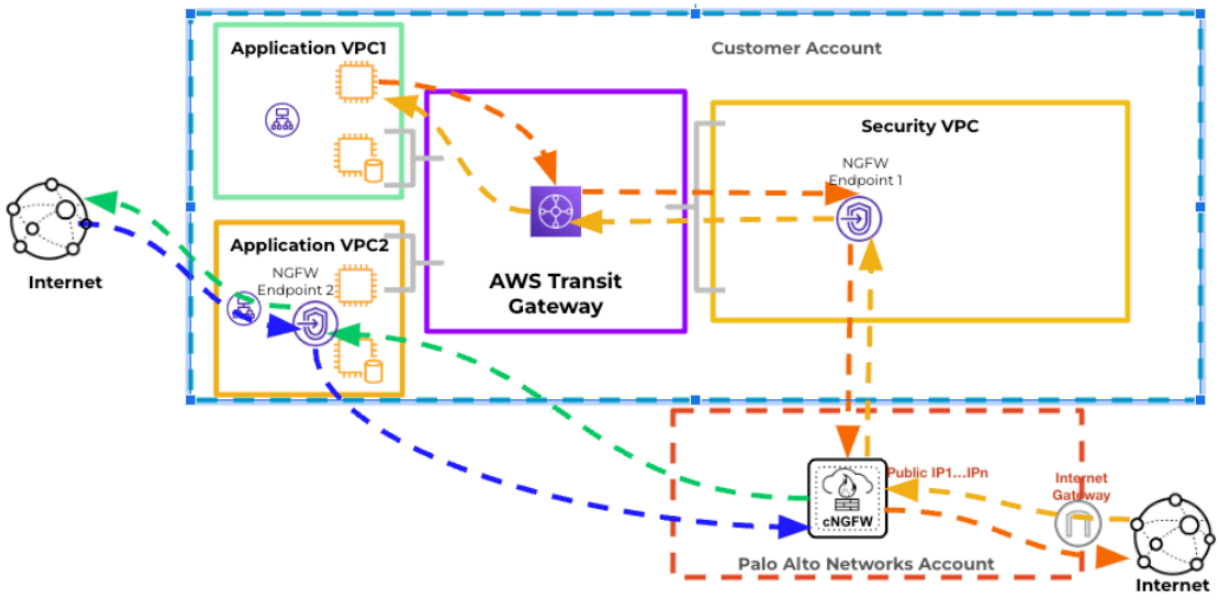


Paramètres NAT hybrides

Vous pouvez activer la NAT de sortie pour une ressource NGFW, mais vous pouvez personnaliser le paramètre NAT de sortie pour le désactiver sur un ou plusieurs terminaux. Le cas échéant, Cloud NGFW fonctionne comme suit :

1. Si vous désactivez la NAT de sortie sur un terminal, Cloud NGFW agit comme un dispositif de sécurité « bump-in-the-wire », dirigeant tout le trafic inspecté vers le terminal.
2. Si vous laissez la NAT de sortie activée sur un terminal, Cloud NGFW redirige le trafic inspecté directement vers Internet.

Dans l'image ci-dessous, la NAT de sortie est activée pour le terminal 1, mais désactivée pour le terminal 2 :



Configurer la NAT de sortie avec des EIP AWS gérées par Palo Alto Networks

Dans AWS, une adresse IP élastique (EIP) représente une adresse IPv4 statique utilisée pour l'informatique en nuage dynamique. Une adresse IP élastique est accessible depuis l'Internet public, mais vous pouvez l'associer à une instance privée pour permettre la communication avec Internet. La NAT de sortie est prise en charge uniquement pour la gestion des politiques de rulestacks et de Panorama.

Pour configurer la NAT de sortie avec des EIP AWS gérées par Palo Alto Networks :

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

STEP 2 | Cliquez sur **NGFWs (NGFW)**.

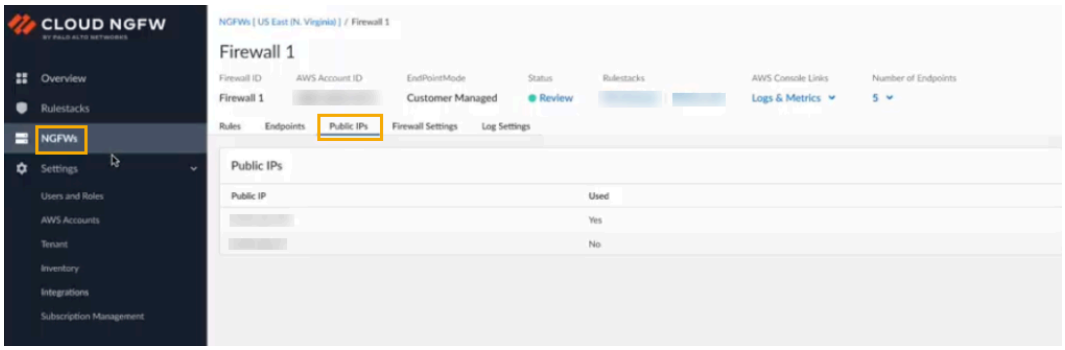
STEP 3 | Créer une nouvelle ressource NGFW.

STEP 4 | Dans la section **Policy Management (Gestion des politiques)**, sélectionnez **Panorama**. Utilisez le menu déroulant pour sélectionner le Panorama intégré.

STEP 5 | Dans la section **Egress NAT (NAT de sortie)**, sélectionnez **Enable Egress NAT (Activer la NAT de sortie)**.

STEP 6 | Dans la section **Public IPs (Adresses IP publiques)**, sélectionnez **AWS Service IPs (Adresses IP de service AWS)**.

*Sélectionnez l'onglet **Public IPs (Adresses IP publiques)** sur la page du pare-feu pour afficher la liste des adresses IP prises en charge pour le trafic NAT de sortie :*



Une fois le pare-feu créé, vérifiez son état.

Configurer la NAT de sortie avec des adresses BYOIP (Bring Your Own IP, apportez votre propre adresse IP)

Dans ce scénario, vous transférerez les adresses BYOIP de votre compte AWS pour éviter de devoir payer des coûts de gestion d'EIP horaires.

Pour utiliser des adresses BYOIP, vous devez créer un groupe IP Address Manager (IPAM) dans votre compte AWS et le partager dans votre compte de déploiement Cloud NGFW pour AWS. IPAM vous aide à gérer votre schéma d'adressage IP pour répondre aux exigences de sécurité. Consultez Bring your own IP addresses (Apportez vos propres adresses IP) sur le site AWS pour en savoir plus. La NAT de sortie est prise en charge uniquement pour la gestion des politiques de rulestacks et de Panorama.

*Lors de la création d'un groupe IPAM dans AWS, vous devez ajouter l'ID de compte AWS de Palo Alto Networks à la liste blanche pour que Cloud NGFW puisse partager des adresses IP entre le plan de données Cloud NGFW et AWS. Lors du processus de création du groupe IPAM, sélectionnez l'option **Allow Amazon VPC IP Address Manager (Autoriser le gestionnaire d'adresses IP Amazon VPC)** (une étape obligatoire pour la création du pool IPAM) ; spécifiez l'ID de compte du plan de données AWS pour votre ressource Cloud NGFW : 010510656586.*

La création d'un groupe IPAM peut prendre jusqu'à 10 minutes.

Créer un groupe IPAM

Pour créer un groupe IPAM :

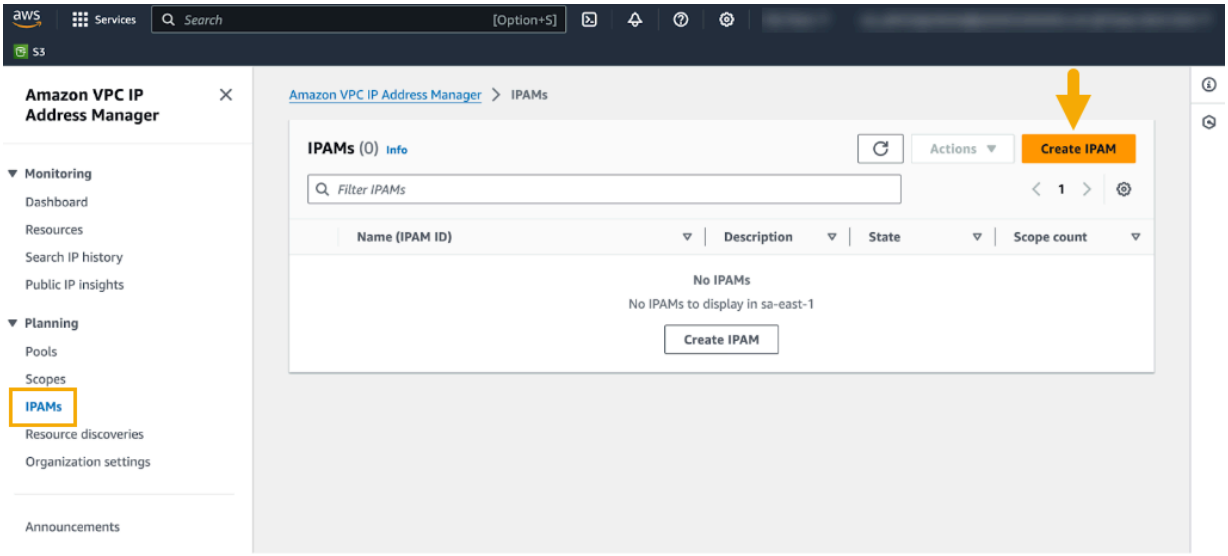
STEP 1 | Connectez-vous au gestionnaire d'adresses IP AWS VPC.

STEP 2 | Sélectionnez **Planning (Planification) > IPAMs (IPAM)**.

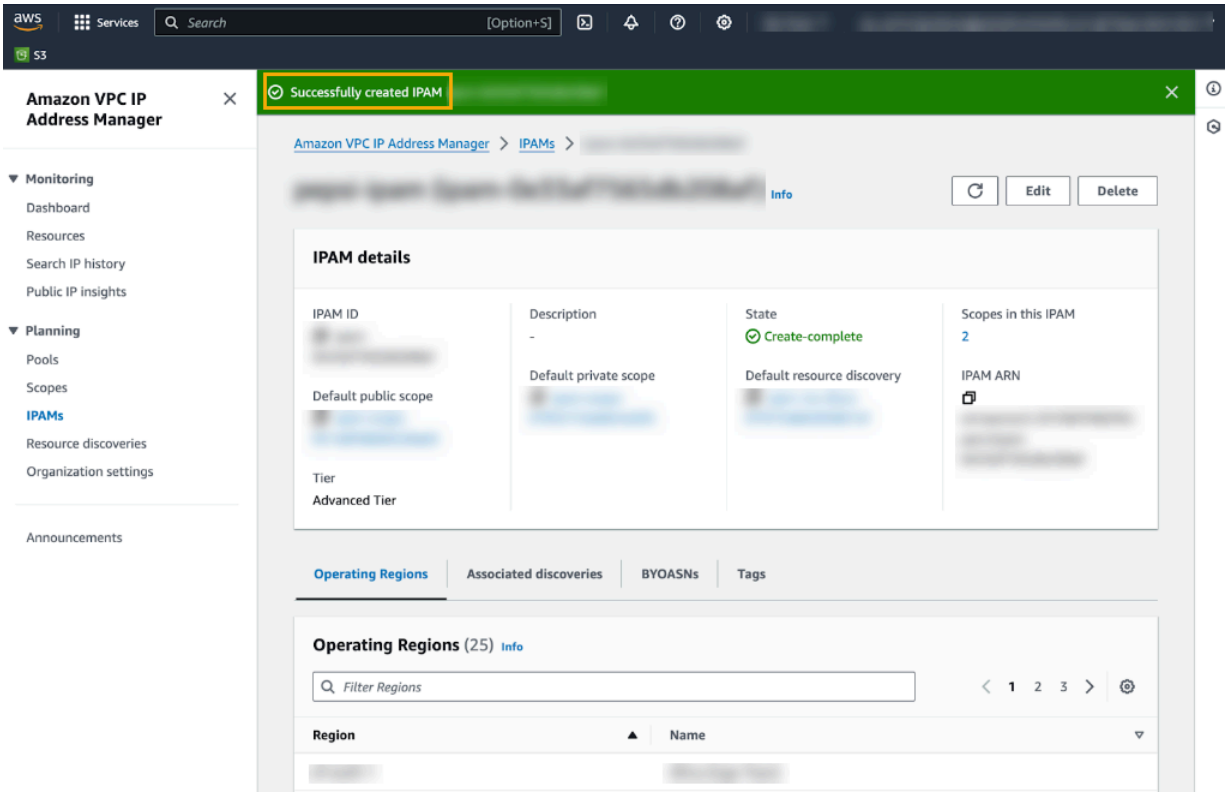
STEP 3 | Sur la page **IPAMs (IPAM)**, cliquez sur **Create IPAM (Créer un IPAM)**.

Pour en savoir plus, consultez les instructions sur la page AWS Create an IPAM (Créer un IPAM).

Une fois que vous avez créé l'IPAM, **AWS VPC IP Address Manager (Gestionnaire d'adresses IP AWS VPC)** affiche les détails de l'IPAM :

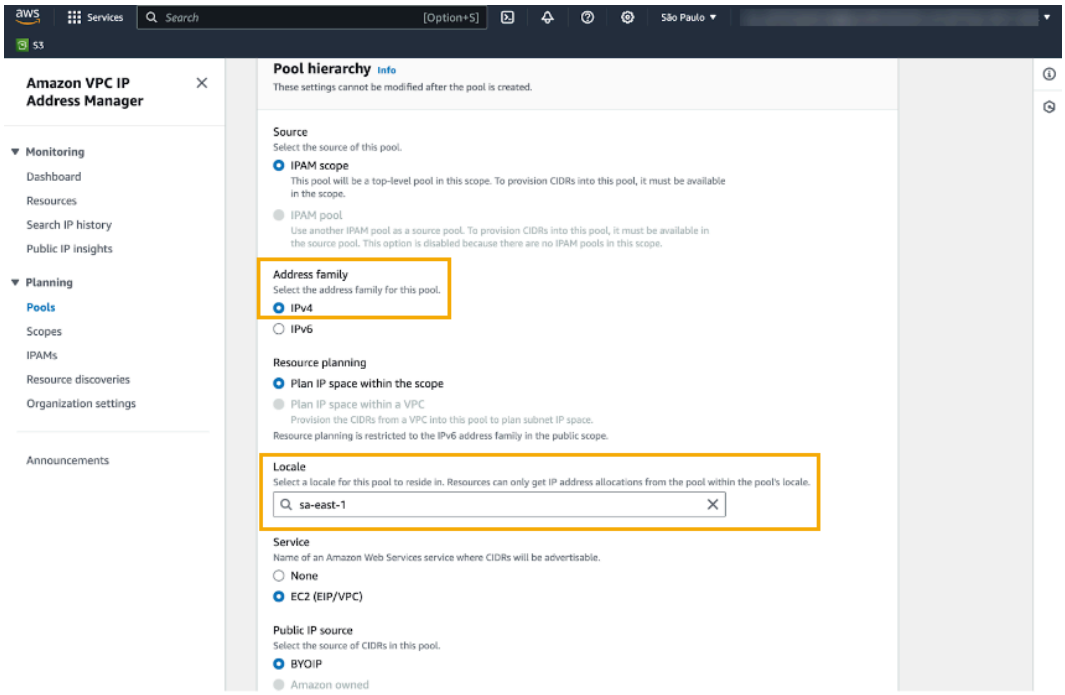


Une fois que vous avez créé l'IPAM, **AWS VPC IP Address Manager (Gestionnaire d'adresses IP AWS VPC)** affiche les détails de l'IPAM :

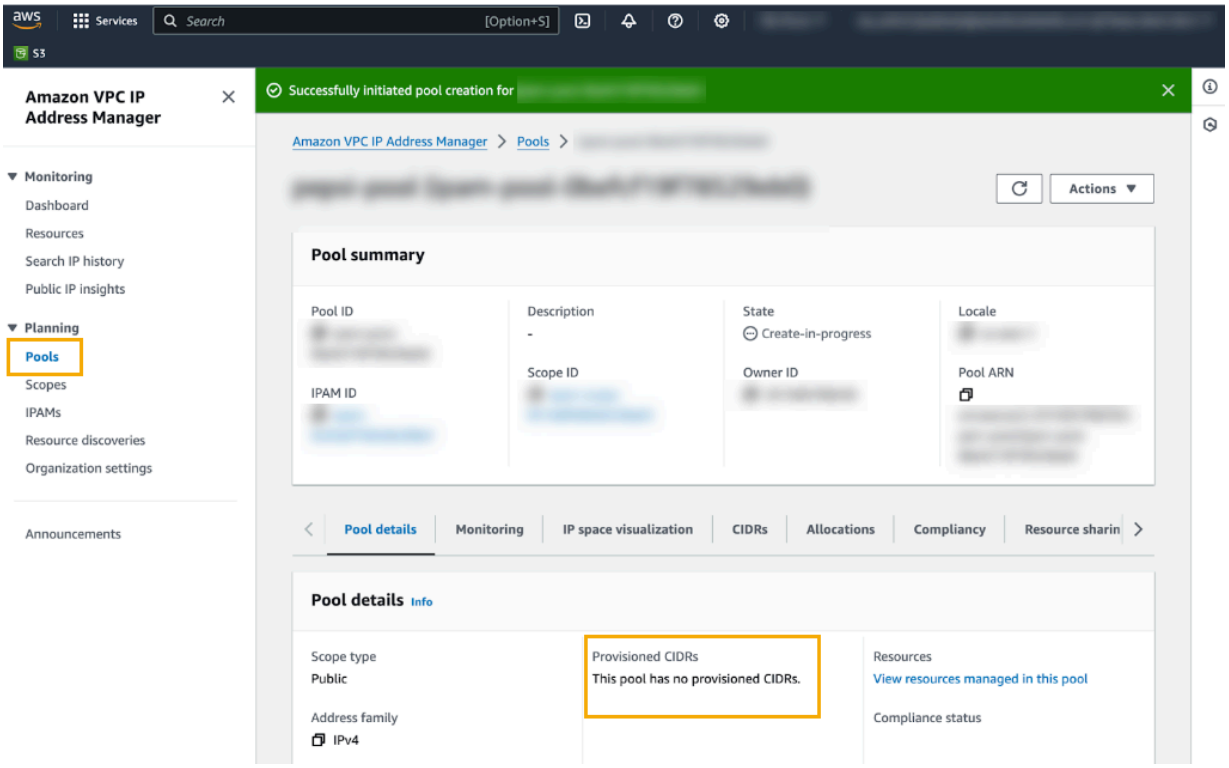


STEP 4 | Créez un groupe IPAM pour planifier le provisionnement d'adresses IP. Sélectionnez **Planning (Planification) > Pools (Groupes)** et cliquez sur **Create pool (Créer un groupe)**.

*Lors de la création d'un pool IPAM, vous devez définir **Address Family (Famille d'adresses)** sur **IPv4** et définir **Locale (Paramètres régionaux)** sur l'endroit où vous souhaitez déployer votre ressource Cloud NGFW, comme illustré sur l'écran **Pool Hierarchy (Hiérarchie des groupes)** :*



Une fois que vous avez créé l'IPAM, **AWS VPC IP Address Manager (Gestionnaire d'adresses IP AWS VPC)** affiche les détails du nouveau groupe :



Aucun CIDR n'est alloué au nouveau groupe. Vous aurez besoin d'une plage CIDR d'adresses IP publiques et de la clé privée du certificat correspondant.

STEP 5 | Allouez des CIDR au groupe que vous avez créé à l'étape précédente. Sélectionnez **Planning (Planification) > Pools (Groupes)**, puis sélectionnez l'onglet **CIDR** sous **Pool Summary (Résumé du groupe)**.

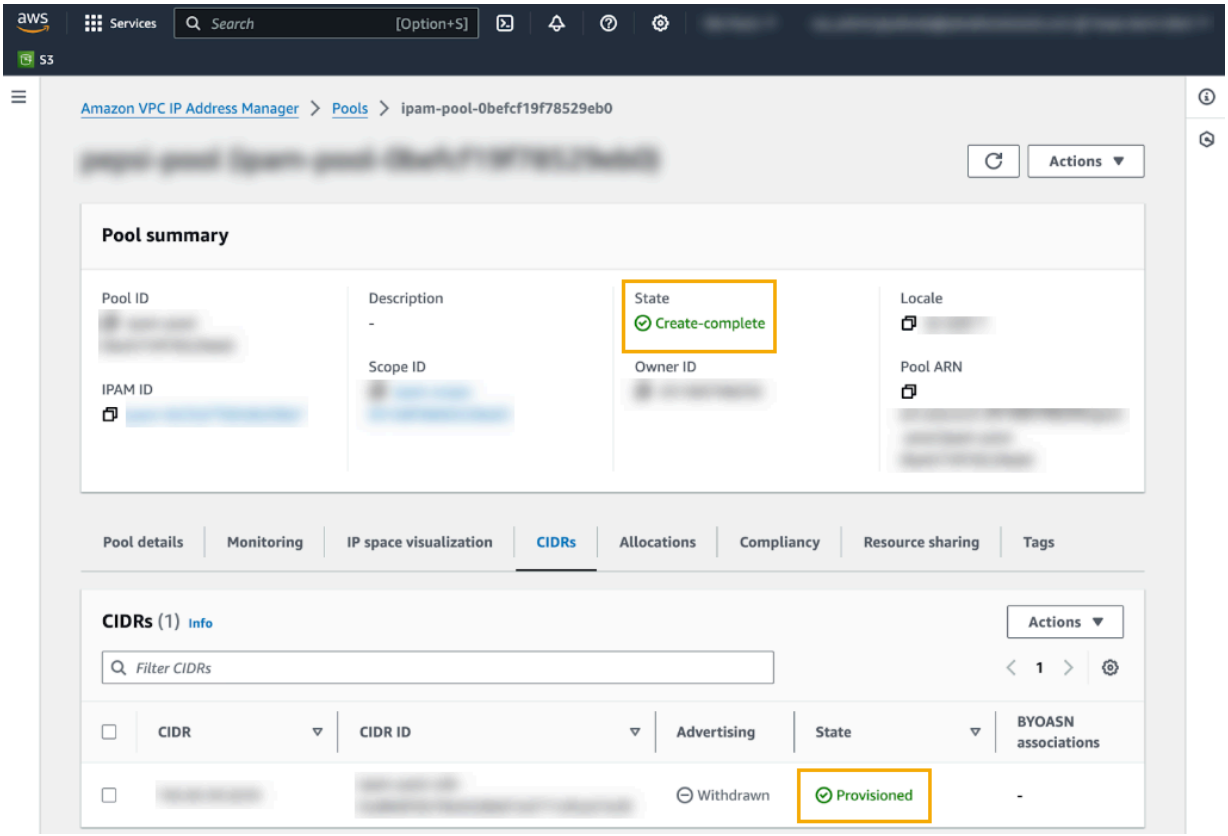
STEP 6 | Sélectionner **Actions > Provision CIDR (Allouer un CIDR).** Vous utiliserez ce processus pour récupérer une plage CIDR d'adresses IP publiques et la clé privée du certificat correspondant. Consultez Provision CIDRs to a pool (Allocation de CIDR à un groupe) pour en savoir plus.

STEP 7 | Dans les CIDR à allouer, cliquez sur **Input a CIDR with a X.509 Certificate (Saisir un CIDR avec un certificat X.509)**.

STEP 8 | Copiez la **Signature**.

STEP 9 | Cliquez sur **Provision (Allouer)**.

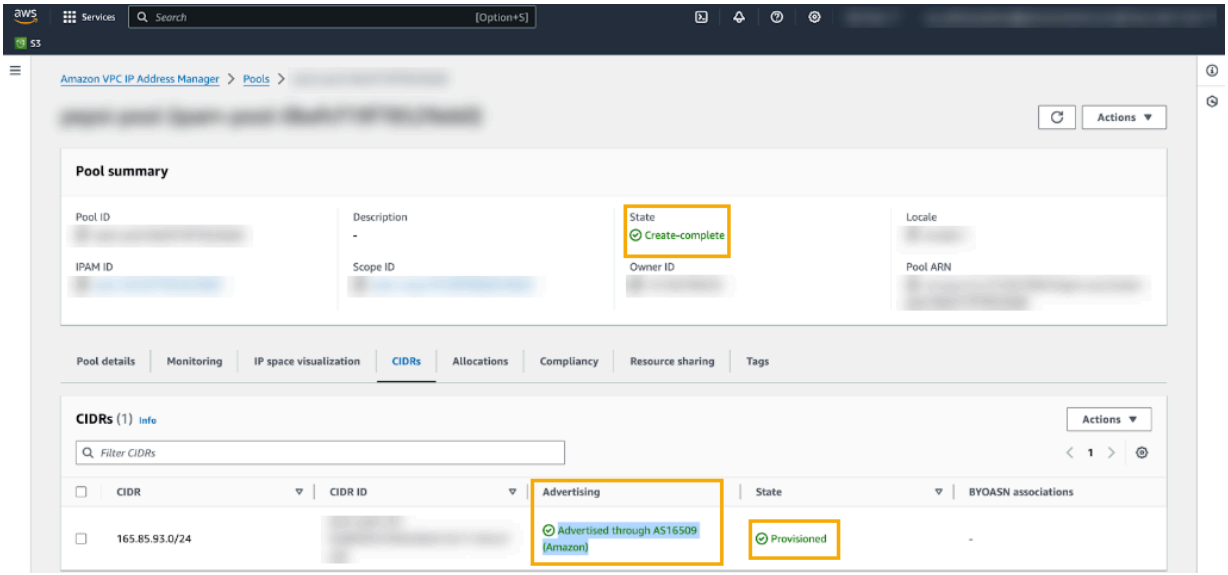
Vérifiez que le CIDR a été correctement alloué et que le groupe a bien été créé :



STEP 10 | Par défaut, lorsque vous ajoutez un CIDR à un groupe, il n'est pas publié. Publiez-le pour le rendre accessible au public sur Internet. Pour publier le CIDR :

1. Sélectionnez le groupe.
2. Cliquez sur l'onglet **CIDR**.
3. Dans le menu **Actions**, sélectionnez **Advertise (Publier)**.
4. Dans le menu **Advertise CIDR (Publier un CIDR)**, utilisez le menu déroulant pour sélectionner l'ASN approprié ; cliquez sur **Advertise CIDR (Publier un CIDR)**. Pour en savoir plus, consultez Advertise your CIDR (Publication de CIDR).

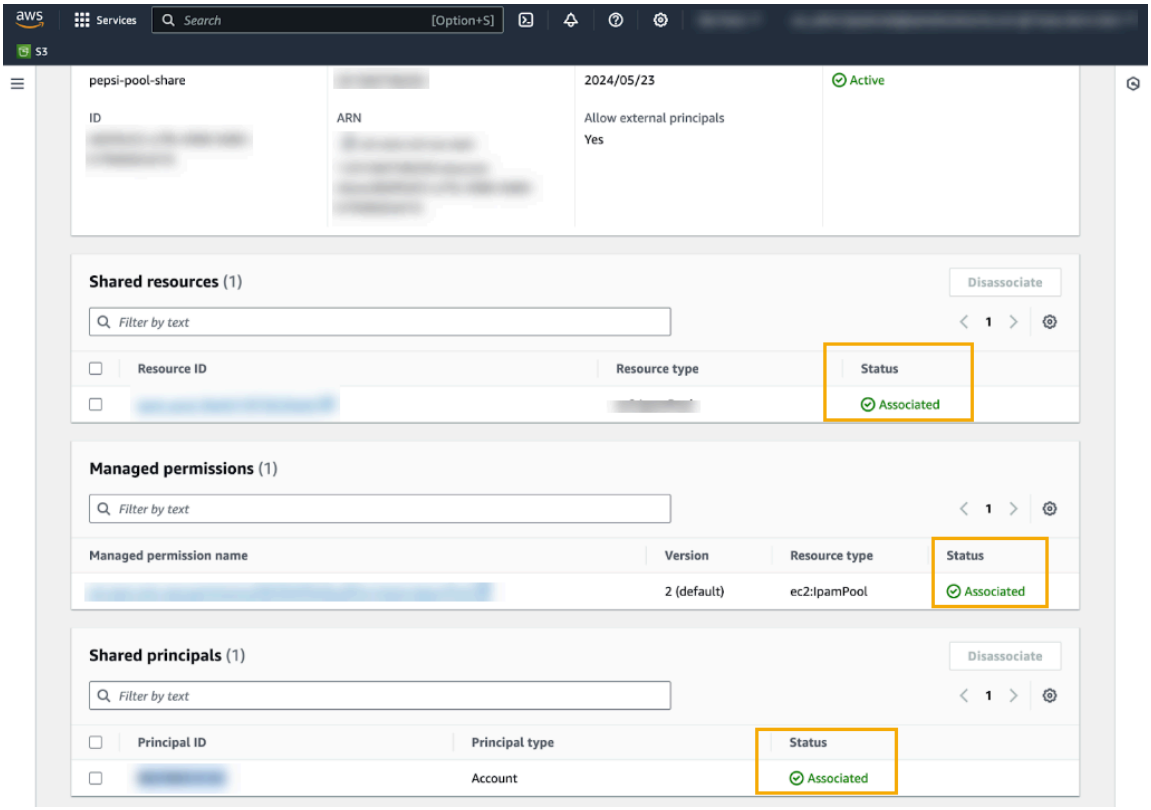
Confirmez que le CIDR est correctement publié :



STEP 11 | Après avoir publié le CIDR, partagez le groupe IPAM avec votre compte de déploiement Cloud NGFW. Pour ce faire :

1. Sélectionnez le groupe.
2. Cliquez sur l'onglet **Resource sharing (Partage des ressources)**.
3. Dans le menu **Resource sharing (Partage des ressources)**, sélectionnez **Create resource share (Créer un partage de ressources)**.
4. Dans le menu **Resource share name (Nom du partage de ressources)**, saisissez le nom du groupe IPAM que vous souhaitez partager.
5. Ajoutez éventuellement l'**ARN** au nom du partage de ressources.
6. Cliquez sur **Next (Suivant)**.
7. Accordez l'accès aux principaux.
8. Examinez les options de partage des ressources et les principaux, puis cliquez sur **Create (Créer)**. Pour en savoir plus, consultez Share an IPAM pool (Partage d'un groupe IPAM).

   Confirmez que les ressources associées au groupe IPAM ont bien été partagées :



Créer une ressource Cloud NGFW, activer la NAT de sortie et spécifier des adresses BYOIP

Après avoir terminé les étapes de création du groupe IPAM, vous devez créer la ressource Cloud NGFW, activer la NAT de sortie et spécifier les adresses BYOIP.

Pour configurer la NAT de sortie avec des adresses BYOIP :

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

STEP 2 | Cliquez sur **NGFWs (NGFW)**.

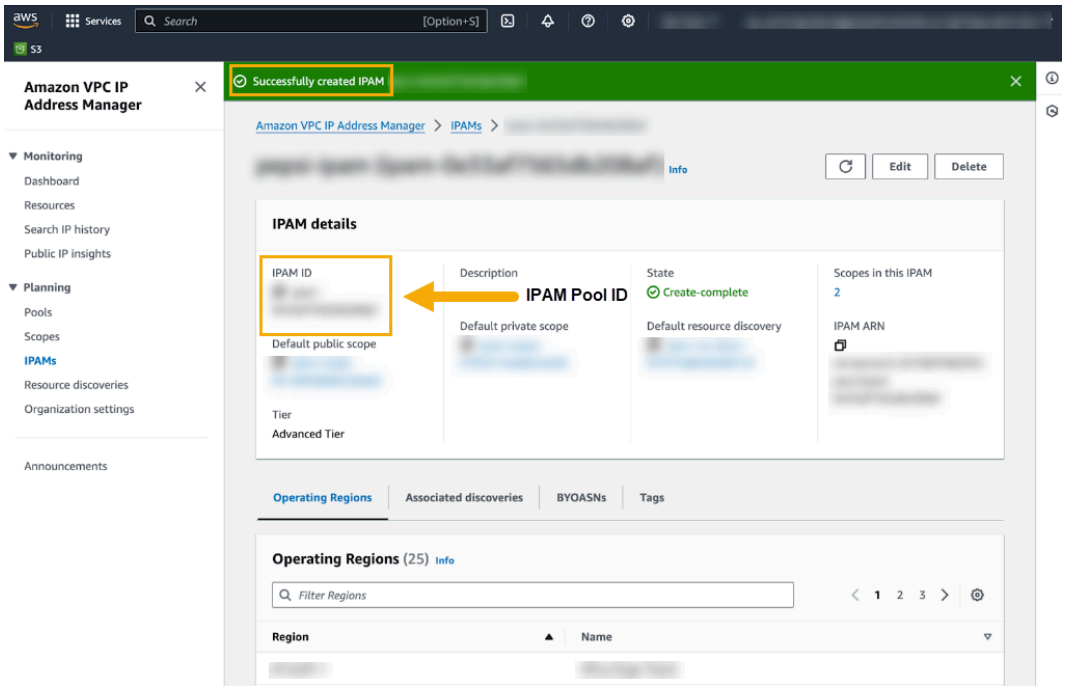
STEP 3 | Créer une nouvelle ressource NGFW.

STEP 4 | Dans la section **Policy Management (Gestion des politiques)**, sélectionnez **Panorama**. Utilisez le menu déroulant pour sélectionner le Panorama intégré.

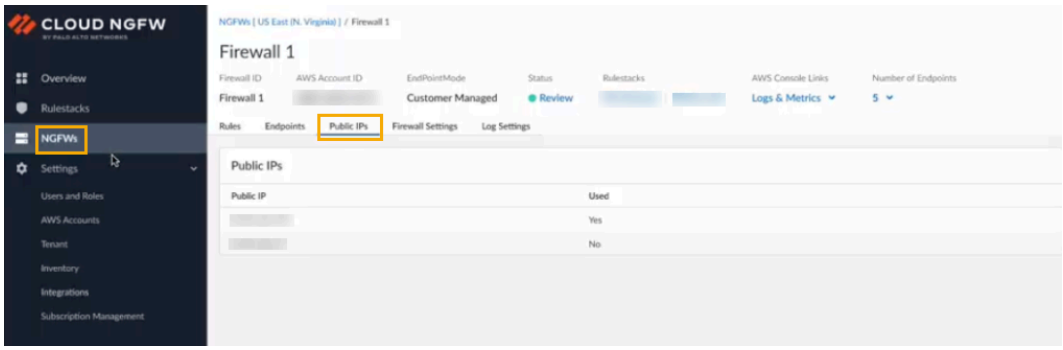
STEP 5 | Dans la section **Egress NAT (NAT de sortie)**, sélectionnez **Enable Egress NAT (Activer la NAT de sortie)**.

STEP 6 | Sélectionnez **Bring Your Public IPs (Apportez vos adresses IP publiques)** et saisissez l'ID du groupe IPAM que vous avez créé à l'étape 3 (ci-dessus).

*L'**IPAM Pool ID (ID du groupe IPAM)** se trouve dans la section **IPAM Pool Details (Détails du groupe IPAM)**.*



*Sélectionnez l'onglet **Public IPs (Adresses IP publiques)** sur la page du pare-feu pour afficher la liste des adresses IP prises en charge pour le trafic NAT de sortie :*



Une fois le pare-feu créé, vérifiez son état.

Pour libérer des adresses dans votre groupe IPAM si vous choisissez de ne pas utiliser d'adresses BYOIP, contactez Palo Alto Networks pour créer un dossier d'assistance.

Protéger

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

Vous pouvez créer différents types de règles de politique pour protéger votre réseau contre les menaces et les perturbations. Cela vous permet d’optimiser l’allocation des ressources réseau et de gérer vos règles de politique afin de hiérarchiser le trafic et de configurer les classifications des applications.

Cloud NGFW évalue les règles dans l’ordre en commençant par le haut ; lorsque le trafic correspond aux critères d’une règle définie, les règles suivantes ne sont pas évaluées. Vous devez ordonner des règles de politique plus spécifiques au-dessus des règles plus génériques afin d’appliquer les meilleurs critères de correspondance possibles. Un journal est généré pour le trafic qui correspond à une règle de politique lorsque la journalisation est activée pour la règle. Les options de journalisation sont configurables pour chaque règle.

Les règles de politique de meilleures pratiques sont disponibles pour la plupart des types de politiques et vous aident à démarrer rapidement et en toute sécurité. Bien que ces règles ne puissent pas être modifiées pour que vous disposiez toujours d’un niveau minimum de sécurité, vous pouvez les cloner si vous souhaitez les utiliser comme base pour personnaliser votre politique.

La plateforme Cloud NGFW pour AWS protège l’ensemble de votre entreprise, quelle que soit sa taille ou sa complexité. Avec une architecture de sécurité réseau unifiée et la possibilité d’exploiter le deep learning en temps réel, Cloud NGFW pour AWS peut vous offrir une visibilité complète et vous aider à tout sécuriser. Cette protection s’étend aux éléments suivants :

- Succursale. Activez la sécurité réseau Zero Trust avec une sécurité simplifiée pour des milliers de succursales.
- Campus. Les fonctionnalités intégrées protègent vos ressources internes et le monde extérieur afin que vos utilisateurs puissent se connecter aux données et aux applications depuis n’importe où.
- Centre de données. Bénéficiez d’une visibilité approfondie ainsi que de contrôles de sécurité cohérents et de premier ordre dans les environnements cloud.
- Cloud public. Sécurisez plusieurs environnements cloud publics avec le même niveau de protection que les centres de données sur site.
- Sécurité 5G. Tirez parti d’une solution simplifiée pour protéger tous les aspects de votre réseau mobile unique.

Avec Cloud NGFW pour AWS, vous n’aurez pas à gérer l’infrastructure. Offrant un déploiement sans stress de la configuration de la rulestack aux profils de sécurité automatisés, ce pare-feu nouvelle génération Palo Alto Networks est conçu pour que vous puissiez répondre facilement aux exigences de sécurité réseau.

Services de sécurité fournis par le cloud (CDSS)

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

La suite de services de sécurité fournis par le cloud (CDSS) de Palo Alto Networks donne accès à des solutions de sécurité spécialisées par abonnement, conçues spécifiquement pour protéger contre les menaces évasives connues, inconnues et avancées. Les données sur les menaces générées par une analyse avancée sont partagées sur les plateformes de sécurité de Palo Alto Networks pour permettre une couverture complète de tous les vecteurs de menace.

Pour sécuriser et protéger votre trafic à l'aide des CDSS, Cloud NGFW pour AWS fournit des protections Palo Alto Networks. En voici quelques exemples :

- App-ID. Basé sur la technologie brevetée de classification du trafic de la couche 7, le service App-ID vous permet de voir les applications sur votre réseau, d'apprendre comment elles fonctionnent, d'observer leurs caractéristiques comportementales et de comprendre leur risque relatif. Cloud NGFW pour AWS identifie les applications et les fonctions d'application via plusieurs techniques, notamment les signatures d'application, le décryptage, le décodage de protocole et l'heuristique. Ces capacités déterminent l'identité exacte des applications traversant votre réseau, y compris celles qui tentent d'échapper à la détection en se faisant passer pour du trafic légitime à l'aide du port hopping ou du cryptage.
- Threat Prevention. Le service Threat Prevention de Palo Alto Networks protège votre réseau en fournissant plusieurs couches de prévention pour faire face à chaque phase d'une attaque. En plus des fonctionnalités essentielles d'un service Intrusion Prevention (prévention des intrusions, IPS), Threat Prevention possède la capacité unique de détecter et de bloquer les menaces sur n'importe quel port, plutôt que de simplement appeler des signatures basées sur un ensemble limité de ports prédéfinis.
- Advanced URL Filtering. Ce service critique intégré à Cloud NGFW pour AWS arrête les attaques web inconnues en temps réel pour éviter le scénario du patient zéro grâce au seul filtrage des URL avancé basé sur le ML du secteur. Advanced URL Filtering associe la célèbre base de données d'URL malveillantes de Palo Alto Networks au premier moteur de protection web en temps réel du secteur afin que les organisations puissent détecter et prévenir automatiquement et instantanément les nouvelles menaces web malveillantes et ciblées.
- DNS. DNS Security vous offre une protection en temps réel, en appliquant des protections inédites dans le secteur pour perturber les attaques qui utilisent le DNS. L'intégration étroite à un pare-feu nouvelle génération (NGFW) Palo Alto Networks vous offre des protections automatisées, empêche les attaquants de contourner les mesures de sécurité et élimine la nécessité d'utiliser des outils indépendants ou de modifier le routage DNS. DNS Security offre à votre organisation un nouveau point de contrôle critique pour arrêter les attaques.
- WildFire. Palo Alto Networks Advanced WildFire® est le plus grand moteur de prévention des logiciels malveillants basé sur le cloud du secteur. Il protège les organisations contre les menaces très évasives

à l’aide de moteurs de détection basés sur le machine learning brevetés qui permettent des protections automatisées sur le réseau, le cloud et les points de terminaison. Advanced WildFire analyse chaque fichier inconnu à la recherche d’intentions malveillantes, puis distribue la prévention en un temps record (60 fois plus rapidement que le concurrent le plus proche) pour réduire le risque de scénario du patient zéro.

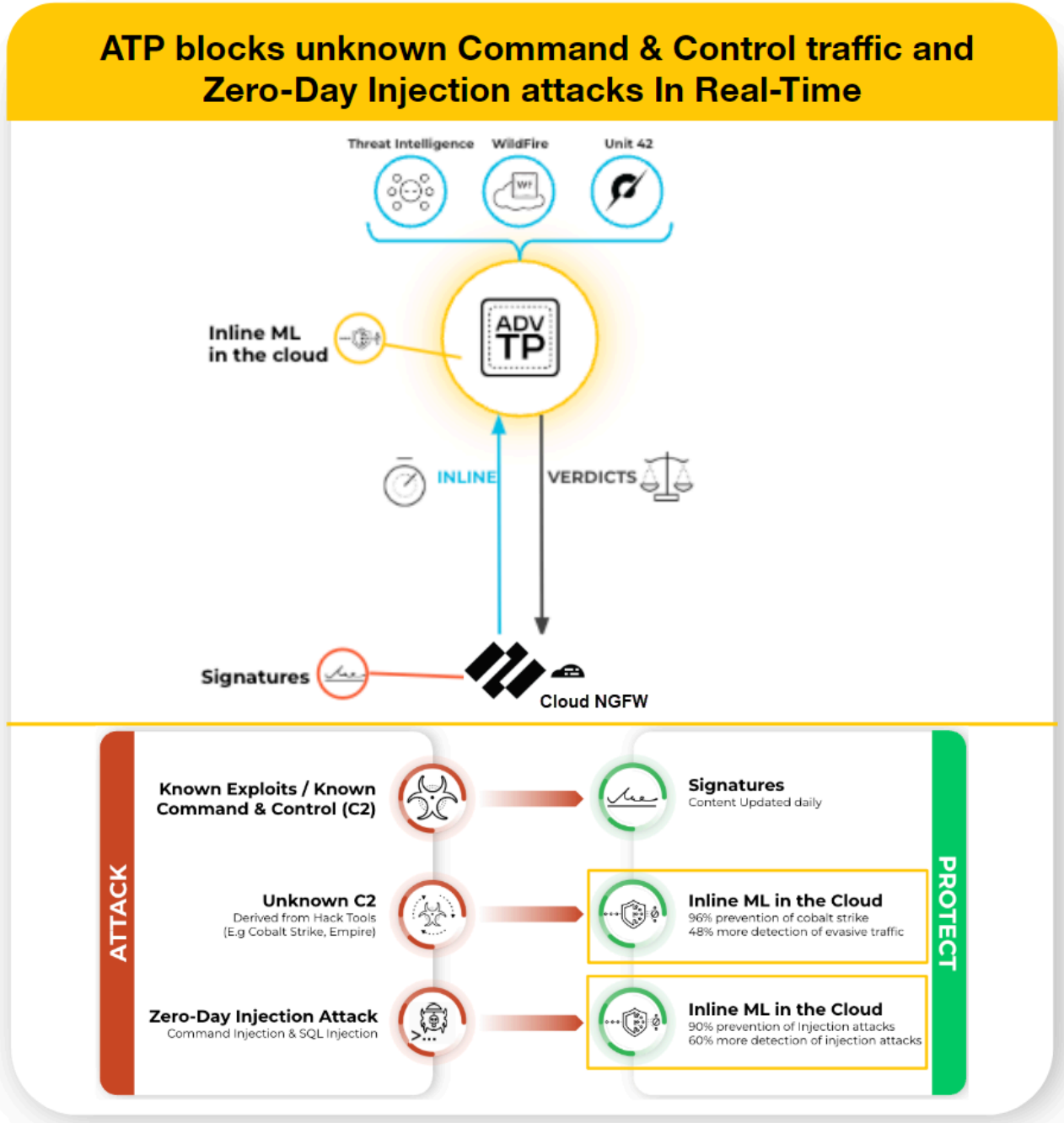
Cloud NGFW pour AWS – Protection avancée contre les menaces

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

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.

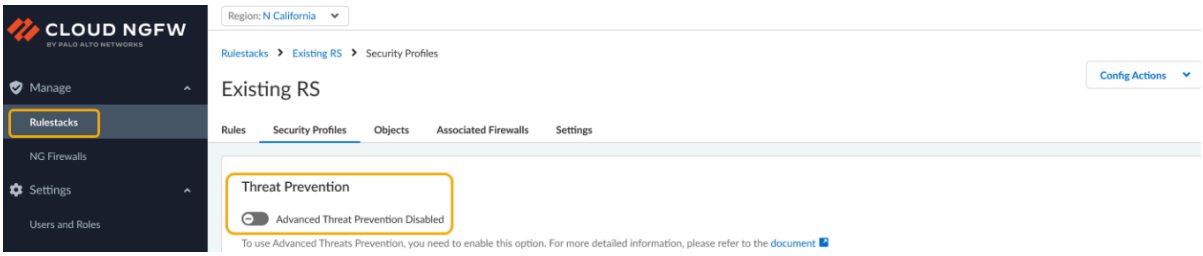
Pour activer ATP pour une rulestack :

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.

Cloud NGFW sur AWS – Advanced URL Filtering

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

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)	

Entrée de la liste d’exceptions d’URL	Sites correspondants
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

Cloud NGFW sur AWS – Protection WildFire

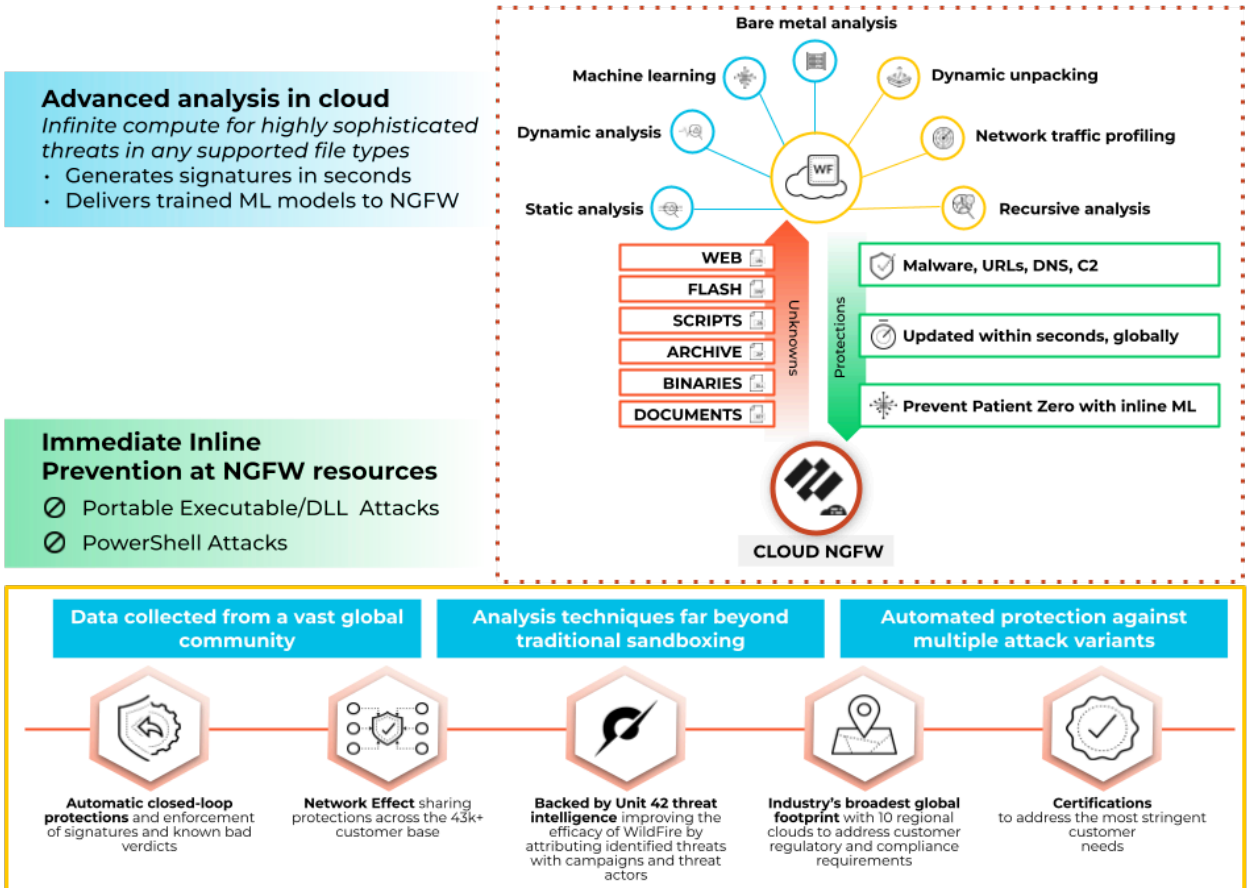
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d’utilisateur (locataire ou administrateur)

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 au service cloud WildFire™ à des fins d’analyse. Wildfire s’appuie ensuite sur des renseignements sur les menaces, l’analytique et des corrélations sur ces fichiers transférés (exécutables ou scripts) afin de rendre un verdict basé 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 afin de former un modèle de machine learning prédictif capable d'identifier de nouveaux logiciels malveillants, ce qui n'est pas possible avec l'analyse statique ou dynamique seule.
- **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.



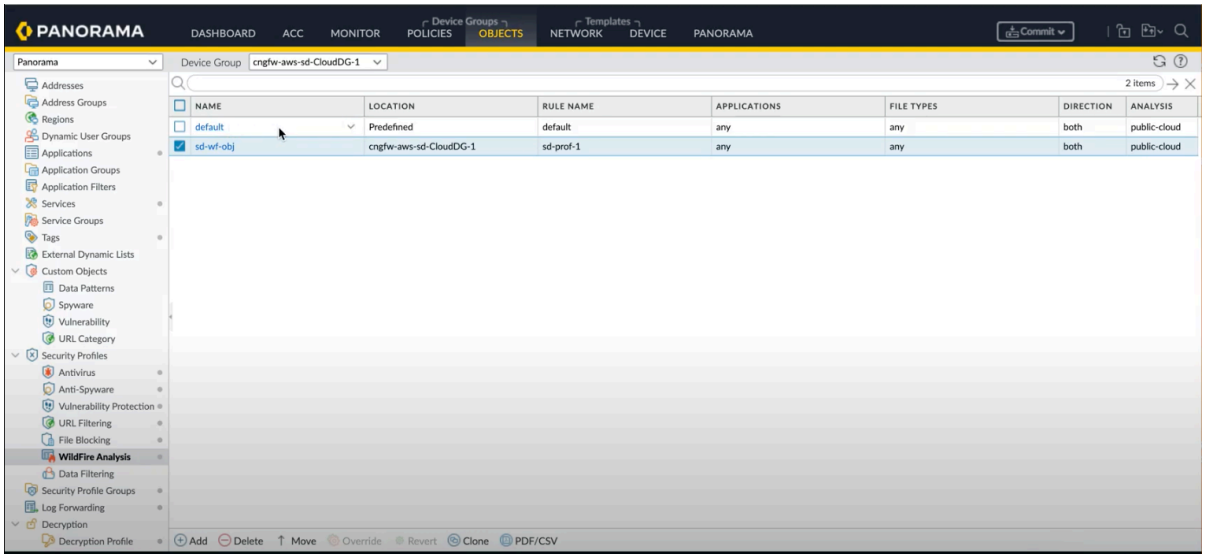
Pour configurer WildFire sur votre ressource AWS Cloud NGFW, vous devez procéder comme suit :

- Configurer 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

Configurer un profil Wildfire

STEP 1 | Connectez-vous à **Panorama** et cliquez sur **Objects (Objets) > WildFire Analysis (Analyse WildFire)**. La fenêtre du 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)**.

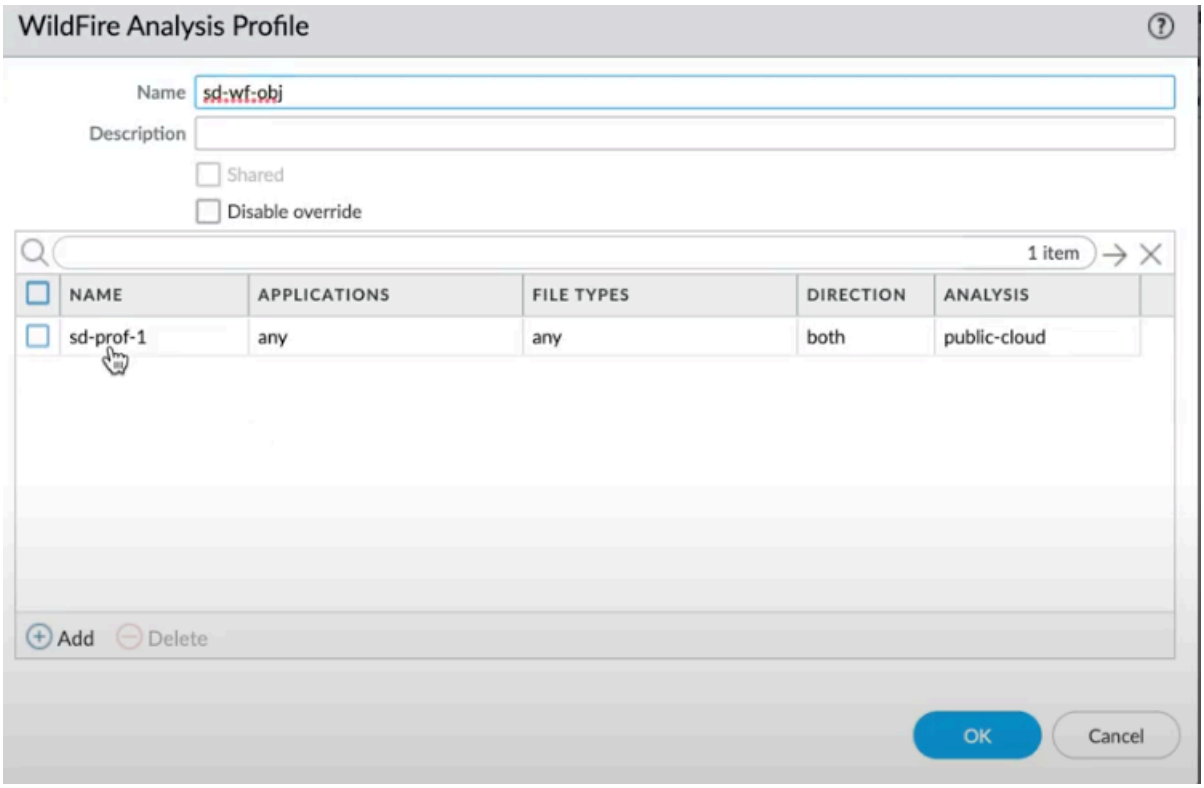
STEP 4 | Saisissez un **Name (Nom)** pour le profil WildFire et cliquez sur **Add (Ajouter)**.

STEP 5 | Dans **Name (Nom)**, donnez un nom descriptif à toute règle que vous ajoutez au profil.

STEP 6 | Dans la section Application, cliquez sur **Add (Ajouter)** pour ouvrir la liste des applications et y sélectionner l'application à laquelle 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, le chargement ou les deux.



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)** si vous souhaitez que tout le 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 **policy rules (règles de politique)**.

STEP 2 | Choisissez le groupe d'appareils requis, puis 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 en savoir plus, consultez Latest WildFire Cloud Features (Dernières fonctionnalités du cloud WildFire).

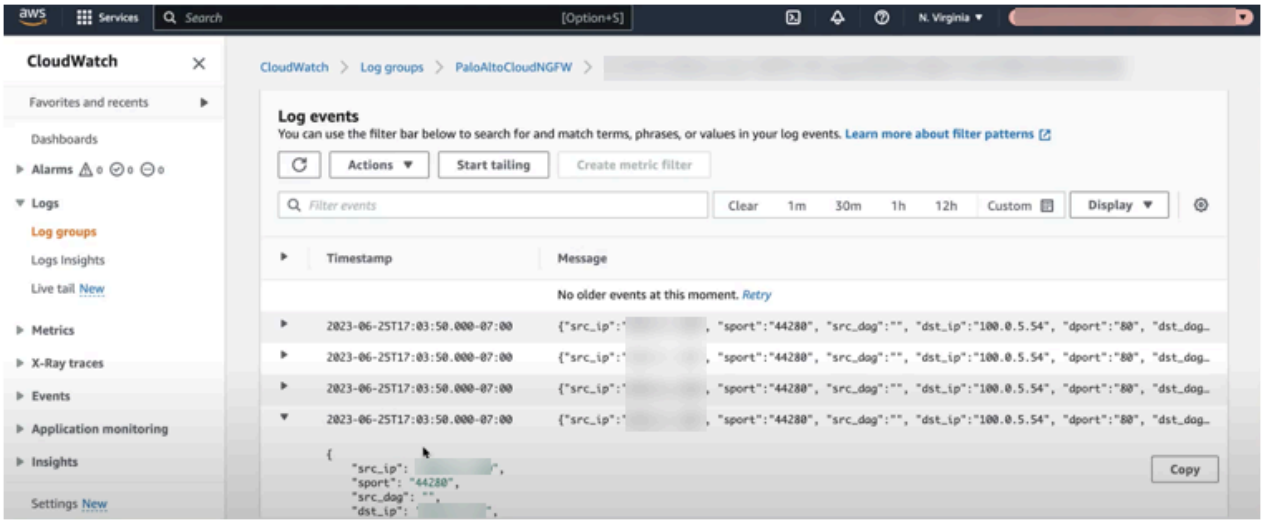
Afficher les journaux d'envois WildFire

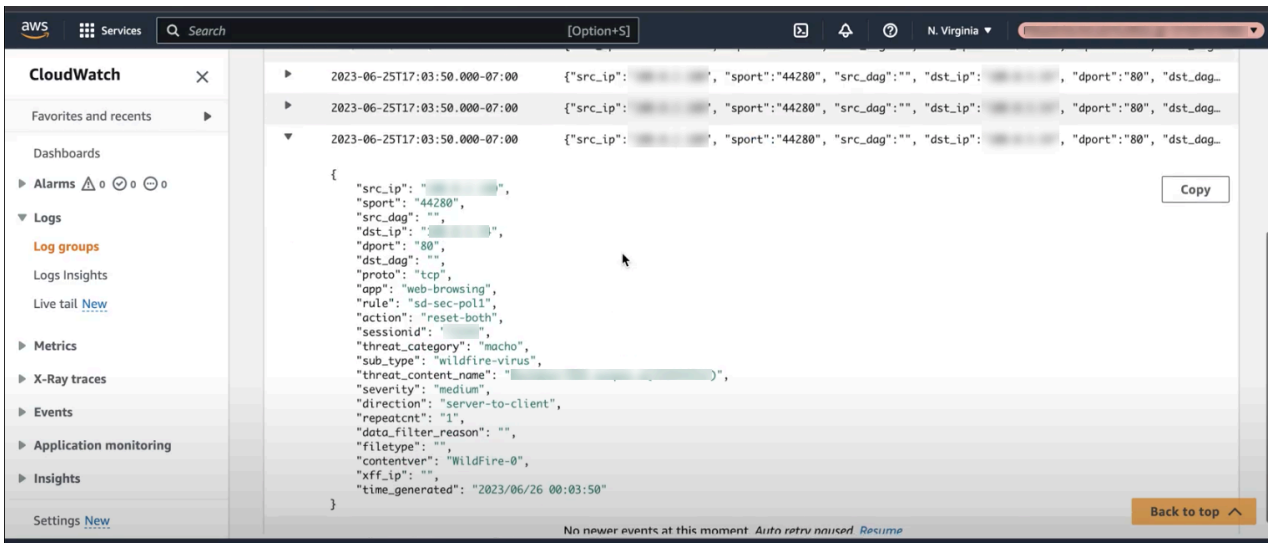
Vous pouvez afficher les journaux d'envois WildFire dans :

1. Destinations des journaux AWS
2. Panorama
3. Service de journalisation Strata

Afficher les journaux dans les destinations AWS

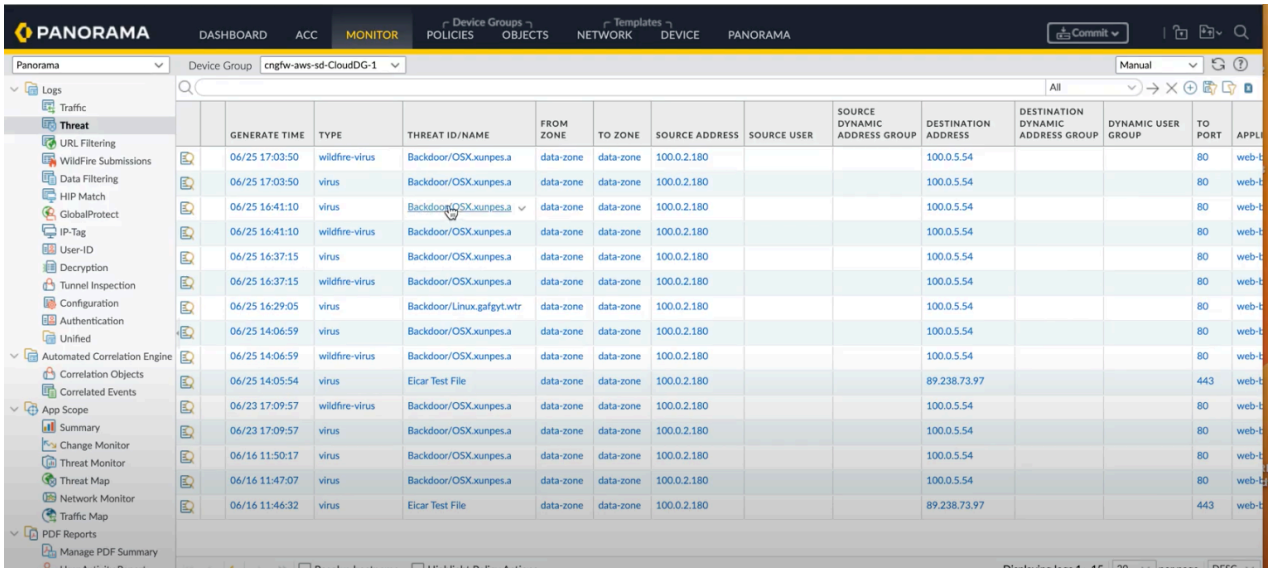
Si vous avez précédemment configuré Amazon CloudWatch, Amazon S3 ou Amazon Kinesis comme destination de journal, vous pouvez les passer en revue à l'aide de WildFire pour détecter les blocs de trafic malveillant.





Afficher les journaux dans Panorama

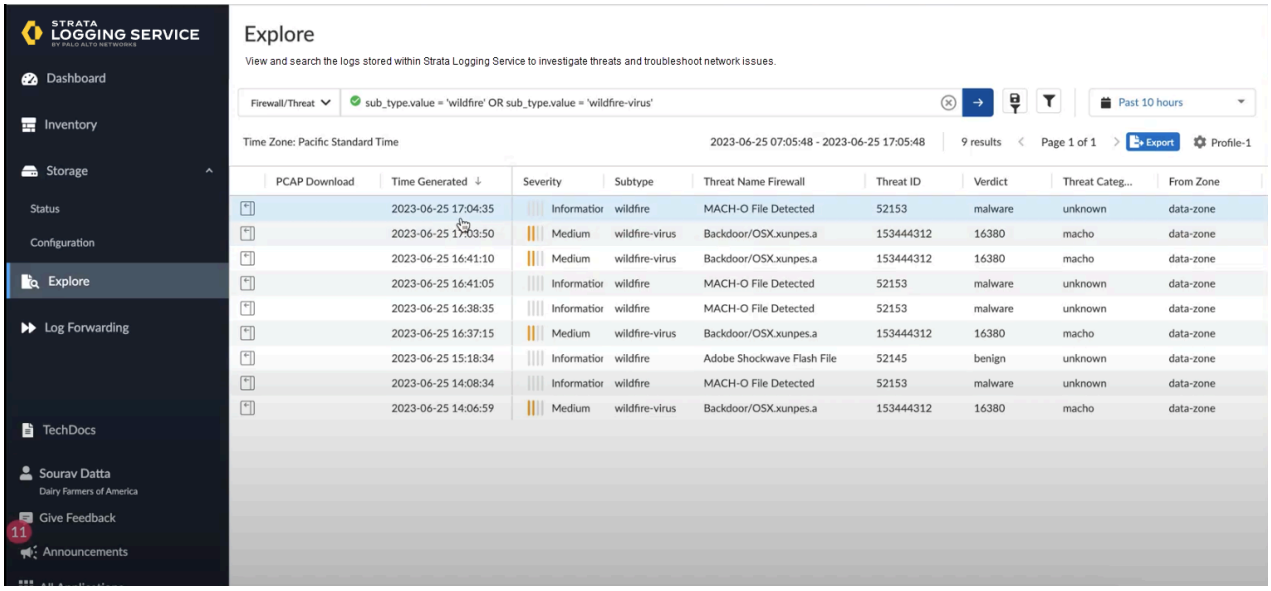
Sur Panorama, vous pouvez afficher les journaux sur le groupe d’appareils en cliquant sur **Monitor (Surveiller) > Threats (Menaces)**.



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.



Cloud NGFW pour AWS – DNS Security

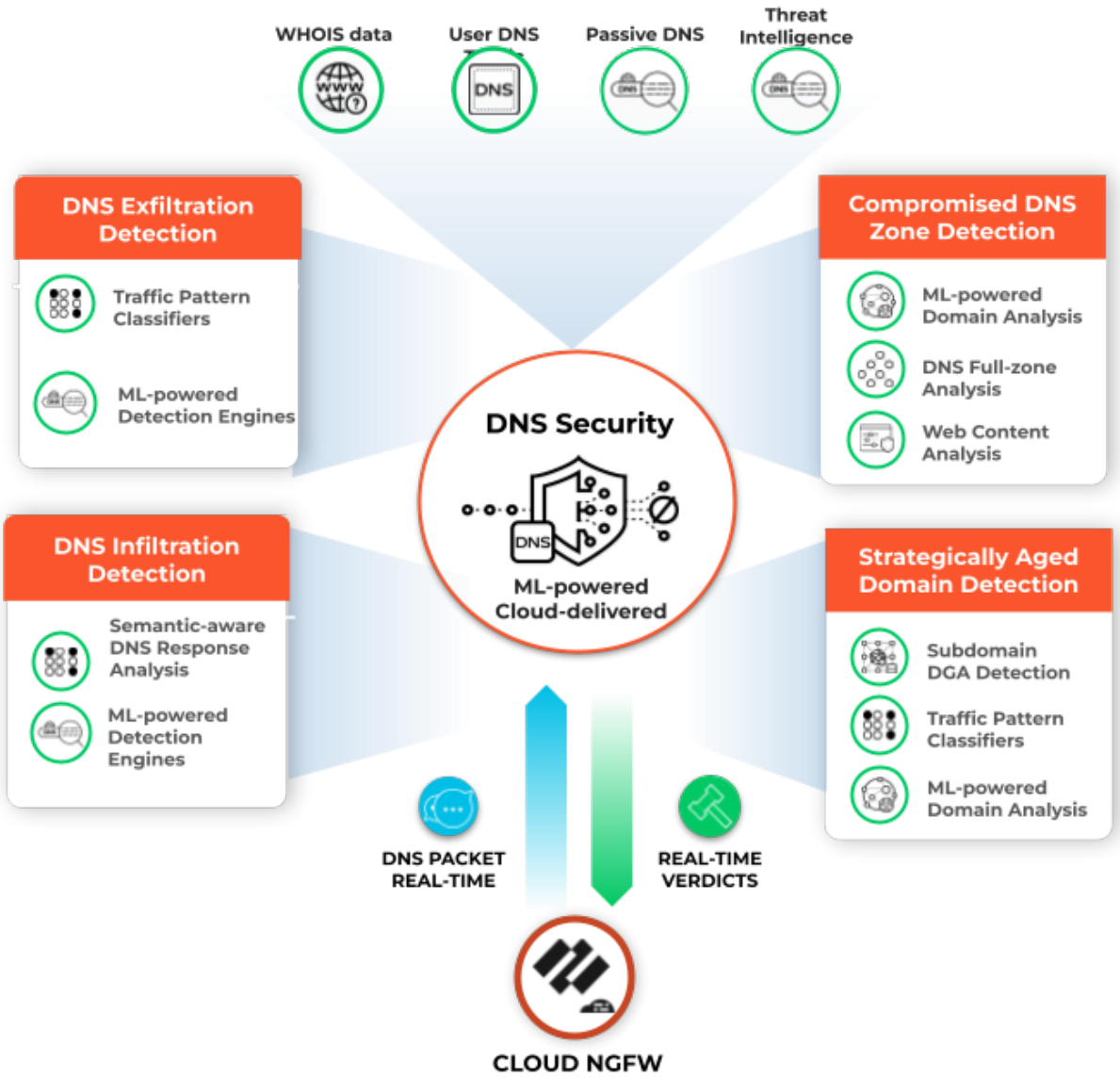
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d'utilisateur (locataire ou administrateur)

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.

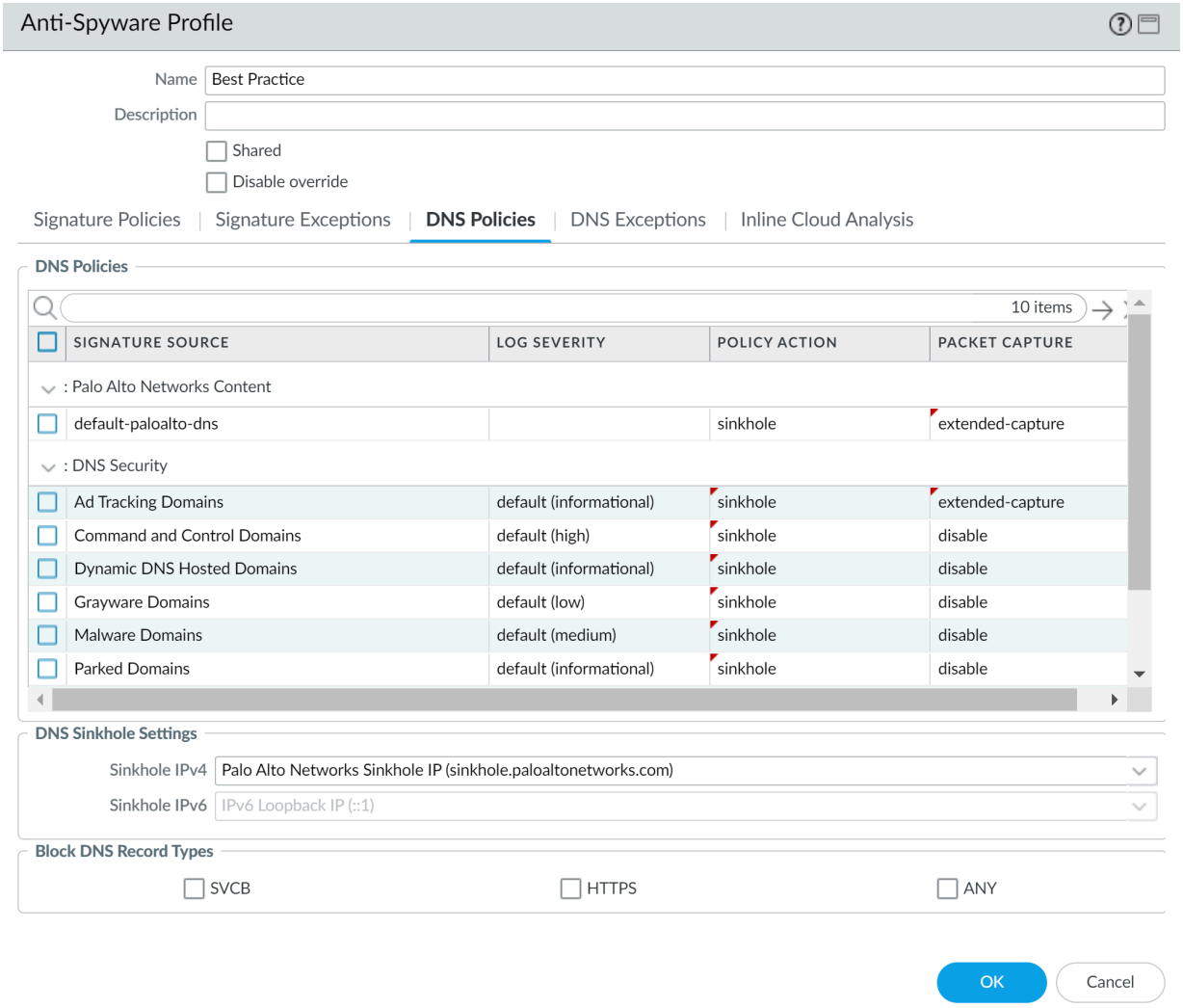
Cloud NGFW utilise le service de sécurité DNS de Palo Alto Networks qui détecte les domaines malveillants de manière proactive en générant des signatures DNS à l'aide d'une analyse prédictive avancée et de machine learning, avec des données provenant de plusieurs sources (telles que l'analyse du trafic 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 DNS Security dans les ressources Cloud NGFW :

STEP 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.



STEP 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

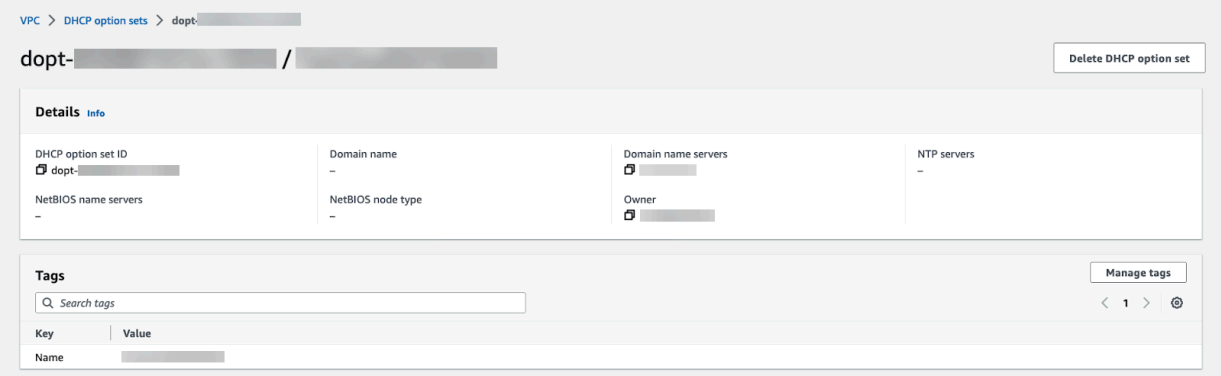
Serveur DNS privé

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)**.

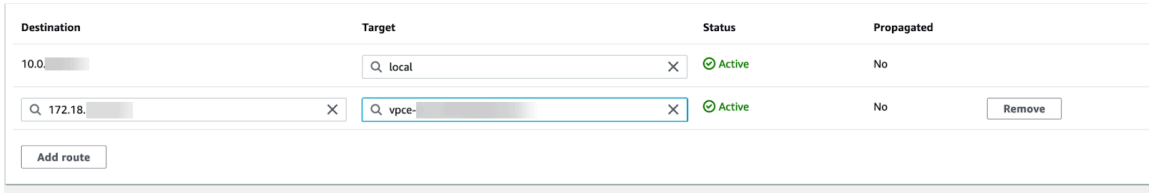
STEP 6 | Sous **DHCP settings (Paramètres DHCP)**, sélectionnez l'ensemble d'options DHCP configuré sur votre serveur DNS privé dans le menu déroulant **DHCP option set (Ensemble d'options DHCP)**.

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.

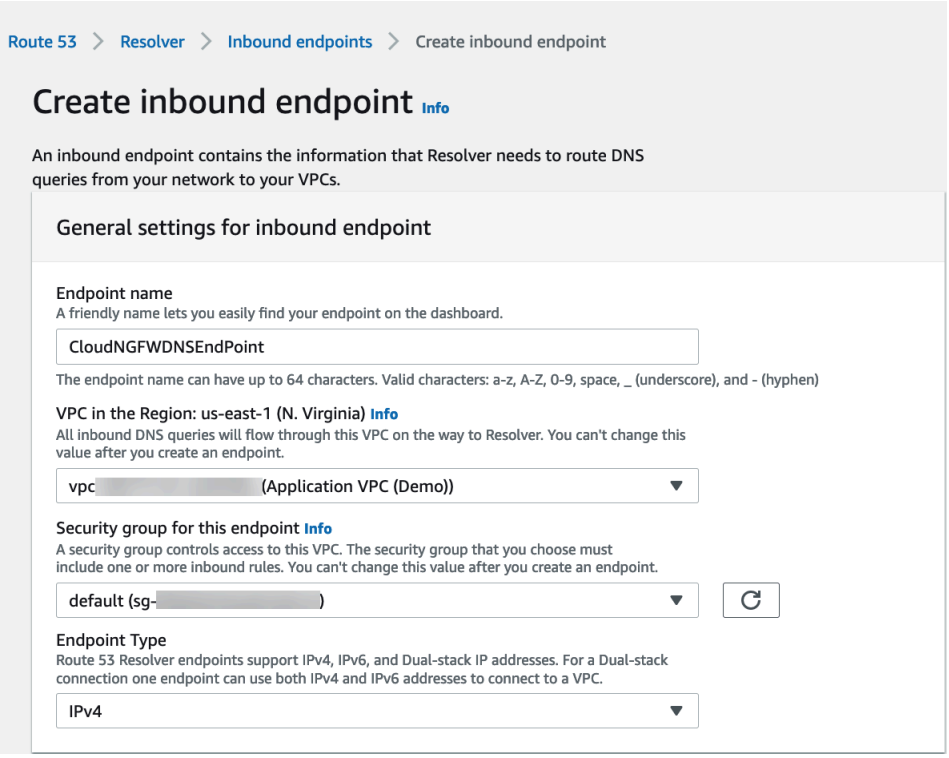
Service DNS Route 53

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.

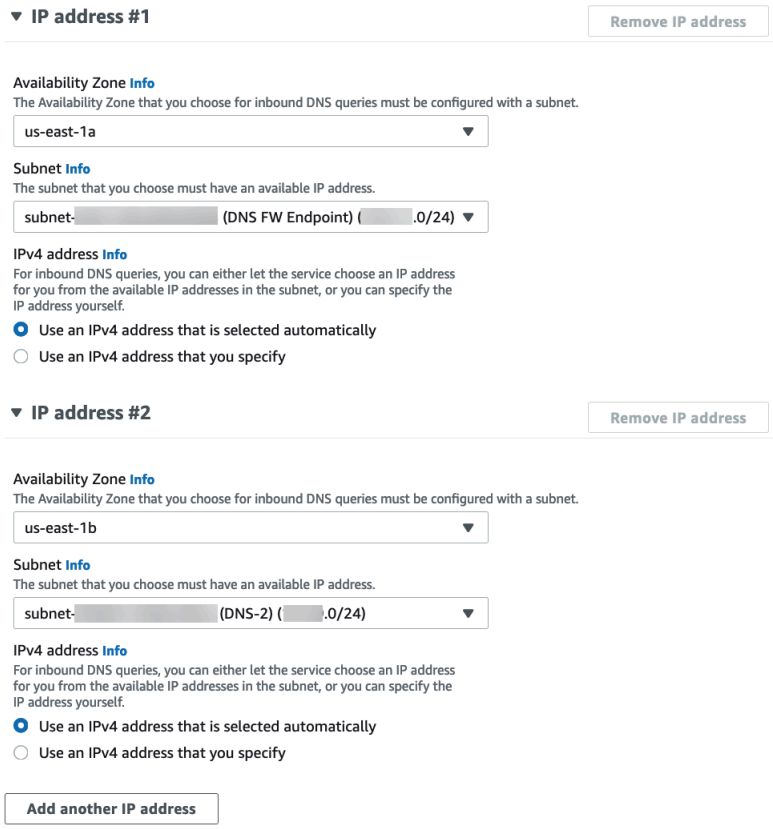
STEP 2 | Créez un terminal entrant.

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.

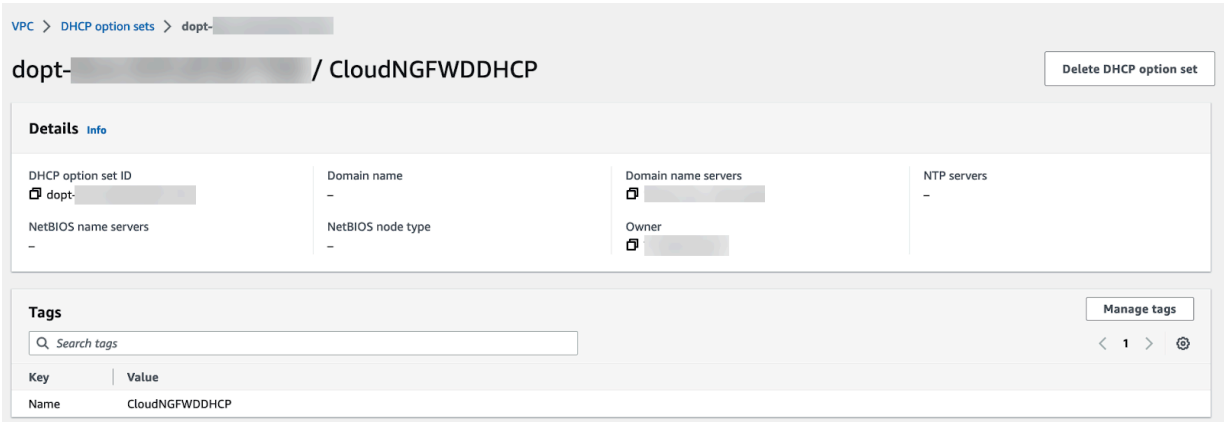
Si vous disposez de plusieurs zones de disponibilité, vous devez spécifier la zone de disponibilité et le sous-réseau de chacune.



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)**.

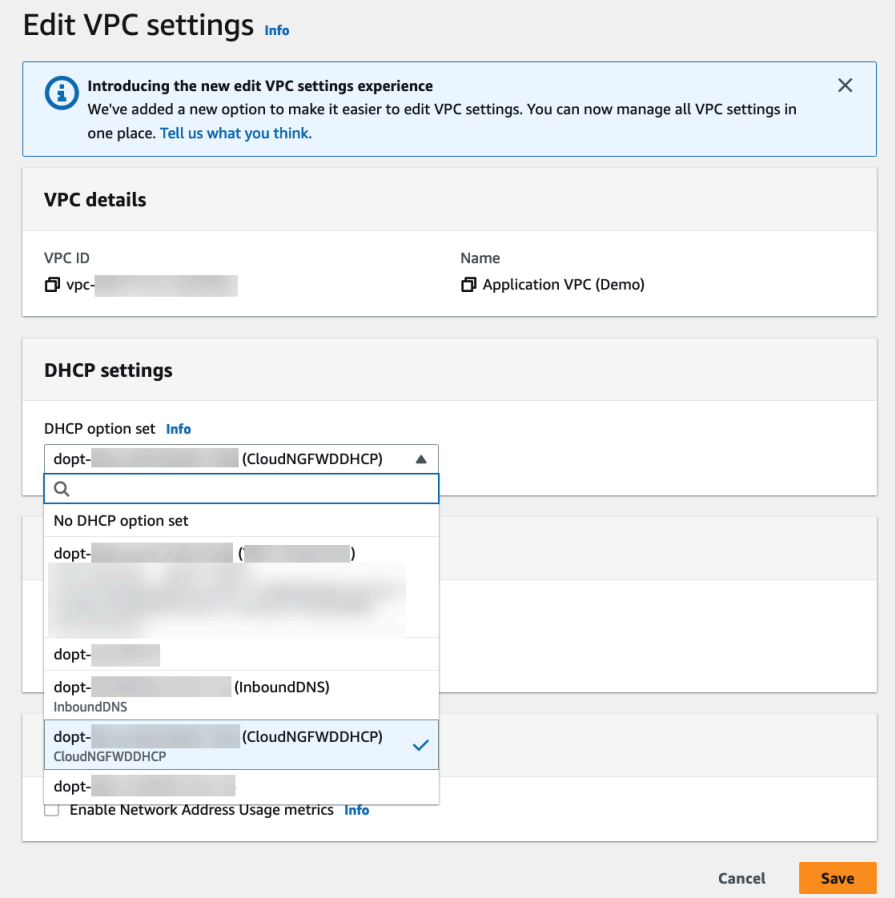
STEP 4 | Vous pouvez créer un nouvel ensemble d'options DHCP et ajouter l'adresse IP de chaque zone de disponibilité. Si vous disposez de plusieurs zones de disponibilité, saisissez chaque adresse IP dans une liste séparée par des virgules.



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)**.

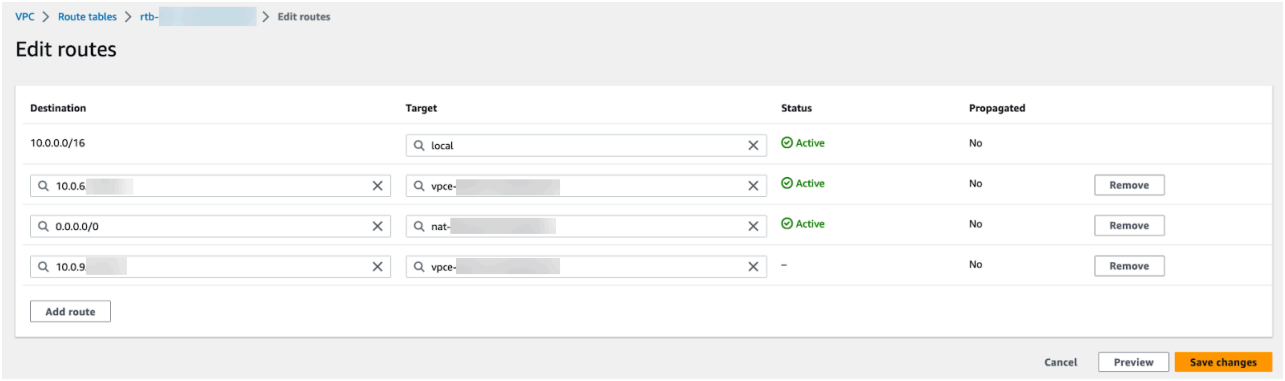


STEP 8 | Cliquez sur **Save changes (Enregistrer les modifications)**.

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

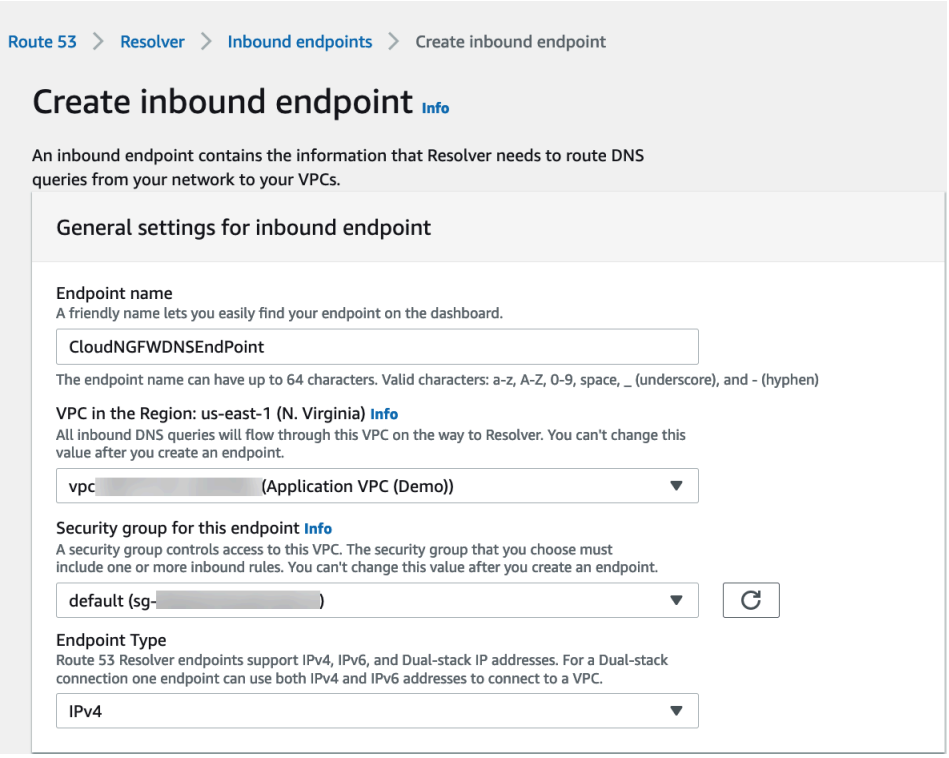
Pour créer une zone privée hébergée dans AWS, consultez Création d'une zone privée hébergée.

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.

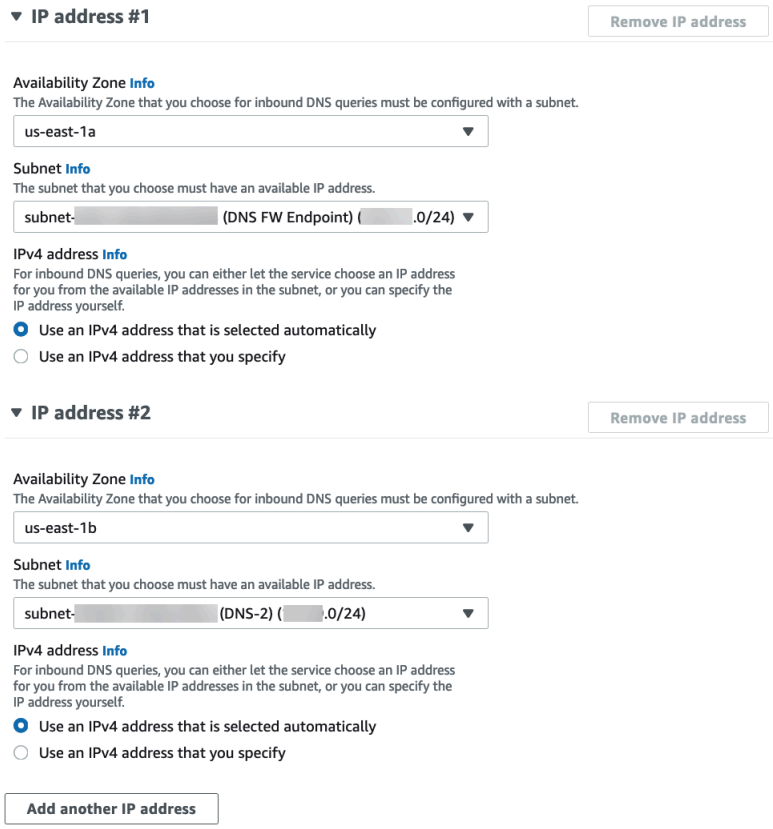
STEP 2 | Créez un terminal entrant.

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.

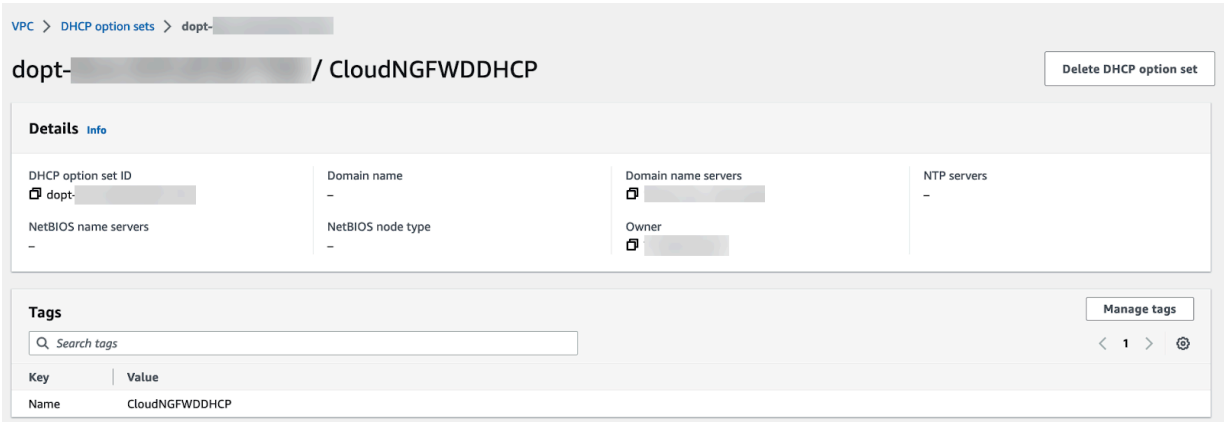
Si vous disposez de plusieurs zones de disponibilité, vous devez spécifier la zone de disponibilité et le sous-réseau de chacune.



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)**.

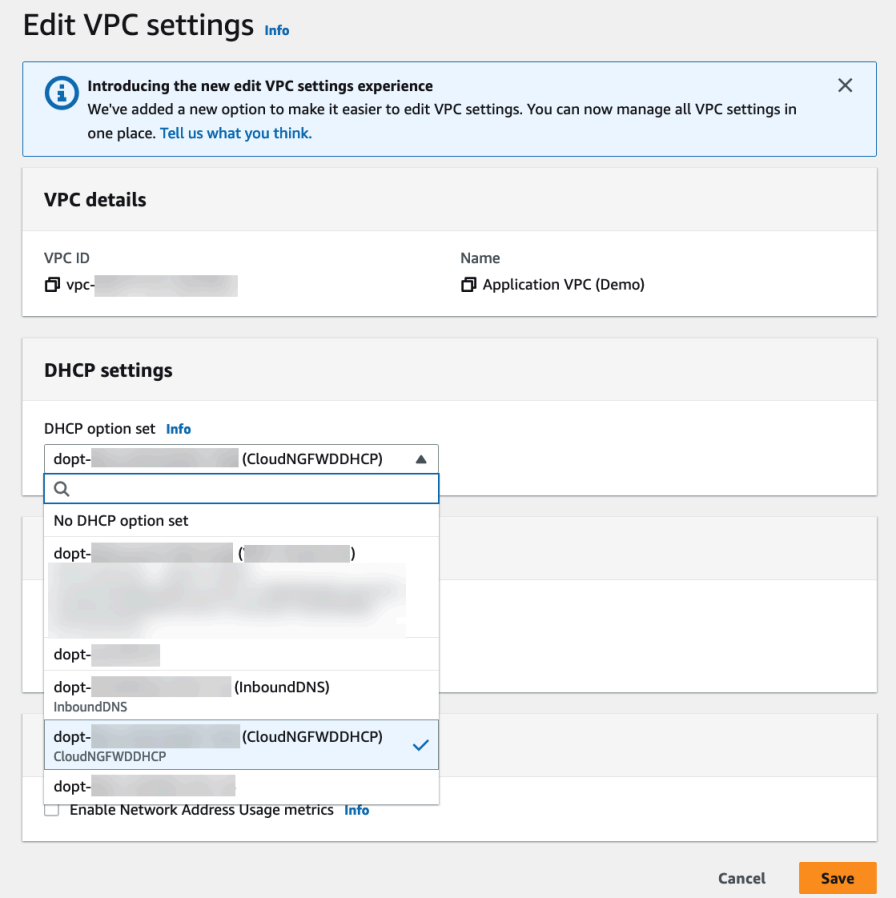
STEP 4 | Vous pouvez créer un nouvel ensemble d'options DHCP et ajouter l'adresse IP de chaque zone de disponibilité. Si vous disposez de plusieurs zones de disponibilité, saisissez chaque adresse IP dans une liste séparée par des virgules.



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)**.

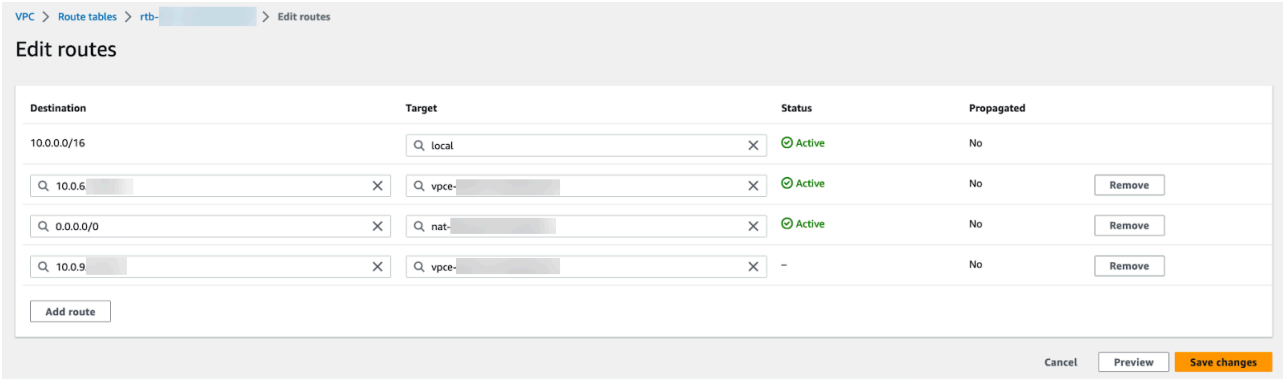
STEP 7 | Sous **DHCP settings (Paramètres DHCP)**, sélectionnez l'ensemble d'options DHCP que vous avez créé ci-dessus dans la liste déroulante **DHCP option set (Ensemble d'options DHCP)**.



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.

Cloud NGFW pour AWS – Intégration de la prévention des pertes de données d'entreprise (E-DLP)

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

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

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

Version Panorama (PAN-OS)	Plug-in DLP	Plug-in AWS
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

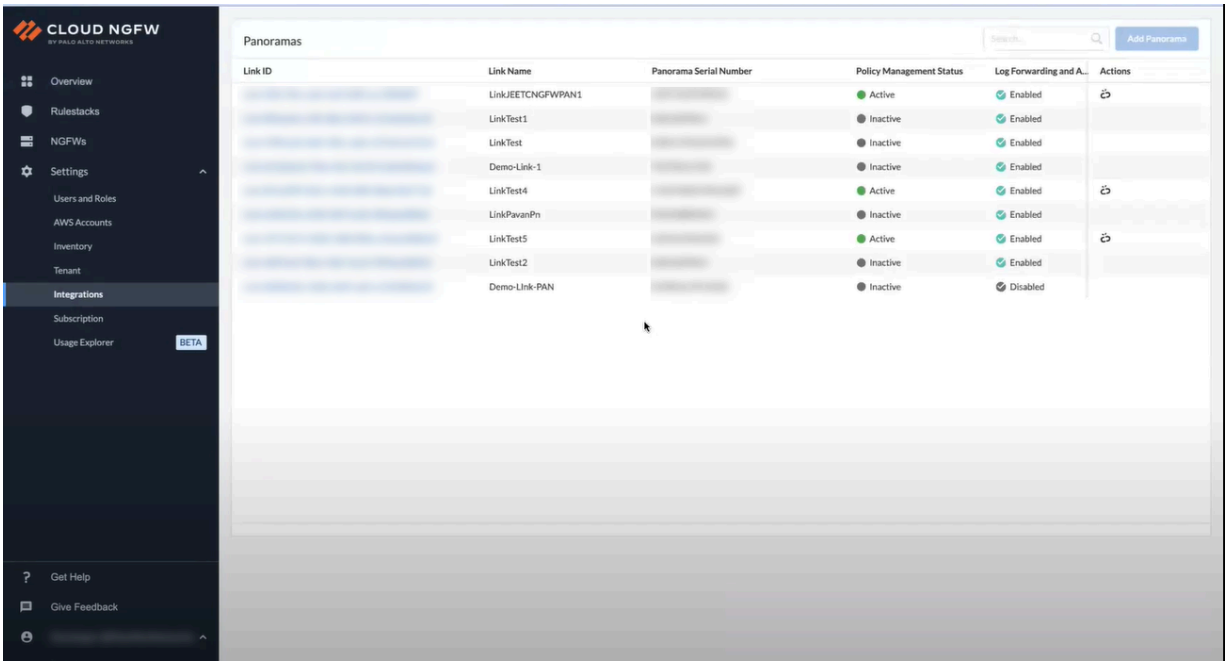
Si vous avez un locataire DLP existant sur votre compte du portail de support client (CSP) approvisionné dans Panorama, le service Cloud NGFW utilisera ce locataire DLP pour intégrer DLP à Cloud NGFW.

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.

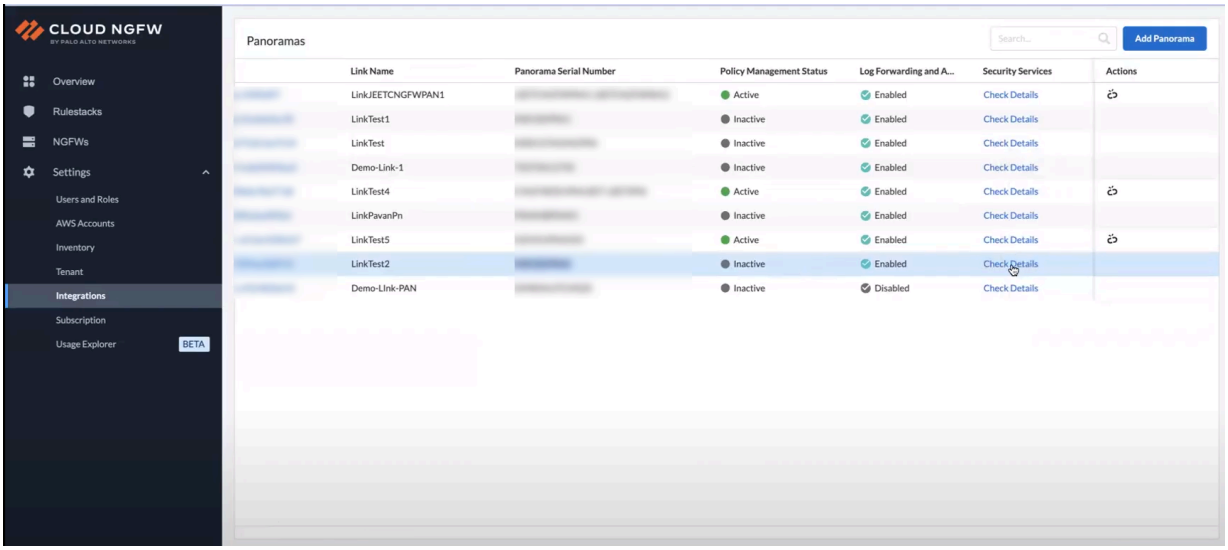
Suivez ces étapes pour activer un nouveau locataire DLP sur la console Cloud NGFW :

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

STEP 2 | Sélectionnez **Integrations (Intégrations)**.

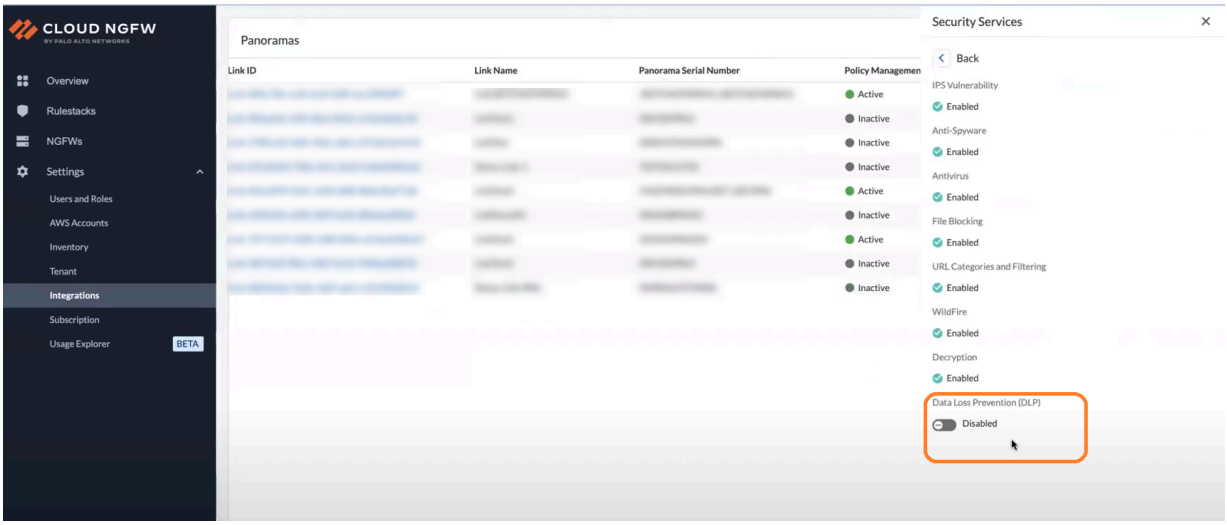


STEP 3 | Dans la colonne Security Service (Service de sécurité), cliquez sur **Check Details (Vérifier les détails)**.

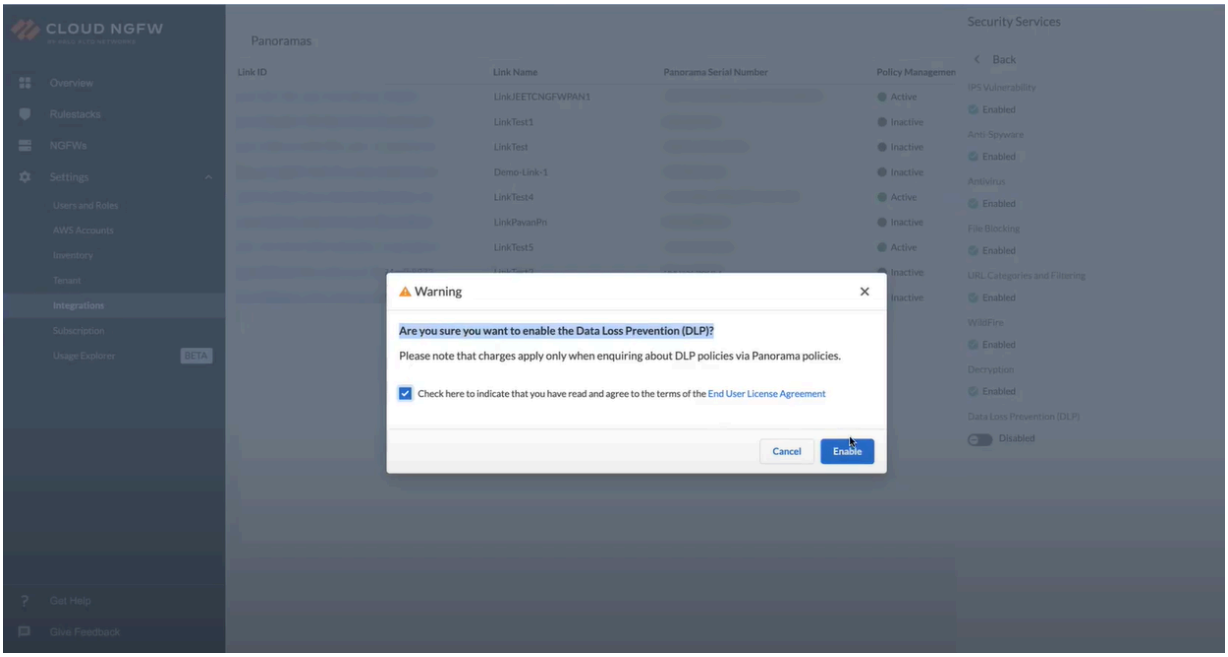


*Vous pouvez également cliquer sur **Link ID (ID de lien)** d'un Panorama lié, puis sur **Check Details (Vérifier les détails)**.*

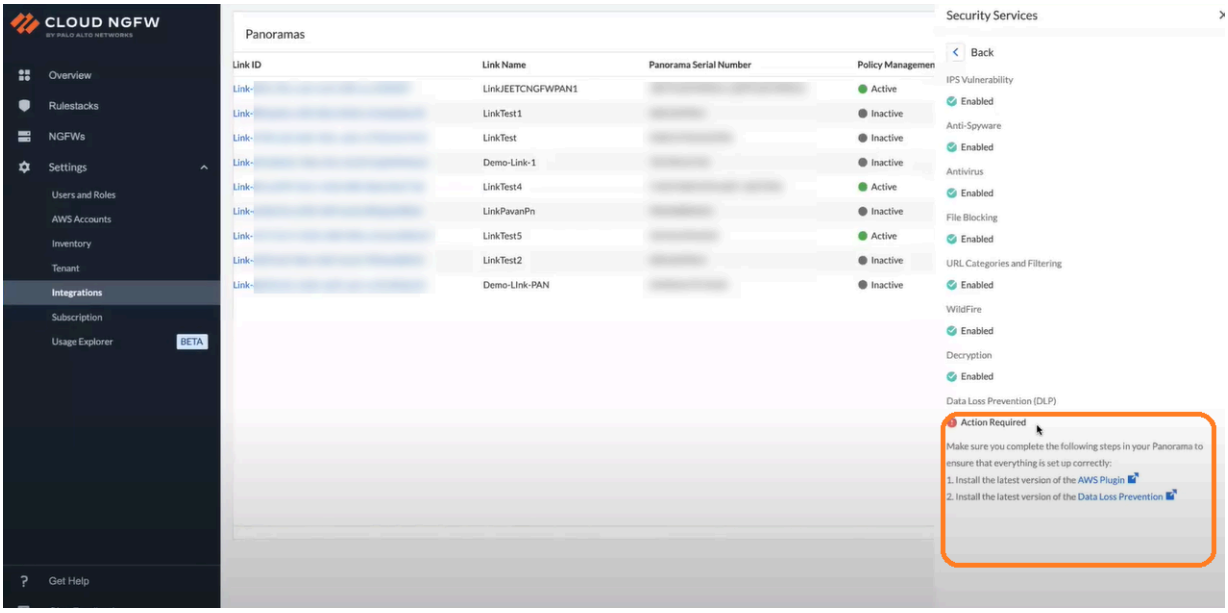
STEP 4 | Dans le panneau **Security Services (Services de sécurité)**, cliquez sur la bascule **Data Loss Prevention (Prévention des pertes de données – DLP)**.



STEP 5 | Cochez la case pour accepter le **End User License Agreement (Contrat de licence utilisateur final)**, puis cliquez sur **Enable (Activer)**.



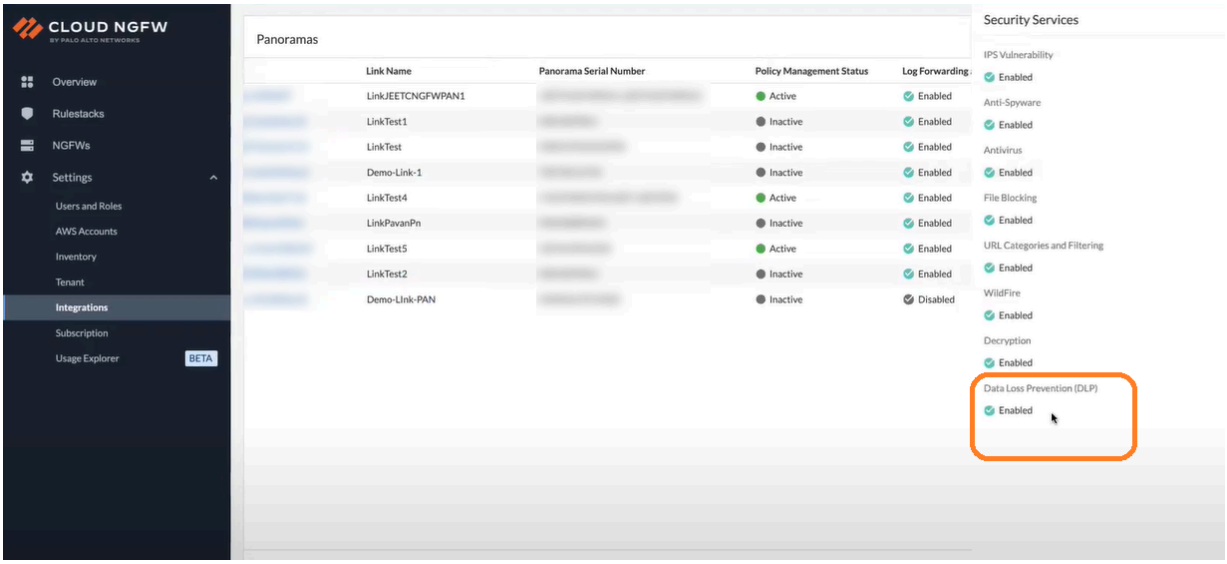
STEP 6 | Passez en revue l'**Action Required (Action requise)** sur le Panorama lié.



Vérifiez que le Panorama lié a la configuration système minimale requise, notée plus haut sur cette page, pour intégrer DLP à votre service Cloud NGFW.

Une fois que vous avez installé le plug-in AWS et DLP requis sur votre Panorama, le locataire DLP sur une console Cloud NGFW est activé.

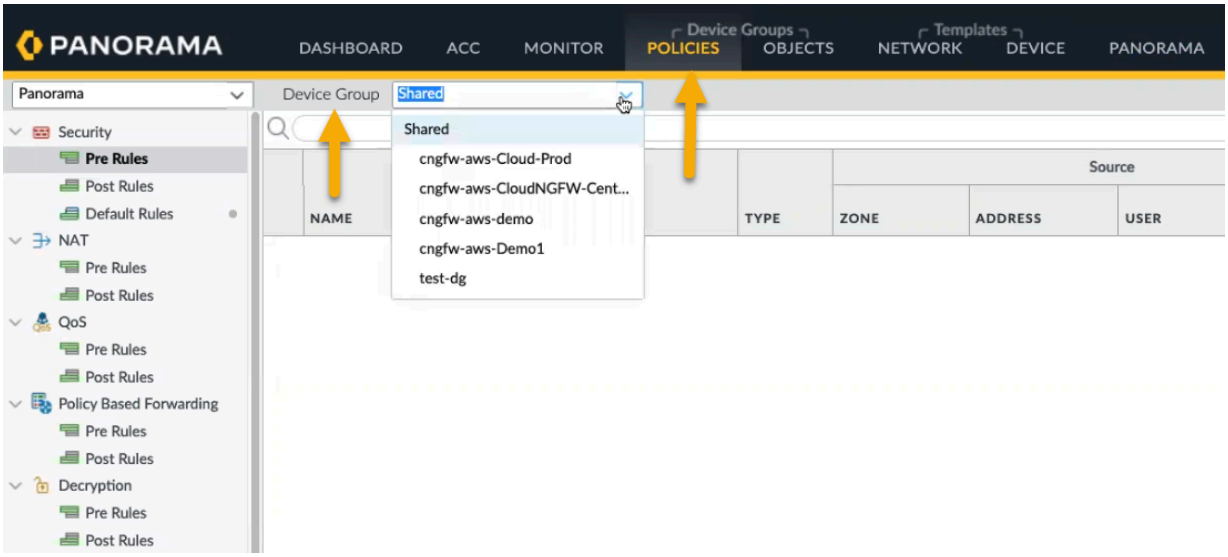
Sur la console Cloud NGFW, accédez à la page **Integrations (Intégrations)**, sélectionnez le Panorama lié, puis cliquez sur **Check Details (Vérifier les détails)** sous la colonne **Security Services (Services de sécurité)**.



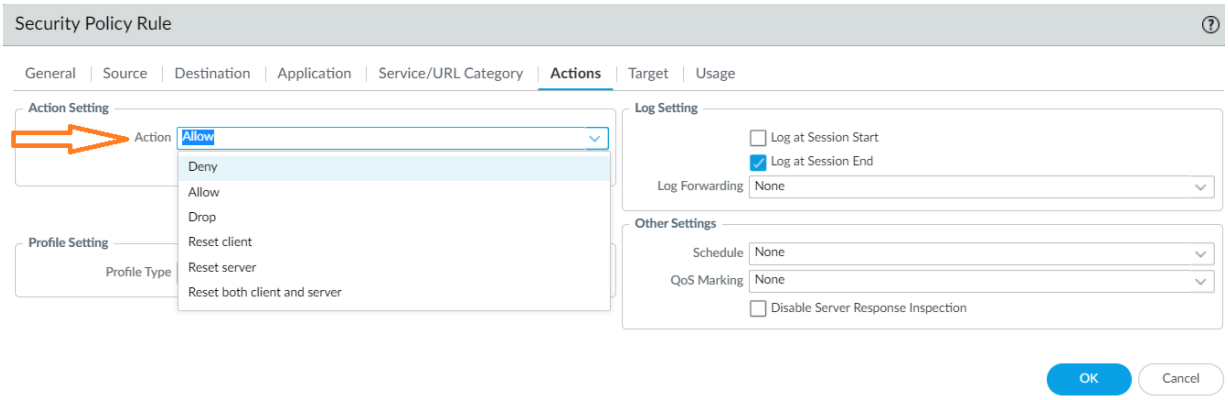
Vous pouvez désormais voir que la **Data Loss Prevention (DLP) (Prévention des pertes de données (DLP))** est activée.

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.

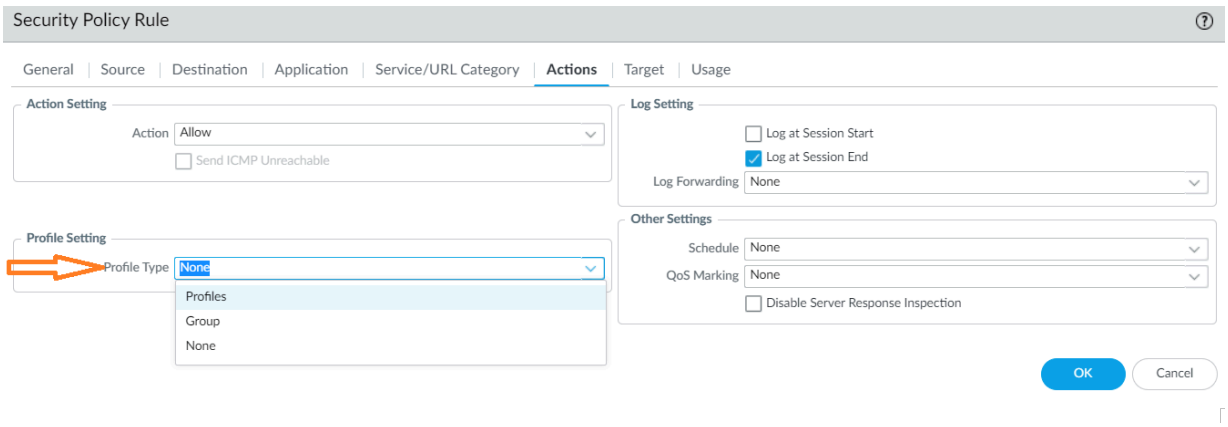
Vous pouvez ajouter un profil de filtrage DLP à votre **Security Policy Rule (Règle de politique de sécurité)** pour votre pare-feu dans Panorama.



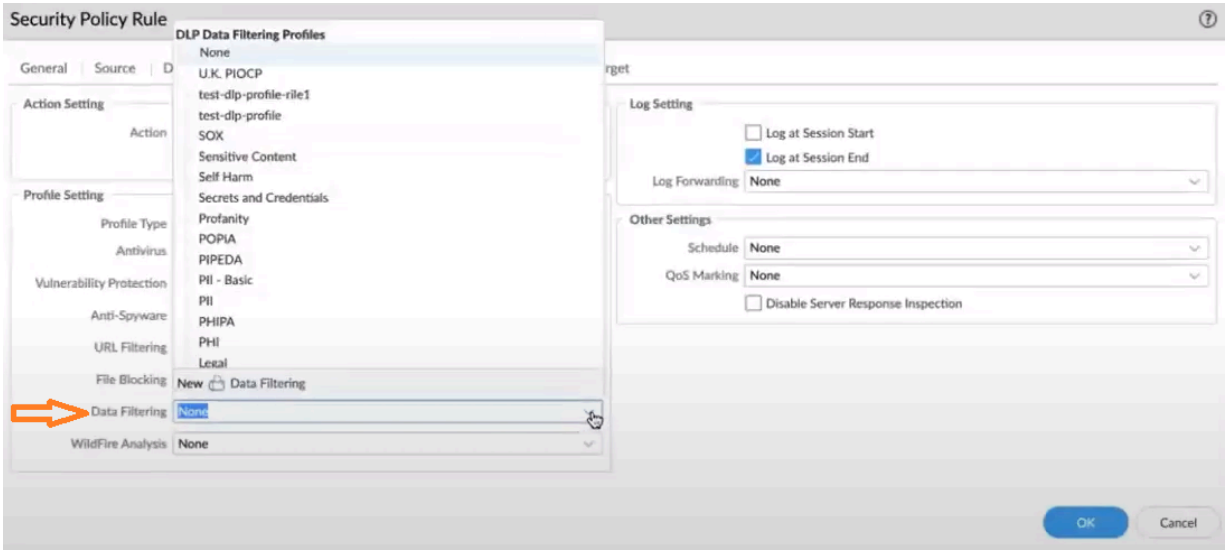
Sur l'écran **Security Policy Rule (Règle de politique de sécurité)**, accédez à l'onglet **Actions**, puis sélectionnez l'action à appliquer (par exemple, autoriser ou refuser).



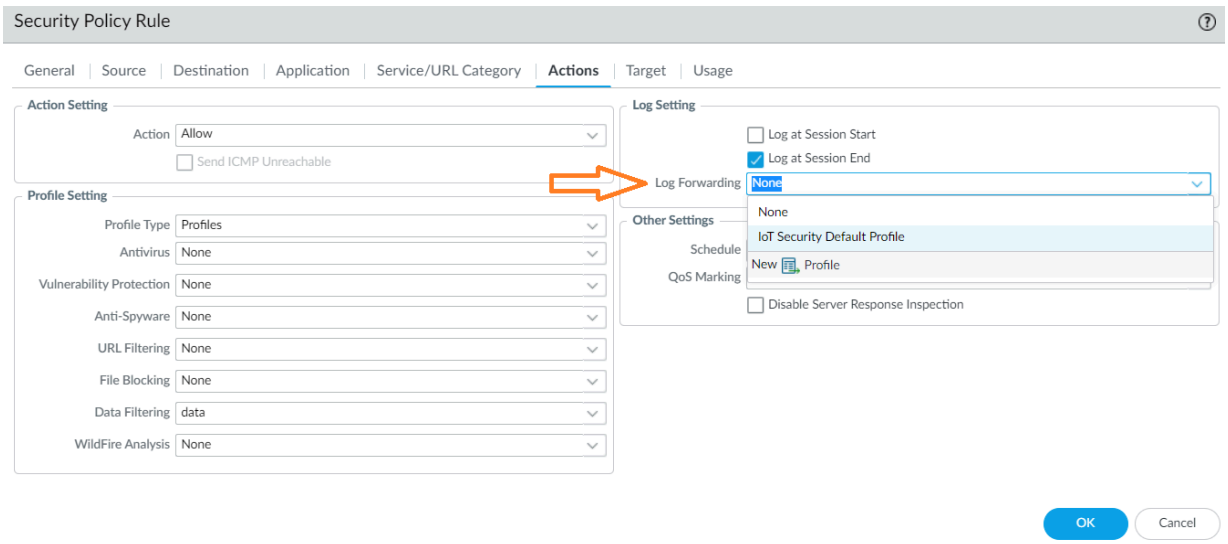
Déterminez les **Profile Setting (Paramètres du profil)**.



Sélectionnez un **DLP data filtering profile (Profil de filtrage des données DLP)**.

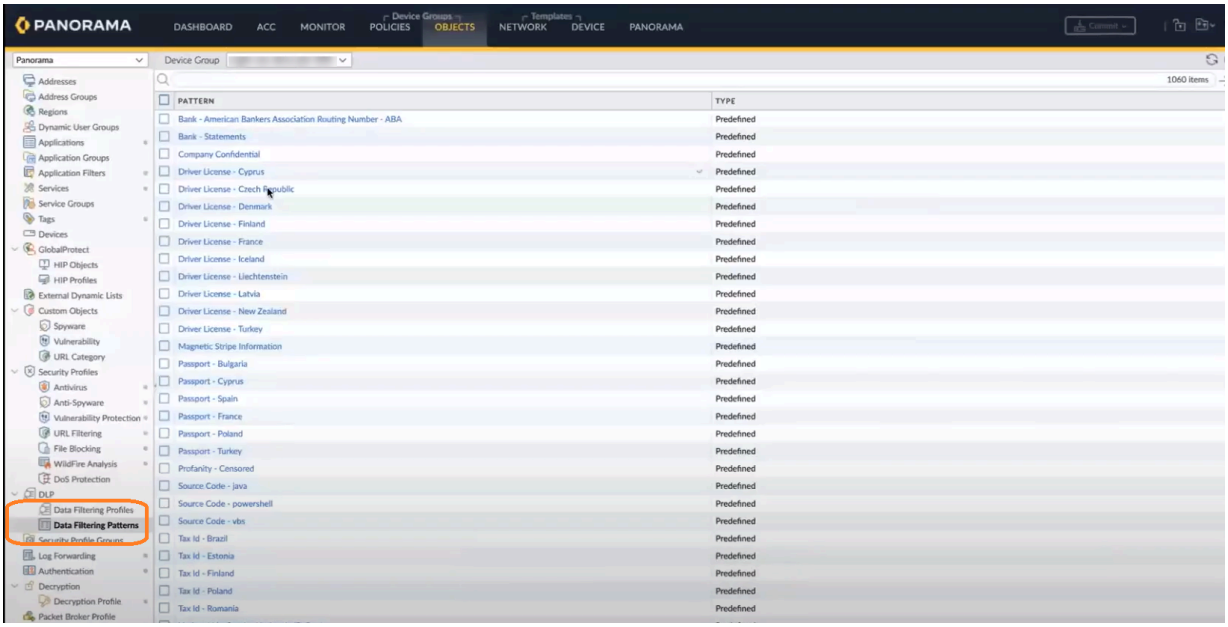


Configurez le **Log Setting (Paramètre des journaux)** et d’autres paramètres.



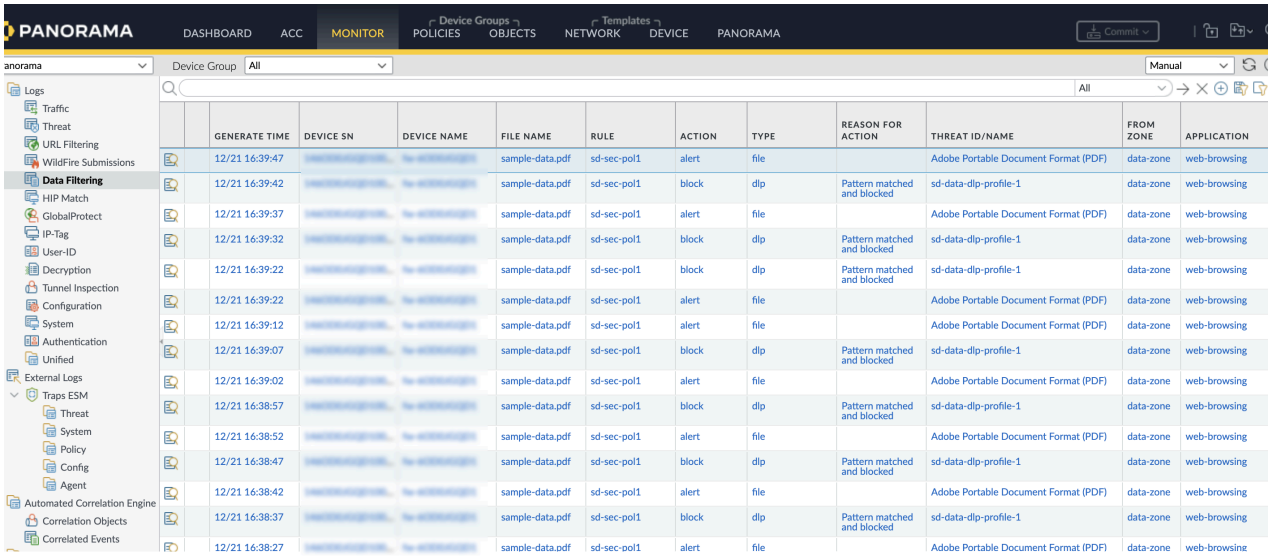
Pour en savoir plus, consultez Utiliser Panorama pour la gestion des politiques Cloud NGFW.

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 le locataire DLP.

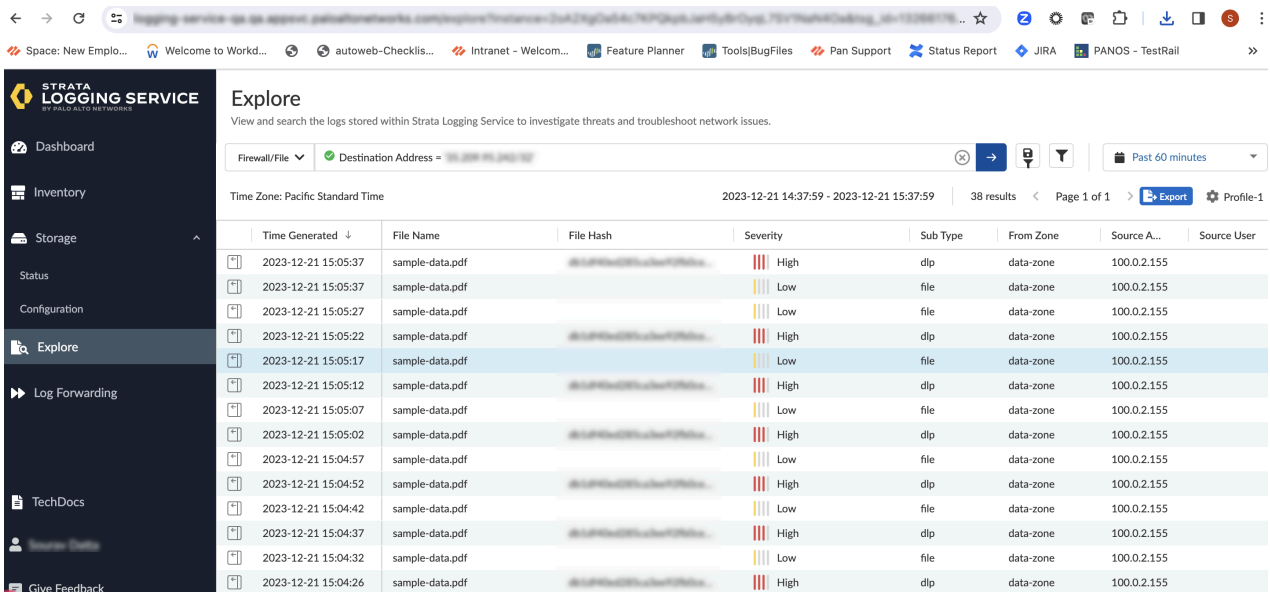


Surveillance des détails des journaux DLP

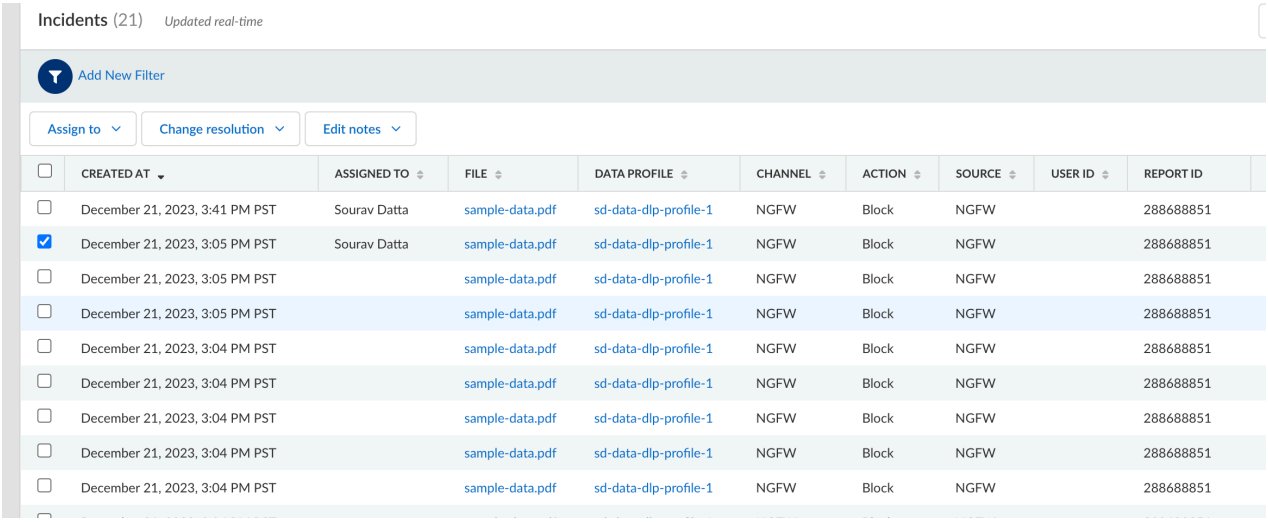
Pour afficher vos journaux DLP dans Panorama, cliquez sur l’onglet **Monitor (Surveiller)** , puis accédez à **Logs (Journaux)** > **Data Filtering (Filtrage des données)**. Pour plus d’informations, consultez Afficher les détails des journaux DLP d’entreprise sur Panorama.



Pour afficher les journaux du service de journalisation Strata pour la DLP, accédez à l'onglet **Explore (Explorer)** et sélectionnez l'option **Firewall or File (Pare-feu ou Fichier)**. Pour en savoir plus, consultez Afficher les détails des journaux sur le service de journalisation Strata.



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.



Pour plus d’informations sur les destinations AWS sur les journaux DLP, consultez Journaux Amazon CloudWatch.

Gestion native des politiques Cloud NGFW

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

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

Alors que les règles de politique de sécurité vous permettent d'autoriser ou de bloquer le trafic sur votre réseau, les profils de sécurité servent à définir une règle `autoriser mais analyser` qui analyse les applications autorisées à la recherche de menaces telles que des logiciels malveillants, des logiciels espions et des attaques DDoS. Lorsque le trafic correspond à la règle d'`autorisation` définie dans la règle de politique de sécurité, les profils de sécurité qui sont associés à la règle sont appliqués à d'autres règles d'inspection du contenu, comme des analyses d'antivirus et un filtrage des données.

Les profils de sécurité ne sont pas utilisés dans les critères de correspondance d'un flux de trafic. Le profil de sécurité est appliqué pour analyser le trafic après qu'une application ou une catégorie a été autorisée par la règle de politique de sécurité.

Le pare-feu fournit par défaut des profils de sécurité que vous pouvez directement utiliser pour commencer à protéger votre réseau des menaces. Reportez-vous à la section Set Up a Basic Security Policy (Configuration d'une politique de sécurité de base) pour plus d'informations sur l'utilisation des profils par défaut dans votre règle de politique de sécurité.

Pour connaître les recommandations relatives aux paramètres de bonnes pratiques en matière de profils de sécurité, reportez-vous aux bonnes pratiques pour la création de profils de sécurité.

Vous pouvez ajouter des profils de sécurité généralement appliqués ensemble pour Create a Security Profile Group (Créer un groupe de profils de sécurité) ; cet ensemble de profils est traité comme une unité et ajouté à des règles de politiques de sécurité en une seule étape (ou inclus par défaut dans des règles de politiques de sécurité), si vous choisissez de configurer un groupe de profils de sécurité par défaut).

Les profils de sécurité offrent des protections fondamentales en recherchant les menaces dans le trafic que vous autorisez sur le réseau. Les profils de sécurité fournissent une suite complète d'outils coordonnés de prévention des menaces qui bloquent le trafic d'applications de commande et contrôle (C2) peer-to-peer, les types de fichiers à risque, les tentatives d'exploitation de vulnérabilités et les signatures antivirus. En outre, ils identifient les programmes malveillants aussi bien nouveaux qu'inconnus.

L'application de profils de sécurité nécessite relativement peu d'effort, car Palo Alto Networks fournit des profils prédéfinis que vous pouvez simplement ajouter aux règles d'autorisation des politiques de sécurité. La personnalisation des profils de sécurité est également aisée, car vous pouvez cloner un profil prédéfini et le modifier. Vous pouvez également créer un profil de sécurité à partir de zéro sur le pare-feu ou sur Panorama.

Pour détecter les menaces connues et inconnues dans votre trafic réseau, associez des profils de sécurité à toutes les règles de politique de sécurité autorisant du trafic sur le réseau afin que le pare-feu inspecte tout le trafic autorisé. Le pare-feu applique les profils de sécurité au trafic correspondant à la règle d'autorisation de la politique de sécurité, analyse le trafic conformément aux paramètres du profil de sécurité, puis prend les mesures appropriées pour protéger le réseau. Sauf indication contraire, les recommandations relatives aux meilleures pratiques en matière de profils de sécurité s'appliquent aux quatre flux de trafic de centre de données.

Téléchargez automatiquement les mises à jour du contenu et installez-les dès que possible afin de disposer des derniers contenus et signatures de prévention des menaces (antivirus, anti-logiciel espion, vulnérabilités, logiciel malveillant, etc.) sur le pare-feu et de bloquer les dernières menaces.

Rulestacks et règles sur Cloud NGFW pour AWS

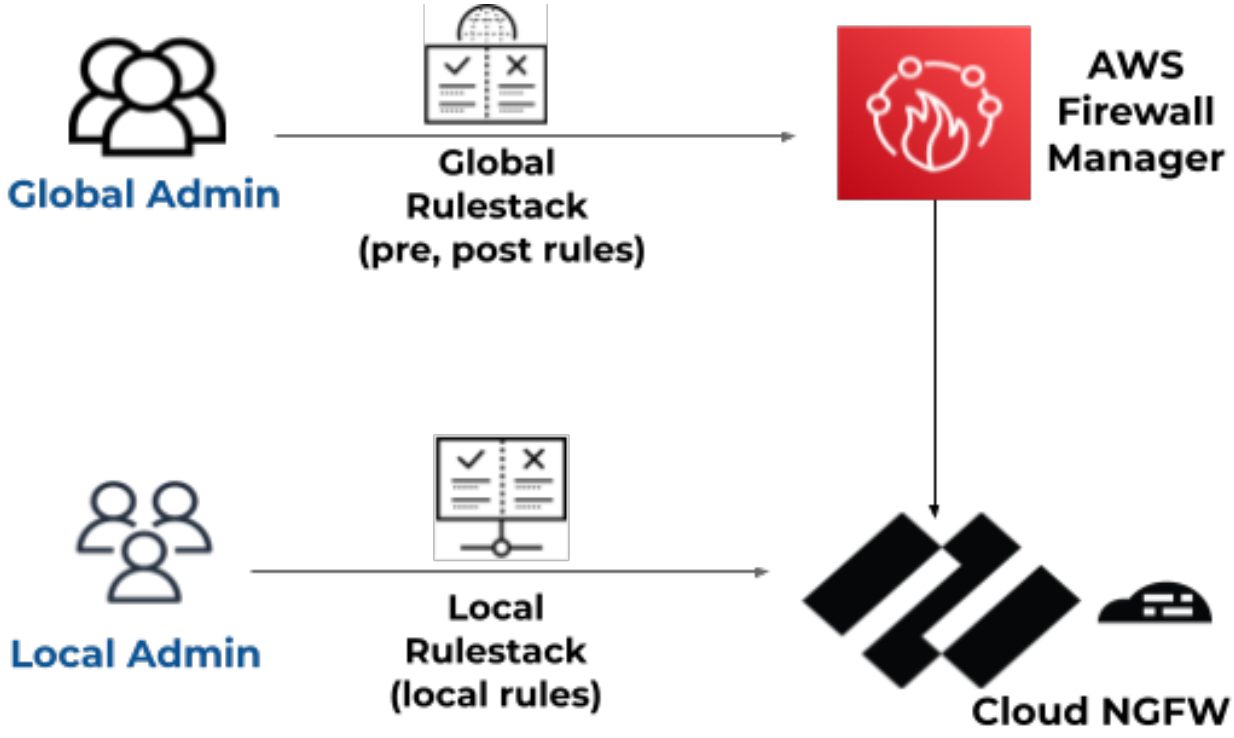
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d'utilisateur (locataire ou administrateur)

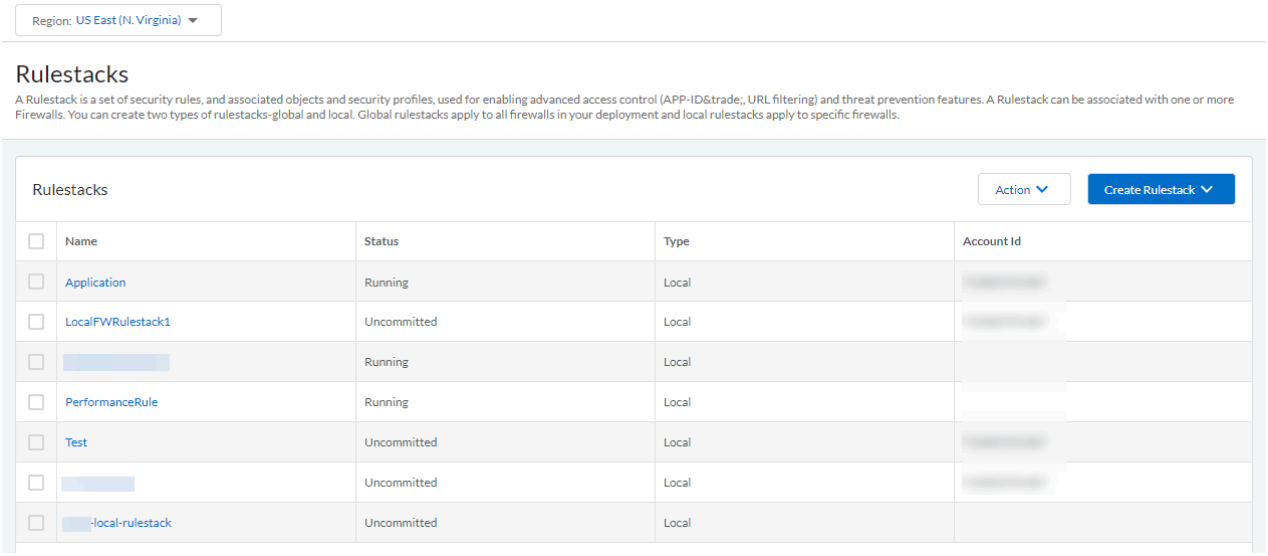
Les rulestacks définissent le contrôle d'accès (App-ID, filtrage des URL) et le comportement de prévention des menaces des ressources Cloud NGFW. Une ressource Cloud NGFW utilise vos définitions de rulestack pour protéger le trafic par un processus en deux étapes. Tout d'abord, elle applique vos règles 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 rulestack 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 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 « avant »** – Règles ajoutées en haut de l'ordre des règles. Ces règles sont évaluées en premier.
  - **Règles « après »** – Règles ajoutées en bas de l'ordre des règles. Ces règles sont évaluées après les règles « avant » et les règles définies dans une rulestack locale appliquées à un NGFW individuel.

Lorsque vous utilisez AWS 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 « après » permettent d'autoriser ou de refuser le trafic qui ne correspond pas aux règles « avant » ou aux règles définies dans la rulestack locale.





Une rulestack globale et une rulestack locale sont appliquées à chaque NGFW.

Si vous utilisez un locataire multicompte ou multi-VPC, tenez compte des modifications suivantes concernant 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 est effectuée par un utilisateur disposant des autorisations LRA dans le compte de la rulestack.

Les certificats de tout compte intégré sont mappés à une rulestack. Par exemple, le certificat dans compte1 et le certificat dans compte2 sont 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

Dans le client 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. Appliquez la rulestack uniquement aux NGFW associés à ce compte AWS. 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.

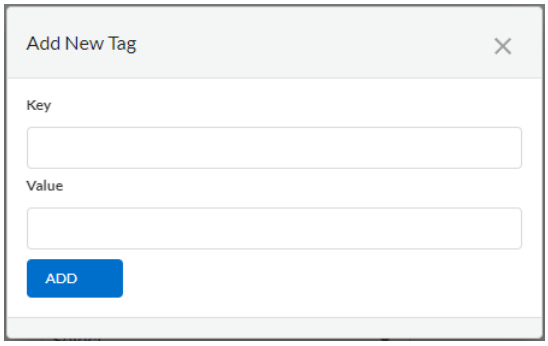
STEP 3 | Saisissez un **Name (Nom)** descriptif pour votre rulestack.

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)**.

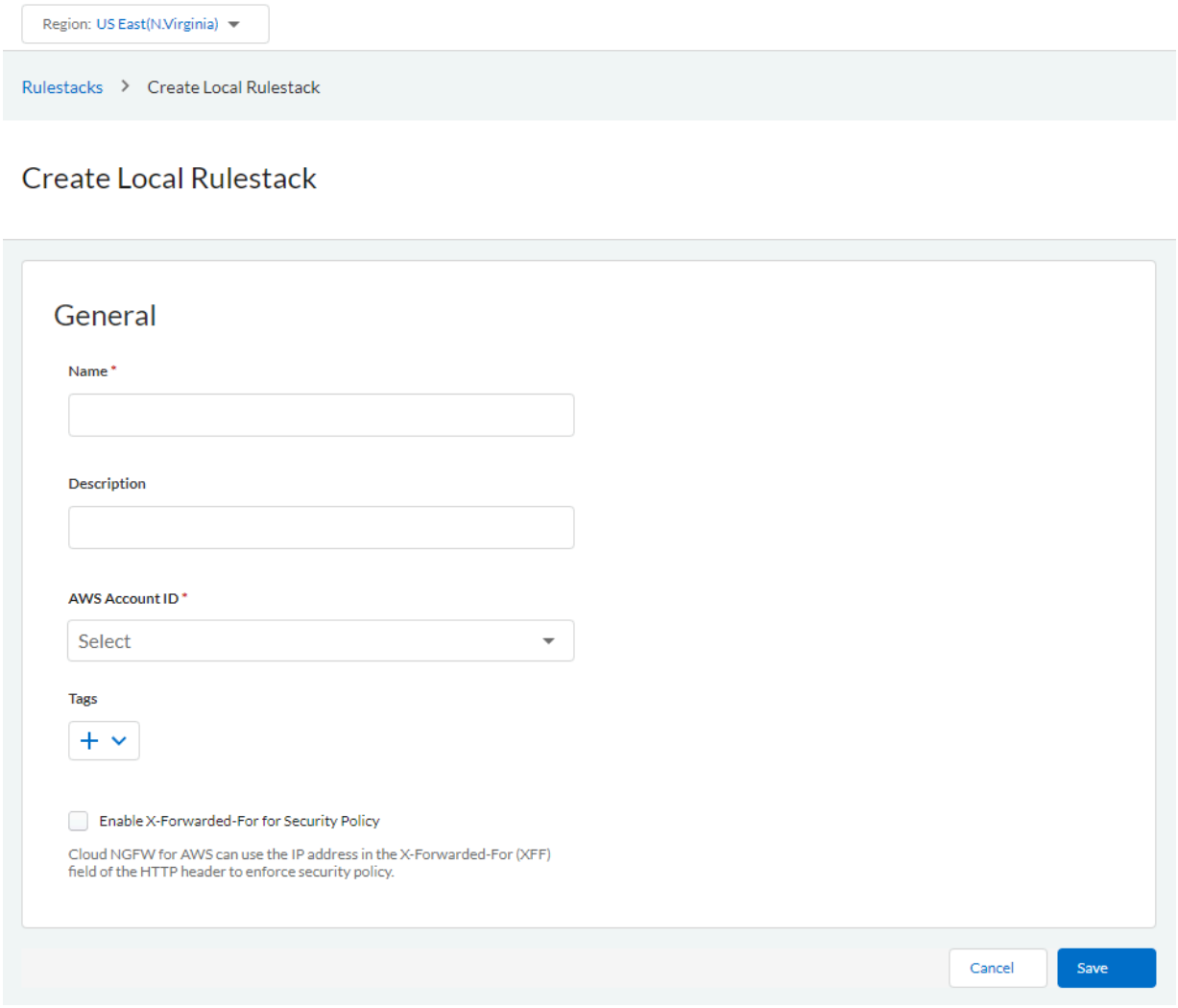
1. Cliquez sur l'icône + et sélectionnez **Add New (Ajouter nouveau)**.
2. Entrez une **Key (Clé)** et une **Value (Valeur)**.
3. Cliquez sur **Add (Ajouter)**.



STEP 7 | (Facultatif) **Enable X-Forwarded-For for Security Policy (Activer X-Forwarded-For pour la politique de sécurité)**. Consultez X-Forwarded-For pour en savoir plus.

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

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



X-Forwarded-For sur Cloud NGFW pour AWS

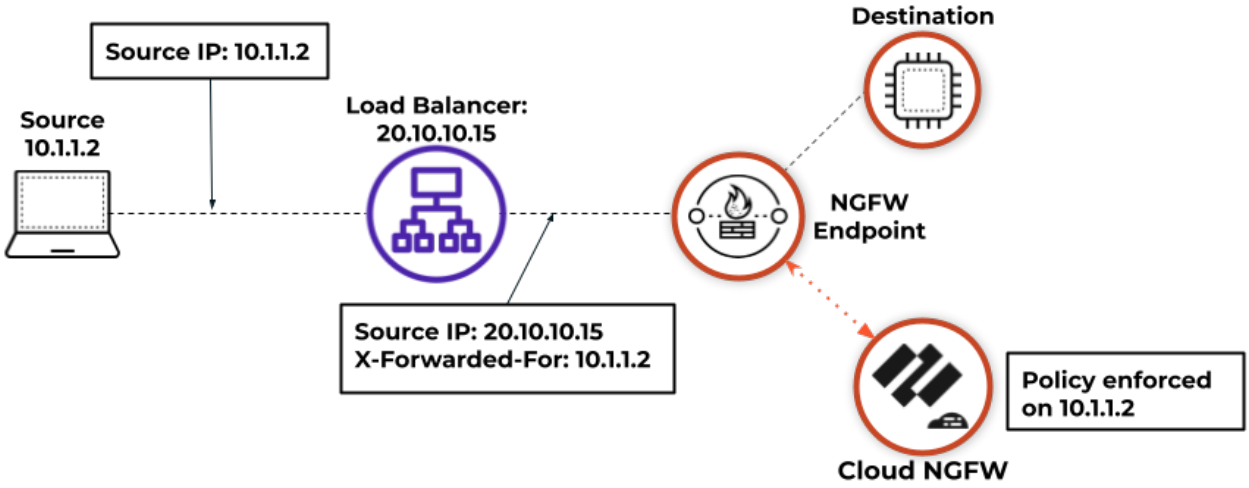
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ Rôle d'utilisateur (locataire ou administrateur)

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 liste de préfixes sur Cloud NGFW pour AWS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW

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

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.

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 des 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)**.

Ajouter un certificat à Cloud NGFW pour AWS

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

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 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-----
```

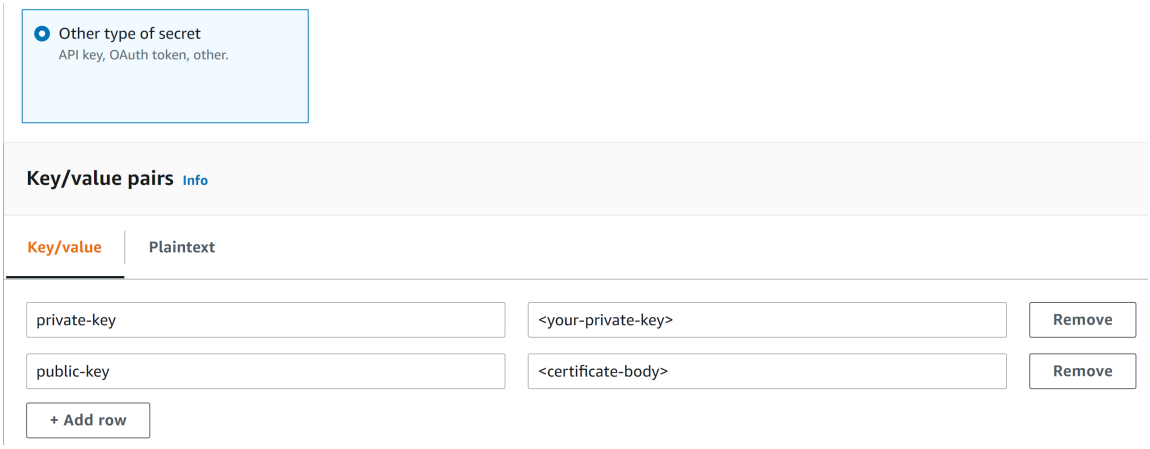
Format PKCS1 non pris en charge :

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

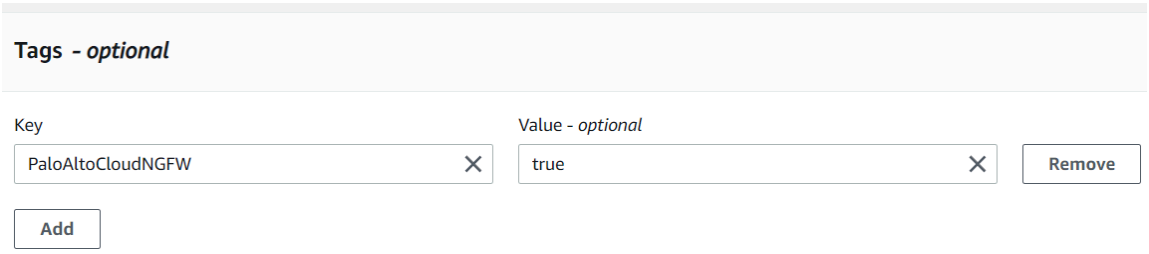
Effectuez la procédure suivante pour ajouter un certificat à utiliser avec Cloud NGFW pour AWS.

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 and value pairs (Paires clé-valeur)**, créez une clé appelée **private-key** et une autre appelée **public-key**.
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.

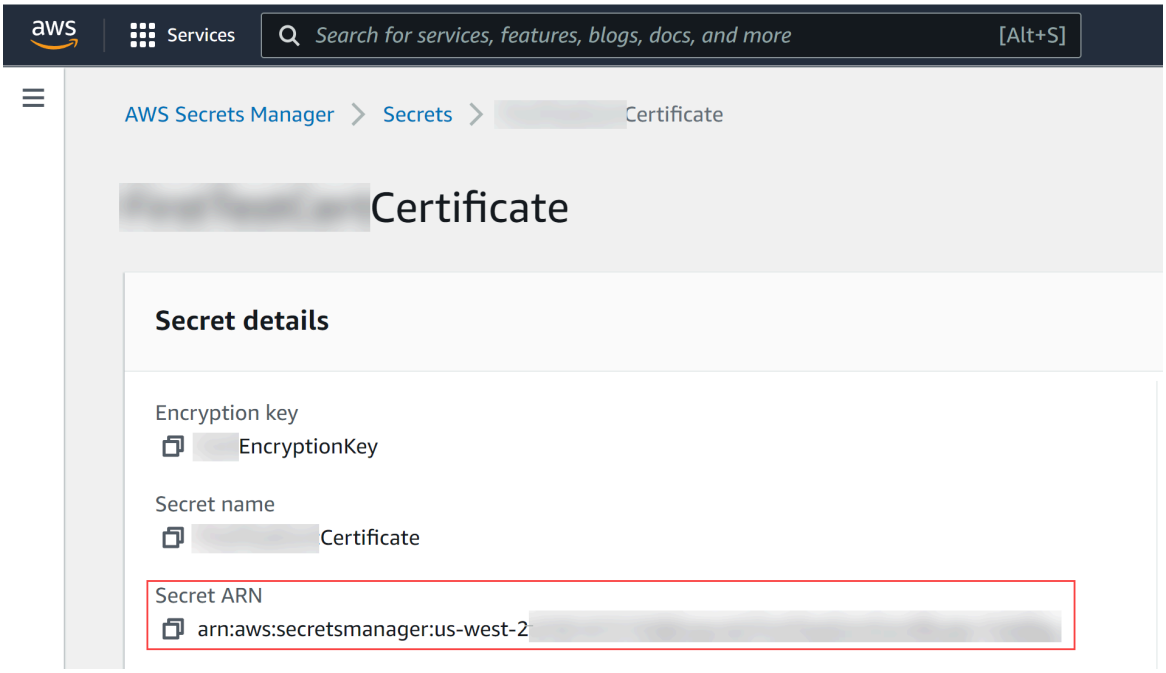
STEP 3 | Sélectionnez **Objects (Objets)** > **Certificate List (Liste des certificats)** > **Add Certificate (Ajouter un certificat)**.

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

STEP 5 | (Facultatif) Saisissez une description pour votre certificat.

STEP 6 | Sélectionnez un 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 une liste FQDN pour Cloud NGFW sur AWS

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

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.

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)**.

Configurer un flux intelligent sur Cloud NGFW pour AWS

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

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
	❑ Compte AWS Marketplace ❑ Rôle d’utilisateur (locataire ou administrateur)

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.

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 la liste, sans vous obliger à apporter des modifications à la configuration.

- **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 restrictions (voire aucune) sur le contenu, les attaquants 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 malveillantes identifiées dans des informations sur les menaces publiées par des 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 ont été jugées malveillantes à la suite de l’analyse effectuée par WildFire, de la recherche de l’Unité 42 et des données recueillies de la télémétrie. Les attaquants se servent de ces adresses IP presque exclusivement pour distribuer des logiciels malveillants, commencer des activités de commande et contrôle et lancer des attaques.
  - **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, mais il est associé de manière disproportionnée à des activités malveillantes, en particulier dans les environnements d’entreprise.

  Vous pouvez connecter votre NGFW à des flux intelligents intégrés de Palo Alto Networks et à des flux intelligents tiers pour obtenir des informations à jour sur les menaces pesant sur votre réseau. Si la connexion nécessite des certificats de décryptage, vous pouvez configurer Cloud NGFW pour qu’il utilise un objet de certificat Cloud NGFW, comme décrit ci-dessous.

Pour les listes d'IP et d'URL :

- **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 Cloud NGFW sur AWS – Advanced URL Filtering.

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)**.

Créer des règles de sécurité sur Cloud NGFW pour AWS

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

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 règles plus génériques afin que les meilleurs critères de correspondance soient appliqués

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 déclenché 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 présumée 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 nombre de correspondances de 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 **Manage (Gérer)** > **Rulestacks** et sélectionnez la rulestack cible pour la 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 application, le trafic est évalué par rapport à la règle s'il 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 s'il correspond à la catégorie d'URL ou au flux intelligent (type URL) spécifiés.

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)**.

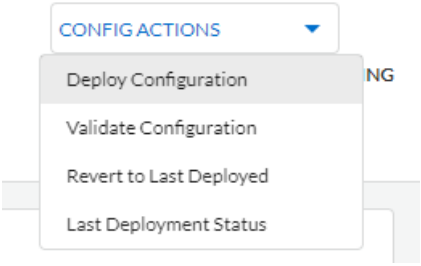
   Si vous choisissez **Any (N'importe lequel)**, le trafic est évalué quels que soient le port et le protocole. Si vous spécifiez un port et un protocole, le trafic est évalué par rapport à la règle si le trafic correspond au port et au protocole spécifiés.
2. Si vous choisissez Select (Sélectionner), 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 indiquer 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.



Profils de sécurité Cloud NGFW pour AWS

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

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 la façon Cloud NGFW doit analyser le trafic autorisé et bloquer les menaces telles que 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 anti-spyware permettent d'identifier les hôtes infectés lorsque le trafic quitte le réseau, tandis que les profils de vulnérabilité 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

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

  Le tableau suivant décrit la configuration anti-spyware par défaut 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

Gravité de la signature	Action
Faible	Par défaut

Le tableau suivant répertorie toutes les signatures possibles pour les catégories Vulnérabilité et Logiciel espion. 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 exécute ou avec quels programmes il est conçu pour interagir. Le plus souvent, des acteurs malveillants dissimulent du code pour dissimuler des logiciels malveillants. Plus rarement, des développeurs légitimes peuvent occulter du code pour protéger la confidentialité ou la propriété intellectuelle, ou pour améliorer l’expérience utilisateur. Par exemple, certains types de dissimulation (tels

Catégorie de menaces	Description
	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 Denial-of-Service (déni de service – DoS) dans le cadre de laquelle un pirate tente de rendre indisponible un système ciblé afin d'interrompre 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 exploitations qui ciblent une ou plusieurs vulnérabilités et expositions courantes (CVE) pour plusieurs navigateurs et plug-ins. 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. Une fuite d'informations est souvent due à l'absence de contrôles complets visant à protéger les données. Les pirates peuvent alors 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.
Overflow	Détecte une vulnérabilité de débordement dans le cadre de laquelle un pirate pourrait exploiter le manque de contrôles adéquats des requêtes. Une attaque réussie pourrait entraîner l'exécution de code à distance avec les privilèges de l'application, du serveur ou du système d'exploitation.
phishing	Détecte une situation où un utilisateur tente de se connecter à une page d'hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d'hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.
protocol-anomaly	Détecte les anomalies de protocole, lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur

Catégorie de menaces	Description
	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 injecte 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 n'effacent pas complètement les données saisies par l'utilisateur.
Signatures 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 utile détectent le trafic C2 (commande et contrôle) 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.
Botnet (Réseau de robots)	Indique une activité de botnet. Un botnet est un réseau d'ordinateurs infectés par des logiciels malveillants (« bots ») qui sont contrôlés par un pirate. Le pirate peut ordonner, de manière centralisée, à chaque ordinateur d'un réseau de botnets d'effectuer simultanément une action coordonnée (par exemple, le lancement d'une attaque par déni de service).
browser-hijack	Détecte la présence d'un plug-in ou d'un logiciel qui modifient les paramètres du navigateur. Un pirate de navigateur peut prendre en charge la

Catégorie de menaces	Description
	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, ce qui rend 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 cyberattaque, 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 formulaire, l’hameçonnage et les escroqueries) Détecte l’accès à des sites web compromis pour lesquels il a été déterminé que du code JavaScript malveillant avait été injecté en vue de la collecte d’informations sensibles sur les utilisateurs (par exemple, nom, adresse, messagerie, numéro de carte de crédit, CVV, date d’expiration) à partir de formulaires de paiement qui sont capturés 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 cyberattaques. 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.
postexploitation	Détecte les activités qui indiquent la phase postexploitation 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 e-mail 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 logiciels malveillants, 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

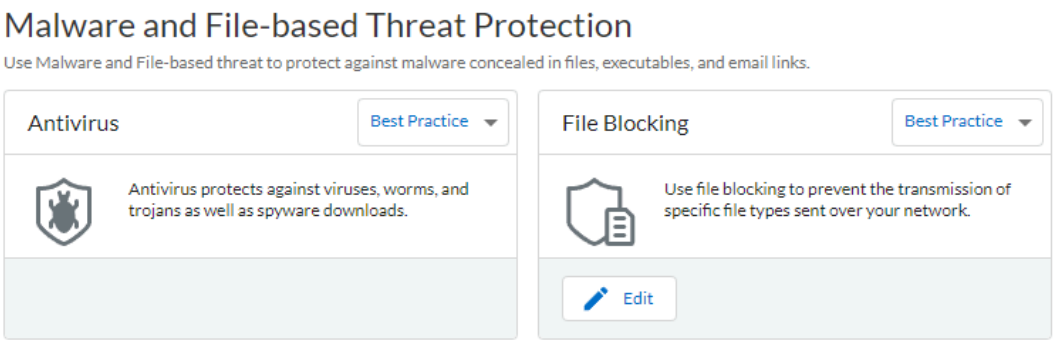
exécutables, les fichiers PDF, le code HTML et le code JavaScript. Il permet également l'analyse des fichiers compressés et des schémas de codage de données.

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.

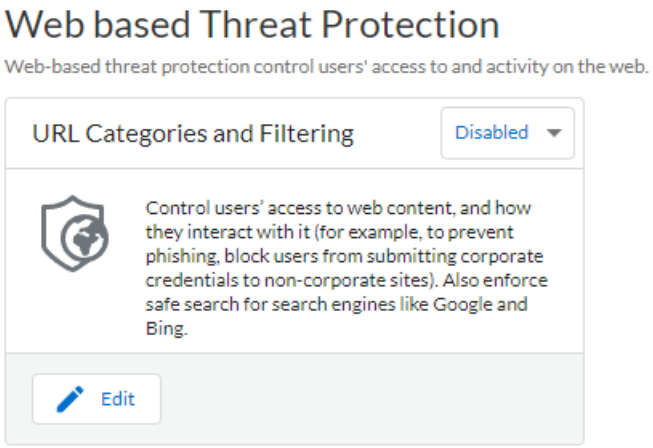
Catégorie de menaces	Description
Signatures antivirus	
APK	Fichiers malveillants d'application Android (APK).
Mac OS X	Fichiers Mac OS X malveillants, notamment : • Fichiers d’image disque Apple (DMG). • Les fichiers objet Mach (Mach-O) sont des exécutables, des bibliothèques et du code objet. • Packages 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 Portable Executable (PE) peuvent s’exécuter automatiquement sur un système Microsoft Windows et ne doivent 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 profils de filtrage des URL vous permettent de surveiller et de contrôler la manière dont les utilisateurs accèdent au web via les protocoles HTTP et HTTPS. Le pare-feu est livré avec un profil par défaut qui est configuré pour bloquer des sites Web tels que les sites renfermant des logiciels malveillants, les sites de hameçonnage et les sites pour adultes connus. Le profil de filtrage des URL n’est pas activé par défaut. Lorsque vous activez le profil de filtrage des URL dans votre rulestack, Cloud NGFW applique le profil de filtrage des URL conforme aux meilleures

pratiques sur votre trafic. Vous avez la possibilité de modifier l'option d'accès par défaut sur chacune des catégories, en fonction de vos besoins



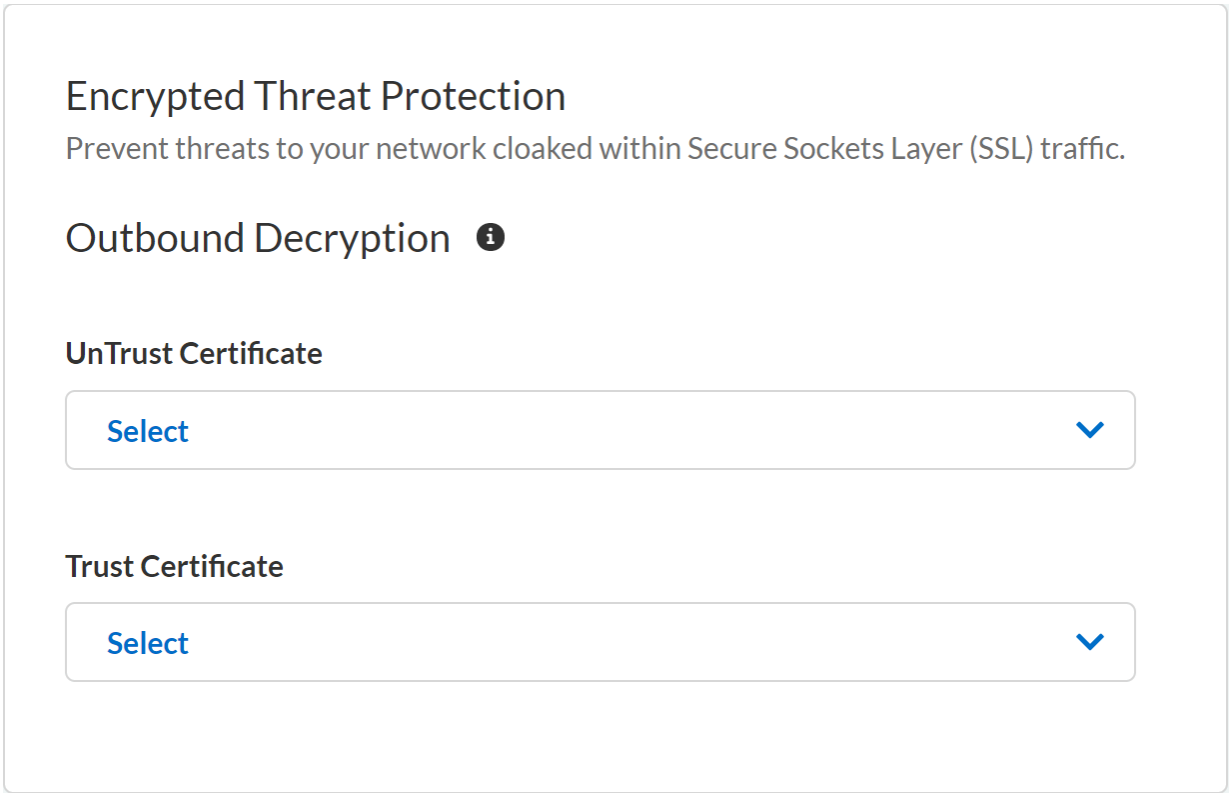
Le tableau suivant décrit la configuration par défaut du filtrage des URL selon les meilleures pratiques.

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 à décrypter 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 décrypter 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 des fichiers. Une fois que le trafic a été décrypté et inspecté, le pare-feu crypte de nouveau le trafic en texte en clair dès sa sortie du pare-feu pour garantir la confidentialité et la sécurité.



Catégories d'URL prédéfinies pour Cloud NGFW pour AWS

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

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.

Catégorie d'URL	Description
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 donc moins fiable.
Logiciel indésirable	Contenu web qui ne constitue pas une menace directe pour la sécurité, mais qui affiche un autre comportement gênant et incite l’utilisateur final à accorder un accès à distance ou à effectuer d’autres actions non autorisées. Les logiciels indésirables comprennent des activités illégales, des activités criminelles, des roguewares, des logiciels publicitaires et d’autres applications indésirables ou non sollicitées, telles que les mineurs de cryptomonnaie intégrés, le clickjacking 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 sont classés dans la catégorie des logiciels indésirables.
Piratage	Sites relatifs à l’accès illégal ou douteux ou à l’utilisation d’équipements et 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 des informations de connexion, des informations de carte de crédit (volontairement ou involontairement), des numéros de compte, des codes PIN et toute information considérée comme une information d’identification personnelle (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

Catégorie d'URL	Description
	une catégorisation différente. Cette catégorie ne devrait pas inclure les sites web fournissant un accès à distance, comme les solutions VPN 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 d'identification. Ces domaines peuvent ressembler à des domaines légitimes, par exemple pal0alto0netw0rks.com ; ils servent toutefois à usurper des informations d'identification 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 de ces sites 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, à des détails concernant les procédures d'avortement ou à des forums d'aide ou de soutien pour ou contre l'avortement, ou sites qui fournissent des informations sur les conséquences et les 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 et la conférence téléphonique, les services d'escorte, les clubs de strip-tease, etc. Tout ce qui contient du contenu pour adultes

Catégorie d'URL	Description
	(même s’il s’agit de jeux ou de bandes dessinées) est classé dans la catégorie Adulte.
Alcool et tabac	Sites qui se rapportent à la vente, à la fabrication ou à la consommation d’alcool et/ou de produits du tabac et d’accessoires connexes. Comprend les sites liés aux cigarettes électroniques.
Enchères	Sites qui favorisent la vente de biens entre particuliers.
Affaires et économie	Marketing, gestion, économie et sites liés à l’entrepreneuriat ou à la gestion d’une entreprise. Comprend les entreprises de publicité et de marketing. Ne devrait pas inclure les sites Web d’entreprise, car ils devraient être classés avec leur technologie. Aussi les sites d’expédition, tels que fedex.com et ups.com.
Informations sur les ordinateurs et Internet	Informations générales concernant les ordinateurs et Internet. Devrait inclure des sites sur l’informatique, l’ingénierie, le matériel, les logiciels, la sécurité, la programmation, etc. La programmation peut avoir un certain chevauchement avec les références, mais la catégorie principale devrait rester l’informatique et l’information Internet.
Réseaux de distribution de contenu	Sites dont l’objectif principal est de fournir à des tiers du contenu tel que des publicités, des médias, des fichiers, etc. Comprend 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	Sites web qui font la promotion de cryptomonnaies, sites web de minage de cryptomonnaies (mais pas les mineurs de cryptomonnaies intégrés), échanges et fournisseurs de cryptomonnaies, et 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).

Catégorie d'URL	Description
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 et outils de programmation, bandes dessinées, arts du spectacle, musées, galeries d'art ou bibliothèques. Comprend des sites de divertissement, de célébrités et de nouvelles de l'industrie.
Extrémisme	Sites web faisant la promotion du terrorisme, du racisme, du fascisme ou d'autres points de vue extrémistes discriminant des personnes ou des groupes d'origines ethniques, de religions ou d'autres croyances différentes. 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.
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 poules. 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 permettent de jouer en ligne ou de télécharger des jeux vidéo et/ou informatiques, des critiques de jeux, des conseils ou des codes de triche, ainsi que des sites pédagogiques pour les jeux non électroniques, la vente et l'échange de jeux de société ou des publications/médias connexes. Comprend les sites qui

Catégorie d'URL	Description
	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, les problèmes de santé et des conseils, remèdes et traitements traditionnels et non traditionnels. Comprend également des sites pour diverses spécialités, pratiques et installations (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.
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 échanges, aux modifications, aux pièces et à d'autres discussions connexes pour les automobiles, les motocyclettes, les bateaux, les camions et les véhicules récréatifs.

Catégorie d'URL	Description
Musique	Vente, distribution ou information musicale. Comprend des sites Web pour les artistes musicaux, les groupes, les labels, les événements, les paroles et d'autres informations concernant l'industrie de la musique. N'inclut pas la musique en streaming.
Actualité	Publications en ligne, agences de presse et autres sites Web qui regroupent l'actualité, la météo ou d'autres questions contemporaines. Comprend les journaux, les stations de radio, les magazines et les podcasts.
Non résolu	Indique que le site web est introuvable dans la base de données de filtrage des URL locale et que le pare-feu n'a pas pu se connecter à la base de données cloud pour vérifier la catégorie. Lorsqu'une recherche de catégorie d'URL est effectuée, le pare-feu vérifie d'abord le cache du plan de données pour l'URL, si aucune correspondance n'est trouvée, il vérifie ensuite le cache du plan de gestion, et si aucune correspondance n'y est trouvée, il interroge la base de données d'URL dans le cloud. Lorsque vous décidez de l'action à entreprendre pour le trafic classé dans la catégorie Non résolu, sachez que le blocage de ce trafic peut entraîner d'importantes perturbations chez 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.
Peer-to-peer	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. Cette catégorie concerne principalement 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 ».

Catégorie d'URL	Description
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 et la vente de propriétés, et conseils ou informations connexes. Comprend des sites pour les agents immobiliers, les entreprises, les services de location, les listes (et les agrégats) et l'amélioration de la propriété.
Loisirs et passe-temps	Informations, forums, associations, groupes et publications sur les loisirs et les loisirs.
Référence et recherche	Portails, documents ou services de référence personnelle, professionnelle ou académique. Comprend des dictionnaires en ligne, des cartes, des almanachs, des données de recensement, des bibliothèques ainsi que des renseignements généalogiques et scientifiques.
Religion	Informations concernant diverses religions et des activités ou événements connexes. Comprend les sites web d'organisations religieuses, de responsables religieux et des lieux de culte. Comprend les 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 et/ou contre des dons à des logiciels, des économiseurs d'écran, des icônes, des fonds

Catégorie d'URL	Description
	d’écran, des utilitaires, des sonneries, des thèmes ou des widgets. Inclut également les projets open source.
Achats	Sites qui facilitent l’achat de biens et de services. Comprend les marchands en ligne, les sites Web des grands magasins, les magasins de détail, les catalogues, ainsi que les sites qui regroupent et surveillent les prix. Les sites énumérés ici devraient être des marchands en ligne qui vendent une variété d’articles (ou dont le but principal est la vente en ligne). Une page Web pour une entreprise de cosmétiques qui autorise également l’achat en ligne devrait être classée avec des cosmétiques et non des achats.
Mise en réseau social	Les communautés d’utilisateurs et les sites où les utilisateurs interagissent les uns avec les autres, publient des messages, des images ou communiquent avec des groupes de personnes. N’inclut pas les blogs ou les sites personnels.
Société	Sujets relatifs à la population en général, questions qui touchent une grande variété de personnes, telles que la mode, la beauté, les groupes philanthropiques, les sociétés ou les enfants. Comprend également les sites Web des restaurants. Comprend des sites Web conçus pour les enfants ainsi que des restaurants.
Sports	Informations sur les événements sportifs, les athlètes, les entraîneurs, les responsables, les équipes ou les organisations, les résultats sportifs, les horaires et les nouvelles connexes, et tout accessoire connexe. Comprend des sites Web concernant les sports fantastiques et d’autres ligues sportives virtuelles.
Conseils et outils boursiers	Informations concernant le marché boursier, la négociation d’actions ou d’options, la gestion du portefeuille de produits Palo Alto Networks, les stratégies d’investissement, les cotations ou les actualités 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 une éducation et une formation en ligne et du matériel connexe. Peut inclure des écoles de conduite, la formation en milieu de travail, etc.

Catégorie d'URL	Description
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 d'hôtels, d'attractions locales, de casinos, de compagnies aériennes, de croisiéristes, d'agences de voyages et de locations de véhicules ainsi que les sites qui fournissent des outils de réservation tels que la surveillance des prix. Comprend les sites web de points d'intérêt locaux et d'attractions touristiques tels que la tour Eiffel, le Grand Canyon, etc.
Armes	Ventes, critiques, descriptions ou instructions concernant les armes et leur utilisation.
Publicités Web	Publicités, médias, contenu et bannières.
Hébergement Web	Services d'hébergement gratuits ou payants de pages web, y compris des informations sur le développement web, la publication, la promotion et d'autres méthodes visant à augmenter le trafic.
Messagerie Web	Tout site Web qui donne accès à une boîte de réception de courrier électronique et la possibilité d'envoyer et de recevoir des e-mails.

Configurer le blocage des fichiers sur Cloud NGFW pour AWS

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

Le blocage des fichiers vous permet 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 des 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 type de fichier 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.

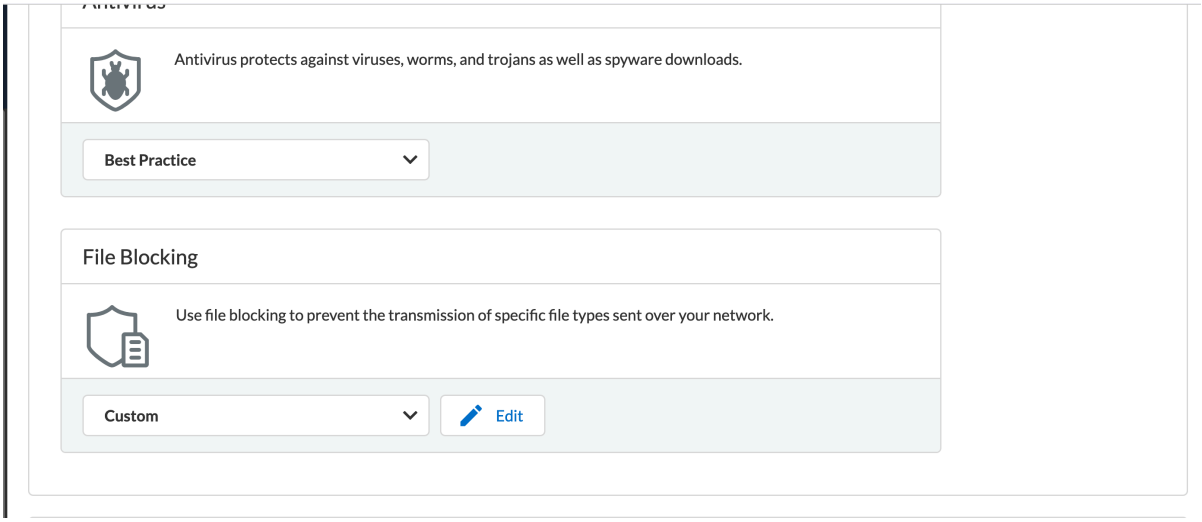
STEP 5 | Cliquez sur **Save (Enregistrer)**.

Modifier le profil de blocage de fichiers

Par défaut, le profil de blocage des fichiers est défini sur **Best Practice (Meilleures pratiques)**. Pour modifier le profil de blocage de fichiers :

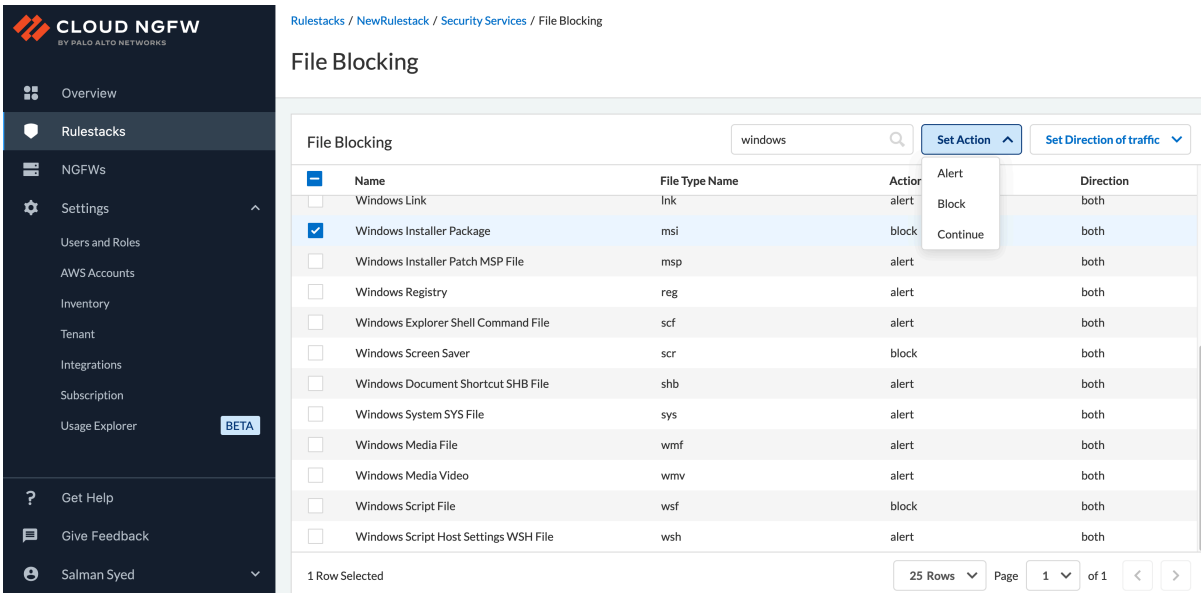
STEP 1 | Dans l’écran **Malware and File-based Threat Protection (Protection contre les logiciels malveillants et les menaces basées sur les fichiers)**, accédez à **File Blocking (Blocage des fichiers)**.

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

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

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
	❑ Rôle d’utilisateur (locataire ou administrateur)

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 (meddler in the middle (MitM)) 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. Autre solution, le NGFW peut présenter le certificat de non-approbation au client qui tente de se connecter à un serveur dont le certificat est signé par une CA que le 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 en clair, notamment les profils d’antivirus, de vulnérabilité, d’antispyware, de filtrage des URL et de blocage des fichiers. Une fois que le trafic a été décrypté et inspecté, le pare-feu crypte de nouveau le trafic en texte en clair 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. Activez 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 un certificat CA racine et un certificat CA intermédiaire dans le magasin de confiance sur le 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 décrypter le trafic, seul le certificat d’entité finale avec clé publique et privée doit être stocké dans l’ASM.

PKCS8 est le format de certificat pris en charge.

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

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

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 vos clés de session sont stockés sur AWS Secrets Manager pour permettre 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 la règle doit autoriser ou bloquer.

  *Vous pouvez créer des règles de décryptage TLS avec **Applications(App-ID) – Any (Toutes)** 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 Deny (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 décrypter 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 respectant les 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.

Utilisation des règles Cloud NGFW pour AWS

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

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 :

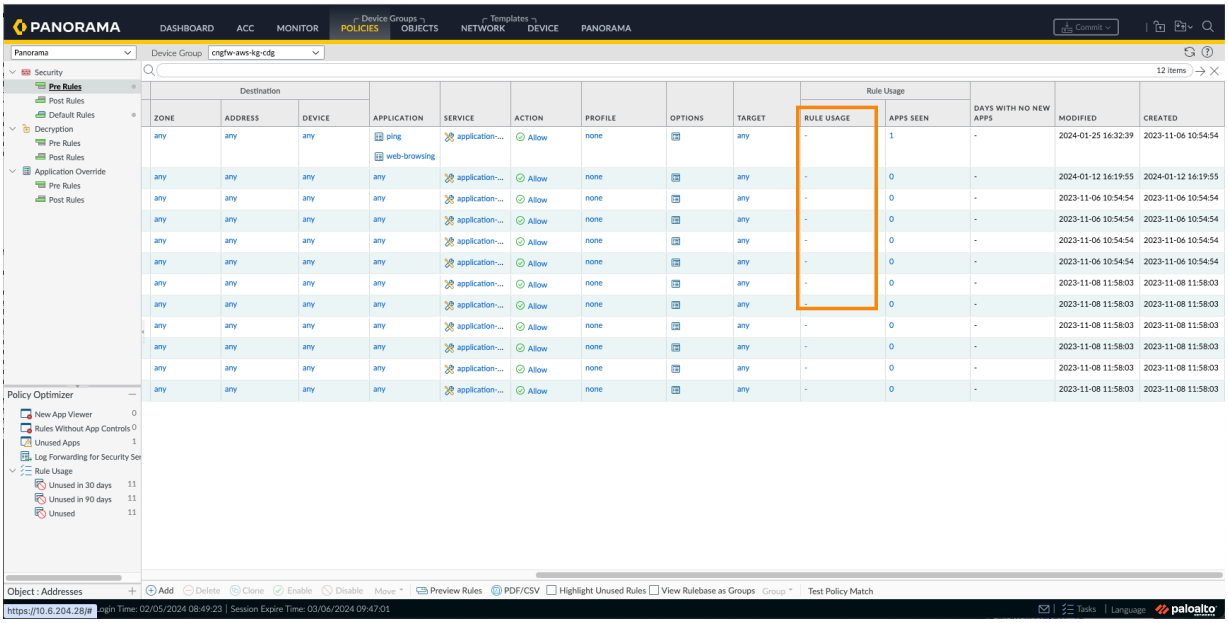
Les ressources de pare-feu NGFW rapportent vos données de correspondance de règle toutes les deux minutes au service Cloud NGFW, et celui-ci dispose alors d'une latence de deux minutes maximum pour interroger les données des ressources de pare-feu. Cela crée une latence maximale de quatre minutes dans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

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

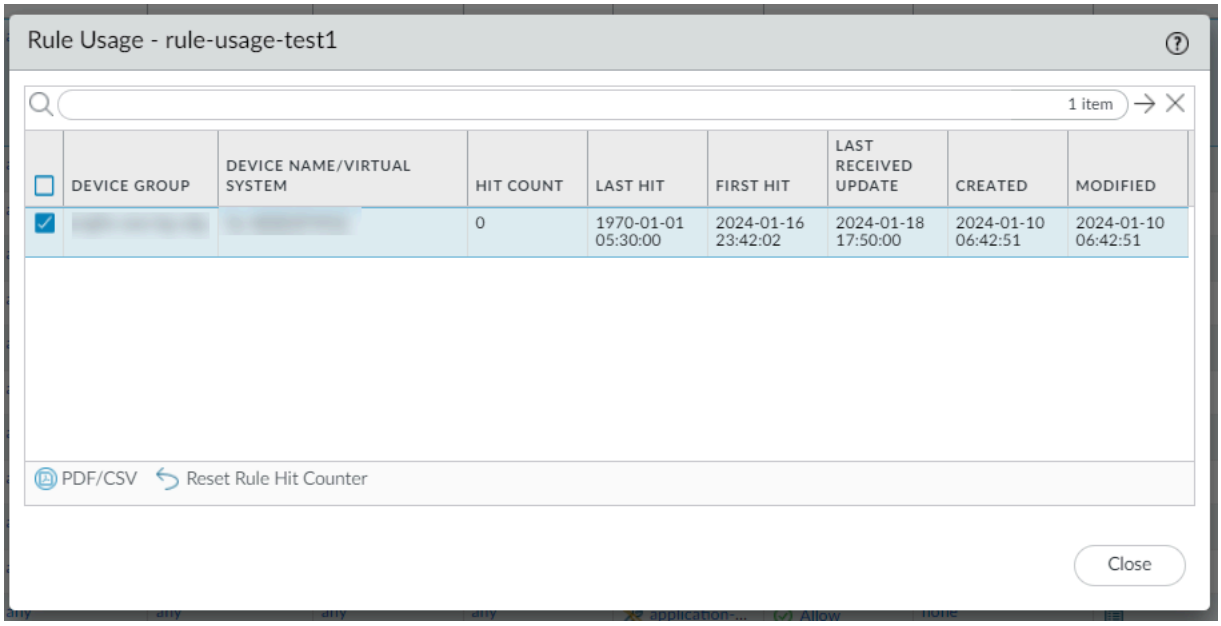
STEP 2 | Dans la section **Device Group (Groupe d'appareils)**, utilisez la liste déroulante pour sélectionner le groupe d'appareils Cloud.

STEP 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.



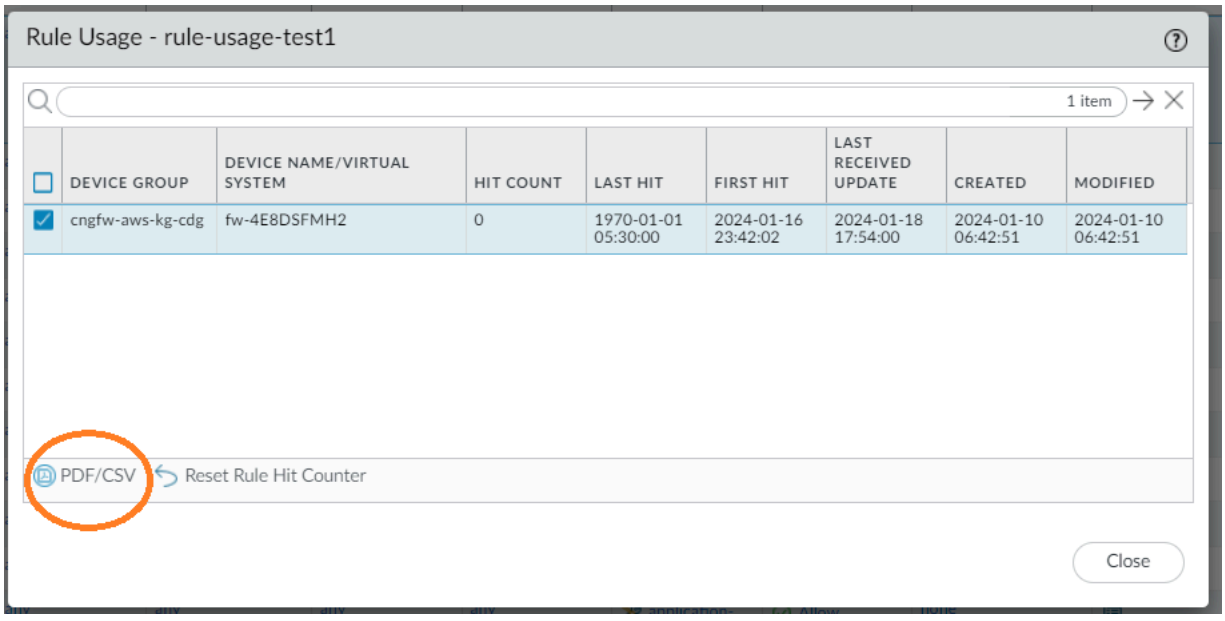
Vous pouvez maintenant voir le **Hit Count (Nombre de correspondances)** de la règle sélectionnée.



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.

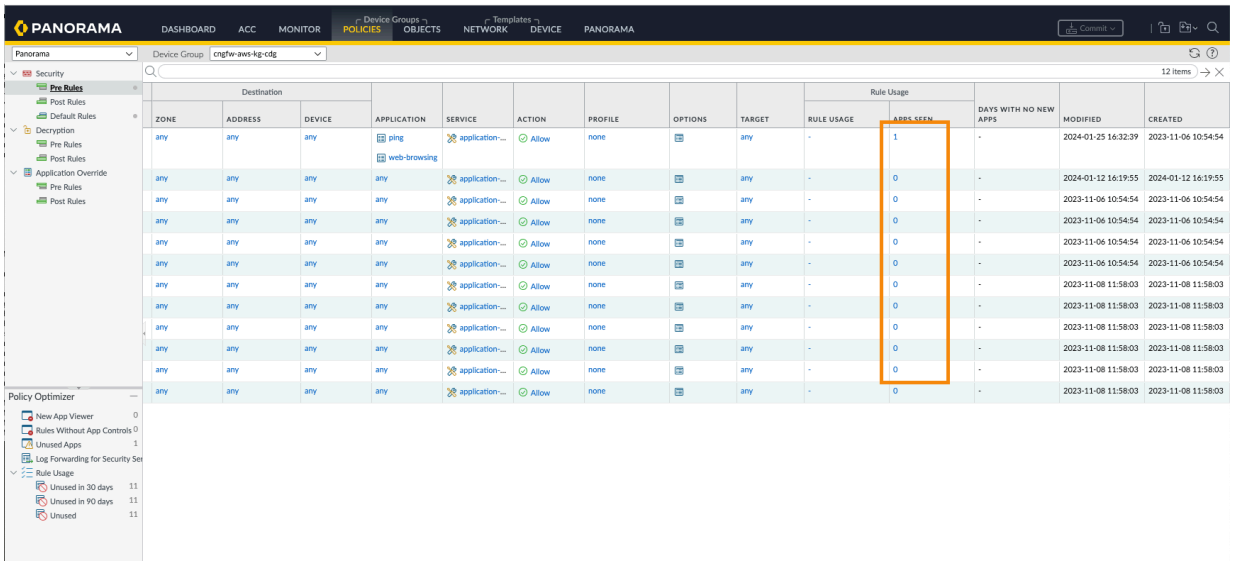


Utilisation des règles – Application vue et optimiseur de politique

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.

Gestion des politiques de Panorama

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

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 depuis une seule console Panorama.

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

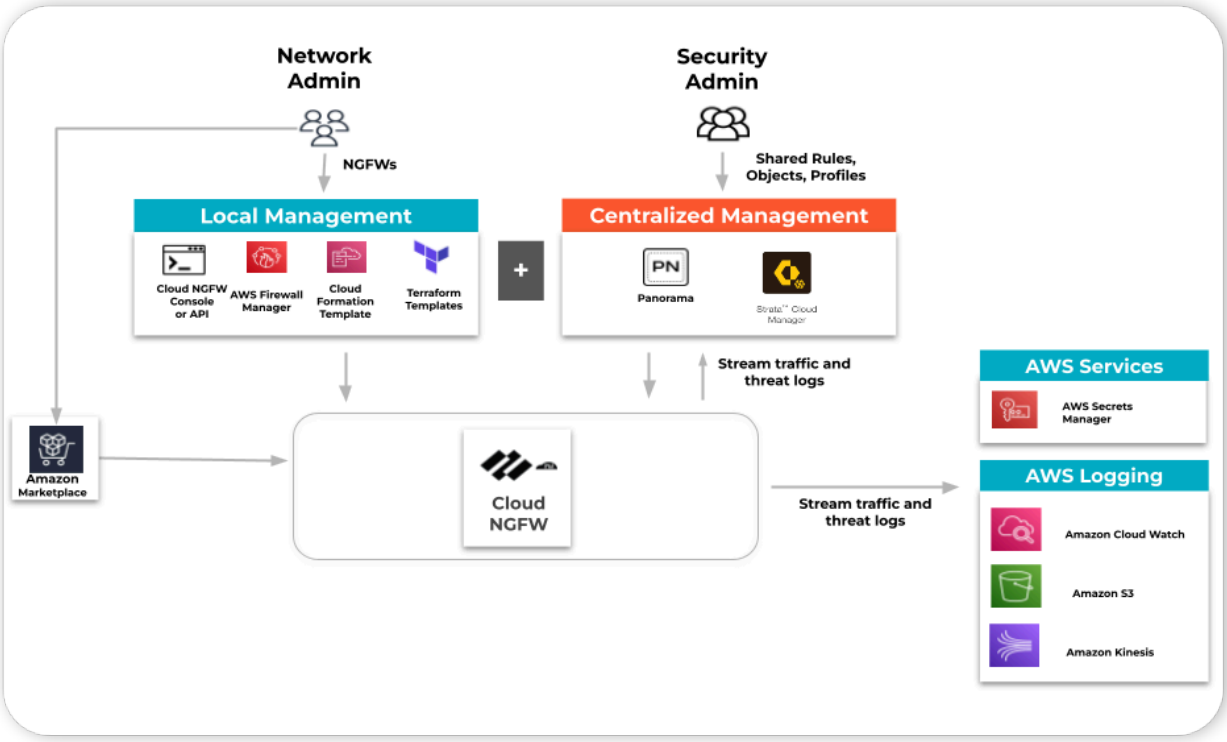
Comment fonctionne l'intégration ?

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 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.

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 vos appareils Panorama permet éventuellement à vos ressources Cloud NGFW de diffuser les journaux vers un compte de service de journalisation Strata. Vous pouvez ensuite utiliser l'interface web du service de journalisation Strata, la visionneuse de journaux Panorama ou l'Application Command Center (Centre de commande des applications – ACC) pour afficher et analyser les journaux du service de journalisation Strata. Panorama utilise le plug-in Cloud Services pour interroger les journaux de votre compte de service de journalisation Strata.

Vous pouvez également configurer les ressources Cloud NGFW pour diffuser les journaux vers des destinations de journaux AWS telles que S3, Cloudwatch et des flux Kinesis.



Vous pouvez lier plusieurs paires Panorama-service de journalisation Strata 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 obligatoire et constitue le composant principal de la solution. Vous devez utiliser l’appareil **Panorama** pour créer et gérer des règles de politique pour vos ressources Cloud NGFW. Le composant de gestion des politiques permet également d’associer les politiques et objets que vous créez 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 pouvez utiliser le service de journalisation Strata si vous préférez afficher les journaux dans la console Panorama. Vous avez également la possibilité d’utiliser l’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 lier votre Panorama à un compte de service de journalisation Strata à l’aide du plug-in Cloud Services dans Panorama. Vous pouvez configurer les ressources Cloud NGFW pour envoyer les journaux simultanément au service de journalisation Strata et à l’une des destinations de journaux AWS (S3, Cloudwatch ou flux Kinesis).

1) Liez le Panorama au service de journalisation Strata avant de le lier au locataire Cloud NGFW. 2) Si vous utilisez plusieurs Panoramas avec le même locataire Cloud NGFW, veillez à ce que chaque Panorama soit lié à des instances individuelles du service de journalisation Strata.

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 règles de politique et les objets sur les ressources NGFW 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 spécialisés 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 ou des API du plug-in AWS Panorama en spécifiant le locataire Cloud NGFW et les informations de région AWS. Le groupe d’appareils cloud se manifeste sous la forme d’une rulestack globale dans ce locataire ou 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 sur l’interface web 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 les profils et objets partagés existants dans les groupes d’appareils Panorama existants en y faisant référence dans les règles de sécurité que vous créez dans les groupes d’appareils cloud.
- Vous pouvez également ajouter ces Cloud DG à la hiérarchie du groupe d’appareils que vous gérez dans Panorama pour hériter des règles et des objets du groupe d’appareils. Toutefois, Cloud NGFW ne peut actuellement pas appliquer toutes les règles héritées par le groupe d’appareils cloud, notamment celles qui utilisent des zones de sécurité ou des utilisateurs.
- Vous pouvez associer le même groupe d’appareils cloud à plusieurs régions du locataire Cloud NGFW. Ce groupe d’appareils cloud 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 spéciales qui permettent aux règles de sécurité dans les groupes d’appareils cloud de faire référence aux paramètres des objets que

Panorama vous permet de gérer à l'aide de modèles. Lors de la création d'un groupe d'appareils cloud, 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 groupe d'appareils Cloud en tant que pile de modèles de référence. Ensuite, vous pouvez utiliser la page de la pile de modèles sur l'interface web 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 ignore 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 des journaux dans vos modèles, tels qu'ils sont référencés par la configuration du groupe d'appareils cloud. 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 sont nécessaires pour intégrer Cloud NGFW à Panorama. Après avoir configuré l'appareil virtuel Panorama et installé les 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.

Préparation à l'intégration de Panorama

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

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

- Vérifiez que vous disposez d'un Panorama enregistré pour lequel vous avez installé des licences, que vous avez activé la licence d'assistance sur le portail du support client (CSP) et que vous utilisez la version 10.2.3 (ou une version ultérieure) du logiciel.

  Vous devez installer le certificat du 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 de Palo Alto Networks, veillez à configurer Panorama pour le service de journalisation Strata.
- Assurez-vous de vous être abonné à Cloud NGFW avec succès pour disposer d'un locataire Cloud NGFW. Utilisez l'abonnement Cloud NGFW pour une intégration réussie 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 l'adresse est différente, vous ne pourrez pas configurer Cloud NGFW et l'intégrer à 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 fourni 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.
```

Remarques 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 si vous mettez à niveau le 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. Vous recevez alors un message d'erreur semblable à ceci : *La transmission ne peut pas être traitée, le chargement de la configuration n'est pas terminé. Veuillez réessayer ultérieurement.* Pour résoudre ce problème, utilisez `commit-force`, puis `commit-all`.

Lier le Cloud NGFW à Palo Alto Networks Management

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
	❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle d’utilisateur (locataire ou administrateur)

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. Associez le locataire Cloud NGFW à Panorama pour la gestion des politiques et au service de journalisation Strata pour la gestion des journaux.

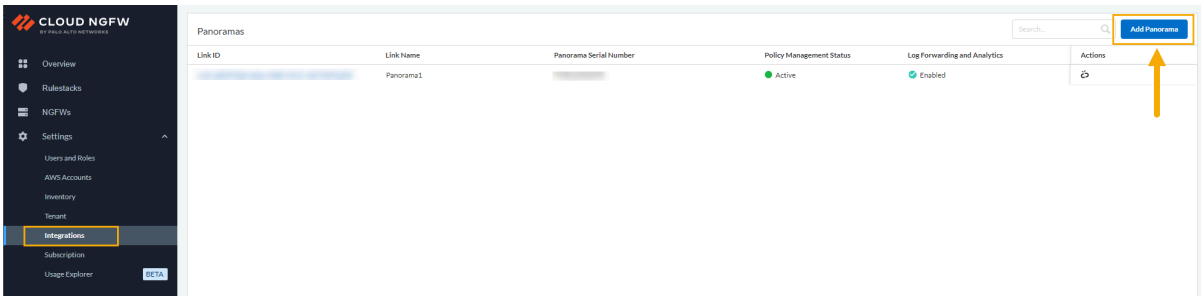
Vous devez être abonné au service Cloud NGFW à l’aide d’AWS Marketplace pour intégrer Cloud NGFW à Panorama. Après avoir lié votre locataire Cloud NGFW à Panorama, vous pouvez afficher les locataires et les ressources, ainsi que leur état, dans la console Panorama sous le plug-in AWS.

Consultez Dissocier de Panorama 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 Panorama de Cloud NGFW 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)**.

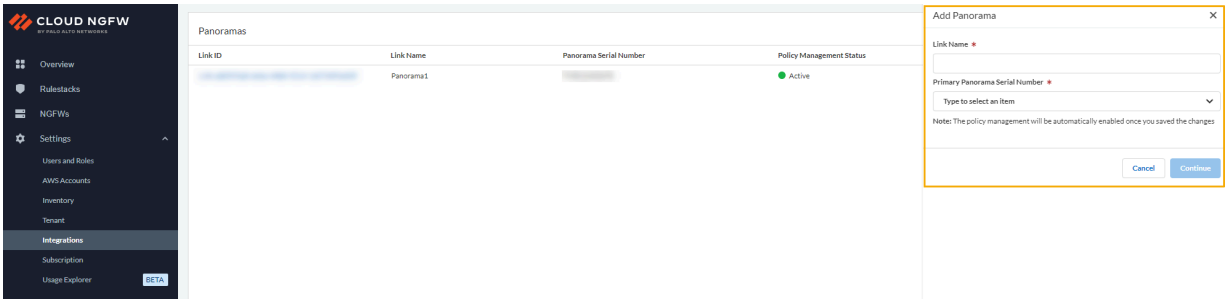
STEP 2 | Sur la page **Integrations (Intégrations)**, cliquez sur **Add Panorama (Ajouter Panorama)**.



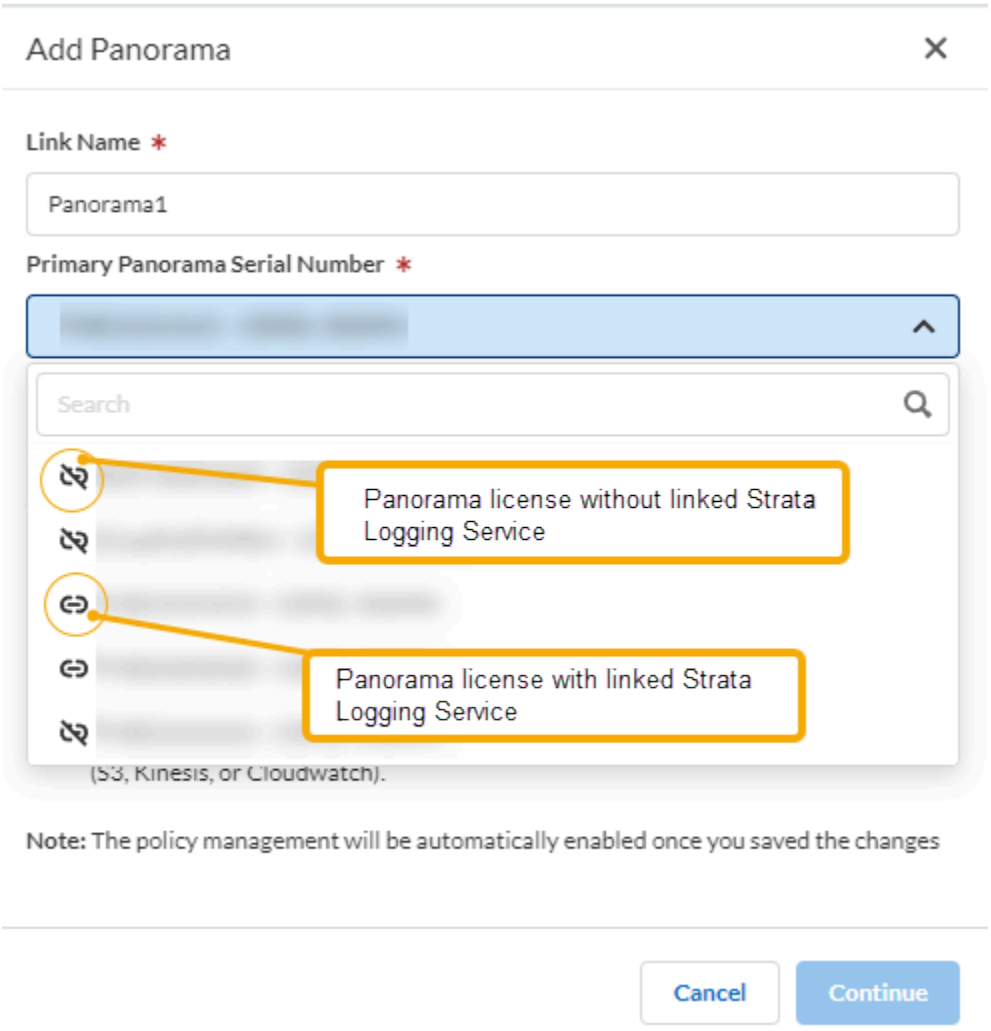
Si vous utilisez un locataire lié à Panorama qui avait été créé à l'aide d'AWS Firewall Manager, vous ne pouvez pas dissocier la ressource Cloud NGFW.

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 au service de journalisation Strata et un Panorama non lié au service de journalisation Strata. Ces icônes sont illustrées dans l'image ci-dessous :

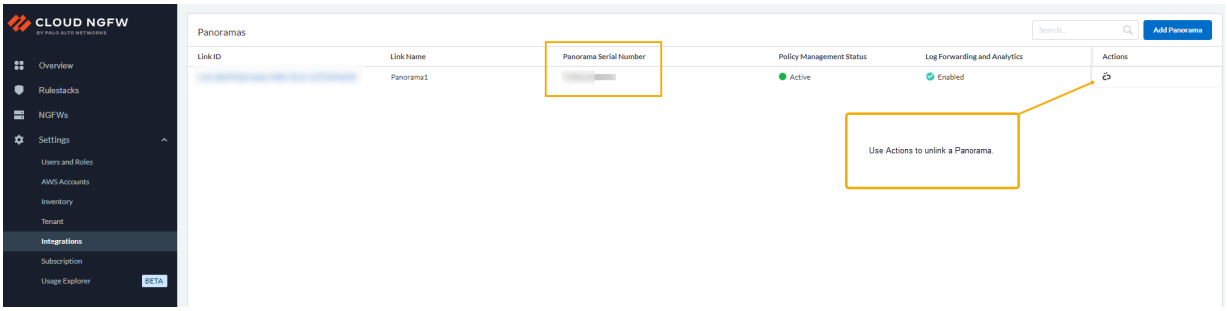


Si vous sélectionnez un numéro de série Panorama qui n'est pas lié au service de journalisation Strata, vous devez spécifier une option : soit vous annulez le processus de liaison, auquel cas vous acceptez

d’acquérir une licence de service de journalisation Strata 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 au service de journalisation Strata, vous devez sélectionner **Confirm (Confirmer)** pour confirmer l’association avant de poursuivre le processus d’intégration.

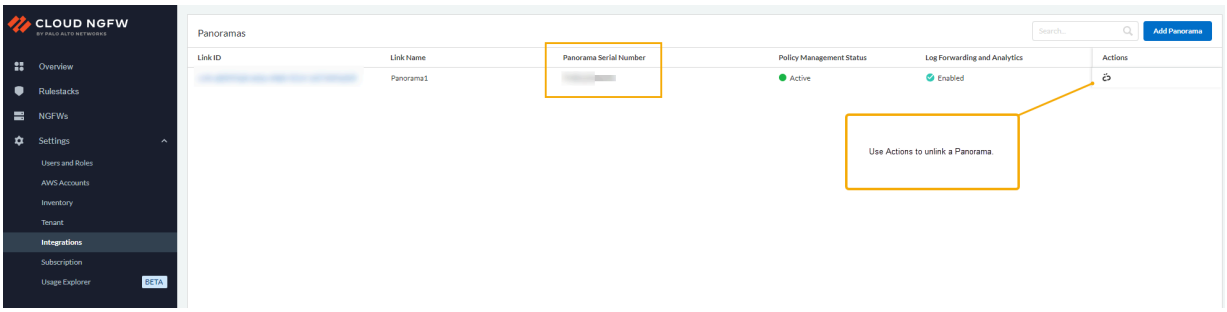
Après avoir sélectionné la licence Panorama, cliquez sur **Continue (Continuer)**. La page **Integrations (Intégrations)** affiche le **Link ID (ID du lien)** et le **Panorama Serial Number (Numéro de série Panorama)** lié :



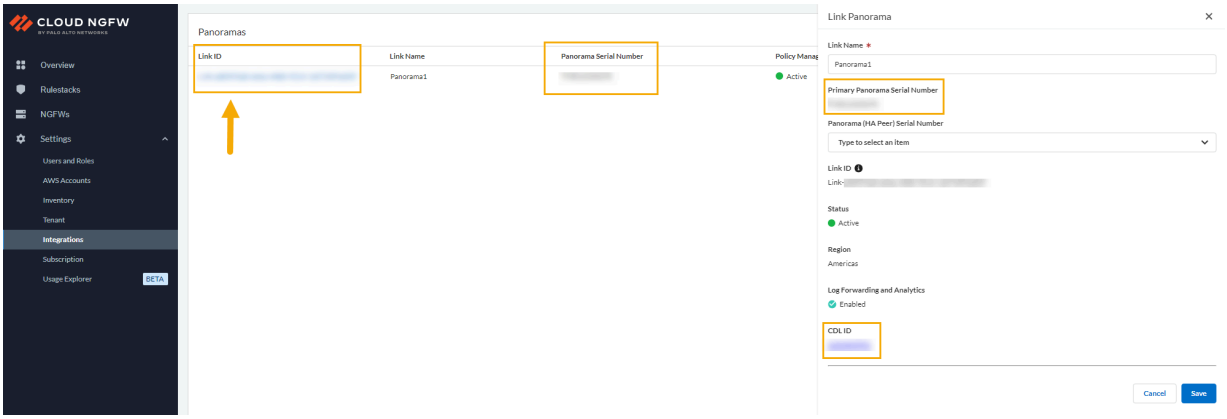
Le locataire Cloud NGFW extrait automatiquement de Panorama les informations sur le service de journalisation Strata. Si vous ne prévoyez pas d’utiliser le service de journalisation Strata, vous pouvez

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 du service de journalisation Strata associé au Panorama lié, cliquez sur **Link ID (ID du lien)** sur 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.

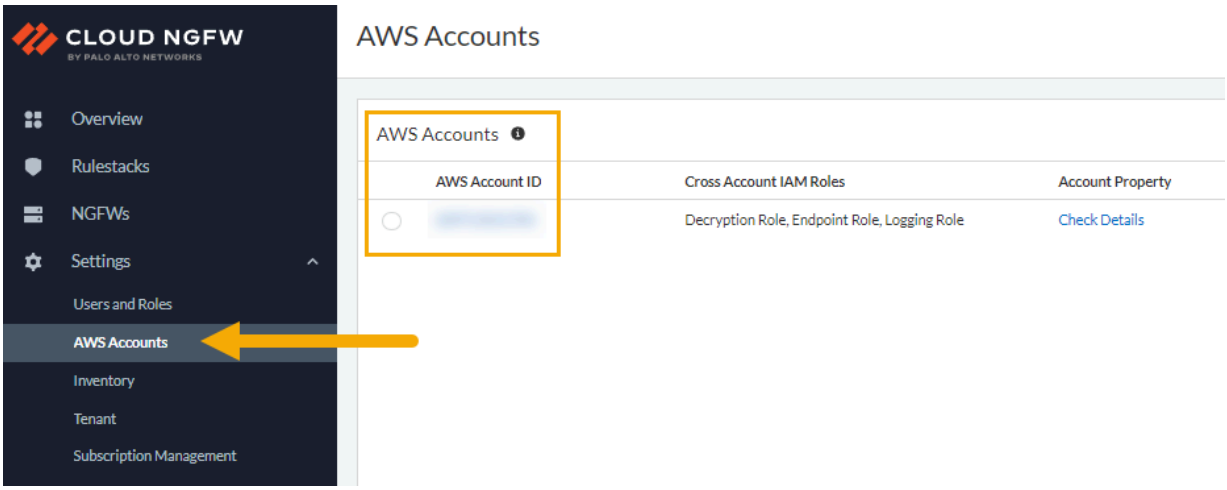
Pour plus d’informations, consultez Annuler votre abonnement.

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.

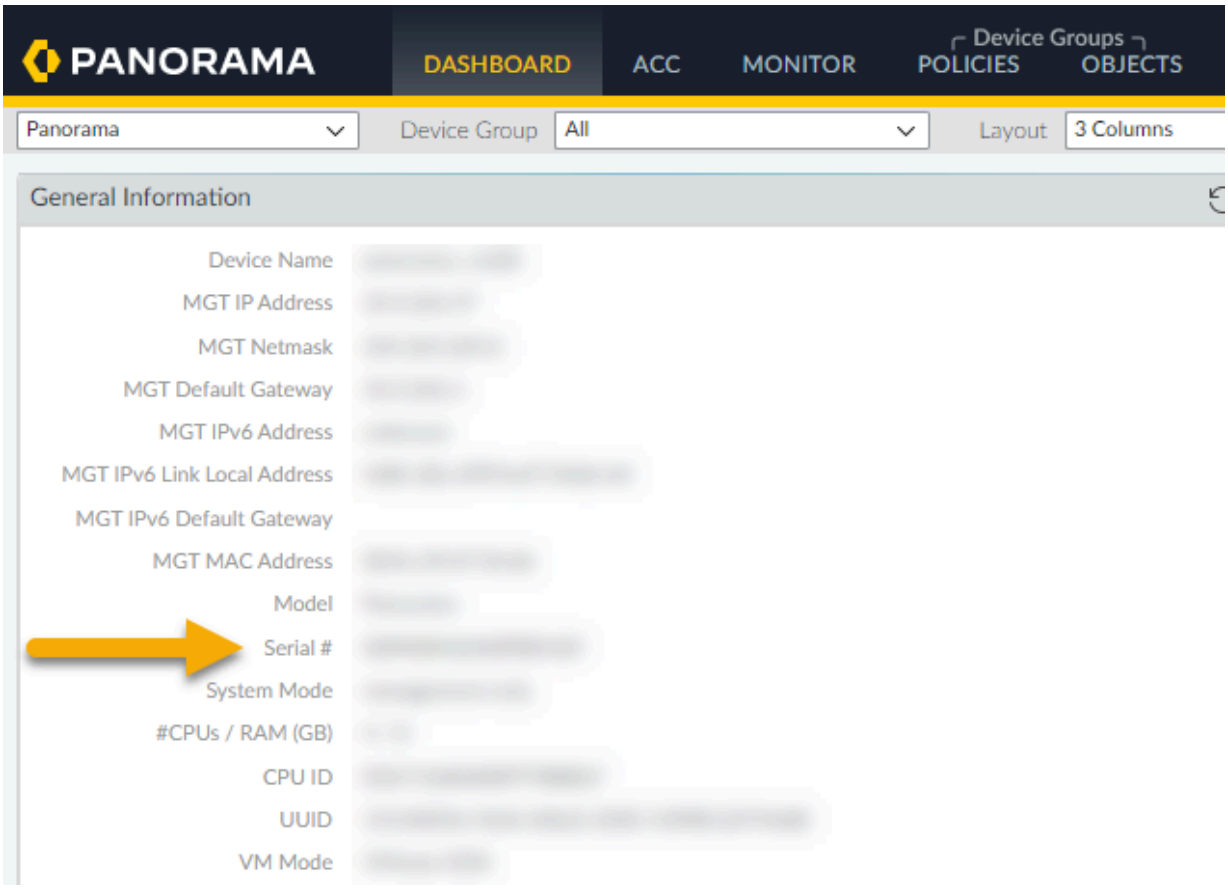
Pour créer une demande de support à l’aide de la console Cloud NGFW :

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

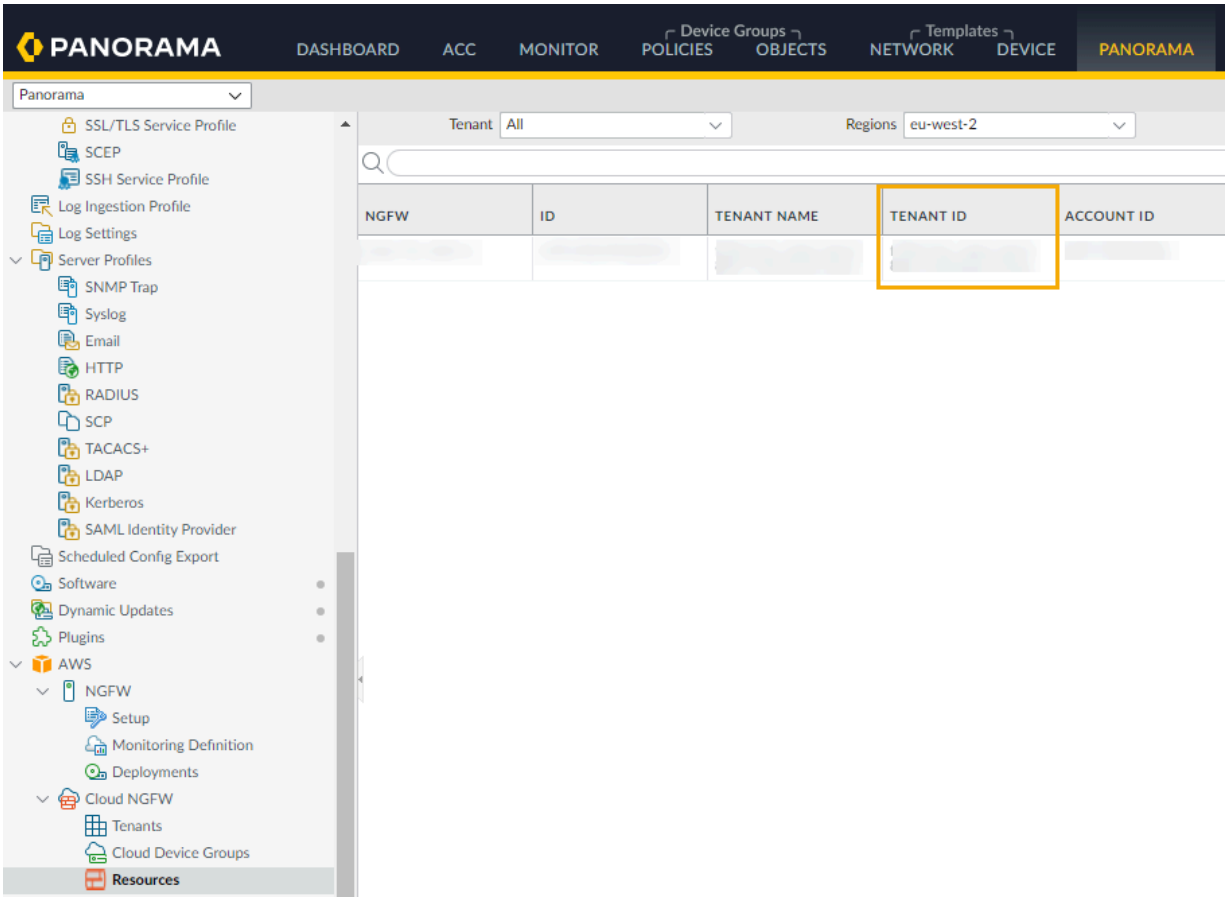


STEP 2 | Si nécessaire, utilisez la console Panorama pour déterminer des informations supplémentaires pour le dossier de support, telles que l'ID du locataire ou le numéro de série de Panorama.

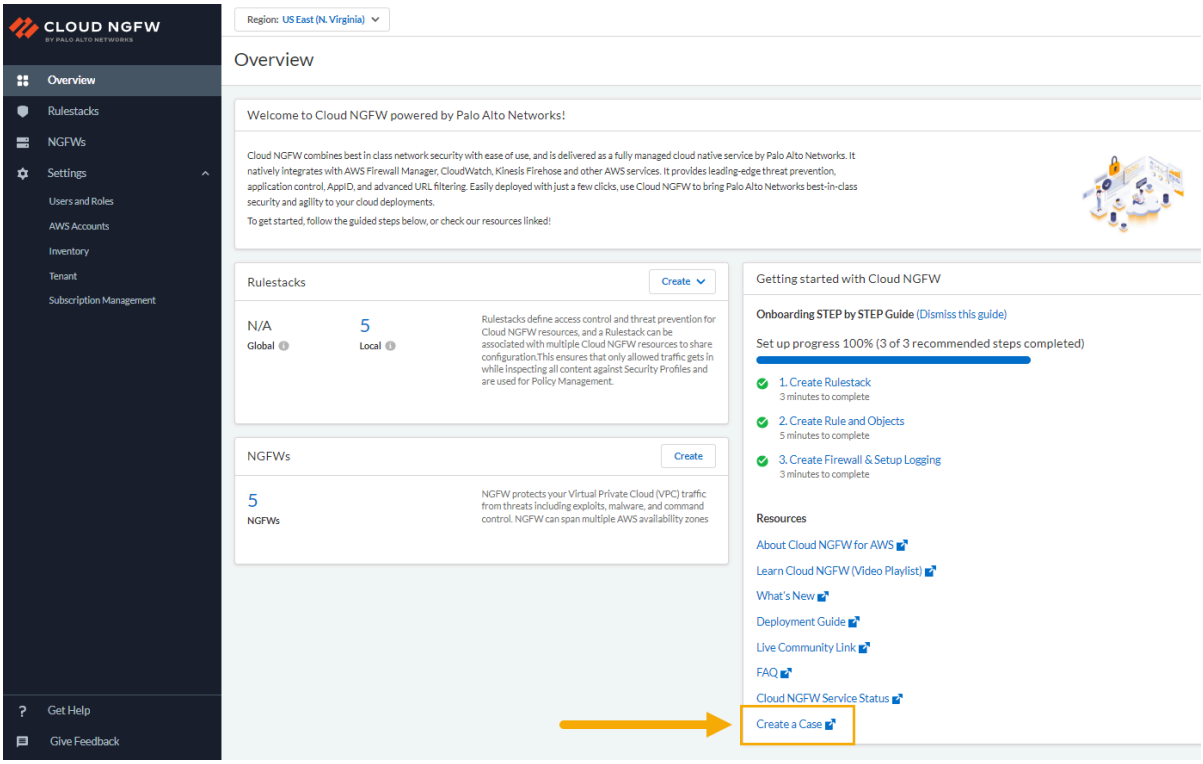
Recherchez le **Panorama serial number (numéro de série Panorama)** à l'aide du **Dashboard (Tableau de bord)** :



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)**.



Associer un Panorama lié à la ressource Cloud NGFW

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

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

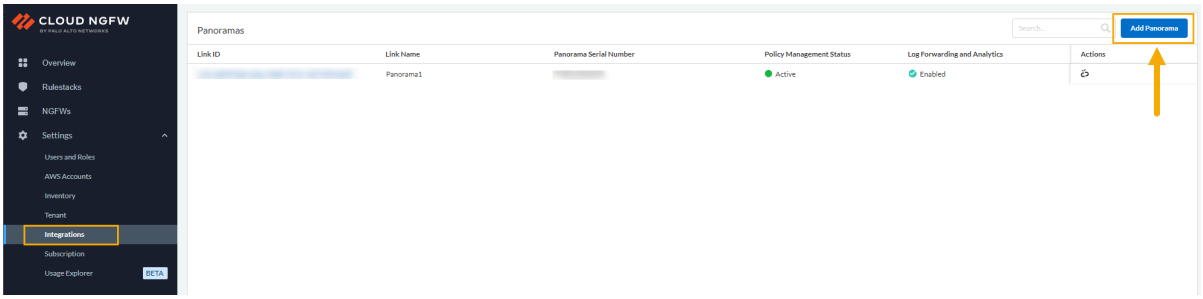
Pour établir des liaisons entre plusieurs Panorama au même locataire Cloud NGFW :

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.

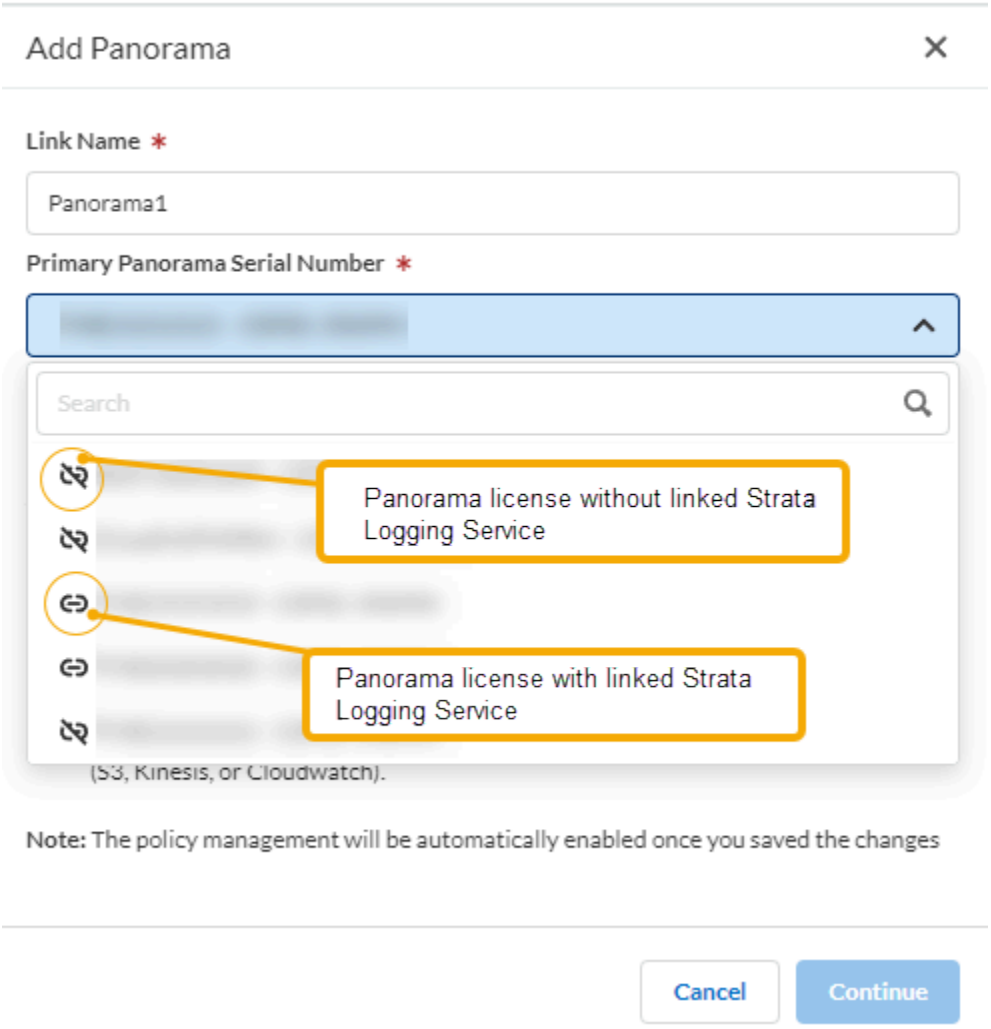
STEP 3 | Utilisez la page **Integrations (Intégrations)** pour ajouter un Panorama supplémentaire. Cliquez sur **Add Panorama (Ajouter un Panorama)**.



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

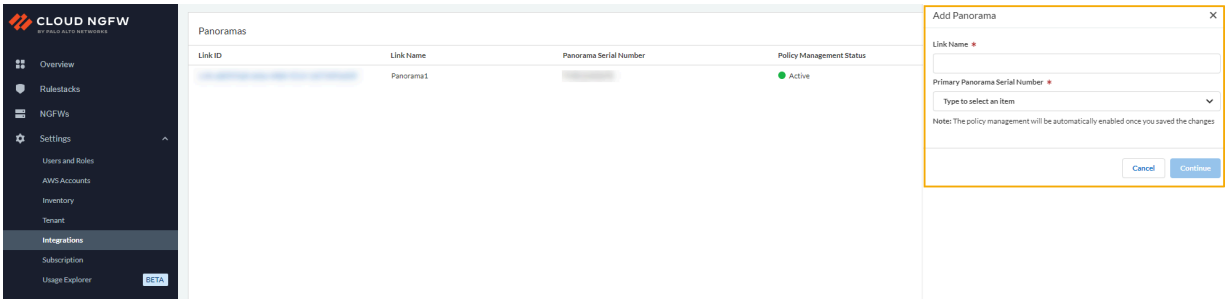
Secondary Panorama Serial Number (Numéro de série du Panorama secondaire) dans la liste déroulante.

Cet écran affiche deux icônes différentes décrivant l'état de la licence Panorama : un Panorama lié au service de journalisation Strata et un Panorama non lié au service de journalisation Strata. Ces icônes sont illustrées dans l'image ci-dessous :



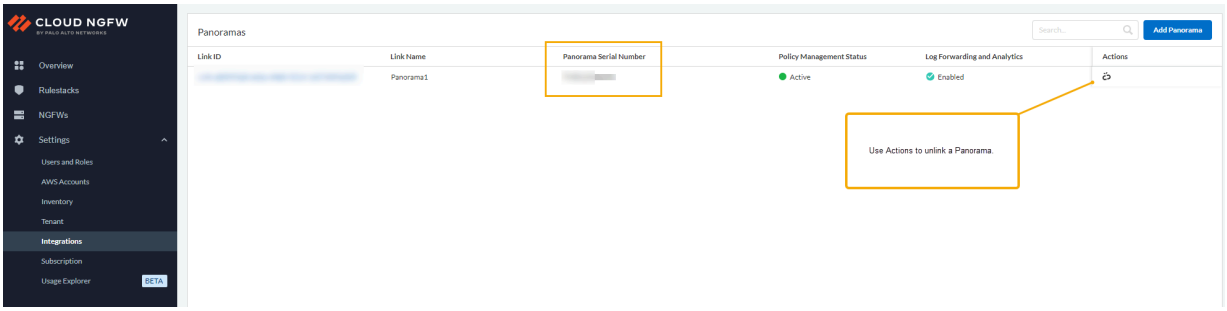
Si vous sélectionnez un numéro de série Panorama qui n'est pas lié au service de journalisation Strata, vous devez spécifier une option : soit vous annulez le processus de liaison, auquel cas vous acceptez

d’acquérir une licence de service de journalisation Strata 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 au service de journalisation Strata, vous devez sélectionner **Confirm (Confirmer)** pour 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.

Dissocier Cloud NGFW de Panorama

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

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 en savoir plus, consultez les sections Supprimer un groupe d’appareils cloud et Dissocier un groupe d’appareils cloud d’une ressource.

Pour dissocier un appareil virtuel Panorama d’une ressource Cloud NGFW :

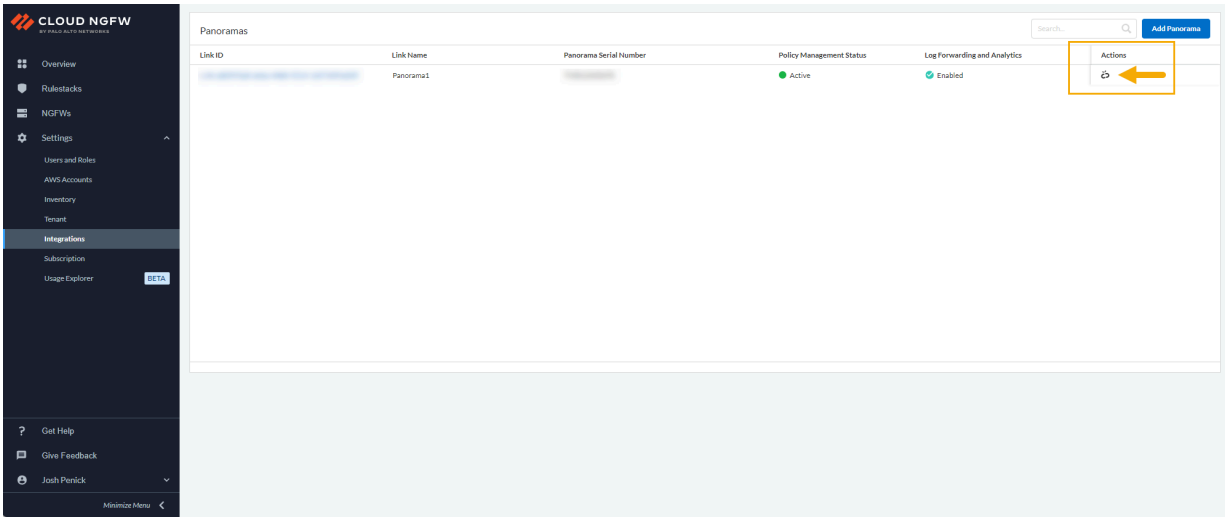
STEP 1 | Choisissez la région, par exemple, **us-east-1**, dans la page du pare-feu ou des rulestacks.

STEP 2 | Dans la console Cloud NGFW, sélectionnez **Integrations (Intégrations)**.

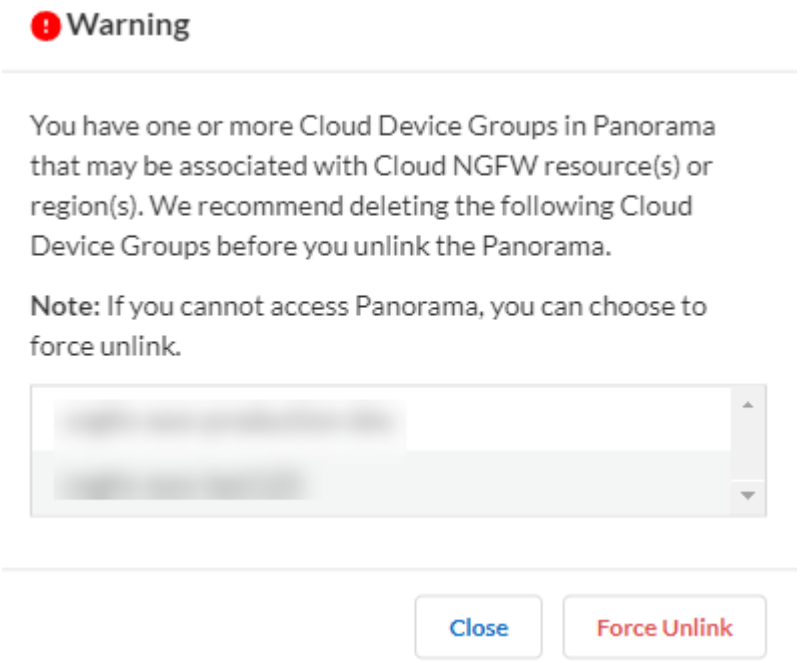
STEP 3 | Sur la page **Integrations (Intégrations)**, localisez la section **Actions**. Un Panorama précédemment lié apparaît grisé.

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
```

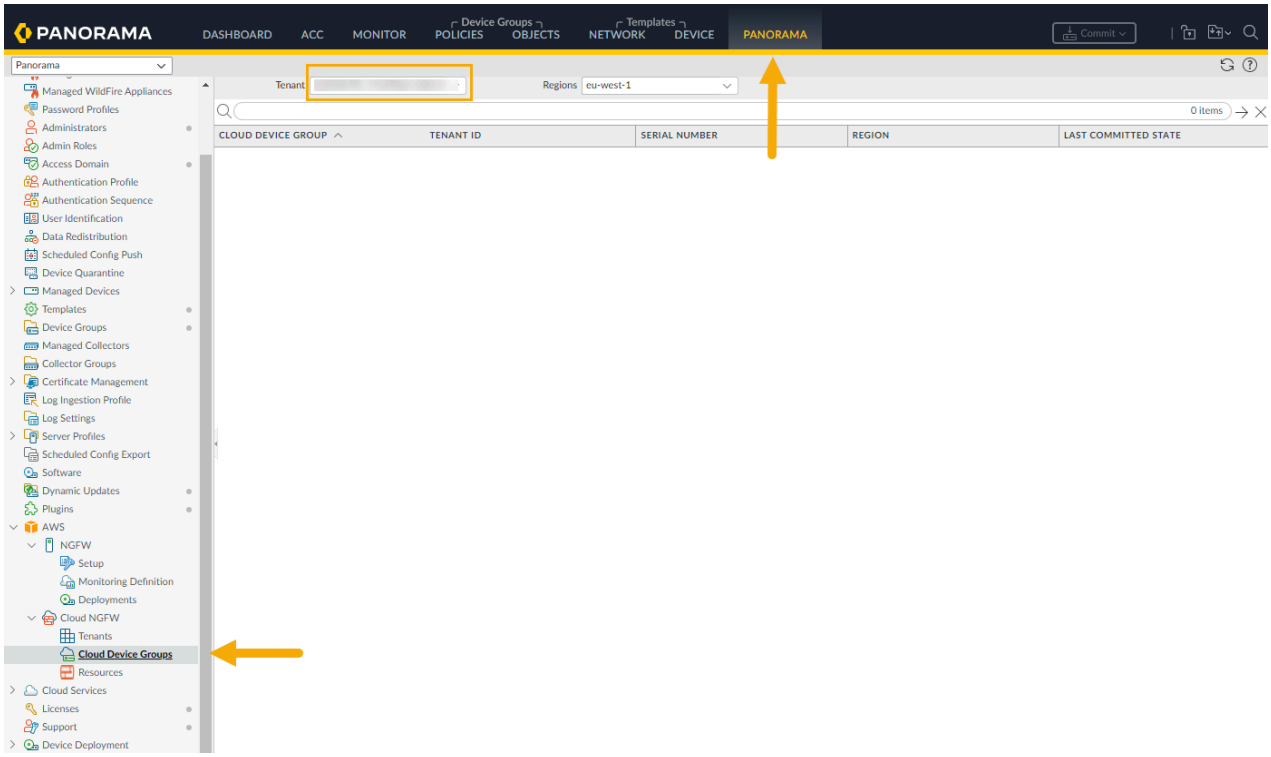

Utiliser Panorama pour la gestion des politiques Cloud NGFW

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

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.

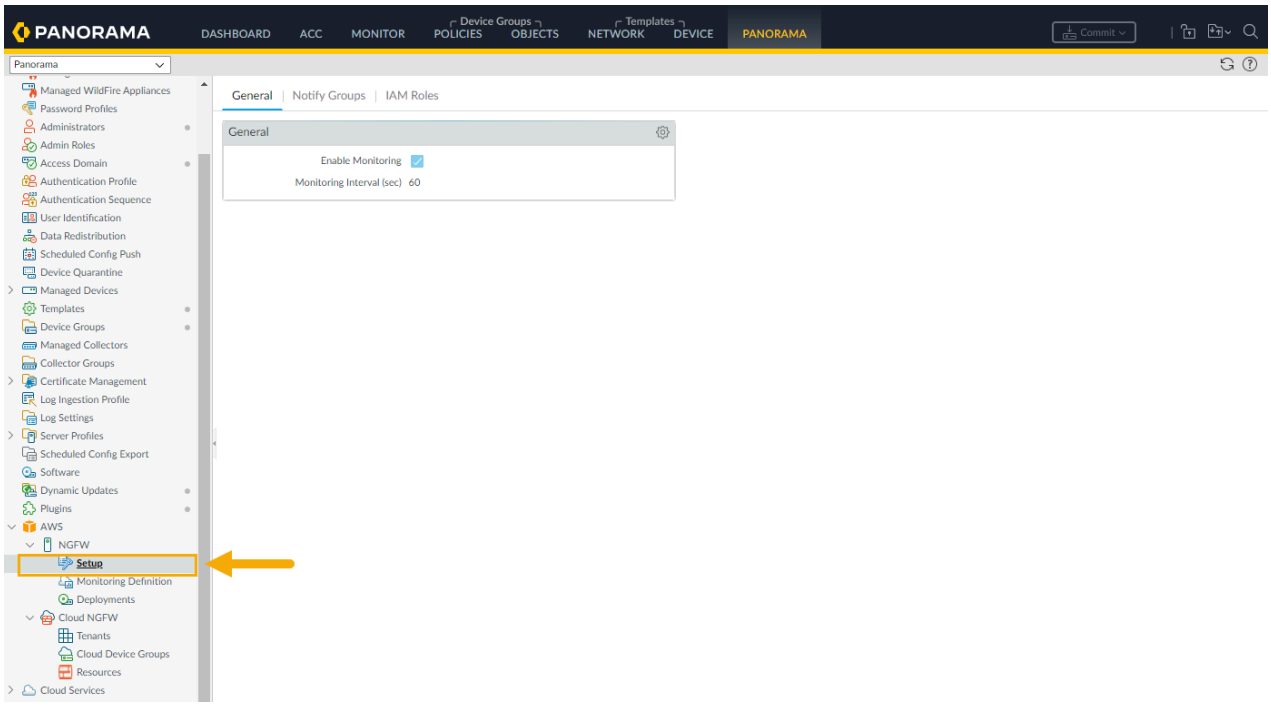
Lorsque vous utilisez la console Panorama pour configurer le Cloud NGFW, le navigateur met en cache les informations locales, telles que le groupe d’appareils Cloud, la pile de modèles et la région, de sorte que lorsque vous basculez entre les tâches Panorama, les informations Cloud NGFW en cache sont 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.

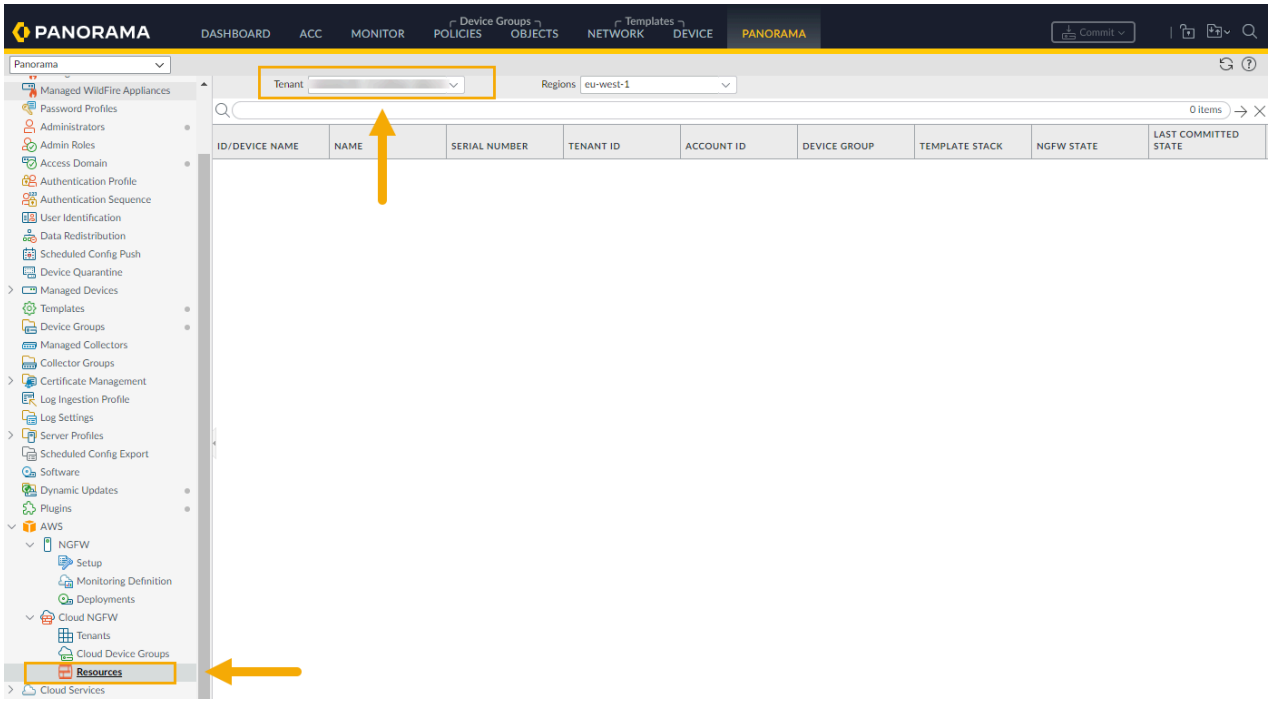


Lorsque vous accédez à une autre zone de la console Panorama, puis revenez à **Cloud NGFW > Groupes d’appareils Cloud**, la console affiche le locataire unique que vous avez précédemment sélectionné. Par

exemple, après avoir affiché les groupes d'appareils cloud pour un locataire, sélectionnez **AWS > Setup (Configuration)**.



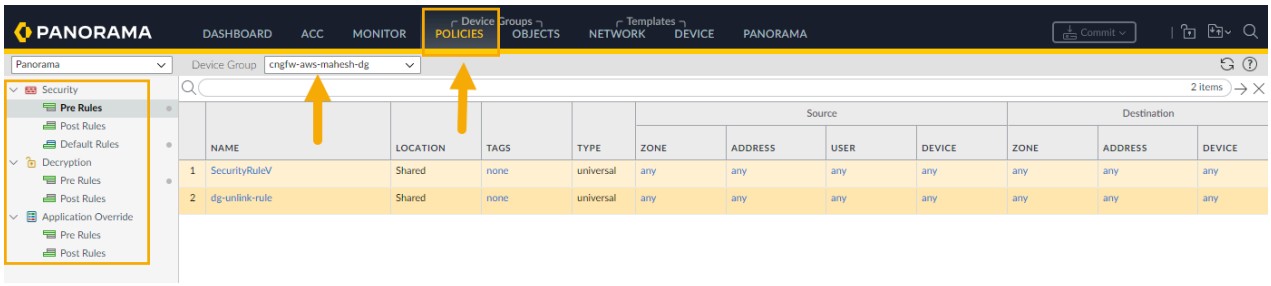
Lorsque vous revenez à l'écran **Cloud NGFW > Ressources**, la console Panorama se souvient du locataire précédemment sélectionné au lieu d'afficher tous les locataires associés à la ressource Cloud NGFW.



Actualisez le navigateur pour effectuer une mise à jour dynamique de l’affichage.

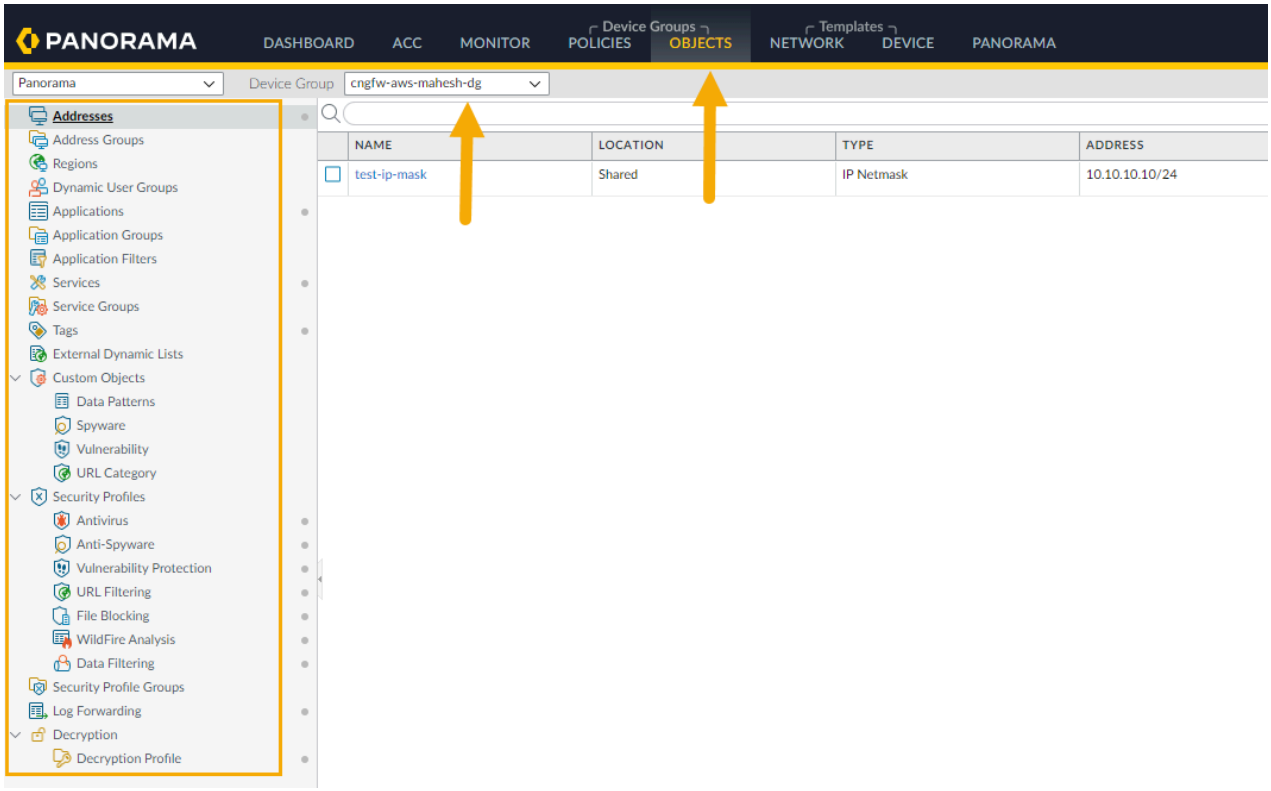
L’intégration Panorama affiche uniquement les options de configuration disponibles pour la ressource Cloud NGFW. Par exemple, pour afficher les options de politique disponibles pour la ressource Cloud

NGFW, sélectionnez **Policies (Politiques)**. La console Panorama n'affiche que les politiques disponibles pour le groupe d'appareils cloud du Cloud NGFW.

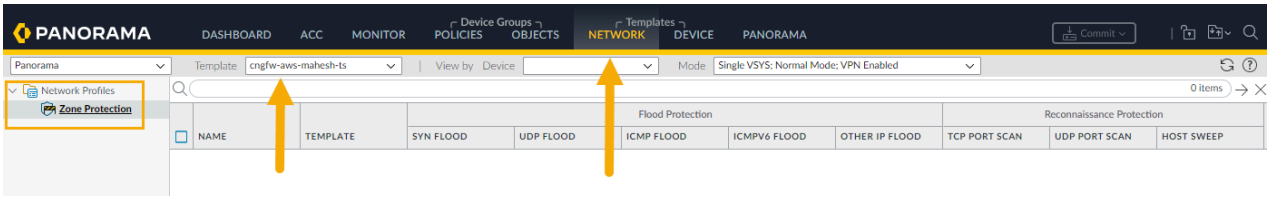


Le nom du groupe d'appareils est doté du préfixe `cngfw-aws`.

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.

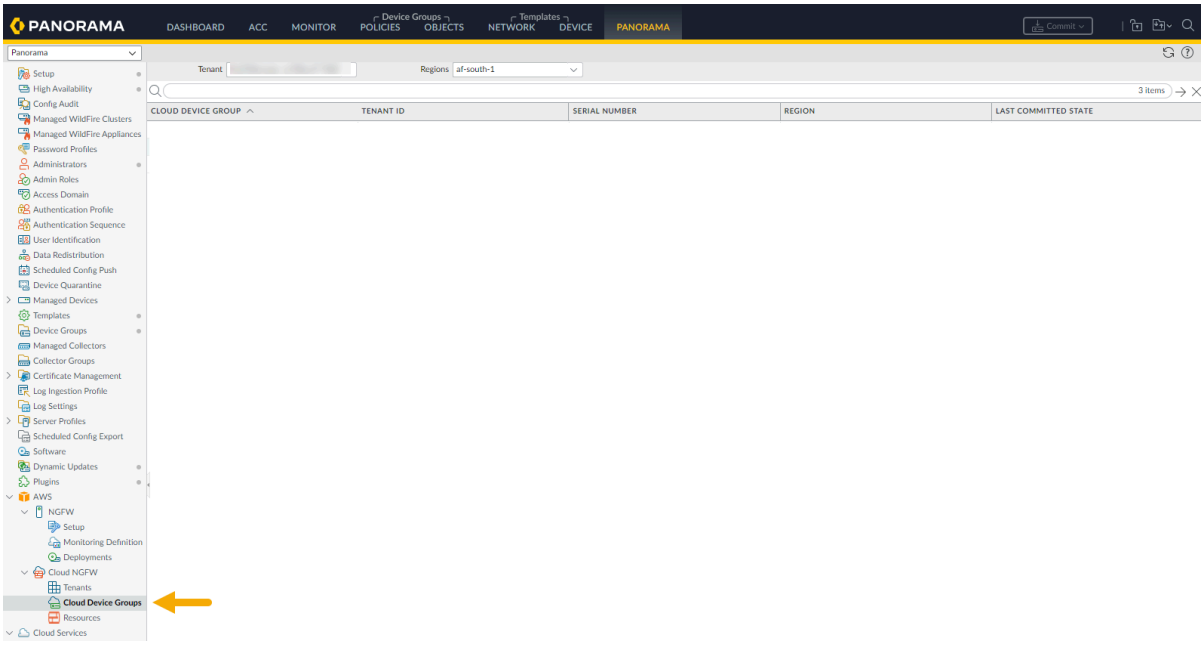
En utilisant des groupes de périphériques, vous pouvez configurer les règles de stratégie et les objets auxquels ils font référence. Vous pouvez organiser un groupe d'appareils hiérarchisé, avec des règles communes et des objets en haut, et des règles spécifiques au groupe d'appareils et des objets à 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 Gérer les groupes d'appareils.

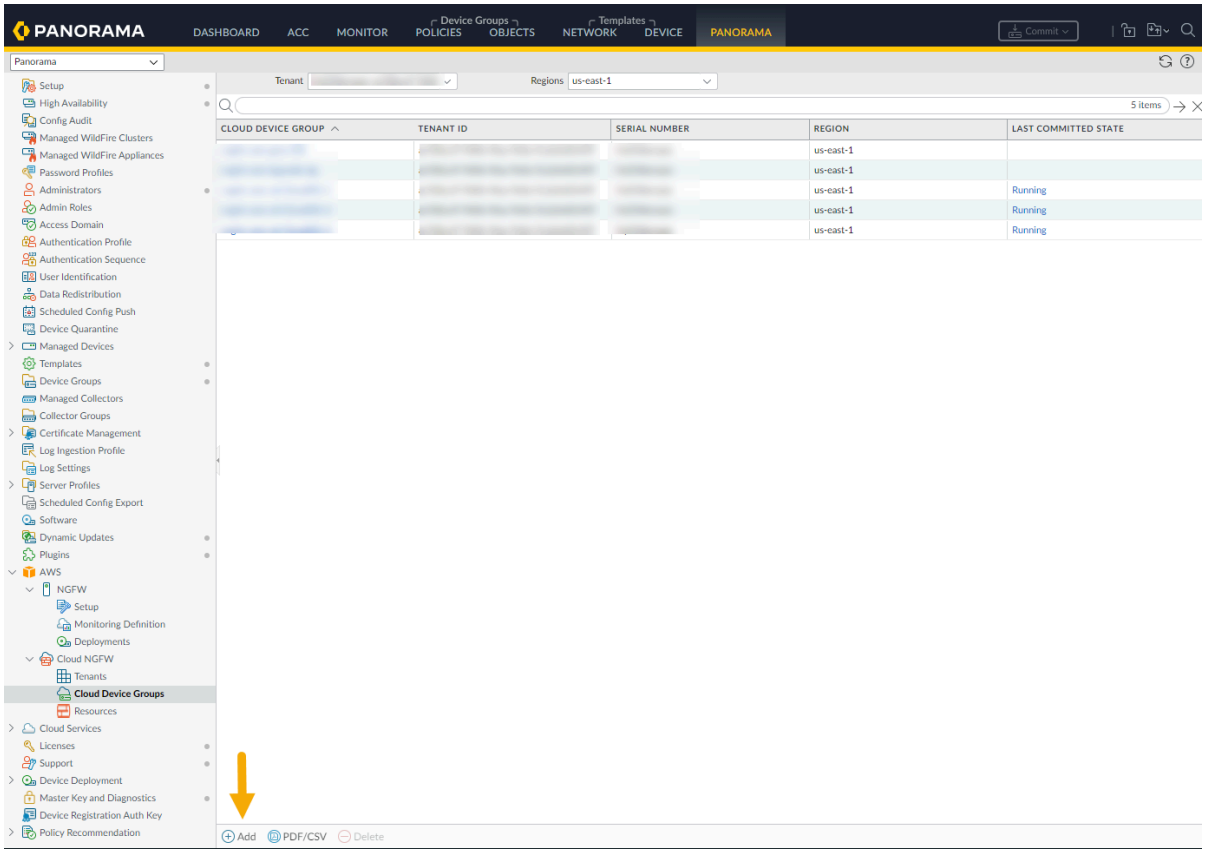
Pour ajouter un groupe d'appareils cloud à l'aide de la console Panorama :

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

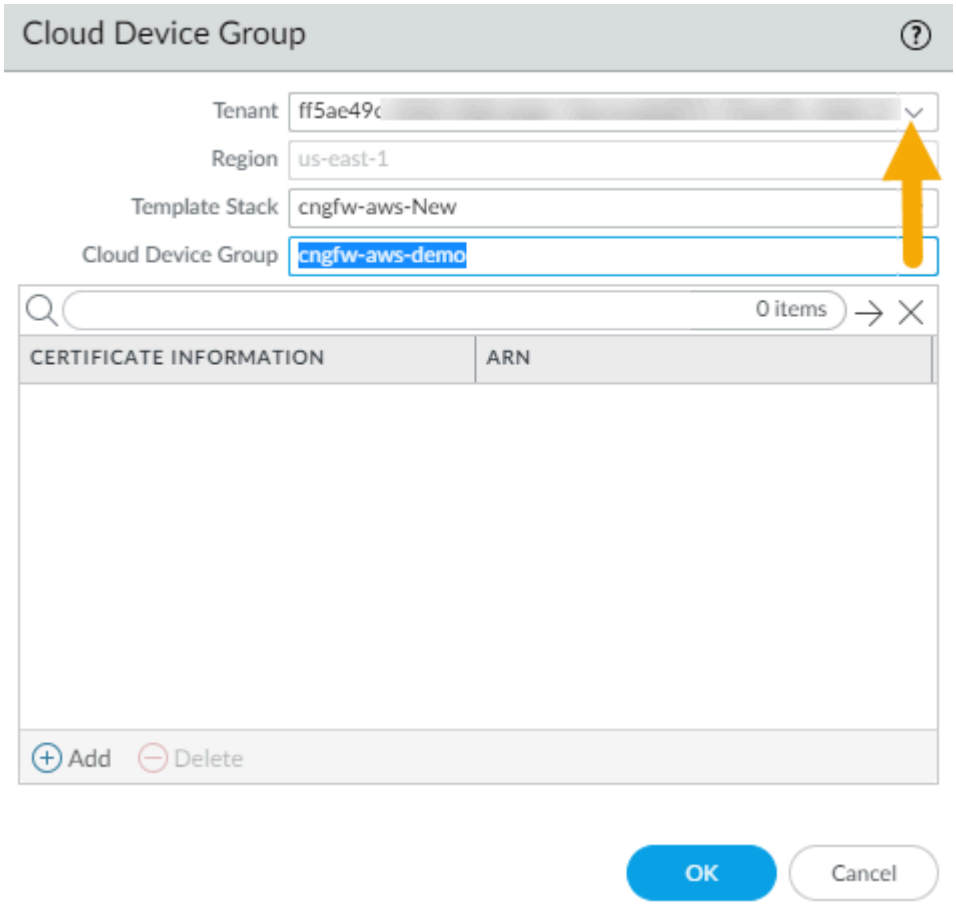
première fois. Les groupes d’appareils Cloud précédemment créés apparaissent s’ils ont été établis pour la ressource Cloud NGFW à l’aide d’AWS.



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



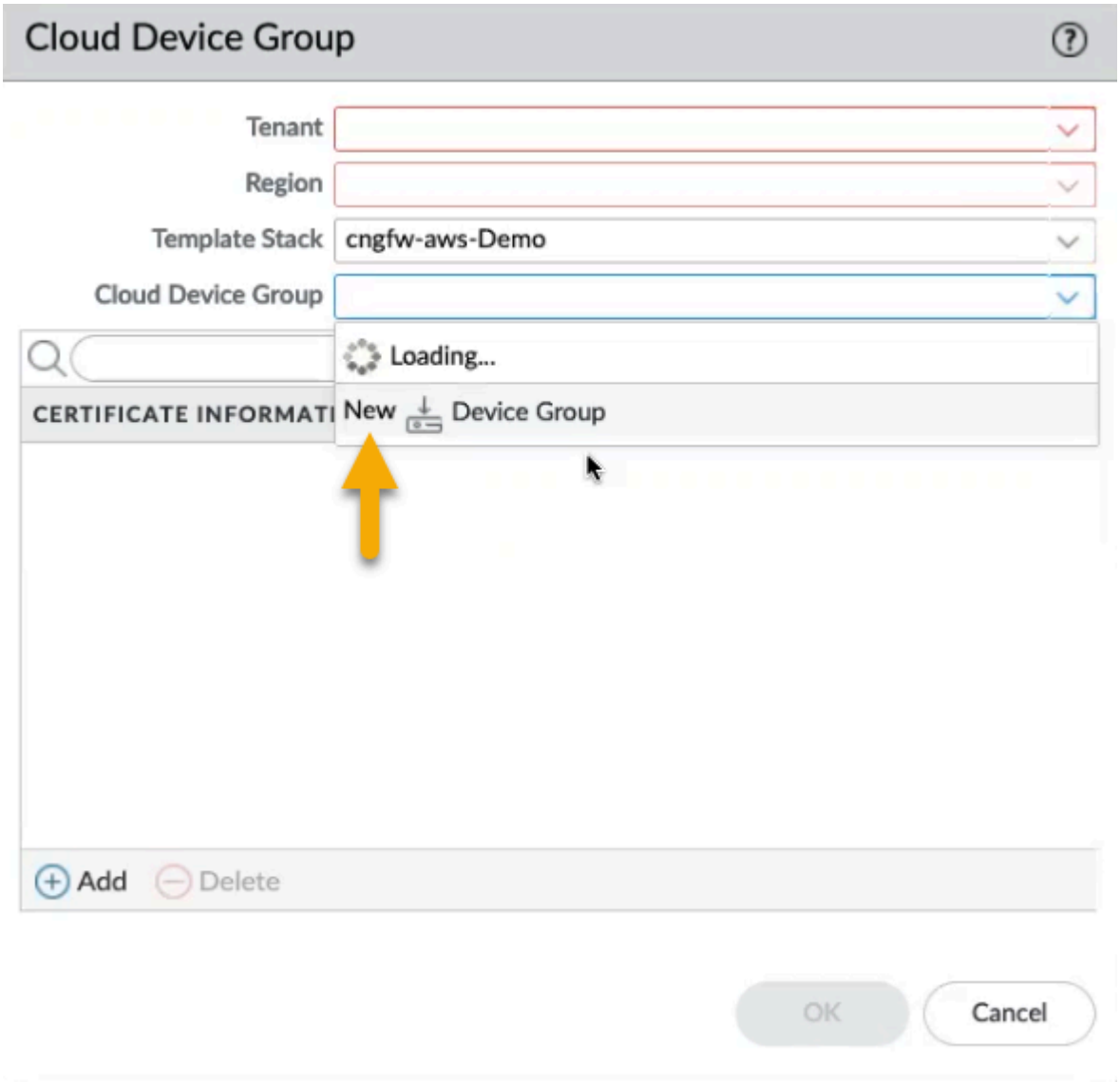
STEP 3 | Dans l’écran **Cloud Device Group (Groupe d’appareils Cloud)**, utilisez le menu déroulant pour sélectionner le **Tenant (Locataire)** que vous souhaitez utiliser.



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

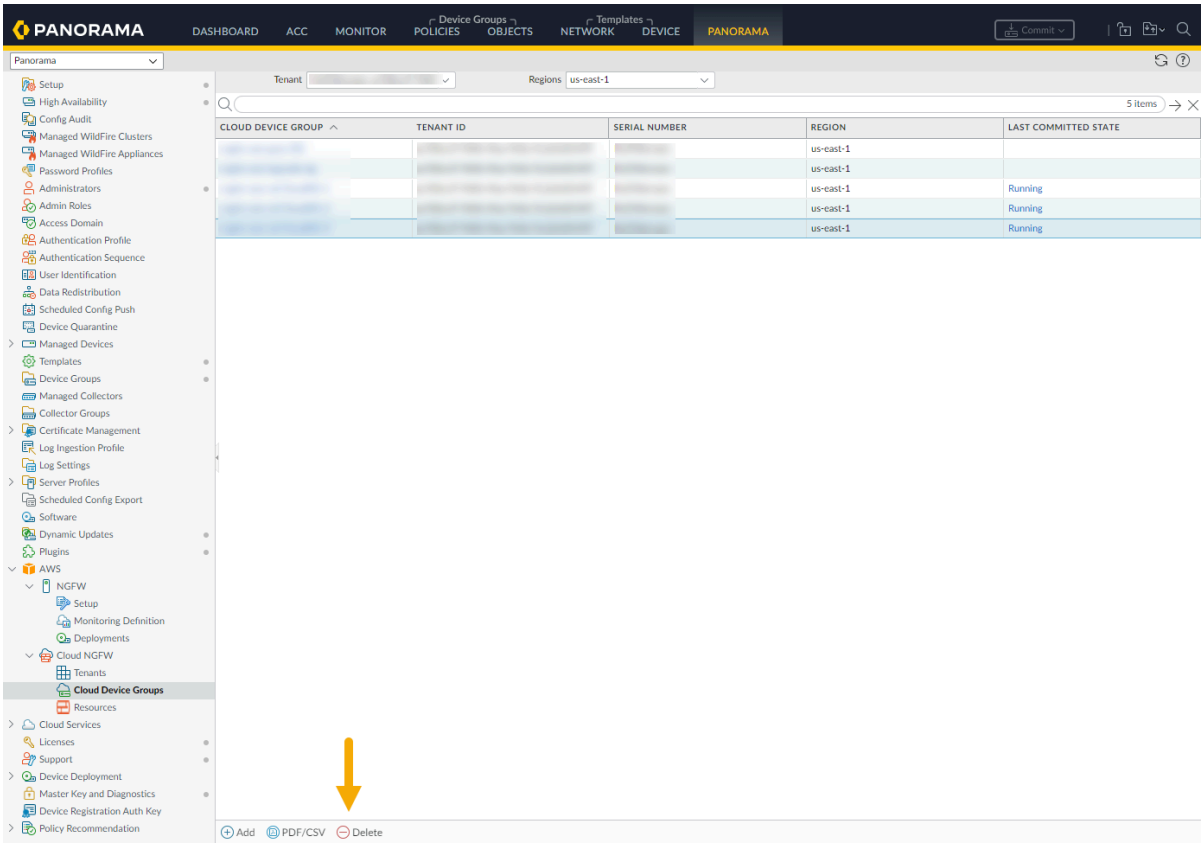
Utilisez la console Panorama pour supprimer un groupe d’appareils Cloud. Vous ne pouvez supprimer un groupe d’appareils Cloud que s’il n’est pas associé à un pare-feu.

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.

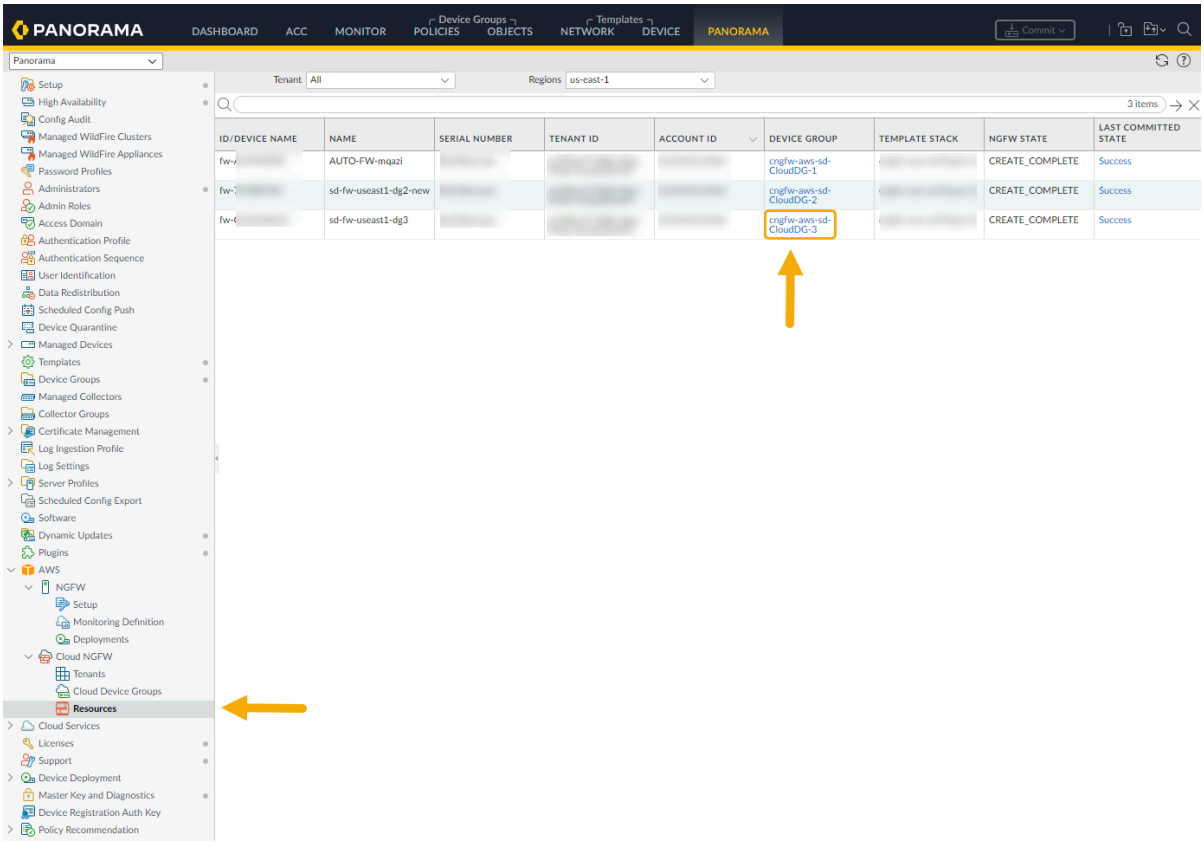
Associer un groupe d’appareils Cloud à une ressource

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

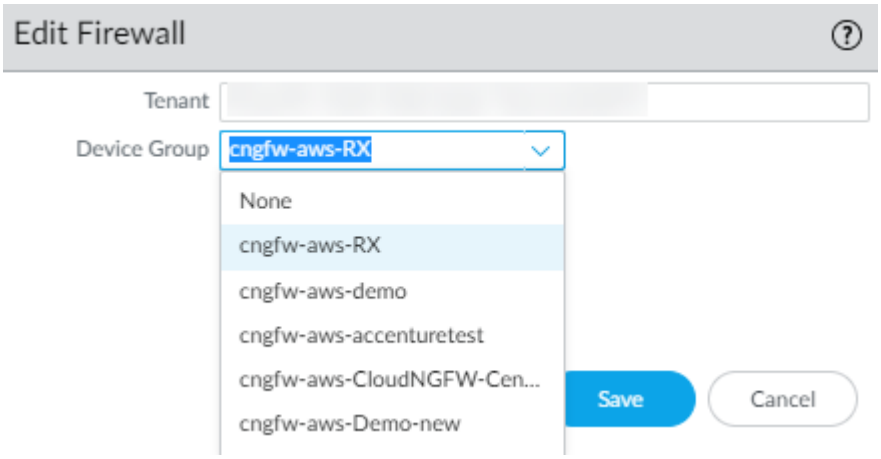
Pour associer un groupe d’appareils cloud à une ressource Cloud NGFW à l’aide de la console Panorama :

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.

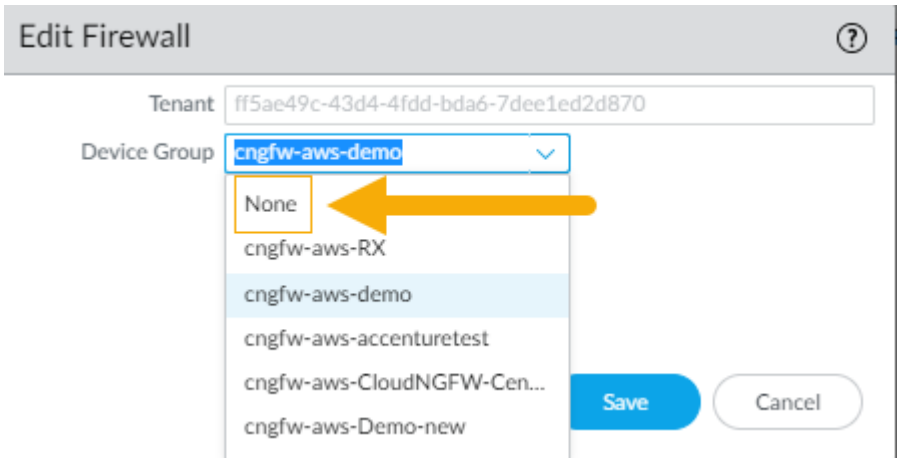
Dissocier un groupe d’appareils Cloud d’une ressource

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

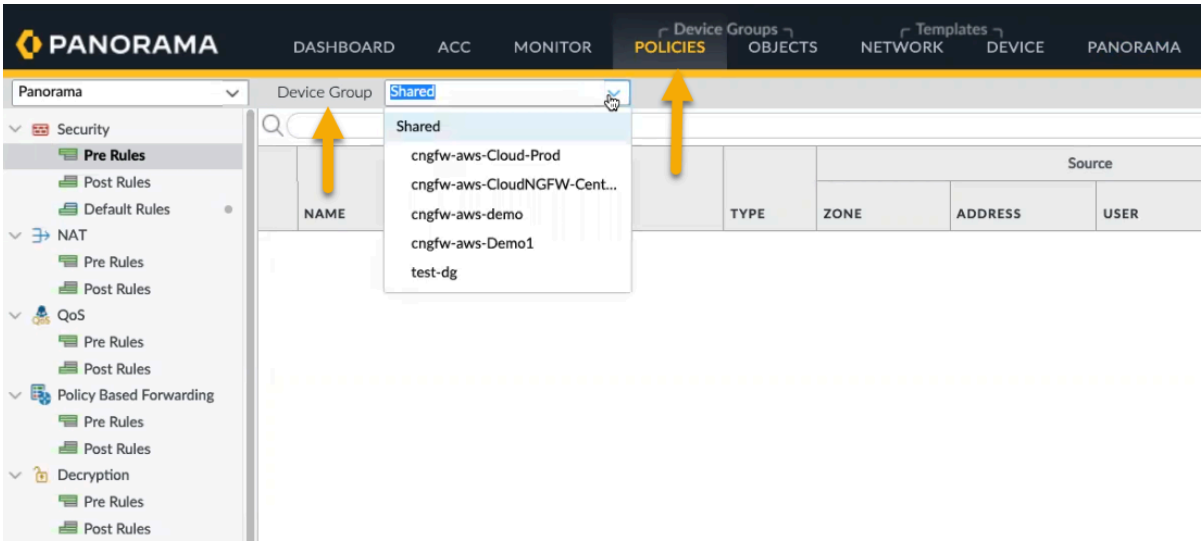
Les groupes d’appareils Cloud sur Panorama vous permettent de gérer les règles de pare-feu de manière centralisée. Vous pouvez créer les politiques sur Panorama en tant que Règles avant ou que Règles après ; les Règles avant et les Règles après vous permettent de créer une approche progressive de la mise en œuvre des politiques. Pour en savoir plus, consultez la section 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 :

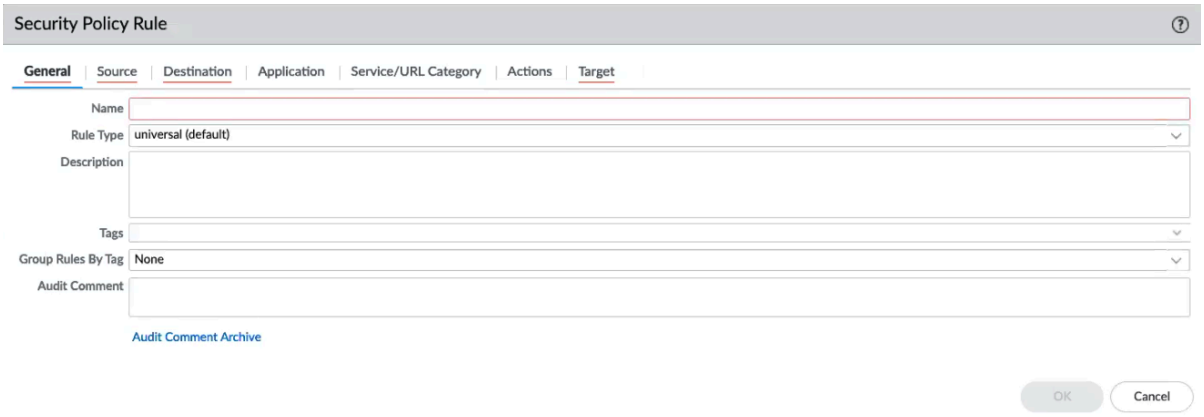
STEP 1 | Sélectionnez **Policies (Politiques)**.

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*.



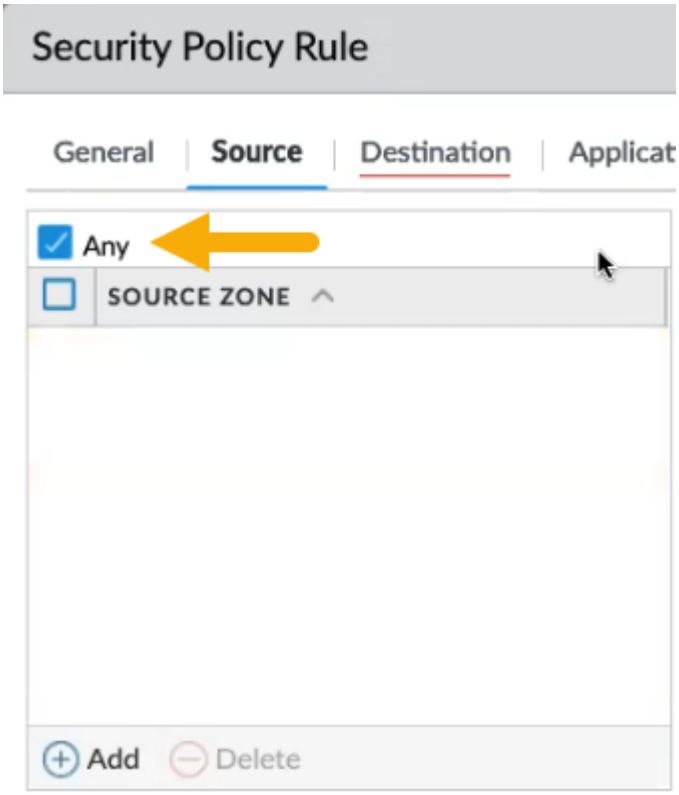
STEP 3 | Dans la partie inférieure gauche de la console, cliquez sur **Add (Ajouter)**.

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

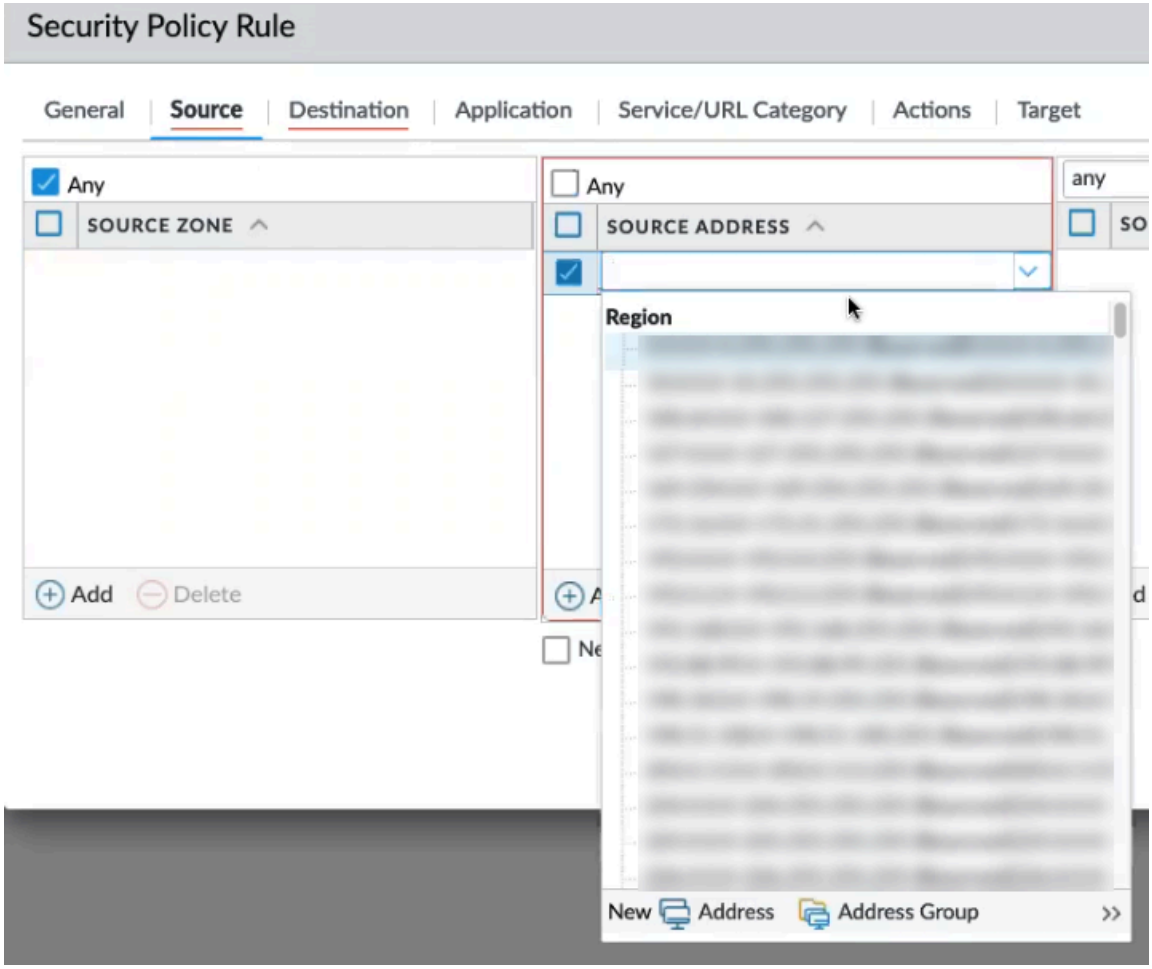


STEP 5 | Dans l’onglet **General (Général)**, saisissez un **nom** pour la politique.

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.

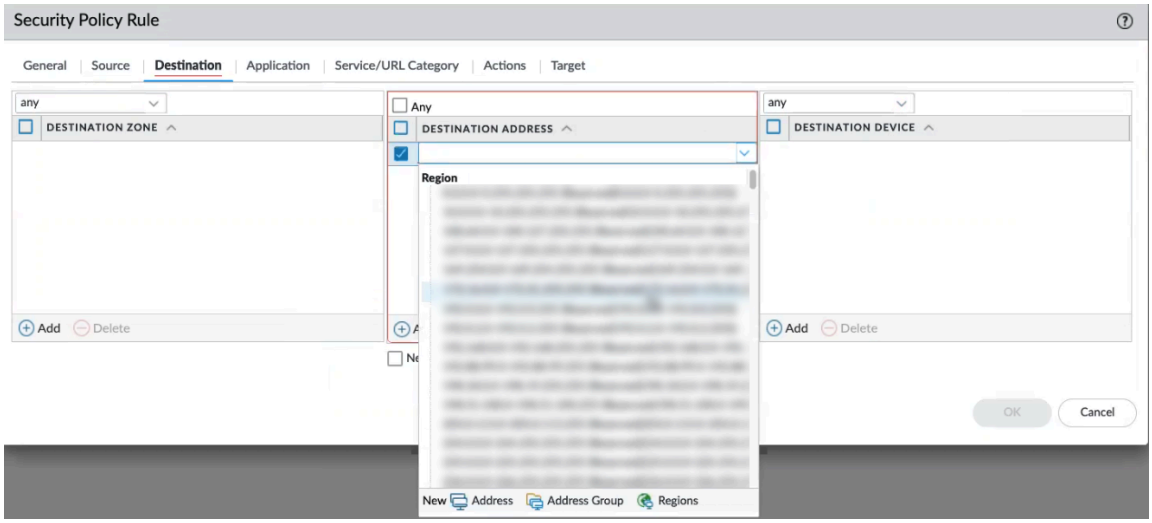


2. Pour la politique**Source User (Utilisateur source)** et **Source Device (Périphérique source)**, cliquez sur **Any (Tout)**. Cloud NGFW ne prend pas en charge la spécification d'utilisateurs ou de périphériques source spécifiques

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 (N'importe laquelle)**. 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.

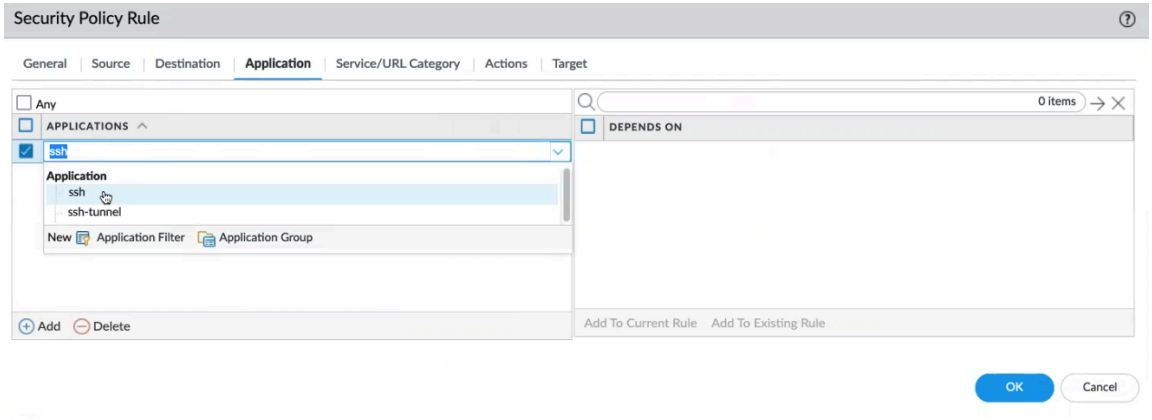
3. Pour le **Destination Device (Périphérique de destination)**, cliquez sur **Any (N'importe lequel)**. Cloud NGFW ne prend pas en charge l'ajout de périphériques de destination individuels.



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

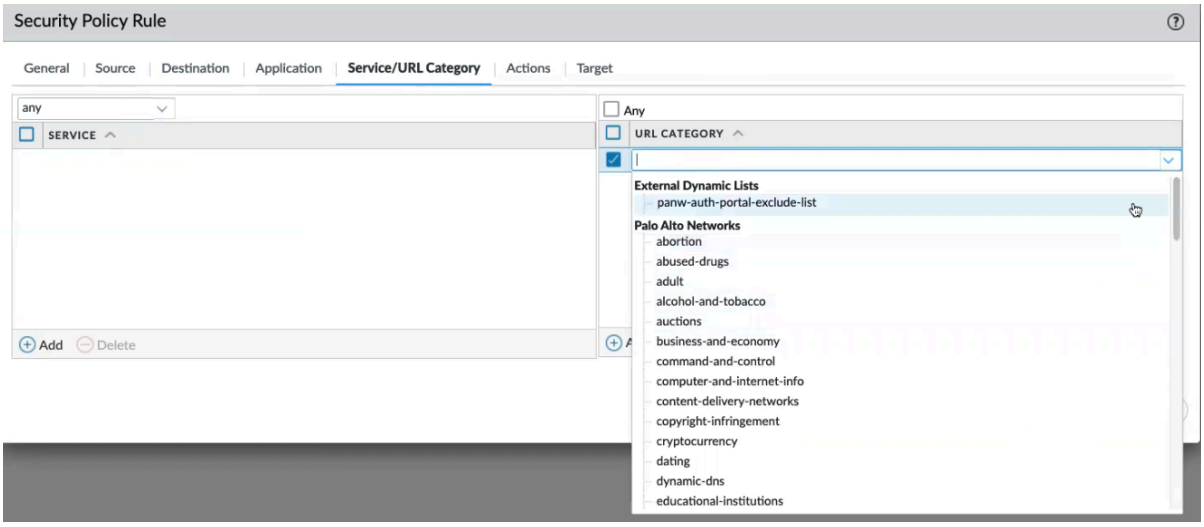
attributs d’une application existante. Les applications propres à l’entreprise sont définies dans **ObjectsApplications (Applications d’objets)**.

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.



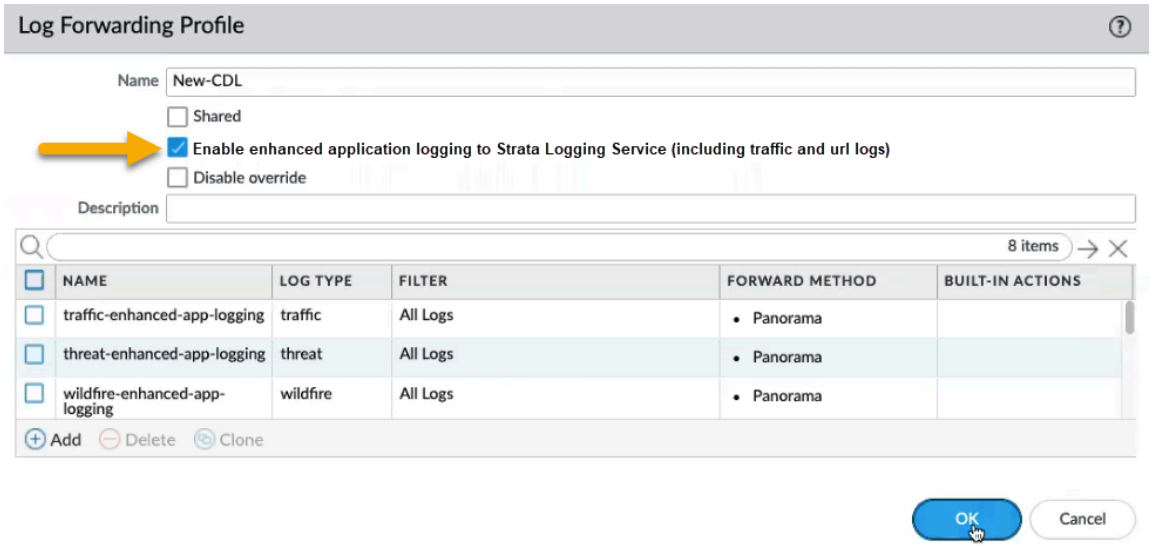
STEP 10 | Configurez une politique **Actions** pour déterminer l'action effectuée en fonction du trafic correspondant aux attributs de politique définis.

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 en savoir plus sur l'utilisation des journaux Panorama, consultez la section Journalisation centralisée et génération de rapports et Afficher des journaux.

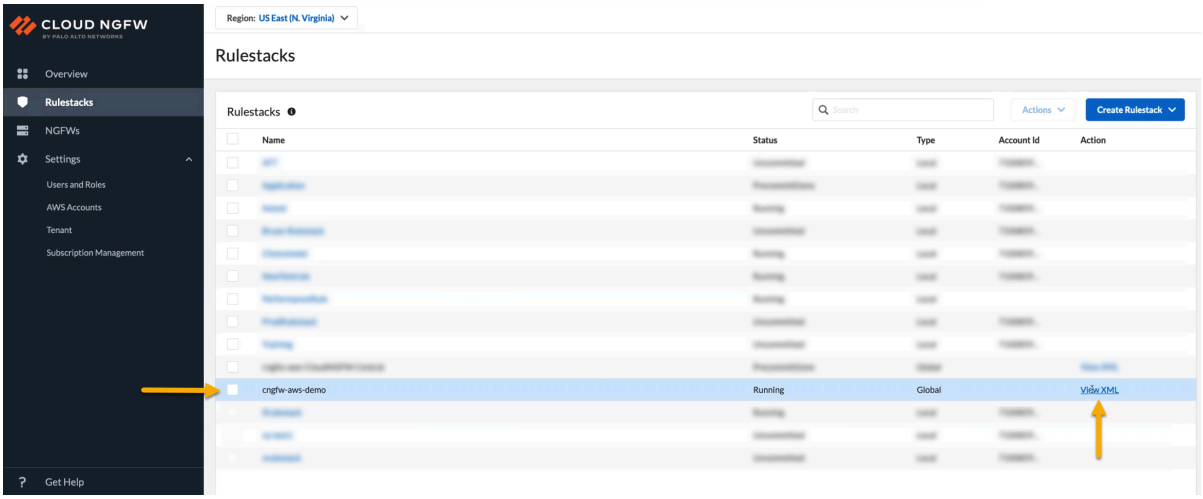
2. Vous pouvez également transférer les journaux au service de journalisation Strata depuis l'écran **Security Policy Rule (Règle de politique de sécurité)**. Dans le champ **Log Setting (Paramètre des journaux)**, sélectionnez la liste déroulante **Log Forwarding (Transfert des journaux)** et cliquez 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**.

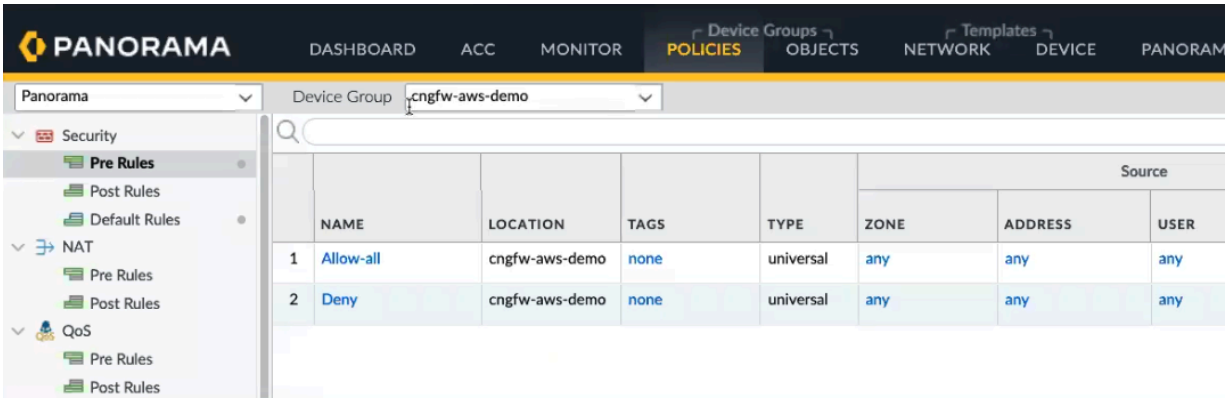


Pour plus d’informations sur le service de journalisation Strata, consultez la section Explore Logs (Explorer les journaux).

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 :

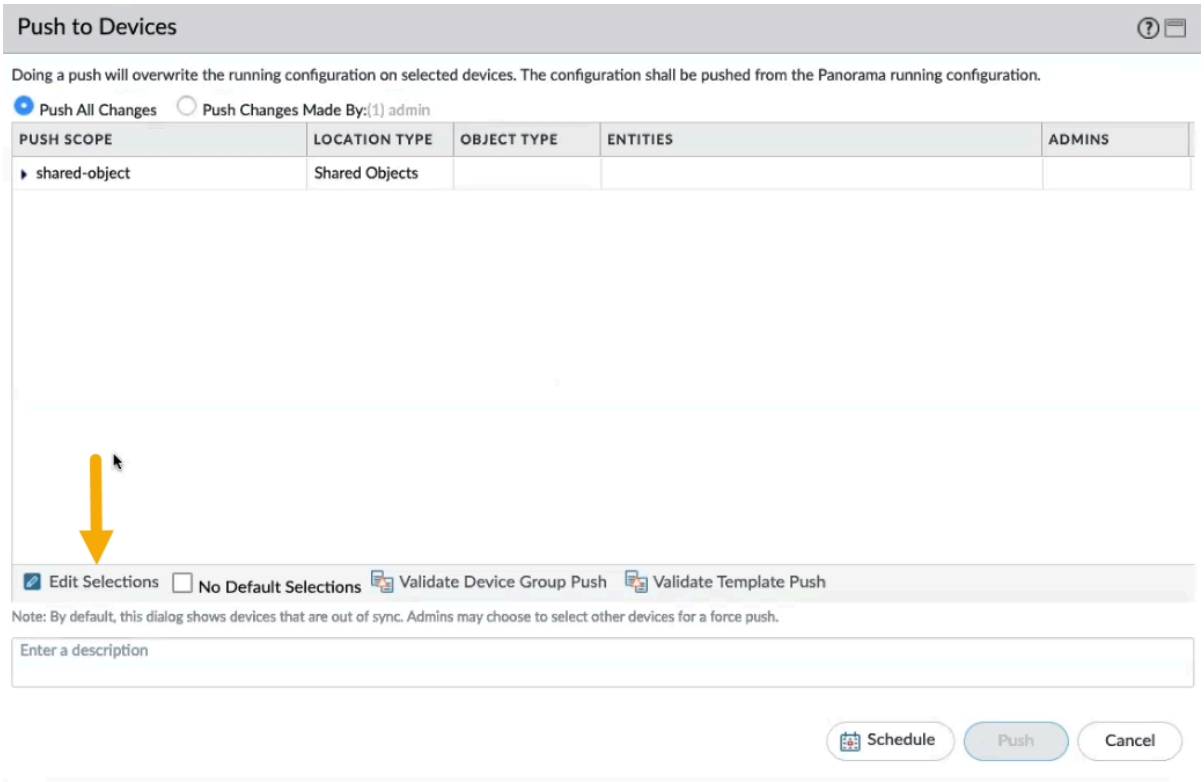


La rulestack est désormais associée aux politiques appliquées au groupe d’appareils Cloud créé dans Panorama :

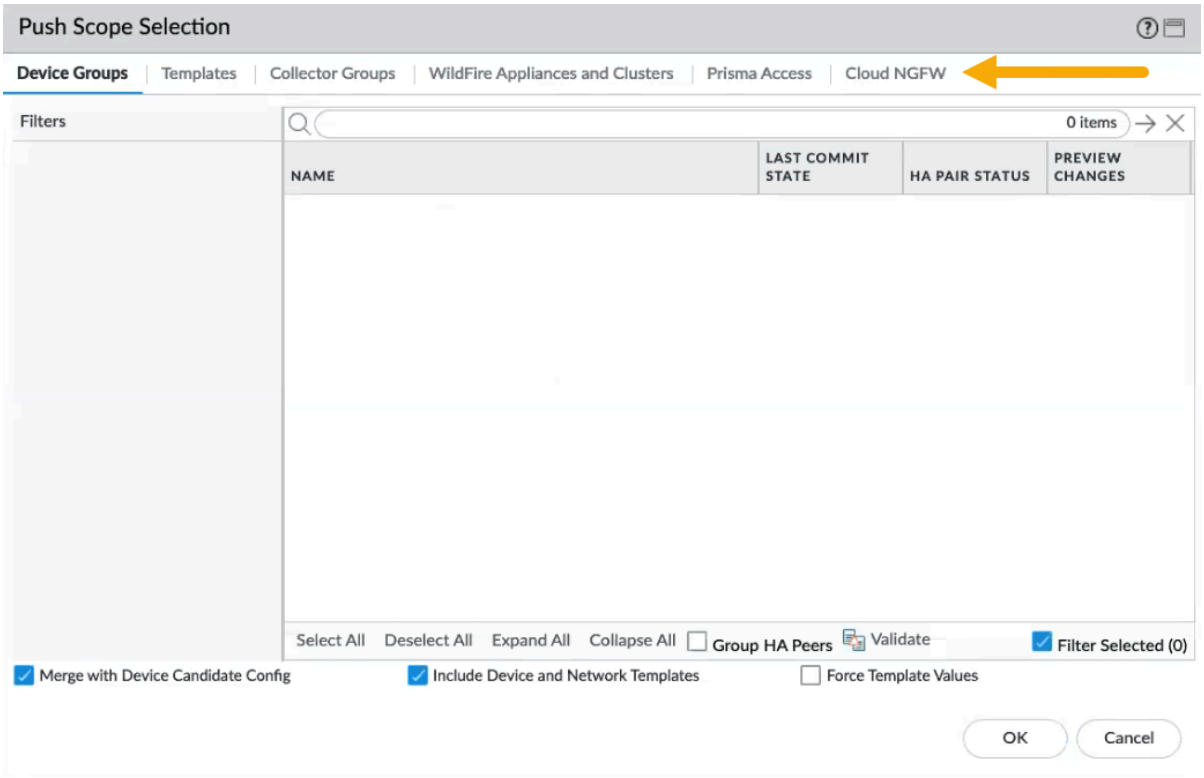


STEP 12 | Après avoir appliqué des politiques au groupe d’appareils cloud pour le locataire Cloud NGFW, transmettez les modifications à la console Panorama.

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

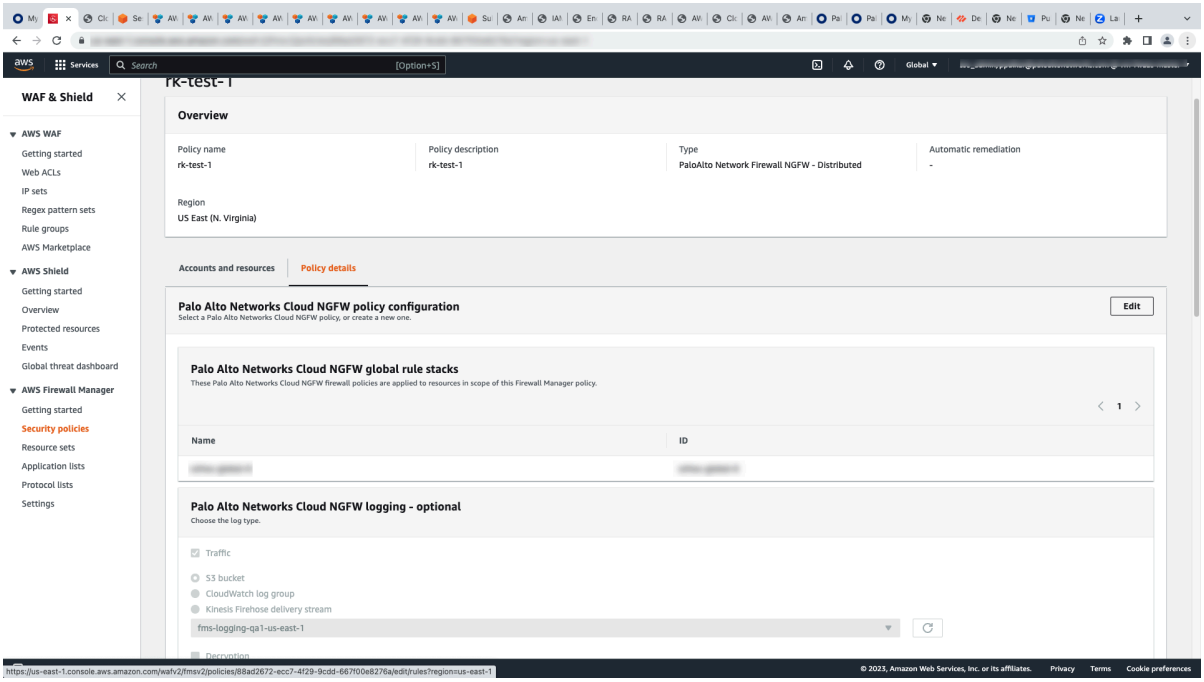
Les informations de cette section sont fournies aux utilisateurs qui utilisent le Service AWS Firewall Manager (FMS) pour configurer les groupes d'appareils transmis depuis Panorama.

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.

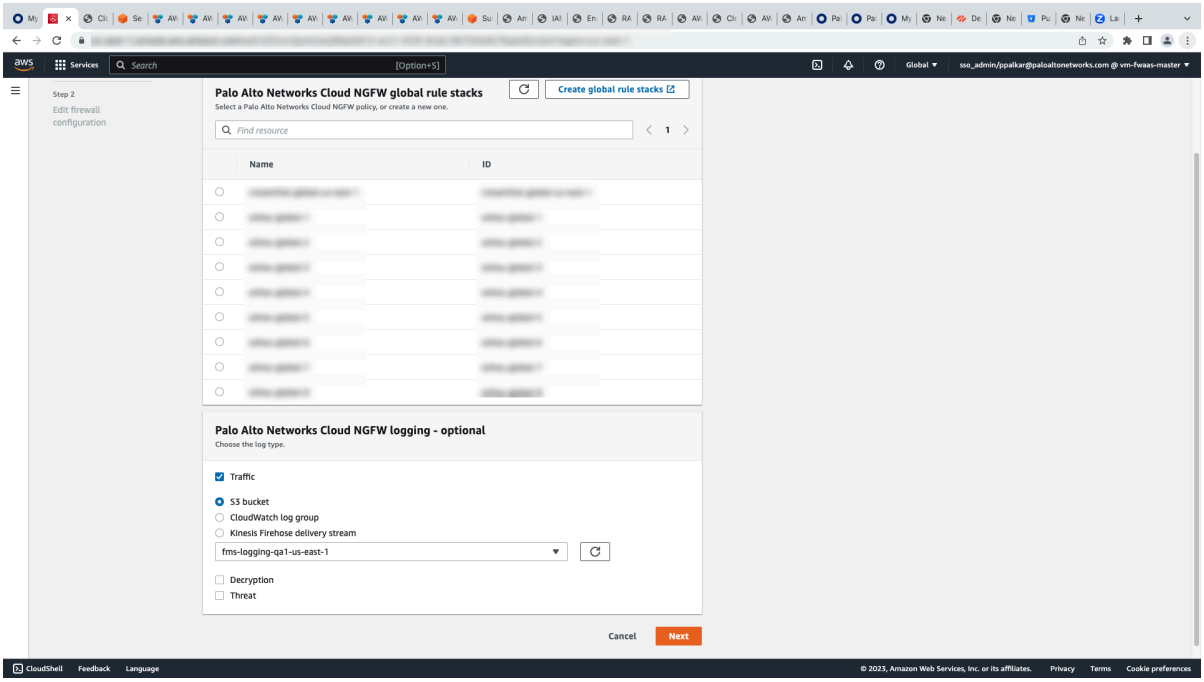
STEP 1 | Reliez un locataire à Panorama.

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.



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)**.

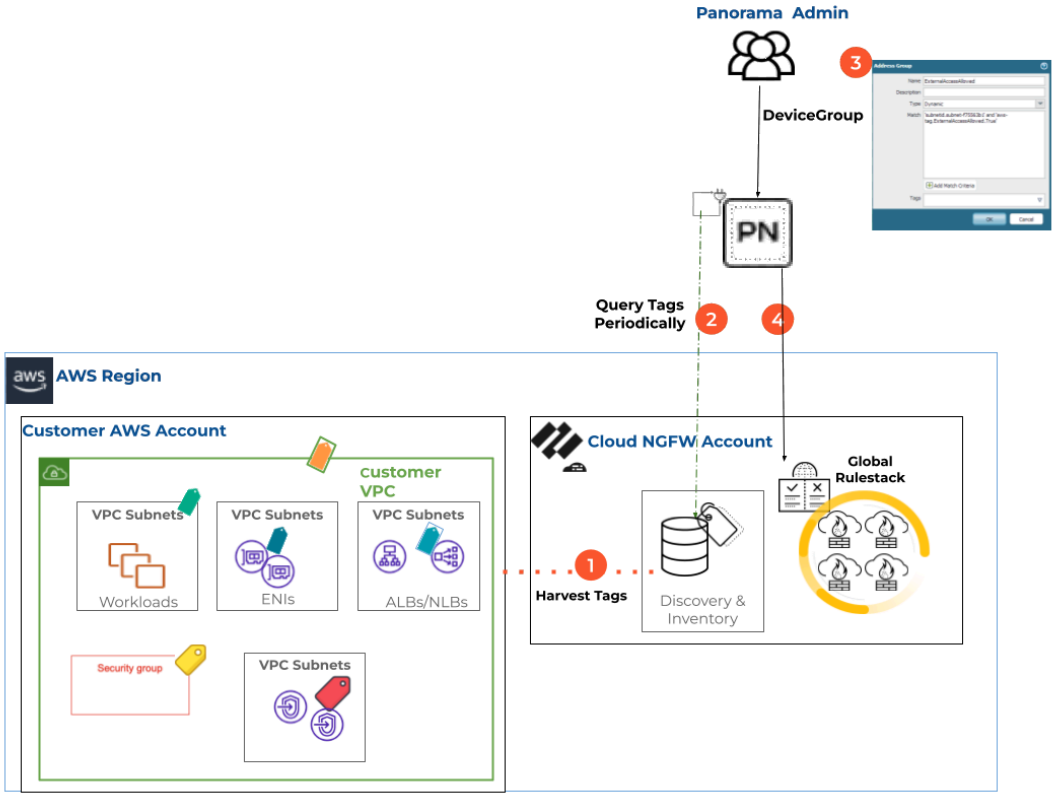
Configurer des politiques basées sur les étiquettes

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

Vous pouvez mettre à jour automatiquement la politique de sécurité sur vos ressources Palo Alto Networks CloudN GFW afin de sécuriser le trafic vers ces ressources AWS pendant que vous déployez ou résiliez des ressources AWS (telles que des instances EC2) dans le cloud public AWS.

Pour activer cette fonctionnalité depuis Panorama, vous devez configurer le plug-in AWS Panorama pour récupérer les adresses IP et les 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 des 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 règles de politique basées sur les étiquettes pour des ressources Cloud NGFW pour AWS, vous devez disposer de la configuration système minimale suivante :

- 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).
- Utilisez la console Cloud NGFW pour ajouter des comptes AWS à un locataire Cloud NGFW et collecter des étiquettes à partir de ceux-ci.
- Utilisez le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama.
- Configurez des objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans des 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 règles de politique basées sur les étiquettes pour des 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 ultérieure. 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 périodiquement les étiquettes de votre locataire Cloud NGFW et ajoutez-le aux groupes d'appareils Panorama pour gérer les règles et les objets Dynamic Address Group (groupe d'adresses dynamiques – DAG).

Pour activer les règles de politique basées sur les étiquettes Cloud NGFW sur votre appareil Panorama :

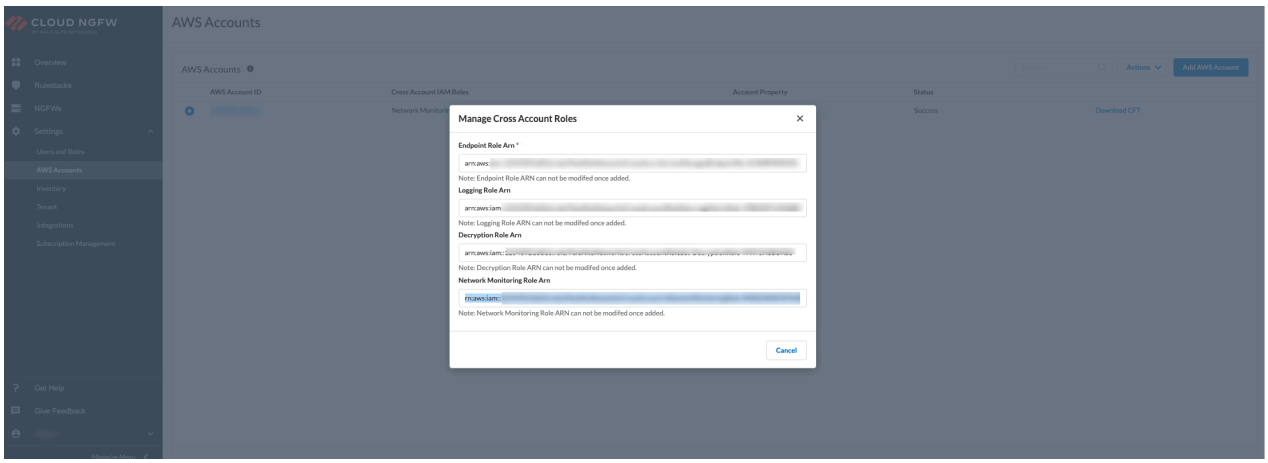
1. Ajoutez des comptes AWS à un locataire Cloud NGFW et collectez des étiquettes à partir de ces comptes.
2. Utilisez le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama.
3. Configurez des objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans des groupes d'appareils.

Ajouter des comptes AWS au locataire Cloud NGFW et collecter des étiquettes à partir de ces comptes

Intégrez votre compte AWS à votre locataire Cloud NGFW. Pour en savoir plus, consultez l'**étape 10** de la section 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

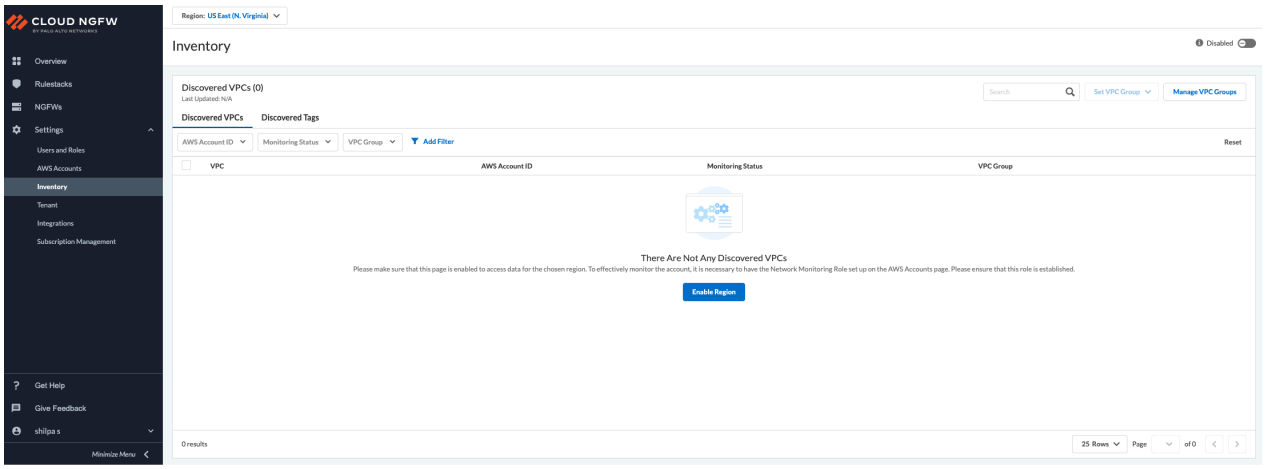
Dans la console Cloud NGFW, vous pouvez activer la découverte des étiquettes de ressources AWS pour les régions souhaitées. Cloud NGFW collectera périodiquement les étiquettes de vos ressources AWS (par

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.

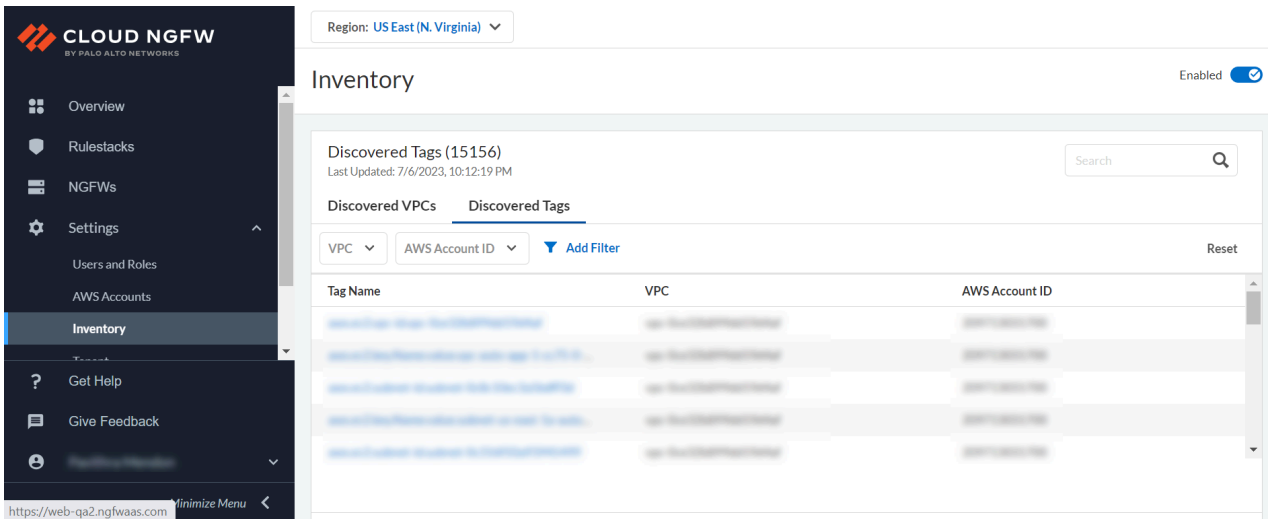
Le bouton **Enable Region (Activer la région)** sous l'onglet **Discovered VPCs (VPC découverts)** apparaît uniquement lors de l'intégration de votre compte AWS pour la première fois. Sélectionnez **Region (Région)** dans la liste déroulante et cliquez sur **Enable Region (Activer la région)** pour activer 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.

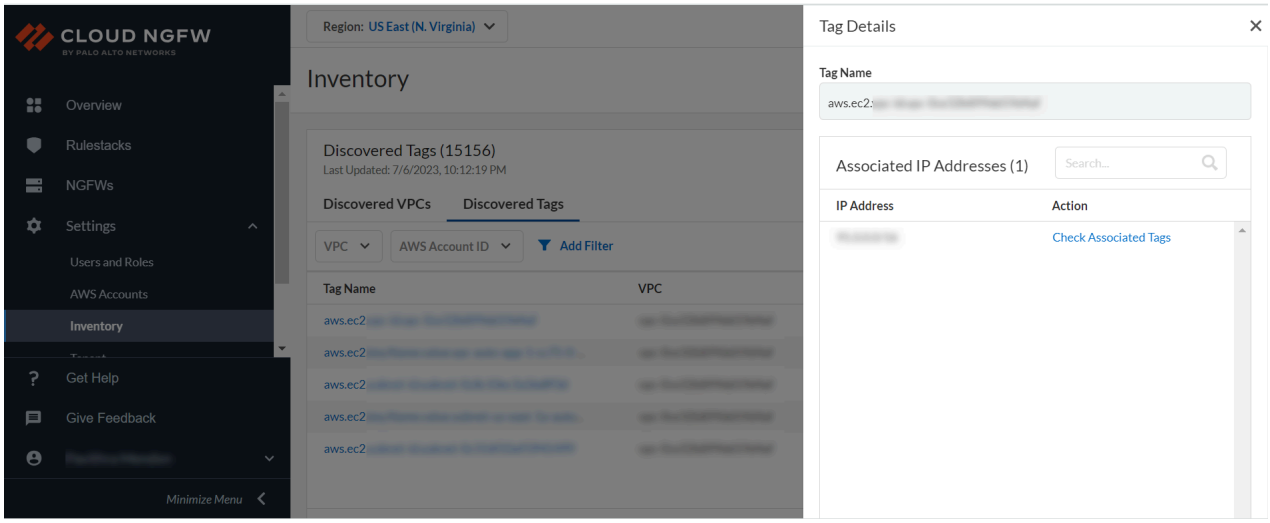


Afficher les étiquettes collectées dans la console Cloud NGFW

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'admin d'inventaire**, vous ne pouvez pas utiliser les options **Set VPC group (Définir un groupe de VPC)** ou **Create New VPC (Créer un 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 :

STEP 1 | Créer et gérer des groupes de VPC.

STEP 2 | Ajouter des étiquettes aux groupes d'appareils à l'aide des définitions de surveillance et de groupes de notification.

Installez et configurez le plug-in AWS 5.1.0 (ou version ultérieure) 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.

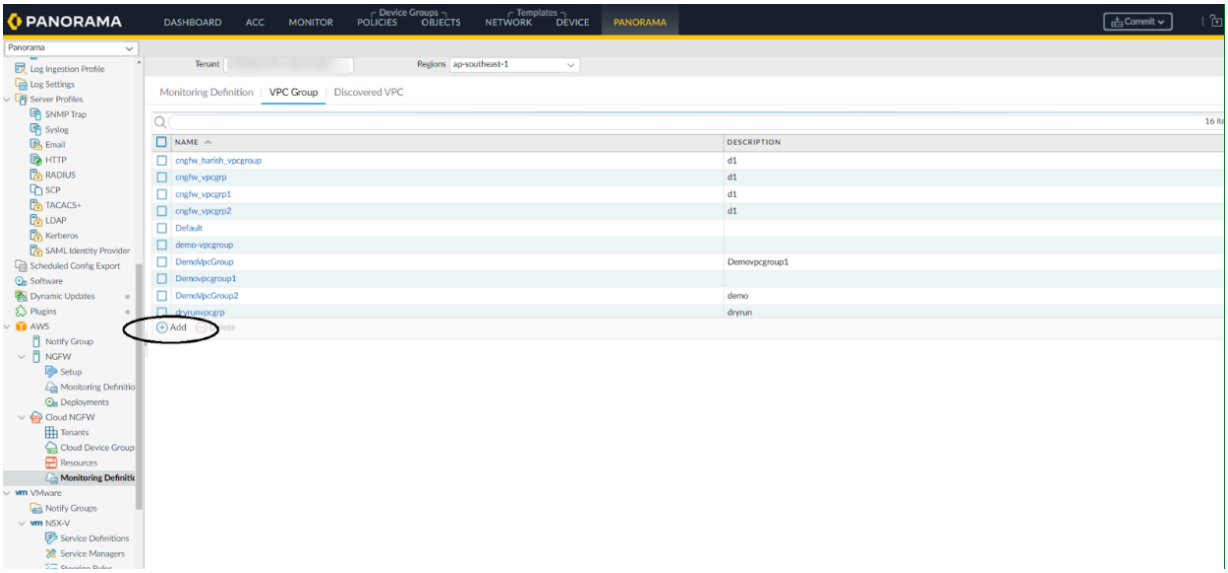
Vous pouvez également créer de nouveaux groupes de VPC et déplacer les VPC vers d'autres groupes de VPC en suivant les étapes ci-dessous :

Si vous souhaitez créer un nouveau **groupe de VPC autre que par défaut** sur Panorama, suivez les étapes décrites dans la procédure ci-dessous :

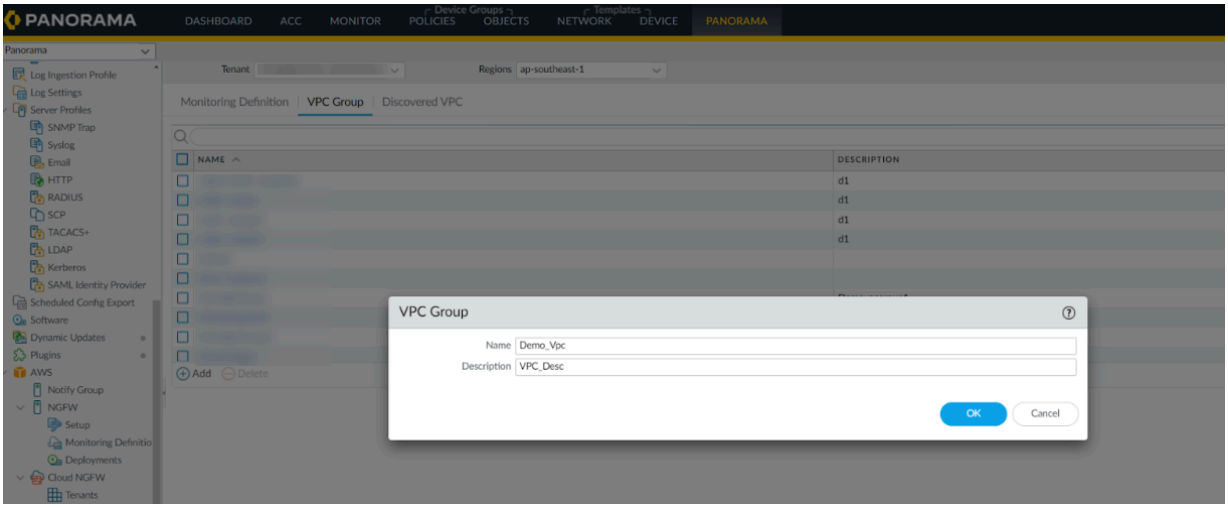
STEP 1 | Dans la console **Panorama**, accédez à l'onglet **Panorama** , puis cliquez sur **AWS**.

STEP 2 | Sélectionnez **Tenant (Locataire)** et **Region (Région)**.

STEP 3 | Accédez à **AWS** > **Cloud NGFW** > **Monitoring Definition (Définition de surveillance)** > **VPC Group (Groupe de VPC)** > **Add (Ajouter)**.

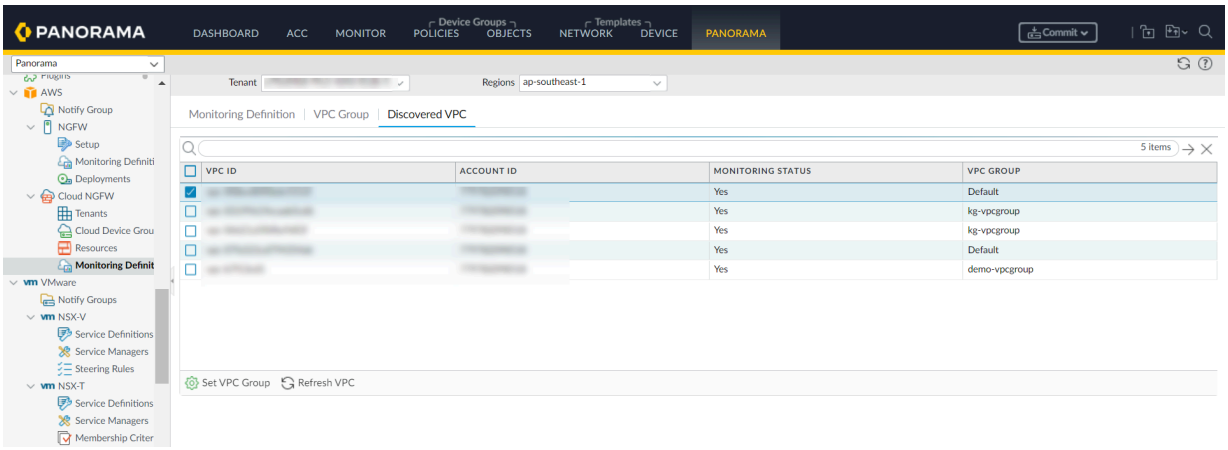


STEP 4 | Saisissez le **Name (Nom)** et la **Description** du groupe de VPC.



STEP 5 | Cliquez sur **OK**.

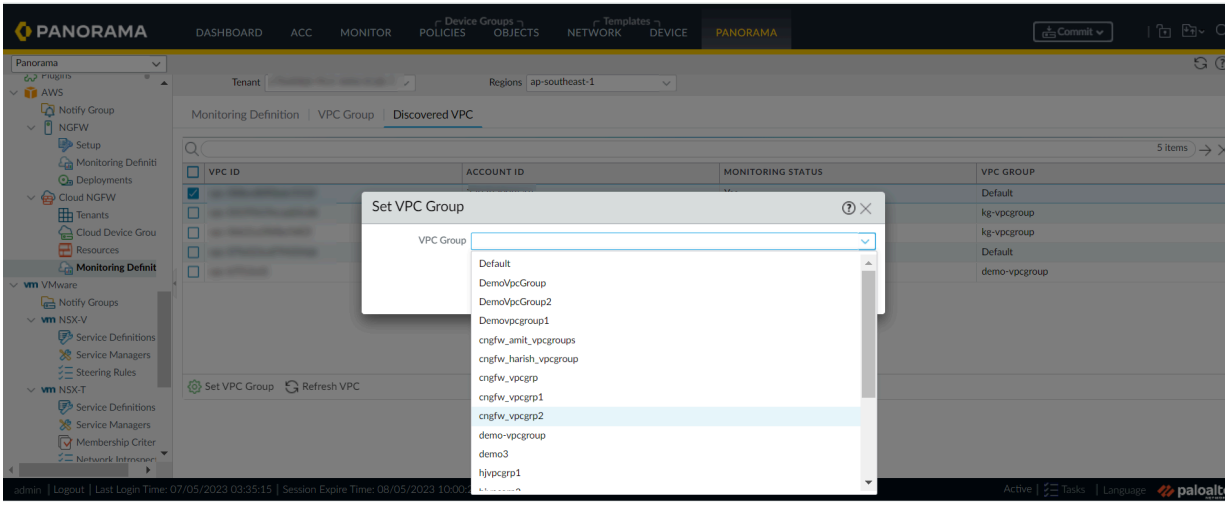
STEP 6 | Accédez à **AWS > Cloud NGFW > Monitoring Definition (Définition de la surveillance) > Discovered VPC (VPC découvert)**.



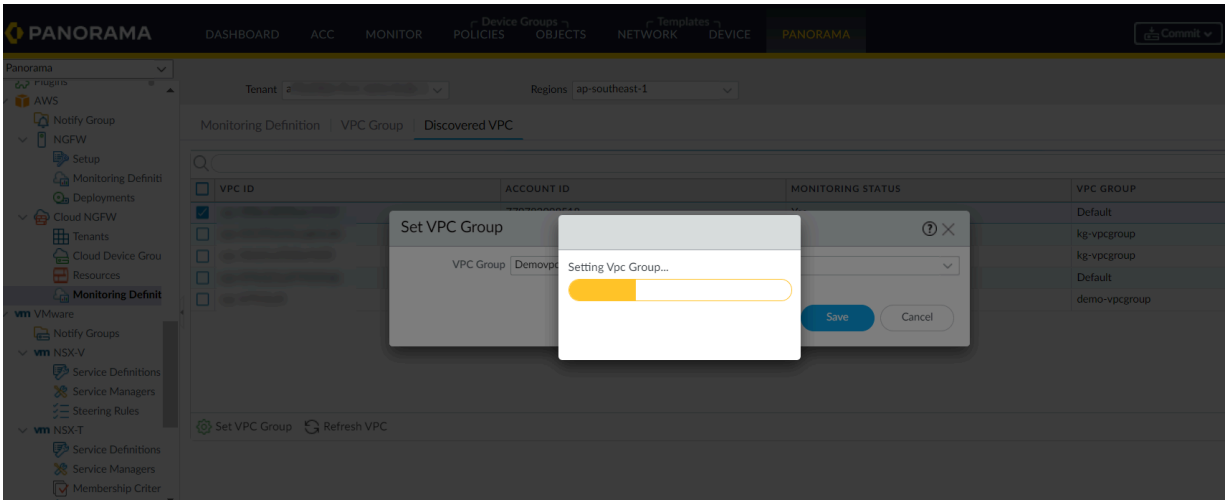
- *Vous ne pouvez pas mapper un **groupe de VPC** sur plus de huit groupes d'appareils. Configurez les définitions de la surveillance sur les groupes de VPC de sorte qu'un groupe de VPC donné n'ait que huit groupes d'appareils mappés (via les groupes de notification) pour de meilleures performances.*
- *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.*

STEP 7 | Cliquez sur **Set VPC Group (Définir le groupe de VPC)**.

STEP 8 | Sélectionnez **VPC Group (Groupe de VPC)**.



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



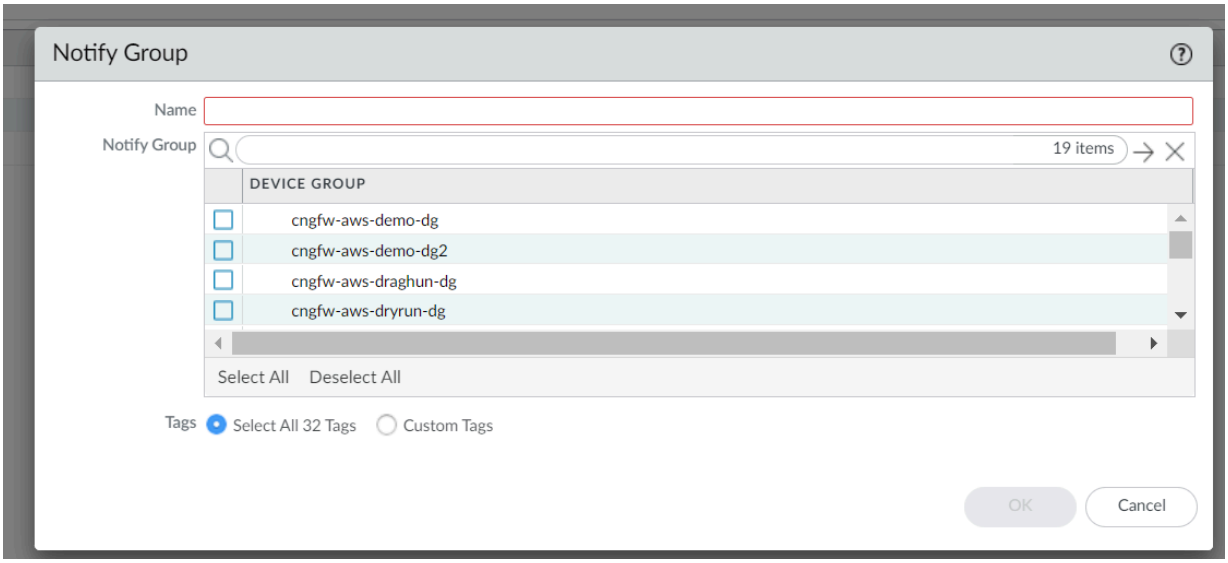
Ajouter des étiquettes aux groupes d'appareils à l'aide de définitions de la surveillance et de groupes d'appareils

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 :

STEP 1 | Dans la console **Panorama Plugin (plug-in Panorama)**, accédez à **AWS > Notify Group (Groupe de notification)**.

STEP 2 | **Ajoutez**.



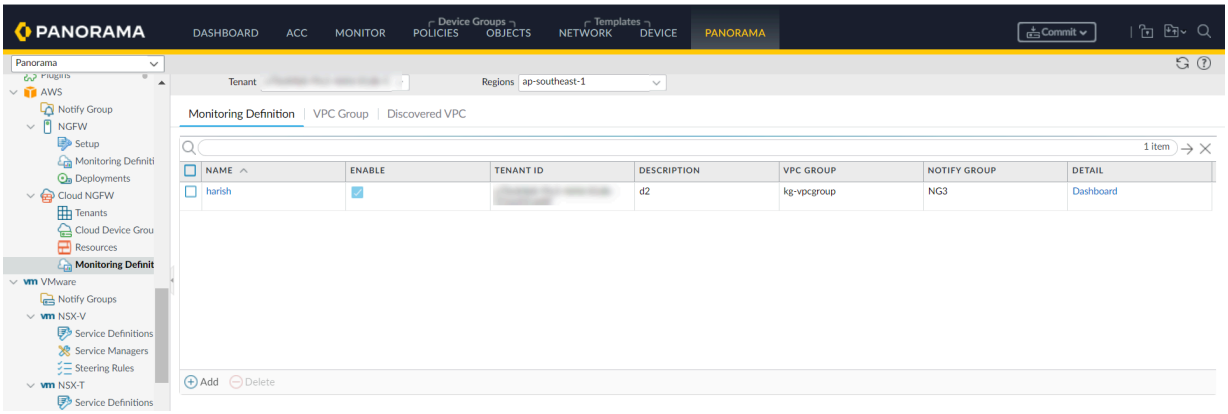
STEP 3 | Saisissez le **Name (Nom)**.

STEP 4 | Sélectionnez le **Device Group (Groupe d’appareils)** et les **Tags (Étiquettes)**.

STEP 5 | Cliquez sur **OK**.

Créez une **monitoring definition (définition de la surveillance)** cloud associant le **VPC group (Groupe de VPC)** requis et le **Notify group (Groupe de notification)** des étiquettes collectées auprès de Cloud NGFW.

STEP 6 | Dans **Panorama**, accédez à **AWS > Cloud NGFW > Monitoring Definition (Définition de la surveillance)**.

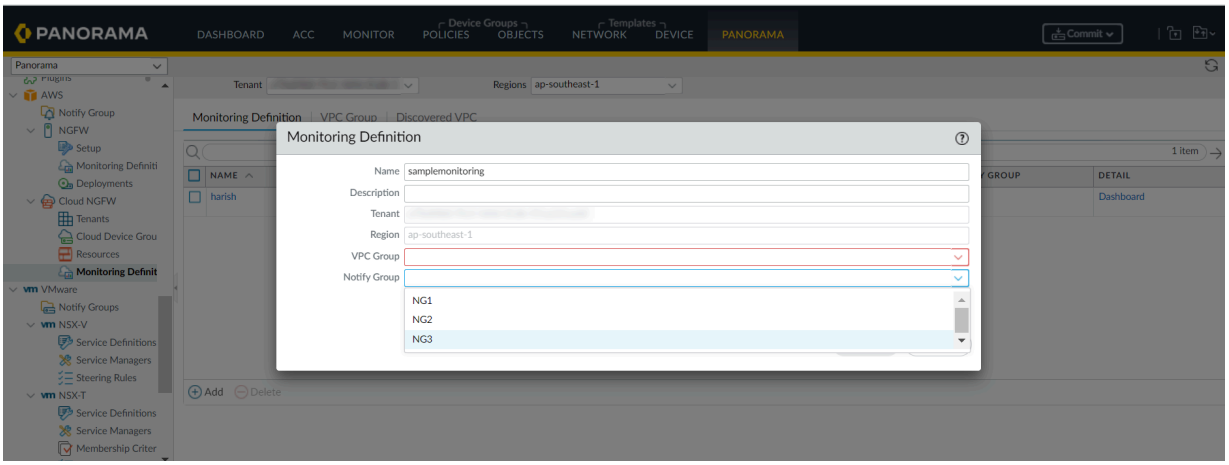


STEP 7 | Cliquez sur **Add (Ajouter)**.

STEP 8 | Saisissez votre **Name (Nom)** et la **Description**.

STEP 9 | Sélectionnez le groupe de VPC requis dans le menu déroulant **VPC Group (Groupe de VPC)**.

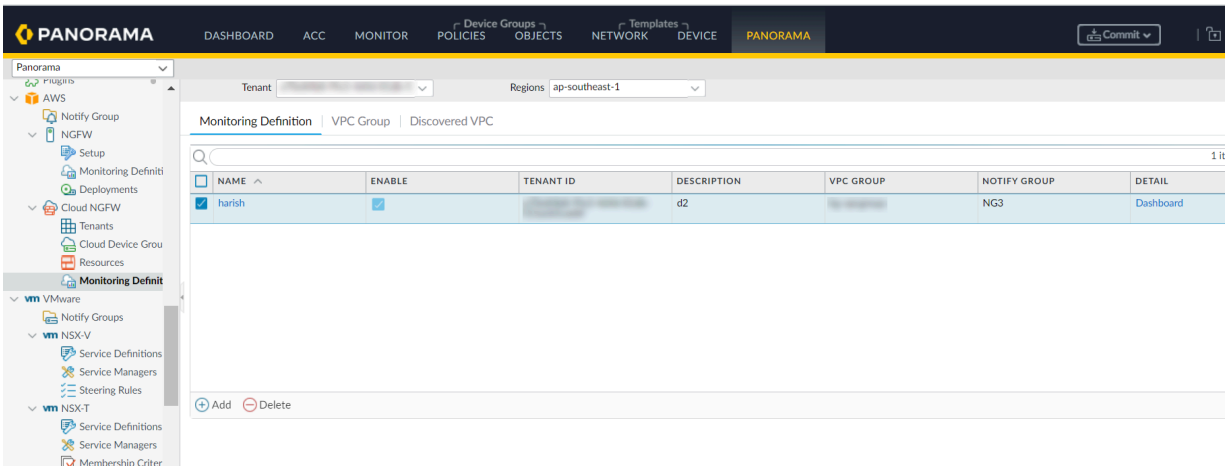
STEP 10 | Sélectionnez le groupe de notification requis dans le menu déroulant **Notify Group (Groupe de notification)**.



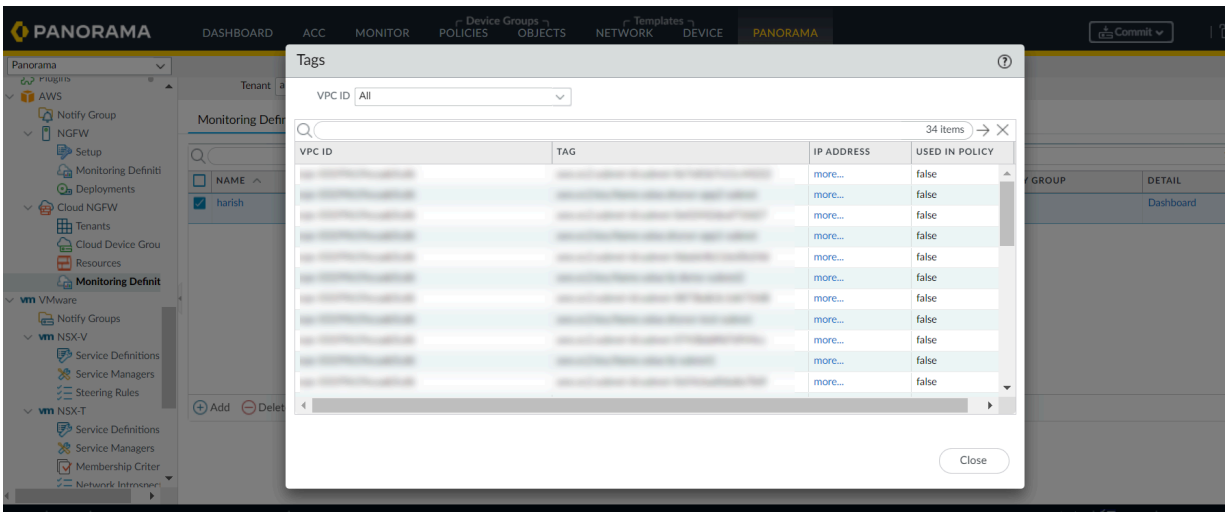
STEP 11 | Cliquez sur **OK**.

STEP 12 | **Validez** et **transmettez** vos modifications sur Panorama.

STEP 13 | Sélectionnez une **Monitoring Definition (Définition de surveillance)** et cliquez sur **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 des objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans des 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 :

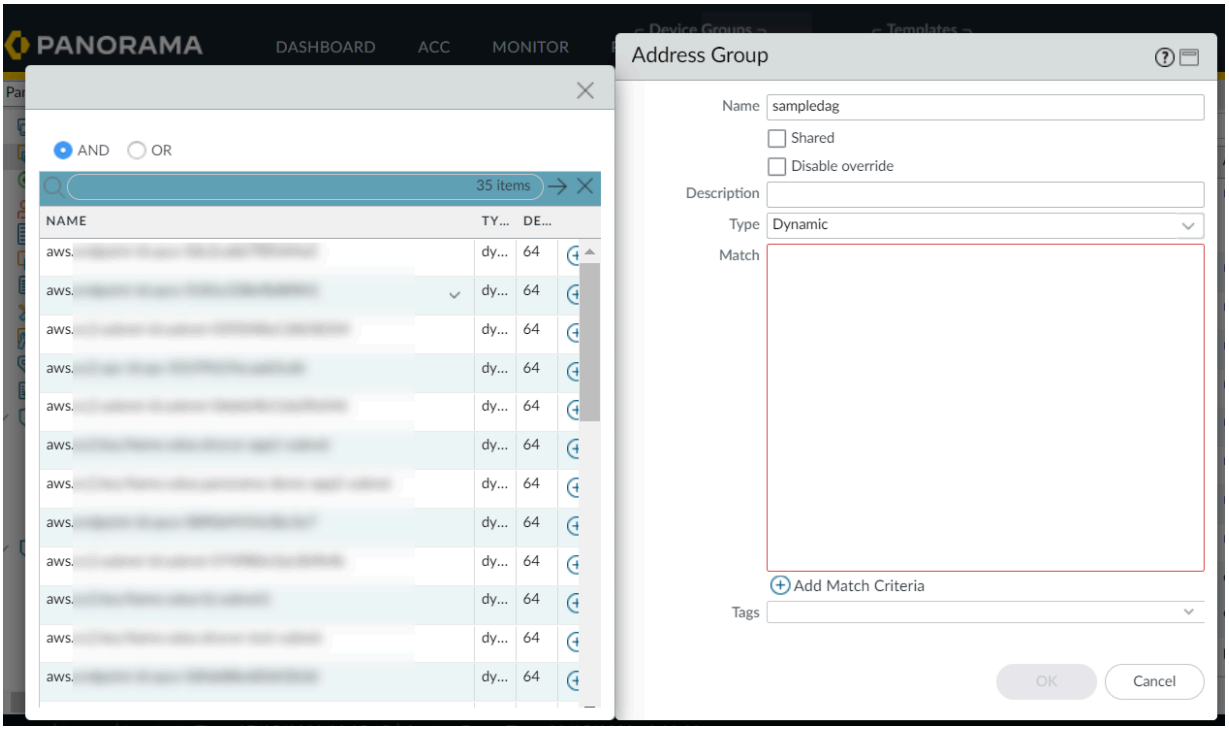
STEP 1 | Dans **Panorama**, sélectionnez l'onglet **Objects (Objets)**.

STEP 2 | Dans le volet de gauche, accédez à **Address Groups (Groupes d'adresses)**.

STEP 3 | Cliquez sur **Add (Ajouter)**.

STEP 4 | Saisissez le **Name (Nom)** de votre groupe d'adresses et sélectionnez le type **Dynamic (Dynamique)**.

STEP 5 | Cliquez sur **Add match Criteria (Ajouter des critères de correspondance)**.

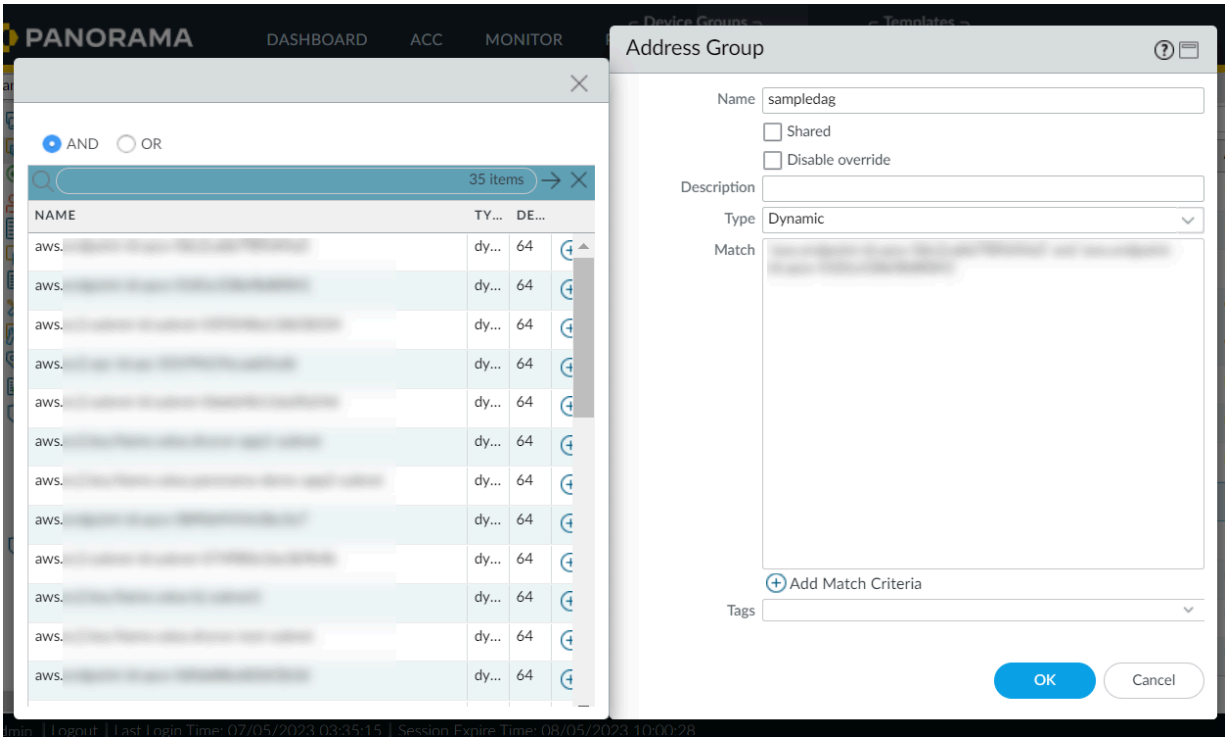


Vous pouvez désormais créer des **règles de politique Dynamic Address Group (groupe d'adresses dynamiques)** faisant référence aux DAG créés ci-dessus pour les groupes d'appareils cloud.

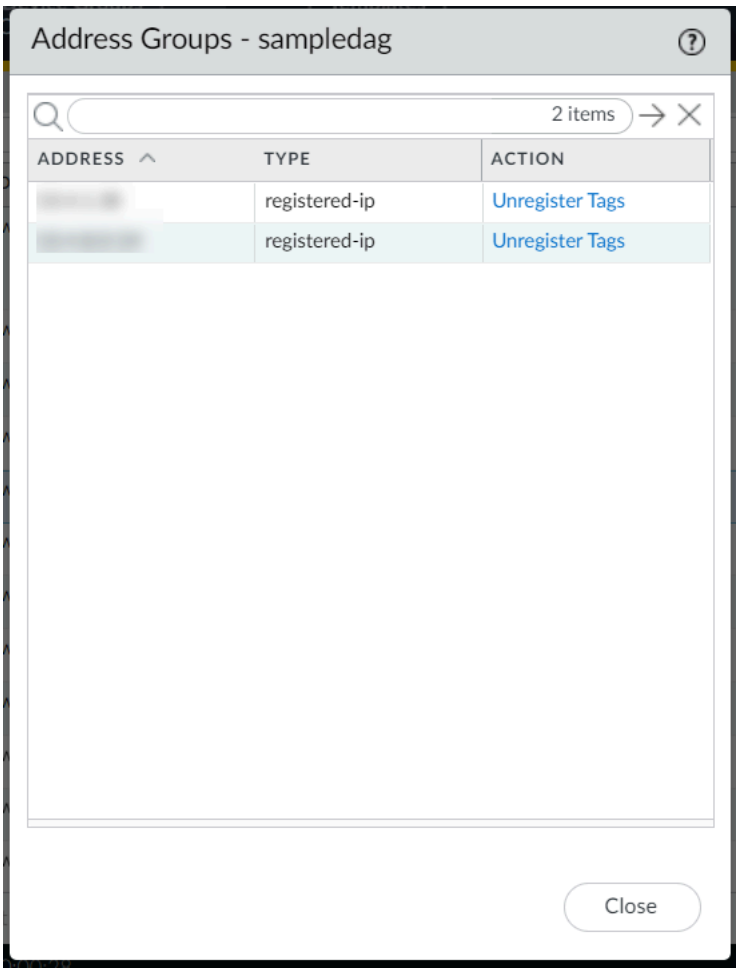
Vous pouvez ajouter des étiquettes de différentes régions sur votre objet Dynamic Address Group (groupe d'adresses dynamiques). Pour utiliser des étiquettes de différentes régions, vous devez créer un groupe d'appareils cloud du même nom dans d'autres régions. En outre, vous devez créer une définition

de la surveillance dans d'autres régions mappant le groupe de notification au groupe de VPC de la région concernée. Pour en savoir plus, consultez Politiques basées sur des étiquettes inter-régions.

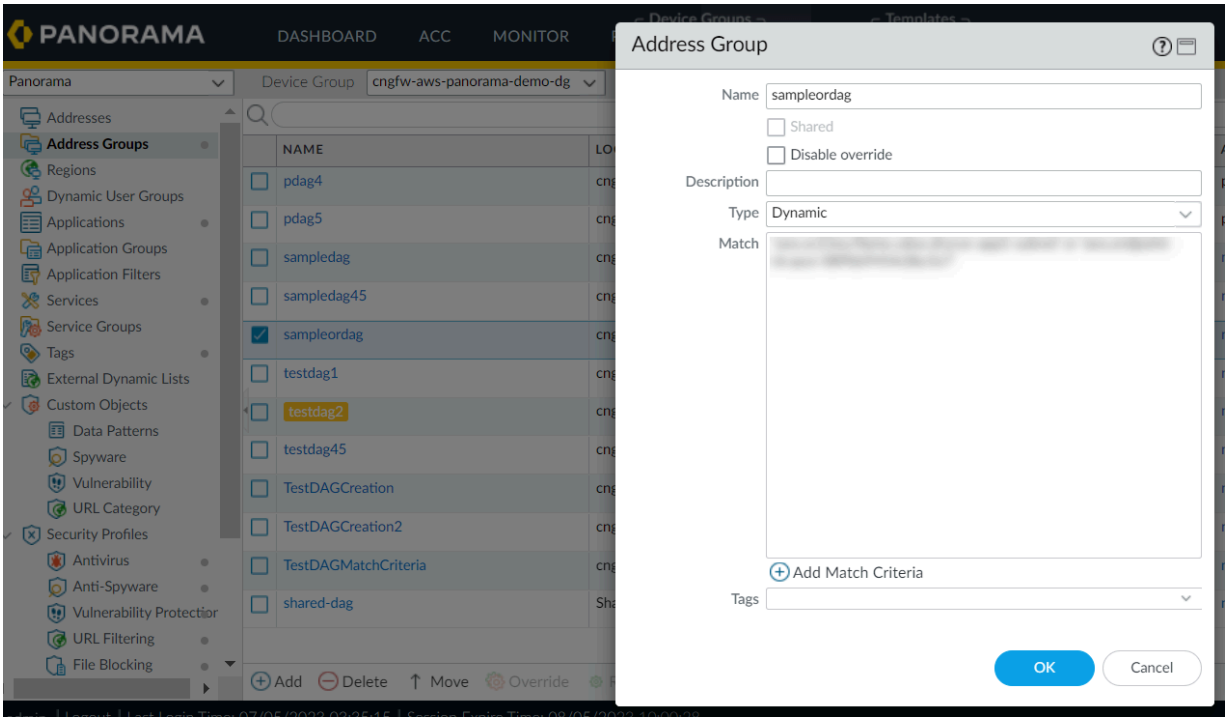
Voici un exemple de création de DAG à l'aide de l'opérateur **AND** :



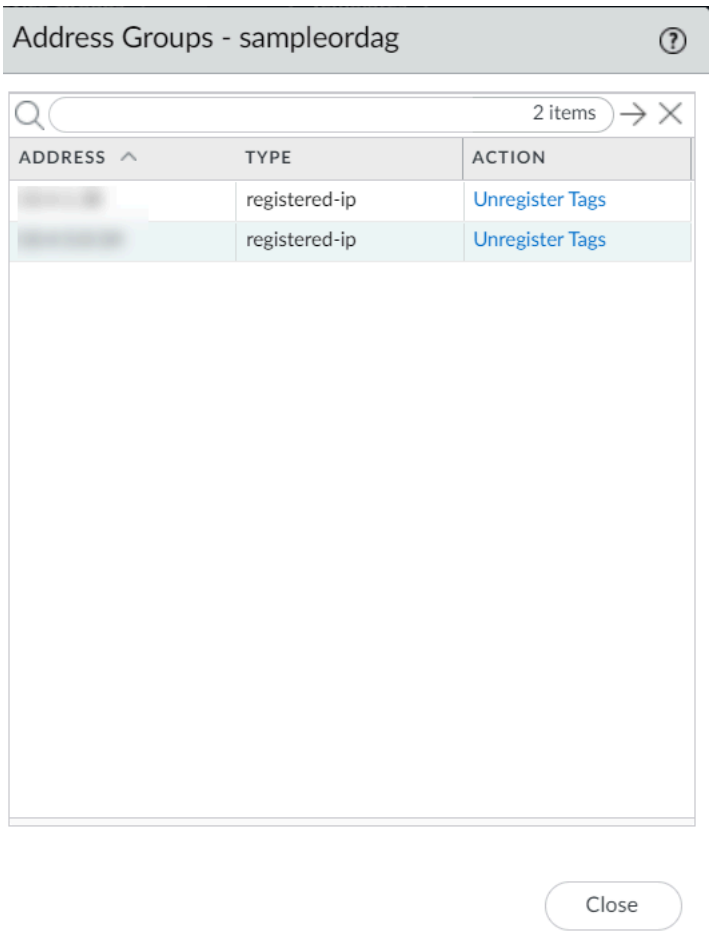
Le groupe d'adresses affiche la liste des adresses qui correspondent aux deux critères de correspondance :



Voici un exemple de création de DAG à l'aide de l'opérateur **OR** :



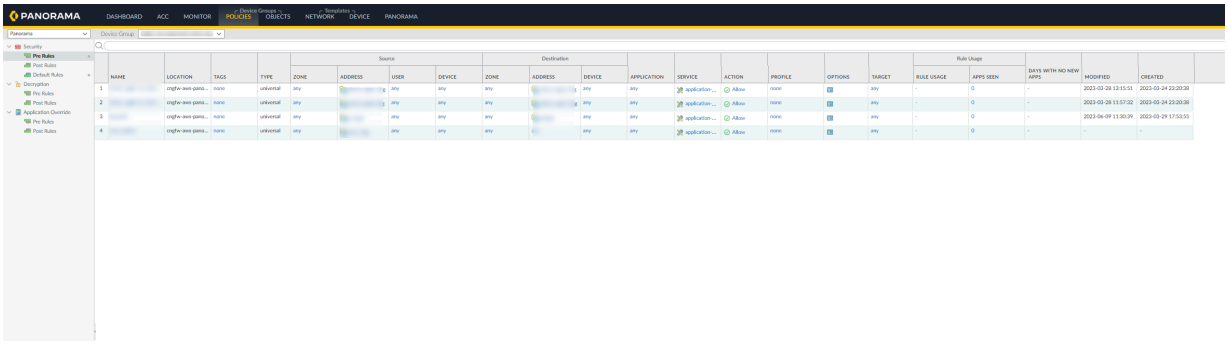
Le groupe d’adresses affiche la liste des adresses qui correspondent à au moins un des critères de correspondance donnés :



Procédez comme suit pour créer des règles de politique d’adresse dynamique faisant référence à des DAG pour les groupes d’appareils cloud :

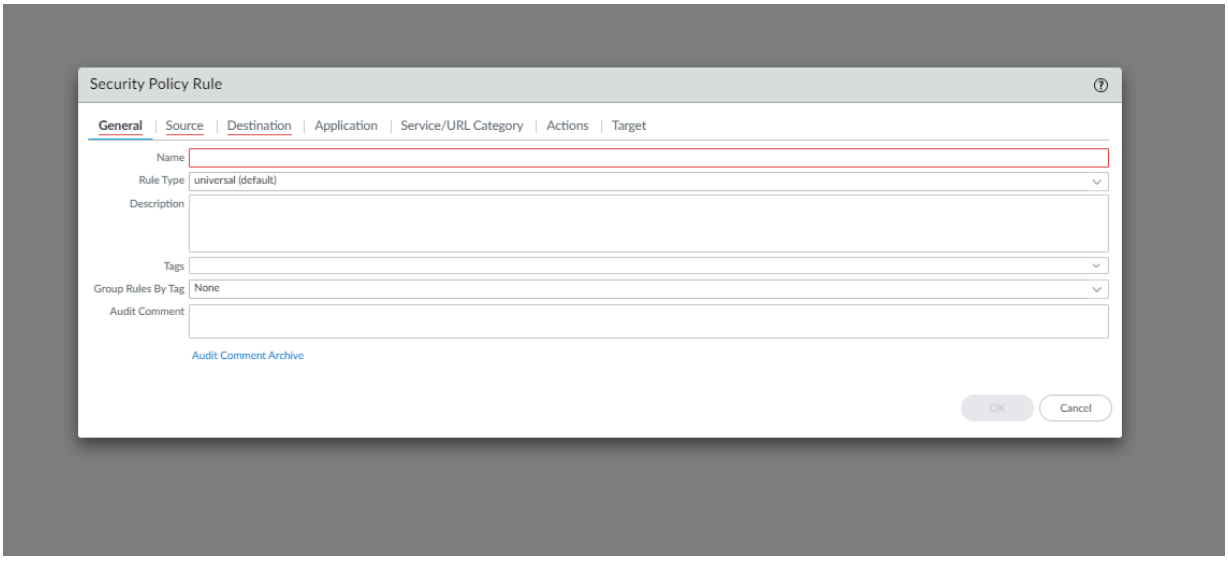
STEP 6 | Dans la console **Panorama**, accédez à l’onglet **Policies (Politiques)**.

STEP 7 | Accédez à **Security (Sécurité) > Pre/Post/Default Rules (Règles « avant »/« après »/par défaut)**.

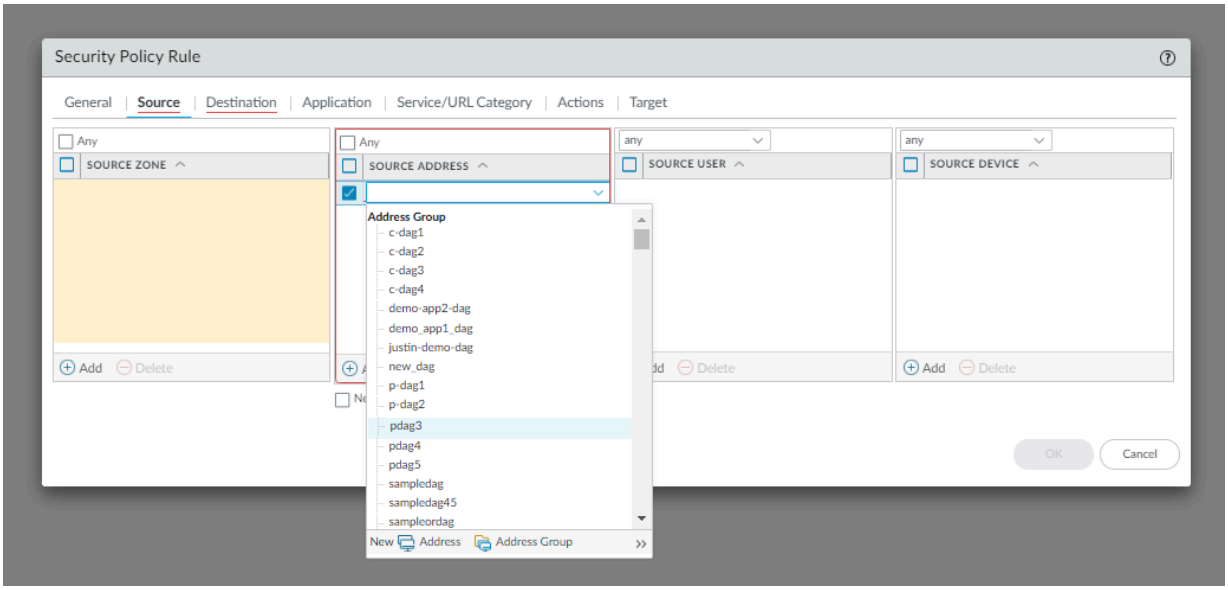


STEP 8 | Cliquez sur **Add (Ajouter)**.

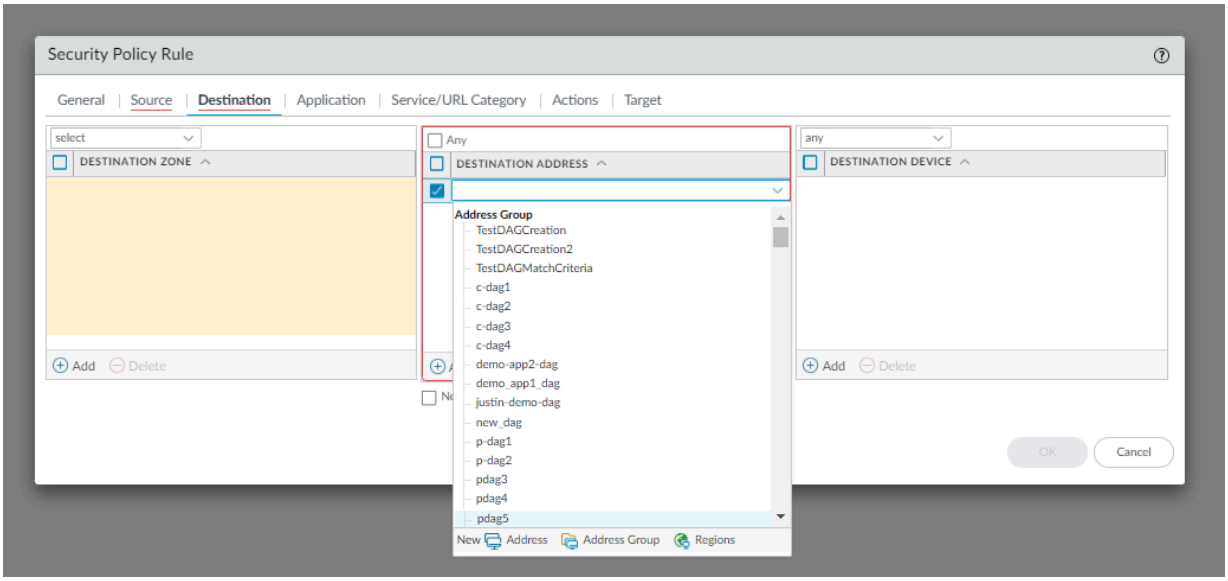
STEP 9 | Dans la boîte de dialogue **Security policy rule (Règle de politique de sécurité)**, saisissez un **Name (Nom)** pour la règle de politique de sécurité.



STEP 10 | Dans l’onglet **Source**, sélectionnez le groupe d’adresses dynamiques du champ **Source Address (Adresse source)** et cliquez sur **Add (Ajouter)**.



STEP 11 | Dans l’onglet **Destination**, sélectionnez le groupe d’adresses dynamiques du champ **Destination Address (Adresse de destination)** et cliquez sur **Add (Ajouter).**



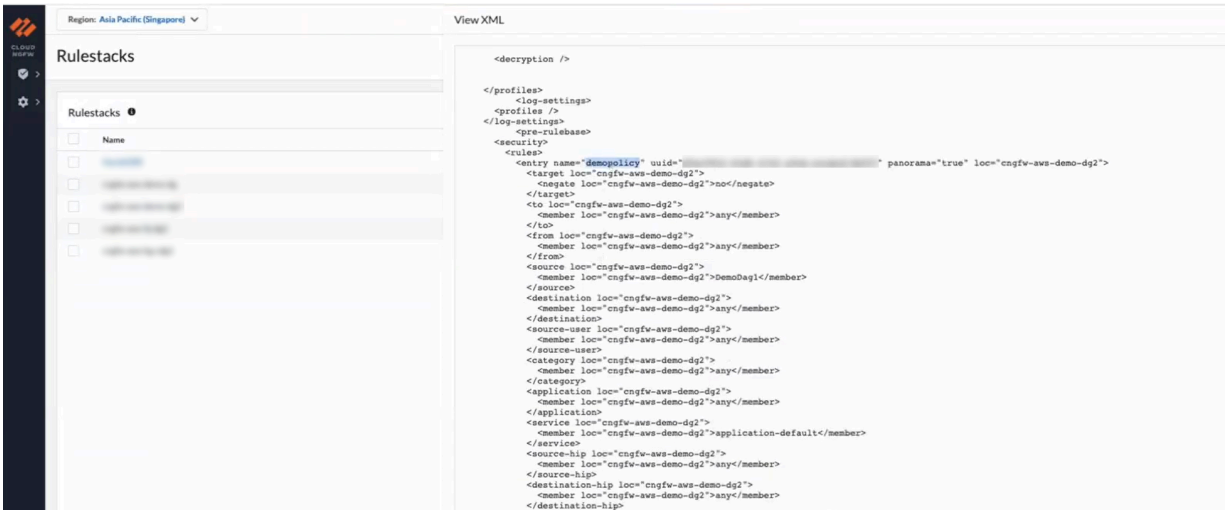
STEP 12 | Cliquez sur **OK**.

STEP 13 | Cliquez sur **Commit (Valider)** et **Push (Pousser)** pour valider et transmettre les 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 règles de politique d’adresse dynamique transmises de Panorama vers le groupe d’appareils cloud respectif. Cliquer

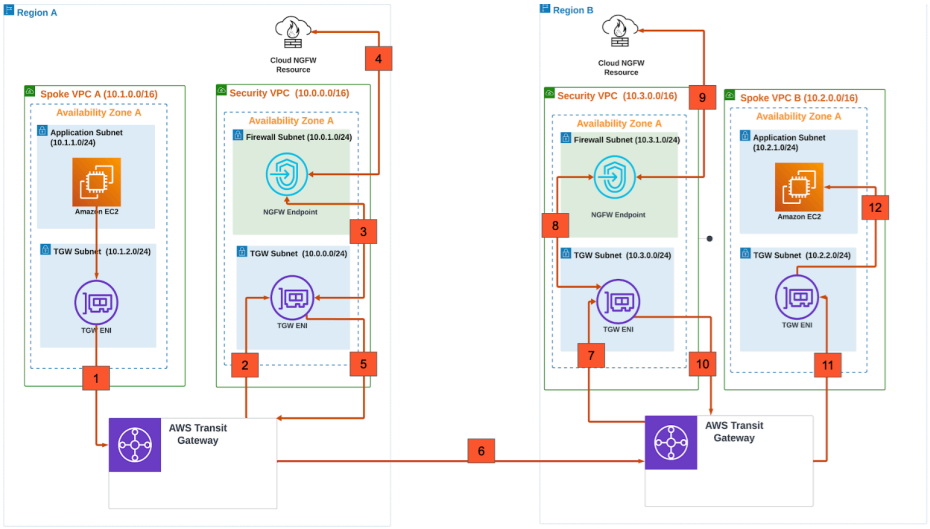
sur **View XML (Afficher XML)** pour afficher des informations sur les règles de politique d’adresse dynamique récemment ajoutées au groupe d’appareils cloud.



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 une ressource CNGFW présente dans la région X doit apprendre les étiquettes de la région Y, puis les utiliser pour le groupe d'appareils cloud dans la région X, effectuez les étapes suivantes :

STEP 1 | Ajoutez des comptes AWS au locataire Cloud NGFW et collectez les étiquettes à partir de ceux-ci.

STEP 2 | Utilisez le plug-in Panorama pour interroger les étiquettes et les ajouter aux groupes d'appareils Panorama.

STEP 3 | Configurez des objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans des groupes d'appareils.

Vous ne pourrez voir que les étiquettes de la région X disponibles pour la configuration des objets Dynamic Address Group (groupe d'adresses dynamiques).

STEP 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.

STEP 5 | Créez une définition de la surveillance dans la région Y, puis sélectionnez le groupe de VPC et le groupe de notification (où le groupe d'appareils cloud est déjà mappé).

STEP 6 | Configurez des objets Dynamic Address Group (groupe d'adresses dynamiques – DAG) avec des étiquettes dans des groupes d'appareils. Vous pouvez maintenant voir que les étiquettes de la région X et de la région Y sont disponibles pour la configuration des objets Dynamic Address Group (groupe d'adresses dynamiques).

STEP 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 Dynamic Address Group (groupe d'adresses dynamiques).

Configurer des règles de politique basées sur les zones

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

La segmentation du réseau en zones fonctionnelles et organisationnelles réduit la surface d'attaque du réseau (la portion exposée aux attaquants éventuels). Les zones de sécurité protègent votre réseau en le segmentant en zones plus petites et plus faciles à gérer et en contrôlant l'accès du trafic à celles-ci.

Dans les pare-feu autogérés de Palo Alto Networks (tels que VM-Series), une zone de sécurité comprend une ou plusieurs interfaces de pare-feu physiques ou virtuelles ainsi que les segments de réseau connectés

aux interfaces de la zone. Vous définissez d'abord des zones, puis vous associez les interfaces physiques et virtuelles à ces zones. Enfin, vous utilisez ces zones dans les règles de politique de sécurité que vous créez.

Toutefois, Cloud NGFW configure automatiquement les constructions de mise en réseau pour vous. Vous n'avez plus à vous soucier de la configuration des interfaces et de leur association aux zones que vous créez. Vous pouvez créer des règles de politique basées sur les zones dans Panorama et les appliquer sur Cloud NGFW.

Zones Cloud NGFW

Cloud NGFW vous permet de classer le trafic de VPC à l'aide de zones **privées** et **publiques** pour simplifier l'application des politiques.

- La **zone privée** inclut votre réseau cloud hybride défini par les préfixes de plage de trafic privé. Ce réseau englobe vos VPC sur AWS et votre réseau sur site (connecté via Direct Connect ou VPN).
- La **zone publique** comprend tous les préfixes en dehors de votre réseau cloud hybride (l'Internet public).

Pour contrôler cette classification, spécifiez de manière appropriée les préfixes de plage de trafic privé pour le terminal sur lequel le trafic entre dans la ressource Cloud NGFW.

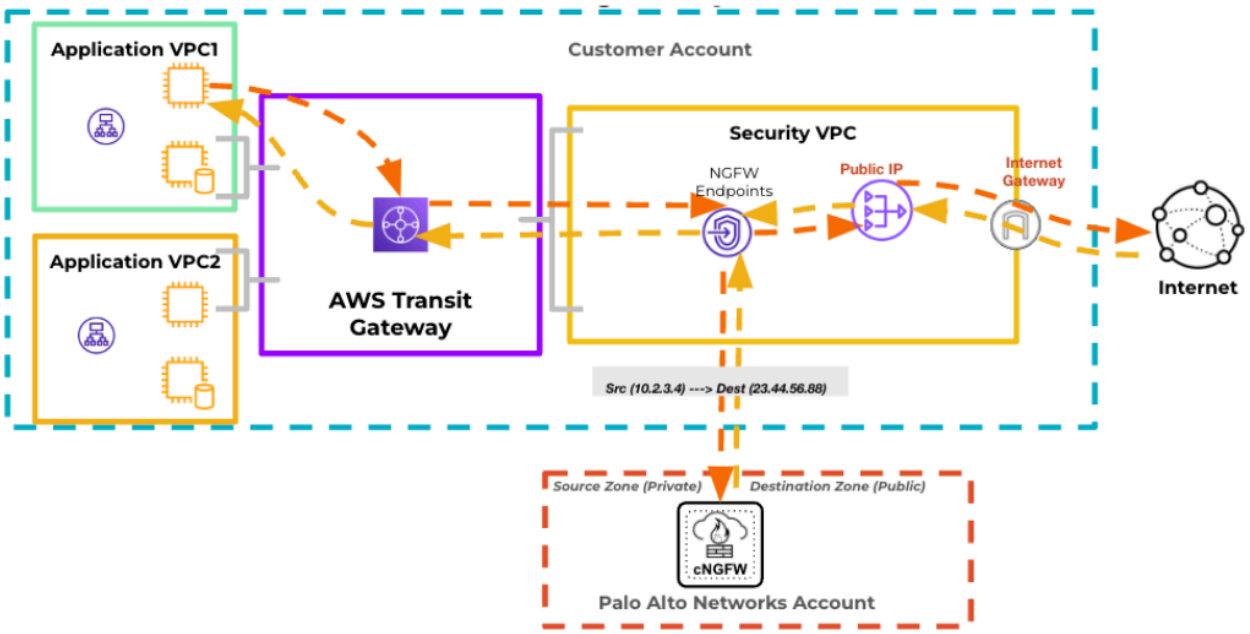
Zones source et de destination

Cloud NGFW définit automatiquement la **zone source** comme **privée** si la session de trafic dispose d'une adresse IP source comprise dans les préfixes de plage de trafic privé définis pour le terminal sur lequel le trafic entre dans la ressource Cloud NGFW. Sinon, Cloud NGFW définit la zone source comme **publique**.

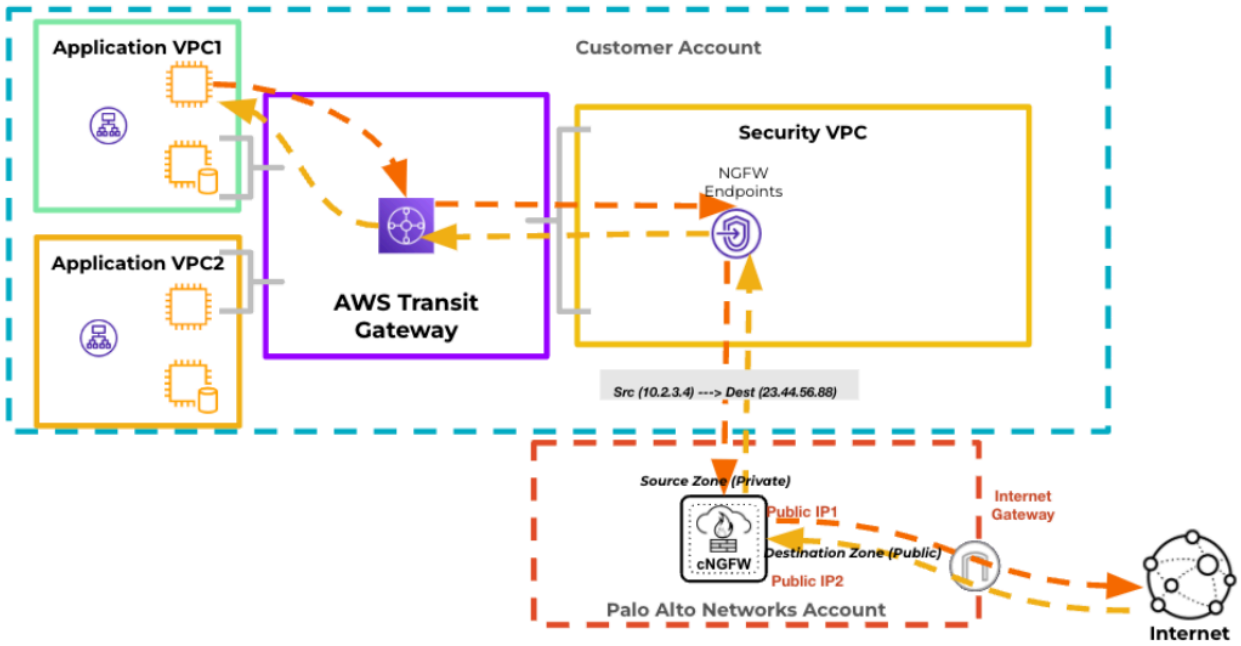
De même, Cloud NGFW définit automatiquement la **zone de destination** comme **privée** si la session de trafic dispose d'une adresse IP de destination comprise dans les préfixes de plage de trafic privé définis pour le terminal sur lequel le trafic entre dans la ressource Cloud NGFW. Sinon, Cloud NGFW définit la zone de destination comme **publique**.

Par exemple, Cloud NGFW définit la zone source (entrée) comme privée et la zone de destination comme publique pour une session avec une adresse IP source 10.2.3.4 et une adresse IP de destination 23.44.55.66.

L'illustration ci-dessous montre les zones source et de destination sur le trafic passant par un terminal avec la NAT de sortie désactivée :



L’illustration ci-dessous montre les zones source et de destination sur le trafic passant par un terminal avec la NAT de sortie activée :



protection de zones

Pour vous défendre efficacement contre les attaques DoS, vous avez besoin d'une approche en couches. La première couche de défense doit être un service de protection DDoS dédié et capable de traiter de gros volumes, comme AWS Shield, pour vous protéger contre les attaques volumétriques que les pare-feu basés sur les sessions ne sont pas en mesure de gérer. Toutefois, Cloud NGFW utilise le profil de protection de zone pour ajouter des couches de défense contre les attaques DoS plus granulaires et fournir une visibilité sur le trafic des applications que les services DDoS dédiés ne fournissent pas.

Une fois que le trafic passe par le service DDoS dédié (tel qu'AWS Shield) et entre dans le VPC, Cloud NGFW applique le profil de protection de zone s'il est attaché à la zone d'entrée (source). Cloud NGFW détermine la zone d'entrée (source) à partir de l'adresse IP source du paquet. Les profils de protection de zone offrent une défense large contre les attaques DoS en fonction du trafic agrégé entrant dans la zone. Si le profil de protection de zone refuse le paquet, Cloud NGFW abandonne ce paquet et ignore la recherche de politique de sécurité. Cloud NGFW applique des profils de protection de zone uniquement aux nouvelles sessions (paquets qui ne correspondent pas à une session existante). Une fois la session établie, le moteur de traitement de paquets Cloud NGFW contourne la recherche de profils de protection de zone pour les paquets suivants dans cette session.

Vous pouvez attacher un profil de protection de zone aux zones privées et publiques à l'aide du modèle de groupe d'appareils cloud Panorama. Un profil de protection de zone protège la zone d'entrée (ou source) contre les attaques par saturation, de reconnaissance et basées sur les paquets les plus courantes.

- Protection contre la saturation. Un profil de protection de zone pour lequel la protection contre la saturation a été configurée permet de protéger une zone d'entrée entière contre les attaques par saturation SYN, ICMP, ICMPv6, UDP et autres attaques basées sur des adresses IP.
- Protection contre la reconnaissance La reconnaissance en matière de sécurité des réseaux, tout comme la reconnaissance militaire, correspond aux tentatives des agresseurs d'obtenir des informations sur les vulnérabilités de vos réseaux en les sondant secrètement pour y trouver des failles. Les activités de reconnaissance préfigurent bien souvent une attaque du réseau. *Activez la protection contre la reconnaissance sur les zones privées et publiques* pour vous protéger contre les analyses des ports et le balayage de l'hôte.

- Protection contre les attaques basées sur les paquets. Les attaques basées sur des paquets prennent de nombreuses formes. Les profils de protection de zone vérifient les en-têtes des paquets IP, TCP, ICMP, IPv6 et ICMPv6 et protègent une zone en abandonnant les paquets présentant des caractéristiques indésirables ou en supprimant les options indésirables des paquets avant de les admettre dans la zone.

Mappage des zones Cloud NGFW

Les zones sont associées à des interfaces sur des pare-feu autogérés tels que VM-Series. Cependant, dans Cloud NGFW, l'infrastructure de mise en réseau est automatiquement configurée pour vous. Cela signifie que vous n'avez plus à vous soucier de la configuration des interfaces et de leur association aux zones que vous créez (en outre, dans les modèles et les piles de modèles Cloud NGFW Panorama, l'interface web permettant de configurer des interfaces est supprimée de Panorama : tous les éléments inutiles de l'interface web de Panorama sont supprimés des groupes d'appareils cloud gérés par Panorama).

Néanmoins, pour permettre une application cohérente des politiques de sécurité, vous devez créer des mappages de zones dans vos groupes d'appareils cloud afin que Cloud NGFW sache s'il faut associer les zones de sécurité présentes dans votre Panorama à la zone privée (interne) ou publique (externe) de Cloud NGFW. Ces mappages permettent à Cloud NGFW d'appliquer correctement vos règles de politique de sécurité.

Dans certains cas, le mappage de zones peut échouer si vous n'exécutez pas la dernière version du plug-in AWS (version 5.3.0). Palo Alto Networks vous recommande de ne pas activer de politiques basées sur les zones pour les pare-feu existants qui n'ont pas été mis à niveau vers la nouvelle AMI de NAT de sortie à l'aide du plug-in AWS version 5.3.0 ou ultérieure.

Configurer le mappage de zones dans les groupes d'appareils cloud Panorama

Les règles de politique basées sur les zones nécessitent la configuration système minimale suivante :

- Plug-in AWS version 5.3.0 ou ultérieure
- PAN-OS version 10.2.8 ou ultérieure
- Plug-in Cloud Connector version 2.0.1 ou ultérieure

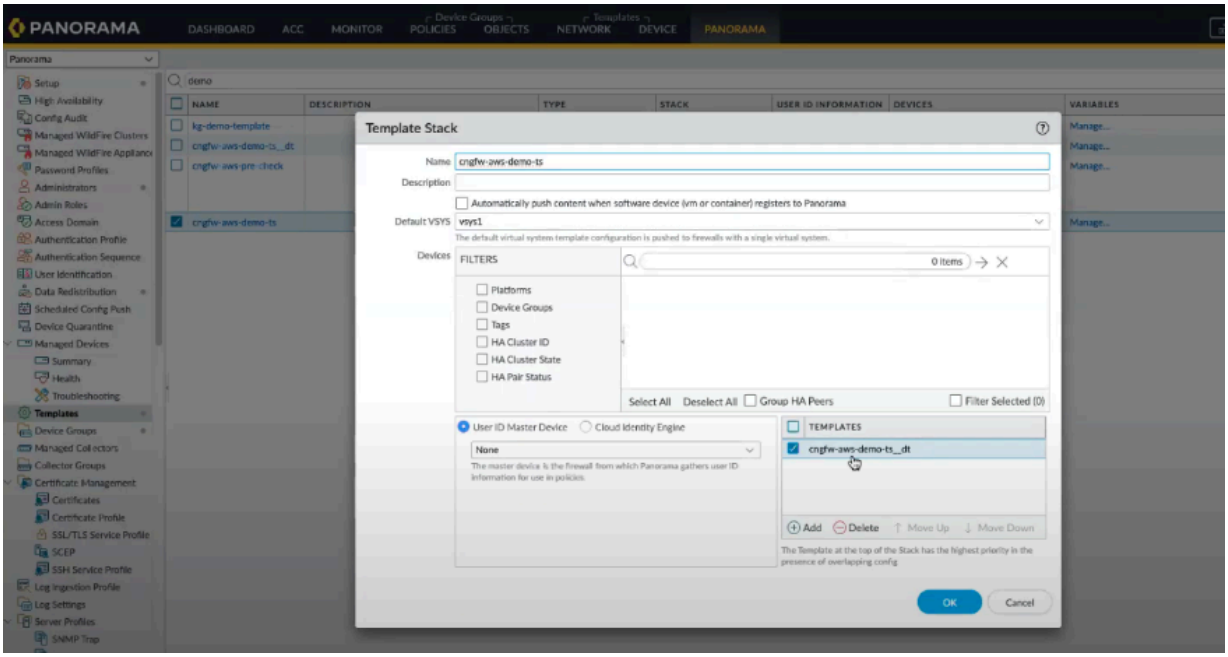
Pour configurer le mappage de zones à l'aide de la console Panorama :

STEP 1 | Ajoutez un groupe d'appareils cloud à l'aide de la console Panorama.

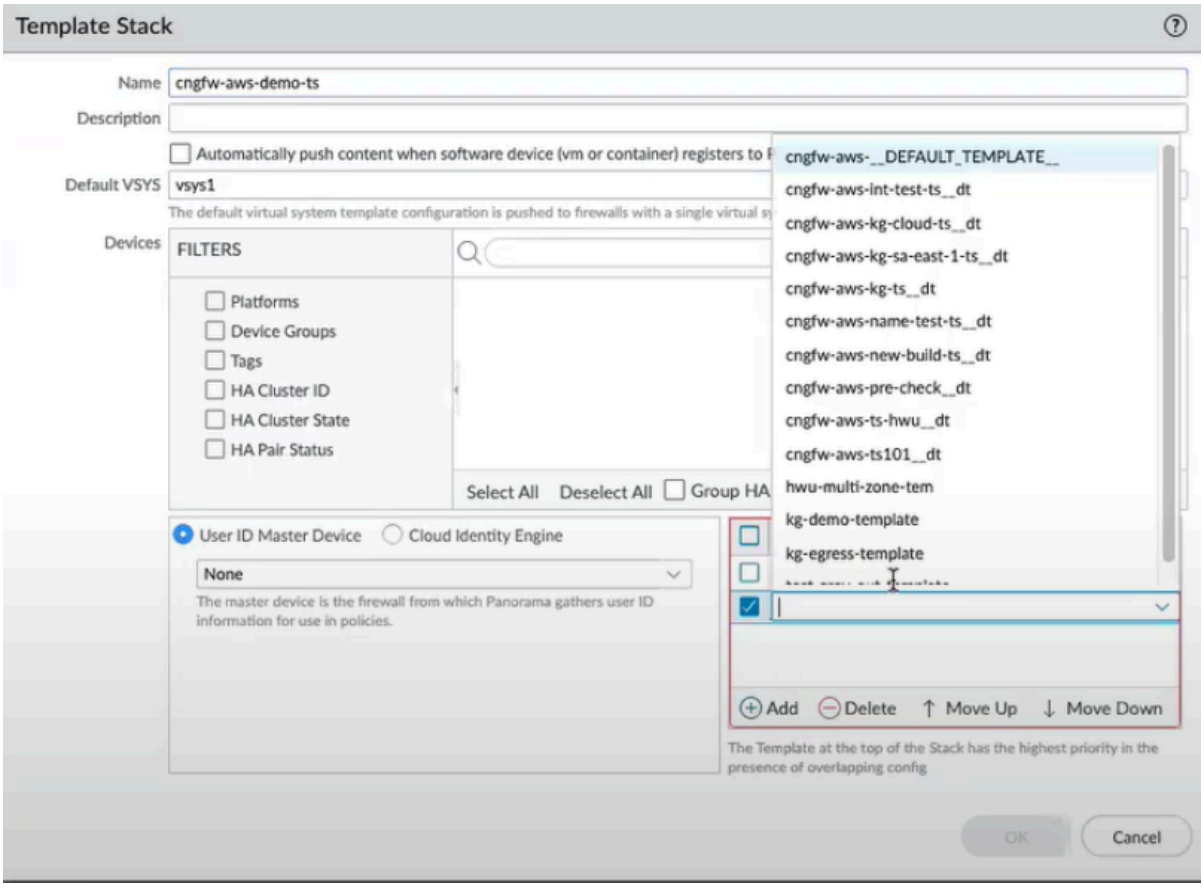
STEP 2 | Accédez à **Panorama > Templates (Modèles)**, puis sélectionnez votre **Template Stack (Pile de modèles)**.

Le plug-in AWS associe la pile de modèles à votre groupe d'appareils cloud. Le plug-in AWS crée un modèle par défaut et ajoute les zones **Public (Publiques)** et **Private (Privées)** à ce modèle par défaut.

Dans la section **Templates (Modèles)**, vous pouvez voir le modèle par défaut créé par le plug-in AWS. Ce modèle portera le même nom que votre pile de modèles, mais avec le suffixe `__dt`.



STEP 3 | Vous pouvez également référencer vos autres modèles Panorama dans la liste de la pile de modèles. Pour ce faire, cliquez sur **Add (Ajouter)**, puis sélectionnez le modèle.



STEP 4 | Créez un profil de protection de zone et associez-le aux zones **Private (Privées)** et **(Public) (Publiques)** par défaut de votre modèle par défaut. Pour créer le profil de protection de zone :

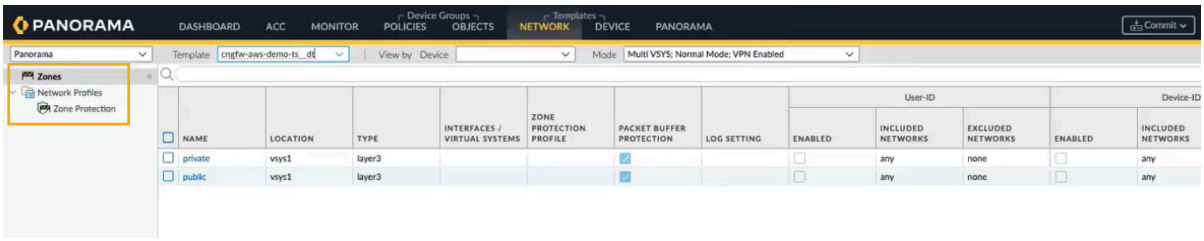
1. Dans la console Panorama, accédez à **Network (Réseau)** > **Zone Protection (Protection de zone)**.
2. Cliquez sur **Add (Ajouter)**.
3. Remplissez les champs **Name (Nom)** et **Description** du profil de protection de zone.
4. Sélectionnez les services de protection de zone.
5. Cliquez sur **OK**.

Après avoir créé les profils de protection de zone, procédez comme suit pour associer les zones **Private (Privées)** et **Public (Publiques)** de votre modèle par défaut :

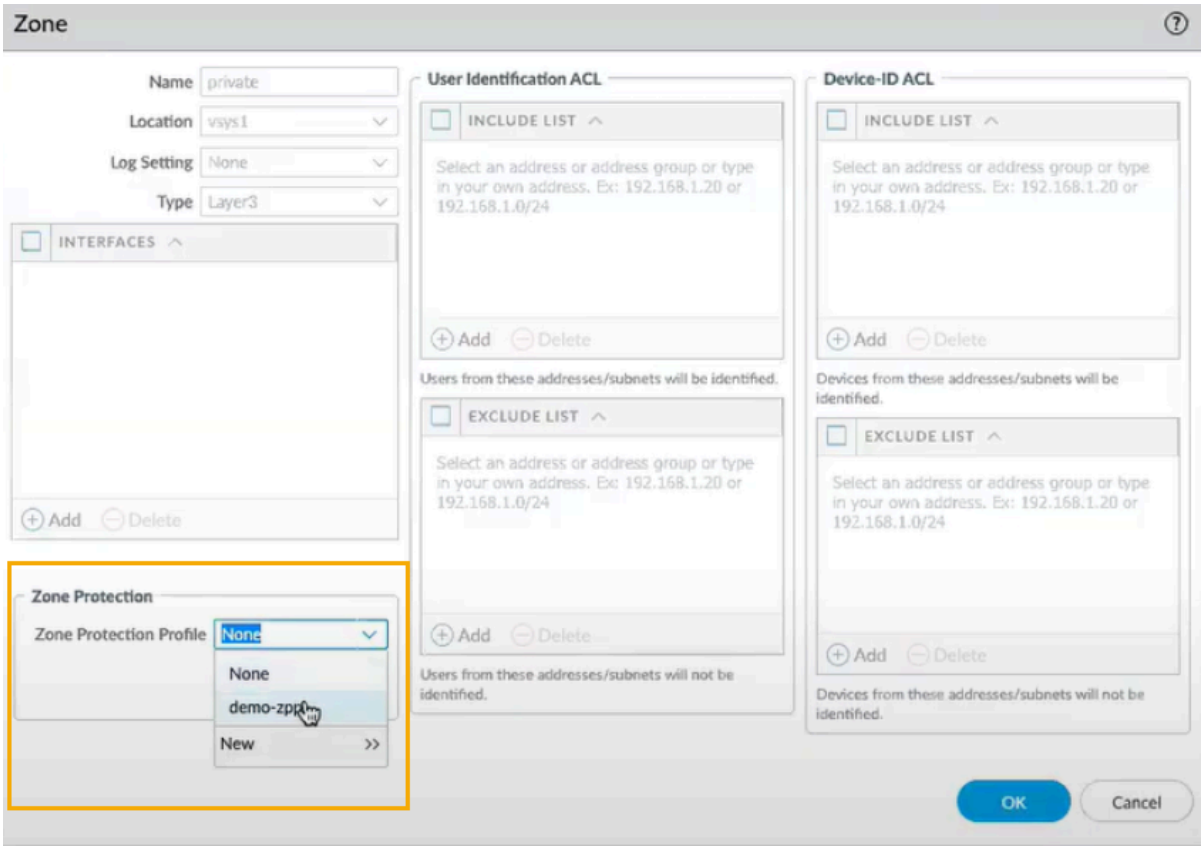
STEP 5 | Dans la console Panorama, sélectionnez l’onglet **Networks (Réseaux)**.

STEP 6 | Sélectionnez votre **Template (Modèle)**.

STEP 7 | Accédez à **Zones**.



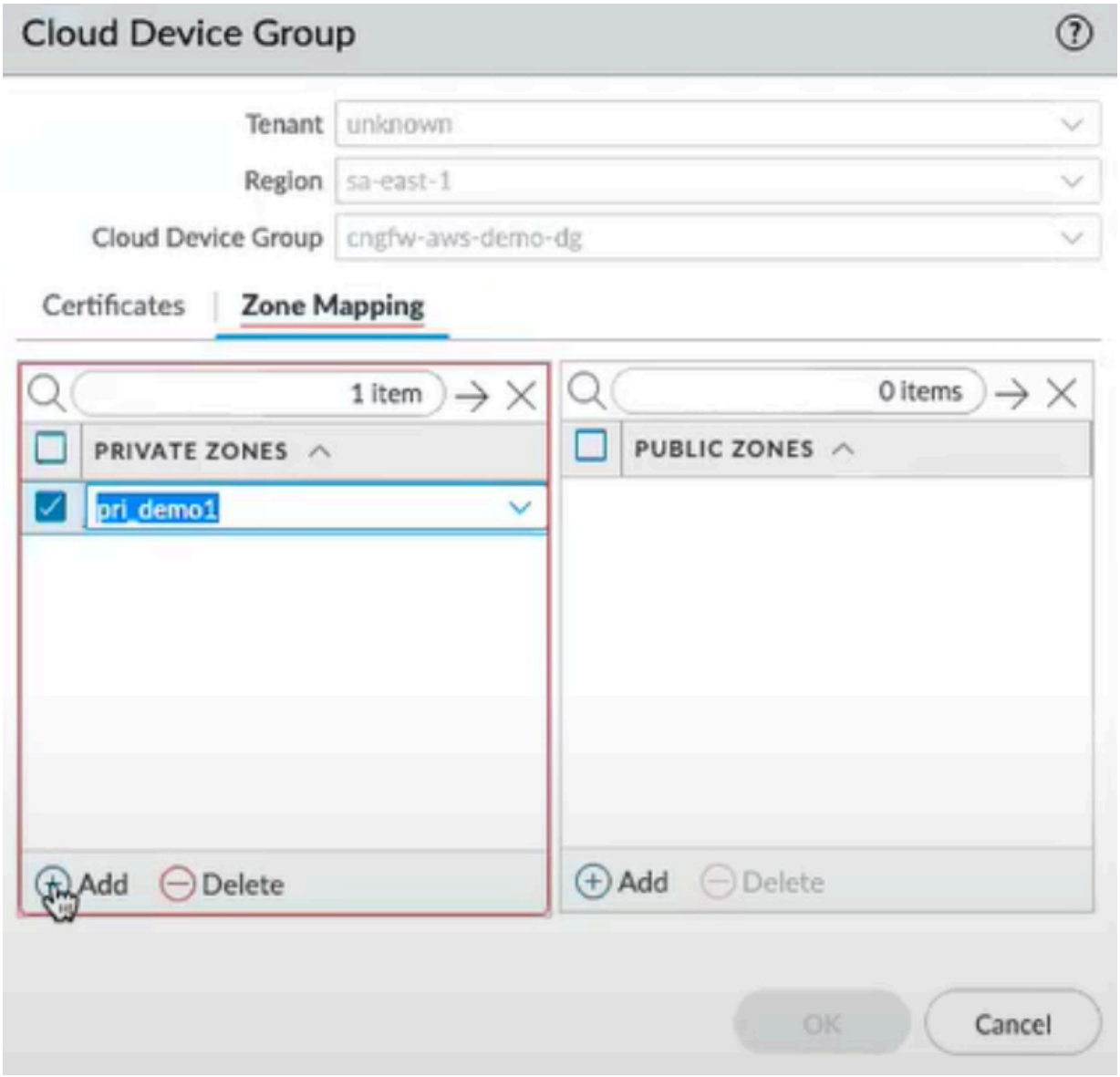
STEP 8 | Cliquez sur **Private (Privées)** et sélectionnez le **Zone Protection Profile (Profil de protection de zone)** pour votre **Private Zone (Zone privée)**.



STEP 9 | Cliquez sur **Public (Publiques)** et sélectionnez le **Zone Protection Profile (Profil de protection de zone)** pour votre zone **Public (Privée)**.

STEP 10 | Revenez au groupe d’appareils cloud. Accédez à l’onglet **Zone Mapping (Mappage de zones)**.

Vous pouvez voir la liste des modèles Panorama que vous avez référencés dans la liste de la pile de modèles. Vous pouvez mapper les zones Panorama aux zones **Private (Privées)** et **Public (Publiques)** par défaut que le plug-in AWS a créées.



STEP 11 | Configurez des règles de politique de sécurité pour les groupes d’appareils cloud dans Panorama. Vous pouvez ensuite utiliser les zones de sécurité Panorama mappées ci-dessus ou les zones **Private**

(Privées) ou **Public (Publiques)** par défaut dans vos politiques de sécurité en tant que zones source ou de destination. Pour en savoir plus, consultez la section Appliquer la politique.

Les règles de politique basées sur les zones autorisées dans les groupes d'appareils cloud Panorama sont les suivantes : privée vers publique, publique vers privée, privée vers privée, n'importe laquelle vers n'importe laquelle, privée vers n'importe laquelle. Les autres combinaisons de zones de sécurité source et de destination ne sont pas prises en charge dans vos règles de sécurité.

STEP 12 | Sélectionnez **Commit (Valider)** et **Push (Pousser)** pour valider et transmettre les modifications sur Panorama.

STEP 13 | Connectez-vous à la console Cloud NGFW pour vérifier le fichier XML contenant le mappage de zones **Private (Privées)** et **Public (Publiques)** qui a été transmis de Panorama au groupe d'appareils cloud respectif.

STEP 14 | Accédez à **Rulestacks**, sélectionnez votre groupe d'appareils cloud, puis cliquez sur **View XML (Afficher XML)** pour afficher des informations sur les zones **Private (Privées)** et **Public (Publiques)** nouvellement ajoutées de Panorama au groupe d'appareils cloud.

À l'aide des étapes indiquées dans la procédure ci-dessus, vous pouvez également configurer des règles de politique basées sur les zones pour vos groupes d'appareils cloud existants en ajoutant les modèles existants à partir de la pile de modèles, puis configurer des règles de politique de sécurité pour ces groupes d'appareils cloud dans Panorama.

Gestion des politiques de Strata Cloud Manager

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

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 web 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 abandonnée dans une ressource Cloud NGFW gérée par SCM.
- La fonctionnalité X-Fowarded 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.
- La DLP n'est pas prise en charge.
- Lors de la configuration de règles de sécurité pour votre ressource Cloud NGFW gérée par SCM, vous devez spécifier **ANY (INDIFFÉRENT)** pour la règle de sécurité. Cependant, la zone **from/to (de/à)** s'affiche comme la **data Zone (Zone de données)** dans le service de journalisation Strata.

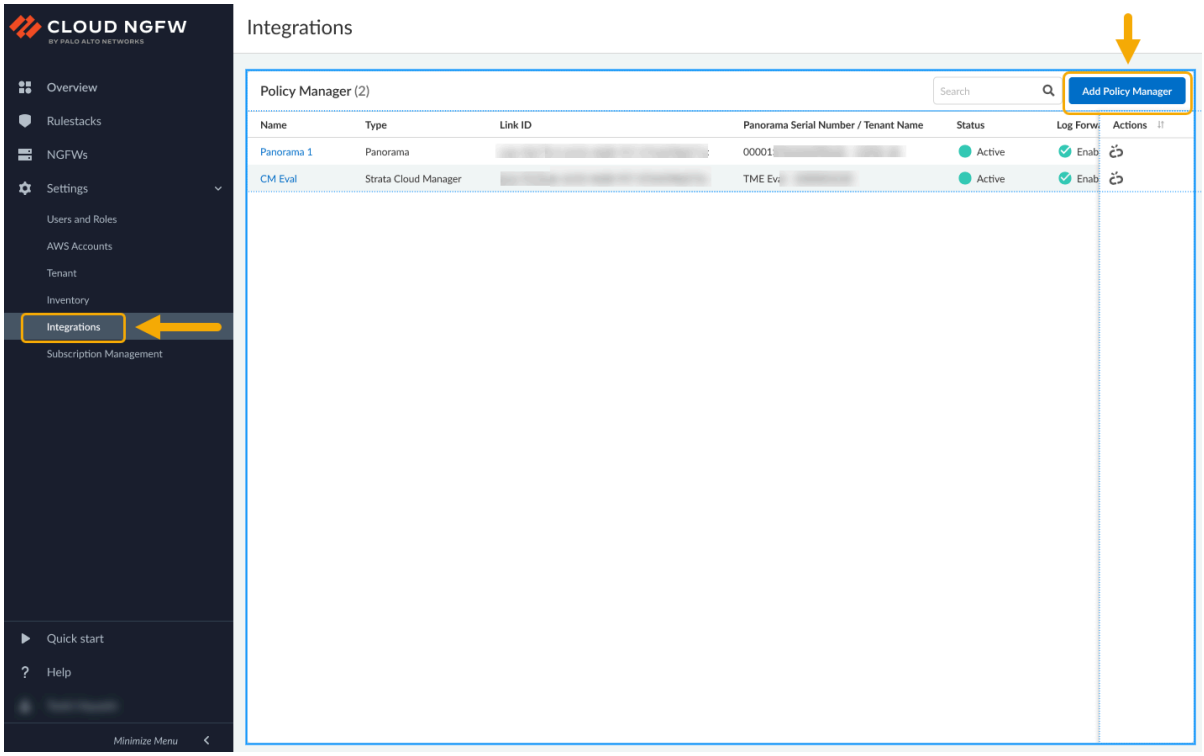
Lier votre ressource Cloud NGFW à la gestion des politiques de Strata Cloud Manager

Pour intégrer votre ressource Cloud NGFW à la gestion des politiques de Strata Cloud Manager :

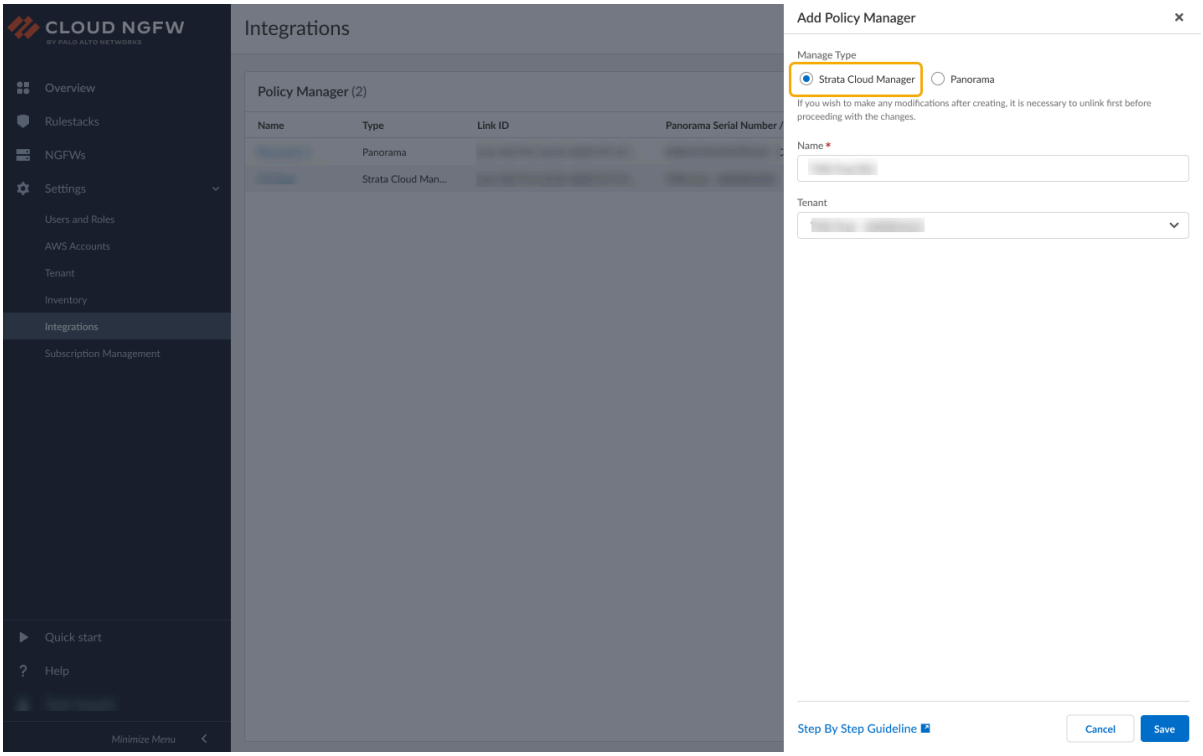
STEP 1 | Connectez-vous à la console Cloud NGFW.

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)**.



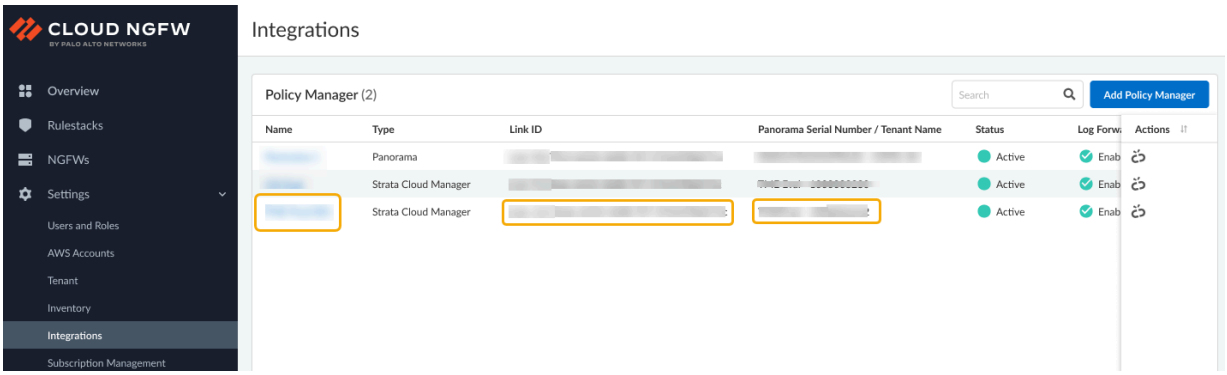
STEP 5 | Saisissez un nom descriptif.

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.

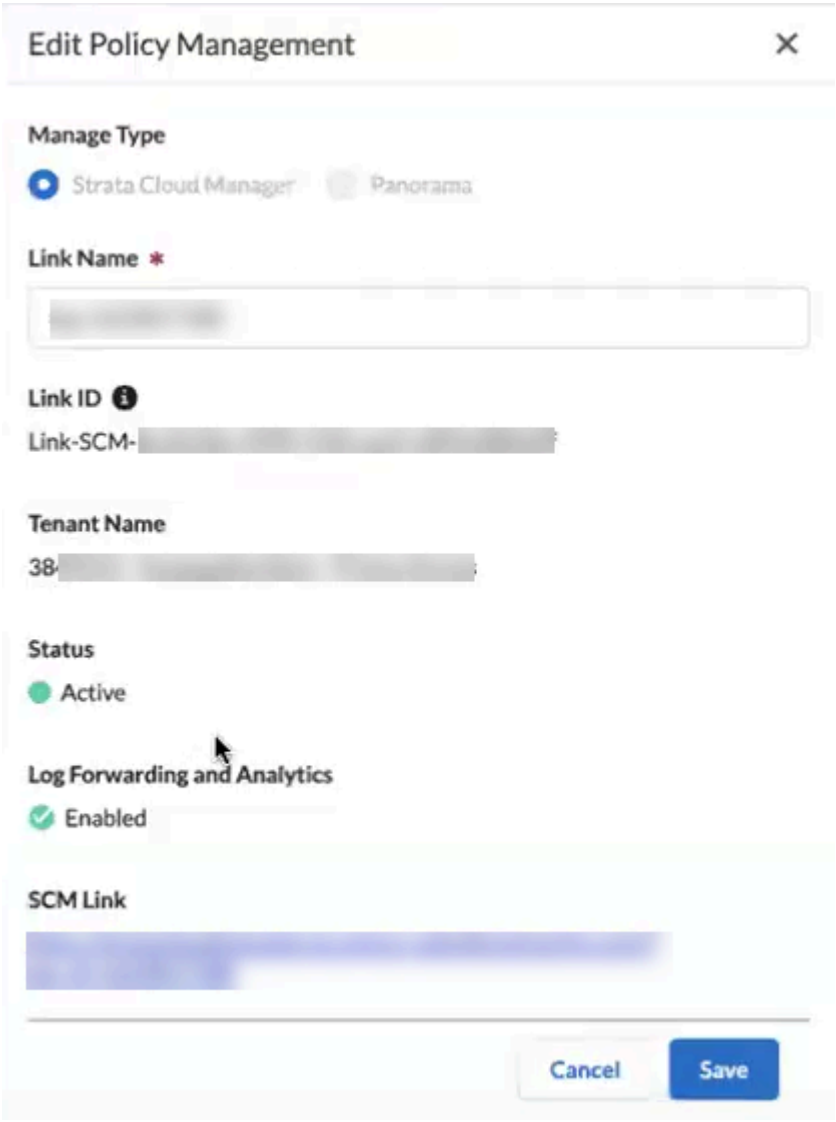
STEP 7 | Cliquez sur **Save (Enregistrer)**. Cela permet de relier efficacement votre ressource Cloud NGFW au locataire SCM.

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 et le 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 :



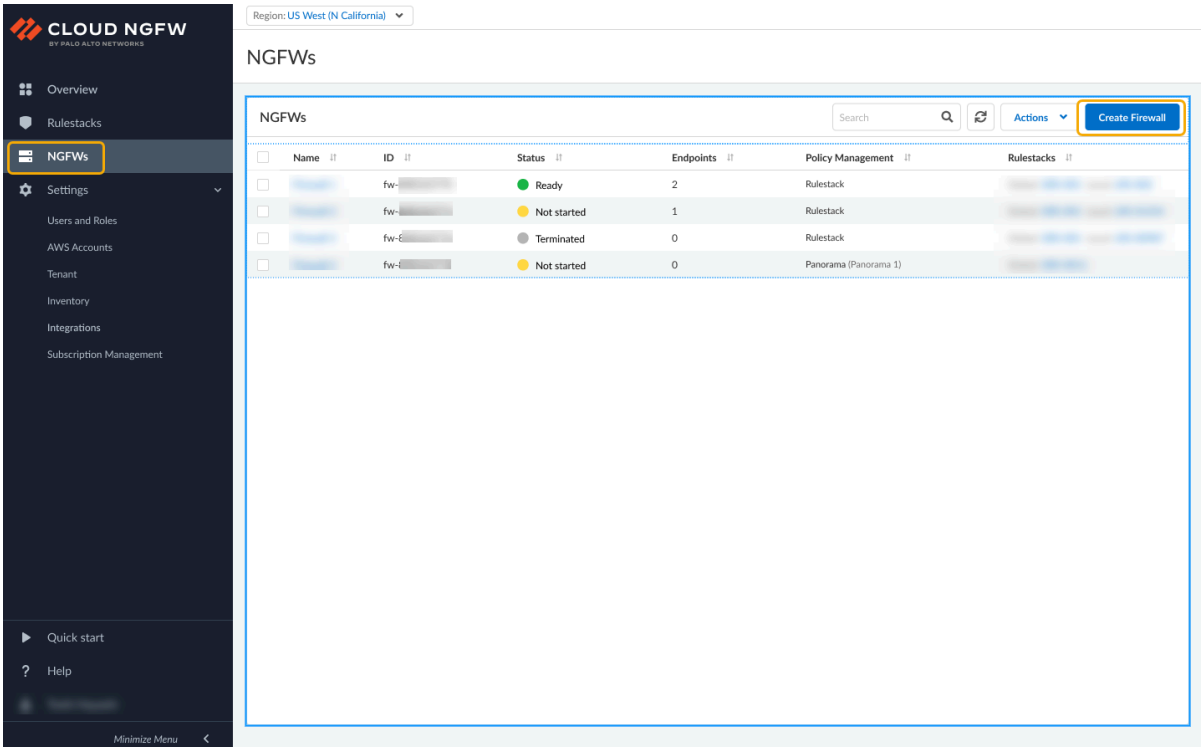
Associer un pare-feu à la gestion des politiques de Strata Cloud Manager

Après avoir établi un lien vers la gestion des politiques de Strata Cloud, vous pouvez associer un nouveau pare-feu au locataire SCM lié :

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

STEP 2 | Sélectionnez **NGFWs (NGFW)**.

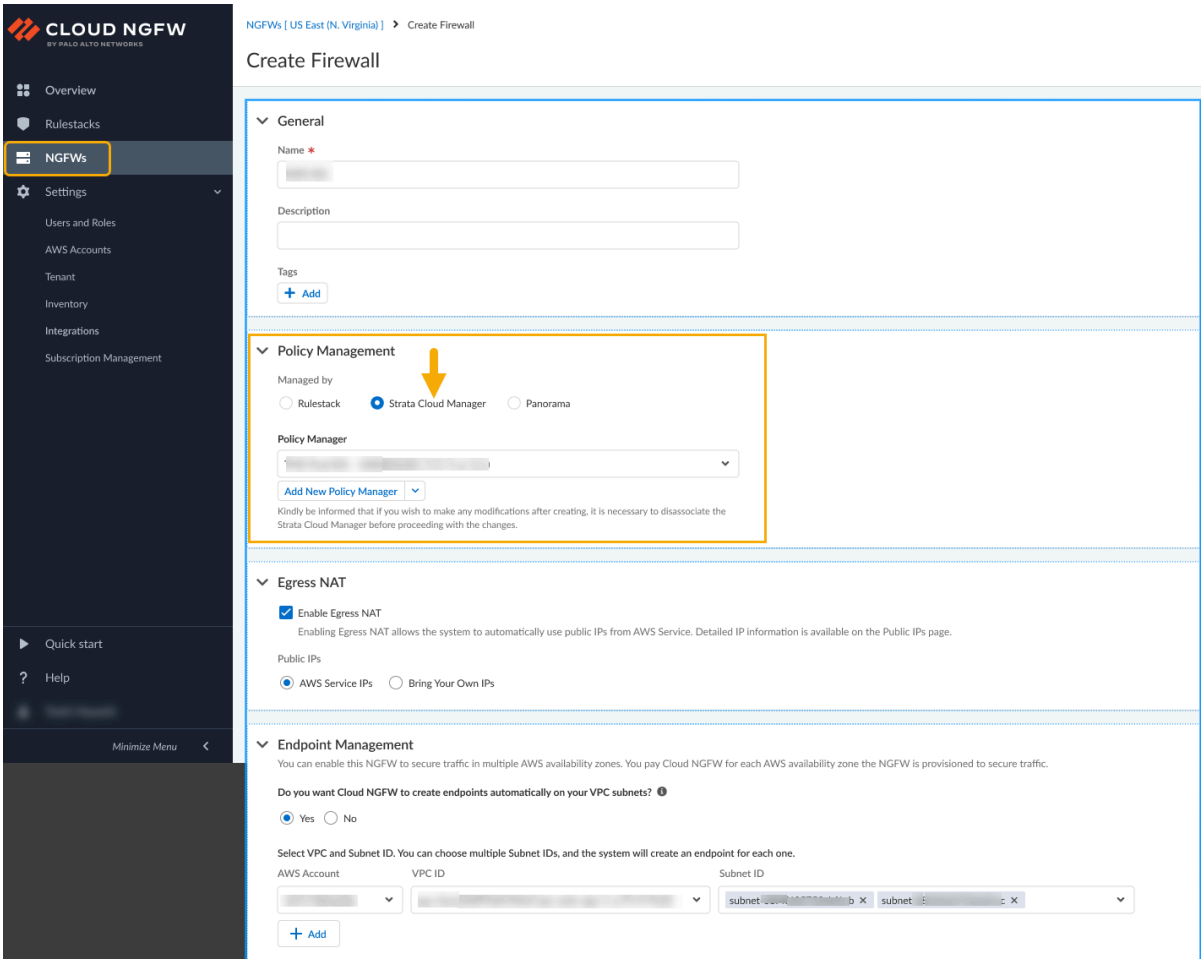
STEP 3 | Cliquez sur **Create Firewall (Créer un pare-feu)**.



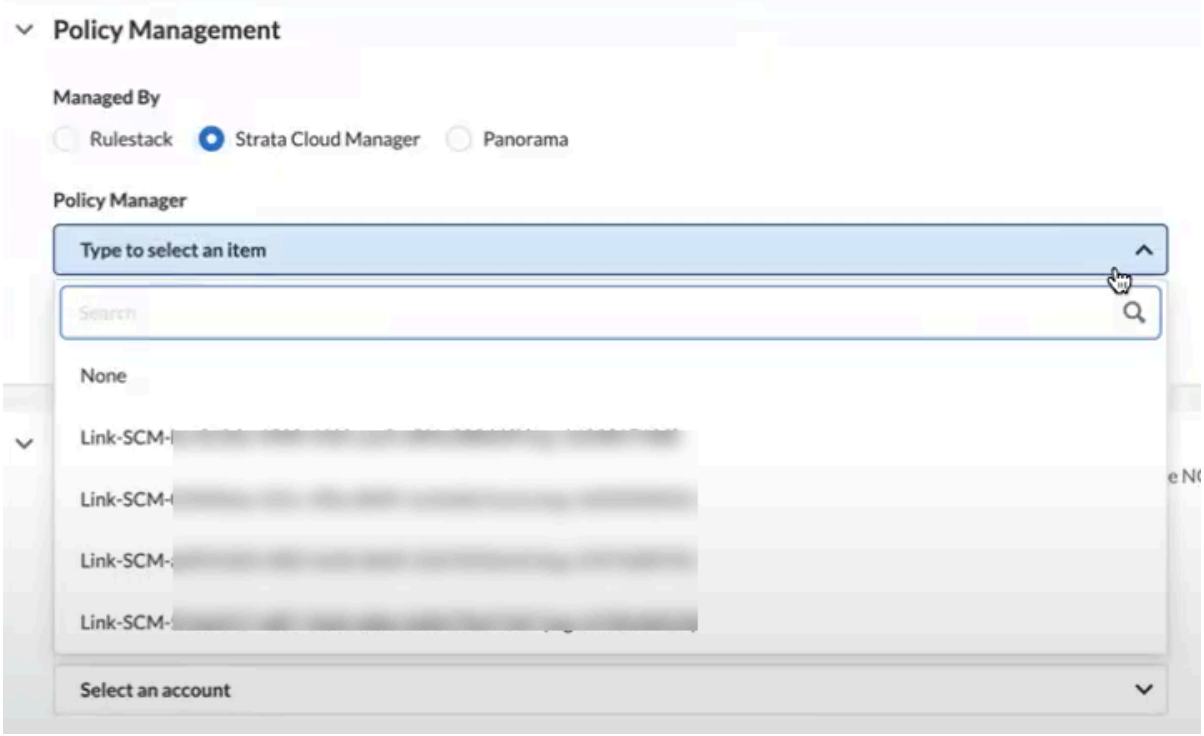
STEP 4 | Dans l’écran **Create Firewall (Créer un pare-feu)**, saisissez un nom pour le pare-feu.

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.



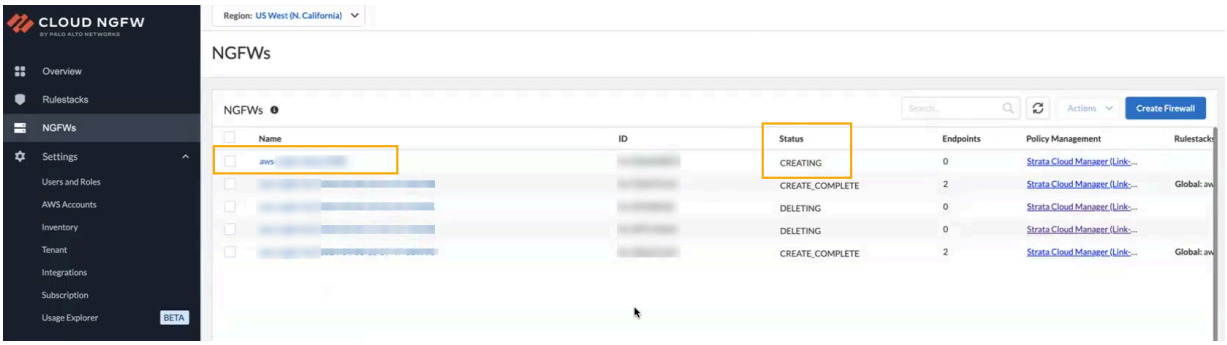
STEP 8 | Configurez **Endpoint Management (Gestion des terminaux)** pour sécuriser le trafic dans plusieurs zones de disponibilité AWS.

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*.

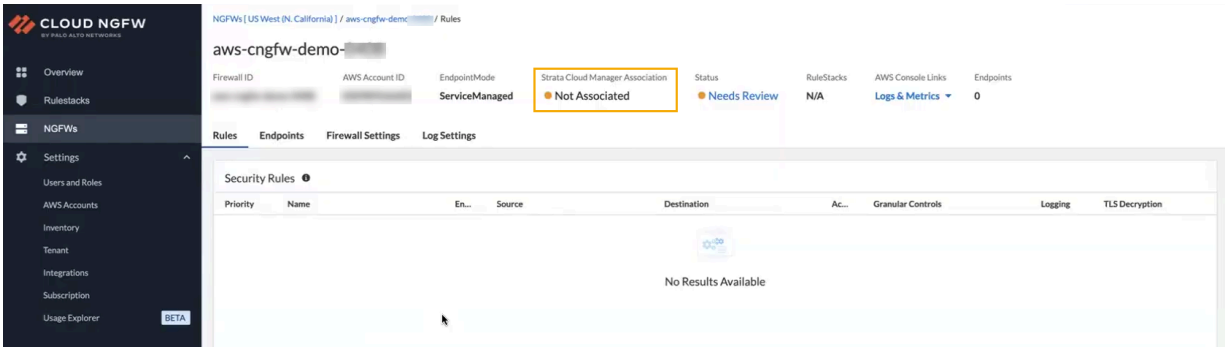
   Par défaut, la ressource Cloud NGFW ne crée pas ces terminaux automatiquement ; le bouton radio est réglé sur ***No (Non).***

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. 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.

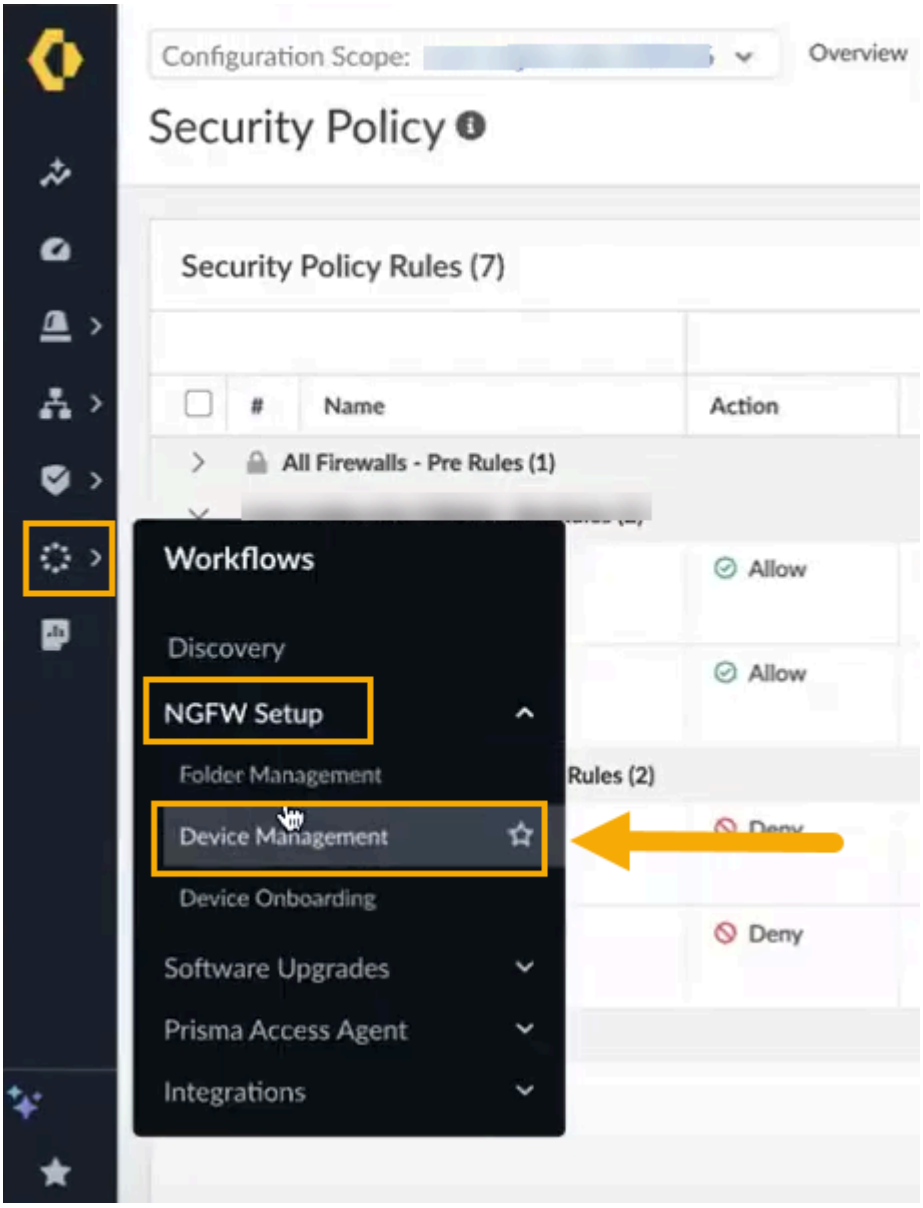
*Quand vous vous connectez à Strata Cloud Manager, le tableau de bord ne parvient pas à afficher le nombre de Cloud NGFW sous **NGFW > Software (Logiciel)**.*

STEP 1 | Connectez-vous à l'application Strata Cloud Manager depuis le hub Palo Alto Networks directement sur le site stratacloudmanager.paloaltonetworks.com.

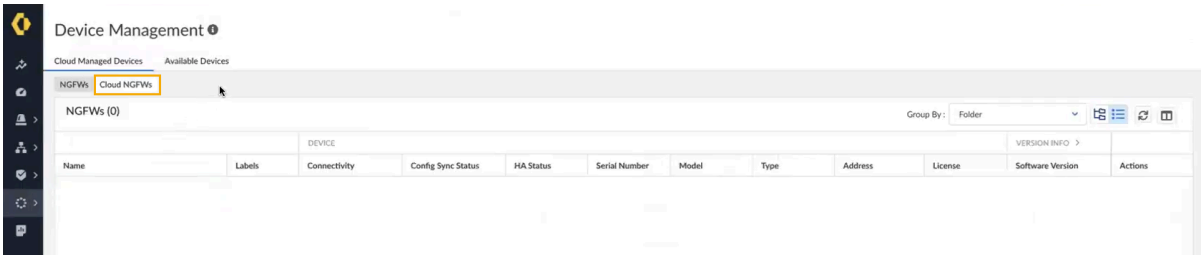
STEP 2 | Dans l’interface Strata Cloud Manager, recherchez votre locataire Cloud NGFW en utilisant l’option de navigation de gauche :

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 de son *identifiant*.

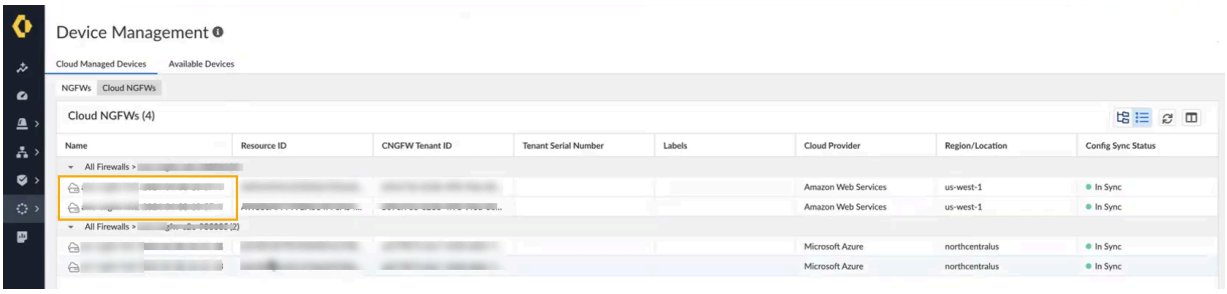
STEP 3 | Sélectionnez **Workflows (Flux de travail) > NGFW Setup (Configuration NGFW) > Device Management (Gestion des périphériques)** :



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 :



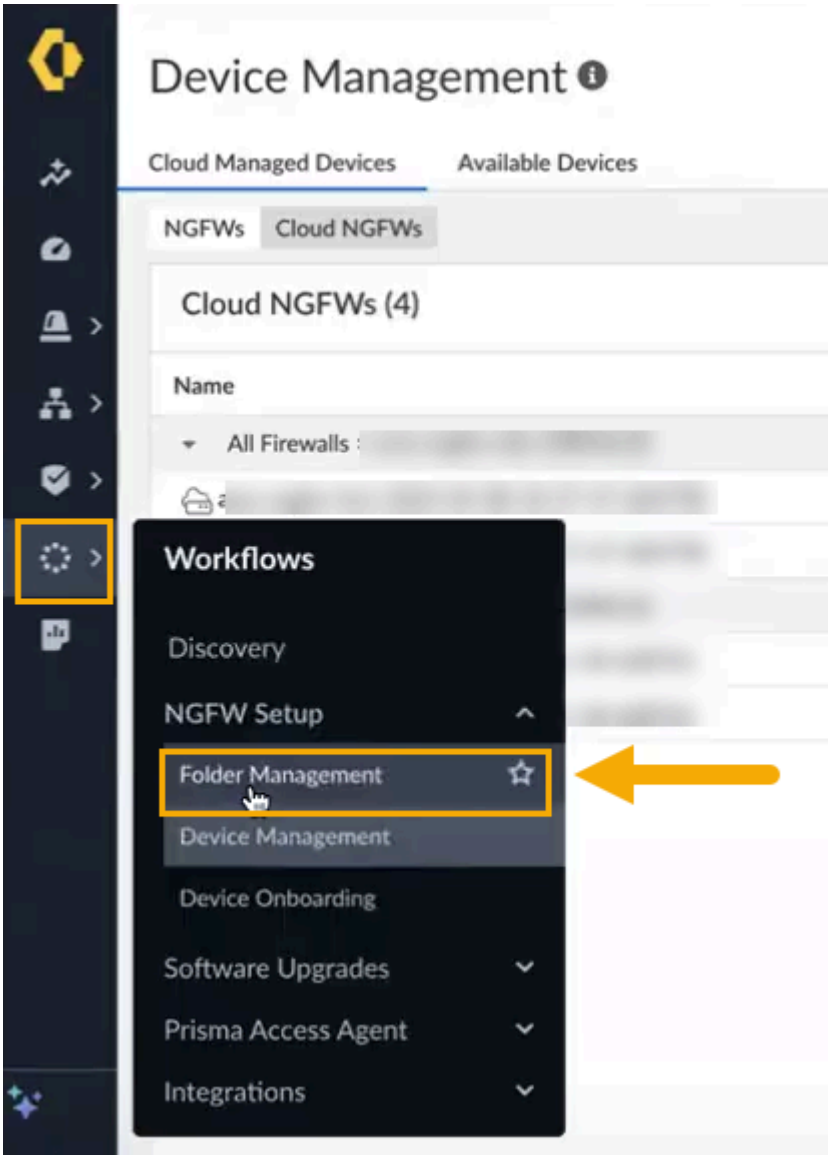
L’écran **Device Management (Gestion des périphériques)** affiche les ressources Cloud NGFW actuellement gérées par SCM :



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 et 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)** :



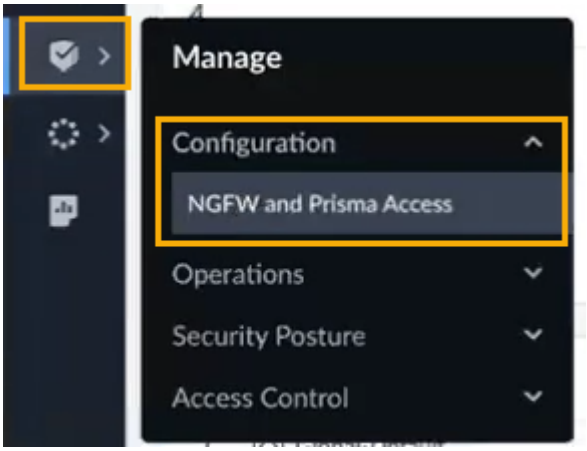
L’écran **Folder Management (Gestion des dossiers)** affiche les ressources Cloud NGFW associées au locataire SCM :

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.

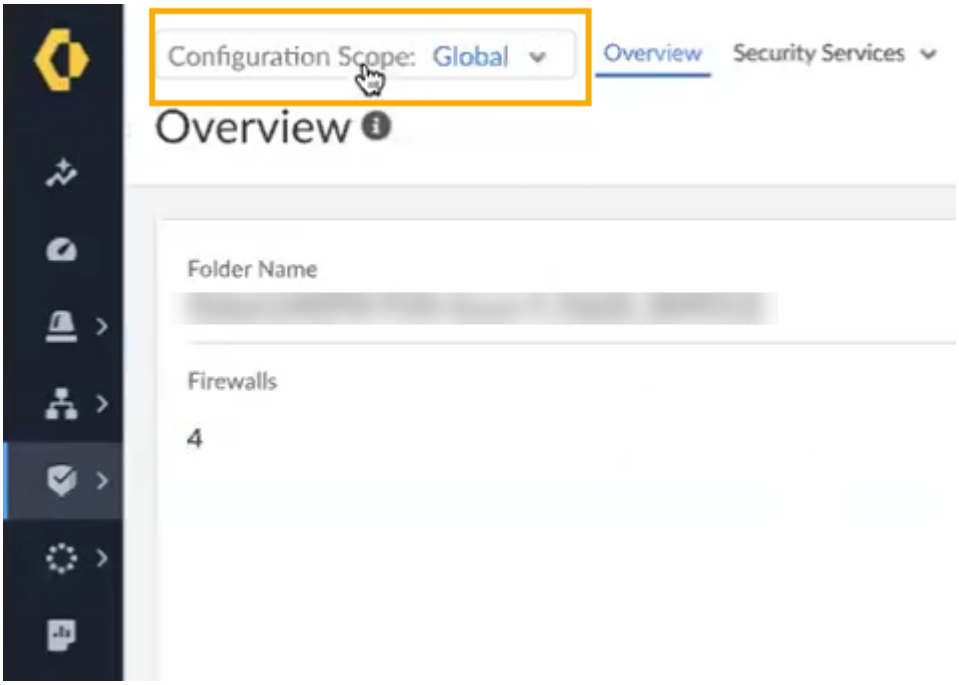
Utiliser Strata Cloud Manager pour la gestion des politiques Cloud NGFW

Vous pouvez utiliser Strata Cloud Manager pour appliquer globalement des règles de politique de sécurité aux ressources Cloud NGFW dans un dossier.

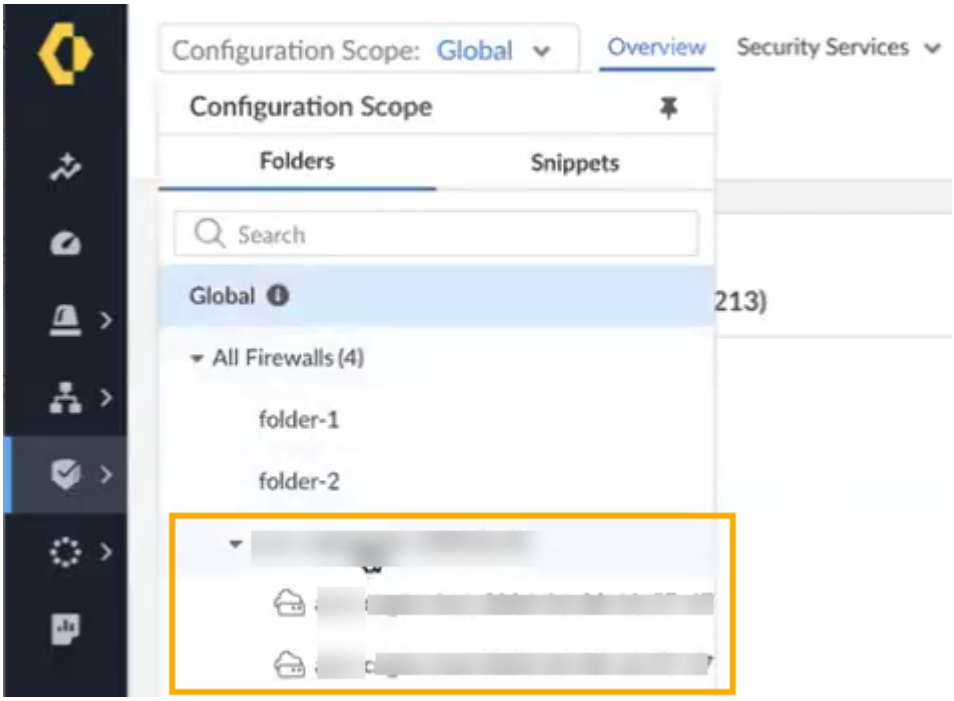
STEP 1 | Dans Strata Cloud Manager, sélectionnez **Manage (Gérer) > Configuration > NGFW and Prisma Access (NGFW et Prisma Access)**.



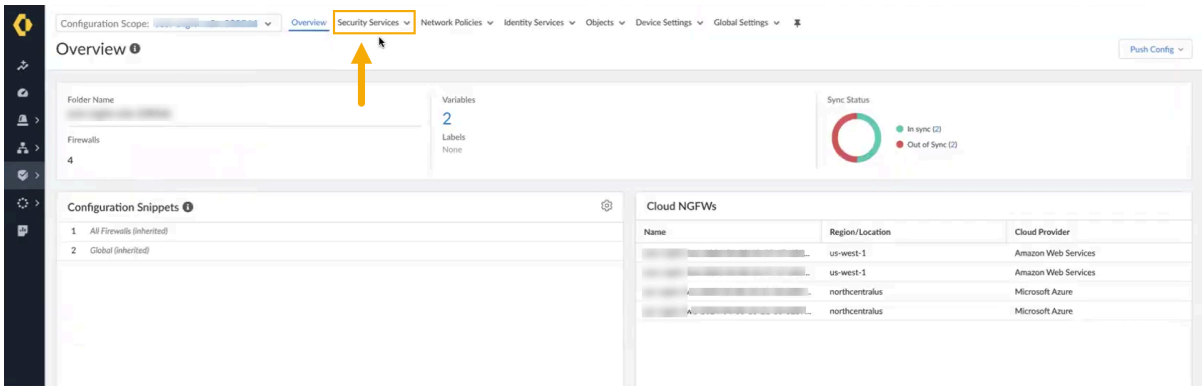
STEP 2 | Sélectionnez **Configuration Scope (Portée de la configuration)**.



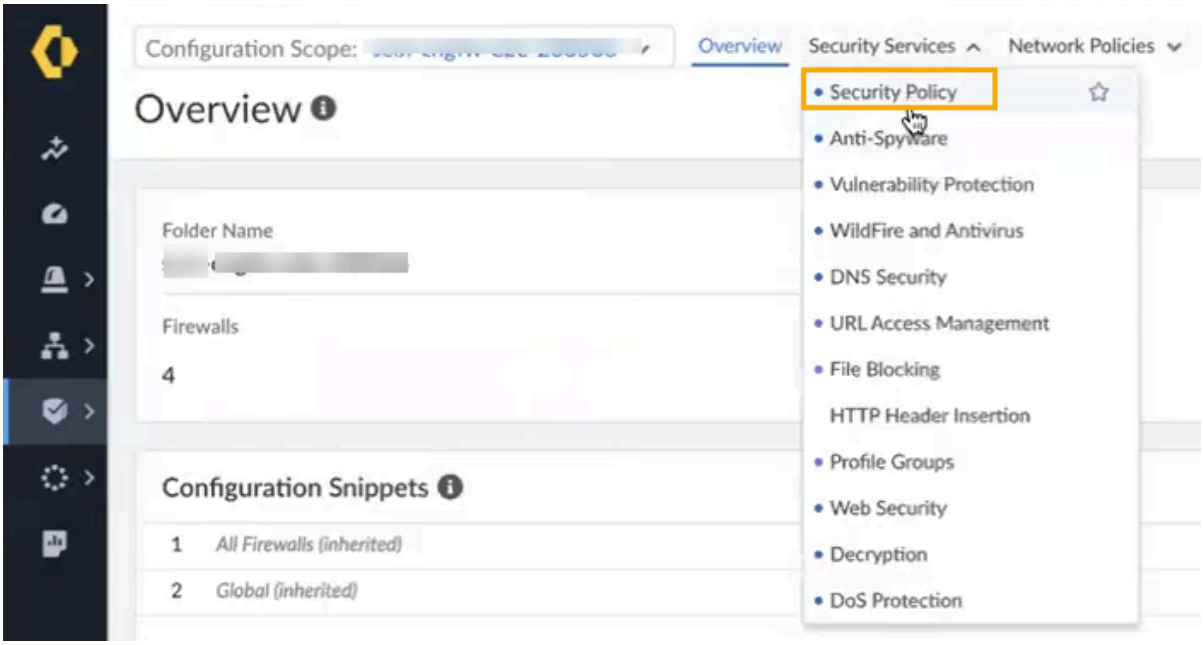
STEP 3 | Dans la liste déroulante, recherchez le dossier contenant les **Cloud NGFW AWS resources (Ressources Cloud NGFW AWS)** :



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 une ressource Cloud NGFW à l'aide de Strata Cloud Manager

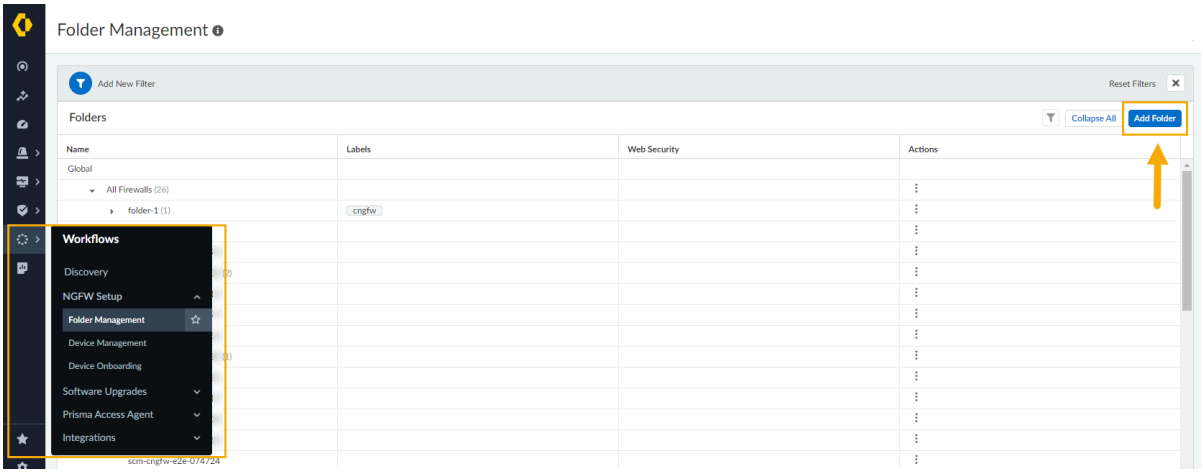
Après avoir configuré l'abonnement approprié pour utiliser le service Strata Cloud Manager pour votre ressource Cloud NGFW, créez un dossier pour afficher les données associées à votre pare-feu. Les dossiers sont utilisés pour effectuer un regroupement logique de vos pare-feu ou types de déploiement (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 :

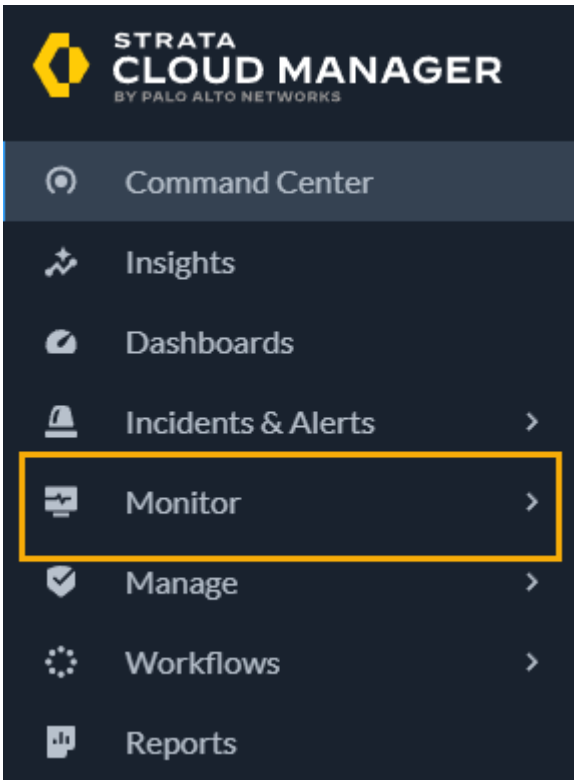
- les produits et abonnements que vous gérez à l’aide de Strata Cloud Manager.
- L’état de santé et de connectivité de vos périphériques Cloud NGFW.

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)** :



Surveiller

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

Bénéficiez d’une visibilité complète sur le trafic de votre réseau et sur les produits et abonnements que vous gérez avec Strata Cloud Manager. Vous pouvez surveiller de manière protectrice l’état de santé et de connectivité de vos réseaux distants, applications, périphériques NGFW et utilisateurs mobiles dans Prisma Access. Strata Cloud Manager fournit également des fonctionnalités permettant de surveiller les performances des services réseau courants et les détails de la consommation de vos licences d’abonnement, et de gérer l’outil utilisé pour analyser les problèmes de connectivité.

Pour anticiper les éventuels problèmes et accélérer la réponse aux incidents lorsque cela est nécessaire, le pare-feu fournit une intelligence sur les modèles de trafic et utilisateur ainsi que des rapports personnalisés et instructifs. Le tableau de bord, l'Application Command Center (Centre de commande des applications ; ACC), les rapports et les journaux sur le pare-feu vous permettent de surveiller l'activité sur votre réseau. Vous pouvez contrôler les journaux et filtrer les informations afin de générer des rapports avec des vues prédéfinies ou personnalisées. Par exemple, utiliser les modèles prédéfinis pour générer des rapports sur les activités d'un utilisateur ou analyser les rapports et les journaux afin d'interpréter un comportement inhabituel sur votre réseau et générer un rapport personnalisé sur le modèle de trafic. Pour une présentation visuelle utile de l'activité réseau, le tableau de bord et l'ACC incluent des widgets, des graphiques et des tableaux avec lesquels vous pouvez interagir pour retrouver les informations dont vous avez besoin. Vous pouvez également configurer le pare-feu pour qu’il transfère les informations surveillées en tant que notifications par e-mail, messages Syslog, pièges SNMP et enregistrements NetFlow à des services externes.

Afficher les journaux nativement dans AWS

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

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 logiciel malveillant, ou une attaque DoS qui correspond aux seuils configurés pour le déclenchement d’une activité d’analyse des ports ou 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 admin Tenet à 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 que les journaux NGFW soient correctement capturés.

Le groupe de journaux CloudWatch, le compartiment S3, l’espace de noms CloudWatch et le flux Kinesis doivent être précréés dans le modèle CloudFormation (CFT).

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 logiciel malveillant ou un logiciel espion) ;

description ou URL de la menace (colonne Name (Nom)) ; action d’alerte (par exemple autorisation ou blocage) ; et 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, comme celles qui affectent les installations par défaut de logiciels déployés à grande échelle, qui mènent à la compromission à la racine des serveurs et qui rendent le code d’exploitation largement accessible aux attaquants. Le pirate n'a généralement pas besoin d'informations d'authentification spéciales ni de connaissances relatives à chaque victime, et la cible n'a pas besoin d'être manipulée au point d'effectuer des fonctions spéciales.
Élevée	Menaces pouvant devenir critiques, mais ayant des facteurs atténuants. Par exemple, elles peuvent être difficiles à exploiter, ne mènent pas à des privilèges élevés ou ne ciblent pas un grand nombre de victimes.
Moyenne	Menaces mineures pour lesquelles l’incidence est minimalisée, comme les attaques DoS qui ne compromettent pas la cible ou les exploitations nécessitant qu’un attaquant réside sur le même réseau local que la victime, qui affectent uniquement les configurations non standard ou des applications peu courantes, ou qui 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 des entrées pour les communications TLS ayant échoué 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 pouvez choisir entre trois destinations 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, il vous est demandé de 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 S3 Bucket (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.

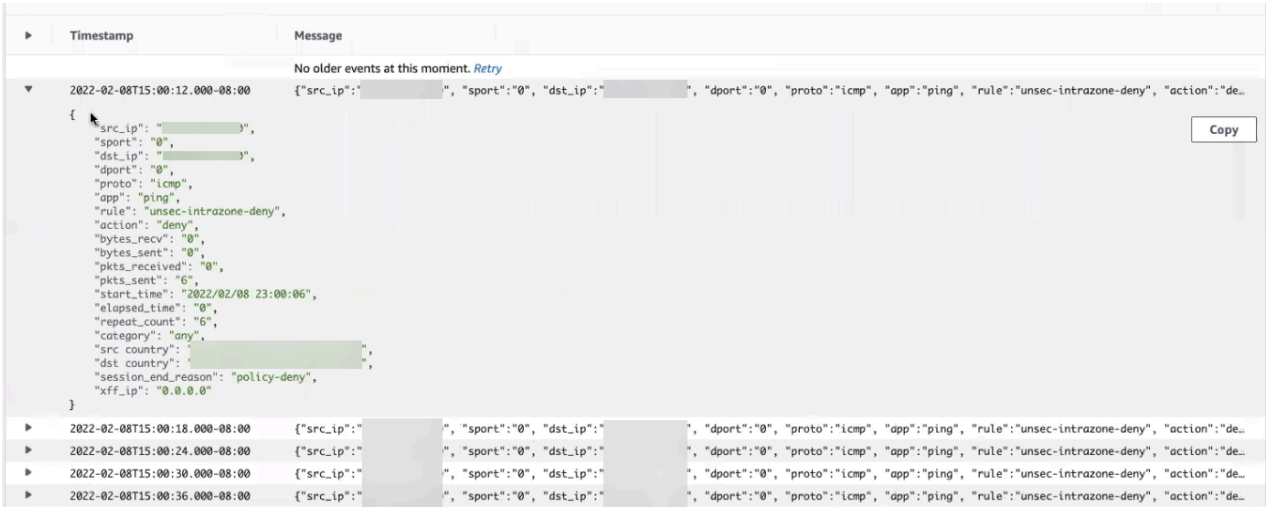
Si vous envoyez les journaux à un groupe de journaux CloudWatch, vous pouvez afficher les entrées de journal directement dans la console AWS CloudWatch. Dans le groupe de journaux de configuration CloudWatch que vous spécifiez lors de la configuration de la journalisation, vous verrez une liste de flux de journaux. Le nom du flux de journaux se présente 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.Twenty-three

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

Vous pouvez cliquer sur le nom du flux pour consulter 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. Le 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 suivent le 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 facile à lire. 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 vous 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

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

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)	Un identificateur numérique interne est 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

Nom du champ	Description
	• 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.
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)	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 la session lorsqu’elle utilise l’authentification du client ou qu’elle utilise un certificat du serveur ayant l’une 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

Nom du champ	Description
	pris en charge), certificate_revoked (certificat révoqué), access_denied (accès refusé), ou no_certificate_RESERVED (aucun certificat réservé) (uniquement SSLv3). • decrypt-unsupport-param : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise une version de protocole, un chiffrement ou un algorithme SSH 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 l'établissement de liaison). • decrypt-error : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque des ressources du pare-feu sont 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

Nom du champ	Description
	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

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

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)	Un identificateur numérique interne est 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

Nom du champ	Description
	• deny : mécanisme de détection de saturation activé et rejet du trafic en fonction de la configuration • drop : menace détectée et session associée abandonnée • 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 abandon aléatoire du paquet • sinkhole : mise en entonnoir DNS activée • syncookie-sent : alerte syncookie • block-continue (sous-type d'URL uniquement) : une requête HTTP est bloquée et redirigée vers une page Continuer sur laquelle se trouve un bouton de confirmation permettant de continuer • 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 code secret de l'administrateur du pare-feu pour pouvoir continuer • 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) : fichier bloqué par le pare-feu et chargé 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 : modèle de données correspondant à un profil de filtrage des données.

Nom du champ	Description
	• file : type de fichier correspondant à un profil de blocage des fichiers. • flood : saturation détectée via un profil de protection de zone. • packet : protection contre les attaques basées sur les paquets qui est déclenchée par un profil de protection de zone. • scan : analyse détectée via un profil de protection de zone. • spyware : logiciel espion détecté via un profil anti-espion. • url : journal de URL Filtering • ml-malware : logiciel malveillant détecté par WildFire Inline ML via un profil antivirus. • Malware : logiciel malveillant détecté via un profil antivirus. • vulnerability : exploitation de vulnérabilités détectée via un profil de protection contre les vulnérabilités. • wildfire : un verdict WildFire généré lorsque le pare-feu envoie un fichier à WildFire conformément à un profil d'analyse WildFire et un verdict (logiciel malveillant, hameçonnage, logiciel indésirable ou bénin, selon les informations que vous consignez) est consigné dans le journal des envois WildFire. • wildFire®malware : logiciel malveillant 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 URL Filtering • 10000-19999 : détection de logiciel espion de type « phone home » • 20000-29999 : détection de téléchargement de logiciel espion • 30000-44999 : détection d'exploitation des vulnérabilités • 52000-52999 : détection de type de fichier • 60000-69999 : détection de filtrage des données

Nom du champ	Description
	Les plages d'ID de menace pour la détection des logiciels malveillants, le flux de signature WildFire et les signatures DNS C2 utilisées dans les versions précédentes ont été remplacées par des ID uniques universels permanents. Consultez les noms de champ Type de menace/contenu (sous-type) et Catégorie de menace (thr_category) pour créer des rapports à jour et 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 au serveur ou serveur au 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 adresses IP de destination, application et type de contenu et 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 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

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

Le tableau suivant contient des informations sur les champs du journal de décryptage :

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)	Un identificateur numérique interne est 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 • 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.

Nom du champ	Description
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 for Forward Proxy (Transférer pour proxy de transfert)**, **Inbound for Inbound Inspection (Entrant pour inspection entrante)**, **No decrypt (Aucun décryptage)** pour le trafic non décrypté, GlobalProtect, etc. *Sélectionner **No Decrypt (Aucun décryptage)** plutôt que **None (Aucun)** entraînera un abandon du trafic.*
État de la chaîne (chain_status)	Si la chaîne est fiable. Les valeurs sont : • Non inspectée • Non approuvée • Fiable • Incomplet

Afficher les journaux du trafic et des menaces et l’activité dans Panorama

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

Afficher les journaux du Cloud NGFW dans Panorama

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

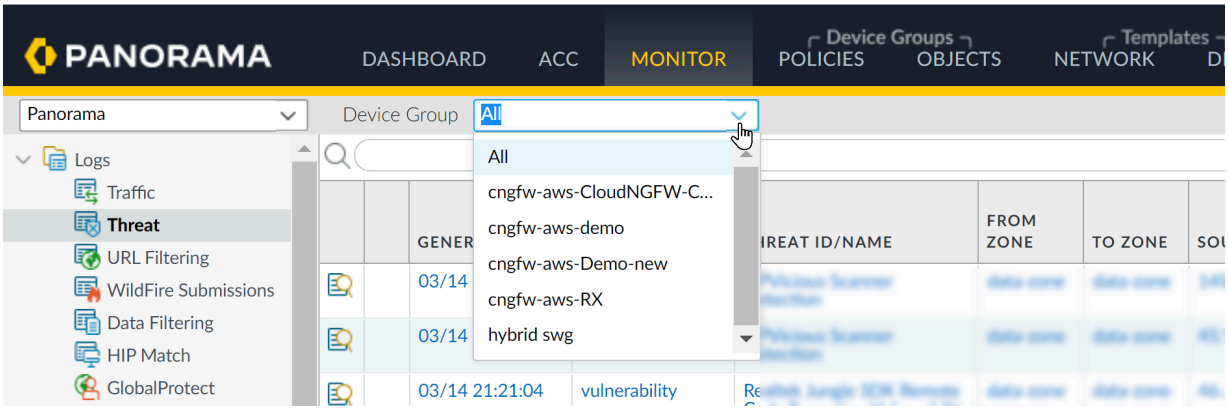
STEP 1 | Connectez-vous à Panorama.

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

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

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

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



Afficher l’activité du Cloud NGFW dans l’ACC

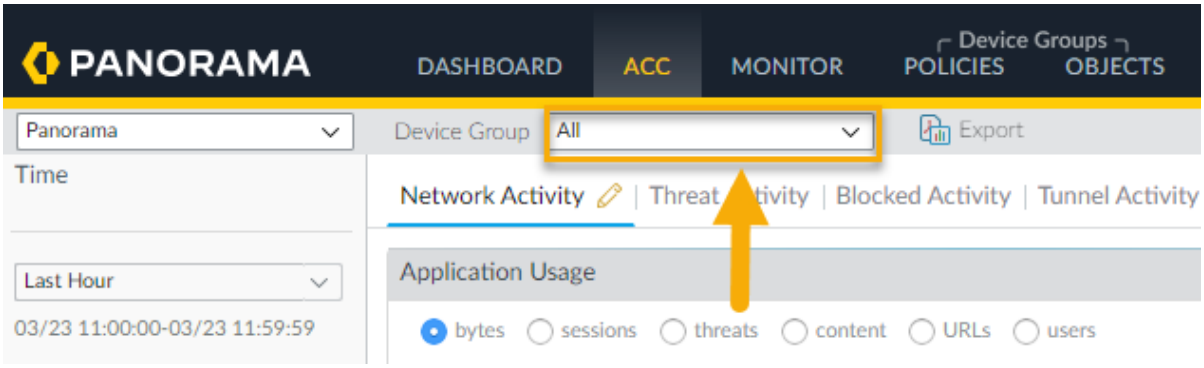
L’ACC est un outil analytique qui fournit des renseignements exploitables concernant l’activité sur votre réseau. L’ACC utilise les journaux du Cloud NGFW pour représenter graphiquement les tendances du trafic sur votre réseau. Cette représentation graphique vous permet d'interagir avec les données et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

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

STEP 1 | Connectez-vous à Panorama.

STEP 2 | Sélectionnez **ACC.**

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



STEP 4 | Vous pouvez utiliser un filtre Panorama pour afficher le journal d’un groupe d’appareils Cloud individuel. Recherchez le **Device Name (Nom du périphérique)**. Cliquez sur l’icône + dans la partie supérieure droite de l’interface Panorama pour ajouter un nouveau filtre. Saisissez le nom

du filtre, puis cliquez sur **Save (Enregistrer)**. Cliquez sur l’icône **Load Filter (Charger le filtre)**. Sélectionnez le filtre nouvellement créé pour afficher les journaux du groupe d’appareils Cloud individuel.

Afficher les journaux du trafic et des menaces dans le service de journalisation Strata

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

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 du service de journalisation Strata, vous pouvez afficher les journaux du trafic, des menaces et de décryptage générés par vos ressources Cloud NGFW.

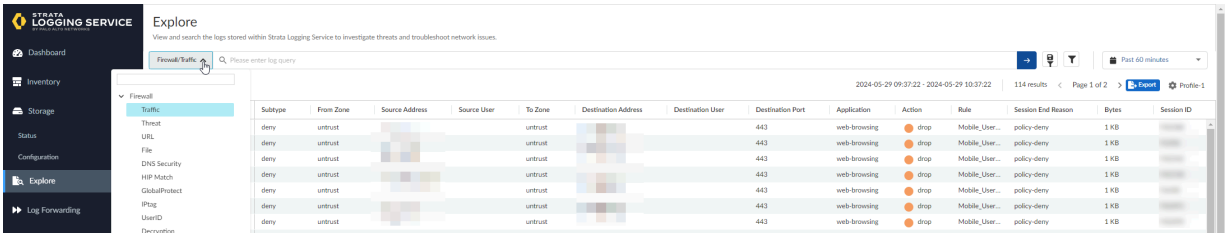
Si vous utilisez Panorama mais que vous n'utilisez pas le service de journalisation Strata pour la collecte de journaux, vous pouvez transférer les journaux à une autre entité. Cependant, vous devez activer le service de journalisation Strata dans votre profil de journalisation.

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.

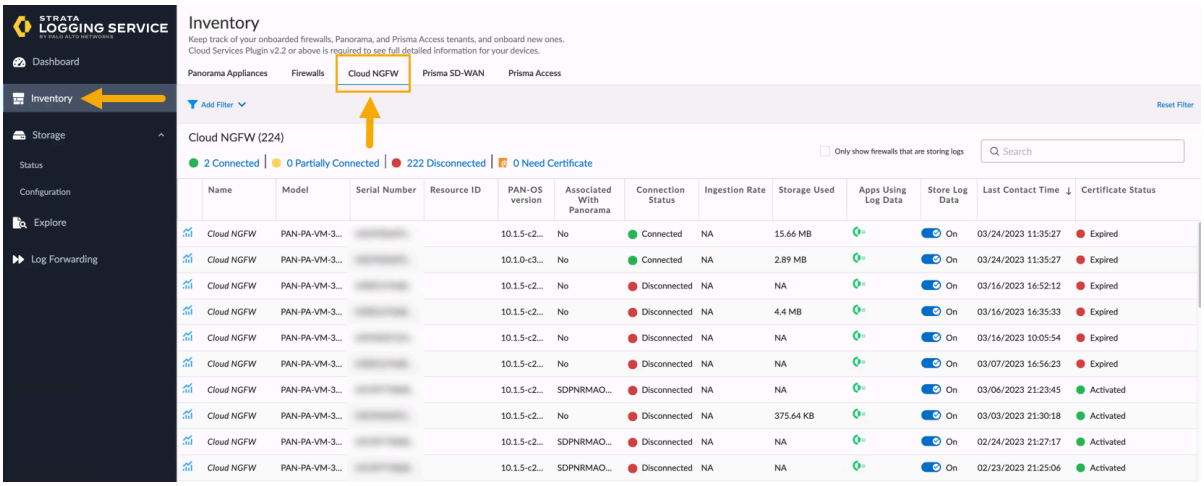
STEP 2 | Sélectionnez **Explore (Explorer)**.

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**.



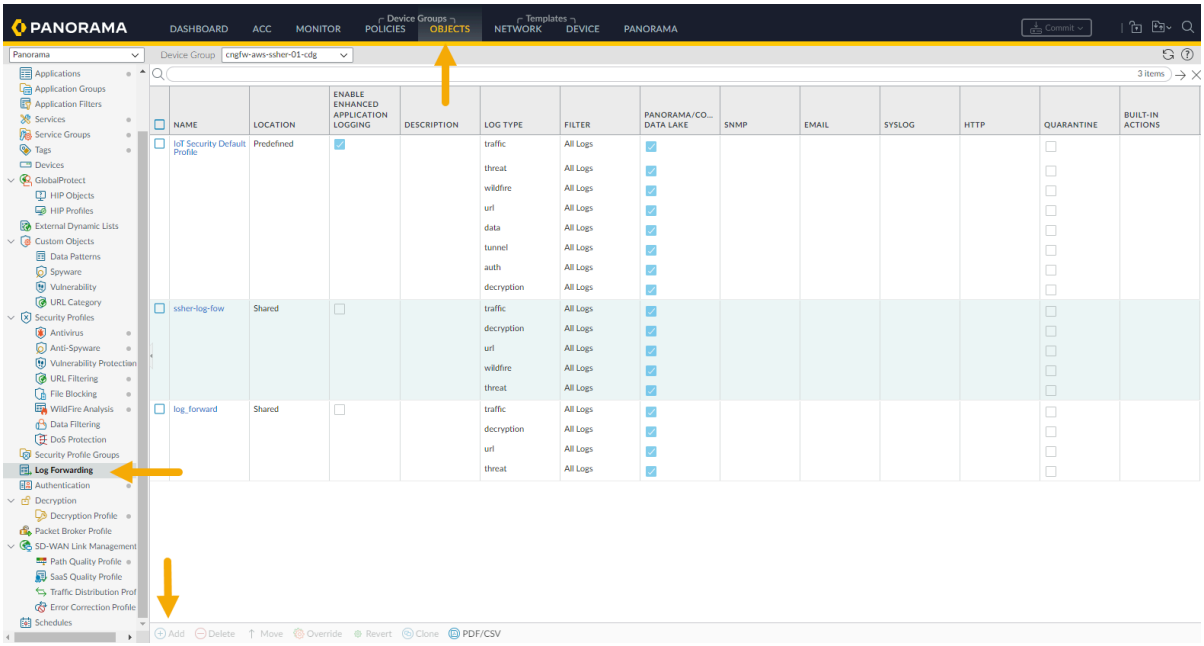
Transférer les journaux vers le service de journalisation Strata

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)**.

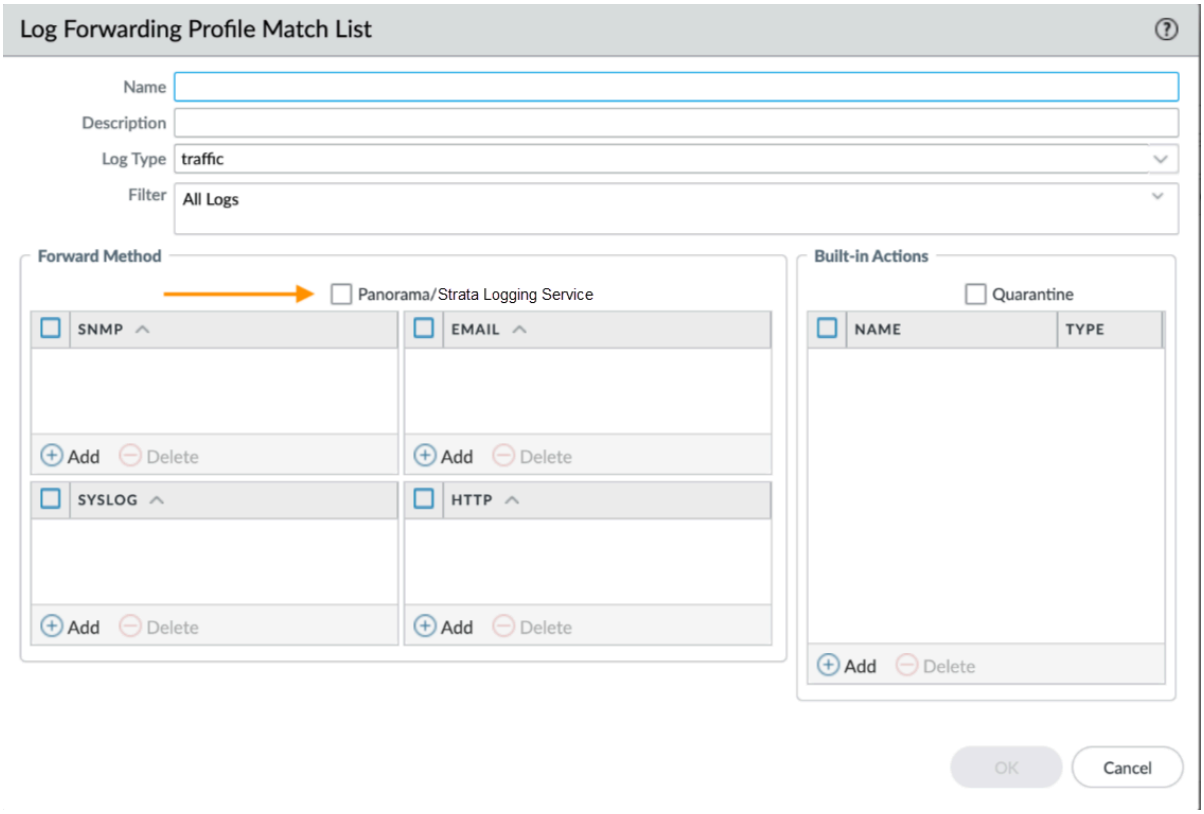
STEP 3 | Cliquez sur **Add (Ajouter)** pour créer un nouveau profil de liste de correspondance de transfert des journaux.



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.

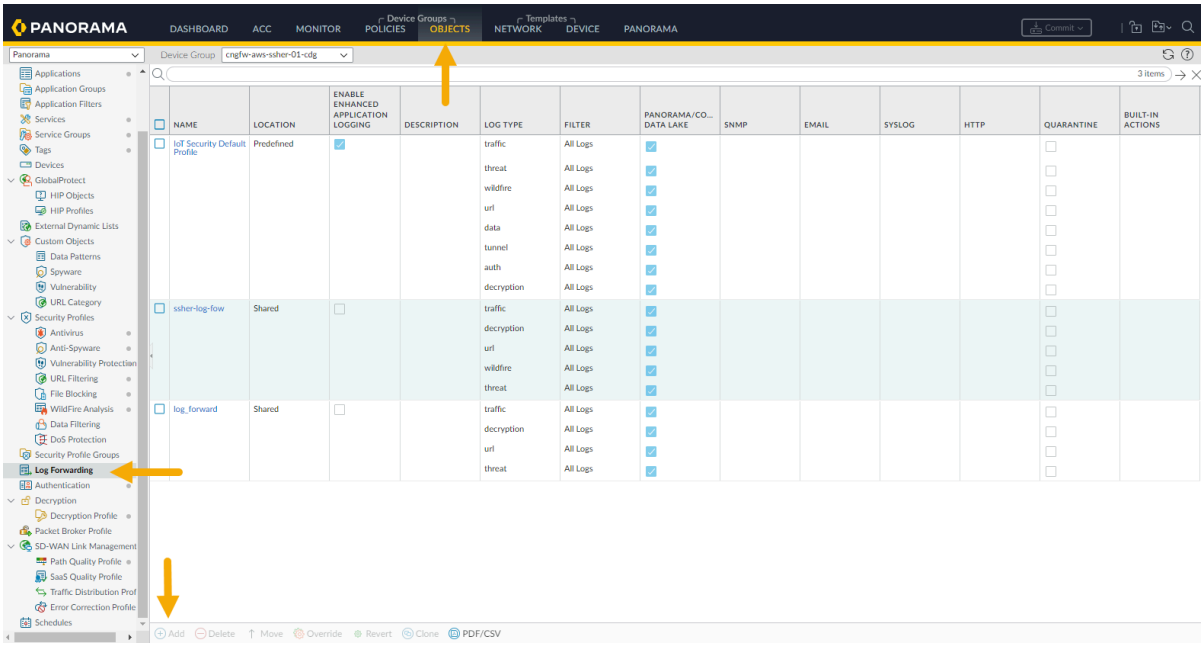
Transférer des journaux sans le service de journalisation Strata

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.

Afficher les journaux d’audit sur Cloud NGFW pour AWS

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

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)**.

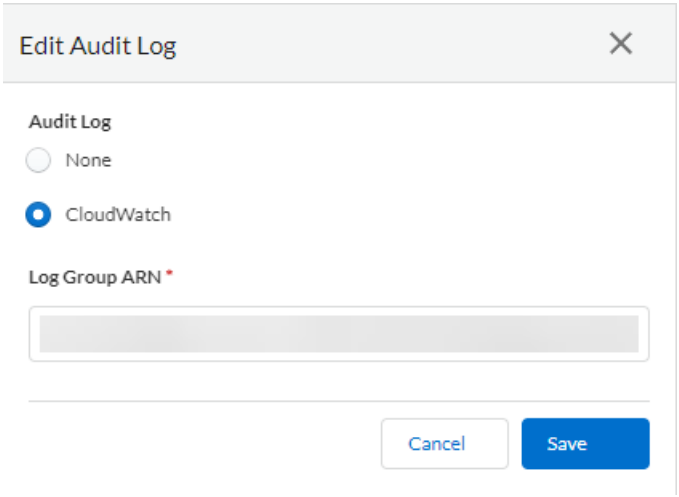
STEP 4 | Cliquez sur l'icône d'édition **Audit Log Settings (Paramètres du journal d'audit)** Edit.

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)**.



Publier et afficher des métriques personnalisées dans AWS CloudWatch

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

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 5 minutes, les métriques sont utiles aux alertes en raison de leur échantillonnage fréquent.

Le groupe de journaux CloudWatch, le compartiment S3, l'espace de noms CloudWatch et le flux Kinesis doivent être précréés dans le modèle CloudFormation (CFT).

Les métriques sont collectées toutes les 5 minutes. Toutes les métriques sont publiées dans un espace de noms. CloudWatch stocke vos métriques afin que vous puissiez accéder à des informations historiques et ainsi voir sous un autre angle 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.

Nom du champ	Description
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 taux de paquets, le taux d'établissement de nouvelles connexions et le débit du pare-feu pour déterminer l'utilisation des sessions.
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.
PktsOut	Nombre de paquets client/serveur de la session.

Pour publier les métriques CloudWatch :

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

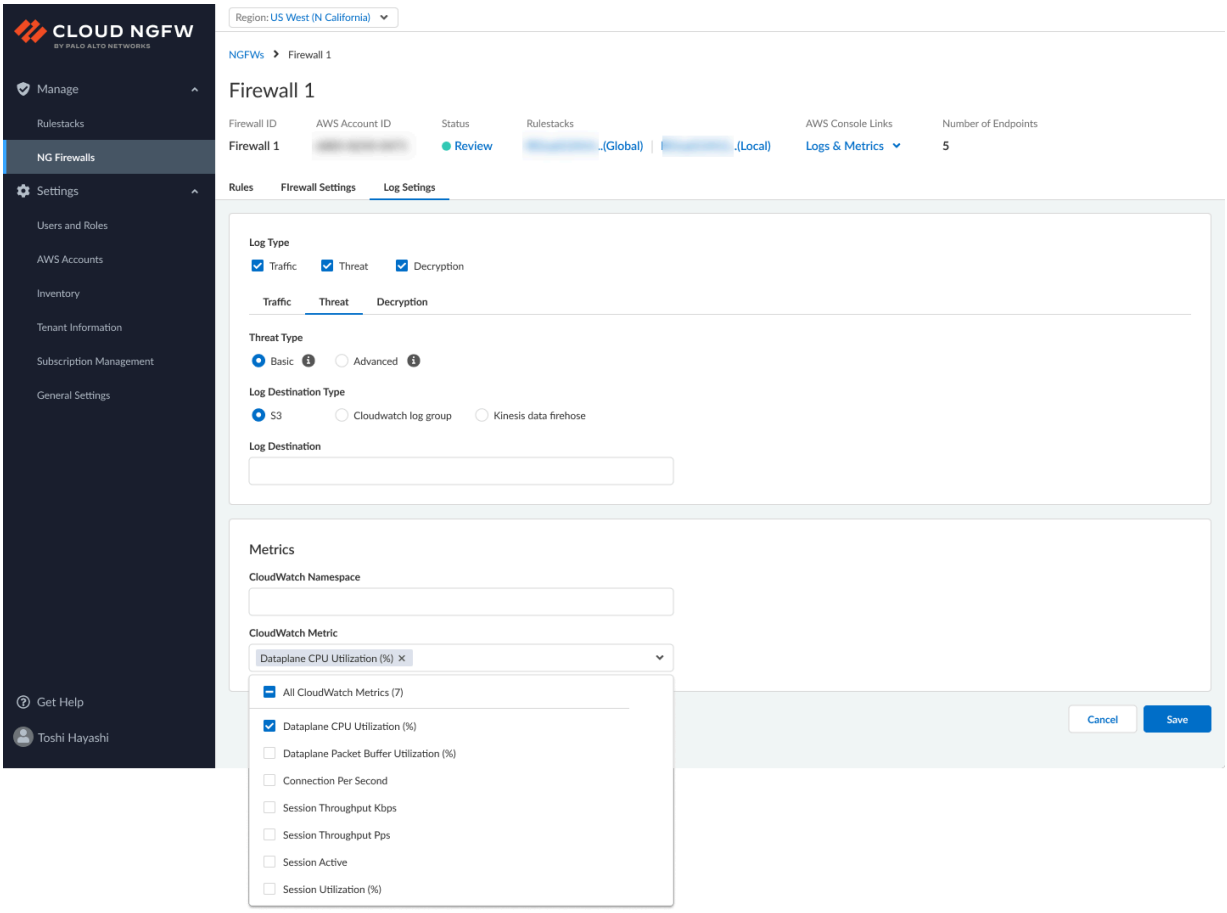
STEP 2 | Sélectionnez **NG Firewalls (Pare-feu NG)**.

STEP 3 | Sélectionnez **Log Settings (Paramètres du journal)**.

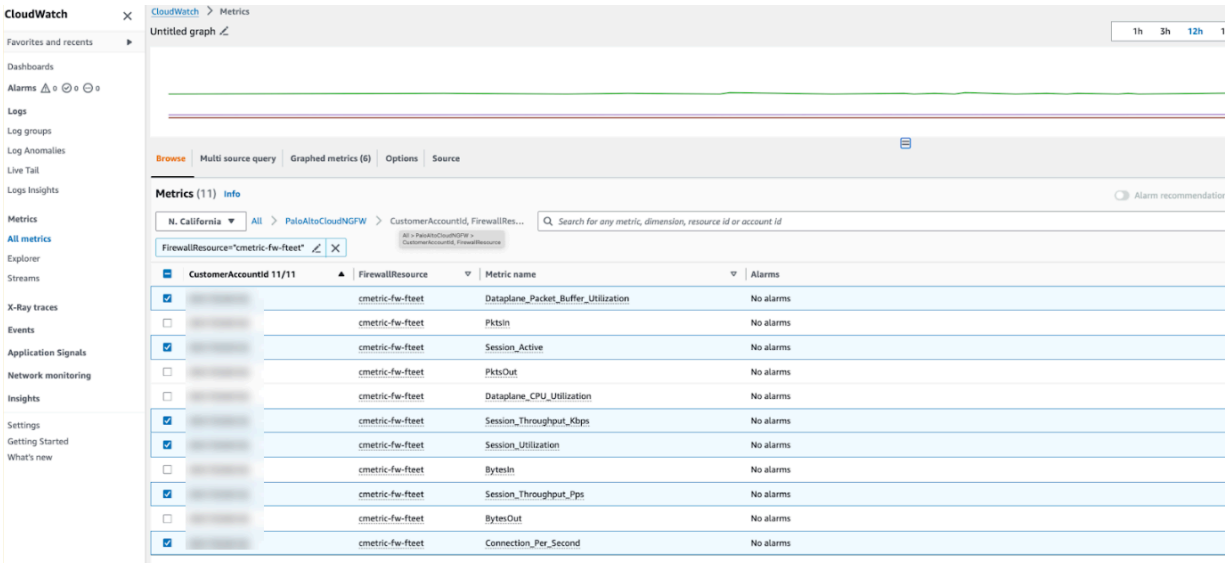
STEP 4 | Sous **Metrics (Métriques)**, spécifiez ce qui suit :

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. Consultez le tableau ci-dessus pour connaître les métriques prises en charge.

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



Voici un exemple de sortie de métriques dans un compte :



Firewall as code

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

Cloud NGFW pour AWS prend en charge le firewall as code (pare-feu en tant que code). Cela inclut la prise en charge de Terraform, un outil open source que vous pouvez utiliser pour définir, gérer et versionner des ressources d’infrastructure à l’aide de fichiers de configuration. En tant qu’outil d’infrastructure as code, Terraform vous permet d’automatiser les ressources cloud et sur site en définissant des ressources dans des fichiers de configuration que vous pouvez réutiliser, partager et versionner aux fins suivantes :

- Diminuer les coûts en réduisant au maximum les flux de travail redondants.
- Réduire les risques en normalisant la codification et la réutilisation de l’infrastructure.
- Utiliser l’automatisation pour réduire le temps nécessaire au déploiement de la ressource Cloud NGFW.
- Améliorer la fiabilité en veillant à ce que les ressources Cloud NGFW soient provisionnées et configurées conformément à la déclaration des fichiers de configuration Terraform.

En plus de la prise en charge de Terraform, la ressource Cloud NGFW prend également en charge AWS CloudFormation. CloudFormation est un service fourni par AWS qui vous aide à modéliser et à configurer vos ressources AWS en créant un modèle qui décrit toutes les ressources AWS que vous utilisez (par exemple, une instance Amazon EC2). Avec le modèle CloudFormation, vous n’avez pas besoin de créer et de configurer individuellement vos ressources AWS. Le modèle s’en occupe à votre place. Plus précisément, il fonctionne ainsi :

- Il simplifie la gestion de l’infrastructure à l’aide d’un modèle pour décrire toutes les ressources (par exemple, un groupe de mise à l’échelle automatique ou un équilibreur de charge élastique) et leurs propriétés.
- Il réplique votre infrastructure, ce qui vous permet de réutiliser votre modèle CloudFormation de manière cohérente et reproductible. Il vous permet de décrire vos ressources à l’aide du modèle une seule fois, puis de provisionner les mêmes ressources à plusieurs reprises dans plusieurs régions.
- Il contrôle et suit les modifications apportées à vos déploiements et prend en charge des situations telles que les mises à niveau incrémentielles. Par exemple, une mise à niveau peut avoir introduit des problèmes de performances imprévus. Pour restaurer manuellement les paramètres d’origine de votre infrastructure, il faut connaître les ressources qui ont été modifiées et les paramètres d’origine. Le modèle CloudFormation, rédigé sous la forme d’un fichier texte facile à lire, permet d’identifier les modifications apportées à votre infrastructure en identifiant clairement les révisions. De plus, lorsque le modèle est associé à un système de contrôle des versions, vous savez exactement quand les modifications ont été apportées, à quel endroit et par qui.

Activer l'accès par programmation

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

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.

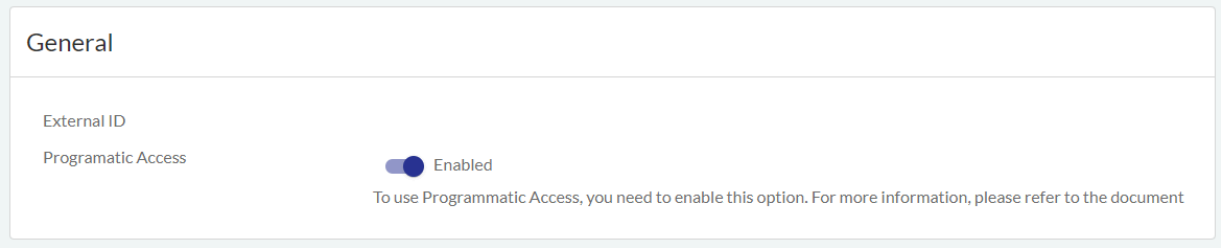
Étant donné que l’accès par programmation est puissant, Cloud NGFW ne fournit pas de clé d’accès ou de clé secrète pour signer les demandes d’autorisation. Au lieu de cela, vous pouvez utiliser le rôle IAM dans votre compte AWS pour accéder aux API Cloud NGFW, puis configurer les ressources IAM qui peuvent 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.

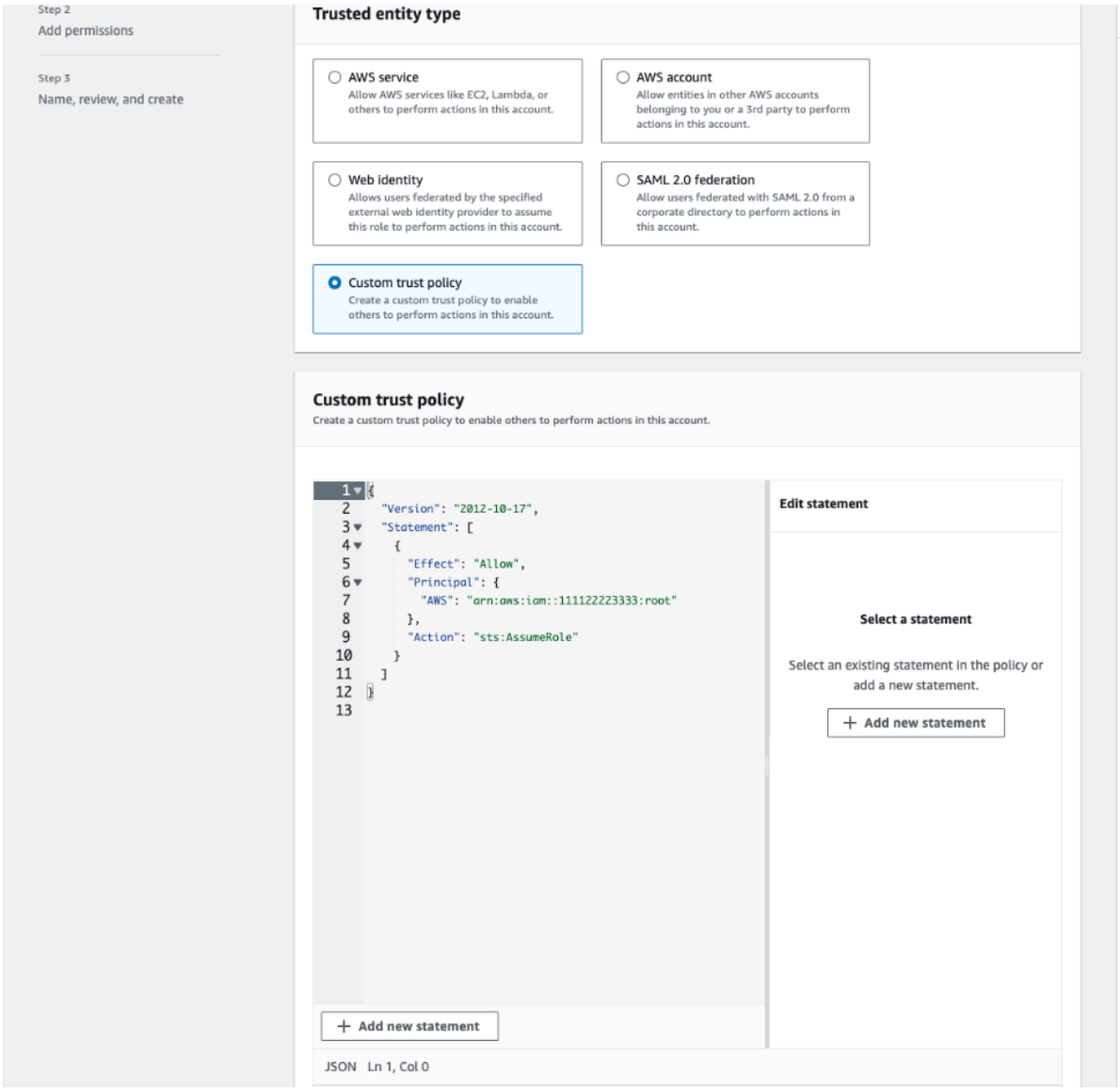
- Sélectionnez **Tenant (Locataire)** dans la console **Cloud NGFW Tenant (Locataire Cloud NGFW)**.
- Sous **General (Général)**, cliquez sur le curseur **Programmatic Access (Accès par programmation)**.
- Cliquez sur **Enable (Activer)** pour confirmer.



STEP 2 | Créez un nouveau rôle avec une *politique de confiance personnalisée*.

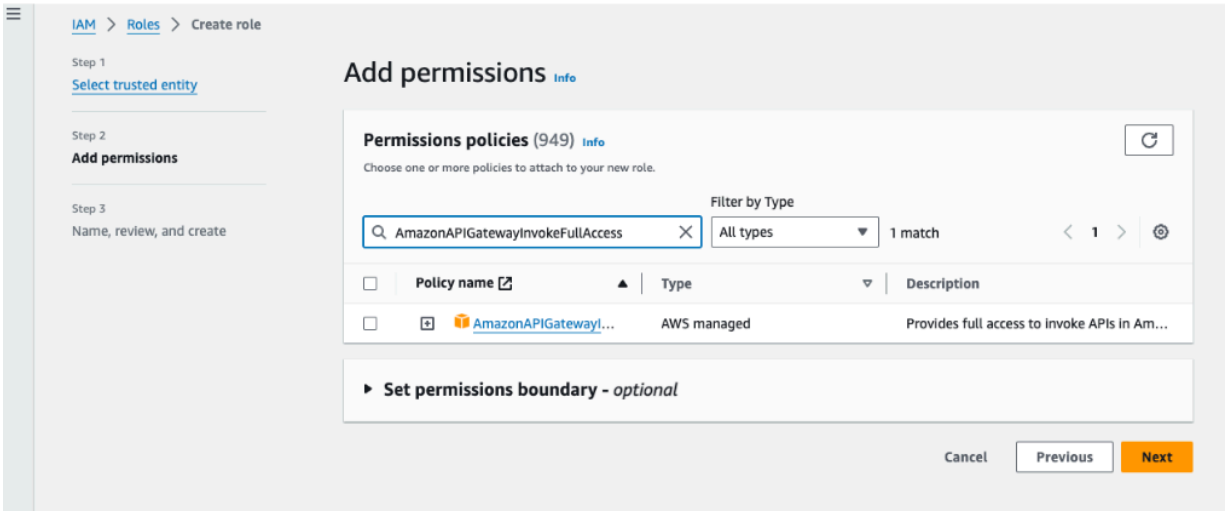
Voici un exemple de politique de confiance personnalisée :

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::111122223333:root" },
 "Action": "sts:AssumeRole" } ] }
```

L’exemple de relation de confiance mentionné ci-dessus avec la racine définie comme principal pourrait donner accès à plus de principaux que prévu. Les éléments Principal et Condition permettent de restreindre l’accès au rôle à des principaux spécifiques. Pour en savoir plus, consultez How to use trust policies with IAM roles (Utilisation de politiques de confiance avec des rôles IAM). *Vous pouvez également créer ce rôle dans un compte AWS et déléguer des autorisations spécifiques à un autre compte à l’aide de l’accès entre comptes. Pour définir une politique de confiance avec l’accès entre comptes, consultez les exemples fournis* ici.

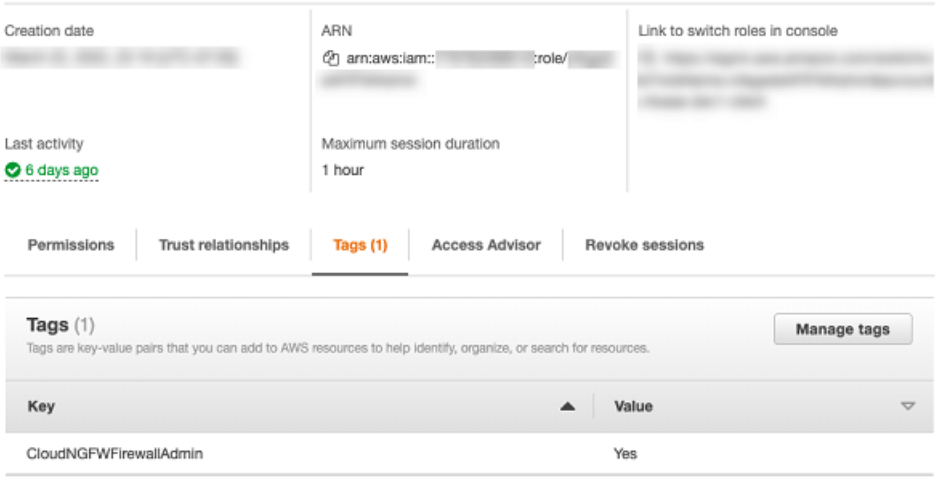
STEP 3 | Ajouter la politique d’autorisation Amazon **APIGatewayInvokeFullAccess** pour appeler des API. Cliquez ici pour en savoir plus.



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	`CloudNGFWAccountAdmin`	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

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

HashiCorp Terraform est un outil d’infrastructure as code (IaC) open source pour les équipes gérant des environnements multicloud. 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 plug-ins interagissent avec des fournisseurs tels qu’AWS pour faciliter la réutilisation en créant des étapes reproductibles pour la création et la maintenance de l’infrastructure cloud, vous permettant ainsi d’effectuer facilement des ajouts sur votre pipeline CI/CD.

Palo Alto Networks ajoute le fournisseur cloudngfwaws pour automatiser le processus de création de l’infrastructure de sécurité et maintenir la posture de sécurité du réseau à l’aide de 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.

Consultez la documentation pour les développeurs Palo Alto Networks pour en savoir plus sur le déploiement de Cloud NGFW sur AWS à l’aide de Terraform et consulter les informations de référence de Terraform.

Vous pouvez utiliser le fournisseur Terraform dans votre configuration pour les actions suivantes :

- Lancer Cloud NGFW.
- Configurer la rulestack utilisée par Cloud NGFW pour récupérer des informations sur les politiques. La rulestack contient des informations sur les politiques 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" }
```


Configurer l’intégration automatisée des comptes

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

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.
- Si vous utilisez un profil AWS pour AUTH, utilisez le profil `CloudNGFWGAccountAdmin` pour l’intégration du compte.
- Créez un rôle avec le modèle CloudFormation (CFT) et *appliquez les autorisations* dans chacun des comptes que vous souhaitez intégrer.
- Soyez abonné à Cloud NGFW via le marketplace et le compte devrait être intégré avec succès.
- Deux rôles sont nécessaires :
  - Créez un rôle `CloudNGFWAccountAdmin` dans le compte administrateur.
  - Créez un rôle qui permet d’exécuter des CFT dans chacun des comptes que vous souhaitez intégrer à l’aide de Terraform.

Ces rôles sont décrits dans la procédure ci-dessous.

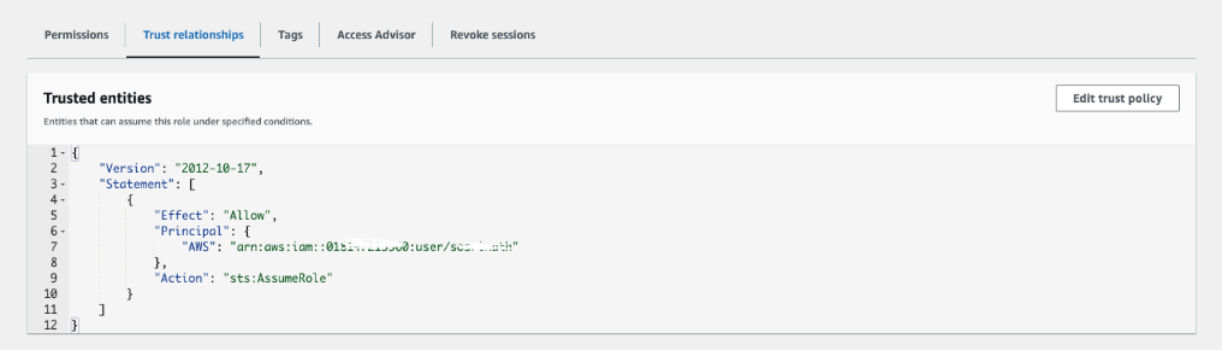
Pour accéder à la fonctionnalité d’intégration automatisée des comptes, vous devrez télécharger le dernier modèle Terraform et activer l’accès par programmation.

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. Suivez les étapes 1 à 4 de la section Activer l’accès par programmation pour créer un rôle avec l’étiquette `CloudNGFWAccountAdmin`.

STEP 2 | Dans chacun des comptes que vous souhaitez intégrer, créez un rôle pour exécuter le modèle CloudFormation (CFT) :

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::ACCOUNT_ID:user/USERNAME" },
 "Action": "sts:AssumeRole" } ] }
```

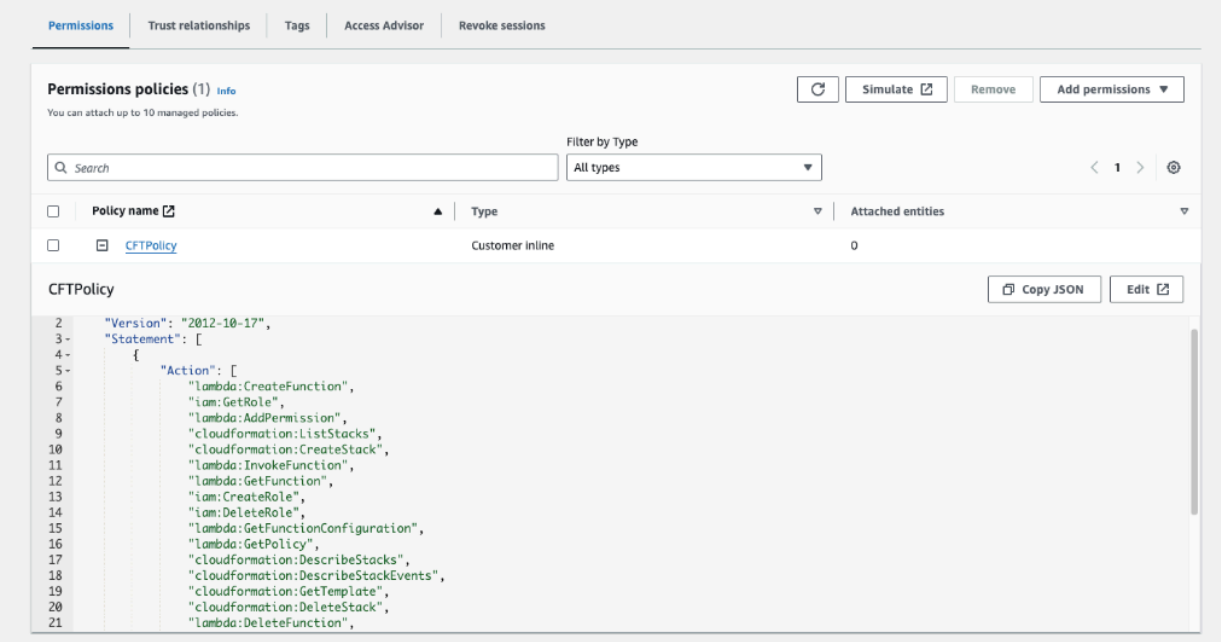


Pour définir la politique d'autorisation du rôle, utilisez l'option **Create Inline Policy (Créer une politique en ligne)**. Par exemple :

```
"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":
"Allow", "Sid": "VisualEditor1" } ] }
```



L'exemple de relation de confiance (ci-dessus) représente un utilisateur spécifique dans un compte spécifique, qui est autorisé à exécuter le CFT. Pour en savoir plus sur la définition de votre propre politique de confiance, consultez How to use trust policies with IAM roles (Utilisation de politiques de confiance avec des rôles IAM).

STEP 3 | 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, car l'intégration de tous les comptes peut prendre jusqu'à 10 minutes.

Exemple de fichier Terraform

L’exemple suivant illustre un fichier Terraform contenant les définitions du fournisseur et du module. Dans cet exemple, account_admin_arn désigne le rôle d’accès par programmation qui a été créé à l’étape 1. Le champ **account_ids** représente la liste des comptes AWS qui doivent être intégrés. Le champ **cft_role_name** représente le rôle qui a été créé à l’étape 2 dans chacun des comptes intégrés.

```
terraform { required_providers { cloudngfwaws = { source
 = "paloaltonetworks/cloudngfwaws" } } } provider
 "cloudngfwaws" { account_admin_arn = "arn:aws:iam::11222333344:role/
fwaas_prog_onboard" json_config_file = "./.cloudngfwaws_creds.json" }
 module "account_onboarding1" { source = “github.com/
PaloAltoNetworks/terraform-provider-cloudngfwaws/modules/
account_onboarding" account_ids = ["ACCOUNT_1", "ACCOUNT_2"....,
 “ACCOUNT_100”] cft_role_name = "cft_apply_role" } module
 "account_onboarding2" { source = “github.com/PaloAltoNetworks/
terraform-provider-cloudngfwaws/modules/account_onboarding"
 account_ids = ["ACCOUNT_101", "ACCOUNT_102"...., “ACCOUNT_200”]
 cft_role_name = "cft_apply_role" }
```

Supprimer un compte intégré

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

Lister un compte non intégré

Utilisez la commande **list** de Terraform. Pour plus d’informations, consultez la Documentation Terraform.

Provisionner des ressources Cloud NGFW sur votre AWS CFT

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

Cloud NGFW vous offre la flexibilité nécessaire pour provisionner des ressources sur le modèle AWS CloudFormation (CFT) en vous permettant de créer vos propres ressources.

Activez l'accès par programmation avant d'utiliser le registre CloudFormation avec Cloud NGFW.

Utilisez les schémas **PaloAltoNetworks::CloudNGFW::RuleStack** et **PaloAltoNetworks::CloudNGFW::NGFW** pour intégrer Cloud NGFW à 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 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,`

Élément	Description
	YAML `RuleStackName: String`

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

Élément	Description
	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`

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 }`

Élément	Description
	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, ... ] }`
	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`

Élément	Description

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 }`
	
	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

Élément	Description

	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 }`
	
	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`

Élément	Description

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 :
	
	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

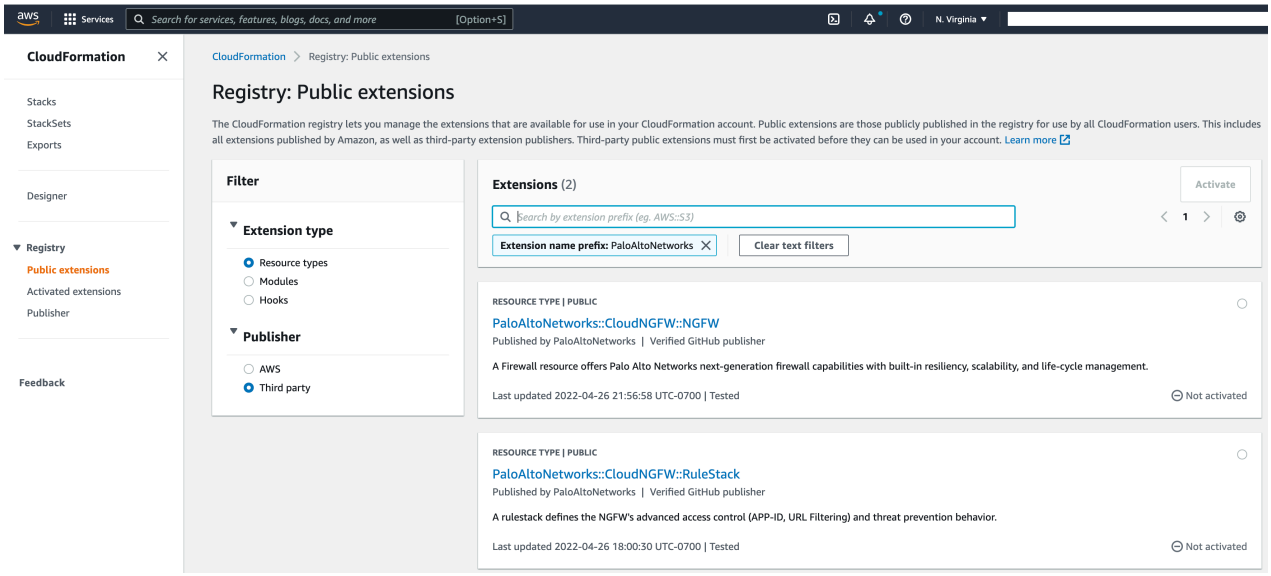
```
Type : PaloAltoNetworks::CloudNGFW::NGFWProperties: AppIdVersion:
 String AutomaticUpgradeAppIdVersion: Boolean Description:
 String EndpointMode: String FirewallName: String RuleStackName:
 String RuleStackName: String SubnetMappings: - String Tags: -
 Map VpcId: String UpdateToken: String LogDestinationConfigs: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

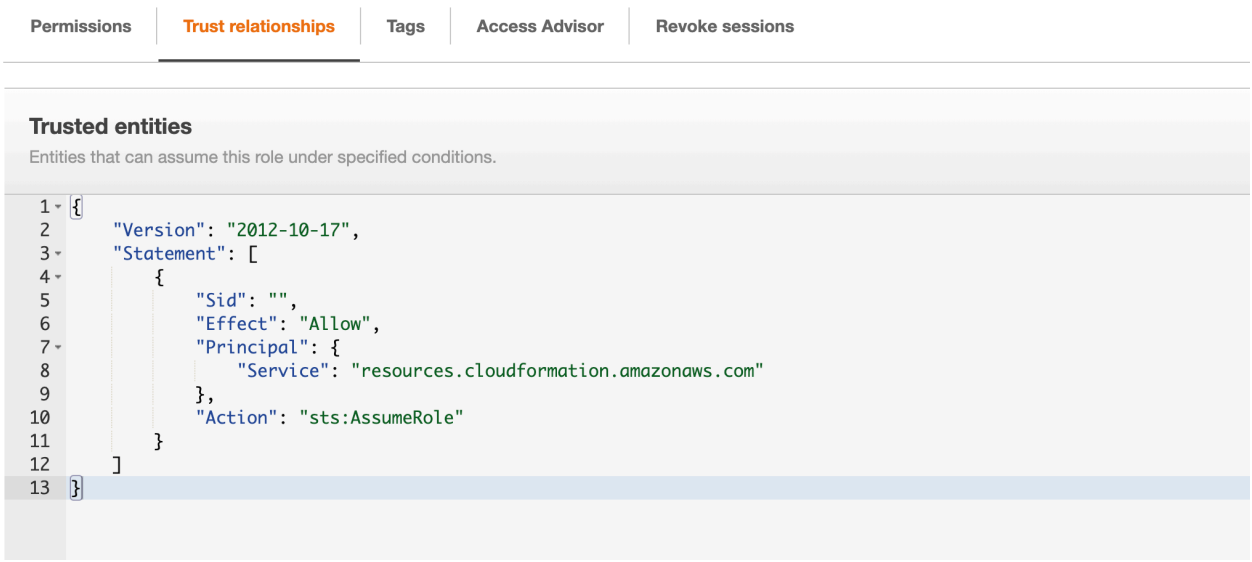
Élément	Description
	YAML `LogDestination: String LogDestinationType: String LogType: String`

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 ou l'utilisation de Cloud NGFW pour 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 de 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" ] } } }
```

Autorisations CFT de rôle entre comptes pour Cloud NGFW

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

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" } ] }
```