paloalto TECHDOCS

Démarrage avec CN-Series

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

August 25, 2023

Table of Contents

Pare-feu CN-Series pour Kubernetes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Les pare-feu natifs en conteneurs (CN-Series) Palo Alto Networks sont intégrés nativement dans Kubernetes (k8s) pour offrir une visibilité complète de la couche 7, une segmentation au niveau de l'application, une sécurité DNS et une protection contre les menaces avancées du trafic passant par des zones approuvées dans les environnements de cloud public et de centre de données. Ils vous permettent d'isoler et de protéger les charges de travail, les piles d'applications et les services, même entre les hôtes ou lorsque des conteneurs individuels sont augmentés ou réduits, et d'appliquer de manière constante les politiques de sécurité basées sur des étiquettes Kubernetes.

Le déploiement d'applications dans un environnement Kubernetes est un processus dynamique et les équipes suivantes sont souvent impliquées dans le cycle de vie des conteneurs :

- **Administrateur de la plateforme (PAAS)** – Gère les clusters Kubernetes et d'autres composants de l'infrastructure dans le cloud public et les centres de données.
- **Équipes d'applications** – Déploient leurs applications conteneurisées individuelles et d'autres applications dans les espaces de noms et projets Kubernetes fournis par l'administrateur PAAS.
- **Administrateur de la sécurité** – Configure la sécurité de l'ensemble du déploiement, y compris les clusters Kubernetes et les applications conteneurisées individuelles.

Dans ce scénario dynamique impliquant de nombreuses équipes, il n'est pas facile d'assurer la gestion et la surveillance de la sécurité. Le CN-Series permet à votre administrateur de la sécurité de configurer la sécurité pour les applications conteneurisées dans un large éventail d'environnements, dont les k8s gérés par le fournisseur cloud (p. ex. GKE, EKS, AKS, AliCloud ACK), les k8s gérés par le client (p. ex. OpenShift) et les k8s natifs sur le cloud public ou les centres de données sur site. Le CN-Series utilise des constructions Kubernetes et une politique basée sur les métadonnées afin que les équipes puissent automatiser le déploiement et appliquer efficacement la politique de sécurité pour une protection cohérente contre les menaces connues et inconnues.

Sécurisation des charges de travail Kubernetes avec le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Les pare-feu CN-Series se déploient sous forme de deux ensembles de pods : un pour le plan de gestion (CN-MGMT) et un autre pour le plan de données du pare-feu (CN-NGFW). Le plan de données du pare-feu s'exécute comme un ensemble de daemons, permettant à une seule commande depuis Kubernetes de déployer des pare-feu sur tous les nœuds d'un cluster Kubernetes à la fois. Le plan de gestion fonctionne comme un service Kubernetes.

Les pare-feu CN-Series sont gérés via la console Panorama. Un plug-in Kubernetes dans Panorama fournit des informations contextuelles sur les conteneurs dans un environnement, ce qui permet de mettre en œuvre de manière transparente des politiques de sécurité réseau basées sur le contexte.

Par exemple, les espaces de noms Kubernetes peuvent être utilisés pour définir une source de trafic dans une politique de pare-feu. Vous pouvez déployer des pare-feu CN-Series dans des environnements Kubernetes hébergés sur site ou dans des cloud publics.

Les pare-feu CN-Series peuvent également être déployés dans des offres Kubernetes gérées dans le cloud, notamment Google Kubernetes Engine (GKE®), Azure Kubernetes Service (AKS), Alibaba Cloud (ACK) et Amazon Elastic Kubernetes Service (EKS). Vous pouvez également déployer via les gestionnaires de packages Kubernetes, tels que Helm.

CN-Series fournit une protection contre les menaces pour le trafic entrant, sortant et est-ouest entre les zones approuvées de conteneurs et d'autres types de charges de travail, sans ralentir la vitesse du développement.

Déployez le CN-Series pour une visibilité Couche 7 dans le trafic du conteneur et renforcez les politiques de sécurité avec des profils de prévention des menaces pour protéger le trafic autorisé au-delà des limites de l'espace de noms Kubernetes et partagez ce contexte avec le matériel et les pare-feu VM-Series pour assurer un modèle d'application des politiques constant sur la totalité de votre environnement de cloud hybride.

Empêcher l'exfiltration de données des environnements Kubernetes :

Les pare-feu CN-Series offrent une multitude de fonctionnalités de sécurité pour empêcher l'exfiltration de données sensibles des environnements Kubernetes. L'inspection du contenu du trafic, y compris l'inspection du trafic chiffré TLS/SSL, garantit que les paquets contenant des charges utiles malveillantes sont identifiés et corrigés. Le filtrage des URL interdit les connexions sortantes vers des sites Web potentiellement néfastes, y compris les référentiels de codes malveillants.

Empêcher la propagation latérale des menaces à travers les limites de l'espace de noms Kubernetes :

Les limites de confiance entre les applications sont des emplacements logiques pour appliquer des politiques de segmentation qui empêchent le mouvement latéral des menaces. Dans de nombreux environnements Kubernetes, l'espace de noms Kubernetes constitue la limite de confiance. Les pare-feu CN-Series peuvent appliquer des politiques de prévention des menaces entre les espaces de noms Kubernetes ainsi qu'entre un espace de noms Kubernetes et d'autres types de charges de travail (par exemple, les machines virtuelles et les serveurs sans système d'exploitation), pour empêcher les menaces de se déplacer entre vos applications cloud natives et votre infrastructure existante.

Concepts clés de CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Le pare-feu CN-Series est conçu pour fournir les outils dont vous avez besoin pour sécuriser les applications dans votre environnement conteneurisé. Pour comprendre comment CN-Series s'intègre dans un réseau conteneurisé, il importe de comprendre certains concepts clés.

- **Cluster** – la base de votre environnement conteneurisé ; toutes vos applications conteneurisées s'exécutent sur un cluster.
- **Nœud** – selon le cluster, un nœud peut être une machine virtuelle ou physique qui contient les services nécessaires requis pour les pods.
- **Pod** – la plus petite unité de calcul déployable que vous pouvez déployer et gérer dans Kubernetes. Le pare-feu CN-Series est déployé dans une architecture PAN-OS distribuée sous la forme de deux pods : CN-MGMT et CN-NGFW. Voir Blocs de construction principaux du pare-feu CN-Series pour plus d'informations.
- **Espace de noms** : un espace de noms est un cluster virtuel soutenu par un cluster physique. Dans un environnement où de nombreux utilisateurs sont répartis sur plusieurs équipes et fonctions, un espace de noms peut être utilisé pour les séparer sur un seul cluster.
- **Container Network Interface (CNI)** – un plug-in qui configure les interfaces réseau pour les conteneurs. En outre, le CNI supprime les ressources allouées utilisées pour la mise en réseau lorsqu'un conteneur est supprimé.
- **DaemonSet** – dans un déploiement Kubernetes, un DaemonSet garantit que certains ou tous les nœuds exécutent une copie d'un pod particulier. Lorsque des nœuds sont ajoutés à un cluster Kubernetes, une copie du pod défini par le DaemonSet est ajoutée à chaque nouveau nœud. Lorsque vous déployez le pare-feu CN-Series en tant que DaemonSet, une copie du pod CN-NGFW est déployée sur chaque nœud (jusqu'à 30 par paire CN-MGMT) de votre cluster.
- **Service Kubernetes** – une abstraction qui expose une application s'exécutant sur un ensemble de pods en tant que service réseau. Lorsque vous déployez CN-Series en tant que service, le nombre de pods CN-NGFW déployés est défini par vous lors de la configuration de vos fichiers yaml.
- **Kuberenetes CNF** – le déploiement CN-series-as-a-kubernetes-CNF résout les problèmes liés au trafic qui utilise le Service Function Chaining (SFC) via des entités externes telles que le routage natif du fournisseur de cloud, les vRouters et les commutateurs Top of Rack (TOR). Le mode de déploiement CN-series-as-a-kubernetes-CNF n'a pas d'impact sur les pods d'application.

- **Horizontal Pod Autoscaler (HPA)** – met automatiquement à l’échelle le nombre de pods dans un déploiement, un jeu de réplicas ou un ensemble avec état en fonction de diverses mesures telles que l’utilisation du processeur ou l’utilisation de la session.

  HPA est pris en charge sur CN-Series en tant que service Kubernetes uniquement.

- **HSF** – Hyperscale Security Fabric (HSF) CN-Series 1.0 de Palo Alto Networks est un cluster de pare-feu conteneurisés de nouvelle génération qui offrent une solution de pare-feu de nouvelle génération hautement évolutive et résiliente pour les fournisseurs de services mobiles déployant des réseaux 5G.

Blocs de construction principaux du pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

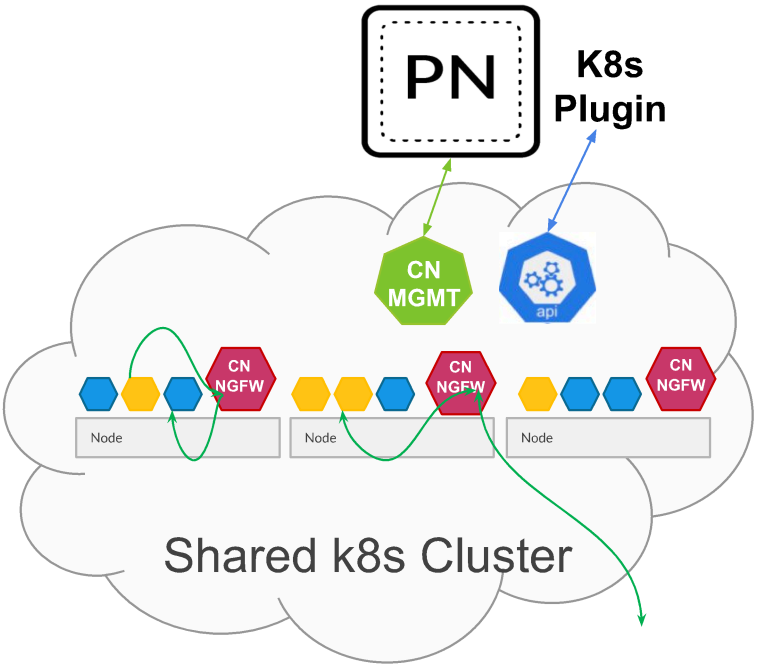
Le pare-feu CN-Series est un pare-feu nouvelle génération conteneurisé permettant la visibilité et la sécurité de vos charges de travail d'applications conteneurisées sur les clusters Kubernetes. Pour y parvenir, le pare-feu CN-Series utilise des constructions Kubernetes (K8s) natives et des composants Palo Alto Networks.

Les blocs de construction principaux pour déployer le pare-feu CN-Series sont :

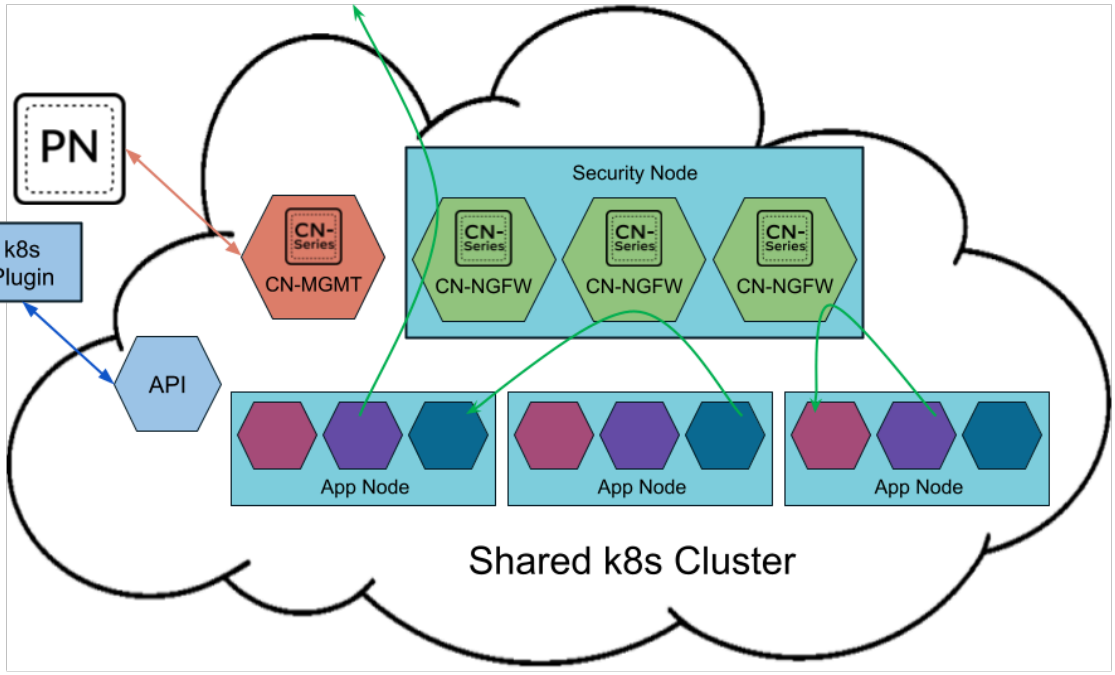
- **Fichiers de déploiement CN-Series** : pour déployer le pare-feu CN-Series dans votre environnement conteneurisé, vous devez télécharger et déployer les différents fichiers de déploiement CN-Series.
  - PAN-CN-MGMT : le conteneur init génère des certificats qui sont utilisés pour sécuriser la communication entre les instances des pods CN-MGMT et entre les pods CN-MGMT et les pods CN-NGFW.
  - PAN-CN-MGMT-CONFIGMAP
  - PAN-CN-MGMT-SECRET : permet à Panorama d'authentifier les pare-feu afin de pouvoir ajouter chaque pare-feu en tant qu'appareil géré. La clé d'authentification VM est requise pour la durée de vie du déploiement. Sans clé valide dans la requête de connexion, le pare-feu CN-Series ne pourra pas s'enregistrer auprès de Panorama.
  - PAN-CN-NGFW
  - PAN-CN-NGFW-CONFIGMAP
  - PAN-CNI
  - PAN-CNI-CONFIGMAP
  - PAN-CNI-MULTUS
- **Architecture PAN-OS distribuée avec pods CN-MGMT et CN-NGFW** – Les plans de gestion (CN-MGMT) et de données (CN-NGFW) du pare-feu conteneurisé sont séparés afin de permettre une meilleure protection de l'exécution pour les applications et de prendre en charge une empreinte plus petite. Les pods CN-MGMT et CN-NGFW sont déployés à l'aide d'images conteneurs et de fichiers manifestes YAML avec objets ConfigMap.
- **CN-MGMT** s'exécute en tant que StatefulSet pour garantir un volume persistant et est exposé comme service K8s pouvant être découvert au moyen d'un DNS dans l'environnement Kubernetes. Le CN-MGMT offre une tolérance aux pannes et un pod CN-MGMT unique peut gérer les pods CN-NGFW existants en cas de redémarrage ou de panne d'un pod CN-MGMT.
- **CN-NGFW** peut être déployé en tant que DaemonSet ou en tant que service Kubernetes. Les déploiements DaemonSet sont adaptés aux environnements Kubernetes avec des nœuds plus grands, des

pods nécessitant une faible latence et/ou une capacité de pare-feu élevée. CN-Series en tant que service Kubernetes est adapté aux environnements Kubernetes avec des nœuds plus petits et/ou nécessite un pare-feu plus dynamique.

- Lorsqu'elle est déployée **en tant que DaemonSet**,chaque instance du pod CN-NGFW peut sécuriser 30 pods d'application s'exécutant sur le même nœud. Cette architecture vous permet de placer le pod DaemonSet CN-NGFW sur chacun des nœuds pour lesquels vous souhaitez protéger des charges de travail dans un cluster. En outre, une paire de pods CN-MGMT peuvent connecter et gérer jusqu'à 30 pods CN-NGFW dans un même cluster. Pour plus d'informations sur les limites, reportez-vous à la section Performances et mise à l'échelle de CN-Series.



- Lorsqu'elles sont déployées **en tant que service Kubernetes**, les instances du pod CN-NGFW peuvent être déployées sur des nœuds de sécurité et le trafic du pod d'application est redirigé vers une instance CN-NGFW disponible pour inspection et application.



- **Plug-in PAN-CNI pour insertion réseau** – Le plug-in PAN-CNI est responsable de l'allocation des interfaces réseau sur chaque pod et permet ainsi la connectivité réseau au pod CN-NGFW. Les fichiers YAML vous permettant de déployer le pare-feu CN-Series contiennent le DaemonSet PAN-CNI, qui insère le plug-in PAN-CNI dans la chaîne de plug-ins CNI sur chacun des nœuds du cluster. Le plug-in

lit les annotations de chacun des pods d'application lorsqu'elles se présentent pour déterminer s'il faut ou non activer la sécurité et rediriger le trafic vers le pod CN-NGFW pour inspection lorsqu'il entre et sort du pod.

- **Panorama pour la gestion centralisée** – Panorama fait office de hub pour gérer la configuration et les licences des pare-feu conteneurisés. Il héberge également le plug-in Kubernetes, qui permet d'activer la surveillance des clusters Kubernetes et la gestion centralisée des politiques de sécurité. Vous pouvez utiliser un appareil Panorama physique ou virtuel et le déployer sur site ou dans un environnement cloud public. Panorama doit disposer d'une connectivité réseau aux pods de plan de gestion (CN-MGMT) du pare-feu pour s'assurer qu'il peut mettre les pare-feu (CN-NGFW) sous licence et transmettre la configuration et les politiques à l'aide des modèles et des groupes d'appareils Panorama. Palo Alto Networks recommande le déploiement Panorama dans une configuration HD.

  Vous avez besoin d'outils Kubernetes standard tels que kubectl ou Helm pour déployer et gérer vos applications, vos services pare-feu et vos clusters Kubernetes. Panorama n'est pas conçu pour être utilisé comme orchestrateur pour le déploiement et la gestion de clusters Kubernetes. Les modèles pour la gestion des clusters sont fournis par les fournisseurs de Kubernetes gérés. Vous pouvez également utiliser les modèles pris en charge par la communauté pour déployer le pare-feu CN-Series avec Helm et Terraform.
- **Plug-in Kubernetes sur Panorama** – Le plug-in Kubernetes gère les licences pour le pare-feu CN-Series. La licence est basée sur le nombre de cœurs que vous choisissez d'allouer aux pods CN-NGFW. Chaque pod CN-NGFW utilise un jeton de licence. Ces jetons sont gérés localement sur Panorama une fois que vous avez activé le code d'autorisation et récupéré le nombre indiqué de jetons sur le serveur de licence Palo Alto Networks. Panorama distribue les jetons de licence localement au fur et à mesure que les pods CN-NGFW apparaissent sur les nœuds Kubernetes.

  Le plug-in Kubernetes sur Panorama vous permet également de surveiller vos clusters et d'exploiter les étiquettes Kubernetes utilisées pour organiser les objets Kubernetes, comme les pods, les services, les déploiements et les attributs d'identification associés. Ainsi, vous pouvez créer des règles de politique de sécurité basées sur le contexte. Le plug-in Kubernetes communique avec le serveur API et récupère les métadonnées en temps quasi réel pour permettre la visibilité des applications en cours d'exécution dans le cluster. Le plug-in Kubernetes collecte les espaces de noms, les services et les étiquettes de vos clusters Kubernetes afin de créer des étiquettes pour le mappage étiquette/adresse IP des objets associés dans le cluster. Ces étiquettes peuvent ensuite être utilisées dans les politiques de sécurité. Pour plus d'informations, reportez-vous à la section Mappage étiquette/adresse IP des attributs Kubernetes

  Il collecte également des informations sur les ports spécifiés dans le YAML de votre application et crée des objets de service.

  Bien que ces étiquettes et objets de services soient automatiquement partagés avec les pods CN-NGFW de chaque cluster, vous pouvez également activer leur partage avec des pare-feu matériels ou VM-Series. Les étiquettes deviennent disponibles comme critères de correspondance dans les groupes d'adresses dynamiques. Vous pouvez ensuite utiliser ces critères pour sécuriser le trafic entre des pods ou des espaces de noms, vers un service exposé à Internet ou des connexions sortantes.

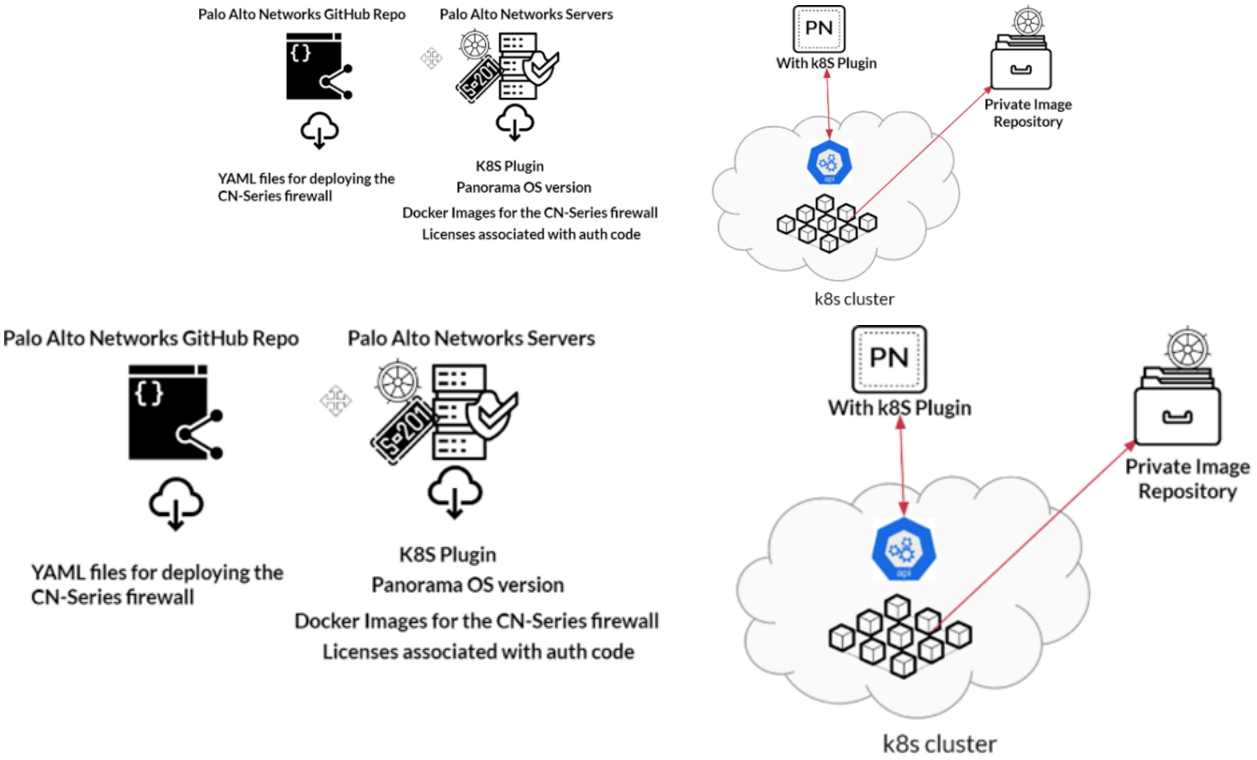
  Palo Alto Networks recommande le déploiement Panorama dans une configuration HA afin que l'homologue Panorama continue de recevoir des mises à jour d'adresse IP en cas de panne. Si vous déployez une instance unique de Panorama, le trafic des pods d'application existants ne sera pas affecté en cas de panne et les politiques actuelles seront appliquées sur les pods CN-NGFW. Lorsqu'un nouveau pod apparaît, toutes les règles possédant la source « ANY » seront mises en correspondance avec le nouveau pod et le trafic de ce dernier sera autorisé ou bloqué, selon vos règles de politique. Par exemple, si une règle de politique antispyware bloque l'accès sortant depuis *toutes* les sources (any)

vers le monde extérieur, cette règle sera appliquée au nouveau pod et le profil pourra sécuriser le trafic. S'il existe une règle *Déni* par défaut, le trafic de ce nouveau pod sera refusé.

Vous pouvez utiliser le plug-in Kubernetes pour distribuer le mappage étiquette/adresse IP pour les pods, les nœuds, les espaces de noms et les services déployés dans le cluster Kubernetes vers des pare-feu physiques ou VM-Series, et ce, même si vous n'avez pas déployé de pare-feu CN-Series dans ce cluster.

Composants requis pour sécuriser des clusters Kubernetes avec le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm



Vous trouverez ci-dessous une liste de ce dont vous avez besoin pour déployer le pare-feu CN-Series et pour sécuriser les applications déployées dans les clusters Kubernetes.

- **Panorama** – Un appareil virtuel ou matériel pouvant se connecter aux clusters Kubernetes dans lesquels les applications et les pare-feu CN-Series sont déployés. Panorama est requis pour la gestion des licences et de la configuration des pare-feu CN-Series. Pour plus d'informations, consultez Blocs de construction principaux du pare-feu CN-Series.
- **Plug-in Kubernetes Plugin sur Panorama** – En raison du taux de changement des applications conteneurisées, ce plug-in est nécessaire pour assurer la visibilité sur l'activité des conteneurs dans un

cluster et pour gérer l'allocation des jetons de licence pour le pare-feu déployé sur chacun des nœuds d'un cluster.

Le plug-in Kubernetes utilise les informations d'identification du compte de service pour se connecter aux clusters Kubernetes. De là, il récupère les étiquettes et attributs de ressources, puis crée des étiquettes et des objets de service. Ces étiquettes peuvent être utilisées pour créer des groupes d'adresses dynamiques et les référencer dans la politique de sécurité pour l'application du trafic IP. Vous pouvez également utiliser les objets de service dans la politique de sécurité pour permettre ou refuser le trafic en fonction des ports et des adresses IP. Les étiquettes et objets de service vous offrent la visibilité et le contrôle granulaire nécessaires à l'application des règles sur le trafic dans votre cluster Kubernetes.

- **Images Docker** – Pour prendre en charge l'architecture distribuée, le pare-feu CN-Series possède quatre images Docker disponibles sur le portail Palo Alto Networks. Ces images sont publiées sous la forme de trois archives tar (format tar.gz). Vous devez les décompresser et utiliser la commande « docker push » pour les transmettre dans votre registre d'images.

  Note : Assurez-vous que les versions des images et des fichiers YAML sont compatibles. Les fichiers compressés sont les suivants :

  - **PanOS_cn-10.1.0.tgz** – Cette archive comprend les images du plan de gestion (CN-MGMT) et du plan de données (CN-NGFW) du pare-feu.

    Les noms des images décompressées sont, par exemple : `panos_cn_ngfw:10.1.0-b7` et `panos_cn_mgmt:10.1.0-b7`

    - **Pan_cn_mgmt_init-2.0.0.tgz** – Cette archive comprend le conteneur init (CN-INIT) contenant les utilitaires requis pour déployer le plan de gestion sur le pare-feu. Le conteneur init permet une communication IPSec sécurisée entre les pods CN-MGMT et CN-NFGW. Le nom de l'image décompressée est, par exemple : `pan_cn_mgmt_init:1.0.0-b1-c1`.
    - **Pan_cni-2.0.0.tgz** – Cette archive comprend le plug-in CNI qui permet la connectivité entre CN-MGMT et CN-NFGW et reconfigure les interfaces réseau sur les pods d'application afin de rediriger le trafic vers le pod CN-NGFW de chaque nœud. Le nom de l'image décompressée est, par exemple : `pan_cni:2.0.0`.

Les noms d'images énumérés ci-dessus sont des exemples et changeront pour refléter la dernière version. Vous pouvez trouver les dernières images sur le portail Palo Alto Networks.

- **Fichiers YAML** – Les fichiers YAML comprenant les spécifications d'objet et les champs requis pour le déploiement des ressources dans vos clusters Kubernetes. Ces fichiers sont publiés sur GitHub.

  Tous les fichiers YAML dont vous avez besoin pour un environnement pris en charge tel qu'un Kubernetes natif ou GKE sont regroupés et compressés dans un dossier unique pour plus de facilité.

  Les fichiers YAML sont automatiquement déployés par le biais de graphiques HELM, méthode recommandée pour déployer le pare-feu CN-Series.

  - CN-MGMT possède trois fichiers YAML : `pan-cn-mgmt.yaml`, `pan-cn-mgmt-configmap.yaml`, `pan-cn-mgmt-secret.yaml`, `pan-cn-mgmt-slot-cr.yaml` et `pan-cn-mgmt-slot-crd.yaml`.
  - CN-NGFW en tant que Daemonset possède deux fichiers YAML : `pan-cn-ngfw.yaml` et `pan-cn-ngfw-configmap.yaml`. CN-NGFW en tant que service Kubernetes a `pan-cn-ngfw-svc.yaml` en plus des fichiers mentionnés précédemment.
  - Le plug-in CNI possède trois fichiers YAML : `pan-cni-configmap.yaml` et `pan-cni.yaml` ou `pan-cni-multus.yaml`.

    Si vous déployez le pare-feu CN-Series sur des environnements sur lesquels la CNI Multus agit comme *méta plug-in* et appelle d'autres plug-ins CNI, vous devez choisir le fichier `pan-cni.yaml` ou `pan-cni-multus.yaml`.

    Si vous déployez le pare-feu CN-Series sur OpenShift, où Multus est activé par défaut, le fichier pan.cni.yaml est approprié. En revanche, si vous déployez le pare-feu CN-Series sur un environnement où la CNI Multus est prise en charge, mais facultative, comme c'est le cas avec les environnements autogérés (natifs), utilisez le fichier pan-cni-multus.yaml au lieu du fichier pan-cni.yaml.

    - *Il existe également un fichier `pan-cni-serviceaccount.yaml`, référencé dans la section Création du compte de service ci-dessous.*
    - *Pour les déploiements OpenShift, il existe un fichier `pan-cni-net-attach-def.yaml` supplémentaire.*

  - **Création du compte de service** – Trois fichiers YAML, `pan-mgmt-serviceaccount.yaml`, `pan-cni-serviceaccount.yaml` et `plugin-serviceaccount.yaml`.

    Les fichiers `pan-mgmt-serviceaccount.yaml` et `pan-cni-serviceaccount.yaml` permettent aux pods CN-MGMT et CN-NGFW de s'authentifier sur le cluster.

    Le fichier `plugin-serviceaccount.yaml` permet au plug-in Kubernetes sur Panorama de s'authentifier sur le cluster.

  - **Fichiers YAML de volume persistant pour les déploiements Kubernetes natifs** – `pan-cn-pv-manual.yaml` et `pan-cn-pv-local.yaml`.

    Le fichier `pan-cn-pv-manual.yaml` est fourni uniquement pour la PoC avec clusters à nœud unique. Palo Alto Networks recommande fortement d'utiliser des volumes persistants configurés de manière dynamique pour stocker la configuration et les journaux des pods CN-MGMT référencés

dans le fichier `pan-cn-mgmt.yaml`. Assurez-vous de configurer un volume persistant dans le cluster pour les deux pods CN-MGMT.

- **Code d'autorisation de licence** – Le code d'autorisation vous permet de mettre sous licence chaque instance du pod CN-NGFW déployé sur chacun des nœuds d'un cluster.

  Le code d'authentification de licence est lié au profil de déploiement CN-Series que vous avez créé sur le CSP Palo Alto Network. En outre, il active tous les abonnements de sécurité que vous avez sélectionnés lors de la création de votre profil de déploiement.

Ressources supplémentaires pour CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Vous pouvez utiliser les ressources suivantes pour en savoir plus sur le pare-feu CN-Series et sur la façon dont il peut vous aider à sécuriser votre réseau conteneurisé.

- Pare-feu CN-Series : regardez ces vidéos pour en savoir plus sur le pare-feu CN-Series.
- Le pourquoi, le quoi et le comment de CN-Series – une série d'articles en trois parties (avec des vidéos intégrées) sur Palo Alto Networks Live Community qui décrit le pourquoi, le quoi et le comment du pare-feu CN-Series.
- Palo Alto Network Qwiklabs – utilisez le Palo Alto Networks Qwiklab pour faire un exercice pratique et essayer le pare-feu CN-Series dans AWS ou GCP.
- Notes de mise à jour du plug-in Panorama pour Kubernetes – lisez les notes de mise à jour pour en savoir plus sur les fonctionnalités et les améliorations introduites dans la dernière version du plug-in Panorama pour Kubernetes.
- Notes de mise à jour de PAN-OS – consultez les notes de mise à jour de PAN-OS pour en savoir plus sur les fonctionnalités et améliorations de CN-Series introduites dans la dernière version de PAN-OS.
- Guide de l'administrateur Panorama – Panorama est l'interface utilisée pour se connecter à votre environnement Kubernetes, gérer les pare-feu CN-Series déployés et définir la politique de sécurité.

Configuration système requise pour CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Cette section couvre la configuration système requise recommandée pour le déploiement du pare-feu CN-Series dans un cluster Kubernetes et un environnement sur site.

Cette section couvre les éléments suivants :

- Configuration système requise CN-Series pour le cluster Kubernetes
- Configuration système requise pour CN-Series pour les déploiements Kubernetes sur site
- Performances et mise à l’échelle de CN-Series
- Déploiement de CN-Series – Environnements pris en charge

Configuration système requise CN-Series pour le cluster Kubernetes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Voici la configuration système recommandée pour le déploiement du pare-feu CN-Series dans ses multiples modes pris en charge.

- PAN-OS 10.1
- PAN-OS 10.2 et versions ultérieures

PAN-OS 10.1

Le tableau suivant indique la configuration système requise pour le cluster sur lequel CN-Series est déployé. Ces valeurs sont des instructions générales pour le processeur, la mémoire et le stockage sur disque ; la quantité de ressources que vous déployez peut varier en fonction de vos besoins.

CN-Series Medium n’est pas disponible pour CN-Series en tant que Daemonset.

Ressource	CN-MGMT-Small	CN-NGFW-Small	CN-MGMT-Medium	CN-NGFW-Medium	CN-MGMT-Large	CN-NGFW-Large
Mémoire (minimum)	3 Go	• 2 Go (Daemonset) • 2,5 Go (service K8s)	3 Go	6 Go	4 Go	48 Go
Processeur min.	2 (recommandé)	2 (recommandé)	2 (recommandé)	4 (recommandé)	4 (recommandé)	12 (recommandé)
Processeur max.	S. O.	31	S. O.	31	S. O.	31
Disque	50 Go	S. O.	50 Go	S. O.	50 Go	S. O.

PAN-OS 10.2 et versions ultérieures

La sécurité native 5G est exclusivement prise en charge sur Daemonset et le mode CNF de Kubernetes.

Les combinaisons de mémoire et de cœur pour CN-MGMT et CN-NGFW s'appliquent respectivement à Petite, Moyenne et Grande. La combinaison de Petite, Moyenne et Grande se rapportant aux cartes CN-MGMT directement avec les CN-NGFW respectifs.

Table 1: Système recommandé de la CN-Series et matrice de capacité

Mode CN	Ressource	Petite	Moyenne	Moyenne	Moyenne	Grande	Grande
DaemonSet	Mémoire CN-MGMT minimale	3G	3G	4G	4G	16G	16G
	Mémoire CN-NGFW minimale	2G	6,5G	16G	32G	48G	56G
	Cœurs CN-MGMT recommandés	2	2	2	4	8	12
	Nombre maximal de cœurs CN-NGFW	2	4	8	16	31	47
	Disque	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	Taille HugePage DPDK	S. O.	S. O.	S. O.	S. O.	S. O.	S. O.
Service Kubernetes	Mémoire CN-MGMT minimale	3G	3G	4G	4G	16G	16G
	Mémoire CN-NGFW minimale	4G	6,5G	16G	32G	48G	56G
	Cœurs CN-MGMT recommandés	2	2	2	4	8	12
	Nombre maximal de	2	4	8	16	31	47

Mode CN	Ressource	Petite	Moyenne	Moyenne	Moyenne	Grande	Grande
	cœurs CN-NGFW						
	Disque	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	Taille HugePage DPDK	S. O.	S. O.	S. O.	S. O.	S. O.	S. O.
Kubernetes CNF	Mémoire CN-MGMT minimale	3G	3G	4G	4G	16G	16G
	Mémoire CN-NGFW minimale	2G	6,5G	16G	32G	48G	56G
	Cœurs CN-MGMT recommandés	2	2	2	4	8	12
	Nombre maximal de cœurs CN-NGFW	2	4	8	16	31	47
	Disque	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	Taille HugePage DPDK	1G	1G	2G	2G	4G	4G

Configuration système requise pour CN-Series pour les déploiements Kubernetes sur site

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Examinez les conditions préalables suivantes pour vos déploiements sur site :

- Assurez-vous que tous les nœuds du cluster Kubernetes peuvent accéder aux images conteneurs.
- Configurez un volume persistant dans le cluster pour les deux pods CN-MGMT. Étant donné que les pods CN-MGMT qui gèrent activement les pods CN-NGFW sont déployés comme un StatefulSet, les deux instances doivent pouvoir accéder au volume persistant.

Pour obtenir l'accès SSH pour votre cluster Rancher, vous devez vous assurer que le contenu du fichier kubeconfig est copié sous l'emplacement `/.kube/config`. *Vous seul pouvez alors exécuter des commandes kubectl pour votre cluster.*

En outre, vous devez vous assurer que l'outil de ligne de commande Kubernetes, kubectl est installé sur votre système. Pour plus d'informations, voir Installer les outils.

Pour CN-Series avec prise en charge de Rancher, installez Docker sur le nœud maître Ubuntu 18.0.4 LTS VM avec 8 vCPU et une mémoire 32G avec un disque minimum 200G. Pour plus d'informations, voir Installer Docker sur Ubuntu 18.04.

Pour Ubuntu 18.0.4, le noyau sur les machines doit être mis à jour vers le dernier noyau à l'aide de la commande suivante :

```
sudo apt install linux-generic-hwe-18.04 -y
```

Performances et mise à l’échelle de CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Les facteurs d’échelle requis par les différents composants pour Sécurisation des charges de travail Kubernetes avec le pare-feu CN-Series sont listés dans les sections suivantes :

- Échelle prise en charge sur les composants CN-Series
- Échelle prise en charge sur le plug-in Kubernetes sur Panorama
- Indicateurs de performance clés CN-Series

Échelle prise en charge sur les composants CN-Series

Pour plus d’informations sur les définitions de processeur, de mémoire et de stockage sur disque de la CN-Series, reportez-vous à la section Configuration système requise CN-Series pour le cluster Kubernetes.

Le tableau suivant sépare certaines données par taille CN-Series : petite, moyenne et grande. Ces tailles CN-Series ont les valeurs de mémoire suivantes :

- **CN-Series, taille petite** – Minimum 2,5G CN-NGFW et 3G CN-MGMT
- **CN-Series, taille moyenne** – Minimum 6G de CN-NGFW et 3G CN-MGMT
- **CN-Series, taille grande** – Minimum 42G de CN-NGFW et 4G de CN-MGMT

Attribut	Échelle CN-Series (DaemonSet)	Échelle CN-Series (service K8s)	Échelle CN-Series (K8s-CNF)
Nombre maximal de paires CN-MGMT par cluster K8s	4 paires CN-MGMT en mode HA actif/passif	4 paires CN-MGMT en mode HA actif/passif	4 paires CN-MGMT en mode HA actif/passif
Nombre maximal de pods CN-NGFW par paire CN-MGMT	30	30	30
Pods Kubernetes sécurisés par	30 (PAN-OS 10.1.8 ou version antérieure)	S. O.	S. O.

Attribut	Échelle CN-Series (DaemonSet)	Échelle CN-Series (service K8s)	Échelle CN-Series (K8s-CNF)
CN-NGFW (par nœud K8s)	125 (PAN-OS 10.1.9 et versions ultérieures avec k8s 2.0.2 installé)	*Ce mode de déploiement est indépendant du nombre de pods d'application sur un nœud K8s.*	*Ce mode de déploiement est indépendant du nombre de pods d'application sur un nœud K8s.*
Nombre maximal de sessions TCP/IP par CN-NGFW	CN-Series Small : 20,000 CN-Series Medium : 819 200 CN-Series Large : 10 000 000	CN-Series Small : 250 000 CN-Series Medium : 819 200 CN-Series Large : 10 000 000	CN-Series Small : 250 000 CN-Series Medium : 819 200 CN-Series Large : 10 000 000
Nombre maximal d'adresses IP de groupes d'adresses dynamiques* par paire CN-MGMT	CN-Series Small : 2 500 (PAN-OS 10.0.6 et inférieur) 10 000 (PAN-OS 10.0.7 et supérieur)	CN-Series Small : 2 500 (PAN-OS 10.0.6 et inférieur) 10 000 (PAN-OS 10.0.7 et supérieur) CN-Series Medium : 200 000 CN-Series Large : 300 000	CN-Series Small : 2 500 (PAN-OS 10.0.6 et inférieur) 10 000 (PAN-OS 10.0.7 et supérieur) CN-Series Medium : 200 000 CN-Series Large : 300 000
Étiquettes par adresse IP* par paire CN-MGMT	32	32	32
Zones de sécurité maximale	CN-Series Small : 2 CN-Series Medium : 40 CN-Series Large : 200	CN-Series Small : 2 CN-Series Medium : 40 CN-Series Large : 200	CN-Series Small : 2 CN-Series Medium : 40 CN-Series Large : 200
Profils de sécurité	CN-Series Small : 38 CN-Series Medium : 375 CN-Series Large : 750	CN-Series Small : 375 CN-Series Medium : 375 CN-Series Large : 750	CN-Series Small : 375 CN-Series Medium : 375 CN-Series Large : 750

Attribut	Échelle CN-Series (DaemonSet)	Échelle CN-Series (service K8s)	Échelle CN-Series (K8s-CNF)
Nombre maximal d'interfaces	**Pour PAN-OS 10.1.8 ou version antérieure :** CN-Series Small : 30 CN-Series Medium : 30 CN-Series Large : 30 **Pour PAN-OS 10.1.9 et versions ultérieures avec k8s 2.0.2 installé :** CN-Series Small : 250 CN-Series Medium : 250 CN-Series Large : 250	CN-Series Small : 2 CN-Series Medium : 2 CN-Series Large : 2	CN-Series Small : 60 CN-Series Medium : 60 CN-Series Large : 60

*Consultez l'outil de comparaison des produits.

Politiques	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Règles de sécurité	1 500	10,000	20,000
Planifications des règles de sécurité	256	256	256
Règles NAT *Les règles NAT sont prises en charge en mode CNF.*	S. O.	S. O.	S. O.
Règles de décryptage	1000	1000	2 000

Politiques	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Règles de remplacement d'application	1000	1000	2 000
Règles d'inspection du contenu du tunnel	100	500	2 000
Règles SD-WAN	S. O.	S. O.	S. O.
Règles de transfert basé sur une politique *Les règles de transfert basé sur une politique sont prises en charge en mode CNF.*	S. O.	S. O.	S. O.
Règles du portail captif	S. O.	S. O.	S. O.
Règles de protection DoS	• 100 (DaemonSet) • 1 000 (service K8s)	1000	1000

Objets (adresses et services)	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Objets d'adresse	10,000	10,000	40 000
Groupes d'adresses	1000	1000	4000
Membres par groupe d'adresses	2 500	2 500	2 500

Objets (adresses et services)	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Objets de service	2 000	2 000	5 000
Groupes de services	500	500	500
Membres par groupes de service	500	500	500
Objets d’adresse FQDN	2 000	2 000	2 000
Nombre maximal d’adresses IP de groupes d’adresses dynamiques	2 500	200 000	300 000
Étiquettes par adresse IP	32	32	32

App-ID	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Signatures d’ID d’application personnalisés	6 000	6 000	6 000
ID d’application personnalisés partagés	512	512	512
ID d’application personnalisés (spécifiques au système virtuel)	6416	6416	6416

Décryptage SSL	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre maximal de certificats entrants SSL	1000	1000	1000

Décryptage SSL	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Cache de certificat SSL (proxy de transfert)	128	2 000	8 000
Nombre maximal de sessions de décryptage simultanées	• 1 024 (DaemonSet) • 6 400 (service K8s)	15 000	100 000
Miroir de port SSL	Non	Non	Non
Agent de décryptage SSL	Non	Non	Non
Pris en charge par HSM	Non	Non	Non

Filtrage d'URL	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre total d’entrées pour la liste verte, la liste de blocage et les catégories personnalisées	25 000	25 000	100 000
Nombre maximal de catégories personnalisées	• 500 (DaemonSet) • 2 849 (service K8s)	2 849	2 849
Taille du cache du plan de données pour le filtrage des URL	• 5 000 (DaemonSet) • 90 000 (service K8s)	90 000	250 000
Taille du cache dynamique du plan de gestion	100 000	100 000	600 000

EDL	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre maximal de listes personnalisées	30	30	30
Nombre maximal d’adresses IP par système	50 000	50 000	50 000
Nombre maximal de domaines DNS par système	50 000	500 000	2 000 000
Nombre maximal d’URL par système	50 000	100 000	100 000
Intervalle de vérification le plus court (minutes)	5	5	5

Affectations d’adresses	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Serveurs DHCP	3	10	125
Relais DHCP	Non	Non	Non
Nombre maximal d’adresses attribuées	64 000	64 000	64 000

Interfaces	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre maximal d’Interfaces (logiques et physiques)	• 60 (DaemonSet) • 2 (service K8s) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (service K8s) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (service K8s) • 2 (K8s-CNF)
Gestion – Hors limite	S. O.	S. O.	S. O.

Interfaces	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Gestion – Haute disponibilité 10/100/1000	S. O.	S. O.	S. O.
Gestion – Haute disponibilité 40G	S. O.	S. O.	S. O.
Gestion – Haute disponibilité 10G	S. O.	S. O.	S. O.
Trafic – 10/100/1000	S. O.	S. O.	S. O.
Trafic – 100/1000/10000	S. O.	S. O.	S. O.
Trafic – 1G SFP	S. O.	S. O.	S. O.
Trafic – 10G SFP+	S. O.	S. O.	S. O.
Trafic – 40/100G QSFP +/QSFP28	S. O.	S. O.	S. O.
Étiquettes 802.1q par appareil	S. O.	S. O.	S. O.
Étiquettes 802.1q par interface physique	S. O.	S. O.	S. O.
Nombre maximal d’interfaces d’agrégation	S. O.	S. O.	S. O.
Nombre maximal d’interfaces virtuelles SD-WAN	S. O.	S. O.	S. O.

NAT	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Capacité totale des règles NAT	S. O.	S. O.	S. O.
Nombre maximal de règles NAT (statiques)	S. O.	S. O.	S. O.
Nombre maximal de règles NAT (DIP)	S. O.	S. O.	S. O.
Nombre maximal de règles NAT (DIPP)	S. O.	S. O.	S. O.
Nombre maximal d’adresses IP traduites (DIP)	S. O.	S. O.	S. O.
Nombre maximal d’adresses IP traduites (DIPP)	S. O.	S. O.	S. O.
Dépassement d’abonnement de pool DIPP par défaut	S. O.	S. O.	S. O.

User-id	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Mappages IP-utilisateur (plan de gestion)	S. O.	S. O.	S. O.
Mappages IP-utilisateur (plan de données)	S. O.	S. O.	S. O.
Groupes actifs et uniques utilisés dans la politique	S. O.	S. O.	S. O.

User-id	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre d’agents d’identification utilisateur	S. O.	S. O.	S. O.
Serveurs surveillés pour l’ID utilisateur	S. O.	S. O.	S. O.
Agents Terminal Server	S. O.	S. O.	S. O.
Étiquettes par utilisateur	S. O.	S. O.	S. O.

Routage	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Dimensions de la table de transfert IPv4	S. O.	S. O.	S. O.
Dimensions de la table de transfert IPv6	S. O.	S. O.	S. O.
Dimensions totales de la table de transfert du système	S. O.	S. O.	S. O.
Nombre maximal d’homologues de routage (dépendant du protocole)	S. O.	S. O.	S. O.
Entrées statiques – Proxy DNS	S. O.	S. O.	S. O.
Sessions bfd (Bidirection Forwarding Detection)	S. O.	S. O.	S. O.

Transfert L2	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Dimensions de la table ARP par périphérique	S. O.	S. O.	S. O.
Dimensions de la table de voisinage IPv6	S. O.	S. O.	S. O.
Dimensions de la table MAC par périphérique	S. O.	S. O.	S. O.
Nombre maximal d’entrées ARP par domaine de diffusion	S. O.	S. O.	S. O.
Nombre maximal d’entrées MAC par domaine de diffusion	S. O.	S. O.	S. O.

QoS	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre de politiques QoS	S. O.	S. O.	S. O.
Interfaces physiques prenant en charge la QoS	S. O.	S. O.	S. O.
Nœuds de texte clair par interface physique	S. O.	S. O.	S. O.
Marquage DSCP par politique	S. O.	S. O.	S. O.
Sous-interfaces prises en charge	S. O.	S. O.	S. O.

VPN IPSec	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Nombre maximal d'homologues IKE	S. O.	S. O.	S. O.
Site à site (avec ID de proxy)	S. O.	S. O.	S. O.
Tunnels IPSec SD-WAN	S. O.	S. O.	S. O.

GlobalProtect	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Client VPN GlobalProtect Nombre maximal de tunnels (SSL, IPSec, IKE avec XAUTH)	S. O.	S. O.	S. O.
VPN sans client GlobalProtect Nombre maximal de tunnels SSL	S. O.	S. O.	S. O.

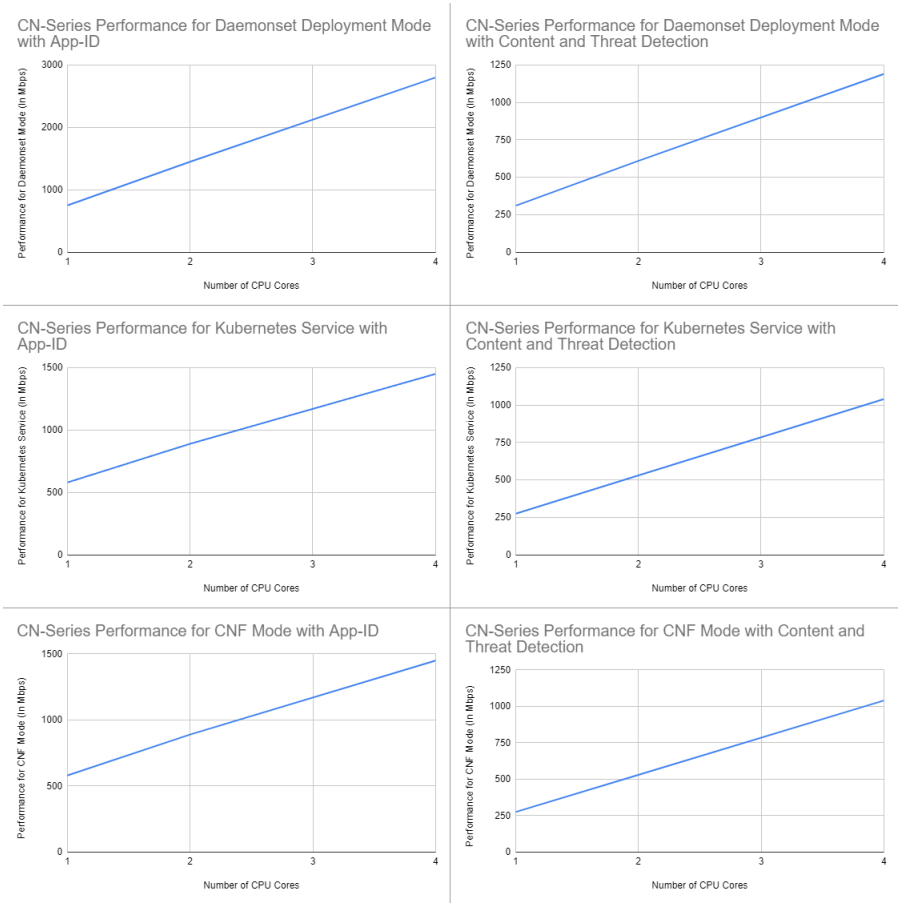
Multicast	CN-Series Small (Min 2,5G CN-NGFW et Min 3G CN-MGMT)	CN-Series Medium (Min 6G CN-NGFW et Min 2G CN-MGMT)	CN-Series Large (Min 42G CN-NGFW et Min 4G CN-MGMT)
Réplication (interfaces de sortie)	S. O.	S. O.	S. O.
Itinéraires	S. O.	S. O.	S. O.

Échelle prise en charge sur le plug-in Kubernetes sur Panorama

Attribut	Échelle du plug-in Kubernetes
Nombre maximal de clusters sur un plug-in Panorama K8s	32 (sur l'ensemble des environnements pris en charge, comme les K8s natifs, AKS, EKS, GKE)

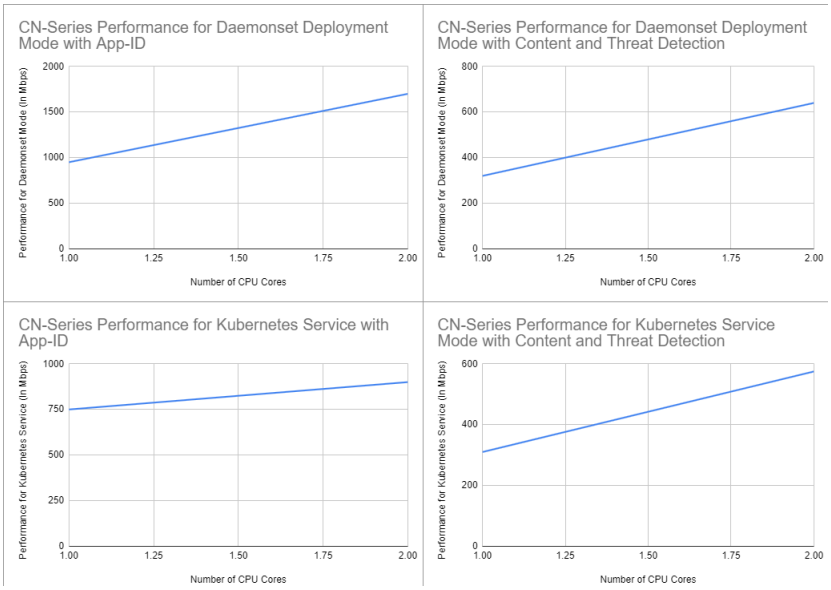
Indicateurs de performance clés CN-Series

CN-Series sur AWS EKS				
	Cœurs de processeu	CN-Series en tant que DaemonSet (MMAP)	CN-Series en tant que service Kubernetes (MMAP)	CN-Series en tant que Kubernetes CNF (MMAP)
App-ID	1	750 Mbit/s	580 Mbit/s	580 Mbit/s
Détection de contenu et de menaces	1	310 Mbit/s	275 Mbit/s	275 Mbit/s
App-ID	2	1,45 Gbit/s	890 Mbit/s	890 Mbit/s
Détection de contenu et de menaces	2	610 Mbit/s	530 Mbit/s	530 Mbit/s
App-ID	4	2,8 Gbit/s	1,45 Gbit/s	1,45 Gbit/s
Détection de contenu et de menaces	4	1,19 Gbit/s	1,04 Gbit/s	1,04 Gbit/s



CN-Series sur Google Cloud GKE (XDP activé)			
	Cœurs de processeur	**CN-Series en tant que DaemonSet**	**CN-Series en tant que service Kubernetes**
App-ID	1	950 Mbit/s	750 Mbit/s
Détection de contenu et de menaces	1	320 Mbit/s	310 Mbit/s
App-ID	2	1,7 Gbit/s	900 Mbit/s
Détection de contenu et de menaces	2	640 Mbit/s	575 Mbit/s

Le test des informations du tableau suivant a été effectué sur Google Kubernetes Engine (GKE) avec un trafic dirigé entre les nœuds et entre les pods sur le même nœud dans le même cluster



Caractéristique/attribut	CN-Series Small	CN-Series Medium	CN-Series Large
Débit du pare-feu (compatible App-ID) par vCPU de CN-NGFW	500 Mbit/s	500 Mbit/s	500 Mbit/s
Débit de Threat Prevention par vCPU de CN-NGFW	250 Mbit/s	250 Mbit/s	250 Mbit/s
Nombre maximal de sessions	• 20 000 (DaemonSet) • 250 000 (service K8s) • 250 000 (K8s-CNF)	819 200	10 000 000
Débit VPN IPSec par vCPU de CN-NGFW	S. O.	S. O.	S. O.
Connexions par seconde	S. O.	S. O.	S. O.

Déploiement de CN-Series – Environnements pris en charge

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec graphique Helm

Ce chapitre fournit des informations sur la compatibilité et les exigences de version pour le pare-feu CN-Series.

- PAN-OS 10.1
- PAN-OS 10.2
- PAN-OS 11.0
- PAN-OS 11.1
- PAN-OS 11.2

PAN-OS 10.1

Vous pouvez déployer le pare-feu CN-Series dans les environnements suivants :

Produit	Version
Runtime de conteneur	Docker CRI-O Containerd
Version de Kubernetes	1.17 à 1.27
Kubernetes gérés par le fournisseur cloud	• AWS EKS (de 1.17 à 1.27 pour le mode de déploiement CN-Series en tant que DaemonSet et CN-Series en tant que service.) • EKS sur AWS Outpost (1.17 à 1.25) *CN-Series pour EKS sur AWS Outpost ne prend pas en charge SR-IOV ou Multus.*

Produit	Version
	• Azure AKS (1.17 à 1.27)  *Dans Azure AKS, PAN-OS 10.1.10h1 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.* • AliCloud ACK (1.26) • GCP GKE (1.17 à 1.27)  *Comprend le plan de données GKE V2.*
Kubernetes gérés par le client	Sur le cloud public ou le centre de données sur site. Assurez-vous que la version de Kubernetes, les types de CNI et les versions du SE de la VM hôte sont répertoriés dans ce tableau. VMware TKG+ version 1.1.2 • Plateforme d'infrastructure – vSphere 7.0 • SE de la VM hôte Kubernetes – Photon OS
VM hôte Kubernetes	Système d'exploitation : • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 et versions ultérieures • CoreOS 21XX, 22XX • SE optimisé pour les conteneurs
	Version du noyau Linux : • 4.18 ou version ultérieure (mode de service K8s uniquement) • 5.4 ou version ultérieure requise pour activer le mode AF_XDP. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers YAML de déploiement CN-Series.
	Netfilter du noyau Linux : Iptables
Plug-ins CNI	Spécification CNI 0.3 et versions ultérieures : • AWS-VPC

Produit	Version

	• Azure
	• Calico
	• Flannel
	• Weave
	• Pour AliCloud, Terway
	• Pour Openshift, OpenshiftSDN
	• Les éléments suivants sont pris en charge sur le pare-feu CN-Series en tant que DaemonSet.
	  • Multus
	  • Pont
	  • SR-IOV
	  • Macvlan

OpenShift	**CN-Series en tant que DaemonSet :** 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13 **CN-Series en tant que service K8s :** (PAN-OS 10.1.2 et versions ultérieures) 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13 *PAN-OS 10.1.10h1 est la version minimale requise pour prendre en charge 4.12 et versions ultérieures.*

Consultez également la Configuration système requise CN-Series pour le cluster Kubernetes, avant de Déployer le pare-feu CN-Series.

PAN-OS 10.2

Vous pouvez déployer le pare-feu CN-Series dans les environnements suivants :

Produit	Version
Runtime de conteneur	Docker CRI-O Containerd
Version de Kubernetes	1.17 à 1.27

Produit	Version
Kubernetes gérés par le fournisseur cloud	• AWS EKS (de 1.17 à 1.27 pour le mode de déploiement CN-Series en tant que DaemonSet et CN-Series en tant que service.) • AWS EKS (1.17 à 1.22 pour CN-Series en tant que mode de déploiement CNF.) • EKS sur AWS Outpost (1.17 à 1.22) *CN-Series pour EKS sur AWS Outpost ne prend pas en charge SR-IOV ou Multus.* • Azure AKS (1.17 à 1.28) *Dans Azure AKS, PAN-OS 10.2.4h3 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.* • GCP GKE (1.17 à 1.27) *Dans GCP GKE, PAN-OS 10.2.4h3 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.* *Comprend le plan de données GKE V2.* • Google Anthos 1.12.3 • OCI OKE (1.23)
Kubernetes gérés par le client	Sur le cloud public ou le centre de données sur site. Assurez-vous que la version de Kubernetes, les types de CNI et les versions du SE de la VM hôte sont répertoriés dans ce tableau. VMware TKG+ version 1.1.2 • Plateforme d'infrastructure – vSphere 7.0 • SE de la VM hôte Kubernetes – Photon OS
VM hôte Kubernetes	Système d'exploitation : • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04

Produit	Version
	• RHEL/Centos 7.3 et versions ultérieures • CoreOS 21XX, 22XX • SE optimisé pour les conteneurs
	Version du noyau Linux : • 4.18 ou version ultérieure (mode de service K8s uniquement) • 5.4 ou version ultérieure requise pour activer le mode AF_XDP. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers YAML de déploiement CN-Series.
	Netfilter du noyau Linux : Iptables

Plug-ins CNI	Spécification CNI 0.3 et versions ultérieures :
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Pour Openshift, OpenshiftSDN, OVN Kubernetes
	• Les éléments suivants sont pris en charge sur le pare-feu CN-Series en tant que DaemonSet.
	  • Multus
	  • Pont
	  • SR-IOV
	  • Macvlan

OpenShift	• Versions 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13 *OpenShift 4.7 est qualifié sur CN-Series en tant que DaemonSet uniquement.* • OpenShift sur AWS *PAN-OS 10.2.4h3 est la version minimale requise pour prendre en charge 4.12 et versions ultérieures.*

Consultez également la Configuration système requise CN-Series pour le cluster Kubernetes, avant de Déployer le pare-feu CN-Series.

PAN-OS 11.0

Vous pouvez déployer le pare-feu CN-Series dans les environnements suivants :

Produit	Version
Runtime de conteneur	Docker CRI-O Containerd
Version de Kubernetes	1.17 à 1.27
Kubernetes gérés par le fournisseur cloud	• AWS EKS (de 1.17 à 1.27 pour le mode de déploiement CN-Series en tant que DaemonSet et CN-Series en tant que service.) • AWS EKS (1.17 à 1.22 pour CN-Series en tant que mode de déploiement CNF.) • EKS sur AWS Outpost (1.17 à 1.25) *CN-Series pour EKS sur AWS Outpost ne prend pas en charge SR-IOV ou Multus.* • Azure AKS (1.17 à 1.27) *Dans Azure AKS, PAN-OS 11.0.2 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.* • GCP GKE (1.17 à 1.27) *Comprend le plan de données GKE V2.* • OCI OKE (1.23)
Kubernetes gérés par le client	Sur le cloud public ou le centre de données sur site. Assurez-vous que la version de Kubernetes, les types de CNI et les versions du SE de la VM hôte sont répertoriés dans ce tableau. VMware TKG+ version 1.1.2 • Plateforme d'infrastructure – vSphere 7.0

Produit	Version
	• SE de la VM hôte Kubernetes – Photon OS
VM hôte Kubernetes	Système d’exploitation : • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 et versions ultérieures • CoreOS 21XX, 22XX • SE optimisé pour les conteneurs
	Version du noyau Linux : • 4.18 ou version ultérieure (mode de service K8s uniquement) • 5.4 ou version ultérieure requise pour activer le mode AF_XDP. Pour plus d’informations, consultez Paramètres modifiables dans les fichiers YAML de déploiement CN-Series.
	Netfilter du noyau Linux : Iptables

Plug-ins CNI	Spécification CNI 0.3 et versions ultérieures :
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Pour Openshift, OpenshiftSDN, OVN Kubernetes
	• Les éléments suivants sont pris en charge sur le pare-feu CN-Series en tant que DaemonSet.
	  • Multus
	  • Pont
	  • SR-IOV
	  • Macvlan

Produit	Version
OpenShift	• Versions 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13.  *OpenShift 4.7 est qualifié sur CN-Series en tant que DaemonSet uniquement.* *PAN-OS 11.0.2 est la version minimale requise pour prendre en charge 4.12 et versions ultérieures.* • OpenShift sur AWS

Consultez également la Configuration système requise CN-Series pour le cluster Kubernetes, avant de Déployer le pare-feu CN-Series.

PAN-OS 11.1

Vous pouvez déployer le pare-feu CN-Series dans les environnements suivants :

Produit	Version
Runtime de conteneur	Docker CRI-O Containerd
Version de Kubernetes	1.17 à 1.27
Kubernetes gérés par le fournisseur cloud	• AWS EKS (de 1.17 à 1.27 pour le mode de déploiement CN-Series en tant que DaemonSet et CN-Series en tant que service.) • AWS EKS (1.17 à 1.22 pour CN-Series en tant que mode de déploiement CNF.) • EKS sur AWS Outpost (1.17 à 1.25)  *CN-Series pour EKS sur AWS Outpost ne prend pas en charge SR-IOV ou Multus.* • Azure AKS (1.17 à 1.27)  *Dans Azure AKS, PAN-OS 11.0.2 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.*

Produit	Version
	• GCP GKE (1.17 à 1.27)  *Comprend le plan de données GKE V2.* • OCI OKE (1.23)
Kubernetes gérés par le client	Sur le cloud public ou le centre de données sur site. Assurez-vous que la version de Kubernetes, les types de CNI et les versions du SE de la VM hôte sont répertoriés dans ce tableau. VMware TKG+ version 1.1.2 • Plateforme d'infrastructure – vSphere 7.0 • SE de la VM hôte Kubernetes – Photon OS
VM hôte Kubernetes	Système d'exploitation : • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 et versions ultérieures • CoreOS 21XX, 22XX • SE optimisé pour les conteneurs
	Version du noyau Linux : • 4.18 ou version ultérieure (mode de service K8s uniquement) • 5.4 ou version ultérieure requise pour activer le mode AF_XDP. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers YAML de déploiement CN-Series.
	Netfilter du noyau Linux : Iptables
Plug-ins CNI	Spécification CNI 0.3 et versions ultérieures : • AWS-VPC • Azure • Calico • Flannel • Weave • Pour Openshift, OpenshiftSDN, OVN Kubernetes

Produit	Version

	• Les éléments suivants sont pris en charge sur le pare-feu CN-Series en tant que DaemonSet.
	  • Multus
	  • Pont
	  • SR-IOV
	  • Macvlan

OpenShift	• Versions 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13. *OpenShift 4.7 est qualifié sur CN-Series en tant que DaemonSet uniquement.* *PAN-OS 11.0.2 est la version minimale requise pour prendre en charge 4.12 et versions ultérieures.* • OpenShift sur AWS

Consultez également la Configuration système requise CN-Series pour le cluster Kubernetes, avant de Déployer le pare-feu CN-Series.

PAN-OS 11.2

Vous pouvez déployer le pare-feu CN-Series dans les environnements suivants :

Produit	Version
Runtime de conteneur	Docker CRI-O Containerd
Version de Kubernetes	1.17 à 1.27
Kubernetes gérés par le fournisseur cloud	• AWS EKS (de 1.17 à 1.27 pour le mode de déploiement CN-Series en tant que DaemonSet et CN-Series en tant que service.) • AWS EKS (1.17 à 1.22 pour CN-Series en tant que mode de déploiement CNF.) • EKS sur AWS Outpost (1.17 à 1.25) *CN-Series pour EKS sur AWS Outpost ne prend pas en charge SR-IOV ou Multus.*

Produit	Version
	• Azure AKS (1.17 à 1.27)  *Dans Azure AKS, PAN-OS 11.0.2 est la version minimale requise pour prendre en charge Kubernetes 1.25 et versions ultérieures.* • GCP GKE (1.17 à 1.27)  *Comprend le plan de données GKE V2.* • OCI OKE (1.23)
Kubernetes gérés par le client	Sur le cloud public ou le centre de données sur site. Assurez-vous que la version de Kubernetes, les types de CNI et les versions du SE de la VM hôte sont répertoriés dans ce tableau. VMware TKG+ version 1.1.2 • Plateforme d'infrastructure – vSphere 7.0 • SE de la VM hôte Kubernetes – Photon OS
VM hôte Kubernetes	Système d'exploitation : • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 et versions ultérieures • CoreOS 21XX, 22XX • SE optimisé pour les conteneurs
	Version du noyau Linux : • 4.18 ou version ultérieure (mode de service K8s uniquement) • 5.4 ou version ultérieure requise pour activer le mode AF_XDP. Pour plus d'informations, consultez Paramètres modifiables dans les fichiers YAML de déploiement CN-Series.
	Netfilter du noyau Linux : Iptables
Plug-ins CNI	Spécification CNI 0.3 et versions ultérieures : • AWS-VPC

Produit	Version

	• Azure
	• Calico
	• Flannel
	• Weave
	• Pour Openshift, OpenshiftSDN, OVN Kubernetes
	• Les éléments suivants sont pris en charge sur le pare-feu CN-Series en tant que DaemonSet.
	  • Multus
	  • Pont
	  • SR-IOV
	  • Macvlan

OpenShift	• Versions 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 et 4.13.  *OpenShift 4.7 est qualifié sur CN-Series en tant que DaemonSet uniquement.* *PAN-OS 11.0.2 est la version minimale requise pour prendre en charge 4.12 et versions ultérieures.* • OpenShift sur AWS

Consultez également la Configuration système requise CN-Series pour le cluster Kubernetes, avant de Déployer le pare-feu CN-Series.

Prérequis au déploiement de CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Pour déployer le pare-feu CN-Series, vous devez vous assurer que les conditions préalables suivantes sont remplies :

- Mettre sous licence le pare-feu CN-Series
- Installer un certificat de périphérique sur le pare-feu CN-Series
- Création de comptes de service pour l’authentification des clusters
- Installer le plug-in Kubernetes et configurer Panorama pour CN-Series
- Obtenir les images et les fichiers pour le déploiement CN-Series

Mettre sous licence le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

La mise sous licence du pare-feu CN-Series est gérée par le plug-in Kubernetes sur Panorama. Les pare-feu CN-Series sont concédés sous licence en fonction du nombre total de vCPU (cœurs) utilisés par les pods CN-NGFW déployés dans votre environnement Kubernetes. Un jeton est consommé pour chaque vCPU utilisé par le CN-NGFW.

- Activer des crédits — commencez par activer vos crédits. Une fois activé, vous pouvez appliquer les crédits de votre pool de crédits à un profil de déploiement CN-Series.
- Créer un profil de déploiement de CN-Series — dans le profil de déploiement, vous spécifierez le nombre de vCPU qui allouent au code d'autorisation de génération. Vous utiliserez ensuite le code d'autorisation associé à votre profil de déploiement CN-Series pour licencier les pare-feux CN-Series dans votre cluster Kubernetes. Le profil de déploiement peut être utilisé sous licence pour les pods CN-NGFW en fonction du nombre de vCPU alloués. Un seul code d'autorisation à partir d'un profil de déploiement peut être utilisé pour licencier le CN-Series sur différents environnements Kubernetes, différents clusters ou sur différentes instances Panorama.

  Dans un déploiement CN-Series en tant que service Kubernetes, si le nombre de pods CN-NGFW déployés dans votre environnement dépassent le nombre de vCPU alloués, vous disposez d'une période de grâce de 30 jours pour ajouter plus de vCPU à votre profil de déploiement ou supprimer suffisamment de pods CN-NGFW. Si vous n'allouez pas de vCPU supplémentaires ou ne supprimez pas de pods sans licence au cours de la période de grâce de 30 jours, tous les pare-feu CN-Series de votre cluster seront supprimés.

  Lorsqu'un CN-Series est déployé en tant que DaemonSet, si le nombre de pods CN-NGFW déployés dépasse le nombre de vCPU alloués, vous disposez d'un délai de grâce de quatre heures pour ajouter plus de vCPU à votre profil de déploiement ou supprimer suffisamment de pods CN-NGFW. Si vous n'allouez pas de vCPU supplémentaires ou ne supprimez pas de pods sans licence dans le délai de grâce de quatre heures, les pods sans licence cesseront de traiter le trafic. Les pods déjà sous licence restent sous licence.

  Vous avez également la possibilité de provisionner un appareil Panorama virtuel lors de la création de votre profil de déploiement CN-Series.
- Gérer les profils de déploiement — vous pouvez modifier, cloner ou supprimer des profils de déploiement CN-Series en fonction des exigences de votre déploiement CN-Series. De plus, vous pouvez ajouter ou supprimer des abonnements du profil de déploiement après sa création.

Les licences sont appliquées à la CN-Series au niveau du cluster. Un CN-NGFW individuel peut apparaître comme sans licence, cependant, tous les pods du cluster sont sous licence jusqu'à ce que l'intégralité du cluster soit retirée de la licence.

Activer des crédits

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Au sein de votre organisation, vous pouvez créer de nombreux comptes ayant chacun un objectif différent. Pendant l'activation, vous ne pouvez choisir qu'un seul compte par pool de crédits par défaut. Une fois que le pool de crédits est actif, les utilisateurs qui se voient attribuer le rôle d'administrateur de crédits peuvent allouer des crédits pour les déploiements, et même transférer des crédits vers d'autres pools.

Si vous avez un compte CSP existant et que vous êtes un super utilisateur ou un administrateur, le système ajoute automatiquement le rôle d'administrateur de crédits à votre profil. Si vous n'avez pas de compte existant, le CSP crée automatiquement un compte pour vous et ajoute le rôle d'administrateur de crédits à votre profil.

Vous (l'acheteur) recevez un e-mail détaillant l'abonnement, l'ID du pool de crédits, la date de début et de fin de l'abonnement, le montant des crédits achetés et la description du pool de crédits par défaut (le pool de crédits créé quand vous activez vos crédits).

Conservez cet e-mail pour référence ultérieure.

STEP 1 | Dans l'e-mail, cliquez sur **Start Activation** (Démarrer l'activation) pour afficher vos pools de crédits disponibles.

STEP 2 | Sélectionnez le pool de crédits que vous souhaitez activer. Vous pouvez utiliser le champ de recherche pour filtrer votre liste de comptes par numéro ou par nom.

Si vous avez acheté plusieurs pools de crédit, les deux sont automatiquement sélectionnés. Les coches représentent les liens d'activation pour les crédits d'intégration.

Vous êtes invité à vous authentifier ou à vous connecter.

*Si vous désélectionnez un pool de crédits, un rappel s'affiche pour indiquer que si vous souhaitez activer ces crédits, vous devez revenir à l'e-mail et cliquer sur le lien **Start Activation** (Démarrer l'activation).*

STEP 3 | Sélectionnez **Start Activation** (Démarrer l'activation).

STEP 4 | Sélectionnez le compte d'assistance (vous pouvez effectuer une recherche par numéro de compte ou par nom).

STEP 5 | Sélectionnez le pool de crédits par défaut.

STEP 6 | Sélectionnez **Deposit Credits** (Déposer des crédits).

Un message indique que le dépôt a réussi.

STEP 7 | (facultatif) S'il s'agit de votre première activation de crédit, la boîte de dialogue **Créer un profil de déploiement** s'affiche.

Passez à la section Créer un profil de déploiement de CN-Series.

Créer un profil de déploiement de CN-Series

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• CN-Series déploiement	• CN-Series 10.1.x or above Container Images • Panoramaexécutant la version PAN-OS 10.1.x ou supérieure • Helm 3.6 or above version clientpour le déploiement de CN-Series avec Helm

Utilisez la procédure suivante pour créer un profil de déploiement de CN-Series.

STEP 1 | Si vous disposez déjà d'un pool de crédits, connectez-vous au compte et, à partir du tableau de bord, sélectionnez **Assets** > **Software NGFW Credits** > **Prisma NGFW Credits** > **Create New Profile**.

Si vous venez d'activer un pool de crédits, l'écran **Create Deployment Profile** (Créer un profil de déploiement) s'affiche.

1. Sélectionnez le type de pare-feu **CN-Series**.
2. Sélectionnez **PAN-OS 10.2 and above (PAN-OS 10.2 et supérieur)**.
3. Cliquez sur **Next (Suivant)**.

STEP 2 | Profil CN-Series.

1. **Profile Name** (Nom du profil).

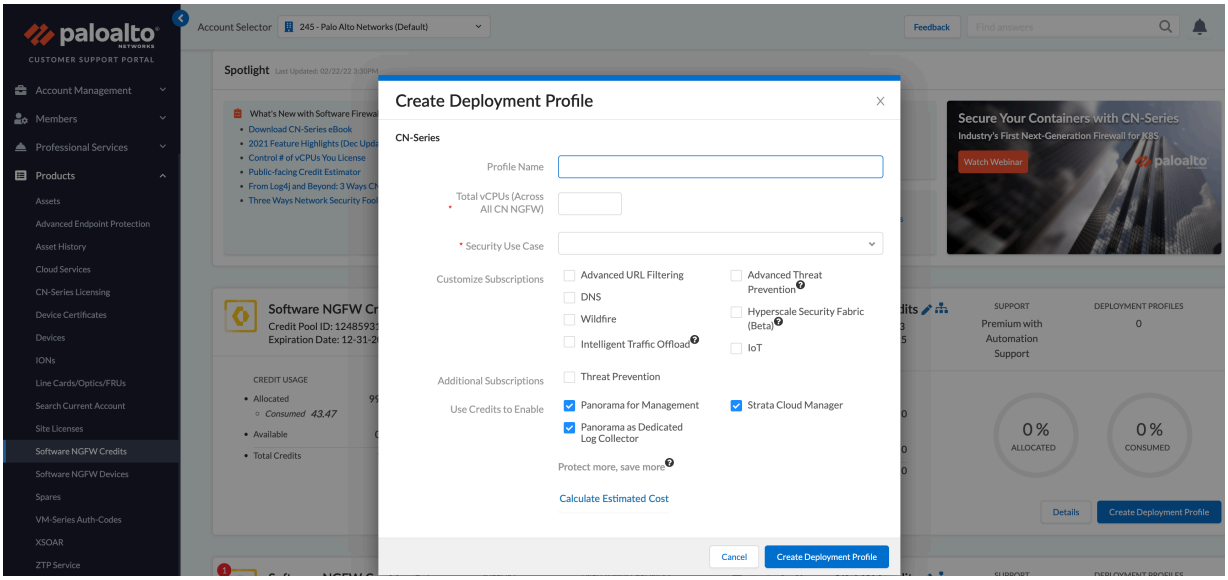
   Nommez le profil.
2. **Total vCPUs** (Total des vCPU).

   Entrez le nombre total de vCPU sur tous les CN-NGFW.
3. Sélectionnez un cas d'utilisation de sécurité dans la liste déroulante. Chaque cas d'utilisation de sécurité dans la liste déroulante sélectionne automatiquement un certain nombre de descriptions recommandées pour le cas d'utilisation choisi. Si vous sélectionnez Custom (Personnalisé), vous pouvez spécifier les abonnements que vous souhaitez utiliser dans votre déploiement.
4. (facultatif) **Utilisez des crédits pour activer VM Panorama — Pour la gestion** ou **Collecteur de journaux dédié**.

STEP 3 | (facultatif) Survolez le point d'interrogation après **Protect more, save more** (Protégez plus, économisez plus) pour voir comment votre allocation de crédit affecte l'épargne.

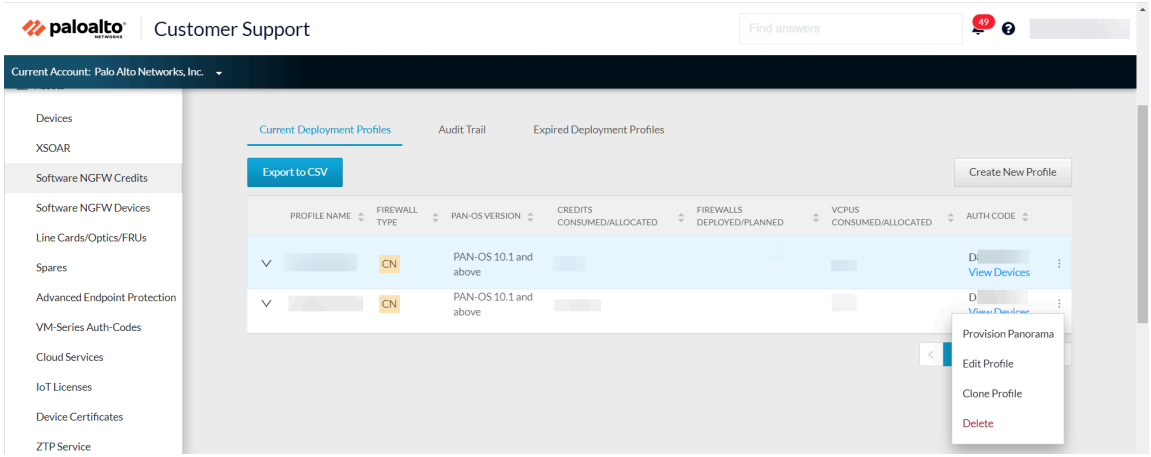
STEP 4 | Cliquez sur **Calculate Estimated Cost** (Calculer le coût estimé) pour afficher le total des crédits et le nombre de crédits disponibles avant le déploiement.

(facultatif) Passez le curseur de la souris sur le point d'interrogation suivant l'estimation pour afficher la répartition des crédits pour chaque élément.



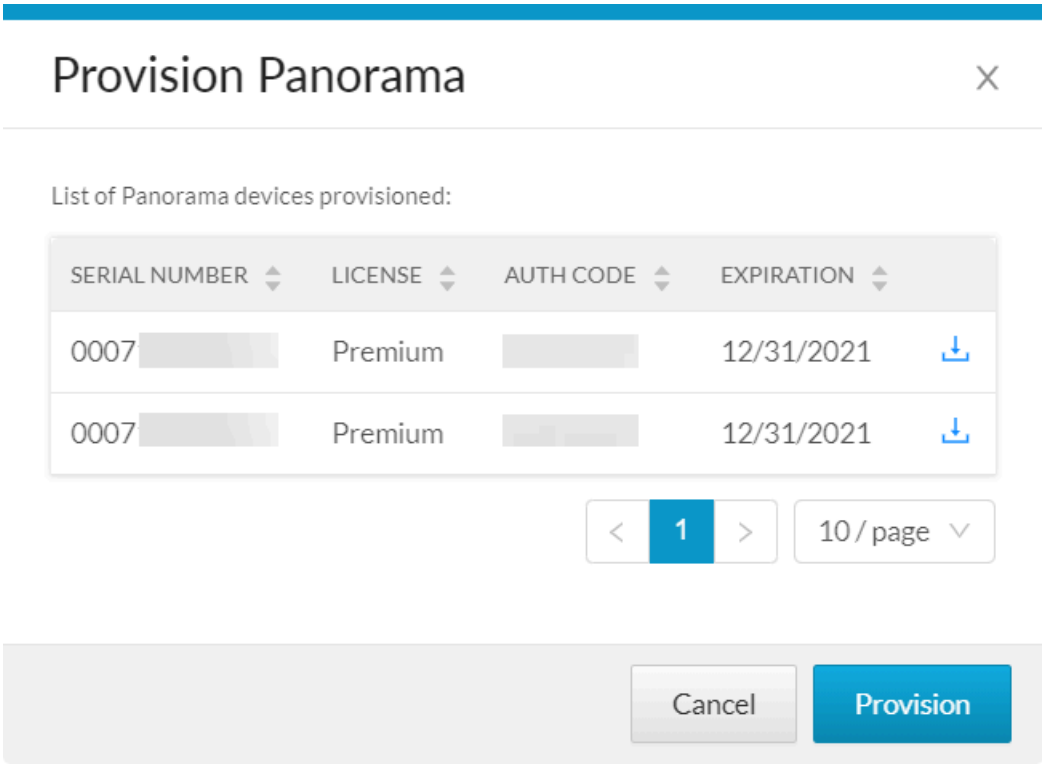
STEP 5 | (facultatif) Configuration de Panomara. Si vous avez utilisé des crédits pour activer une VM Panorama, procédez comme suit pour configurer Panorama et générer un numéro de série. Panorama doit gérer les déploiements de CN-Series. Une fois que vous avez appliqué le numéro de série à Panorama, Panorama contacte le serveur de mise à jour des licences et récupère la licence.

1. Sélectionnez **Assets** > **Software NGFW Credits** > **Prisma NGFW Credits** et localisez votre profil de déploiement.
2. Tout à droite, sélectionnez les points de suspension verticaux, puis **Provision Panorama** (Configuration de Panorama).



3. Cliquez sur Provision Panorama (Configuration de Panorama) pour générer un numéro de série.

4. Enregistrez ou copiez le numéro de série à appliquer à votre instance Panorama.



5. Enregistrez Panorama.

Gérer les profils de déploiement

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec Helm

Vous pouvez utiliser les procédures suivantes pour gérer vos profils de déploiement existants.

- Modifier un profil de déploiement
- Cloner un profil de déploiement
- Supprimer un profil de déploiement
- Transférer des crédits au pool dans le même compte
- Transférer des crédits vers un autre compte CSP

Modifier un profil de déploiement

Vous pouvez modifier un profil de déploiement existant pour ajouter plus de crédits ou attribuer des vCPU supplémentaires à votre déploiement. Le code d'autorisation associé au profil de déploiement à modifier ne doit pas être utilisé sur Panorama.

STEP 1 | Sélectionnez **Assets** > **Software NGFW Credits** et choisissez un profil (sélectionnez une ligne).

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Edit Profile** (Modifier le profil).

STEP 3 | Apportez vos modifications et sélectionnez **Update Deployment Profile** (Mettre à jour le profil de déploiement).

Cloner un profil de déploiement

Effectuez la procédure suivante pour cloner un profil de déploiement existant.

STEP 1 | Accédez à **Assets** > **Software NGFW Credits** et sélectionnez un profil (sélectionnez une ligne).

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Clone Profile** (Cloner le profil).

STEP 3 | Modifiez le nom du profil, apportez d'autres modifications, puis sélectionnez **Create Deployment Profile** (Créer un profil de déploiement).

Supprimer un profil de déploiement

Avant de supprimer un profil de déploiement, vous devez supprimer tous les pare-feu qui utilisent le profil. Le code d'autorisation associé au profil de déploiement à supprimer ne doit pas être utilisé sur Panorama.

STEP 1 | Dans le CSP, sélectionnez **Assets** > **Software NGFW Credits** et sélectionnez un profil (sélectionnez une ligne).

STEP 2 | Tout à droite, sélectionnez les points de suspension verticaux (More Options [Plus d'options]) et sélectionnez **Delete** (Supprimer).

Transférer des crédits au pool dans le même compte

Vous pouvez transférer des crédits vers un pool de crédits dans un autre compte auquel vous pouvez accéder.

STEP 1 | Connectez-vous à votre compte CSP.

STEP 2 | Sélectionnez **Assets** > **Software NGFW Credits**.

- Identifiez le pool de crédits source et notez l'ID du pool de crédits.
- Identifiez le pool de crédits de destination et notez l'ID du pool de crédits.

STEP 3 | Accédez au pool de crédits source et sélectionnez **Transfer Credits** (Transférer des crédits) en bas à gauche.

STEP 4 | Sélectionnez **Different CSP account** (Autre compte CSP).

1. **New credit type** (Nouveau type de crédit) — Choisissez un type de crédit. À ce stade, le type de source et de destination doit être le même.
2. **Credit Pool ID#** (N° ID pool de crédits) — Choisissez un numéro d'identification de pool de crédits. Si le compte de destination n'a pas de pool de crédits du type choisi, le CSP vous invite à créer un pool de crédits.
3. **Amount to Transfer** (Montant à transférer) — Entrez le montant à transférer.

STEP 5 | Sélectionnez **Update Credits** (Mettre à jour les crédits).

Transférer des crédits vers un autre compte CSP

Vous pouvez transférer des crédits vers un pool de crédits dans le même compte.

STEP 1 | Connectez-vous à votre compte CSP.

STEP 2 | Sélectionnez **Assets** > **Software NGFW Credits**.

- Identifiez le pool de crédits source et notez l'ID du pool de crédits.
- Identifiez le pool de crédits de destination et notez l'ID du pool de crédits.

  Si la destination se trouve dans un autre compte, sélectionnez-le dans la liste déroulante **Current Account** (Compte courant) en haut à gauche et sélectionnez **Assets** > **Software NGFW Credits**. Recherchez la destination et notez le type de crédit et l'ID du pool de crédits.

STEP 3 | Accédez au pool de crédits source et cliquez sur **Transfer Credits** (Transférer des crédits) en bas à gauche.

STEP 4 | Choisissez un autre compte CSP.

1. **Transfer to** (Transférer vers) — Choisissez un nom de compte.
2. **As credit type** (Comme type de crédit) — Choisissez un type de crédit. À ce stade, le type de source et de destination doit être le même.
3. **Credit Pool ID#** (N° ID pool de crédits) — Choisissez un numéro d'identification de pool de crédits. Si le compte de destination n'a pas de pool de crédits du type choisi, le CSP vous invite à créer un pool de crédits.
4. **Amount to Transfer** (Montant à transférer) — Entrez le montant à transférer.

STEP 5 | Sélectionnez **Update Credits** (Mettre à jour les crédits).

Installer un certificat de périphérique sur le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Le pare-feu nécessite un certificat de périphérique qui autorise un accès sécurisé aux services de sécurité fournis dans le cloud (CDSS) de Palo Alto tels que WildFire, AutoFocus et le service de journalisation Strata. Vous devez appliquer un code PIN d'enregistrement automatique pour appliquer une licence CDSS à votre déploiement de pare-feu CN-Series. Chaque mot de passe ou PIN est généré sur le portail de support client (CSP) et est unique à votre compte de support Palo Alto Networks. Pour réussir l'installation du certificat de périphérique, le pod du plan de gestion série CN (CN-MGMT) doit disposer d'une connexion Internet sortante, et les noms de domaine complets (FQDN) et ports suivants doivent être autorisés sur votre réseau.

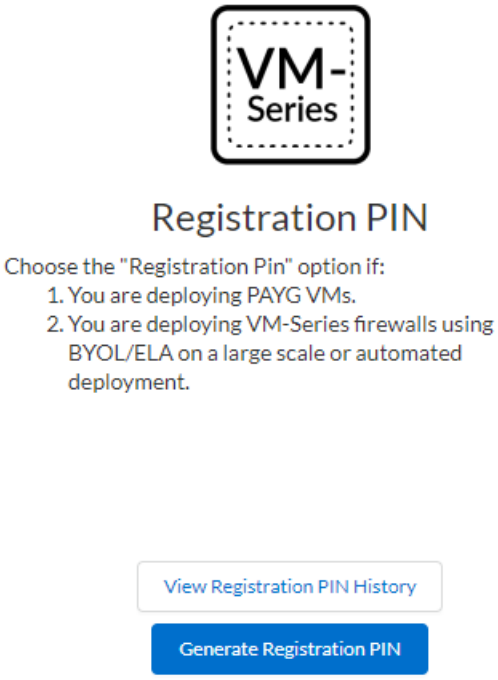
Nom de domaine complet	Ports
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 et TCP 443

Pour ajouter un certificat de périphérique à un déploiement existant sans certificat de périphérique existant, vous devez redéployer le pare-feu CN-Series après avoir ajouté l'ID PIN et la valeur valides à `pan-cn-mgmt-secret.yaml`. *Pour le déploiement de cloud public CN-Series, vous devez supprimer la revendication de volume persistant avant le redéploiement. Pour les déploiements Kubernetes statiques/natifs, vous devez supprimer la revendication de volume persistant et le volume persistant avant le redéploiement.*

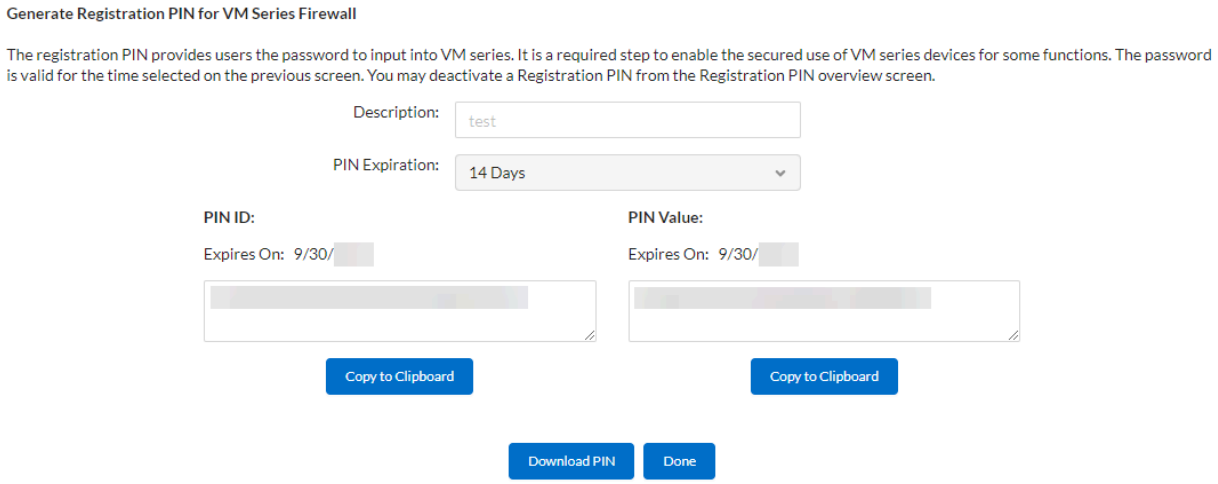
STEP 1 | Connectez-vous au Portail assistance clientèle de Palo Alto Networks avec vos identifiants de compte.

Si vous avez besoin d'un nouveau compte, consultez la section Comment créer un nouveau compte utilisateur pour le portail d'assistance client.

STEP 2 | Sélectionnez **Assets** > **Device Certificates** > **Generate Registration PIN**.



STEP 3 | Entrez une **Description** et sélectionnez une **PIN Expiration** (Expiration du PIN) dans la liste déroulante.



STEP 4 | Enregistrez l'ID et la valeur du PIN.

Enregistrez l'ID et la valeur du PIN. L'ID et la valeur de ce PIN sont saisis dans le fichier `pan-cn-mgmt-secret.yaml` utilisé pour déployer le pare-feu de CN-Series. Veillez à lancer le pare-feu avant l'expiration du PIN.

```
# Thermite Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<your-pin-id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<your-pin-value>"
```


Création de comptes de service pour l’authentification des clusters

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series avec graphique Helm

Le pare-feu CN-Series nécessite trois comptes de service avec les autorisations minimales qui l’autorisent à communiquer avec les ressources de votre cluster Kubernetes. Le compte de service (pan-plugin-user) créé avec le `plugin-serviceaccount.yaml` permet au plug-in Kubernetes sur Panorama de s’authentifier auprès du cluster Kubernetes pour la récupération des métadonnées sur les pods. Les deux autres fichiers yaml, `pan-mgmt-serviceaccount.yaml` et `pan-cni-serviceaccount.yaml`, créent les comptes de service pan-mgmt-sa et pan-cni-sa pour permettre l’authentification entre les pods CN-Mgmt tolérants aux pannes, et entre le pod CN-MGMT et les pods CN-NGFW.

Par défaut, les fichiers YAML créent le compte de service et le secret dans l’espace de noms kube-system ; le plug-in Kubernetes ne cherchera le secret que dans l’espace de noms kube-system.

Pour créer les comptes de service, votre cluster Kubernetes doit être prêt.

STEP 1 | Exécutez le compte de service YAML pour le `plugin-serviceaccount.yaml`.

Ce compte de service permet d'obtenir les autorisations dont Panorama a besoin pour s'authentifier auprès du cluster GKE afin de récupérer les étiquettes Kubernetes et les informations sur les ressources. Ce compte de service est nommé pan-plugin-user par défaut.

1. **`kubectl apply -f plugin-serviceaccount.yaml`**
2. **`kubectl -n kube-system get secrets | grep pan-plugin-user`**

   Pour consulter les secrets associés à ce compte de service.

   Si vous utilisez Kubernetes version 1.24 ou supérieure, exécutez la commande suivante pour afficher les secrets associés à ce compte de service :

   `kubectl -n kube-system get secrets | grep pan-plugin-user-secret`
3. **`kubectl -n kube-system get secrets <secrets-from-above-command> -o json >> cred.json`**

   Créez le fichier d'identification contenant les secrets, appelé cred.json dans cet exemple, puis enregistrez ce fichier. Vous devez télécharger ce fichier sur Panorama afin de configurer le plug-in Kubernetes pour la surveillance des clusters dans Installer le plug-in Kubernetes et configurer Panorama pour CN-Series.

STEP 2 | Exécutez `pan-mgmt-serviceaccount.yaml` et `pan-cni-serviceaccount.yaml`.

`pan-mgmt-serviceaccount.yaml` crée un compte de service appelé pan-sa. Il est nécessaire pour permettre aux Pods CN-MGMT et CN-NGFW de communiquer entre eux, avec PAN-CNI et avec le serveur API Kubernetes. Si vous modifiez ce nom de compte de service, vous devez également mettre à jour les fichiers YAML que vous utilisez pour déployer les Pods CN-MGMT et CN-NFGW.`pan-cni-serviceaccount.yaml` crée un compte de service nommé pan-cni-sa.

`kubectl apply -f pan-mgmt-serviceaccount.yaml`

`kubectl apply -f pan-cni-serviceaccount.yaml`

STEP 3 | Vérifiez les comptes de service.

`kubectl get serviceaccounts -n kube-system`

Si vous utilisez un graphique HELM, les étapes 2,3 sont automatisées par le graphique HELM et ne doivent pas être exécutées manuellement.

Installer le plug-in Kubernetes et configurer Panorama pour CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

Vous pouvez déployer l'appareil Panorama sur site ou sur le cloud, à condition que l'appareil Panorama puisse se connecter avec les clusters Kubernetes où vous souhaitez déployer les pare-feu CN-Series. Ce flux de production vous guide à travers le processus d'installation du plug-in Kubernetes, l'activation du code d'authentification et la mise en place du plug-in Kubernetes pour surveiller vos clusters.

Vous devez planifier prudemment le nombre de crédits que vous souhaitez attribuer à Panorama. Après avoir modifié le nombre de crédits, vous n'avez pas besoin de redéployer le pare-feu CN-Series sur le système d'exploitation Panorama 11.0.

Pour plus d'informations, consultez Mettre sous licence le pare-feu CN-Series *et* le logiciel NGFW Credit Estimator.

STEP 1 | Déployez un Panorama avec la version 11.0 du logiciel et installez la version de contenu minimale.

1. Accédez à **Panorama** > **Dynamic Updates (Mises à jour dynamiques)** pour connaître la version de contenu minimale sur PAN-OS 11.0.

   Consultez PAN-OS Release Notes (Notes de version PAN-OS).
2. Accédez à **Panorama** > **Software (Logiciel)** pour connaître la version du logiciel.

   Localisez et téléchargez le fichier spécifique au modèle pour la version finale vers laquelle vous effectuez la mise à niveau. Par exemple, pour mettre à niveau un appareil M-Series vers Panorama 11.0, téléchargez l'image Panorama_m-11.0.0. Pour mettre à niveau un appareil virtuel Panorama vers Panorama 11.0.0, téléchargez l'image Panorama_pc-11.0.0.

   Après un téléchargement réussi, la colonne **Action** passe de Download (Télécharger) à Install (Installer) pour l'image téléchargée.

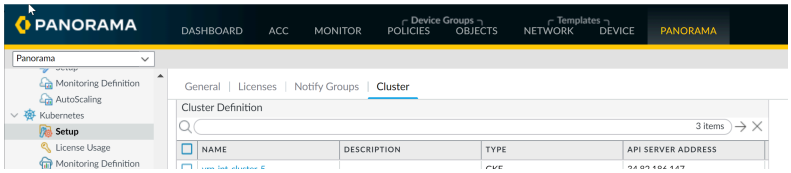
STEP 2 | Vérifiez que votre Panorama est en Panorama mode (mode Panorama), si vous voulez que Panorama collecte les journaux du pare-feu.

STEP 3 | Installez le plug-in Kubernetes sur Panorama. Si vos appareils Panorama sont déployés en tant que paire HA, vous devez d'abord installer le plug-in Kubernetes sur le pair principal (actif).

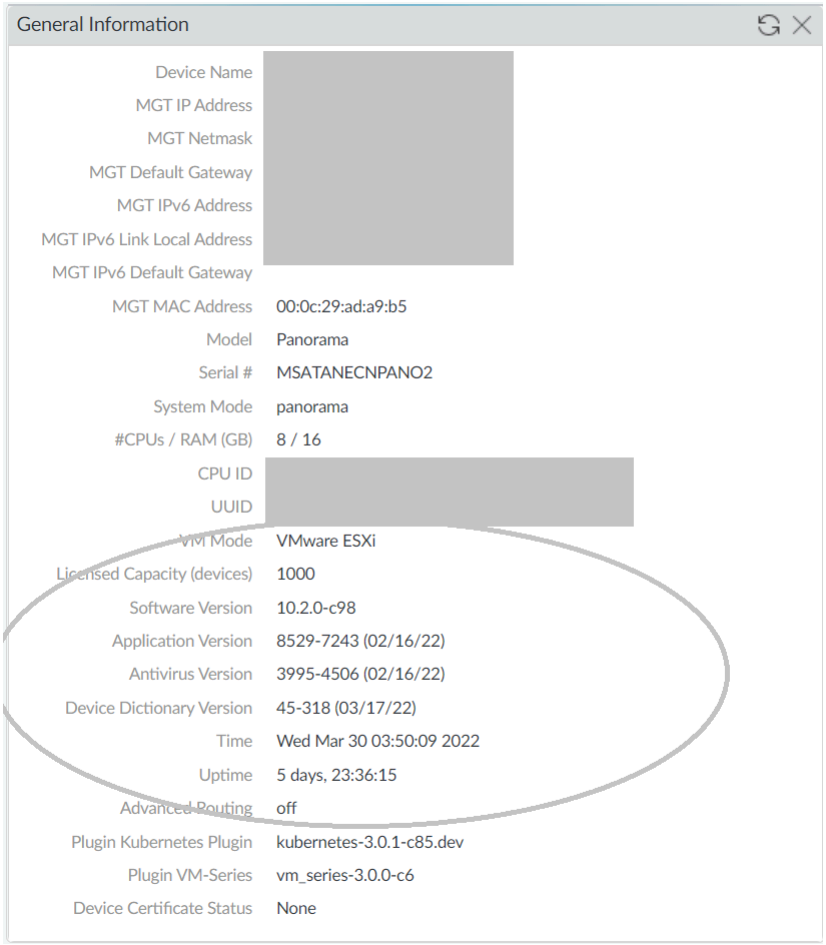
1. Connectez-vous à l'interface Web Panorama et sélectionnez **Panorama** > **Plugins** et cliquez sur **Check Now** pour obtenir le plugin AWS.
2. Sélectionnez **Download (Télécharger)** et **Install (Installer)** le plug-in Kubernetes

Une fois l'installation réussie, Panorama s'actualise et le plug-in Kubernetes s'affiche sur l'onglet **Panorama**.

Si Panorama est déployé dans une paire HA, installez le plug-in Kubernetes sur le Panorama secondaire (passif) en suivant les étapes ci-dessus décrites à l'étape 3.



Vous pouvez également vérifier le widget General Information (Informations générales) sur le **Dashboard (Tableau de bord)** Panorama.

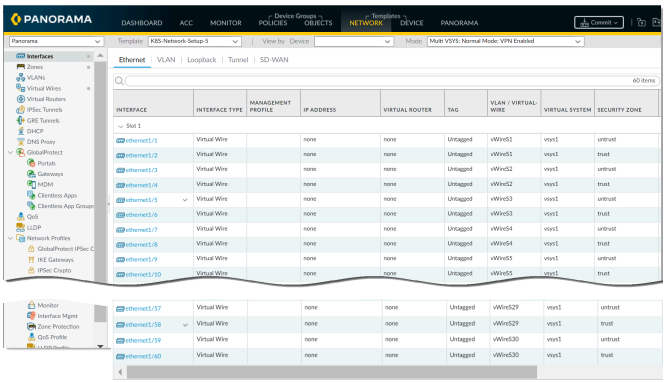


STEP 4 | Validez vos modifications sur Panorama.

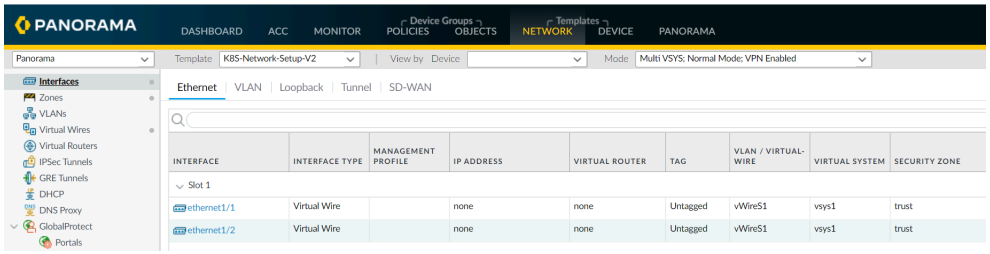
Cliquez sur **Commit to Panorama (Valider sur Panorama)**. La validation crée quatre modèles : **K8S-Network-Setup**, **K8S-Network-Setup-V2**, **K8S-Network-Setup-V3**et **K8S-Network-Setup-V3-HA**. L'affichage des interfaces sur Panorama peut prendre jusqu'à une minute.

- **K8S-Network-Setup** est destiné à être utilisé avec CN-Series en tant que DaemonSet et dispose de 30 fils virtuels ; une paire d'interfaces qui font partie d'un fil virtuel pour sécuriser une application.

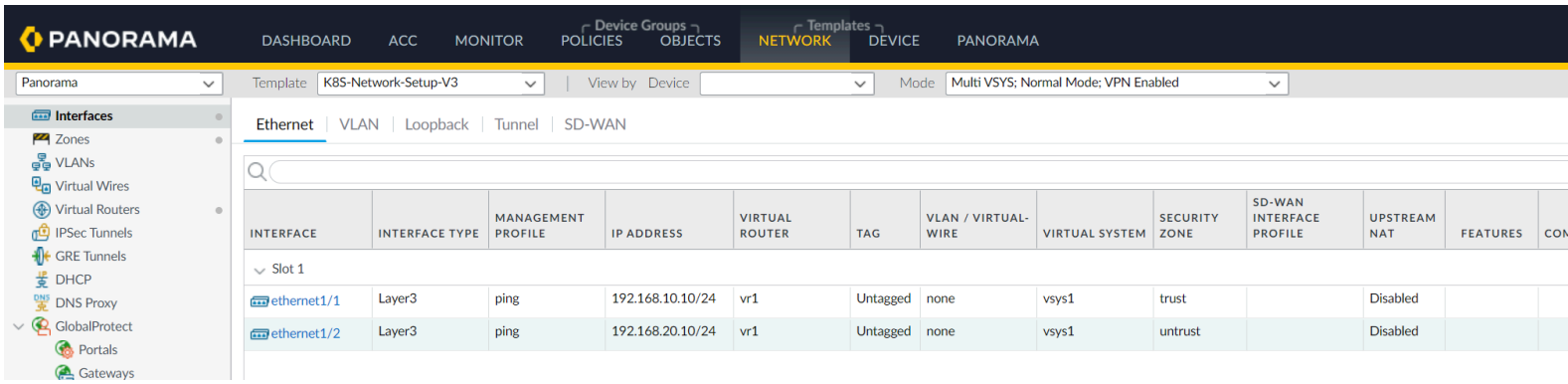
Par conséquent, le CN-NGFW en tant que DaemonSet peut sécuriser un maximum de 30 pods d'application sur un nœud.



- **K8S-Network-Setup-V2** est destiné à être utilisé avec CN-Series en tant que service Kubernetes et dispose d'un câble virtuel ; une paire d'interfaces qui font partie du fil virtuel pour sécuriser des applications de pod.



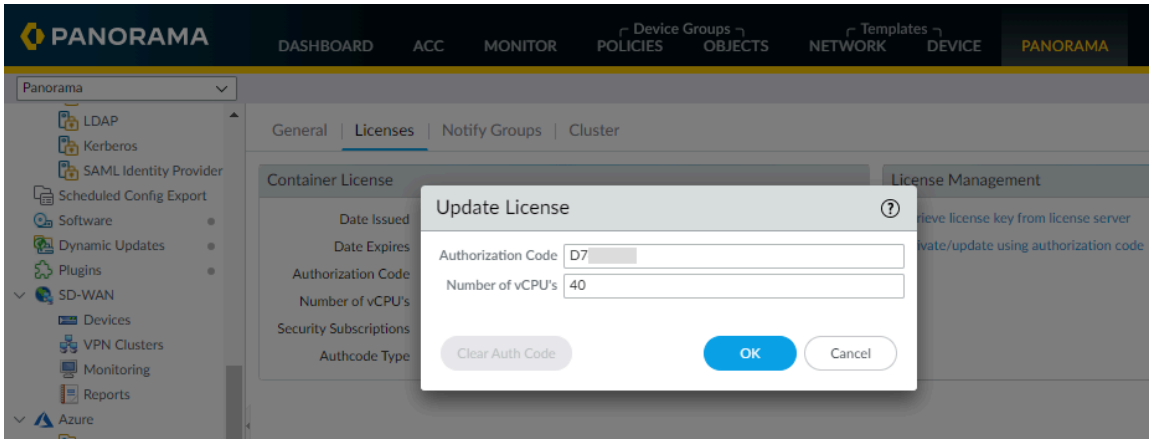
- Le modèle **K8S-Network-Setup-V3** contient un exemple de configuration que vous pouvez cloner et vous pouvez le modifier pour qu'il corresponde aux configurations souhaitées. Le mode Kubernetes CNF de déploiement protège à la fois les charges de travail conteneurisées et non conteneurisées. Vous pouvez déployer en tant que déploiement de couche 3 autonome.



STEP 5 | Obtenez les crédits de licence CN-Series sur Panorama.

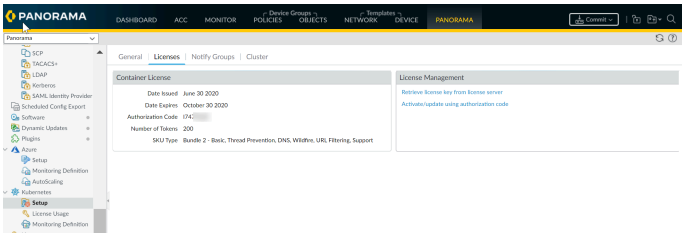
1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Kubernetes** > **Setup (Configuration)** > **Licenses (Licences)**.
2. Sélectionnez **Activate/update using authorization code (Activer/mettre à jour à l'aide du code d'autorisation)**, puis saisissez le code d'autorisation et le nombre total de vCPU de plan de

données nécessaires. Vous devez Créer un profil de déploiement de CN-Series pour obtenir votre code d'autorisation CN-Series.



Si vous déployez le pare-feu CN-Series sans activer la licence, vous disposez d'un délai de grâce de 4 heures après laquelle les pare-feu cessent de traiter le trafic. Après le délai de grâce, les instances CN-NGFW seront soit en mode « failopen » (par défaut) soit en mode « failclosed » sur la base de (FAILOVER_MODE) défini dans le fichier `pan-cn-ngfw-configmap.yaml`. En mode « fail-open », le pare-feu recevra les paquets et les enverra sans appliquer aucune politique de sécurité. Le passage en mode « fail-open » nécessitera un redémarrage et provoquera une brève interruption du trafic pendant ce temps (environ 10 à 30 secondes). En mode « fail-closed », le pare-feu supprime tous les paquets qu'il reçoit. Le mode « fail-close » réduira le Pod CN-NGFW et libérera les crédits dans le pool de crédits disponible pour la mise sous licence de nouveaux Pods CN-NGFW.

3. Vérifiez que le nombre de crédits de licence disponibles est mis à jour.



STEP 6 | Générez une clé d'authentification de VM.

1. Vérifiez que les conditions suivantes sont remplies :
   - Vous avez un ordinateur avec un accès au réseau Panorama
   - Vous connaissez l'adresse IP panorama.
   - L'interface de gestion prend en charge SSH, qui est le paramètre par défaut. Si un administrateur a désactivé SSH et que vous voulez le réactiver, sélectionnez **Panorama** > **Setup** > **Interfaces**, cliquez sur **Management** (Gestion), sélectionnez **SSH**, cliquez sur **OK**,

sélectionnez **Commit** > **Commit to Panorama**, et **Commit** (Validez) vos modifications à la configuration Panorama.

2. Pour accéder à l'ILC en utilisant SSH :
   1. Saisissez l'adresse IP Panorama dans le client SSH et utilisez le port 22.
   2. Saisissez vos informations d'accès administratif à l'invite. Après avoir connecté, le message du jour s'affiche, suivi de l'invite ILC en mode opérationnel. Par exemple :

      ```
      admin@ABC_Sydney>
      ```

3. Utilisez la commande opérationnelle suivante :

   request bootstrap vm-auth-key generate lifetime <1-8760>

   Par exemple, pour générer une clé dont la validité est de 24 heures, saisissez :

   request bootstrap vm-auth-key generate lifetime 24

   ```
   Clé d’authentification VM 755036225328715 générée.   Expire
   à : 2020/01/29 12:03:52
   ```

4. Vous devez vous assurer que vous enregistrez la clé d’authentification VM quelque part car elle est requise pour l’étape ultérieure.

STEP 7 | Créez un groupe de d’appareils parent et une pile de modèles.

Vous devez créer une pile de modèles et un groupe d’appareils. Vous ferez plus tard référence à cette pile de modèles et à ce groupe d’appareils lorsque vous modifierez le fichier YAML pour déployer les Pods CN-MGMT. Le plug-in Kubernetes sur Panorama crée un modèle appelé K8S-Network-Setup, et ce modèle fera partie de la pile de modèles que vous définissez ici.

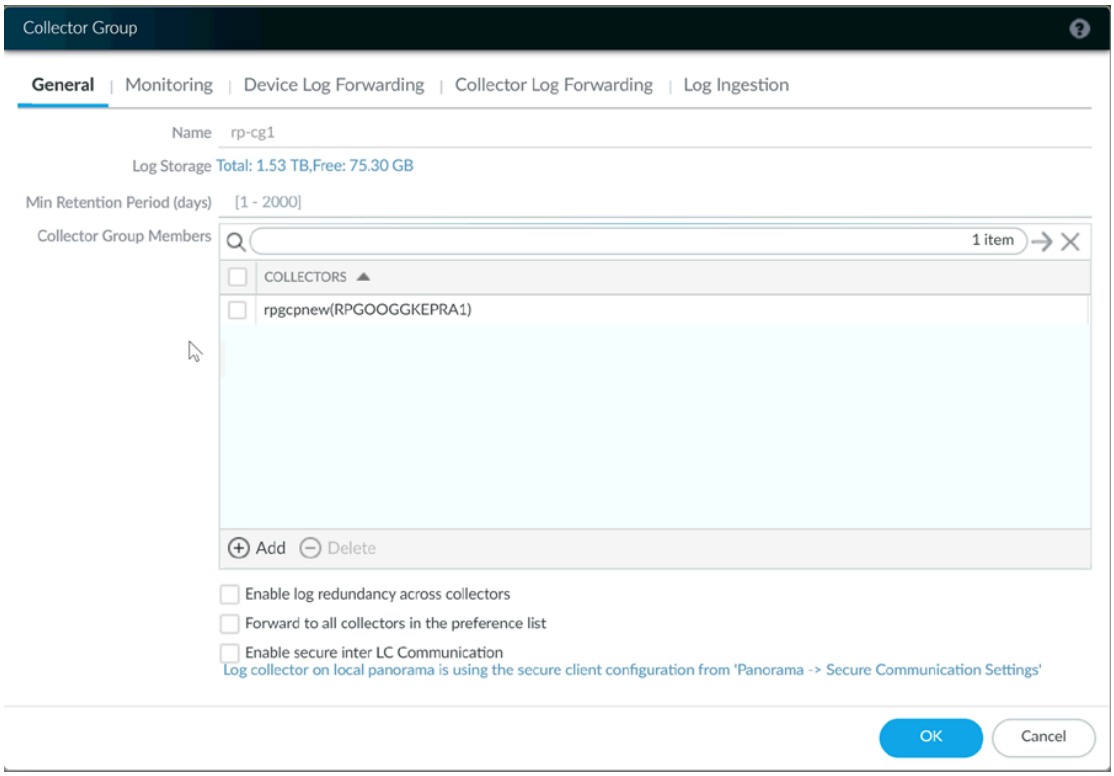
1. Configurez une pile de modèles et ajoutez le modèle K8S-Network-Setup à la pile de modèle.
   1. Sélectionnez **Panorama** > **Templates (Modèles)** et **Add Stack (Ajouter une pile)**.
   2. Entrez un **Name (Nom)** unique pour identifier la pile.
   3. Ajoutez et sélectionnez le modèle **K8S-Network-Setup** pour daemonset, **K8S-Network-Setup-V2** pour kubernetes en tant que déploiement de service, **K8S-Network-Setup-**

V3 pour un déploiement CNF autonome ou **K8S-Network-Setup-V3-HA** pour un déploiement CNF HA.

4. Cliquez sur **OK**.

2. Créez un groupe d’appareils.
   1. Accédez à **Panorama** > **Device Groups (Groupes d’appareils)**, puis cliquez sur **Add (Ajouter)**.
   2. Entrez un **Name (Nom)** unique et une **Description** pour identifier le groupe de périphériques.
   3. Sélectionnez le **Parent Device Group (Groupe de périphériques Parent)** (la valeur par défaut est **Shared (partagé)**) qui sera juste au-dessus de l’ensemble d’appareils que vous créez dans la hiérarchie de groupes de périphériques.
   4. Cliquez sur **OK**.
3. Si vous utilisez un appareil virtuel Panorama, vous pouvez créer un collecteur de journaux et l’ajouter à un groupe de collecteurs de journaux.
   1. Accédez à **Panorama** > **Collector Groups (Groupes de collecteurs)** et **Add (Ajoutez)** un groupe de collecteurs.
   2. Saisissez un **Name (Nom)** pour identifier le groupe de collecteurs.
   3. Entrez la **Minimum Retention Period (Période de conservation minimale)** en jours (1 à 2 000) pendant laquelle le groupe de collecteurs sera conservé pour les journaux de pare-feu.

      Par défaut, le champ est vide, ce qui signifie que le groupe de collecteurs conserve indéfiniment les journaux.
   4. **Add (Ajoutez)** les collecteurs de journaux (1 à 16) à la liste des membres du groupe de collecteurs.



5. Sélectionnez **Commit** > **Commit and Push**, puis **Commit and Push** (Valider et appliquer) vos modifications à Panorama et au groupe de collecteurs que vous avez configuré.

4. Si vous utilisez le routage avancé, activez-le.

   1. Accédez à **Panorama** > **Templates (Modèles) > Device (Périphérique)**.
   2. Dans l'onglet **Gestion**, sélectionnez **Advanced Routing** (Routage avancé) (ceci est applicable au mode de déploiement de Kubernetes CNF uniquement).

STEP 8 | Configurez le plug-in Kubernetes pour la surveillance des clusters.

L'étape suivante du processus consiste à ajouter les informations de cluster Kubernetes à Panorama pour s'assurer que les deux peuvent communiquer entre eux.

Panorama prend en charge jusqu'à 32 clusters Kubernetes.

Pour s'assurer que le plug-in et les clusters Kubernetes sont synchronisés, le plug-in interroge le serveur API Kubernetes à un intervalle configuré et écoute les notifications de l'API Kubernetes Watch à un intervalle prédéfini.

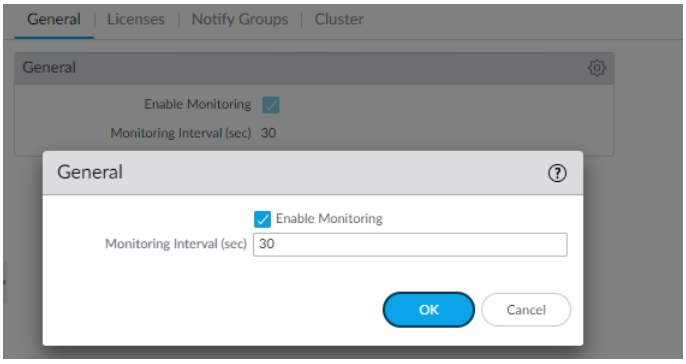
Après avoir ajouté les informations sur les clusters, Panorama récupère toujours l'ensemble du service, du nœud et de la réplique, puis crée des étiquettes pour chacun d'entre eux afin de vous permettre de gagner en visibilité et de contrôler le trafic vers et depuis ces clusters. En option, vous pouvez spécifier si vous souhaitez que Panorama récupère des informations sur les étiquettes Kubernetes et

crée des étiquettes pour celles-ci également. Reportez-vous à la section Mappage étiquette/adresse IP des attributs Kubernetes pour une liste des attributs pris en charge.

1. Vérifiez l'intervalle de surveillance.

   L'intervalle par défaut utilisé par Panorama pour interroger le terminal du serveur API Kubernetes est de 30 secondes.

   1. Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Kubernetes** > **Setup (Configuration)** > **General (Général)**.
   2. Vérifiez que **Enable Monitoring (Activer la surveillance)** est sélectionné.
   3. Cliquez sur l'icône de l'engrenage pour modifier **l'intervalle de surveillance** et passer à une plage de 30-300 secondes.



2. Sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Kubernetes** > **Setup (Configuration)** > **Cluster**, puis **Add Cluster (Ajouter cluster)**.

   Veillez à ne pas ajouter le même cluster Kubernetes à plus d'un appareil Panorama (instance unique ou paire HA), car vous pourriez constater des incohérences dans la manière dont les correspondances entre les adresses IP et les groupes d'appareils sont enregistrées.

3. Saisissez un **nom** et **l'adresse serveur API**.

   Il s'agit de l'adresse IP du terminal pour le cluster que vous devez obtenir de votre déploiement Kubernetes. Saisissez un nom, jusqu'à 20 caractères, pour identifier de manière unique le nom du cluster. Vous ne pouvez pas modifier ce nom car Panorama utilise le nom du cluster lorsqu'il crée des étiquettes pour les pods, nœuds, services qu'il découvre au sein du cluster.

   Le format de l'adresse du serveur API peut être un nom d'hôte ou une adresse IP : numéro de port. Vous n'avez pas besoin de spécifier le port si vous utilisez le port 443, étant celui par défaut.

4. Sélectionnez le **Type** d'environnement sur lequel votre cluster est déployé.

   Les options disponibles sont AKS, EKS, GKE, Native Kubernetes, OpenShift et autres.

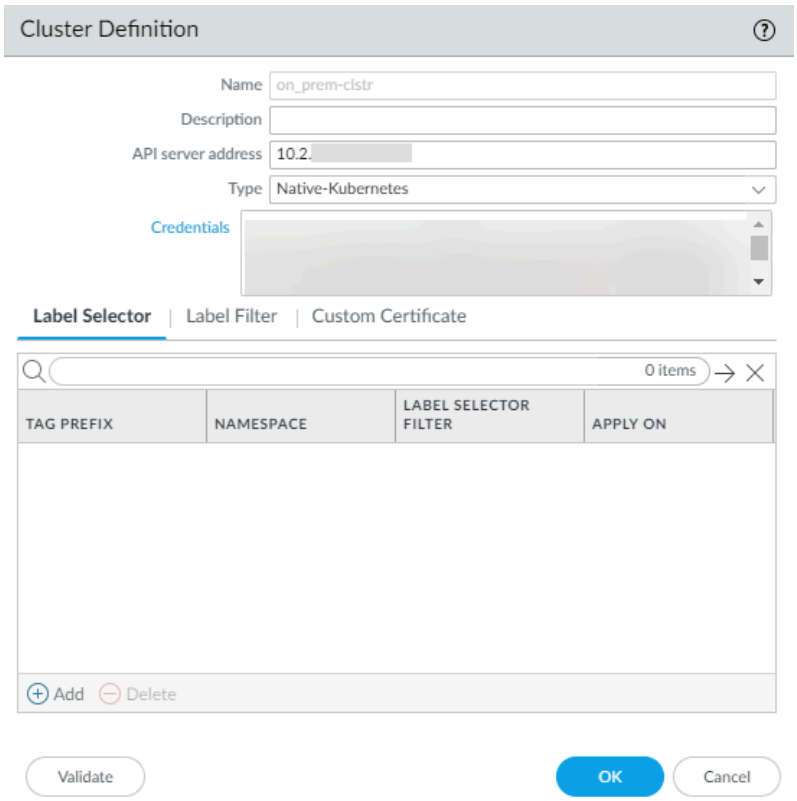
5. Téléchargez les **informations d'identification** du compte de service dont Panorama a besoin pour communiquer avec le cluster. Comme décrit dans le Création de comptes de service pour

l'authentification des clusters flux de production, le nom de fichier de ce compte de service est `plugin-svc-acct.json`.

Si vous téléchargez les informations d'identification de service via un CLI / une API, vous devez compresser le fichier puis effectuer un encodage base64 du fichier compressé avant de télécharger ou de coller le contenu du fichier dans l'API ou le CLI Panorama. Ces étapes ne sont pas nécessaires si vous téléchargez le fichier d'informations d'identification du service sur l'interface graphique.

6. Cliquez sur **OK**.

   Vous pouvez reporter à plus tard la configuration du Sélecteur de filtres et du Sélecteur d'étiquettes. Il s'agit d'une tâche facultative qui vous permet de récupérer les étiquettes personnalisées ou définies par l'utilisateur pour lesquelles vous souhaitez que Panorama crée des étiquettes.

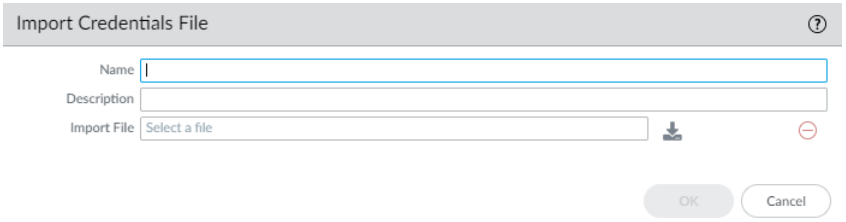


STEP 9 | (Facultatif) Si votre certificat de serveur API de cluster Kubernetes est signé par une chaîne de certificats, l'authentification à partir du plug-in Kubernetes pour Panorama nécessite chaque certificat

de la chaîne. Si votre serveur API utilise une chaîne de certificats, vous devez combiner tous les certificats de la chaîne dans un seul fichier .crt et les ajouter au plug-in.

Le plug-in Kubernetes prend en charge jusqu'à quatre certificats.

1. Sélectionnez **Panorama** > **Kubernetes** > **Setup** > **Cluster** > **Add** > **Custom Certificate** > **Add** pour importer un fichier d'informations d'identification.
2. Saisissez un **Name (Nom)** descriptif.
3. (Facultatif) Saisissez une **Description (Description)**.
4. Cliquez sur l'icône d'importation et accédez au fichier de certificat.
5. Cliquez sur **OK**.



STEP 10 | (Facultatif) Configurez un proxy pour chaque cluster.

Contrairement aux autres plug-ins, le plug-in Kubernetes n'utilise pas le proxy configuré sous **Panorama** > **Setup (Configuration)** > **Services**. En revanche, si vous souhaitez activer ou ignorer un proxy, vous devez entrer le proxy pour chaque cluster. Lorsqu'il est configuré, le plug-in Kubernetes utilise l'adresse IP de ce serveur proxy pour effectuer tous les appels API au serveur API de ce cluster.

1. Connectez-vous au CLI de Panorama.
2. Saisissez les commandes CLI suivantes pour configurer le serveur proxy de ce cluster Kubernetes.

```
> configure> set plugins kubernetes setup cluster-credentials <cluster-name>  cluster-proxy enable-proxy <yes/no> proxy-port <port>  proxy-server <IP> proxy-user <username>  secure-proxy-password <password>
```

```
*** le nom d'utilisateur et le mot de passe sont facultatifs ***
```

STEP 11 | Étapes suivantes :

1. Obtenir les images et les fichiers pour le déploiement CN-Series
2. Déploiement du pare-feu CN-Series
3. Configurer Panorama pour sécuriser un déploiement Kubernetes

Obtenir les images et les fichiers pour le déploiement CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Déploiement CN-Series	• CN-Series 10.1.x or above Container Images • Panorama sous PAN-OS 10.1.x ou une version supérieure • Helm 3.6 or above version client pour le déploiement CN-Series à l'aide de Helm

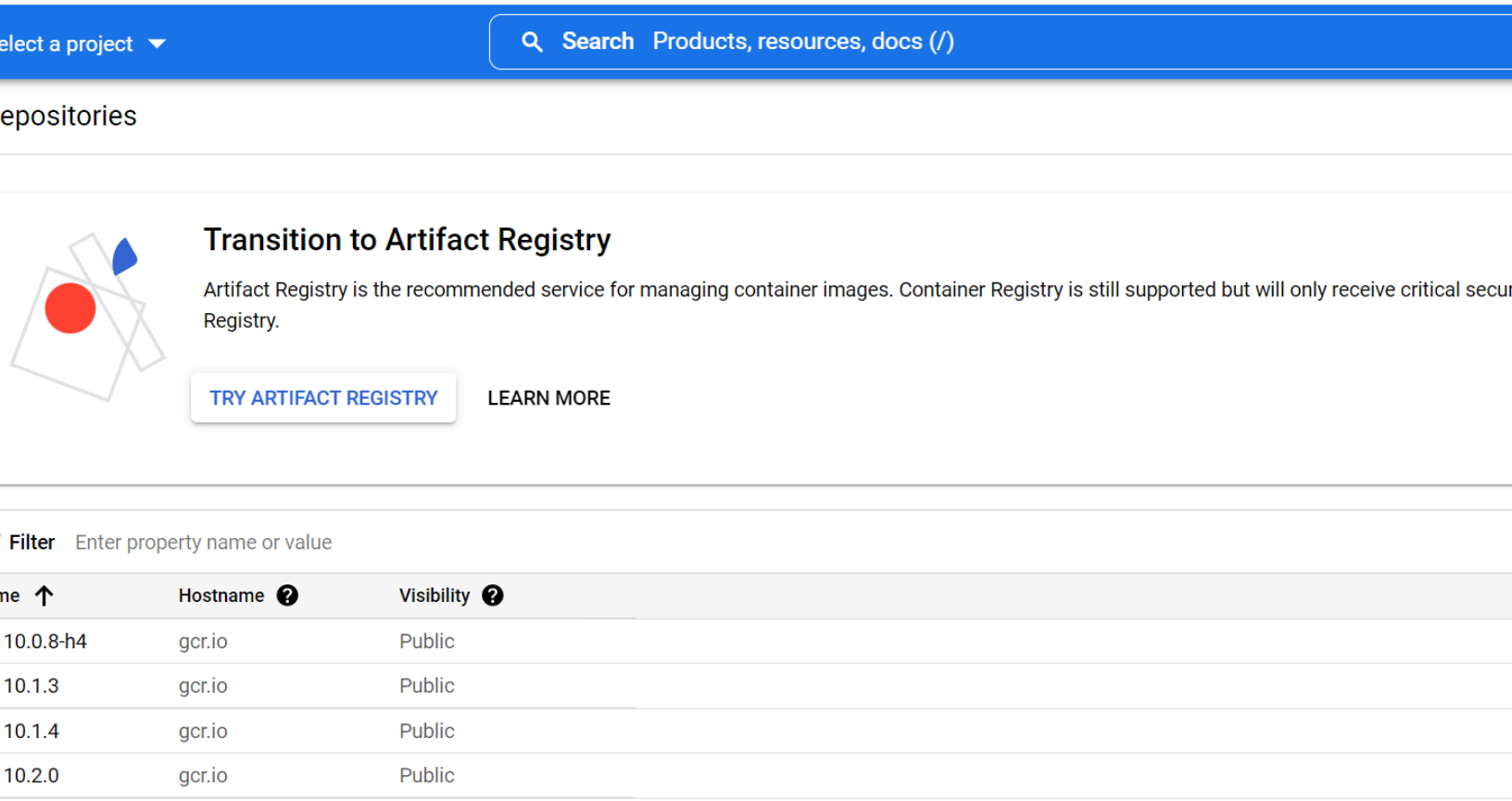
Reportez-vous au tableau suivant avant de commencer votre déploiement pour vous assurer que vous avez téléchargé les fichiers compatibles.

Version PAN-OS	Version YAML	Version CNI	Version MGMT-INIT
PAN-OS 11.1.x	3.0.x	3.0.x	3.0.x
PAN-OS 11.0.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.2.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.1.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.0.x	1.0.x	1.0.x	3.0.x

Procédez comme suit pour extraire les images docker du répertoire des conteneurs publics sur Google Cloud Platform, puis continuez vers déployer le pare-feu CN-Series :

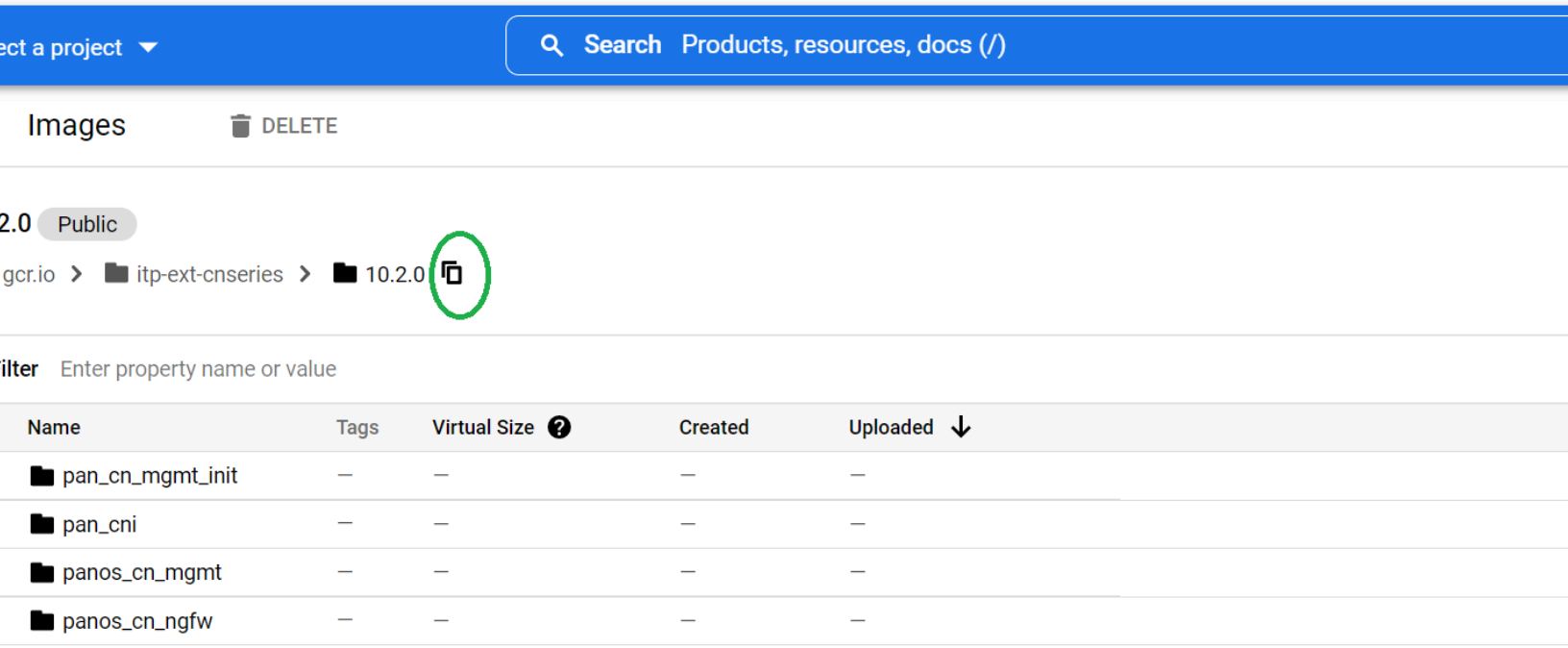
Images Docker du répertoire de conteneurs publics :

1. En fonction de votre version PAN-OS, extrayez les images docker requises du répertoire cloud public.



2. Sélectionnez la version PAN-OS requise.

3. Copiez le lien de chaque chemin d'accès d'image à l'emplacement approprié dans vos fichiers YAML de déploiement.



Procédez comme suit pour obtenir les fichiers YAML à partir de GitHub :

1. Ouvrez le dossier de la méthode de déploiement (DaemonSet, Kubernetes Service ou Kubernetes CNF) que vous prévoyez d'utiliser.
2. Téléchargez les fichiers yaml à partir du dossier correspondant à votre environnement.

   Récupérez les fichiers à partir du dossier Native-k8s pour les déploiements de Kubernetes natif sur site ou sur le cloud.

   Récupérez les fichiers à partir du dossier Managed Kubernetes correspondant pour GKE.

Images Docker du CSP Palo Alto Networks :

Utilisez les étapes suivantes pour obtenir les fichiers YAML à partir de GitHub et pour télécharger les images docker à partir du CSP de Palo Alto Networks et transférez-les vers votre répertoire privé avant de continuer vers déployer le pare-feu CN-Series.

STEP 1 | Téléchargez les images du docker et les fichiers YAML.

1. Récupérez les archives compressées tar à partir du portail d'assistance client (CSP) de Palo Alto Networks.
   1. Connectez-vous au CSP à l'aide de votre compte d'assistance.
   2. Sélectionnez **Updates** > **Software Updates**.
   3. Sélectionnez **Pan-OS Container Images** (Images de conteneur Pan-OS) dans la liste déroulante **Please Select** (Veuillez sélectionner).
   4. Téléchargez les fichiers suivants pour la version PAN-OS que vous souhaitez déployer.

      PanOS_cn-X.X.X.tgz - pour les pods CN-MGMT et CN-NGFW.

      Pan_cn_mgmt_init-X.X.X.tgz - pour le conteneur init qui fait partie du pod CN-MGMT.

      Pan_cni-2.0.0.tgz - pour le pod PAN-CNI.
2. Récupérez les fichiers YAML à partir de GitHub.
   1. Ouvrez le dossier de la méthode de déploiement (DaemonSet, Kubernetes Service ou Kubernetes CNF) que vous prévoyez d'utiliser.
   2. Téléchargez les fichiers yaml à partir du dossier correspondant à votre environnement.

      Récupérez les fichiers à partir du dossier Native-k8s pour le déploiement de Kubernetes natif sur site ou sur le cloud.

      Récupérez les fichiers à partir du dossier Managed Kubernetes correspondant pour AKS, EKS ou GKE.

STEP 2 | Récupérez les images du docker et transférez-les vers votre registre de conteneur.

Par exemple, lors d'un déploiement GKE, vous allez télécharger les images dans un registre de conteneur sur GKE et obtenir le chemin d'accès des images pour les référencer dans les fichiers YAML. Utilisez les commandes suivantes sur un système client exécutant le moteur docker.

Remplacez les variables x dans les étapes suivantes par les valeurs qui correspondent à la version de l'image que vous utilisez. Par exemple, Pan_cn_mgmt-init-2.0.0.tgz ou pan_cni:2.0.0.

1. Chargez les images.

   docker load -i PanOS_cn-x.x.x.tgz

   docker load -i Pan_cn_mgmt-init-x.x.x.tgz

   docker load -i Pan_cni-x.x.x.tgz

   Après ces étapes, les « images docker » afficheront l'image, par exemple, « paloaltonetworks/panos_cn_mgmt:x.x.x ».

2. Étiquetez ces images pour y inclure les détails de votre registre privé.

   docker tag paloaltonetworks/panos_cn_mgmt:x.x.x <your_registry>/paloaltonetworks/panos_cn_mgmt:x.x.x

   docker tag paloaltonetworks/panos_cn_ngfw:x.x.x <your_registry>/paloaltonetworks/panos_cn_ngfw:x.x.x

   docker tag paloaltonetworks/pan_cn_mgmt_init:x.x.x <your_registry>/paloaltonetworks/pan_cn_mgmt_init:x.x.x

   docker tag paloaltonetworks/pan_cni:x.x.x <your_registry>/paloaltonetworks/pan_cni:x.x.x

3. Transférez ces images dans votre registre privé.

   docker push <your_registry>/paloaltonetworks/panos_cn_mgmt:x.x.x

   docker push <your_registry>/paloaltonetworks/panos_cn_ngfw:x.x.x

   docker push <your_registry>/paloaltonetworks/pan_cn_mgmt_init:x.x.x

   docker push <your_registry>/paloaltonetworks/pan_cni:x.x.x

Service de journalisation Strata avec le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Service de journalisation Strata avec le pare-feu CN-Series	• Panorama fonctionnant avec la version minimale de PAN-OS 11.1 • Licence de service de journalisation Strata

Le service de journalisation Strata permet des innovations basées sur l'IA pour la cybersécurité avec la seule approche du secteur pour normaliser et assembler les données de votre entreprise. Pour plus d'informations, consultez la section Introduction au service de journalisation Strata et au service de journalisation Strata pour les pare-feu gérés par Panorama. Le service de journalisation Strata peut désormais collecter des données de journal à partir du pare-feu nouvelle génération CN-Series. Lorsque vous achetez une licence pour le service de journalisation Strata, tous les pare-feu enregistrés sur votre compte d'assistance reçoivent une licence pour le service de journalisation Strata. Vous recevrez également un lien Magic que vous devrez utiliser pour activer votre instance de service de journalisation Strata.

Pour démarrer avec la journalisation du service de journalisation Strata du pare-feu CN-Series, vous devez vous assurer d'installer le plug-in Kubernetes et de configurer Panorama pour votre pare-feu CN-Series. Fournissez le certificat de périphérique au pod CN-MGMT pour la connectivité du service de journalisation Strata. Il est important d'enregistrer votre pod CN-MGMT auprès d'un compte CSP pour garantir que le pod CN-MGMT est reflété dans votre instance de service de journalisation Strata. Ajoutez le code PIN et la valeur PIN valides au fichier `pan-cn-mgmt-secret.yaml` pour installer avec succès le certificat de périphérique. Le pare-feu CN-Series nécessite un certificat de périphérique qui autorise un accès sécurisé au service de journalisation Strata. Pour plus d'informations, consultez Installer un certificat de périphérique sur le pare-feu CN-Series.

Après avoir déployé votre pare-feu CN-Series, vérifiez que votre pod CN-MGMT est visible sur votre compte de service de journalisation Strata, sous **Périphériques enregistrés**. Pour plus d'informations, consultez Enregistrer le pare-feu. Assurez-vous de configurer votre pare-feu CN-Series avec Panorama, de créer un profil de déploiement de CN-Series sur votre compte CSP et d'utiliser le code d'authentification pour transmettre les licences de Panorama vers votre pare-feu CN-Series.

Configuration du service de journalisation Strata pour le pare-feu CN-Series

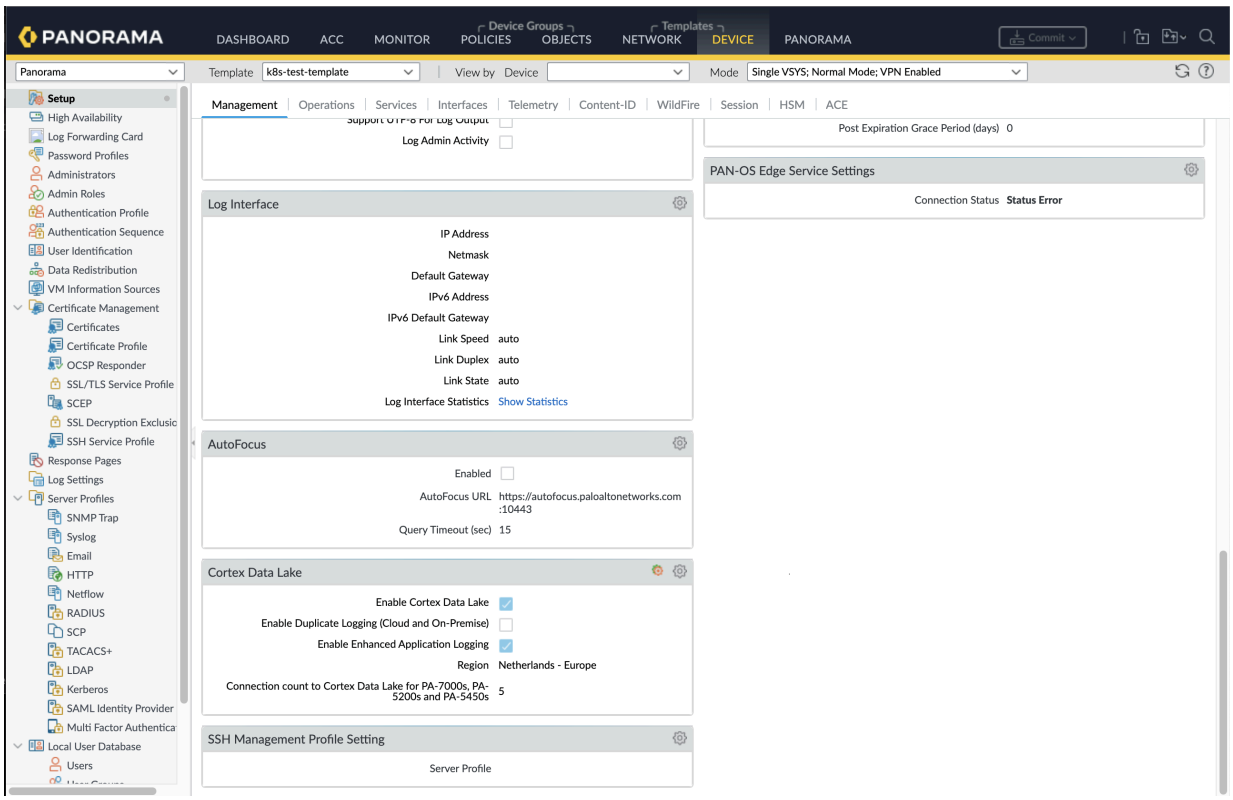
Le service de journalisation Strata fournit un stockage et une agrégation centralisés des journaux dans le cloud pour les services et applications fournis dans le cloud.

Assurez-vous de disposer d'une licence de journalisation et d'une instance de service de journalisation Strata créée dans votre compte CSP. Pour plus d'informations, consultez Service de journalisation Strata.

Effectuez les étapes suivantes pour configurer les paramètres du service de journalisation Strata sur Panorama et les transmettre au pare-feu :

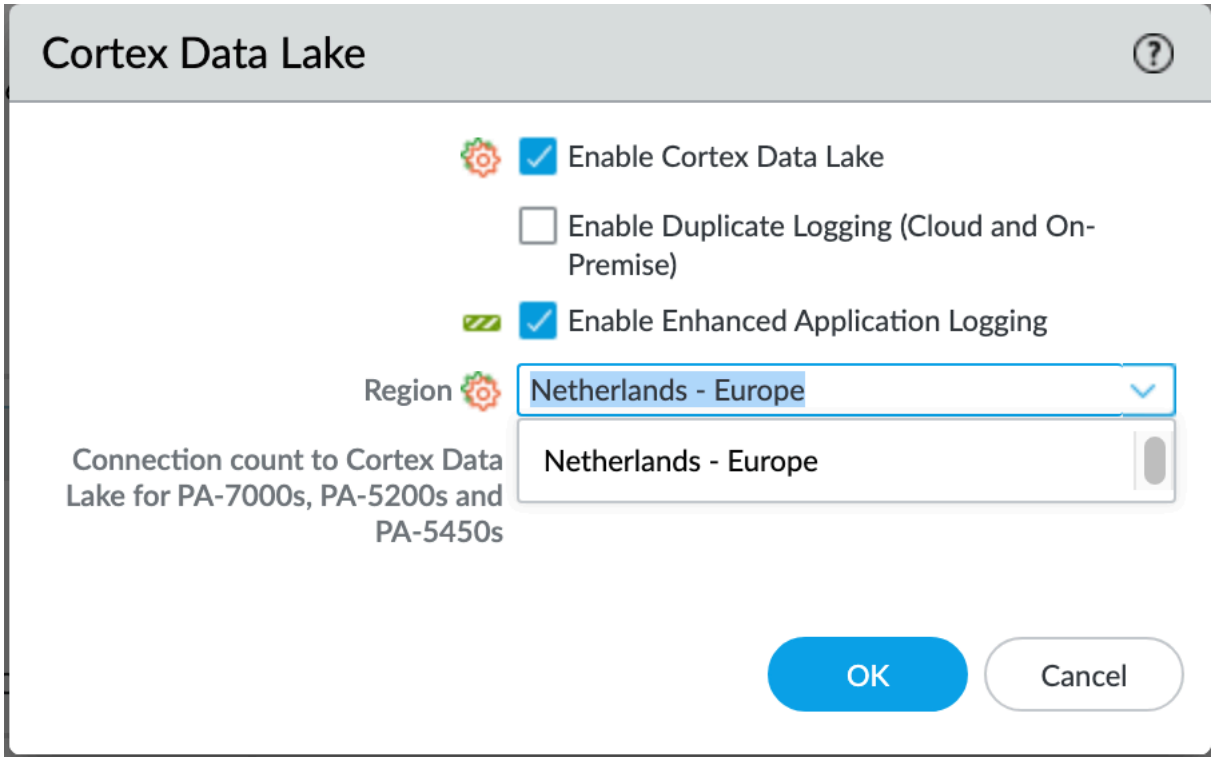
1. Intégrez votre Panorama au service de journalisation Strata pour activer les paramètres des configurations du service de journalisation Strata sur le périphérique.
2. Intégrez votre pare-feu CN-Series à l’instance de service de journalisation Strata.

3. Dans votre panorama, accédez à l’onglet **Device** (Appareil), puis cliquez sur **Settings** (Paramètres) dans le volet **Service de journalisation Strata**.



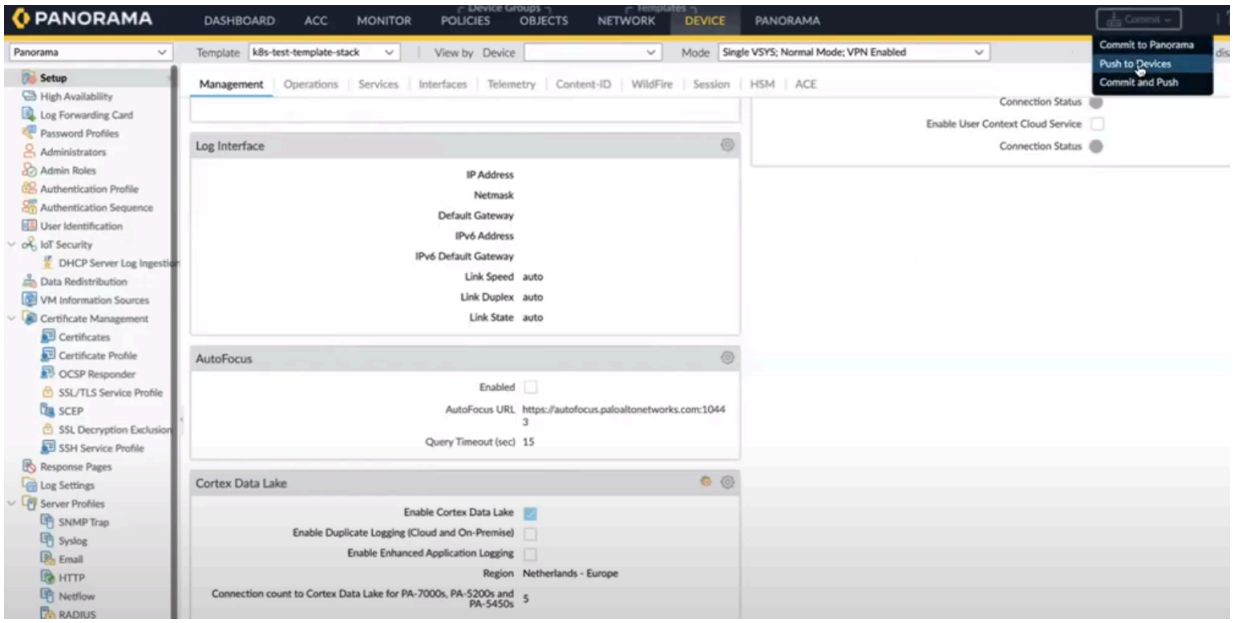
Vous pouvez maintenant voir que la **région** est générée.

4. Cliquez sur **Enable Strata Logging Service** (Activer le service de journalisation Strata).



5. Cliquez sur **OK**.

6. Allez dans **Commit** (Valider) > **Push to Devices** (Appliquer aux périphériques).



7. Sélectionnez votre pod **CN-MGMT**.
8. Cliquez sur **OK**.

   La configuration du service de journalisation Strata pour le pod CN-MGMT est désormais transmise. Le pod CN-MGMT va maintenant initier sa connexion à l'instance de service de journalisation Strata.

Une fois que votre pare-feu intégré est **connecté**, vous pouvez commencer à envoyer des journaux à votre instance de service de journalisation Strata. Pour plus d'informations, consultez Commencer l'envoi de journaux au service de journalisation Strata (géré par Panorama).

Prise en charge de la solution IoT Security pour le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Sécurité IoT pour le pare-feu CN-Series	• Licence de service de journalisation Strata pour l'abonnement IoT qui stocke les données dans le service de journalisation Strata • Panorama fonctionnant avec la version minimale de PAN-OS 11.1

Pour le pare-feu CN-Series de nouvelle génération de Palo Alto Networks, la solution IoT Security utilise le machine learning (ML) pour fournir une visibilité des périphériques IoT découverts en fonction des métadonnées contenues dans les journaux qu'elle reçoit du pare-feu. IoT Security identifie également les vulnérabilités et évalue les risques liés aux périphériques en fonction de leurs comportements de trafic réseau et des flux de menaces mis à jour de manière dynamique.

Vous pouvez utiliser les recommandations de règles de politique générées par IoT Security comme référence lors de l'ajout manuel de règles à votre pare-feu CN-Series. IoT Security génère toujours des recommandations de règles de politique de sécurité, quelle que soit la version de PAN-OS.

*Lorsque vous utilisez **l'abonnement de sécurité IoT**, qui stocke des données dans le service de journalisation Strata, vous avez besoin d'une licence de service de journalisation Strata par compte et devez vous assurer que la* configuration de service de journalisation Strata pour votre pare-feu CN-Series *est complète.*

Pour plus d'informations, consultez Conditions préalables à IoT Security.

Configurer la prise en charge IoT pour le pare-feu CN-Series

Vous devez vous assurer que votre environnement répond à toutes les conditions préalables au déploiement de la solution IoT Security avec le pare-feu CN-Series. Pour plus d'informations, consultez Conditions préalables à IoT Security.

Pour configurer l'abonnement **IoT, nécessite un abonnement à Data Lake** pour le pare-feu CN-Series, vous devez suivre les étapes suivantes :

Vous devez vous assurer d'intégrer votre Panorama à l'instance du service de journalisation Strata. Pour plus d'informations, consultez Pare-feu intégrés à Panorama.

1. Créez un groupe de services aux locataires (TSG). Pour plus d'informations, reportez-vous à **l'étape 3** dans Activer les abonnements de sécurité IoT via les services communs.
2. Intégrez le locataire du service de journalisation Strata au TSG. Vous devez vous assurer d'acheter le service de journalisation Strata et de l'activer en utilisant le lien Magic avant de l'utiliser dans le TSG.
3. Créez un profil de déploiement CN-Series avec l'option **IoT, nécessite un abonnement à Data Lake**.

4. Cliquez sur **Finish Setup** (Terminer la configuration). Une fois que vous associez le profil de déploiement au TSG et cliquez sur **Activate** (Activer), un locataire IoT sera créé s'il n'en existe pas déjà un.

   Vous pouvez ensuite transmettre les métadonnées collectées au service de journalisation basé sur le cloud où IoT Security les utilise pour identifier divers périphériques IoT sur le réseau.
5. Provisionnez Panorama et générez un numéro de série. Pour plus d'informations, consultez Enregistrer Panorama et installer les licences.
6. Configurez votre pare-feu CN-Series avec Panorama à l'aide du code d'authentification pour transférer les licences de Panorama vers le pare-feu CN-Series à l'aide du plug-in Kubernetes. Pour plus d'informations, consultez Configurer Panorama pour sécuriser un déploiement Kubernetes.

   Appliquez le code d'authentification de déploiement au plug-in Kubernetes dans Panorama.

   Vous pouvez désormais voir votre pare-feu CN-series intégré sur un locataire IoT.
7. Configurez le modèle de câble virtuel pour autoriser et activer l'ID de périphérique dans la zone.

   Vous pouvez utiliser le modèle par défaut **K8S-Network-Setup-V2** et y apporter les modifications suivantes :

   - Activer la transmission d'état de liaison et le pare-feu multicast pour câble virtuel par défaut.
   - Activer l'identification du périphérique pour la zone par défaut.

   Pour plus d'informations, voir Configurer les câbles virtuels.
8. Configurez les options **Activer Cortex Data Lake** et **Activer l'enregistrement amélioré des applications** Panorama au pare-feu CN-Series. Pour plus d'informations, consultez la section Configuration du service de journalisation Strata pour votre pare-feu CN-Series.

Pour configurer **IoT Security, ne nécessite pas d'abonnement à Data Lake** pour le pare-feu CN-Series, vous devez suivre les étapes suivantes :

Note : Vous devez vous assurer d'intégrer votre Panorama sur l'instance du service de journalisation Strata. Lorsque vous utilisez IoT Security, ne nécessite pas d'abonnement à Data Lake, vous devez enregistrer votre Panorama sur le portail IoT après avoir ajouté le pare-feu CN-series. Pour plus d'informations, consultez **l'étape 2** dans Préparez votre pare-feu pour IoT Security.

1. Créez un groupe de services aux locataires (TSG). Pour plus d'informations, reportez-vous à **l'étape 3** dans Activer les abonnements de sécurité IoT via les services communs.
2. Créez un profil de déploiement CN-Series avec l'option **IoT, ne nécessite pas d'abonnement à Data Lake**.
3. Configurez votre instance IOT et sélectionnez l'option **Finish Setup** (Terminer la configuration) pour associer votre profil de déploiement au groupe de services aux locataires (TSG) afin d'activer le service de journalisation sur votre pare-feu CN-Series et de le configurer pour obtenir et journaliser les métadonnées du trafic réseau. Pour plus d'informations, consultez Préparez votre pare-feu pour IoT Security.

   Vous pouvez ensuite transmettre les métadonnées collectées au service de journalisation basé sur le cloud où IoT Security les utilise pour identifier divers périphériques IoT sur le réseau.
4. Provisionnez Panorama et générez un numéro de série. Pour plus d'informations, consultez Enregistrer Panorama et installer les licences.

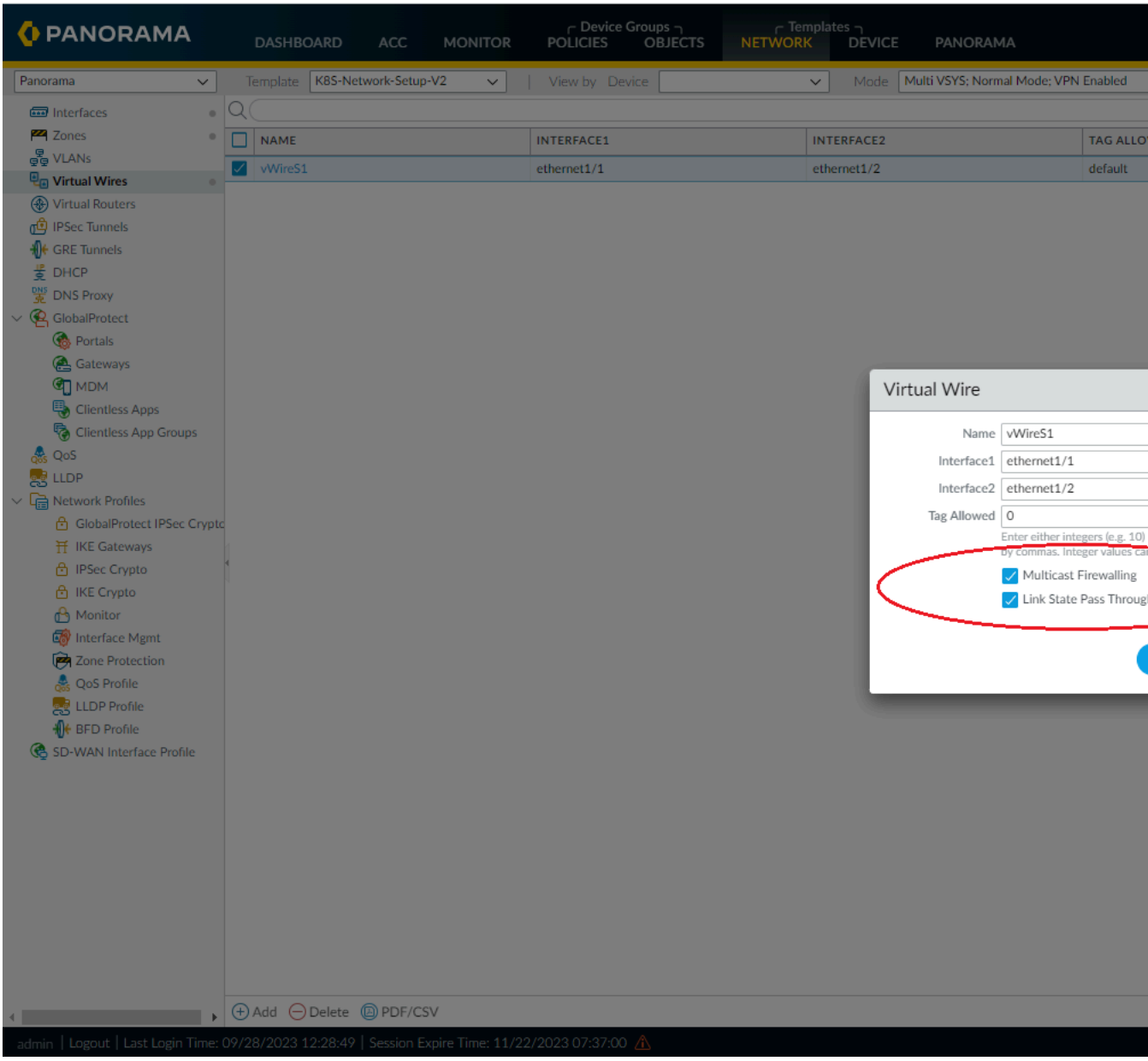
5. Configurez votre pare-feu CN-Series avec Panorama à l'aide du code d'authentification pour transférer les licences de Panorama vers le pare-feu CN-Series à l'aide du plug-in Kubernetes. Pour plus d'informations, consultez Configurer Panorama pour sécuriser un déploiement Kubernetes.

   Appliquez le code d'authentification de déploiement au plug-in Kubernetes dans Panorama. Vous pouvez désormais voir votre pare-feu CN-series intégré sur un locataire IoT.

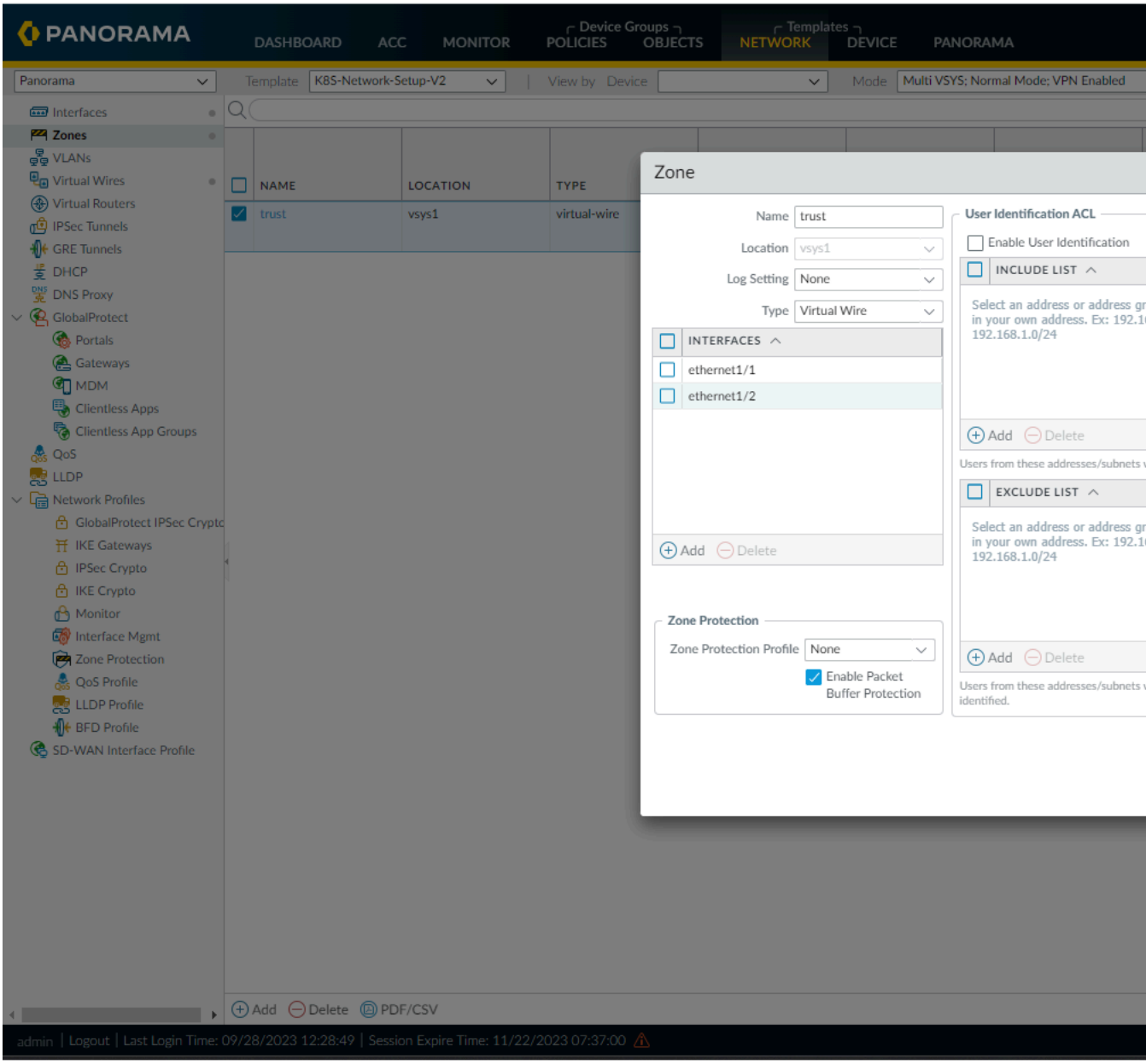
6. Configurez le modèle de câble virtuel pour autoriser et activer l'ID de périphérique dans la zone. Pour plus d'informations, voir Configurer les câbles virtuels.

   Vous pouvez utiliser le modèle par défaut **K8S-Network-Setup-V** et y apporter les modifications suivantes :

   - Activer la transmission d'état de liaison et le pare-feu multicast pour câble virtuel par défaut.



   - Activer l'identification du périphérique pour la zone par défaut.



Pour plus d'informations, voir Configurer les câbles virtuels.

Le câble virtuel configuré dans k8s-template-v2 permet le passage d'état de liaison et le pare-feu multicast. La configuration de zone du k8s-template-v2 permet l'identification du périphérique

7. Configurez les options **Activer Cortex Data Lake** et **Activer l'enregistrement amélioré des applications** Panorama au pare-feu CN-Series. Pour plus d'informations, consultez la section Configuration du service de journalisation Strata pour votre pare-feu CN-Series

Après avoir intégré avec succès votre pare-feu Panorama et CN-Series au service de journalisation basé sur le cloud, accédez à votre instance IoT.

Une fois qu'IoT Security dispose de suffisamment d'informations pour identifier les périphériques à partir de leur comportement réseau, il fournit au pare-feu CN-Series des mappages d'adresse IP vers le périphérique et à Panorama des recommandations de politique que l'administrateur de Panorama peut

importer puis transmettre au pare-feu CN-Series pour appliquer la politique sur le trafic des périphériques IoT.

Cliquez sur **Administration** > **Sites and Firewalls** (Sites et pare-feu) > **Firewalls** (Pare-feu) dans le portail IoT Security pour voir l'état des journaux que le service de journalisation diffuse vers l'application IoT Security. Pour plus d'informations, consultez État de l'intégration d'IoT Security avec les pare-feu.

Déchargement basé sur la méthode à la volée logicielle sur le pare-feu CN-Series

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• CN-Series comme déploiement Kubernetes CNF	• CN-Series 10.1.x or above Container Images • Pour le pare-feu CN-Series géré par Panorama, Panorama exécutant PAN-OS 11.0.4 ou une version supérieure

Vue d'ensemble

Grâce au service Intelligent Traffic Offload (ITO) basé sur la méthode à la volée logicielle, le pare-feu CN-Series élimine le compromis entre les performances du réseau, la sécurité et le coût. Pour chaque nouveau flux sur le réseau, le service ITO détermine si le flux peut ou non bénéficier d'un contrôle de sécurité. Le service ITO achemine les premiers paquets du flux vers le pare-feu pour inspection, qui détermine s'il faut inspecter ou décharger le reste des paquets du flux. Cette détermination est basée sur la politique ou sur l'incapacité du flux à inspecter. En inspectant uniquement les flux pouvant bénéficier de l'inspection de sécurité, la charge globale sur le pare-feu est réduite et les performances augmentent sans sacrifier la posture de sécurité.

Pour les infrastructures dépourvues de DPU, l'ITO basé sur la méthode à la volée logicielle est capable de fonctionner en tirant parti des cartes réseau disponibles. Consultez la matrice de prise en charge des hyperviseurs pour en savoir plus sur les cartes réseau et les hyperviseurs pris en charge.

Le déchargement basé sur la méthode à la volée logicielle prend en charge le protocole de tunnel GTP-U. Au sein d'un GTP-U avec le logiciel de session interne GTPU coordonné avec le temps universel, une fois que la session interne GTPU a terminé l'inspection de la couche 7, le paquet GTPU suivra le chemin de données de méthode à la volée logicielle du logiciel existant, contournera les opérations inutiles et profitera d'un cache FIB/MAC et s'exécutera jusqu'à la fin. Le pare-feu CN-Series prend en charge la fonctionnalité à la volée logicielle PAN-OS pour le déchargement du trafic spécifique GTP-U lors du déploiement du pare-feu CN-Series en tant que service Kubernetes CNF.

Déchargement de trafic spécifique GTP-U sur le pare-feu CN-Series

GTP comprend un plan de contrôle (GTP-C), un plan utilisateur (GTP-U) et un trafic de facturation (GTP' dérivé de GTP-C) transféré sur UDP/IP. Affichez les versions de PAN-OS par modèle qui prennent en charge GTP et les normes techniques 3GPP prises en charge par GTPv1-C, GTPv2-C et GTP-U. L'activation de la sécurité GTP sur les pare-feu Palo Alto Networks® vous permet de protéger l'infrastructure du réseau central mobile contre les paquets GTP mal formés, les attaques par denial-of-Service (déni de service – DoS) et les messages GTP hors état, et vous permet également de protéger les abonnés mobiles contre les paquets IP falsifiés et les attaques de surfacturation.

GTP-U est défini dans 3GPP TS 29.281. Il encapsule et achemine le trafic du plan utilisateur sur plusieurs interfaces de signalisation telles que S1, S5 et S8. Les messages GTP-U sont soit des plans utilisateur,

soit des messages de signalisation. Le numéro de port enregistré pour GTP-U est 2152. Pour plus d'informations, consultez Profil de protection GTP.

Le déchargement basé sur la méthode à la volée logicielle sur CN-Series prend également en charge les déchargements de trafic GTP-U. Vous pouvez désormais utiliser l'abonnement Intelligent Traffic Offload sur CN-Series en tant que mode Kubernetes CNF pour débloquer plus de performances et protéger les réseaux mobiles en tirant parti de la sécurité GTP. Pour chaque paquet GTP-U inspecté par CN-Series en mode Kubernetes CNF, une inspection complète de la couche 7 sera effectuée sur les sessions internes. Si le pare-feu détermine que les sessions internes de ce paquet GTP-U peuvent être déchargées, tous les paquets GTP-U suivants appartenant à cette session seront déchargés.

Voici les points importants à prendre en compte avant de configurer le déchargement basé sur la méthode à la volée logicielle sur un pare-feu CN-Series :

- Par défaut, les configurations ITO basées sur la méthode à la volée logicielle sont désactivées.
- Vous pouvez activer cette fonctionnalité uniquement à l'aide de bootstrap/CLI.
- Vous pouvez utiliser simultanément un ITO basé sur la méthode à la volée logicielle pour le trafic simple et un déchargement GTP-U au sein d'un ITO basé sur la méthode à la volée logicielle.
- Pour les mises à niveau vers la version actuelle avec ITO activé, activez le déchargement de session à l'aide de la post-mise à niveau CLI.

Dans CN-Series, seul CN-Series en tant que mode de déploiement Kubernetes CNF prend en charge l'ITO basé sur la méthode à la volée logicielle.

Activer les déchargements de session interne GTP-U sur le pare-feu CN-Series

Pour activer les déchargements de session interne GTP-U sur le pare-feu CN-Series, voici les conditions préalables à l'activation de la sécurité GTP ou de la sécurité 5G.

Vous devez modifier le fichier **`pan-cn-mgmt-configmap.yaml`** avec les modifications suivantes :

Dans le fichier `pan-cn-mgmt-configmap.yaml`, la valeur des paramètres `PAN_GTP_ENABLED, PAN_GTP_CUT_THRU et PAN_SW_CUT_THRU` doit être `true` (vrai) pour activer les déchargements de session interne GTP-U.

Voici un exemple de fichier `pan-cn-mgmt-configmap.yaml` mis à jour :

```
# Start MGMT pod with GTP enabled. Pour une fonctionnalité
 complète, vous devez également activer GTP # dans Panorama.
 PAN_GTP_ENABLED: "true" # Start MGMT pod with GTP SW cut Through
 enable. PAN_GTP_CUT_THRU: "true" # Start MGMT pod with SW cut
 Through enable. PAN_SW_CUT_THRU : "true"
```

