paloalto TECHDOCS

Mise en route avec Cloud NGFW pour AWS

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

Présentation de Cloud NGFW pour AWS

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

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

Composants Cloud NGFW

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

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

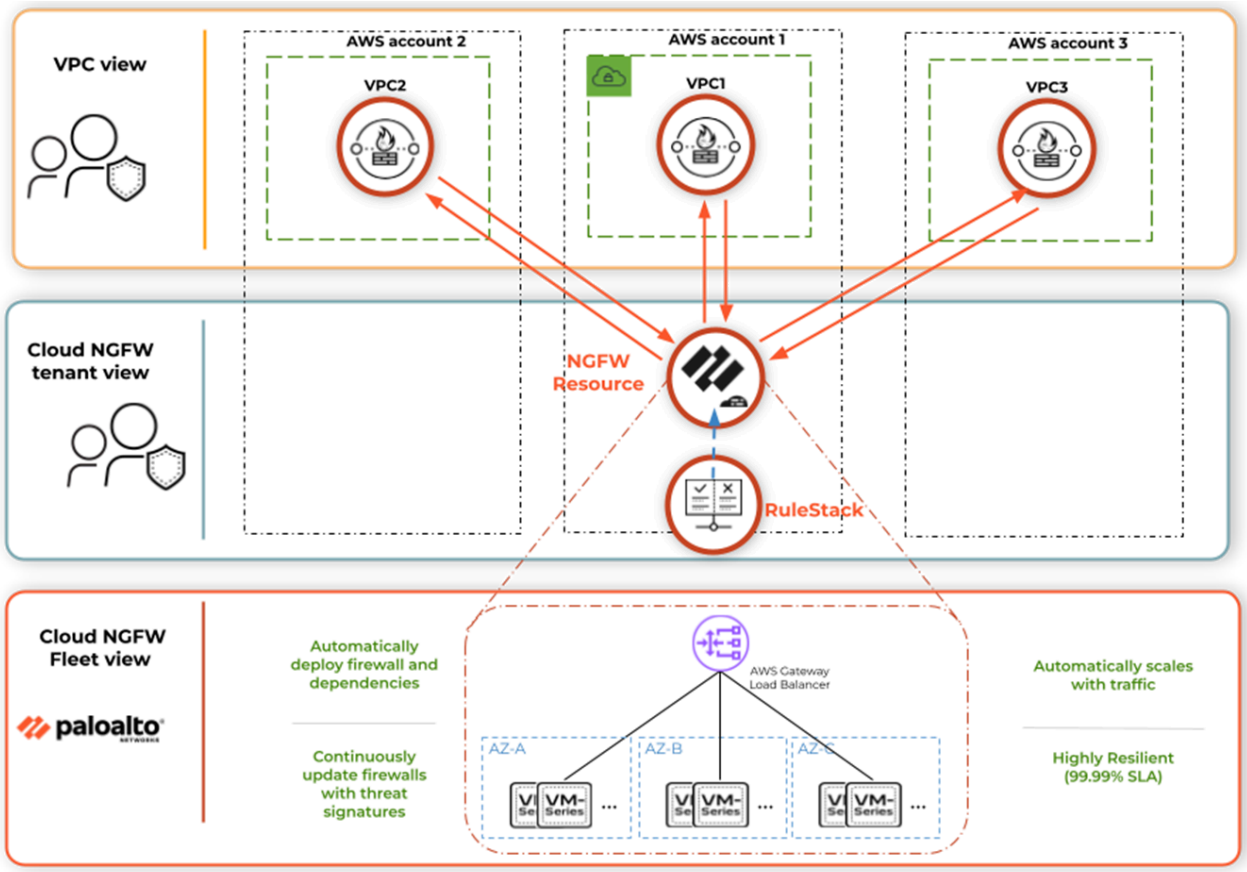
  Cloud NGFW prend en charge deux types de rulestacks :

  - **Rulestack locale** : Les administrateurs de compte locaux peuvent associer une rulestack locale à un NGFW dans leur compte AWS. Une rulestack locale inclut des règles locales.

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

À propos des terminaux Cloud NGFW

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



Les terminaux des NGFW sont chargés de diriger le trafic vers le NGFW pour inspection et application. Les terminaux NGFW interceptent le trafic et l'acheminent vers le NGFW pour inspection et application des politiques. Vous pouvez utiliser deux modes de gestion pour créer des terminaux automatiquement ou manuellement.

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

Après avoir créé un NGFW et des terminaux NGFW vous devez mettre à jour vos tables de routage AWS pour vous assurer que le trafic est envoyé au NGFW. Les tables de routage que vous mettez à jour et la façon dont vous les mettez à jour dépendent de votre déploiement spécifique. Consultez Redirection du trafic vers Cloud NGFW pour plus d'informations.

Cloud NGFW en action

1. **S'abonner au service Cloud NGFW** : commencez par vous abonner au service Cloud NGFW pour AWS via AWS Marketplace. Après votre abonnement, vous pouvez créer un locataire Cloud NGFW. L'utilisateur AWS IAM abonné est l'administrateur de locataire (TenantAdmin), ce qui permet à cet utilisateur d'inviter des utilisateurs supplémentaires et d'attribuer des rôles. Ajoutez votre compte AWS au locataire Cloud NGFW. L'ajout de votre compte accorde les autorisations nécessaires à Cloud NGFW pour stocker les journaux, créer des terminaux NGFW et accéder aux clés nécessaires au décryptage.
2. **Créer des rulestacks** : après avoir ajouté des utilisateurs et attribué des rôles dans la console de locataire Cloud NGFW, les administrateurs de rulestack locale peuvent créer une règle et des rulestacks.
3. **Créer des NGFW** : déployez des ressources de pare-feu NGFW pour protéger vos VPC. Lors de la création de vos NGFW, associez les rulestacks locales que vous avez créées précédemment.

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

Cas pratiques de Cloud NGFW

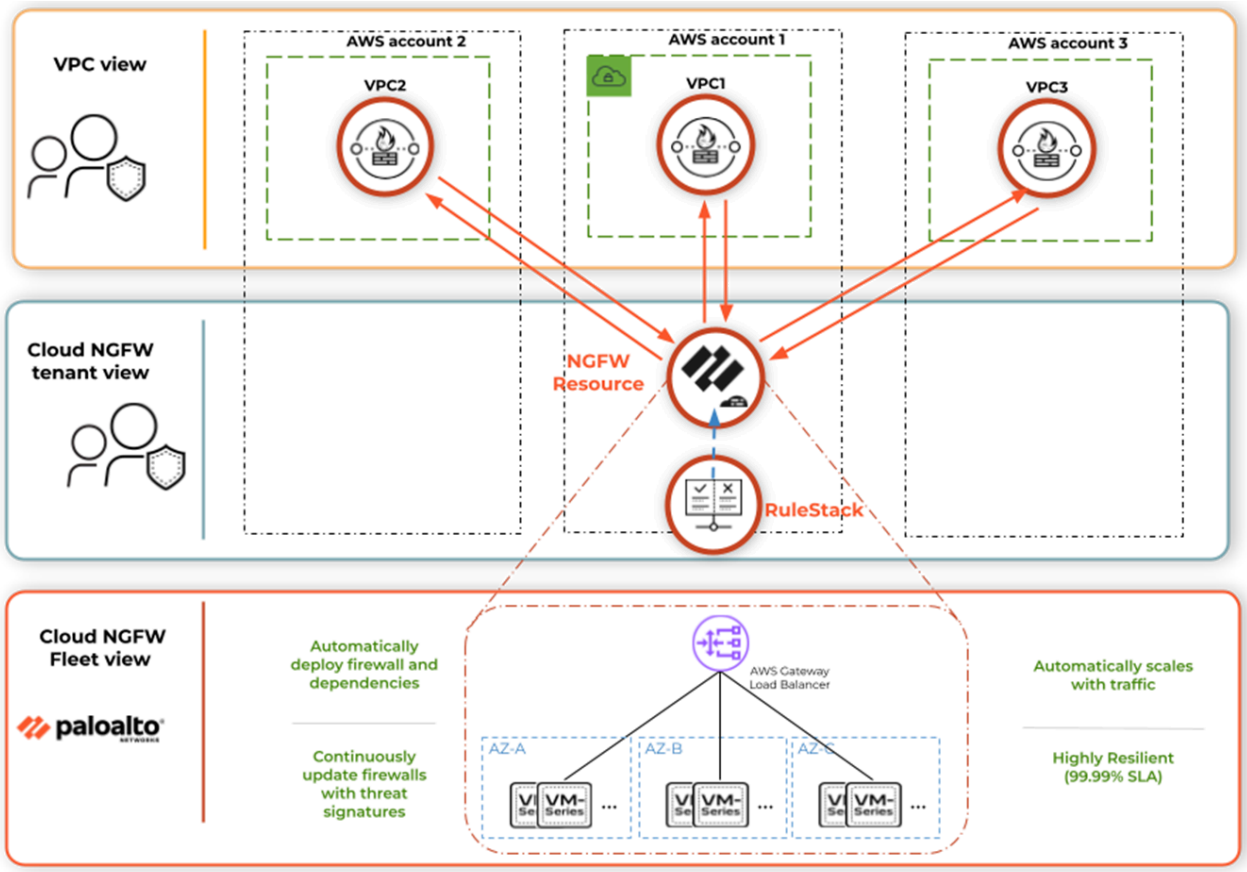
Cloud NGFW vous fournit les outils et les fonctionnalités nécessaires pour sécuriser le trafic entrant, le trafic sortant et le trafic est-ouest.

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

Ressource Cloud NGFW et terminaux 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 utilisateur (locataire ou administrateur)

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



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

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

Après avoir créé un NGFW et des terminaux NGFW vous devez mettre à jour vos tables de routage AWS pour vous assurer que le trafic est envoyé au NGFW. Les tables de routage que vous mettez à jour et la façon dont vous les mettez à jour dépendent de votre déploiement spécifique. Consultez Redirection du trafic vers le cloud NGFW pour plus d'informations pour découvrir des exemples de déploiement avec des exemples de tables de routage pour vous guider.

Fonctionnalités de gestion et de déploiement de NGFW Cloud prises en charge

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

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

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

Fonctionnalités de gestion de la politique de sécurité prises en charge

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

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
Outils	Vous disposez de plusieurs options de configuration pour créer des politiques pour vos Cloud NGFW.	• Console Cloud NGFW • API Cloud NGFW • Cloud Formation • Terraform	• Console Panorama • API Panorama • Terraform	• Console SCM
Types de journaux	Cloud NGFW génère des journaux horodatés qui constituent une piste d'audit pour les événements de trafic réseau surveillé par le pare-feu. Les entrées de journal contiennent des artefacts, qui sont des propriétés, des activités ou des comportements associés avec l'événement journalisé, tels que le type d'application ou l'adresse IP d'un pirate. Chaque type de journal enregistre des informations sur un type	• Journaux du trafic • Journaux des menaces • Journaux de décryptage • Journaux d'audit	• Journaux du trafic • Journaux des menaces • Journaux de URL Filtering • Journaux de décryptage	• Visionneuse de journaux • Journaux du trafic • Journaux des menaces • Journaux de URL Filtering • Journaux de décryptage

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	d'événement distinct. Par exemple, Cloud NGFW génère un journal des menaces pour enregistrer le trafic correspondant à un logiciel espion, une vulnérabilité ou une signature de virus.			
Destinations des journaux	Cloud NGFW peut livrer les journaux générés à des destinations AWS et au service de journalisation Strata.	• Compartiment Amazon Simple Storage Service (S3) • Groupe de journaux Amazon CloudWatch • Amazon Kinesis Data Firehose	• Compartiment Amazon Simple Storage Service (S3) • Groupe de journaux Amazon CloudWatch • Amazon Kinesis Data Firehose • Service de journalisation Strata • Transférer les journaux du service de journalisation Strata vers un serveur Syslog • Transférer les journaux du service de journalisation Strata vers un serveur HTTPS	• Compartiment Amazon Simple Storage Service (S3) • Groupe de journaux Amazon CloudWatch • Amazon Kinesis Data Firehose • Service de journalisation Strata • Transférer les journaux du service de journalisation Strata vers un serveur Syslog • Transférer les journaux du service de journalisation Strata vers un serveur HTTPS

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
Visualisation et analytique des journaux	Examinez les journaux Cloud NGFW pour vérifier un grand nombre d'informations sur votre trafic de VPC. Ces informations sont, notamment, la source, la destination, les URL, les protocoles de ports, l'App-ID, les menaces, les pays, les URL, etc.	• Explorer les journaux dans les Destinations Amazon	• Explorer les journaux dans les Destinations Amazon • Explorer les journaux dans le service de journalisation Strata • Surveiller les journaux dans Panorama • Surveiller l'Application Command Center (Centre de commande des applications – ACC) dans Panorama	• Explorer les journaux dans les Destinations Amazon • Explorer les journaux dans le service de journalisation Strata • Informations sur l'activité dans Strata Cloud Manager • Centre de commande de Strata Cloud Manager
Rapports	Générez des rapports prédéfinis et personnalisés sur les applications, les menaces et les activités URL de votre trafic de VPC.	—	• Rapports planifiés et personnalisés	• Rapports planifiés et personnalisés
Analyse et optimisation des politiques	La surveillance de l'utilisation des règles vous permet d'évaluer si votre mise en œuvre de la politique continue de répondre à	—	• Rule Usage (Utilisation d'une règle) • Optimiseur de politique	• Rule Usage (Utilisation d'une règle) • Optimiseur de politique

Gestion des politiques de sécurité, visualisation et rapports	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	vos besoins de sécurité. Policy Analyzer analyse vos règles Cloud NGFW et peut recommander une consolidation ou une suppression de règles spécifiques pour atteindre votre posture de sécurité souhaitée. Il vérifie également les anomalies, telles que les effets d'ombre, les redondances, les généralisations, les corrélations et les consolidations dans votre base de règles.			
Capture de paquets	Pare-feu Palo Alto Networks pour effectuer une capture de paquets personnalisée ou une capture de paquets de menace.	—	—	—

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
Politique de Sécurité	La politique de sécurité protège votre trafic de VPC contre les menaces et les perturbations. Les règles des politiques de sécurité individuelles déterminent si une session de trafic de VPC doit être bloquée ou autorisée en fonction des attributs du trafic, comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service.	• Rulestack locale • Rulestack globale	• Politiques de sécurité • Pré-règles • Post-règles • Règles par défaut	• Politiques de sécurité • Pré-règles • Post-règles • Règles par défaut
Adresse	Vous pouvez spécifier un objet d'adresse pour inclure des adresses IPv4, un FQDN ou une adresse générique (adresse IPv4 suivie d'une barre oblique et d'un masque générique).	• Listes des préfixes • Liste FQDN	• Masque réseau IPv4 • Plages IPv4 • Masquage générique IPv4 • FQDN	• Masque réseau IPv4 • Plages IPv4 • Masquage générique IPv4 • FQDN
Groupes d'adresses	Vous pouvez regrouper des adresses sources	—	• Groupes d'adresses	• Groupes d'adresses

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	ou de destination spécifiques qui nécessitent l'application d'une politique identique.			
Régions	Vous pouvez autoriser ou bloquer le trafic provenant (ou à destination) d'adresses IP en fonction de leur emplacement géographique tel qu'un comté. La région est disponible en option lors de la spécification de la source et de la destination de vos politiques. Vous pouvez choisir parmi une liste standard de pays ou spécifier une région/ géolocalisation personnalisée avec ses adresses IP associées	• Pays	• Régions prédéfinies • Régions personnalisées	• Régions
Service (port et protocole)	Vous pouvez contrôler de manière granulaire l'utilisation de sessions de trafic de VPC vers des ports spécifiques de votre réseau (en	• Port et protocole	• Services	• Services

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	d'autres termes, vous pouvez définir le port par défaut pour l'application). Cloud NGFW contient deux services prédéfinis (service-http et service-https) qui utilisent les ports TCP 80 et 8080 pour HTTP et le port TCP 443 pour HTTPS. Vous pouvez cependant créer n'importe quel service personnalisé sur un quelconque port TCP/UDP de votre choix.			
Groupes de services	Vous pouvez combiner des services ayant les mêmes paramètres de sécurité dans des groupes de services afin de réduire le nombre de règles dans la politique de sécurité.	—	• Groupes de services	• Groupes de services
Liste dynamique externe	Vous pouvez contrôler votre trafic de VPC de manière granulaire à l'aide d'une liste dynamique d'adresses IP,	• Flux de renseignement • Flux intégrés • Flux de services	• Listes dynamiques externes • EDL intégré • Listes de services	• Listes dynamiques externes • EDL intégré • Listes de services

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

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d’appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	ID™ de Palo Alto Networks qui s’appuie sur les signatures d’applications pour identifier avec précision les applications de votre réseau.			
Groupe d'applications	Vous pouvez regrouper un ensemble d’App-ID qui nécessitent la même application de politique.	—	• Groupes d'application	• Groupes d'application
Filtres de l'application	Vous pouvez contrôler votre trafic de VPC de manière granulaire en définissant un filtre d’application qui regroupe les App-ID actuels et les App-ID futurs correspondant à certains attributs. Par exemple, vous pouvez procéder à la création d’un filtre d’application selon un ou plusieurs attributs (catégorie, sous-catégorie, technologie, risque, caractéristiques). Désormais, chaque fois qu’un nouvel App-ID	—	• Filtres de l'application	• Filtres de l'application

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	est introduit dans Cloud NGFW sur la base d'une mise à jour de contenu, toutes les nouvelles applications correspondant aux critères du filtre sont automatiquement ajoutées à votre ensemble.			
Contrôle prioritaire sur l'application	Vous pouvez configurer Cloud NGFW de manière à disposer d'un contrôle prioritaire sur l'identification d'application (App-ID) normale du trafic spécifique transitant par le pare-feu. Dès que la politique de contrôle prioritaire sur l'application entre en vigueur, toutes les inspections supplémentaires d'App-ID du trafic sont arrêtées et la session est identifiée avec les signatures d'application propre à	—	• Contrôle prioritaire sur l'application	• Contrôle prioritaire sur l'application

Politique et articles de politique	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d’appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	l’entreprise que vous fournissez.			
Étiquettes	Les étiquettes vous permettent de regrouper des objets à l'aide de mots-clés ou d'expressions. Vous pouvez appliquer des étiquettes à des objets d'adresse, à des groupes d'adresses (statiques et dynamiques), à des applications, à des zones, à des services, à des groupes de services et à des règles de politique.	—	• Étiquettes	• Étiquettes
Groupe d’utilisateurs dynamiques	Vous permet de créer une liste d'utilisateurs à partir de la base de données locale ou d'une base de données externe et de les regrouper.	—	—	—
Périphériques	Egalement connu sous le nom de Dictionnaire des périphériques, cette page contient les métadonnées des objets de périphériques.	—	—	—

Certificats et décryptage	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
Gestion des certificats	Cloud NGFW utilise des certificats pour accéder à un flux intelligent et pour activer le décryptage entrant et sortant. Chaque certificat contient une clé cryptographique pour crypter un texte brut ou décrypter un texte crypté. Chaque certificat contient également une signature numérique pour authentifier l'identité de l'émetteur.	• Certificats TLS/SSL dans AWS Secrets Manager	• Certificats CA racine auto-signés • Importation d'un certificat et d'une clé privée • Certificats TLS/SSL dans AWS Secrets Manager • Générer des certificats • Obtenir un certificat auprès d'une CA externe • Répondeur Online Certificate Status Protocol (protocole de vérification des certificats en ligne, OCSP) • CA de confiance par défaut • Profil du certificat	• Gestion : Gestion des certificats *Le certificat Cloud n'est pas encore pris en charge par Cloud NGFW.*
Déchiffrement	Cloud NGFW peut décrypter, inspecter et recrypter votre trafic d'entrée et de sortie de VPC en tant que décision basée sur une	• Décryptage SSL sortant • Inspection SSL entrante	• Politique de décryptage • Profil de décryptage • Proxy de transfert SSL (décryptage sortant)	• Gérer le décryptage

Certificats et décryptage	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	politique. Vous pouvez contrôler de manière granulaire le trafic de VPC à décrypter et celui à ne pas décrypter, ainsi que le type de décryptage SSL que vous souhaitez effectuer sur le trafic indiqué.. Pour activer le décryptage, vous configurez les certificats requis pour agir en tant que tiers de confiance d'une session.		• Inspection SSL entrante • Proxy SSH • Vérification des certificats du serveur • Exclusion du décryptage • Désactivation temporaire du décryptage SSL	

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
Protection contre les vulnérabilités IPS	La protection contre les vulnérabilités protège contre les menaces entrantes, dans lesquelles un attaquant tente d'exploiter la vulnérabilité d'un système pour violer votre réseau, Les vulnérabilités	• Meilleures pratiques	• Profil par défaut • Profil strict • Profil personnalisé (exceptions de menaces) • Signatures personnalisées des vulnérabilités	• Protection contre les vulnérabilités

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	du système peuvent être des dépassements de tampon, une exécution de code illégale, etc.		• Signatures Snort/Suricata	
Logiciel anti-espion	Le logiciel antispyware détecte et bloque les menaces sortantes, en particulier les activités de commande et de contrôle (C2), initiées par des charges de travail infectées par un logiciel malveillant (cyberattaque exploitée) dans votre VPC AWS. Vous pouvez également définir des modèles d'expressions régulières personnalisés pour identifier les communications des logiciels espions aux téléphones fixes.	• Meilleures pratiques	• Profil par défaut • Profil strict • Profil personnalisé (exceptions de menaces) • Signatures personnalisées de logiciels espions • Signatures Snort/Suricata	• Logiciel anti-espion
Blocage des fichiers	Le blocage de fichiers vous permet de contrôler de manière granulaire les types de fichiers de votre trafic de	• Meilleures pratiques et personnalisations	• Profil de base • Profil strict • Profil personnalisé	• Blocage des fichiers

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	VPC dans une direction spécifiée (entrant/sortant/ les deux). Vous pouvez bloquer de façon proactive les fichiers réputés porter des menaces ou qui n'ont pas de cas d'utilisation réel pour le chargement et le téléchargement.			
Antivirus	L'antivirus détecte et protège contre les logiciels malveillants dissimulés dans des fichiers compressés, des exécutables, des fichiers PDF et des virus HTML et JavaScript dans votre trafic de VPC	• Meilleures pratiques	• Profil par défaut • Profil personnalisé (exceptions de menaces)	• Anti-Virus
Analyse WildFire	Cloud NGFW détecte et transfère des fichiers et des exécutables de votre trafic de VPC vers le service cloud WildFire™ pour analyse, et effectue également une analyse ML en ligne de certains	—	Analyse WildFire	Analyse WildFire

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	fichiers. Si une menace est détectée sur les fichiers, WildFire crée des protections pour bloquer les logiciels malveillants et distribue une protection contre cette menace à l'échelle mondiale en moins de cinq minutes.			
Filtrage d'URL	Le filtrage des URL analyse le trafic de VPC et contrôle les URL accédées par vos charges de travail de VPC (trafic en clair et crypté) en effectuant une analyse en ligne et en comparant avec les catégories d'URL gérées par Palo Alto Networks ou les catégories personnalisées que vous fournissez.	• Contrôle d'accès pour les catégories d'URL gérées par Palo Alto Networks • Catégories d'URL personnalisées	• Contrôle d'accès pour les catégories d'URL gérées par Palo Alto Networks et les catégories d'URL personnalisées • Catégorisation en ligne dans le cloud	• Contrôle d'accès pour les catégories d'URL gérées par Palo Alto Networks et les catégories d'URL personnalisées • Catégorisation en ligne dans le cloud
Sécurité DNS	La sécurité DNS protège les requêtes DNS sortantes de vos VPC contre les menaces telles que la	—	Sécurité DNS	Sécurité DNS

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	tunnellisation DNS, la détection des algorithmes de génération de domaine (DGA), les domaines de logiciels malveillants, etc.			
Filtrage des données et DLP d'entreprise	Le filtrage des données détecte les informations sensibles dans votre trafic de VPC, telles que les numéros de carte de crédit ou de sécurité sociale ou les documents internes de l'entreprise, et empêche ces données de quitter votre environnement AWS. Avec le DLP d'entreprise, vous bénéficiez d'un filtrage avancé des données sur votre trafic de VPC grâce à une liste prédéfinie de modèles de données avec une analytique basée sur le cloud.	—	• Modèles prédéfinis, expressions régulières et propriétés de fichiers • Enterprise DLP	*DLP n'est actuellement pas pris en charge.*
Groupes de profils de sécurité	Un groupe de profils de sécurité est un ensemble de profils de	—	• Groupes de profils de sécurité	• Groupes de profils de sécurité

Services de sécurité	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	sécurité qui peut être traité comme une unité puis facilement ajouté à des politiques de sécurité.			

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

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
XFF	Le trafic vers vos charges de travail de VPC peut être passé par plus d'un serveur proxy (tel que CDN ou ALB) avant d'atteindre le Cloud NGFW. S'il y a un en-tête XFF existant, ces proxys lui ajoutent son adresse IP ou l'ajoutent avec son adresse IP. Par conséquent, l'en-tête de requête XFF peut contenir plusieurs adresses IP séparées par des virgules. Le Cloud NGFW utilise le champ d'en-tête HTTP X-Forwarded-For (XFF) qui identifie l'adresse IP d'origine du client. Le Cloud NGFW utilise toujours la dernière adresse ajoutée dans l'en-tête XFF pour appliquer la politique.	• Support des en-têtes XFF dans les politiques • Afficher les valeurs XFF dans les journaux	• Utiliser les valeurs XFF dans la politique • Afficher les valeurs XFF dans les journaux • Afficher les valeurs XFF dans les rapports	*XFF n'est actuellement pas pris en charge.*
NAT	Les pare-feu Palo Alto Networks peuvent imposer le NAT de	NAT de sortie	NAT de sortie	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	destination sur votre trafic de VPC entrant et le NAT source sur votre trafic de VPC sortant.			
Proxy DNS	Lorsque vous configurez Cloud NGFW en tant que proxy DNS, il agit comme un intermédiaire entre les clients et les serveurs, et comme un serveur DNS en résolvant les requêtes du cache DNS ou en transférant les requêtes à d'autres serveurs DNS. Cette page vous permet de configurer les paramètres qui déterminent comment le pare-feu sert de proxy DNS.	—	—	—
Gestion d'interface	Les pare-feu Palo Alto Networks vous permettent de configurer des VLAN, des câbles virtuels Link Layer Discovery Protocol (protocole de découverte de la couche de liaison – LLDP),	—	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	Bidirectional Forwarding Detection (détection de transfert bidirectionnel – BFD) sur leurs interfaces			
QoS	Les pare-feu Palo Alto Networks vous permettent de spécifier le trafic nécessitant un traitement préférentiel ou une limitation de bande passante. Les règles QoS vous permettent d'exécuter de manière fiable les applications et le trafic à priorité élevée avec une capacité réseau limitée.	—	—	—
Gestion du routage	Les pare-feu Palo Alto Networks vous permettent de configurer un routage statique et des protocoles de routage (BGP, BFD, OSPF, OSPFv3, multicast, RIPv2 et des filtres).	—	—	—
Gestion de tunnels IPSec	Les pare-feu Palo Alto Networks résilient les tunnels IPSec et	—	—	—

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

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d'appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	virtuelle et prennent en charge la sélection dynamique et intelligente des chemins d'accès en fonction des applications et des services et des conditions des liaisons que chaque application ou service est autorisé à utiliser.			
Transfert basé sur une politique	Les règles de transfert basé sur les politiques des pare-feu Palo Alto Networks permettent au trafic d'emprunter un chemin alternatif pour des raisons de sécurité ou de performances. Supposons que votre entreprise dispose de deux liaisons entre le siège social et la succursale : une liaison Internet bon marché et une ligne louée plus coûteuse. Afin de renforcer la sécurité, vous pouvez utiliser le transfert basé sur une politique pour envoyer	—	—	—

Services de mise en réseau	Description	Gestion native des politiques (Rulestacks)	Gestion des politiques de Panorama (groupes d’appareils cloud)	Gestion des politiques de Strata Cloud Manager (SCM)
	des applications qui ne sont pas du trafic crypté, notamment du trafic FTP, sur la ligne privée louée et tout autre trafic sur la liaison Internet. Sinon, afin d'améliorer les performances, vous pouvez choisir d'acheminer les applications essentielles sur la ligne louée et d'envoyer tout autre trafic, tel que la navigation Web, sur la liaison meilleur marché.			

Démarrage dans AWS Marketplace

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

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

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

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

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

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

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

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

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

les API Cloud NGFW pour créer les NGFW et d'appeler les API AWS pour créer les terminaux NGFW dans les VPC clients.

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

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

Démarrer à partir d’un compte AWS Members

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

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

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

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

- Abonnement Cloud NGFW PAYG SaaS
- Sécuriser votre accès actuel au Cloud NGFW à l’aide de SSO et de la MFA
- Utilisateur multilocataire d’un utilisateur unique pris en charge sur plusieurs locataires
- Ajouter plusieurs comptes AWS

Abonnement Cloud NGFW PAYG SaaS

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

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

Kinesis Data Firehose. Pour que Cloud NGFW envoie ces journaux à la destination prévue, vous devez fournir les autorisations nécessaires.

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

La pile préremplit les destinations de journalisation pour le groupe de journaux CloudWatch et le flux de diffusion Kinesis Data Firehose avec une destination appelée **PaloAltoCloudNGFW**. Le champ de compartiment S3 n'est pas prérempli. Si vous souhaitez envoyer les journaux vers une autre destination, vous devez créer cette destination et remplacer la valeur par défaut par le nom avant de terminer la création de la pile.

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

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

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

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

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

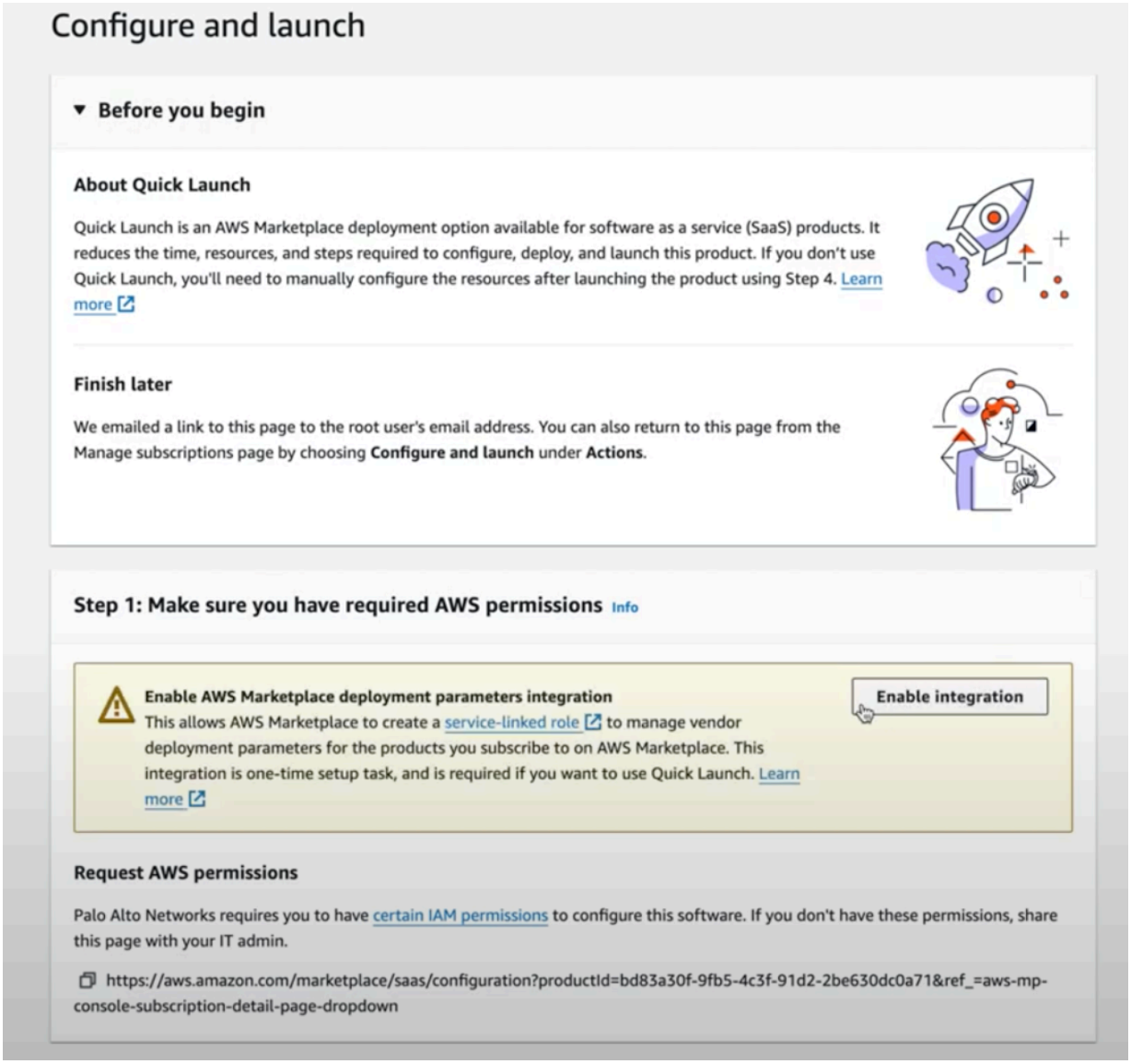
STEP 1 | Connectez-vous à la console AWS.

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

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

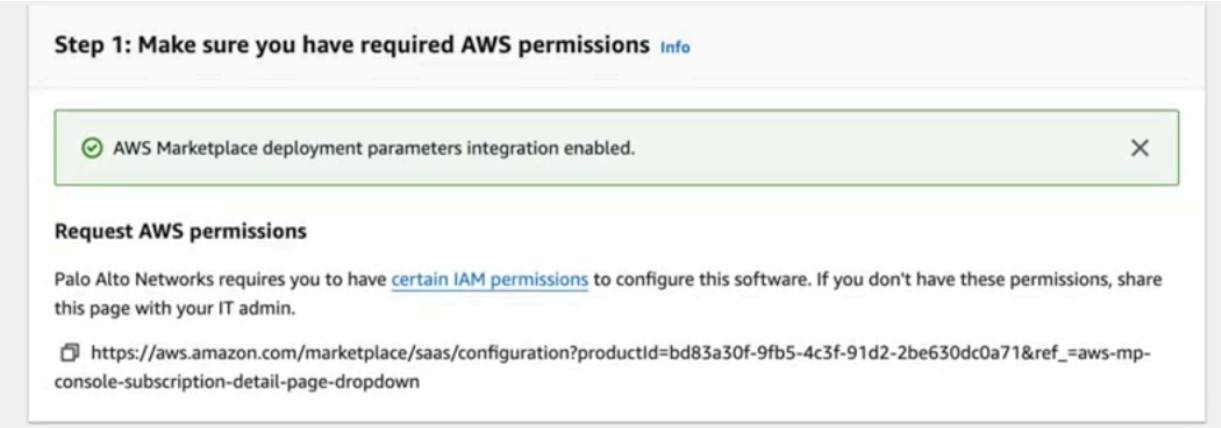
STEP 4 | Cliquez sur **Configurer le produit**. Cela lance la page Configure and Launch (Configurer et lancer) (SaaS Quick Launch [Lancement rapide de SaaS]) sur AWS Marketplace. Palo Alto Networks a

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

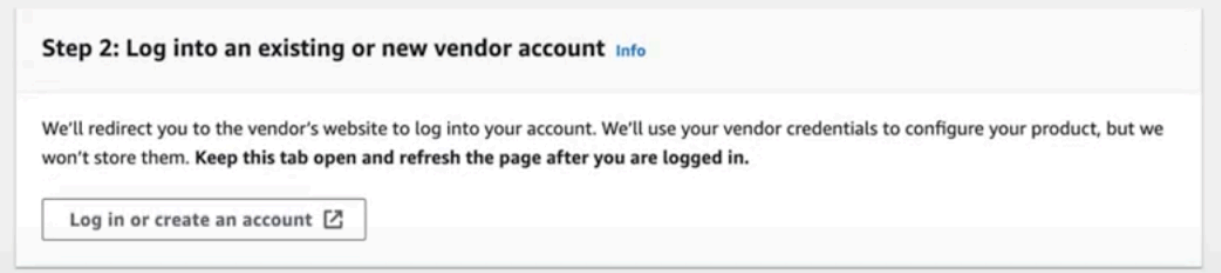


STEP 5 | Cliquez sur **Enable integration (Activer l’intégration)** sur la page Configurer et lancer du lancement rapide afin de vous assurer de disposer des autorisations IAM requises d’AWS.

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



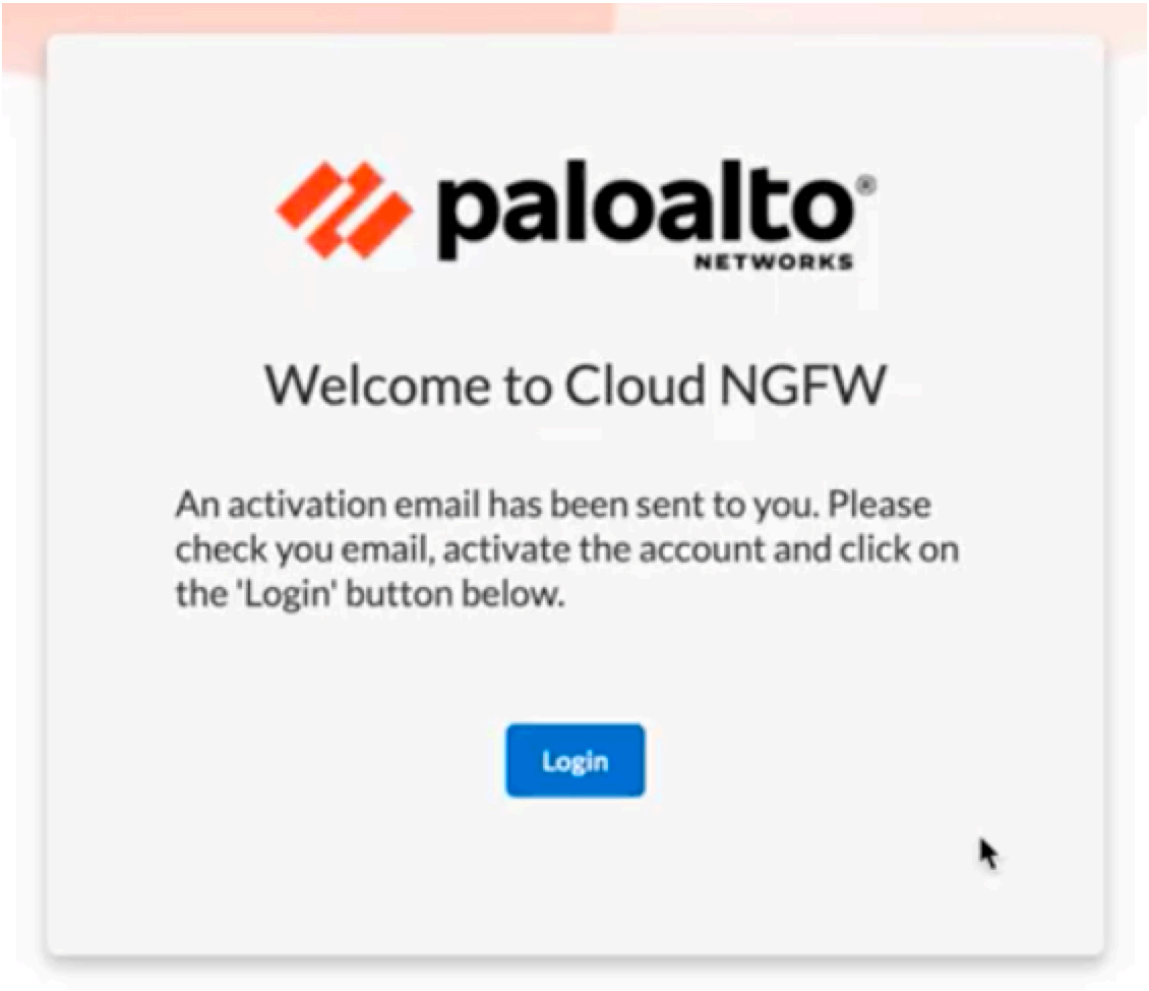
STEP 6 | Cliquez sur le bouton **Login or create an account (Se connecter ou créer un compte)** pour vous connecter à un compte existant ou en créer un nouveau sur le site Web du fournisseur. Cela vous amène à une page d'enregistrement de création de locataire du Cloud NGFW pour le locataire AWS.



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

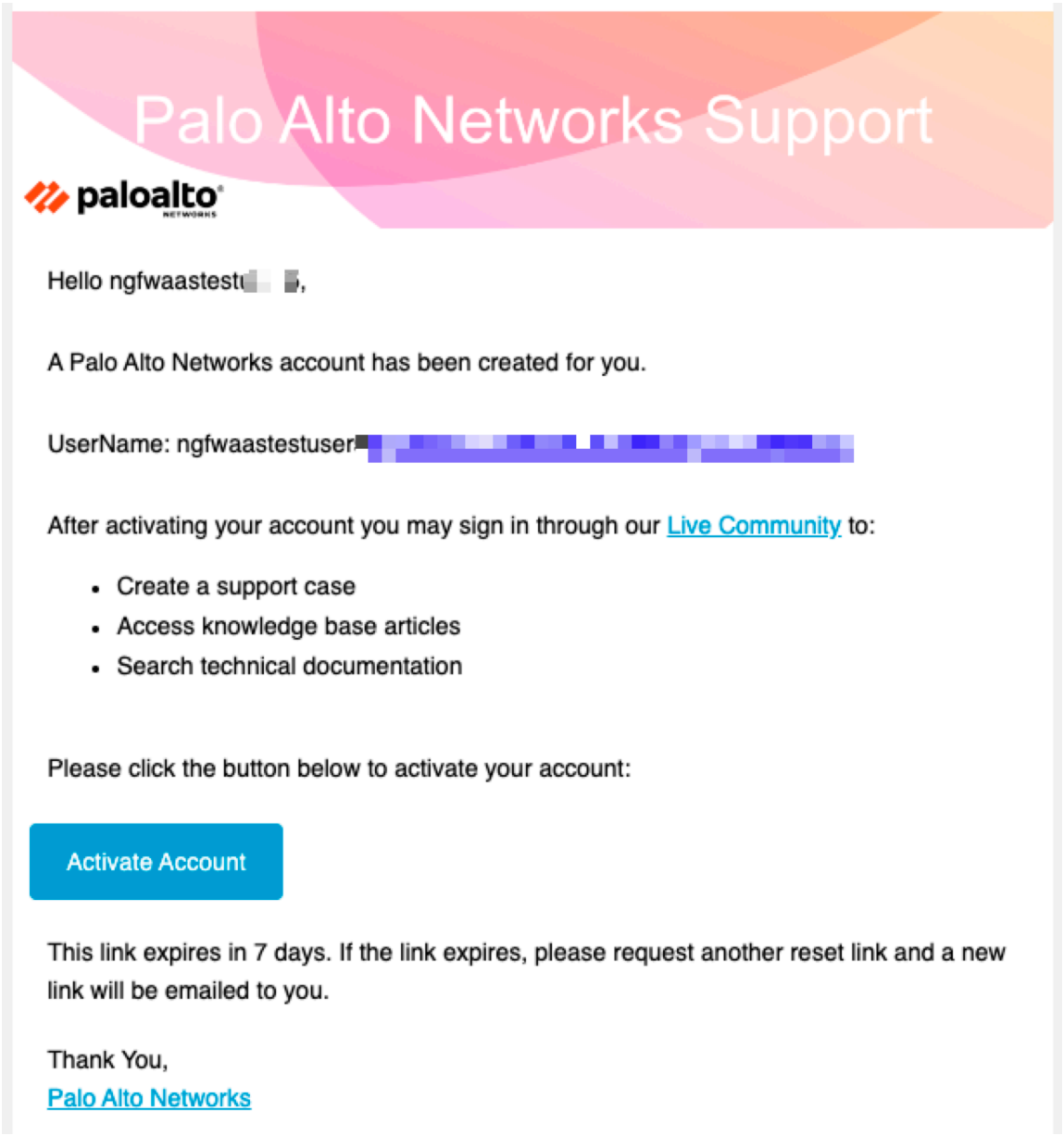
   Vous devez utiliser le même e-mail lorsque vous vous connectez au service Cloud NGFW pour la première fois. De plus, lors de la première connexion, cette adresse e-mail est utilisée pour créer le premier utilisateur, un admin locataire. En outre, le domaine de l'adresse e-mail des utilisateurs invités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

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

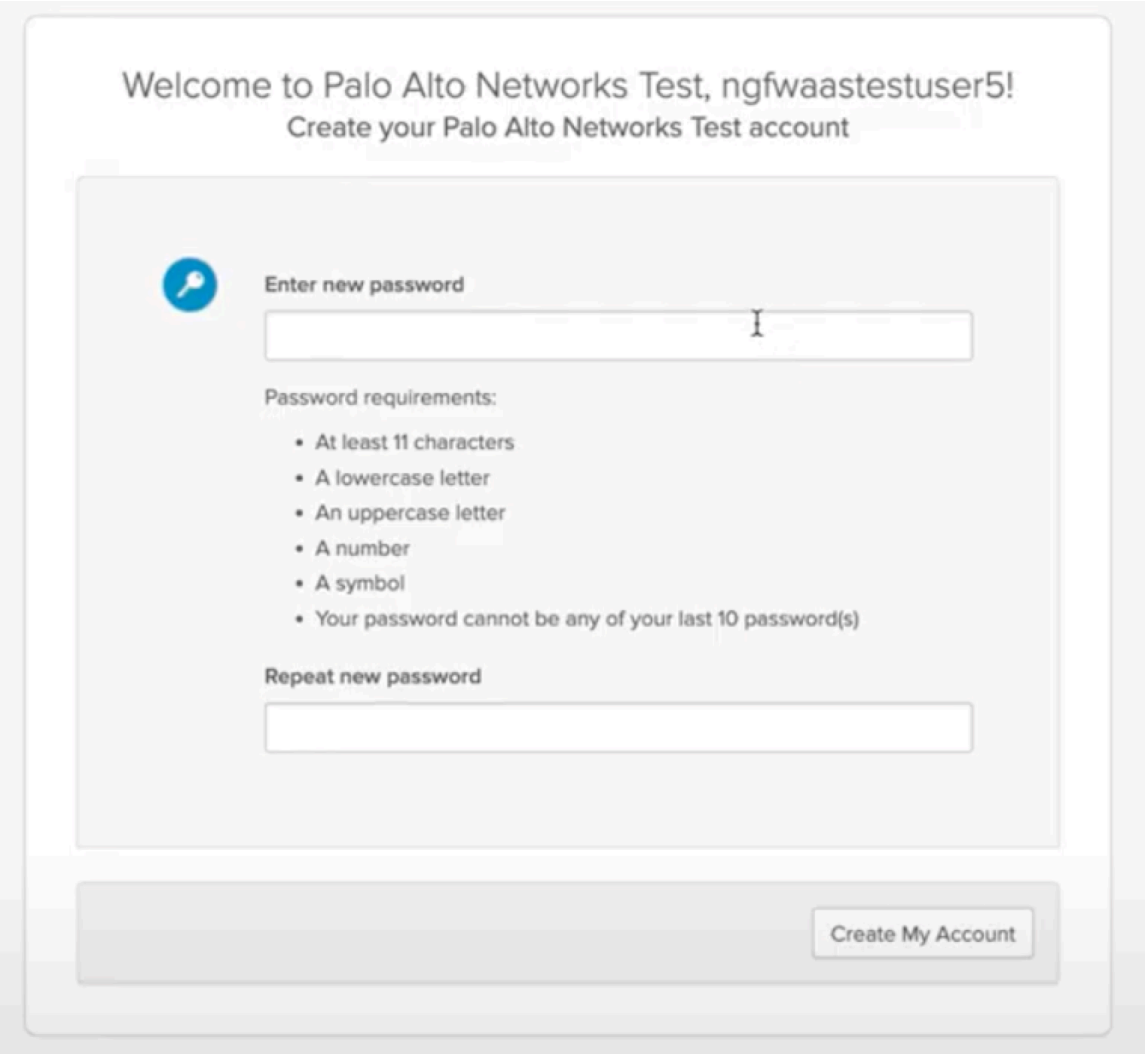


4. Cliquez sur le bouton **Activate Account (Activer le compte)** dans l’e-mail que vous avez reçu.

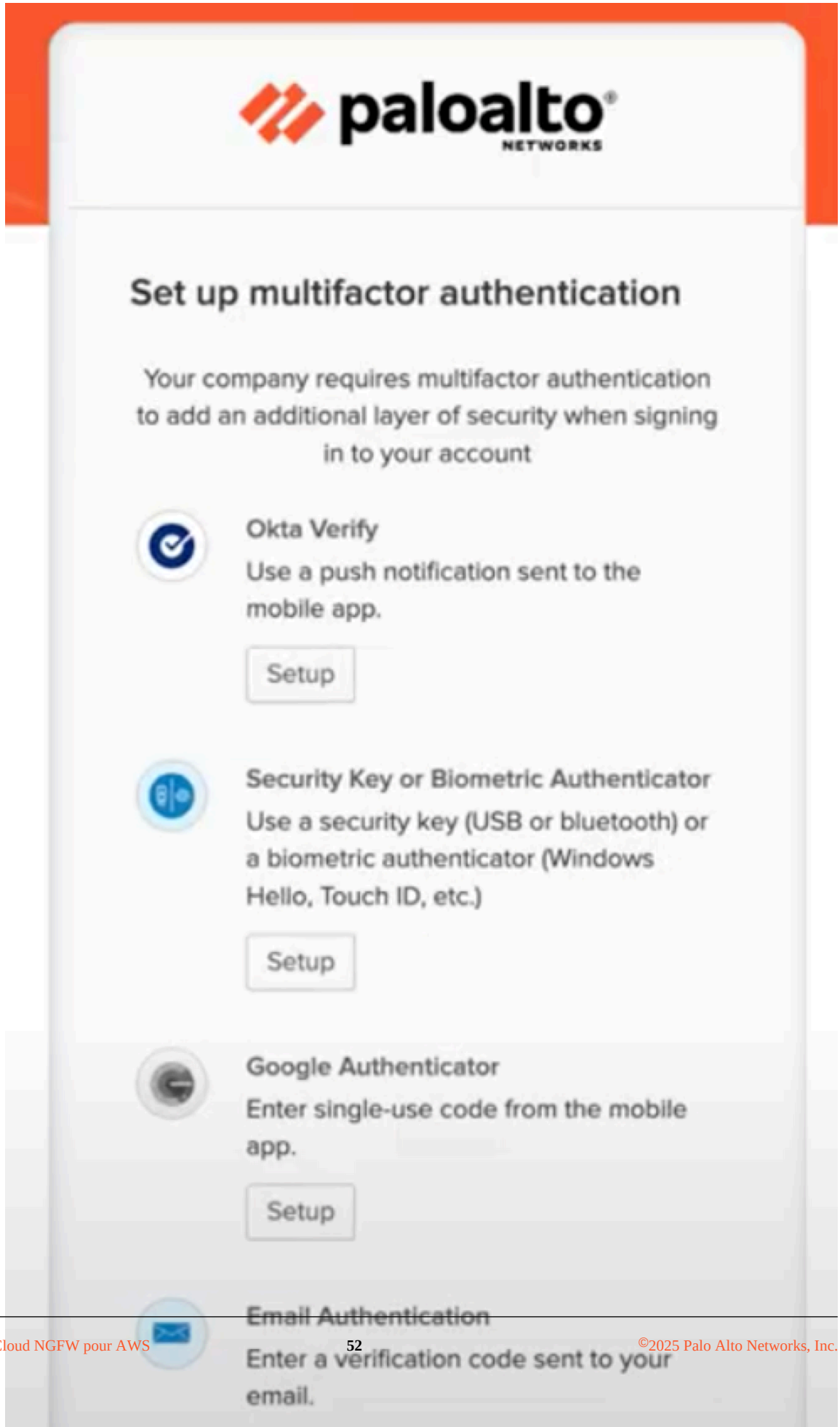
   Le lien reste actif pendant 7 jours. Si vous ne cliquez pas sur le lien dans les 7 jours, vous devrez demander l’envoi d’un e-mail d’activation.



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



7. Configurez votre authentification multifactorielle (MFA).

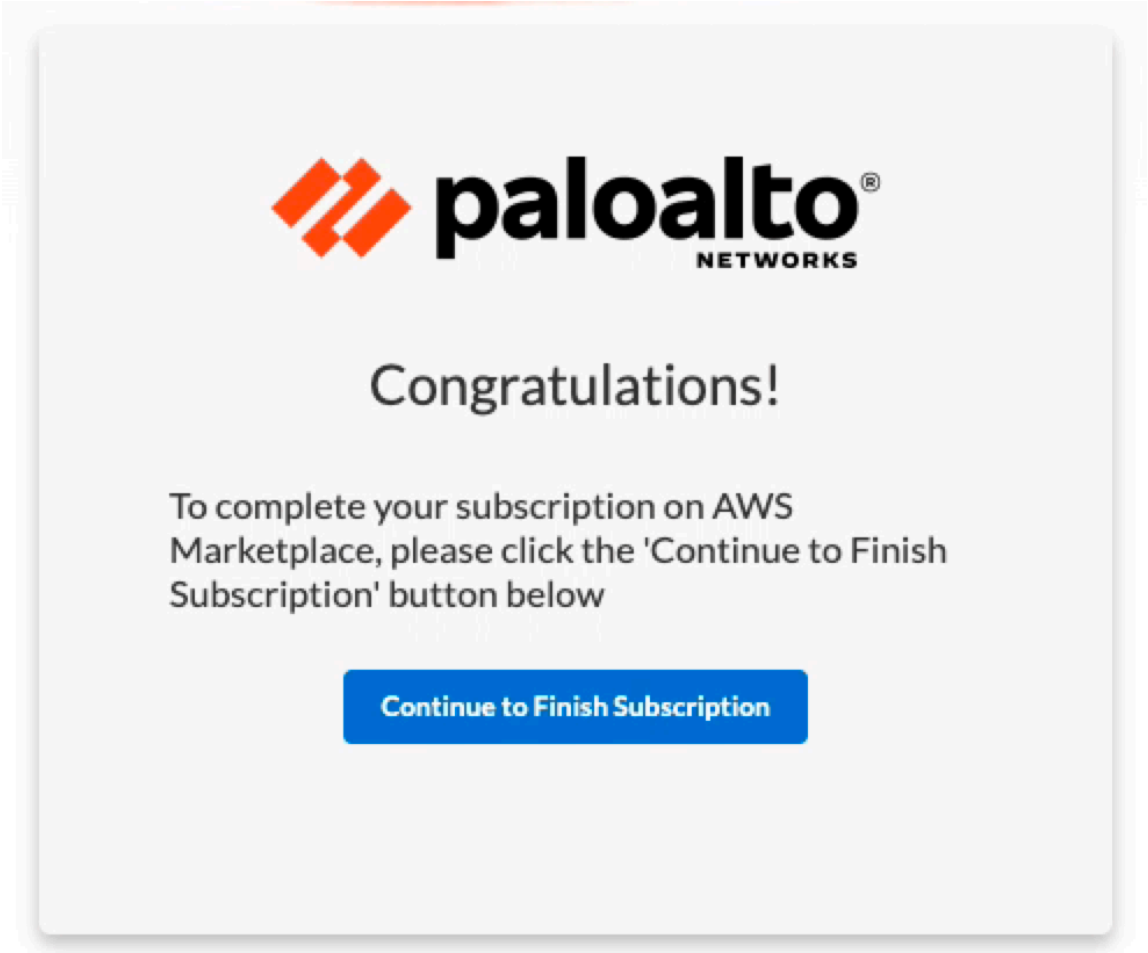


Si vous n'êtes pas encore enregistré à l'authentification multifactorielle, mais que vous connaissez votre mot de passe SSO, vous êtes invité à vous enregistrer à l'authentification multifactorielle lors de votre première connexion à l'une des applications. Créez un ticket d'assistance si vous souhaitez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

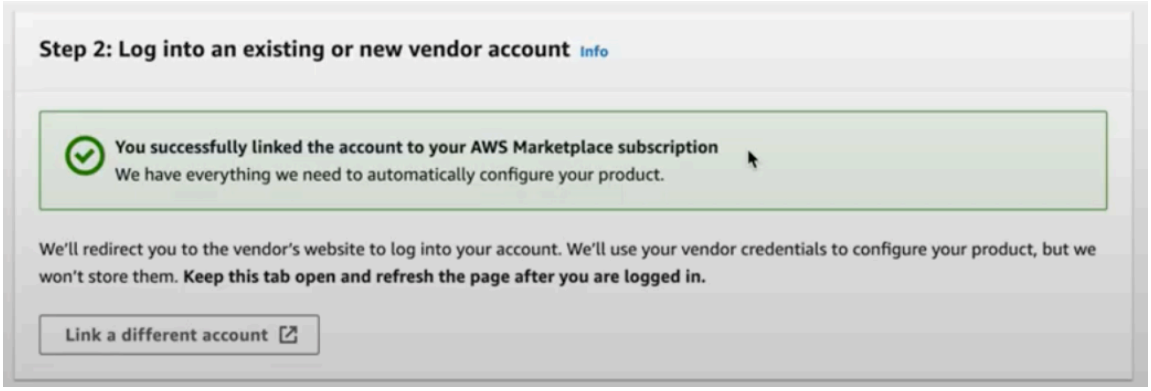
8. Choisissez l'une des méthodes MFA et cliquez sur **Setup (Configuration)**.
9. Terminez le processus de vérification MFA : par exemple, si vous cliquez sur le bouton Configuration pour l'authentification par e-mail, vous serez invité à cliquer sur **le bouton Send me the code (Envoyez-moi le code)**.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

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

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



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



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

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

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

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

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

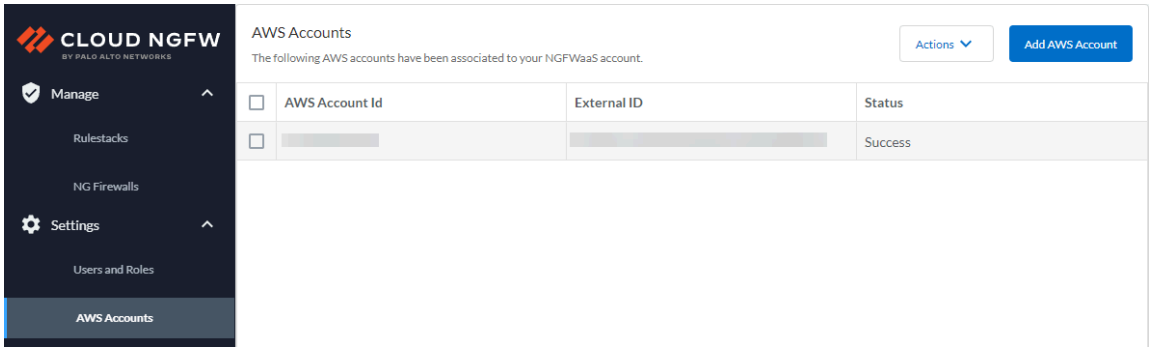
STEP 8 | Dans la section Capacités en bas de la console CFT, cochez **I acknowledge that AWS CloudFormation might create IAM resources (Je reconnais qu'AWS CloudFormation peut créer des ressources IAM)**.

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

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

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

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

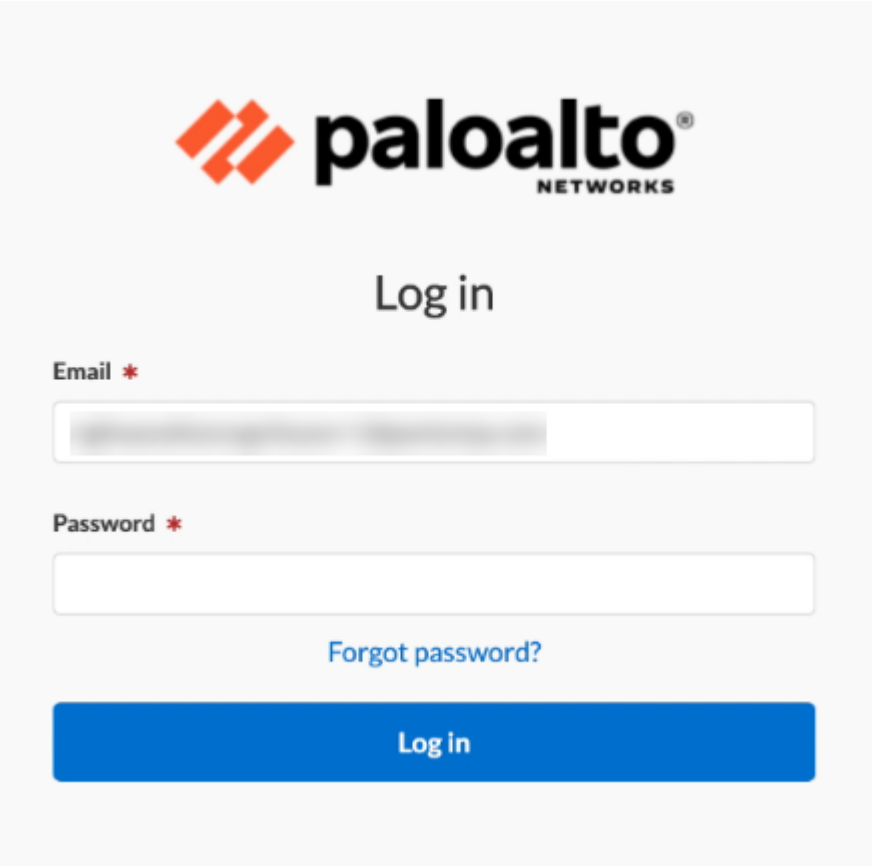


SAML 2.0 peut être utilisé comme fournisseur d'identité pour Cloud NGFW pour AWS. Pour plus d'informations, consultez Gérer les intégrations de fournisseurs d'identité tiers via les services communs *et* Comment activer un fournisseur d'identité tiers (IDP).

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

informations d’identification de connexion sont utilisées pour plusieurs locataires, la page de connexion vous invite à sélectionner le locataire que vous souhaitez configurer.

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

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

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

Ajouter plusieurs comptes AWS

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

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

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

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

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

Dix comptes en attente sont pris en charge par locataire.

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

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

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

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

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

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

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

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

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

STEP 1 | Accédez à votre abonnement sur AWS Marketplace.

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

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

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

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

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

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

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

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

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

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

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

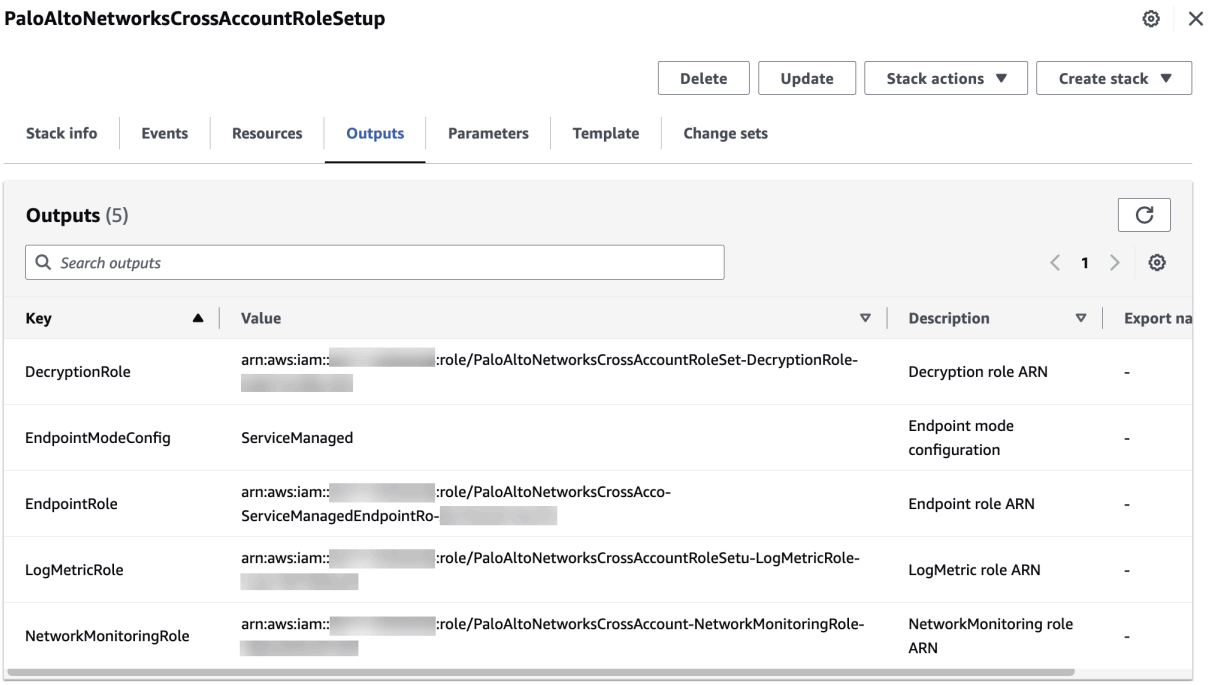
STEP 12 | Connectez-vous à votre compte AWS.

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

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

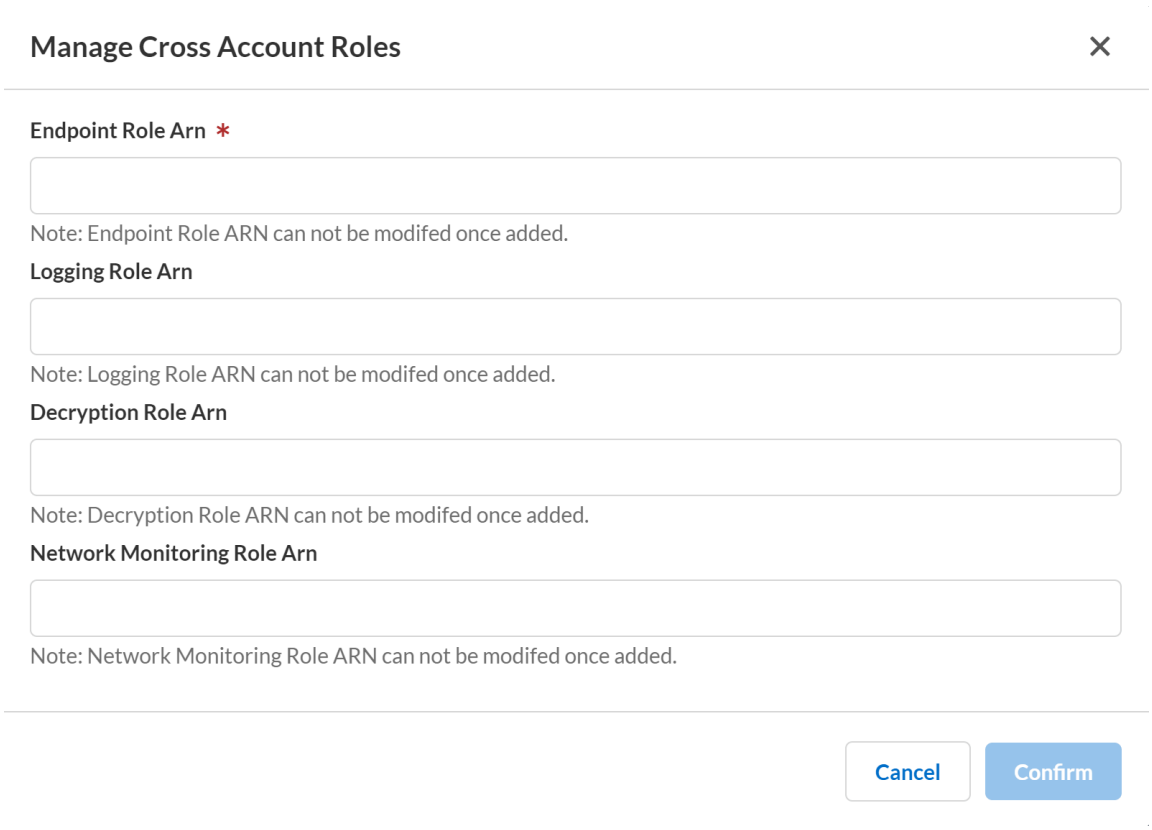
STEP 15 | Cliquez sur **Create Stack (Créer une pile)**.

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



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

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



Prise en main à partir d’un compte AWS Firewall Manager

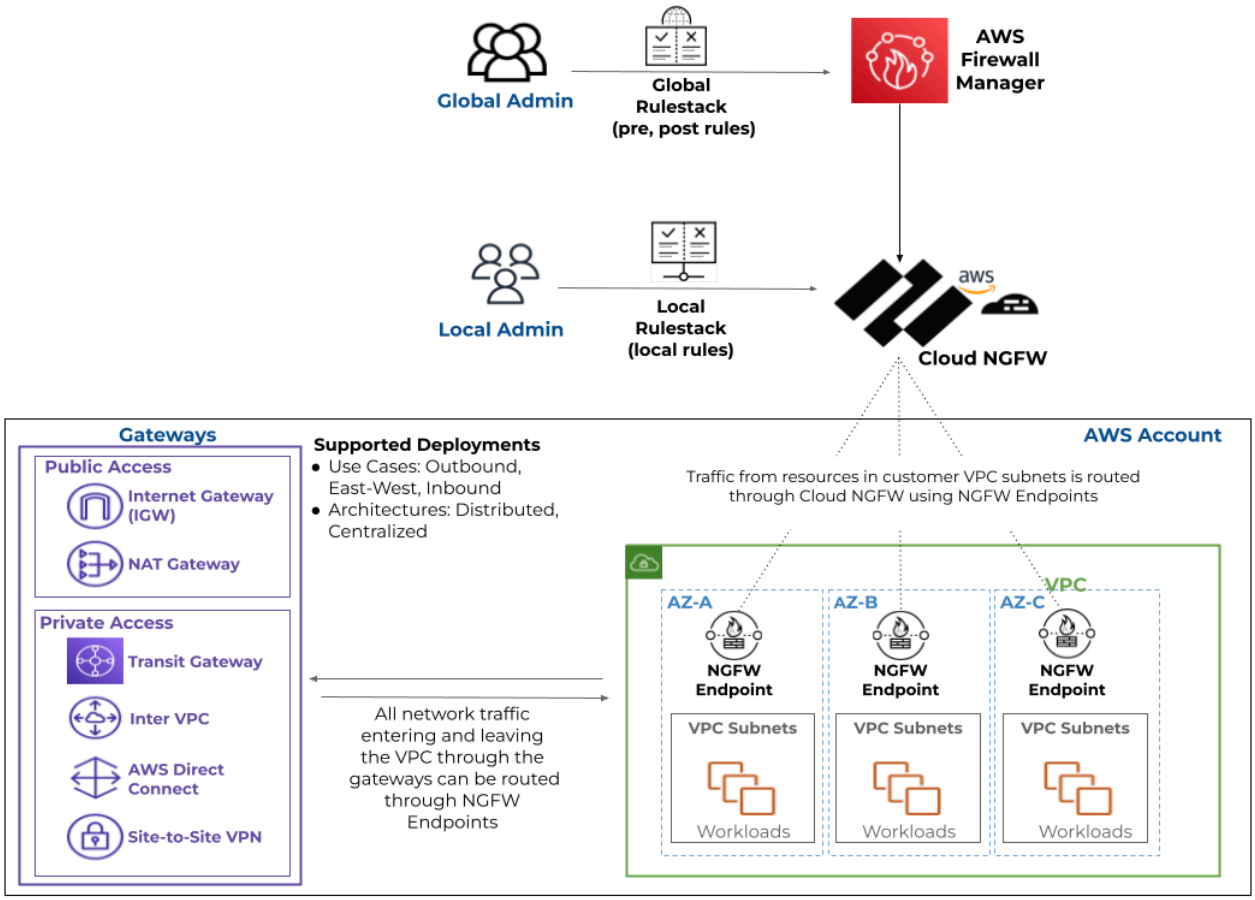
Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Cloud NGFW pour AWS	❑ Abonnement Cloud NGFW ❑ Compte de support client (CSP) de Palo Alto Networks ❑ Compte AWS Marketplace ❑ Rôle utilisateur (locataire ou administrateur)

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

AWS Firewall Manager fournit un flux de travail qui vous permet de :

- déployer le Cloud NGFW en tant que politique FMS ;
- sélectionner une région et un mode de déploiement ;
- créer une rulestack globale ;
- configurer des terminaux NGFW ; et
- définir la portée du Cloud NGFW dans votre organisation.

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



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

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

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

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

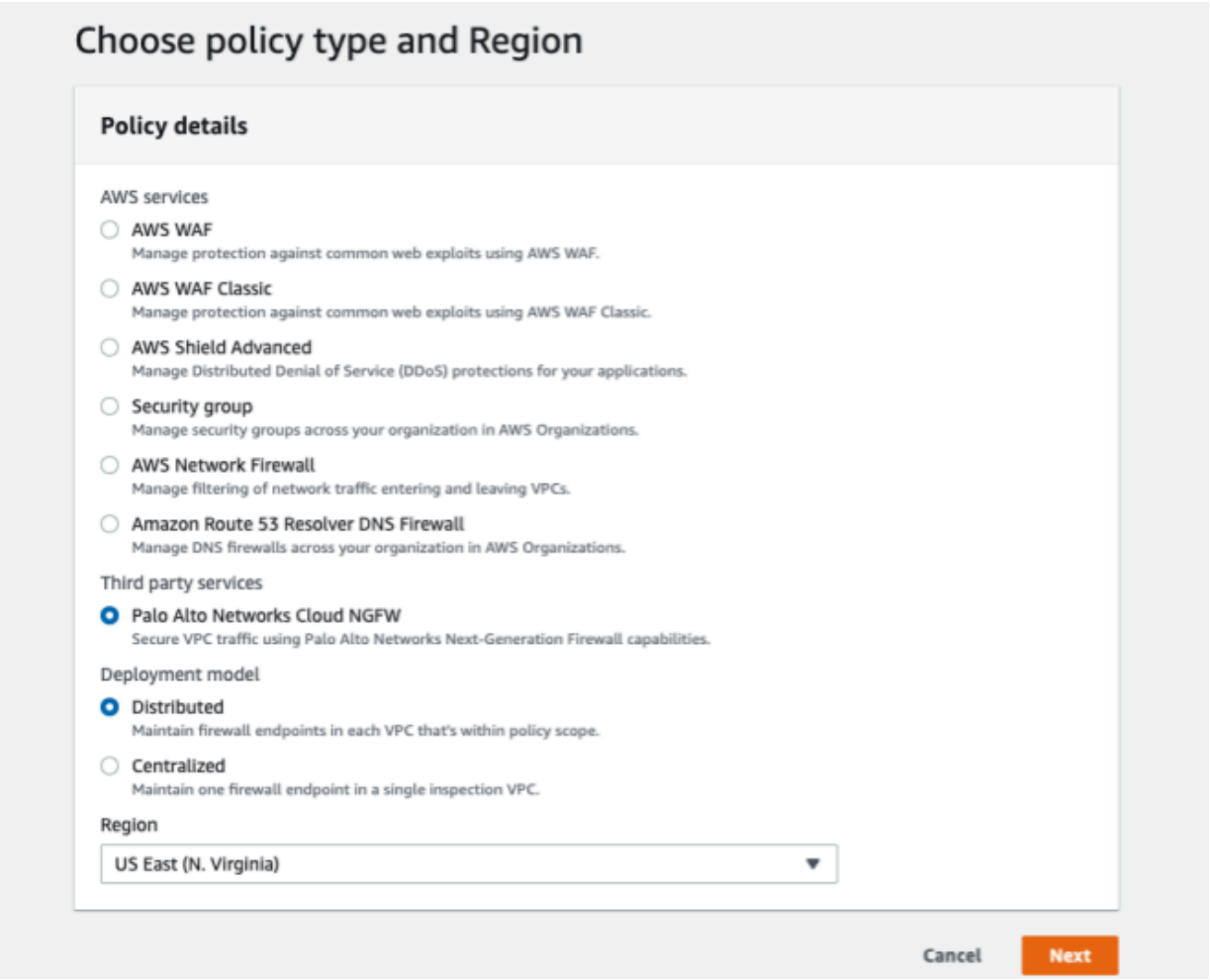
1. Connectez-vous à la console AWS et sélectionnez **Services** > **AWS Firewall Manager** > **Settings (Paramètres)**.
2. Sous Third Party Firewall Association Status (État de l’association de pare-feu tiers), sélectionnez Palo Alto Networks Cloud NGFW.
3. Cliquez sur **Associate (Associer)**.

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

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

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

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



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

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

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

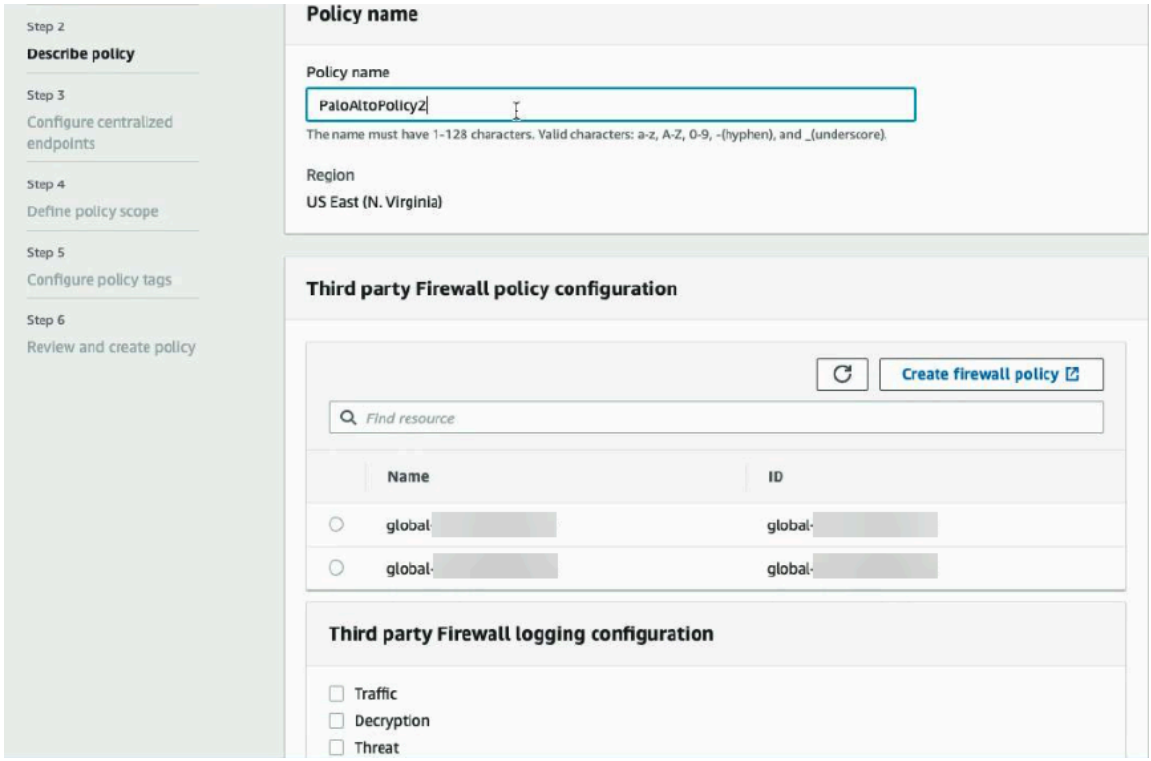
1. Entrez un **Policy Name (Nom de la politique)** descriptif.
2. Sélectionnez ou créez une **Third Party Firewall Policy Configuration (Configuration de politique de pare-feu tiers)**.

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

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

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

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



STEP 7 | Configurez les terminaux NGFW.

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

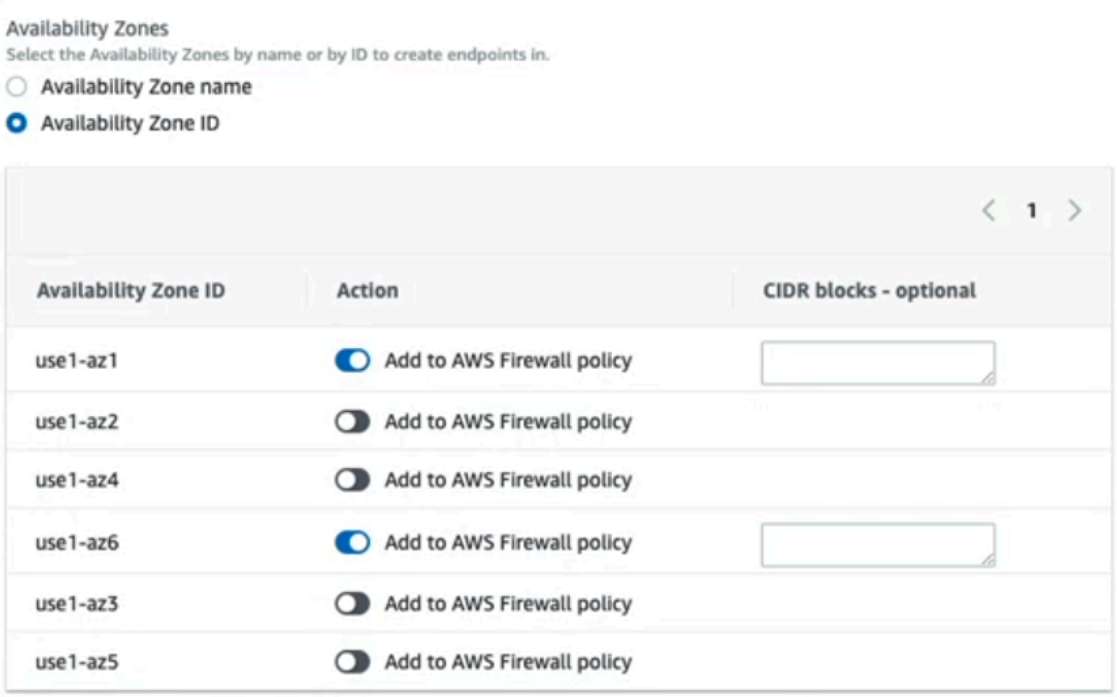
Vous sélectionnez les emplacements des terminaux NGFW en choisissant des noms de zone de disponibilité ou des ID de zone de disponibilité. Gardez à l'esprit que les noms des zones de

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

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

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

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



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

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

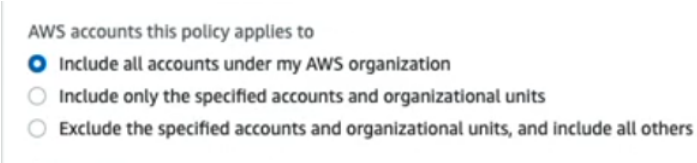
politiques Cloud NGFW FMS à tous les comptes AWS et VPC de votre organisation ou spécifier un sous-ensemble de comptes et/ou de VPC.

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

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

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

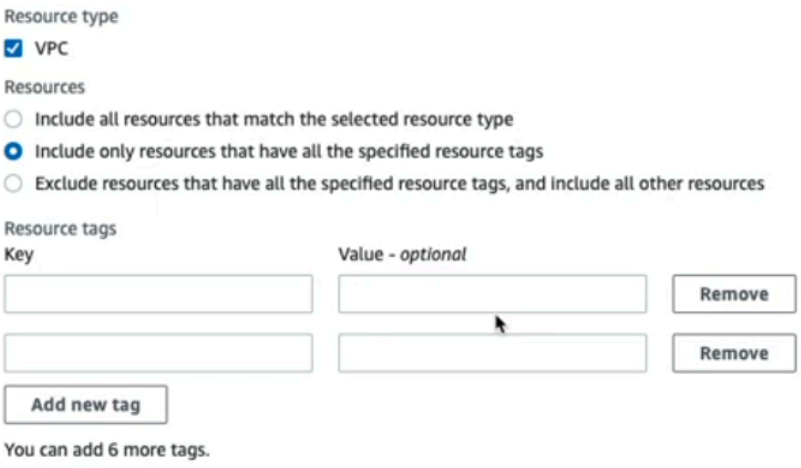
   Si vous choisissez d'inclure ou d'exclure un sous-ensemble de comptes et d'unités d'organisation, la console FMS affiche un champ qui vous permet de spécifier ces comptes et unités d'organisation. Cliquez sur **Edit List (Modifier la liste)** pour créer votre liste d'inclusion ou d'exclusion.

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

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

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

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

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

Essai gratuit de Cloud NGFW pour AWS

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

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

Pour activer cet essai gratuit, le Cloud NGFW associe les crédits d’essai gratuit au locataire que vous venez de créer. Ces crédits vous permettent de créer jusqu’à deux pare-feu sécurisant jusqu’à 100 Go de trafic. Vous pouvez :

- Intégrer vos comptes AWS à vos locataires.
- Créer jusqu’à deux ressources NGFW sur vos VPC AWS.
- Rédiger des rulestacks.

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

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