paloalto TECHDOCS

Introducción a CN-Series

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

August 25, 2023

Table of Contents

Cortafuegos CN-Series para Kubernetes

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Los cortafuegos nativos de contenedores de Palo Alto Networks (CN-Series) se integran de forma nativa en kubernetes (k8s) para proporcionar visibilidad de nivel 7 (L7) completa, segmentación a nivel de aplicación, seguridad DNS y protección frente a amenazas avanzadas para el tráfico que atraviesa zonas de confianza en la nube pública o entornos de centros de datos. Le permite aislar y proteger cargas de trabajo, pilas de aplicaciones y servicios, incluso cuando los contenedores individuales se amplían verticalmente, reducen verticalmente o entre hosts y aplican de manera coherente políticas de seguridad basadas en etiquetas de kubernetes.

La implementación de aplicaciones en un entorno kubernetes es dinámica y los siguientes equipos a menudo están involucrados en el ciclo de vida del contenedor:

- **Platform (PAAS) Admin (Administrador de plataforma (PAAS))**: administra los clústeres de Kubernetes y otros componentes de infraestructura en la nube pública y los centros de datos.
- **App Teams (Equipos de aplicaciones)**: implementan sus aplicaciones individuales en contenedores y otras aplicaciones en los espacios de nombres/proyectos de kubernetes proporcionados por el administrador de PAAS.
- **Security Admin (Administrador de seguridad)**: proporciona seguridad para toda la implementación, incluidos los clústeres de kubernetes y las aplicaciones en contenedores individuales.

En este escenario dinámico e de interacción con múltiples equipos, la gestión y supervisión de la seguridad representan un desafío. El CN-Series permite a su administrador de seguridad proporcionar seguridad para las aplicaciones en contenedores en una amplia gama de entornos, incluidos los k8 gestionados por el proveedor de la nube, como GKE, EKS, AKS, AliCloud ACK y los k8 gestionados por el cliente, como Openshift y los k8 nativos en la nube pública o en centros de datos locales. El CN-Series utiliza construcciones de Kubernetes y políticas basadas en metadatos para que los equipos puedan automatizar la implementación y aplicar de manera eficiente la política de seguridad para proporcionar protección de manera coherente frente a amenazas conocidas y desconocidas.

Proteja las cargas de trabajo de Kubernetes con el cortafuegos CN-series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Los cortafuegos CN-Series se implementan como dos conjuntos de pods: uno para el plano de gestión (CN-MGMT) y otro para el plano de datos del cortafuegos (CN-NGFW). El plano de datos del cortafuegos se ejecuta como un conjunto de daemons, lo que permite que un solo comando desde Kubernetes implemente cortafuegos en todos los nodos de un clúster de Kubernetes a la vez. El plano de gestión se ejecuta como un servicio de Kubernetes.

Los cortafuegos CN-Series se gestionan a través de la consola Panorama. Un complemento de Kubernetes dentro de Panorama proporciona información contextual sobre los contenedores en un entorno, y esto habilita de forma fluida políticas de seguridad de red basadas en contexto.

Por ejemplo, los espacios de nombres de Kubernetes se pueden utilizar para definir una fuente de tráfico en una política de cortafuegos. Puede implementar cortafuegos CN-Series en entornos de Kubernetes alojados localmente o en nubes públicas.

Los cortafuegos CN-series también se pueden implementar en ofertas de Kubernetes gestionadas en la nube, incluidos Google Kubernetes Engine (GKE®), Azure Kubernetes Service (AKS), Alibaba Cloud (ACK) y Amazon Elastic Kubernetes Service (EKS). También puede implementar a través de administradores de paquetes de Kubernetes, como Helm.

CN-Series ofrece protección frente a amenazas para el tráfico de entrada, saliente y de este a oeste entre las zonas de confianza (trust) de contenedores y otros tipos de cargas de trabajo, sin ralentizar la velocidad de desarrollo.

Implemente la serie CN-Series para visibilidad de capa 7 del tráfico de contenedores y haga cumplir las políticas de seguridad con perfiles de prevención frente a amenazas para proteger el tráfico permitido a través de los límites del espacio de nombres de Kubernetes, y compartir ese contexto con el hardware y los cortafuegos CN-Series, para garantizar un modelo de cumplimiento de políticas coherente en todo su entorno.

Evite la filtración de datos de entornos de Kubernetes:

Los cortafuegos CN-Series ofrecen una multitud de capacidades de seguridad para evitar la filtración de datos confidenciales de los entornos de Kubernetes. La inspección del contenido del tráfico, incluida la inspección del tráfico cifrado con TLS/SSL, garantiza que los paquetes que contienen cargas útiles maliciosas se identifiquen y remedien. El filtrado de URL bloquea las conexiones salientes a sitios web potencialmente maliciosos, incluidos repositorios de códigos maliciosos.

Evitar la propagación lateral de amenazas en los límites del espacio de nombres de Kubernetes:

Los límites de confianza entre aplicaciones son ubicaciones lógicas para aplicar políticas de segmentación que impidan el movimiento lateral de las amenazas. En muchos entornos de Kubernetes, el espacio de nombres de Kubernetes es el límite de confianza. Los cortafuegos CN-Series pueden aplicar políticas de prevención de amenazas entre espacios de nombres de Kubernetes, así como entre un espacio de nombres de Kubernetes y otros tipos de cargas de trabajo (por ejemplo, máquinas virtuales y servidores bare metal), para impedir que las amenazas se muevan entre sus aplicaciones nativas de la nube y su infraestructura heredada.

Conceptos clave de la serie CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

El cortafuegos CN-Series está diseñado para proporcionar las herramientas que necesita para proteger las aplicaciones en su entorno en contenedores. Para entender cómo encaja la CN-Series en una red en contenedores, es importante comprender algunos conceptos clave.

- **Clúster**: la base de su entorno en contenedores; todas sus aplicaciones en contenedores se ejecutan sobre un clúster.
- **Nodo**: dependiendo del clúster, un nodo puede ser una máquina virtual o física que contiene los servicios necesarios requeridos para los pods.
- **Pod**: la unidad informática desplegable más pequeña que usted puede implementar y gestionar en Kubernetes. El cortafuegos CN-Series se implementa en una arquitectura PAN-OS distribuida como dos pods: CN-MGMT y CN-NGFW. Consulte los Componentes básicos de la serie CN-series para obtener más información.
- **Espacio de nombres**: un espacio de nombres es un clúster virtual respaldado por un clúster físico. En un entorno con muchos usuarios repartidos en varios equipos y funciones, se puede usar un espacio de nombres para separarlos en un único clúster.
- **Interfaz de red de contenedores (CNI)**: un complemento que configura interfaces de red para contenedores. Además, el CNI elimina los recursos asignados utilizados para la creación de redes cuando se elimina un contenedor.
- **DaemonSet**: en una implementación de Kubernetes, un DaemonSet garantiza que algunos o todos los nodos ejecuten una copia de un pod en particular. Y a medida que se añaden nodos a un clúster de Kubernetes, se añade una copia del pod definido por DaemonSet a cada nuevo nodo. Al implementar el cortafuegos CN-Series como un DaemonSet, se implementa una copia del pod CN-NGFW en cada nodo (hasta 30 por par de CN-MGMT) del clúster.
- **Servicio de Kubernetes**:una abstracción que expone una aplicación que se ejecuta en un conjunto de pods como servicio de red. Al implementar la serie CN-Series como un servicio, usted define el número de pods de CN-NGFW implementados al configurar los archivos yaml.
- **Kuberenetes CNF**: la implementación de CN-series-as-a-kubernetes-CNF resuelve desafíos relacionados con el tráfico que usa Service Function Chaining (SFC) a través de entidades externas, como el enrutamiento nativo del proveedor de la nube, vRouters y conmutadores Top of Rack (TOR). El modo de implementación CN-series-as-a-kubernetes-CNF no afecta a los pods de aplicaciones.

- **Escalador automático horizontal de pods (HPA)**: amplía automáticamente el número de pods en una implementación, un conjunto de réplicas o un conjunto con estado en función de varias métricas, como la utilización de la CPU o la utilización de la sesión.

  HPA solo es compatible en el CN-Series como un servicio de Kubernetes.

- **HSF**: CN-Series Hyperscale Security Fabric 1.0 de Palo Alto Networks es un grupo de cortafuegos de nueva generación en contenedores que ofrece una solución de cortafuegos de nueva generación altamente escalable y resistente para proveedores de servicios móviles que implementan redes 5G.

Componentes básicos del CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

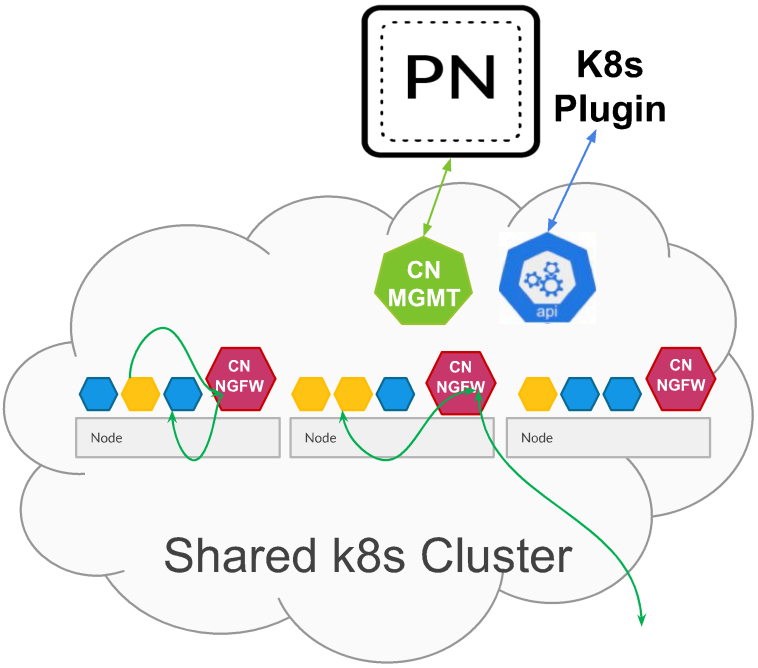
El cortafuegos CN-Series es el cortafuegos de próxima generación en contenedores que proporciona visibilidad y seguridad para sus cargas de trabajo de aplicaciones en contenedores en clústeres de Kubernetes. El cortafuegos CN-Series utiliza construcciones nativas de Kubernetes (K8s) y componentes de Palo Alto Networks para hacer esto posible.

Los componentes básicos para implementar el cortafuegos cn-series son:

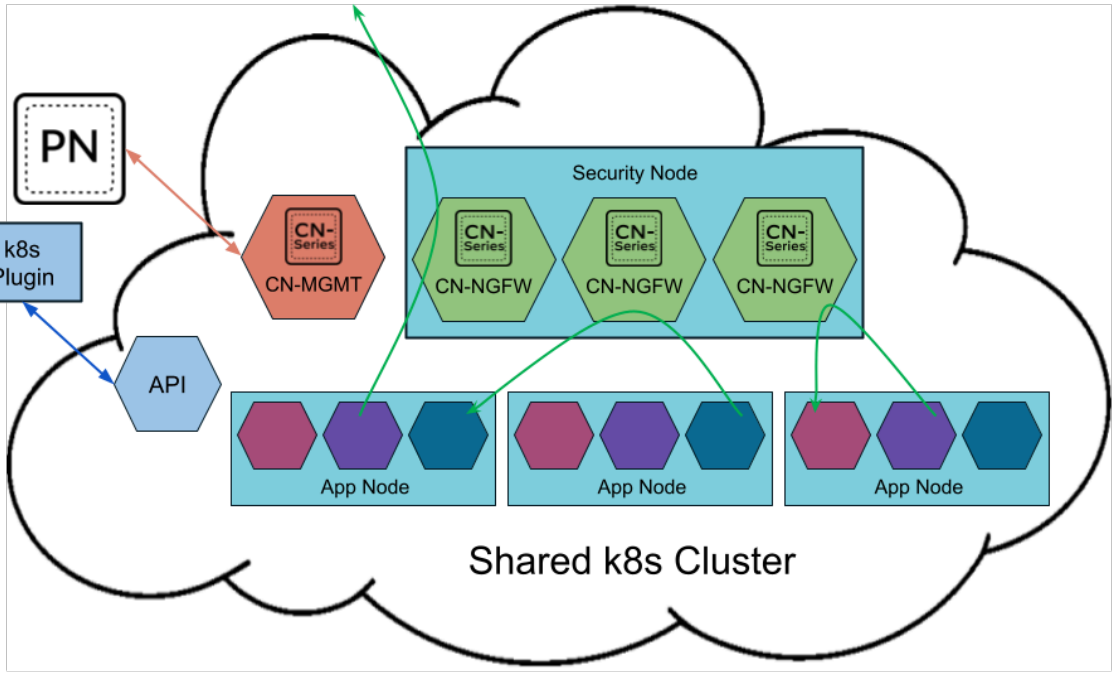
- **CN-Series Deployment Files (Archivos de implementación de CN-Series)**: para implementar la serie CN-Series en su entorno en contenedores, debe descargar e implementar los diversos archivos de implementación de la serie CN-Series.
  - PAN-CN-MGMT: el contenedor de inicialización genera certificados que se utilizan para asegurar la comunicación entre instancias de pods CN-MGMT y entre pods CN-MGMT y pods CN-NGFW.
  - PAN-CN-MGMT-CONFIGMAP
  - PAN-CN-MGMT-SECRET: permite que Panorama autentique los cortafuegos para que pueda añadir cada cortafuegos como dispositivo gestionado. La clave de autenticación de máquina virtual es necesaria durante todo el periodo de duración de la implementación. Sin una clave válida en la solicitud de conexión, el cortafuegos CN-Series no podrá registrarse con Panorama.
  - PAN-CN-NGFW
  - PAN-CN-NGFW-CONFIGMAP
  - PAN-CNI
  - PAN-CNI-CONFIGMAP
  - PAN-CNI-MULTUS
- **Arquitectura distribuida de PAN-OS con pods CN-MGMT y CN-NGFW**: el plano de administración (CN-MGMT) y el plano de datos (CN-NGFW) del cortafuegos en contenedor están separados para permitir una mejor protección en tiempo de ejecución para las aplicaciones y para admitir una huella más pequeña. CN-MGMT y CN-NGFW se implementan mediante imágenes de contenedor y archivos de manifiesto YAML con objetos ConfigMap.
- **CN-MGMT** se ejecuta como un StatefulSet para garantizar que tenga un volumen persistente y esté expuesto como un servicio de K8 que se puede descubrir mediante DNS en el entorno de Kubernetes. El CN-MGMT proporciona tolerancia a fallos y un único pod CN-MGMT puede gestionar los pods CN-NGFW existentes en caso de que un pod-MGMT se reinicie o falle.
- **CN-NGFW** se puede implementar como un DaemonSet o como un servicio de Kubernetes. Implementaciones de DaemonSet compatibles con entornos de Kubernetes con nodos más grandes,

pods que requieren baja latencia y/o requieren una alta capacidad de cortafuegos. La serie CN-series como servicio de Kubernetes es adecuada para entornos de Kubernetes con nodos más pequeños y/o requiere un cortafuegos más dinámico.

- Cuando se implementa **as a DaemonSet (como un DaemonSet)**, cada instancia del pod CN-NGFW puede proteger 30 pods de aplicaciones que se ejecuten en el mismo nodo. Esta arquitectura le permite colocar el pod CN-NGFW DaemonSet en cada nodo donde desee proteger las cargas de trabajo en un clúster, y un par de pods CN-MGMT pueden conectarse y gestionar hasta 30 pods CN-NGFW dentro de un clúster. Para obtener más información sobre los límites, consulte Rendimiento y ampliación de la serie CN-Series.



- Cuando se implementa **as a Kubernetes Service (como un servicio de Kubernetes)**, las instancias de CN-NGFW se pueden implementar en nodos de seguridad y el tráfico de pods de aplicaciones se redirige a una instancia CN-NGFW disponible para su inspección y aplicación.



- **Complemento de PAN-CNI para inserción de red**: el complemento PAN-CNI es responsable de la asignación de interfaces de red en cada pod, lo que permite la conectividad de red al pod CN-NGFW. Los archivos YAML que le permiten implementar CN-Series incluyen el PAN-CNI DaemonSet, que insertan el complemento PAN-CNI en la cadena del complemento CNI en cada nodo dentro del clúster.

El complemento lee la anotación en cada pod de aplicación a medida que aparece para determinar si habilitar la seguridad y redirigir el tráfico al pod CN-NGFW para su inspección a medida que accede y sale del pod.

- **Panorama para la gestión centralizada**: Panorama funciona como el centro para gestionar la configuración y las licencias de los cortafuegos en contenedores. También aloja el complemento de Kubernetes, que habilita la supervisión de los clústeres de Kubernetes y la gestión centralizada de políticas de seguridad. Puede utilizar un dispositivo Panorama físico o virtual e implementarlo en las instalaciones o en un entorno de nube pública. Panorama debe poder conectarse a la red de los pods del plano de administración del cortafuegos (CN-MGMT) para asegurarse de que puede autorizar a los cortafuegos (CN-NGFW) y enviar la configuración y las políticas utilizando plantillas y grupos de dispositivos de Panorama. Palo Alto Networks recomienda implementar Panorama en una configuración de HA.

  Necesita herramientas estándar de Kubernetes, como kubectl o Helm, para implementar y gestionar sus clústeres, aplicaciones y servicios de cortafuegos de Kubernetes. Panorama no está diseñado para ser un orquestador para la implementación y gestión de clústeres de Kubernetes. Los proveedores gestionados de Kubernetes proporcionan las plantillas para la gestión de clústeres. También puede utilizar las plantillas respaldadas por la comunidad para implementar CN-Series con Helm y Terraform.
- **Complemento de Kubernetes en Panorama**: el complemento de Kubernetes gestiona las licencias para el cortafuegos CN-Series. La licencia se basa en el número de núcleos que selecciona para asignar a los pods CN-NGFW. Cada pod CN-NGFW utiliza un token de licencia, y los tokens se gestionan localmente en Panorama después de activar el código de autenticación y recuperar el número especificado de tokens del servidor de licencias de Palo Alto Networks. A medida que cada CN-NGFW aparece en los nodos de Kubernetes, Panorama distribuye los tokens de licencia localmente.

  El complemento de Kubernetes en Panorama también le permite supervisar sus clústeres y aprovechar las etiquetas de Kubernetes que usa para organizar objetos de Kubernetes como pods, servicios, implementaciones y los atributos de identificación asociados, para que pueda crear reglas de política de seguridad relacionadas con el contexto. El complemento de Kubernetes se comunica con el servidor API y recupera metadatos en casi tiempo real para permitir la visibilidad de las aplicaciones que se ejecutan dentro del clúster. El complemento de Kubernetes recopila espacios de nombres, servicios y etiquetas de sus clústeres de Kubernetes para crear etiquetas para la asignación de dirección IP a etiqueta para los objetos asociados dentro del clúster que luego se pueden usar en las políticas de seguridad. Para obtener detalles, consulte Asignación de dirección IP a etiqueta de atributos de Kubernetes

  También recopila información sobre los puertos especificados en su aplicación YAML y crea objetos de servicio.

  Si bien estas etiquetas y objetos de servicio se comparten automáticamente con los pods CN-NGFW en cada clúster, también puede habilitar el uso compartido de etiquetas y objetos de servicio con cortafuegos basados en hardware o de la serie VM-Series. Las etiquetas pasan a estar disponibles como criterios de coincidencia en Grupos de direcciones dinámicas, que luego puede utilizar para proteger el tráfico entre pods o espacios de nombres, a un servicio expuesto a Internet o a conexiones salientes.

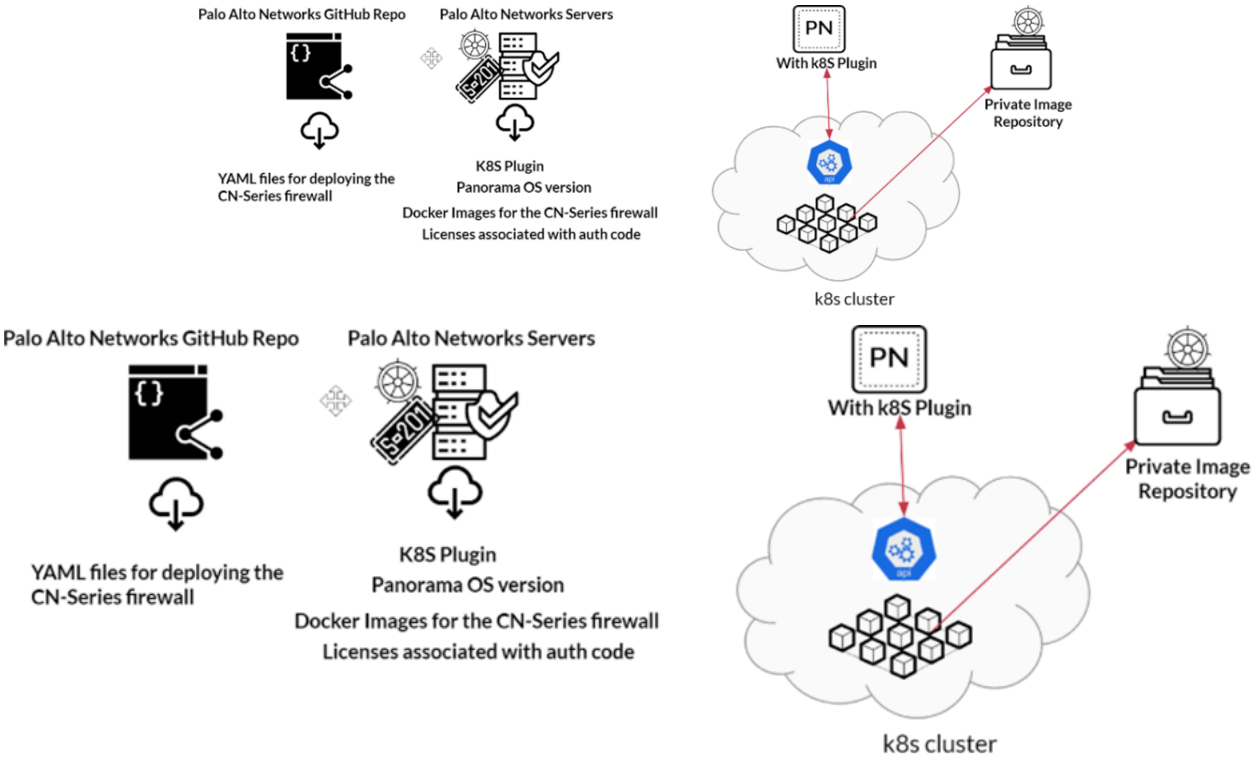
  Palo Alto Networks recomienda implementar Panorama en una configuración de HA para que el par de Panorama continúe recibiendo actualizaciones de direcciones IP en caso de fallos. Si implementa una instancia única de Panorama, en caso de fallo, el tráfico de los pods de aplicaciones existentes no se ve afectado y las políticas actuales se aplican en los pods CN-NGFW. Cuando un nuevo pod aparece, todas las reglas con la fuente "CUALQUIERA" coincidirán con este nuevo pod y el tráfico de este nuevo pod se permitirá o bloqueará dependiendo de las reglas de su política. Por ejemplo, si hay una regla de política antispyware para bloquear el acceso saliente desde *cualquier* fuente al mundo exterior,

esta regla se aplicará al nuevo pod y el perfil podrá proteger el tráfico. Si hay una regla *Denegar* predeterminada, entonces el tráfico de este nuevo pod se denegará.

Puede usar el complemento de Kubernetes para distribuir la asignación de dirección IP a etiqueta para pods, nodos, espacios de nombres y servicios implementados dentro del clúster de Kubernetes a cortafuegos físicos o VM-Series, incluso si no ha implementado cortafuegos CN-Series en ese grupo.

Componentes necesarios para proteger los clústeres de Kubernetes con el cortafuegos CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm



La siguiente es una lista de lo que necesita para la Implementación del cortafuegos CN-Series y proteger las aplicaciones implementadas dentro de los clústeres de Kubernetes.

- **Panorama**: un dispositivo virtual o basado en hardware que puede conectarse a los clústeres de Kubernetes donde se implementan las aplicaciones y los cortafuegos CN-Series. Se requiere Panorama para la gestión de licencias y la gestión de la configuración de los cortafuegos CN-Series. Para obtener más información, consulte Componentes básicos del CN-Series.
- **Kubernetes Plugin on Panorama (Complemento de Kubernetes en Panorama)**: debido a la tasa de cambio con las aplicaciones en contenedores, este complemento es necesario para la visibilidad de la

actividad del contenedor dentro de un clúster y para gestionar la asignación del token de licencia para el cortafuegos implementado en cada nodo dentro de un clúster.

El complemento de Kubernetes se conecta a los clústeres de Kubernetes mediante las credenciales de la cuenta de servicio. A partir de ahí, recupera etiquetas y atributos de recursos y crea etiquetas y objetos de servicio. Las etiquetas se pueden utilizar para crear grupos de direcciones dinámicas y hacer referencia a ellos en la política de seguridad para la aplicación del tráfico IP. También puede utilizar los objetos de servicio en la política de seguridad para permitir o denegar el tráfico según los puertos y las direcciones IP. Las etiquetas y los objetos de servicio le proporcionan visibilidad y control granular para la aplicación del tráfico dentro de su clúster de Kubernetes.

- **Docker Images (Imágenes de docker)**: para apoyar la arquitectura distribuida, el cortafuegos CN-Series tiene cuatro imágenes de docker que están disponibles en el Portal de Palo Alto Networks. Estas imágenes se publican como tres archivos tar comprimidos (formato tar.gz), y debe descomprimir estas imágenes y llevar a cabo un envío de docker a su registro de imágenes.

  Nota: Asegúrese de que las imágenes y las versiones de los archivos YAML sean compatibles. Los archivos comprimidos son:

  - **PanOS_cn-10.1.0.tgz**: este archivo incluye el plano de gestión del cortafuegos (CN-MGMT) y las imágenes del plano de datos del cortafuegos (CN-NGFW).

    Los nombres de las imágenes descomprimidas son, por ejemplo: `panos_cn_ngfw:10.1.0-b7` y `panos_cn_mgmt:10.1.0-b7`

    - **Pan_cn_mgmt_init-2.0.0.tgz**: este archivo incluye el contenedor de inicialización (CN-INIT) que contiene las utilidades necesarias para implementar el plano de administración en el cortafuegos. El contenedor de inicialización habilita la comunicación IPSec segura entre los pods CN-MGMT y CN-NFGW. El nombre de la imagen descomprimida es, por ejemplo: `pan_cn_mgmt_init:1.0.0-b1-c1`.
    - **Pan_cni-2.0.0.tgz**: este archivo incluye el complemento CNI que permite la conectividad entre CN-MGMT y CN-NFGW, y reconfigura las interfaces de red en los pods de aplicaciones para redirigir el tráfico al pod CN-NGFW en cada nodo. El nombre de la imagen descomprimida es, por ejemplo: `pan_cni:2.0.0`.

Los nombres de las imágenes enumerados anteriormente son ejemplos y cambiarán para reflejar la última versión. Puede encontrar las últimas imágenes en el Portal de Palo Alto Networks.

- **YAML Files (Archivos YAML)**: los archivos YAML que incluyen los campos obligatorios y las especificaciones de objeto para implementar los recursos en sus clústeres de Kubernetes y se publican en GitHub.

  Todos los archivos YAML necesarios, para un entorno compatible como Kubernetes nativo o GKE, se combinan y comprimen en una única carpeta para su comodidad.

  Los archivos YAML se implementan automáticamente a través de gráficos HELM, que es el método recomendado para implementar el cortafuegos CN-Series.

  - CN-MGMT tiene tres archivos YAML:`pan-cn-mgmt.yaml`, `pan-cn-mgmt-configmap.yaml`,`pan-cn-mgmt-secret.yaml`, `pan-cn-mgmt-slot-cr.yaml`, y `pan-cn-mgmt-slot-crd.yaml`.
  - CN-NGFW como un DaemonSet tiene dos archivos YAML: `pan-cn-ngfw.yaml` y `pan-cn-ngfw-configmap.yaml`. El CN-NGFW como servicio de Kubernetes tiene `pan-cn-ngfw-svc.yaml` además de los archivos mencionados anteriormente.
  - El complemento CNI tiene tres archivos YAML: `pan-cni-configmap.yaml` y `pan-cni.yaml` o `pan-cni-multus.yaml`.

    Si está implementando el CN-Series en entornos con Multus CNI que actúa como un *meta-plugin* y llama a otros complementos CNI, debe elegir `pan-cni.yaml` o `pan-cni-multus.yaml`.

    En una implementación de CN-Series en OpenShift, Multus está habilitado de forma predeterminada, pan-cni.yaml es adecuado. Mientras que, si va a implementar el CN-Series en un entorno donde se admite Multus CNI pero es opcional, como con entornos autogestionados (nativos), utilice pan-cni-multus.yaml en lugar de pan-cni.yaml.

    - *También hay un `pan-cni-serviceaccount.yaml` al que se hace referencia en la sección de creación de cuenta de servicio a continuación.*
    - *Para las implementaciones de OpenShift, hay un `pan-cni-net-attach-def.yaml` adicional.*
  - **Service Account Creation (Creación de cuenta de servicio)**: tres archivos YAML, `pan-mgmt-serviceaccount.yaml`, `pan-cni-serviceaccount.yaml` y `plugin-serviceaccount. yaml`.

    `pan-mgmt-serviceaccount.yaml` y `pan-cni-serviceaccount.yaml` son para que los pods CN-MGMT y CN-NGFW se autentiquen en el clúster.

    El archivo `plugin-serviceaccount.yaml` es para que el complemento de Kubernetes en Panorama se autentique en el clúster.
  - **Persistent volume YAML for Native Kubernetes deployments (YAML de volumen persistente para implementaciones nativas de Kubernetes)**: `pan-cn-pv-manual.yaml` y `pan-cn-pv-local.yaml`.

    El archivo `pan-cn-pv-manual.yaml` solo se proporciona para PoC con clústeres de un solo nodo. Palo Alto Networks recomienda encarecidamente el uso de volúmenes persistentes aprovisionados dinámicamente para almacenar la configuración y los registros de los pods CN-

MGMT a los que `pan-cn-mgmt.yaml` hace referencia. Asegúrese de configurar un volumen persistente dentro del clúster para ambos pods CN-MGMT.

- **License auth code (Código de autorización de licencia)**: el código de autorización le permite autorizar cada instancia del pod CN-NGFW implementado en cada nodo dentro de un clúster.

  El código de autenticación de licencia está vinculado al perfil de implementación de la serie CN-Series que creó en el CSP de Palo Alto Network. Además, este habilita cualquier suscripción de seguridad que haya seleccionado al crear su perfil de implementación.

Recursos adicionales de la serie CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Puede utilizar los siguientes recursos para obtener más información sobre el cortafuegos CN-Series y cómo puede ayudarle a proteger su red de contenedores.

- Cortafuegos CN-Series: vea estos videos para obtener información sobre el cortafuegos CN-Series.
- El por qué, el qué y el cómo de la serie CN-Series: una serie de blogs de tres partes (con vídeos integrados) en la comunidad en directo de Palo Alto Networks que describe el por qué, el qué y el cómo de los cortafuegos CN-series.
- Palo Alto Network Qwiklabs: utilice palo Alto Networks Qwiklab para realizar un ejercicio de laboratorio y probar el cortafuegos CN-Series en AWS o GCP.
- Notas de la versión del complemento de Panorama para Kubernetes:lea las notas de la versión para conocer las características y mejoras introducidas en la última versión del complemento de Panorama para Kubernetes.
- Notas de la versión de PAN-OS: consulte las notas de la versión de PAN-OS para obtener más información sobre las características y mejoras de la serie CN-Series introducidas en la última versión de PAN-OS.
- Guía del administrador de Panorama: Panorama es la interfaz que se utiliza para conectarse con su entorno de Kubernetes, administrar los cortafuegos CN-Series implementados y definir la política de seguridad.

Requisitos del sistema de la serie CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Esta sección cubre los requisitos del sistema recomendados para implementar el cortafuegos CN-series en el clúster Kubernetes y en un entorno local.

Esta sección cubre lo siguiente:

- Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes
- Requisitos del sistema de la serie CN-Series para implementaciones de Kubernetes locales
- Rendimiento y ampliación de la serie CN-Series
- Implementación de CN-Series: entornos compatibles

Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Estos son los requisitos de sistema recomendados para implementar el cortafuegos CN-Series en sus múltiples modos admitidos.

- PAN-OS 10.1
- PAN-OS 10.2 y posterior

PAN-OS 10.1

La siguiente tabla muestra los requisitos del sistema para el clúster en el que se implementa el cortafuegos CN-Series. Estos valores son pautas generales para la CPU, la memoria y el almacenamiento en disco; la cantidad de recursos que implemente puede variar según sus necesidades.

La serie CN-Series mediana no está disponible para la serie CN-Series como Daemonset.

Recurso	CN-MGMT-pequeño	CN-NGFW-pequeño	CN-MGMT-mediano	CN-NGFW-mediano	CN-MGMT-grande	CN-NGFW-grande
Memoria (mínimo)	3 GB	• 2 GB (Daemonset) • 2,5 GB (servicio K8s)	3 GB	6 GB	4 GB	48 GB
CPU mín.	2 (recomendado)	2 (recomendado)	2 (recomendado)	4 (recomendado)	4 (recomendado)	12 (recomendado)
CPU máx.	n/c	31	n/c	31	n/c	31
Disco	50 GB	n/c	50 GB	n/c	50 GB	n/c

PAN-OS 10.2 y posterior

La seguridad nativa de 5G (5G-Native Security) es compatible exclusivamente con Daemonset y el modo CNF para Kubernetes.

Las combinaciones de memoria y núcleo para CN-MGMT y CN-NGFW se aplican a Pequeño, Mediano y Grande respectivamente. La combinación de Pequeño, Mediano y Grande perteneciente a CN-MGMT se asigna directamente con el respectivo CN-NGFW.

Table 1: Matriz de capacidad y sistema de CN-Series recomendados

Modo CN	Recurso	Pequeño	Intermedia	Intermedia	Intermedia	Grande	Grande
DaemonSet	Memoria CN-MGMT mínima	3 G	3 G	4 G	4 G	16 G	16 G
	Memoria CN-NGFW mínima	2 G	6,5 G	16 G	32 G	48 G	56 G
	Núcleos CN-MGMT recomendados	2	2	2	4	8	12
	Número máximo de núcleos de CN-NGFW	2	4	8	16	31	47
	Disco	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi
	Tamaño de Hugepage de DPDK	n/c	n/c	n/c	n/c	n/c	n/c
Servicio Kubernetes	Memoria CN-MGMT mínima	3 G	3 G	4 G	4 G	16 G	16 G
	Memoria CN-NGFW mínima	4 G	6,5 G	16 G	32 G	48 G	56 G
	Núcleos CN-	2	2	2	4	8	12

Modo CN	Recurso	Pequeño	Intermedia	Intermedia	Intermedia	Grande	Grande
	MGMT recomendados						
	Número máximo de núcleos de CN-NGFW	2	4	8	16	31	47
	Disco	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi
	Tamaño de Hugepage de DPDK	n/c	n/c	n/c	n/c	n/c	n/c
CNF de Kubernetes	Memoria CN-MGMT mínima	3 G	3 G	4 G	4 G	16 G	16 G
	Memoria CN-NGFW mínima	2 G	6,5 G	16 G	32 G	48 G	56 G
	Núcleos CN-MGMT recomendados	2	2	2	4	8	12
	Número máximo de núcleos de CN-NGFW	2	4	8	16	31	47
	Disco	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi	52 Gi
	Tamaño de Hugepage de DPDK	1 G	1 G	2 G	2 G	4 G	4 G

Requisitos del sistema de la serie CN-Series para implementaciones de Kubernetes locales

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Revise los siguientes requisitos previos para sus implementaciones locales:

- Asegúrese de que las imágenes del contenedor sean accesibles para todos los nodos del clúster de Kubernetes.
- Configure un volumen persistente dentro del clúster para ambos pods CN-MGMT. Dado que los pods CN-MGMT que gestionan activamente los pods CN-NGFW, están implementados como un StateSet, ambas instancias deben tener acceso al volumen persistente.

Para obtener el acceso SSH para su clúster de Rancher, debe asegurarse de que el contenido del archivo kubeconfig se copie en la ubicación `/.kube/config`*, y a continuación, solo usted puede ejecutar comandos kubectl para su clúster.*

Además, deberá asegurarse de que la herramienta de línea de comandos de Kubernetes, kubectl, esté instalada en su sistema. Para obtener más información, consulte Instalar herramientas.

Para los CN-Series con capacidad para Rancher, instale Docker en el nodo maestro Ubuntu 18.0.4 LTS VM con 8 vCPU y 32 G de memoria con un disco mínimo de 200 GB. Para obtener más información, consulte Instalar Docker en Ubuntu 18.04.

Para Ubuntu 18.0.4, el kernel en las máquinas se debe actualizar al kernel más reciente usando el siguiente comando:

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

Rendimiento y ampliación de la serie CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Los números de escalado que los diferentes componentes han requerido para Proteja las cargas de trabajo de Kubernetes con el cortafuegos CN-series se enumeran en las siguientes secciones:

- Escalado compatible con los componentes de la serie CN-Series
- Escalado compatible con el complemento de Kubernetes en Panorama
- Métricas clave de rendimiento de la serie CN-Series

Escalado compatible con los componentes de la serie CN-Series

Para obtener información sobre las definiciones de CPU, memoria y almacenamiento en disco de la serie CN-Series, consulte Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes.

La siguiente tabla separa algunos datos por tamaños de la CN-Series: pequeño, mediano y grande. Estos tamaños de la serie CN-Series tienen los siguientes valores de memoria:

- **CN-Series pequeño**: mínimo 2.5G CN-NGFW y 3G CN-MGMT
- **CN-Series mediano**: mínimo 6G CN-NGFW y 3G CN-MGMT
- **CN-Series grande**: mínimo 42G CN-NGFW y 4G CN-MGMT

Atributo	Escalado de la serie CN-Series (DaemonSet)	Escalado de la serie CN-Series (servicio K8s)	Escala de la CN-Series (K8s-CNF)
Pares de CN-MGMT máximos por clúster de K8s	4 pares de CN-MGMT en modo HA activo/pasivo	4 pares de CN-MGMT en modo HA activo/pasivo	4 pares de CN-MGMT en modo HA activo/pasivo
Número máximo de pods CN-NGFW por cada par de CN-MGMT	30	30	30
Pods de Kubernetes protegidos por CN-	30 (PAN-OS 10.1.8 o versión anterior)	n/c	n/c

Atributo	Escalado de la serie CN-Series (DaemonSet)	Escalado de la serie CN-Series (servicio K8s)	Escala de la CN-Series (K8s-CNF)
NGFW (por cada nodo de K8s)	125 (PAN-OS 10.1.9 y versión superior con k8s 2.0.2 instalado)	*Este modo de implementación es independiente del número de pods de aplicación en un nodo K8s.*	*Este modo de implementación es independiente del número de pods de aplicación en un nodo K8s.*
Número máximo de sesiones TCP/IP por CN-NGFW	CN-Series pequeño: 20.000 CN-Series mediano: 819.200 CN-Series grande: 10.000.000	CN-Series pequeño: 250.000 CN-Series mediano: 819.200 CN-Series grande: 10.000.000	CN-Series pequeño: 250.000 CN-Series mediano: 819.200 CN-Series grande: 10.000.000
Máximo de direcciones IP de grupos de direcciones dinámicas* por par de CN-MGMT	CN-Series pequeño: 2500 (PAN-OS 10.0.6 e inferior) 10.000 (PAN-OS 10.0.7 y superior)	CN-Series pequeño: 2500 (PAN-OS 10.0.6 e inferior) 10.000 (PAN-OS 10.0.7 y superior) CN-Series mediano: 200.000 CN-Series grande: 300.000	CN-Series pequeño: 2500 (PAN-OS 10.0.6 e inferior) 10.000 (PAN-OS 10.0.7 y superior) CN-Series mediano: 200.000 CN-Series grande: 300.000
Etiquetas por dirección IP* por par de CN-MGMT	32	32	32
Número máximo de zonas de seguridad	CN-Series pequeño: 2 CN-Series mediano: 40 CN-Series grande: 200	CN-Series pequeño: 2 CN-Series mediano: 40 CN-Series grande: 200	CN-Series pequeño: 2 CN-Series mediano: 40 CN-Series grande: 200
Perfiles de seguridad	CN-Series pequeño: 38 CN-Series mediano: 375	CN-Series pequeño: 375	CN-Series pequeño: 375 CN-Series mediano: 375

Atributo	Escalado de la serie CN-Series (DaemonSet)	Escalado de la serie CN-Series (servicio K8s)	Escala de la CN-Series (K8s-CNF)
	CN-Series grande: 750	CN-Series mediano: 375 CN-Series grande: 750	CN-Series grande: 750
Núm, máx. de interfaces	**Para PAN-OS 10.1.8 o una versión anterior:** CN-Series pequeño: 30 CN-Series mediano: 30 CN-Series grande: 30 **Para PAN-OS 10.1.9 y versiones superiores con k8s 2.0.2 instalado:** CN-Series pequeño: 250 CN-Series mediano: 250 CN-Series grande: 250	CN-Series pequeño: 2 CN-Series mediano: 2 CN-Series grande: 2	CN-Series pequeño: 60 CN-Series mediano: 60 CN-Series grande: 60

*Consulte la Herramienta de comparación de cortafuegos.

Políticas	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Reglas de seguridad	1500	10.000	20.000
Programaciones de reglas de seguridad	256	256	256
Reglas NAT *Las reglas NAT son compatibles con el modo CNF.*	n/c	n/c	n/c

Políticas	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Reglas de descifrado	1000	1000	2000
Reglas de anulación de aplicación	1000	1000	2000
reglas de inspección del contenido de túnel	100	500	2000
Reglas SD-WAN	n/c	n/c	n/c
Reglas de reenvío basado en políticas *Las reglas de reenvío basadas en políticas son compatibles con el modo CNF.*	n/c	n/c	n/c
Reglas del portal cautivo	n/c	n/c	n/c
Reglas de protección contra ataques por denegación de servicio	• 100 (DaemonSet) • 1000 (Servicio K8s)	1000	1000

Objetos (direcciones y servicios)	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Objetos de dirección	10.000	10.000	40.000
Grupos de direcciones	1000	1000	4000
Miembros por grupo de direcciones	2500	2500	2500

Objetos (direcciones y servicios)	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Objetos de servicio	2000	2000	5000
Grupos de servicios	500	500	500
Miembros por grupos de servicios	500	500	500
Objetos de dirección de FQDN	2000	2000	2000
Núm. máximo de direcciones IP del grupo de direcciones dinámicas	2500	200.000	300.000
Etiquetas por dirección IP	32	32	32

App-ID	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Firmas de App-ID personalizadas	6000	6000	6000
App-ID personalizados compartidos	512	512	512
App-ID personalizados (específicos del sistema virtual)	6416	6416	6416

Descifrado SSL	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Máximo de certificados de entrada SSL	1000	1000	1000

Descifrado SSL	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Caché de certificados SSL (proxy de reenvío)	128	2000	8000
Núm. más. de sesiones de descifrado simultáneas	• 1024 (DaemonSet) • 6400 (Servicio K8s)	15 000	100 000
Espejo de puerto SSL	No	No	No
Intermediario de descifrado SSL	No	No	No
Compatible con HSM	No	No	No

URL Filtering	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Núm. total de entradas para la lista de permitidos, la lista de bloqueo y las categorías personalizadas	25.000	25.000	100 000
Núm. máx. de categorías personalizadas	• 500 (DaemonSet) • 2849 (Servicio K8s)	2849	2849
Tamaño de la caché del plano de datos para el filtrado de URL	• 5000 (DaemonSet) • 90.000 (Servicio K8s)	90.000 (+)	250.000
Tamaño de la caché dinámica del plano de administración	100 000	100 000	600.000

EDL	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número máximo de listas personalizadas	30	30	30
Número máximo de IP por sistema	50.000	50.000	50.000
Número máximo de dominios DNS por sistema	50.000	500 000	2.000.000
Número máximo de URL por sistema	50.000	100 000	100 000
Intervalo de comprobación más corto (minutos)	5	5	5

Asignaciones de direcciones	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Servidores DHCP	3	10	125
Agentes de retransmisión de DHCP	No	No	No
Número máximo de direcciones asignadas	64.000	64.000	64.000

Interfaces	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número máx. de interfaces (lógicas y físicas)	• 60 (DaemonSet) • 2 (Servicio K8s) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (Servicio K8s) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (Servicio K8s) • 2 (K8s-CNF)
Gestión: fuera de banda	n/c	n/c	n/c

Interfaces	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Gestión: alta disponibilidad 10/100/1000	n/c	n/c	n/c
Gestión: alta disponibilidad 40G	n/c	n/c	n/c
Gestión: alta disponibilidad 10G	n/c	n/c	n/c
Tráfico: 10/100/1000	n/c	n/c	n/c
Tráfico: 100/1000/10000	n/c	n/c	n/c
Tráfico: 1G SFP	n/c	n/c	n/c
Tráfico: 10G SFP+	n/c	n/c	n/c
Tráfico - 40/100G QSFP +/QSFP28	n/c	n/c	n/c
Etiquetas 802.1q por dispositivo	n/c	n/c	n/c
Etiquetas 802.1q por interfaz física	n/c	n/c	n/c
Número máx. de interfaces agregadas	n/c	n/c	n/c
Número máx. de interfaces virtuales SD-WAN	n/c	n/c	n/c

NAT	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Capacidad total de reglas NAT	n/c	n/c	n/c

NAT	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número máx. de reglas NAT (estáticas)	n/c	n/c	n/c
Número máx. de reglas NAT (DIP)	n/c	n/c	n/c
Número máx. de reglas NAT (DIPP)	n/c	n/c	n/c
Número máx. de IP traducidas (DIP)	n/c	n/c	n/c
Número máx. de IP traducidas (DIPP)	n/c	n/c	n/c
Sobresuscripción predeterminada del grupo DIPP	n/c	n/c	n/c

User-ID	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Asignaciones de IP-User (plano de administración)	n/c	n/c	n/c
Asignaciones de IP-User (plano de datos)	n/c	n/c	n/c
Grupos activos y únicos utilizados en la política	n/c	n/c	n/c
Número de agentes de User-ID	n/c	n/c	n/c
Servidores supervisados para User-ID	n/c	n/c	n/c
Agentes de Terminal Server	n/c	n/c	n/c

User-ID	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Etiquetas por usuario	n/c	n/c	n/c

Enrutamiento	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Tamaño de la tabla de reenvío de IPv4	n/c	n/c	n/c
Tamaño de la tabla de reenvío de IPv6	n/c	n/c	n/c
Tamaño de la tabla de reenvío total del sistema	n/c	n/c	n/c
Número máx. de pares de enrutamiento (dependiente del protocolo)	n/c	n/c	n/c
Entradas estáticas: Proxy DNS	n/c	n/c	n/c
Sesiones de detección de reenvío bidireccional (BFD)	n/c	n/c	n/c

Reenvío de L2	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Tamaño de la tabla ARP por dispositivo	n/c	n/c	n/c
Tamaño de la tabla de vecinos de IPv6	n/c	n/c	n/c
Tamaño de la tabla de MAC por dispositivo	n/c	n/c	n/c

Reenvío de L2	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número máx. de entradas ARP por dominio de difusión	n/c	n/c	n/c
Número máx. de entradas MAC por dominio de difusión	n/c	n/c	n/c

QoS	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número de directivas de QoS	n/c	n/c	n/c
Interfaces físicas compatibles con QoS	n/c	n/c	n/c
Nodos de texto no cifrado por interfaz física	n/c	n/c	n/c
Marcado DSCP por política	n/c	n/c	n/c
Subinterfaces compatibles	n/c	n/c	n/c

IPSec VPN	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Número máx. de pares de IKE	n/c	n/c	n/c
Sitio a sitio (con ID de proxy)	n/c	n/c	n/c
Túneles SD-WAN IPSec	n/c	n/c	n/c

GlobalProtect	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
VPN de cliente de GlobalProtect Número máx. de túneles (SSL, IPSec, IKE con XAUTH)	n/c	n/c	n/c
VPN sin cliente de GlobalProtect Número máx. de túneles SSL	n/c	n/c	n/c

Multidifusión	CN-Series pequeño (Mín. 2.5G CN-NGFW y Mín. 3G CN-MGMT)	CN-Series mediano (Mín. 6G CN-NGFW y Mín. 2G CN-MGMT)	CN-Series grande (Mín. 42G CN-NGFW y Mín. 4G CN-MGMT)
Replicación (interfaces de salida)	n/c	n/c	n/c
Rutas	n/c	n/c	n/c

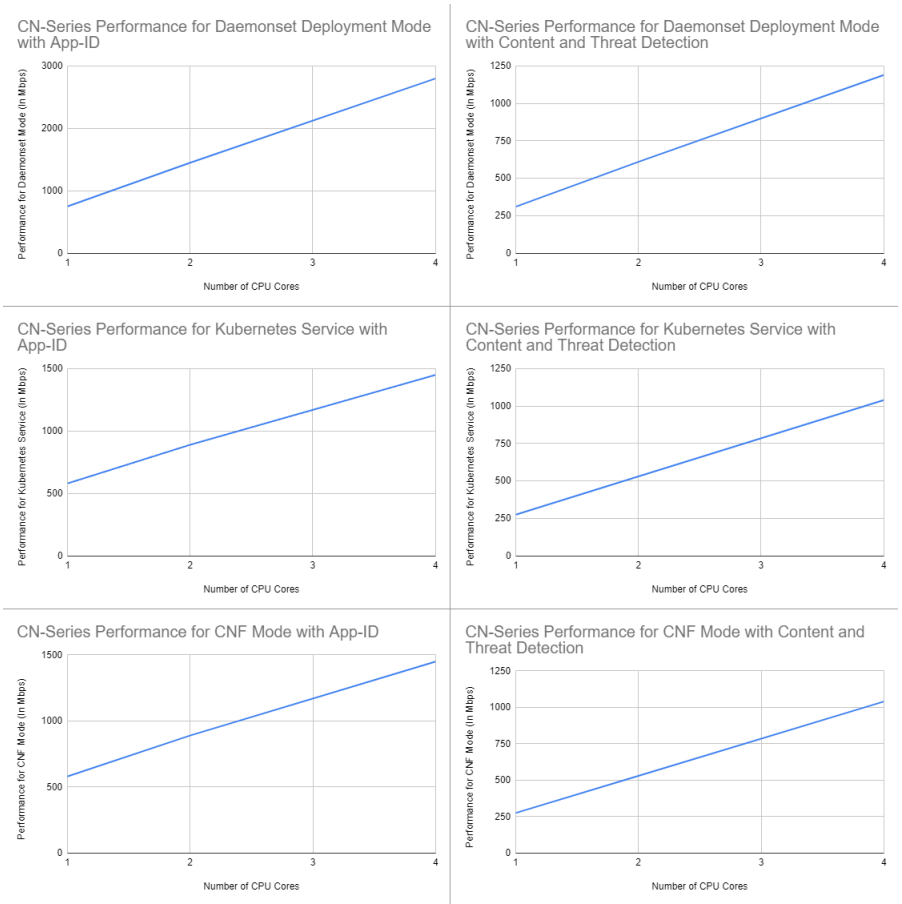
Escalado compatible con el complemento de Kubernetes en Panorama

Atributo	Escalado de complementos de Kubernetes
Número máximo de clústeres en un complemento de panorama de K8s	32 (en todos los entornos compatibles, como K8 nativos, AKS, EKS, GKE)

Métricas clave de rendimiento de la serie CN-Series

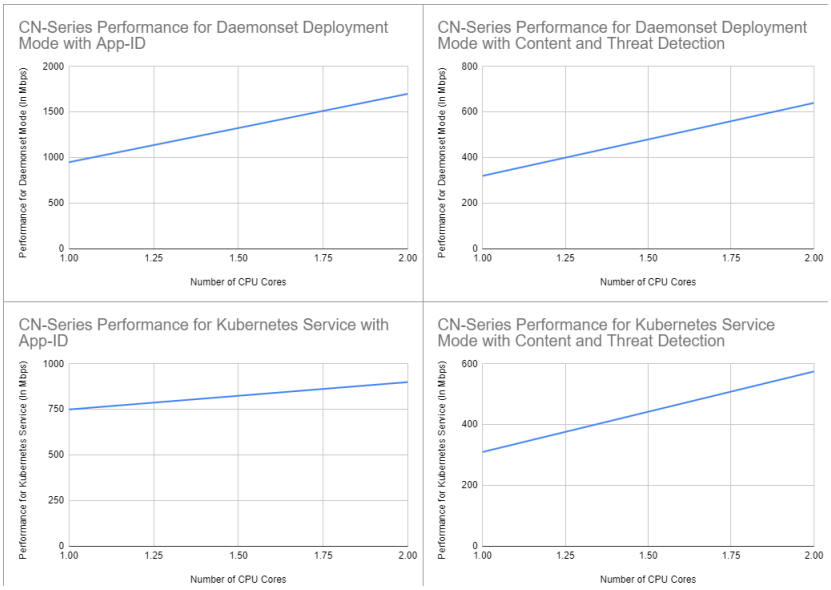
CN-Series en EKS en AWS				
	Núcleos de CPU	CN-Series como un DaemonSet (MMAP)	CN-Series como un servicio de Kubernetes (MMAP)	CN-Series como CNF de Kubernetes (MMAP)
App-ID	1	750 Mbps	580 Mbps	580 Mbps

CN-Series en EKS en AWS				
	Núcleos de CPU	**CN-Series como un DaemonSet (MMAP)**	**CN-Series como un servicio de Kubernetes (MMAP)**	**CN-Series como CNF de Kubernetes (MMAP)**
Detección de contenido y amenazas	1	310 Mbps	275 Mbps	275 Mbps
App-ID	2	1,45 Gbps	890 Mbps	890 Mbps
Detección de contenido y amenazas	2	610 Mbps	530 Mbps	530 Mbps
App-ID	4	2,8 Gbps	1,45 Gbps	1,45 Gbps
Detección de contenido y amenazas	4	1,19 Gbps	1,04 Gbps	1,04 Gbps



CN-Series en Google Cloud GKE (habilitado para XDP)			
	Núcleos de CPU	**CN-Series como un DaemonSet**	**CN-Series como un servicio de Kubernetes**
App-ID	1	950 Mbps	750 Mbps
Detección de contenido y amenazas	1	320 Mbps	310 Mbps
App-ID	2	1,7 Gbps	900 Mbps
Detección de contenido y amenazas	2	640 Mbps	575 Mbps

Las pruebas de la información de la siguiente tabla se realizaron en Google Kubernetes Engine (GKE) con tráfico dirigido entre nodos y entre pods en el mismo nodo en el mismo clúster



Función/Atributo	CN-Series pequeño	CN-Series mediano	CN-Series grande
Rendimiento del cortafuegos (App-ID habilitado) por vCPU de CN-NGFW	500 Mbps	500 Mbps	500 Mbps
Rendimiento de prevención de amenazas por vCPU de CN-NGFW	250 Mbps	250 Mbps	250 Mbps
Núm. máx. de sesiones	• 20.000 (DaemonSet)	819.200	10.000.000

Función/Atributo	CN-Series pequeño	CN-Series mediano	CN-Series grande
	• 250.000 (Servicio K8s) • 250.000 (K8s-CNF)		
Rendimiento de VPN IPSec por vCPU de CN-NGFW	n/c	n/c	n/c
Connections per Second (Conexiones por segundo)	n/c	n/c	n/c

Implementación de CN-Series: entornos compatibles

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la serie CN-Series con gráfico de Helm

Este capítulo proporciona información sobre la compatibilidad y los requisitos de versión del cortafuegos 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

Puede implementar el cortafuegos CN-Series en los siguientes entornos:

Producto	Versión
Tiempo de ejecución del contenedor	Docker CRI-O Containerd
Versión de Kubernetes	1.17 a 1.27
Kubernetes gestionado por el proveedor de la nube	• AWS EKS (1.17 a 1.27 para CN-Series como un daemonset demonio y CN-Series como un modo de servicio de implementación.) • EKS en AWS Outpost (1.17 a 1.25) *CN-Series para EKS en AWS Outpost no es compatible con SR-IOV ni Multus.*

Producto	Versión
	• Azure AKS (1.17 a 1.27)  *En Azure AKS, PAN-OS 10.1.10h1 es la versión mínima necesaria compatible con kubernetes 1.25 y superiores.* • AliCloud ACK (1.26) • GCP GKE (1.17 a 1.27)  *Incluye GKE Dataplane V2.*
Kubernetes gestionado por el cliente	En la nube pública o en el centro de datos local. Asegúrese de que la versión de Kubernetes, los tipos de CNI y las versiones de Host VM OS sean según se enumeran en esta tabla. VMware TKG+ versión 1.1.2 • Plataforma de infraestructura: vSphere 7.0 • SO de VM de host de Kubernetes—Photon OS
VM de host de Kubernetes	Sistema operativo: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL / Centos 7.3 y posterior • CoreOS 21XX, 22XX • SO optimizado para contenedores
	Versión del kernel de Linux: • 4.18 o posterior (solo modo de servicio K8s) • 5.4 o posterior necesario para habilitar el modo AF_XDP. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.
	Filtro de red del kernel de Linux: Iptables
Complementos CNI	CNI Spec 0.3 y posterior: • AWS-VPC • Azure • Calico

Producto	Versión

	• Flannel
	• Weave
	• Para AliCloud, Terway
	• Para Openshift, OpenshiftSDN
	• Lo siguiente se admite en el cortafuegos CN-Series como un DaemonSet.
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	**CN-Series como un DaemonSet:** 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13 **CN-Series como servicio K8s:** (PAN-OS 10.1.2 y posterior) 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13 *PAN-OS 10.1.10h1 es la versión mínima requerida compatible con 4.12 y superiores.*

Revise también los Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes, antes de implementar el cortafuegos CN-series.

PAN-OS 10.2

Puede implementar el cortafuegos CN-Series en los siguientes entornos:

Producto	Versión
Tiempo de ejecución del contenedor	Docker CRI-O Containerd
Versión de Kubernetes	1.17 a 1.27
Kubernetes gestionado por el proveedor de la nube	• AWS EKS (1.17 a 1.27 para CN-Series como un daemonset demonio y CN-Series como un modo de servicio de implementación.)

Producto	Versión
	• AWS EKS (1.17 a 1.22 para la CN-Series como modo de implementación CNF). • EKS en AWS Outpost (1.17 a 1.22) *CN-Series para EKS en AWS Outpost no es compatible con SR-IOV ni Multus.* • Azure AKS (1.17 a 1.28) *En Azure AKS, PAN-OS 10.2.4h3 es la versión mínima necesaria compatible con kubernetes 1.25 y superiores.* • GCP GKE (1.17 a 1.27) *En GCP GKE, PAN-OS 10.2.4h3 es la versión mínima requerida compatible con kubernetes 1.25 y superiores.* *Incluye GKE Dataplane V2.* • Google Anthos 1.12.3 • OCI OKE (1.23)
Kubernetes gestionado por el cliente	En la nube pública o en el centro de datos local. Asegúrese de que la versión de Kubernetes, los tipos de CNI y las versiones de Host VM OS sean según se enumeran en esta tabla. VMware TKG+ versión 1.1.2 • Plataforma de infraestructura: vSphere 7.0 • SO de VM de host de Kubernetes—Photon OS
VM de host de Kubernetes	Sistema operativo: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL / Centos 7.3 y posterior • CoreOS 21XX, 22XX • SO optimizado para contenedores
	Versión del kernel de Linux:

Producto	Versión
	• 4.18 o posterior (solo modo de servicio K8s) • 5.4 o posterior necesario para habilitar el modo AF_XDP. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.
	Filtro de red del kernel de Linux: Iptables

Complementos CNI	CNI Spec 0.3 y posterior:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Para Openshift, OpenshiftSDN, OVN Kubernetes
	• Lo siguiente se admite en el cortafuegos CN-Series como un DaemonSet.
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• Versiones 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13 *OpenShift 4.7 está clasificado en la serie CN-Series como DaemonSet únicamente.* • OpenShift en AWS *PAN-OS 10.2.4h3 es la versión mínima necesaria compatible con la versión 4.12 y superiores.*

Revise también los Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes, antes de implementar el cortafuegos CN-series.

PAN-OS 11.0

Puede implementar el cortafuegos CN-Series en los siguientes entornos:

Producto	Versión
Tiempo de ejecución del contenedor	Docker CRI-O Containerd
Versión de Kubernetes	1.17 a 1.27
Kubernetes gestionado por el proveedor de la nube	• AWS EKS (1.17 a 1.27 para CN-Series como un daemonset demonio y CN-Series como un modo de servicio de implementación.) • AWS EKS (1.17 a 1.22 para la CN-Series como modo de implementación CNF). • EKS en AWS Outpost (1.17 a 1.25) *CN-Series para EKS en AWS Outpost no es compatible con SR-IOV ni Multus.* • Azure AKS (1.17 a 1.27) *En Azure AKS, PAN-OS 11.0.2 es la versión mínima necesaria compatible con kubernetes 1.25 y superiores.* • GCP GKE (1.17 a 1.27) *Incluye GKE Dataplane V2.* • OCI OKE (1.23)
Kubernetes gestionado por el cliente	En la nube pública o en el centro de datos local. Asegúrese de que la versión de Kubernetes, los tipos de CNI y las versiones de Host VM OS sean según se enumeran en esta tabla. VMware TKG+ versión 1.1.2 • Plataforma de infraestructura: vSphere 7.0 • SO de VM de host de Kubernetes—Photon OS
VM de host de Kubernetes	Sistema operativo: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL / Centos 7.3 y posterior

Producto	Versión
	• CoreOS 21XX, 22XX • SO optimizado para contenedores
	Versión del kernel de Linux: • 4.18 o posterior (solo modo de servicio K8s) • 5.4 o posterior necesario para habilitar el modo AF_XDP. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.
	Filtro de red del kernel de Linux: Iptables

Complementos CNI	CNI Spec 0.3 y posterior:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Para Openshift, OpenshiftSDN, OVN Kubernetes
	• Lo siguiente se admite en el cortafuegos CN-Series como un DaemonSet.
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• Versiones 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13. *OpenShift 4.7 está clasificado en la serie CN-Series como DaemonSet únicamente.* *PAN-OS 11.0.2 es la versión mínima requerida compatible con 4.12 y superior.* • OpenShift en AWS

Revise también los Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes, antes de implementar el cortafuegos CN-series.

PAN-OS 11.1

Puede implementar el cortafuegos CN-Series en los siguientes entornos:

Producto	Versión
Tiempo de ejecución del contenedor	Docker CRI-O Containerd
Versión de Kubernetes	1.17 a 1.27
Kubernetes gestionado por el proveedor de la nube	• AWS EKS (1.17 a 1.27 para CN-Series como un daemonset demonio y CN-Series como un modo de servicio de implementación.) • AWS EKS (1.17 a 1.22 para la CN-Series como modo de implementación CNF). • EKS en AWS Outpost (1.17 a 1.25) *CN-Series para EKS en AWS Outpost no es compatible con SR-IOV ni Multus.* • Azure AKS (1.17 a 1.27) *En Azure AKS, PAN-OS 11.0.2 es la versión mínima necesaria compatible con kubernetes 1.25 y superiores.* • GCP GKE (1.17 a 1.27) *Incluye GKE Dataplane V2.* • OCI OKE (1.23)
Kubernetes gestionado por el cliente	En la nube pública o en el centro de datos local. Asegúrese de que la versión de Kubernetes, los tipos de CNI y las versiones de Host VM OS sean según se enumeran en esta tabla. VMware TKG+ versión 1.1.2 • Plataforma de infraestructura: vSphere 7.0 • SO de VM de host de Kubernetes—Photon OS
VM de host de Kubernetes	Sistema operativo: • Ubuntu 16.04

Producto	Versión
	• Ubuntu 18.04 • Ubuntu 22.04 • RHEL / Centos 7.3 y posterior • CoreOS 21XX, 22XX • SO optimizado para contenedores
	Versión del kernel de Linux: • 4.18 o posterior (solo modo de servicio K8s) • 5.4 o posterior necesario para habilitar el modo AF_XDP. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.
	Filtro de red del kernel de Linux: Iptables

Complementos CNI	CNI Spec 0.3 y posterior:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Para Openshift, OpenshiftSDN, OVN Kubernetes
	• Lo siguiente se admite en el cortafuegos CN-Series como un DaemonSet.
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• Versiones 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13. *OpenShift 4.7 está clasificado en la serie CN-Series como DaemonSet únicamente.* *PAN-OS 11.0.2 es la versión mínima requerida compatible con 4.12 y superior.* • OpenShift en AWS

Revise también los Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes, antes de implementar el cortafuegos CN-series.

PAN-OS 11.2

Puede implementar el cortafuegos CN-Series en los siguientes entornos:

Producto	Versión
Tiempo de ejecución del contenedor	Docker CRI-O Containerd
Versión de Kubernetes	1.17 a 1.27
Kubernetes gestionado por el proveedor de la nube	• AWS EKS (1.17 a 1.27 para CN-Series como un daemonset demonio y CN-Series como un modo de servicio de implementación.) • AWS EKS (1.17 a 1.22 para la CN-Series como modo de implementación CNF). • EKS en AWS Outpost (1.17 a 1.25) *CN-Series para EKS en AWS Outpost no es compatible con SR-IOV ni Multus.* • Azure AKS (1.17 a 1.27) *En Azure AKS, PAN-OS 11.0.2 es la versión mínima necesaria compatible con kubernetes 1.25 y superiores.* • GCP GKE (1.17 a 1.27) *Incluye GKE Dataplane V2.* • OCI OKE (1.23)
Kubernetes gestionado por el cliente	En la nube pública o en el centro de datos local. Asegúrese de que la versión de Kubernetes, los tipos de CNI y las versiones de Host VM OS sean según se enumeran en esta tabla. VMware TKG+ versión 1.1.2 • Plataforma de infraestructura: vSphere 7.0 • SO de VM de host de Kubernetes—Photon OS

Producto	Versión
VM de host de Kubernetes	Sistema operativo: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL / Centos 7.3 y posterior • CoreOS 21XX, 22XX • SO optimizado para contenedores
	Versión del kernel de Linux: • 4.18 o posterior (solo modo de servicio K8s) • 5.4 o posterior necesario para habilitar el modo AF_XDP. Consulte Parámetros editables en archivos YAML de la implementación CN-Series para obtener más información.
	Filtro de red del kernel de Linux: Iptables

Complementos CNI	CNI Spec 0.3 y posterior:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Para Openshift, OpenshiftSDN, OVN Kubernetes
	• Lo siguiente se admite en el cortafuegos CN-Series como un DaemonSet.
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• Versiones 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12 y 4.13.  *OpenShift 4.7 está clasificado en la serie CN-Series como DaemonSet únicamente.* *PAN-OS 11.0.2 es la versión mínima requerida compatible con 4.12 y superior.*

Producto	Versión
	• OpenShift en AWS

Revise también los Requisitos del sistema de la serie CN-Series para el clúster de Kubernetes, antes de implementar el cortafuegos CN-series.

Requisitos previos de implementación de CN-series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Para implementar el cortafuegos CN-series, debe asegurarse de que se cumplen los siguientes requisitos previos:

- Autorización de licencia para el cortafuegos CN-Series
- Instalación de un certificado de dispositivo en el cortafuegos CN-Series
- Creación de cuentas de servicio para la autenticación de clúster
- Instalación del complemento de Kubernetes y configuración de Panorama para el CN-Series
- Obtención de las imágenes y los archivos para la implementación del CN-Series

Autorización de licencia para el cortafuegos CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

El complemento de Kubernetes en Panorama gestiona la concesión de licencias del cortafuegos CN-Series. Las licencias de los cortafuegos de la serie CN-Series se basan en el número total de vCPU (núcleos) utilizadas por los pods CN-NGFW implementados en su entorno de Kubernetes. Se consume un token por cada vCPU utilizada en el CN-NGFW.

- Activación de créditos—comience activando sus créditos. Una vez activados, puede aplicar créditos de su grupo de créditos a un perfil de implementación de la serie CN-Series.
- Creación de un perfil de implementación de la serie CN-Series: en el perfil de implementación, especificará el número de las vCPU que se asignan al código de autenticación de generación. A continuación, utilizará el código de autenticación asociado con su perfil de implementación de CN-Series para dar licencia a los cortafuegos CN-Series en su clúster de Kubernetes. El perfil de implementación se puede utilizar para licenciar los pods CN-NGFW en función del número de las vCPU asignadas. Se puede usar un único código de autenticación de un perfil de implementación para licenciar la serie CN-Series en diferentes entornos de Kubernetes, diferentes clústeres o en diferentes instancias de Panorama.

  En una implementación de CN-Series-as-a-Kubernetes-Service, si el número de pods CN-NGFW implementados en su entorno supera el número de las vCPU asignadas, tiene un período de gracia de 30 días para añadir más vCPU a su perfil de implementación o eliminar suficientes pods CN-NGFW. Si no asigna las vCPU adicionales ni elimina los pods sin licencia dentro del período de gracia de 30 días, todos los cortafuegos CN-series en el clúster se eliminarán de la licencia.

  Cuando CN-Series se implementa como DaemonSet, si el número de pods CN-NGFW implementados supera el número de vCPU asignadas, tiene un período de gracia de cuatro horas para añadir más vCPU a su perfil de implementación o eliminar suficientes pods CN-NGFW. Si no asigna vCPU adicionales ni elimina pods sin licencia dentro del período de gracia de cuatro horas, los pods sin licencia dejarán de procesar el tráfico. Los pods que ya tienen licencias permanecen licenciados.

  También tiene la opción de aprovisionar un dispositivo Panorama virtual al crear el perfil de implementación de CN-Series.
- Gestión de perfiles de implementación: puede editar, clonar o eliminar perfiles de implementación de CN-Series en función de los requisitos de su implementación de la serie CN-Series. Además, puede añadir o quitar suscripciones del perfil de implementación una vez creado.

Las licencias se aplican a la serie CN-Series a nivel de clúster. CN-NGFW individuales pueden aparecer como sin licencia, sin embargo, todos los pods en el clúster tienen licencia hasta que todo el clúster se quede sin licencias.

Activación de créditos

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Dentro de su organización puede crear muchas cuentas, cada una con un propósito distinto. Durante la activación, solo puede elegir una cuenta por grupo de crédito predeterminado. Una vez que el grupo de créditos está activo, los usuarios a los que se les concedió la función de administrador de créditos pueden asignar los créditos para las implementaciones e incluso transferir créditos a otros grupos.

Si tiene una cuenta CSP existente y es un superusuario o un administrador, el sistema añade automáticamente la función de administrador de crédito a su perfil. Si no tiene una cuenta existente, el CSP crea automáticamente una cuenta para usted y añade la función de administrador de crédito a su perfil.

Usted (el comprador) recibe un correo electrónico detallando la suscripción, el ID del grupo de créditos, la fecha de inicio y finalización de la suscripción, la cantidad de créditos comprados y la descripción del grupo de créditos predeterminado (el grupo de créditos creado cuando activa sus créditos).

Guarde este correo electrónico en un sitio seguro para futuras referencias.

STEP 1 | En el correo electrónico, haga clic en **Start Activation (Iniciar activación)** para ver los grupos de crédito disponibles.

STEP 2 | Seleccione el grupo de créditos que desea activar. Puede usar el campo de búsqueda para filtrar su lista de cuentas por número o nombre.

Si ha comprado varios grupos de crédito, ambos se seleccionan automáticamente. Las marcas de verificación representan los enlaces de activación para los créditos de incorporación.

Se le solicitará una autenticación o inicio de sesión.

Si anula la selección de un grupo de créditos, verá un recordatorio que le pregunta si desea activar esos créditos, debe volver al correo electrónico y hacer clic en el vínculo ***Start Activation (Iniciar activación)****.*

STEP 3 | Seleccione **Start Activation (Iniciar activación)**.

STEP 4 | Seleccione la cuenta de soporte (puede buscar por número de cuenta o nombre).

STEP 5 | Seleccione el grupo de créditos predeterminado.

STEP 6 | Seleccione **Deposit Credits (Depositar créditos)**.

Verá un mensaje que indica que el depósito se realizó correctamente.

STEP 7 | (opcional) Si esta es su primera activación de crédito, verá el cuadro de diálogo **Create Deployment Profile (Crear perfil de implementación)**.

Continúe a Creación de un perfil de implementación de la serie CN-Series.

Creación de un perfil de implementación de la serie CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para implementación de CN-Series con Helm

Utilice el siguiente procedimiento para crear un perfil de implementación de CN-Series.

STEP 1 | Si ya tiene un grupo de créditos, inicie sesión en la cuenta y, desde el panel de control, seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de software de NGFW)** > **Prisma NGFW Credits (Créditos de NGFW Prisma)** > **Create New Profile (crear nuevo perfil)**.

Si acaba de activar un grupo de créditos, verá el formulario **Create Deployment Profile (Crear perfil de implementación)**.

1. Seleccione el tipo de cortafuegos **CN-Series**.
2. Seleccione **PAN-OS 10.2 and above (PAN-OS 10.2 y superior)**.
3. Haga clic en **Next (Siguiente)**.

STEP 2 | Perfil de la serie CN-Series.

1. **Nombre de perfil**.

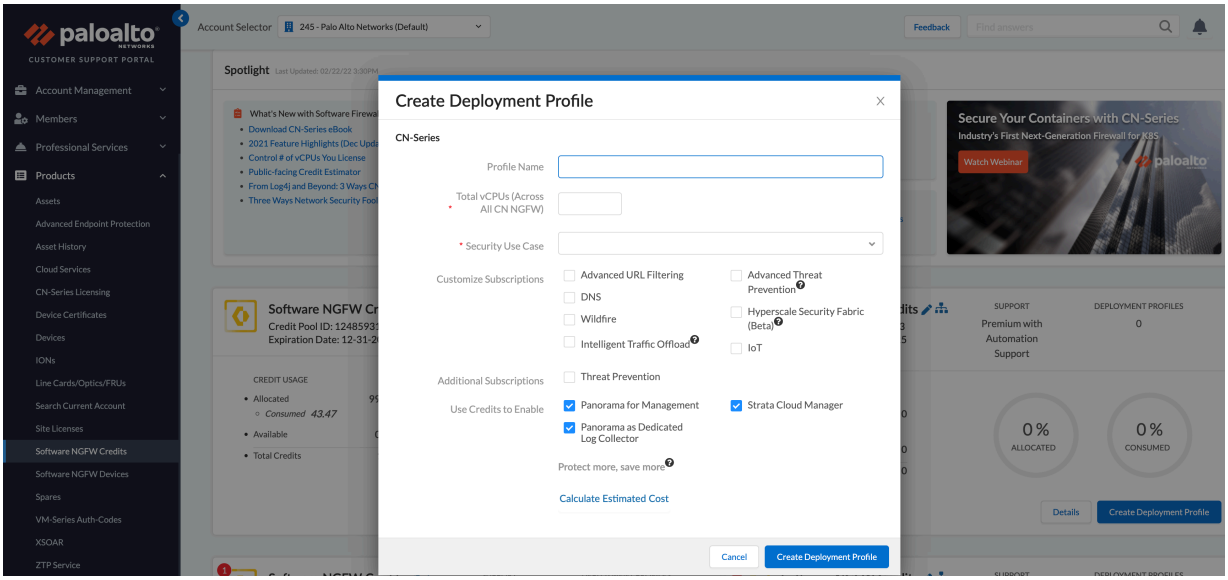
   Asigne un nombre al perfil.
2. **vCPU totales**

   Introduzca el número total de vCPU en todas los CN-NGFW.
3. Seleccione un caso de uso de seguridad en el menú desplegable. Cada caso de uso de seguridad en el menú desplegable selecciona automáticamente una serie de descripciones que se recomiendan para el caso de uso seleccionado. Si selecciona Personalizado, puede especificar las suscripciones que desea usar en su implementación.
4. (opcional) **Use Credits to Enable VM Panorama (Utilice Créditos para habilitar VM Panorama)**: Para **Management (Administración)** o **Dedicated Log Collector (Recopilador de logs dedicado)**.

STEP 3 | (opcional) Coloque el ratón sobre el signo de interrogación después de **Protect more, save more (Proteger más, ahorrar más)** para ver cómo su asignación de crédito afecta los ahorros.

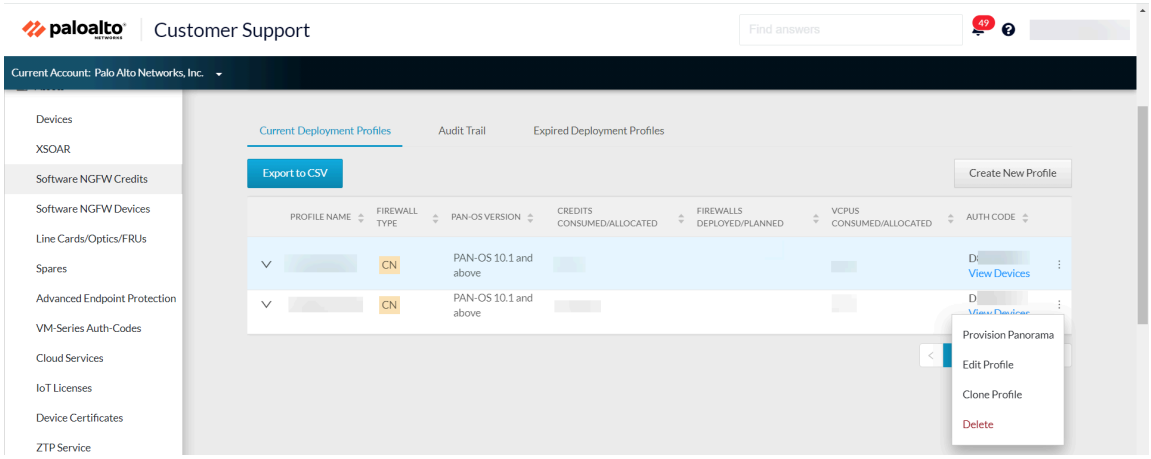
STEP 4 | Haga clic en **Calculate Estimated Cost (Calcular coste estimado)** para ver el total de crédito y el número de créditos disponibles antes de la implementación.

(opcional) Pase el ratón sobre el signo de interrogación después de la estimación para ver el desglose del crédito para cada componente.



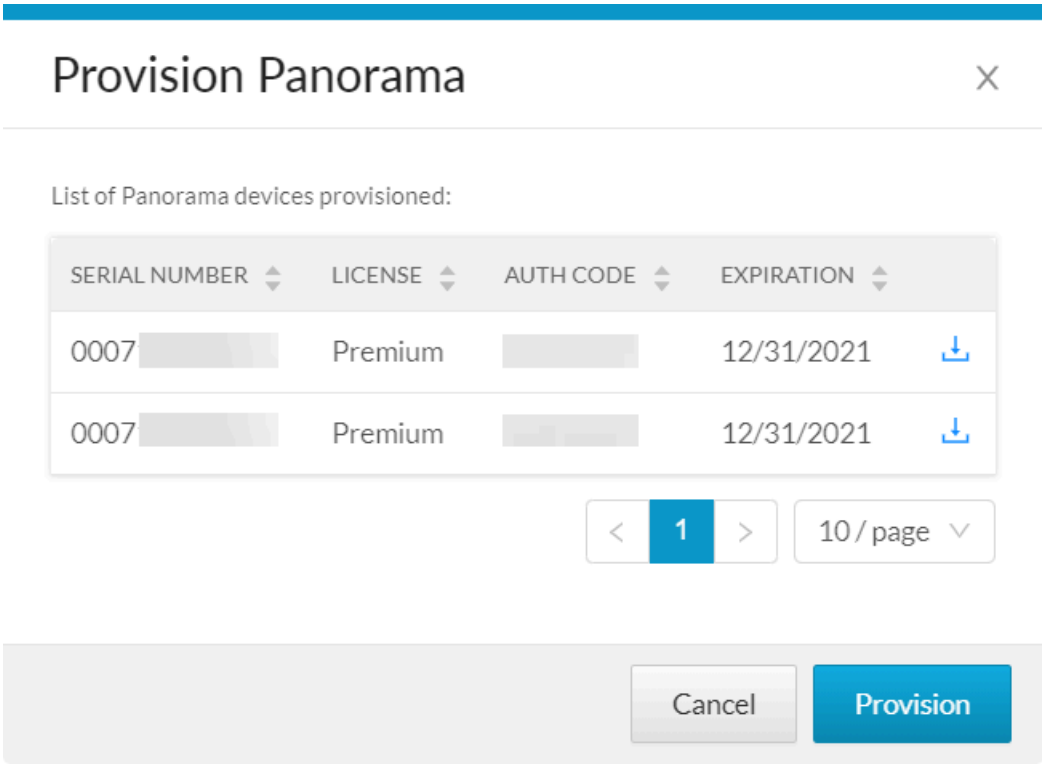
STEP 5 | (opcional) Aprovisionamiento de Panorama. Si usó créditos para Habilitar un máquina virtual de panorama, complete los pasos siguientes para aprovisionar Panorama y generar un número de serie. Se requiere Panorama para gestionar implementaciones de CN-Series. Una vez que haya aplicado el número de serie a Panorama, Panorama se pondrá en contacto con el servidor de actualización de licencias y recuperará la licencia.

1. Seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de software de NGFW)** > **Prisma NGFW Credits (Créditos de NGFW Prisma)** y localice su perfil de implementación.
2. En el extremo derecho, seleccione los puntos suspensivos verticales y seleccione **Provision Panorama (Aprovisionar Panorama)**.



3. Haga clic en Aprovisionar Panorama para generar un número de serie.

4. Registre o copie el número de serie para aplicarlo a la instancia de Panorama.



5. Registre Panorama.

Gestión de perfiles de implementación

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la CN-Series con Helm

Puede utilizar los siguientes procedimientos para gestionar sus perfiles de implementación existentes.

- Editar un perfil de implementación
- Clonación de un perfil de implementación
- Eliminar un perfil de implementación
- Transferir créditos al grupo en la Misma cuenta
- Transferir créditos a una cuenta de CSP diferente

Editar un perfil de implementación

Puede modificar un perfil de implementación existente para añadir más créditos o asignar CPU virtuales adicionales a su implementación. El código de autenticación asociado con el perfil de implementación que se va a modificar no debe estar en uso en Panorama.

STEP 1 | Seleccione **Assets (Activos)** > **Software** y seleccione un perfil (seleccione una fila).

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Edit Profile (Editar perfil)**.

STEP 3 | Realice los cambios y seleccione **Update Deployment Profile (Actualizar perfil de implementación)**.

Clonación de un perfil de implementación

Complete el siguiente procedimiento para clonar un perfil de implementación existente.

STEP 1 | Vaya a **Assets (Activos)** > **Software** y seleccione un perfil (seleccione una fila).

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Clone Profile (Clonar perfil)**.

STEP 3 | Cambie el nombre del perfil, realice cualquier otro cambio y seleccione **Create Deployment Profile (Crear perfil de implementación)**.

Eliminar un perfil de implementación

Antes de eliminar un perfil de implementación, debe eliminar cualquier cortafuegos que utilice el perfil. El código de autenticación asociado con el perfil de implementación que se eliminará no debe estar en uso en Panorama.

STEP 1 | En el CSP, seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de software de NGFW)** y seleccione un perfil (seleccione una fila).

STEP 2 | En el extremo derecho, seleccione los puntos suspensivos verticales (Más opciones) y seleccione **Delete (Eliminar)**.

Transferir créditos al grupo en la Misma cuenta

Puede transferir créditos a un grupo de créditos en una cuenta diferente a la que puede acceder.

STEP 1 | Inicie sesión en su cuenta de CSP.

STEP 2 | Seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)**.

- Identifique el grupo de crédito de origen y anote el ID del grupo de crédito.
- Identifique el grupo de crédito de destino y anote el ID del grupo de crédito.

STEP 3 | Vaya al grupo de crédito de origen y seleccione **Transfer Credits (Transferir créditos)** en la parte inferior izquierda.

STEP 4 | Seleccione una **Different CSP account (Cuenta de CSP diferente)**.

1. **New credit type (Nuevo tipo de crédito)**: elija un tipo de crédito. En estos momentos, el tipo de origen y destino debe ser el mismo.
2. **Credit Pool ID# (Nº de ID del grupo de crédito)**: elija un número de identificación del grupo de crédito. Si la cuenta de destino no tiene ningún grupo de crédito del tipo elegido, el CSP le solicitará que cree un grupo de crédito.
3. **Amount to transfer (Cantidad a transferir)**: introduzca la cantidad a transferir.

STEP 5 | Seleccione **Update Credits (Actualizar créditos)**.

Transferir créditos a una cuenta de CSP diferente

Puede transferir créditos a un grupo de créditos en la misma cuenta.

STEP 1 | Inicie sesión en su cuenta de CSP.

STEP 2 | Seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)**.

- Identifique el grupo de crédito de origen y anote el ID del grupo de crédito.
- Identifique el grupo de crédito de destino y anote el ID del grupo de crédito.

  Si el destino está en una cuenta diferente, selecciónelo en el menú desplegable **Current Account (Cuenta actual)** en la parte superior izquierda y seleccione **Assets (Activos)** > **Software NGFW Credits (Créditos de NGFW de software)**. Busque el destino y anote el tipo de crédito y el ID del grupo de créditos.

STEP 3 | Vaya al grupo de crédito de origen y haga clic en **Transfer Credits (Transferir créditos)** en la parte inferior izquierda.

STEP 4 | Seleccione una cuenta CSP diferente.

1. **Transfer to (Transferir a)**: seleccione un nombre de cuenta.
2. **As Credit Type (Como tipo de crédito)**: seleccione un tipo de crédito. En estos momentos, el tipo de origen y destino debe ser el mismo.
3. **Credit Pool ID# (Nº de ID del grupo de crédito)**: elija un número de identificación del grupo de crédito. Si la cuenta de destino no tiene ningún grupo de crédito del tipo elegido, el CSP le solicitará que cree un grupo de crédito.
4. **Amount to transfer (Cantidad a transferir)**: introduzca la cantidad a transferir.

STEP 5 | Seleccione **Update Credits (Actualizar créditos)**.

Instalación de un certificado de dispositivo en el cortafuegos CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

El cortafuegos requiere un certificado de dispositivo que autorice el acceso seguro a los servicios de seguridad entregados en la nube (CDSS) de Palo Alto, como WildFire, AutoFocus y Strata Logging Service. Debe aplicar un PIN de registro automático para aplicar una licencia CDSS a su implementación de cortafuegos CN-Series. Cada PIN se genera en el Portal de atención al cliente (CSP) y es exclusivo de su cuenta de asistencia de Palo Alto Networks. Para instalar correctamente el certificado del dispositivo, el pod de plano de gestión de la serie CN-Series (CN-MGMT) debe tener una conexión a Internet saliente y se deben permitir los siguientes nombres de dominio completos (FQDN) y puertos en su red.

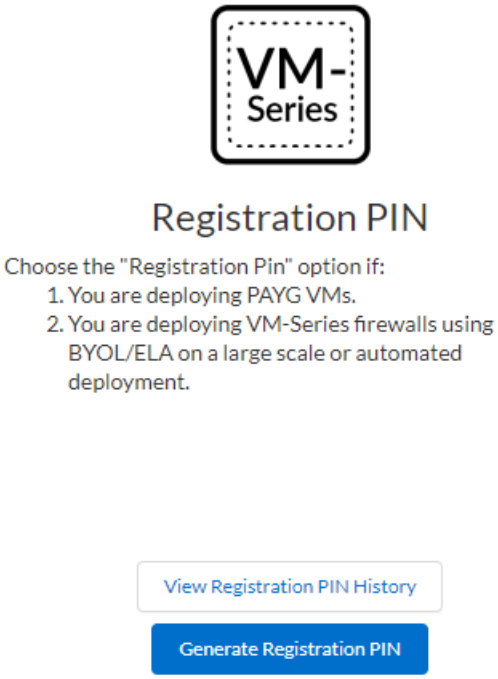
FQDN	Ports (Puertos)
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 y TCP 443

Para añadir un certificado de dispositivo a una implementación existente sin un certificado de dispositivo existente, debe volver a implementar el cortafuegos CN-Series después de agregar el ID de PIN y el valor válidos a `pan-cn-mgmt-secret.yaml`*. Para la implementación de la serie CN-Series de nube pública, debe eliminar la reclamación de volumen persistente antes de que se vuelva a realizar la implementación. Para implementaciones estáticas/nativas de Kubernetes, debe eliminar la reclamación de volumen persistente y el volumen persistente antes de volver a realizar la implementación.*

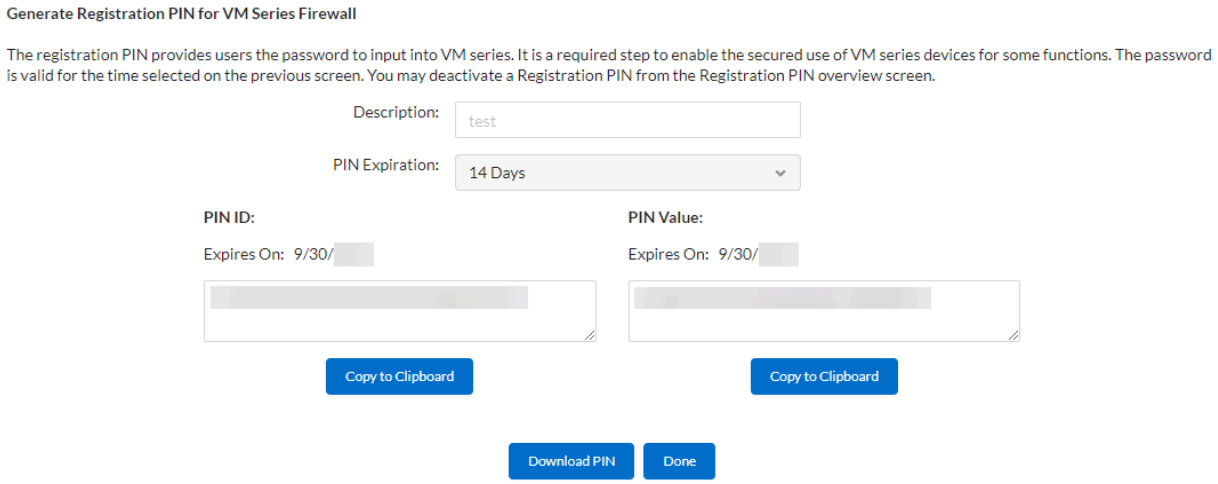
STEP 1 | Inicie sesión en el portal de asistencia técnica de Palo Alto Networks con las credenciales de su cuenta.

Si necesita una nueva cuenta, consulte Cómo crear una nueva cuenta de usuario del portal de atención al cliente.

STEP 2 | Seleccione **Assets (Activos)** > **Device Certificates (Certificados de dispositivo)** > **Generate Registration PIN (Generar PIN de registro)**.



STEP 3 | Introduzca una **Description (Descripción)** y seleccione un **PIN Expiration (Vencimiento de PIN)** en el menú desplegable.



STEP 4 | Guarde el ID y el valor del PIN.

Guarde el ID y el valor del PIN. Este ID de PIN y valor son entradas en el archivo `pan-cn-mgmt-secret.yaml` utilizado para implementar el cortafuegos cn-series. Asegúrese de iniciar el cortafuegos antes de que caduque el PIN.

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


Creación de cuentas de servicio para la autenticación de clúster

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de la serie CN-Series con gráfico helm

El cortafuegos CN-Series requiere tres cuentas de servicio con los permisos mínimos que le autorizan a comunicarse con los recursos del clúster de Kubernetes. La cuenta de servicio (pan-plugin-user) creada con `plugin-serviceaccount.yaml` permite que el complemento de Kubernetes en Panorama se autentique con el clúster de Kubernetes para recuperar metadatos en los pods. Los otros dos archivos yaml, `pan-mgmt-serviceaccount.yaml` y `pan-cni-serviceaccount.yaml`, crean las cuentas de servicio pan-mgmt-sa y pan-cni-sa para habilitar la autenticación entre los pods CN-Mgmt tolerantes a los fallos, y entre los pods CN-MGMT y los pods CN-NGFW.

De forma predeterminada, los archivos YAML crean la cuenta de servicio y el secreto en el espacio de nombres del sistema kube; el complemento de Kubernetes solo buscará el secreto en el espacio de nombres del sistema kube.

Para crear las cuentas de servicio, su clúster de Kubernetes debería estar listo.

STEP 1 | Ejecute la cuenta de servicio YAML para `plugin-serviceaccount.yaml`.

Esta cuenta de servicio habilita los permisos que Panorama requiere para autenticarse en el clúster de GKE para recuperar las etiquetas de Kubernetes y la información de recursos. Esta cuenta de servicio se denomina pan-plugin-user de forma predeterminada.

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

   Para ver los secretos asociados con esta cuenta de servicio.

   Si utiliza kubernetes versión 1.24 o superior, ejecute el siguiente comando para ver los secretos asociados con esta cuenta de servicio:

   `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`**

   Cree el archivo de credenciales, denominado cred.json en este ejemplo, que incluye los secretos y guarde este archivo. Debe cargar este archivo en Panorama para configurar el complemento de Kubernetes para supervisar los clústeres en Instalación del complemento de Kubernetes y configuración de Panorama para el CN-Series.

STEP 2 | Ejecute `pan-mgmt-serviceaccount.yaml` y `pan-cni-serviceaccount.yaml`.

`pan-mgmt-serviceaccount.yaml` crea una cuenta de servicio denominada pan-sa, y es necesario para permitir que los pods CN-MGMT y CN-NGFW se comuniquen entre sí, el PAN-CNI y el Servidor de API de Kubernetes. Si modifica el nombre de esta cuenta de servicio, también debe actualizar los archivos YAML que usa para implementar los pods CN-MGMT y CN-NFGW. `pan-cni-serviceaccount.yaml` crea una cuenta de servicio llamada pan -cni-sa.

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

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

STEP 3 | Verifique las cuentas de servicio.

`kubectl get serviceaccounts -n kube-system`

Si está utilizando el gráfico HELM, los pasos 2 y 3 están automatizados por el gráfico HELM y no es necesario realizarlos de forma manual.

Instalación del complemento de Kubernetes y configuración de Panorama para el CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

Puede implementar el dispositivo Panorama de modo local o en la nube, siempre que el dispositivo Panorama pueda conectarse con los clústeres de Kubernetes donde desee implementar los cortafuegos CN-Series. Este flujo de trabajo le lleva a través del proceso de instalación del complemento de Kubernetes, la activación del código de autorización y la configuración del complemento de Kubernetes para supervisar sus clústeres.

Debe planificar cuidadosamente el número de créditos que desea asignar a Panorama. Después de cambiar el número de créditos, no es necesario volver a implementar el cortafuegos CN-Series en Panorama OS 11.0.

Para obtener más información, consulte Autorización de licencia para el cortafuegos CN-Series *y* Software NGFW Credit Estimator.

STEP 1 | Implemente un Panorama con la versión de software 11.0 e instale la versión mínima de contenido.

1. Vaya a **Panorama** > **Dynamic Updates (actualizaciones dinámicas)** para ver la versión mínima de lanzamiento de contenido en PAN-OS 11.0.

   Consulte Notas de la versión de PAN-OS .

2. Vaya a **Panorama** > **Software** para obtener la versión del software.

   Localice y descargue el archivo específico del modelo para la versión de lanzamiento a la que está actualizando. Por ejemplo, para actualizar un dispositivo M-Series a Panorama 11.0, descargue la imagen Panorama_m-11.0.0; para actualizar un dispositivo virtual Panorama a Panorama 11.0.0, descargue la imagen Panorama_pc-11.0.0.

   Después de una descarga correcta, la columna **Acción** cambia de Descargar a Instalar para instalar la imagen descargada.

STEP 2 | Compruebe que su Panorama está en Modo Panorama, si desea que Panorama recopile los logs del cortafuegos.

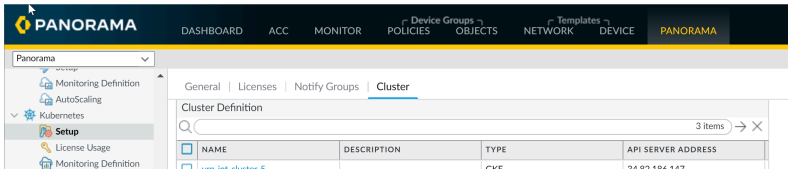
STEP 3 | Instale el complemento de Kubernetes en Panorama. Si los dispositivos Panorama se implementan como una pareja de alta disponibilidad (HA), primero se debe instalar el complemento de Kubernetes en el equipo principal (activo).

1. Inicie sesión en la interfaz web de Panorama, seleccione **Panorama** > **Plugins (Complementos)** y haga clic en **Check Now (Comprobar ahora)** para obtener la lista de complementos disponibles.

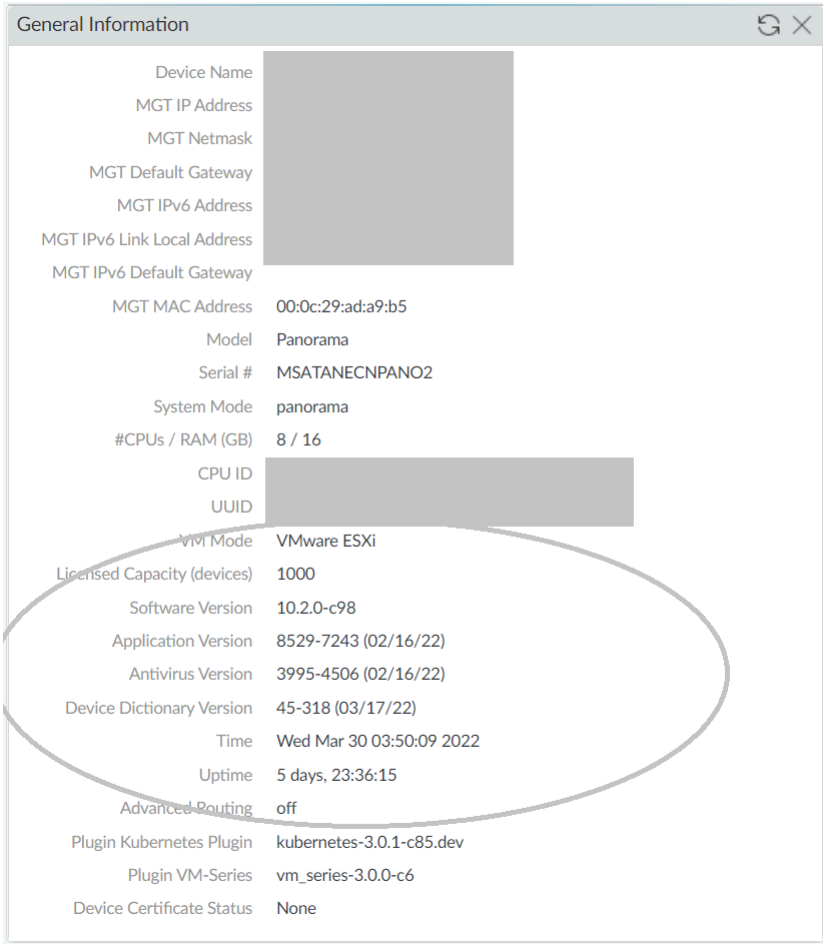
2. Seleccione **Download (Descargar)** e **Install (Instalar)** para descargar e instalar el complemento de Kubernetes

   Después de realizar la instalación correctamente, Panorama se actualiza y el complemento de Kubernetes se muestra en la pestaña **Panorama**.

Si Panorama se implementa en un par de alta disponibilidad, instale el complemento de Kubernetes en el Panorama secundario (pasivo) siguiendo los pasos anteriores descritos en el Paso 3.



También puede comprobar el widget de Información general en el **Dashboard (panel)** de Panorama.

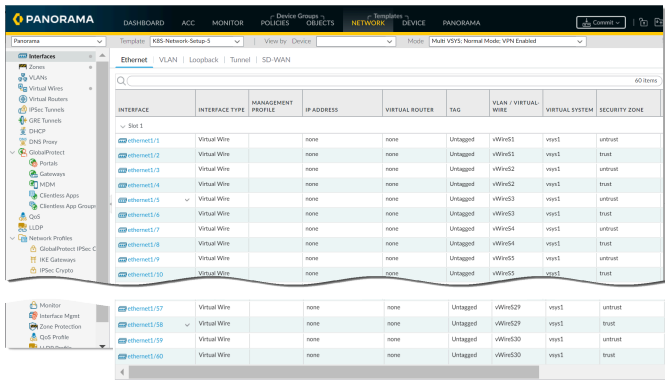


STEP 4 | Confirme los cambios realizados en Panorama.

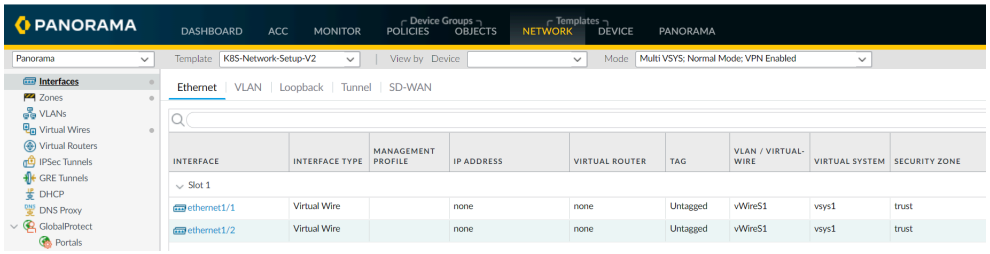
Haga clic en**Commit to Panorama (Confirmar en Panorama)**. La confirmación crea cuatro plantillas:**K8S-Network-Setup**, **K8S-Network-Setup-V2**, **K8S-Network-Setup-V3**, y **K8S-Network-Setup-V3-HA**. Las interfaces pueden tardar hasta un minuto en mostrarse en Panorama.

- **K8S-Network-Setup** es para usar con la serie CN-Series como un DaemonSet y tiene 30 cables virtuales; un par de interfaces que forman parte de un cable virtual para proteger una aplicación. Por

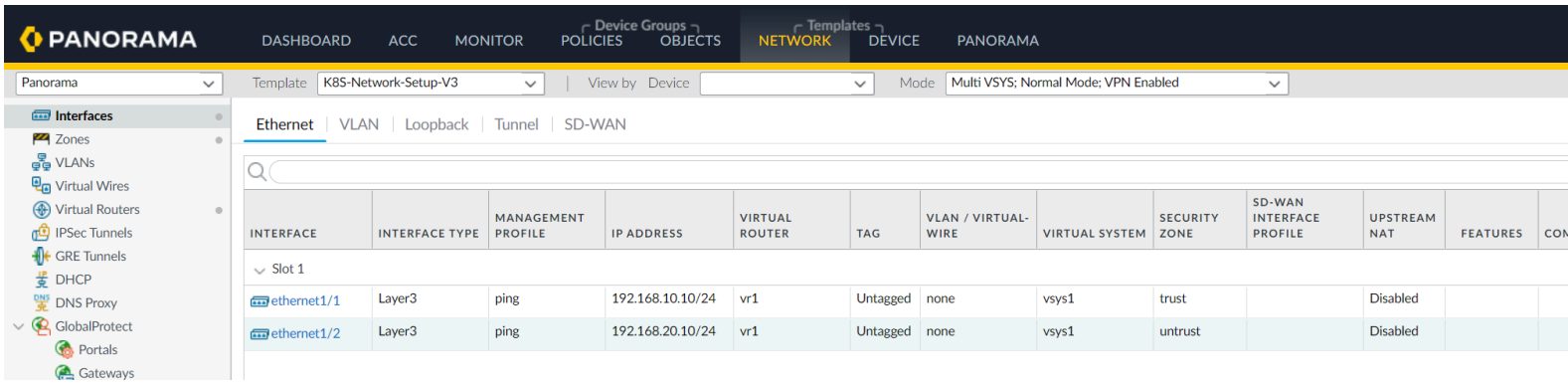
lo tanto, CN-NGFW como DaemonSet puede proteger un máximo de 30 pods de aplicaciones en un nodo.



- **K8S-Network-Setup-V2** se usa con la serie CN-Series como un servicio de Kubernetes y tiene un cable virtual; un par de interfaces que forman parte del cable virtual para proteger aplicaciones de pods.



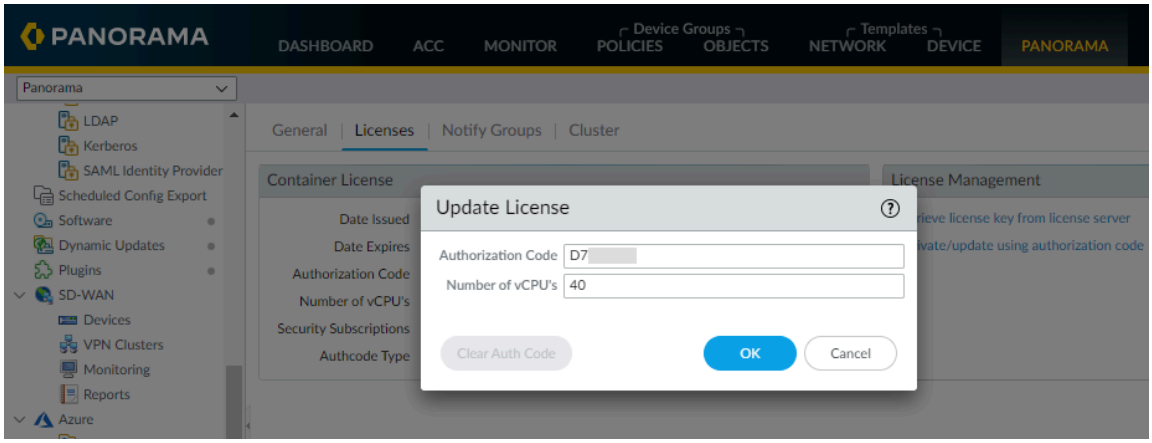
- La plantilla **K8S-Network-Setup-V3** tiene una configuración de ejemplo que puede clonar y puede modificarla para que coincida con las configuraciones deseadas. El modo de implementación CNF de Kubernetes protege las cargas de trabajo tanto de contenedores como de no contenedores. Puede implementar como una implementación de capa 3 independiente.



STEP 5 | Obtenga los créditos de licencia de la serie CN-Series en Panorama.

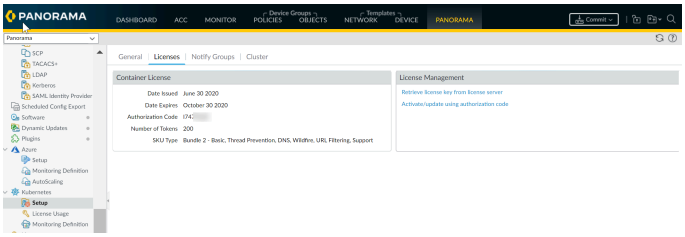
1. Seleccione **Panorama** > **Plugins (Complementos)** > **Kubernetes** > **Setup (Configuración)** > **Licenses (Licencias)**.
2. Seleccione **Activate/update using authorization code (Activar/actualizar mediante el código de autorización)** e introduzca el código de autorización y el número total de vCPU de plano

de datos necesarias. Debe Creación de un perfil de implementación de la serie CN-Series para obtener su código de autenticación CN-Series.



Si implementa el cortafuegos CN-Series sin activar la licencia, tiene un período de gracia de 4 horas después del cual los cortafuegos dejan de procesar el tráfico. Después del período de gracia, las instancias del CN-NGFW continuarán operando (predeterminado) o dejarán de funcionar según el modo de conmutación por error (FAILOVER_MODE) definido en el `pan-cn-ngfw-configmap.yaml`. En el modo de abierto con fallo recibirá los paquetes y los enviará sin aplicar ninguna política de seguridad. La transición a abierto con fallo requerirá un reinicio y provocará una breve interrupción del tráfico durante ese tiempo (se prevé alrededor de 10 a 30 segundos). En el modo de cierre por fallo, el cortafuegos descartará todos los paquetes que reciba. Un cierre por fallo desactivará el pod CN-NGFW y liberará los créditos al grupo de créditos disponible para otorgar licencias para nuevos pods CN-NGFW.

3. Compruebe que se ha actualizado el número de créditos de licencia disponibles.



STEP 6 | Genere una clave de autenticación de máquina virtual.

1. Asegúrese de que se cumplen los siguientes requisitos previos:
   - Tiene un ordenador con acceso de red a Panorama.
   - Conoce la dirección IP de Panorama.
   - La interfaz de gestión admite SSH, la cual es la configuración predeterminada. Si un administrador ha deshabilitado SSH y desea volver a habilitarlo: seleccione **Panorama** > **Setup (Configuración)** > **Interfaces**, haga clic en **Management (Gestión)**, seleccione **SSH**, haga clic en **OK (Aceptar)**, seleccione **Commit (Confirmar)** > **Commit to**

Panorama (Confirmar en Panorama) y seleccione **Commit (Confirmar)** sus cambios a la configuración de Panorama.

2. Para acceder a la CLI usando SSH:
   1. Introduzca la dirección IP de Panorama en el cliente SSH y utilice el puerto 22.
   2. Introduzca las credenciales de acceso administrativo cuando se le soliciten. Después de iniciar sesión, se muestra el mensaje del día, seguido del mensaje de la CLI en modo operativo. Por ejemplo:

      ```
      admin@ABC_Sydney>
      ```

3. Utilice el siguiente comando operativo:

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

   Por ejemplo, para generar una tecla con validez de 24 horas, introduzca lo siguiente:

   request bootstrap vm-auth-key generate lifetime 24

   ```
    VM auth key 755036225328715 generated.   Expires at:
   2020/01/29 12:03:52
   ```

4. Debe asegurarse de guardar la clave de autenticación de máquina virtual en algún lugar, ya que es necesaria para el paso posterior.

STEP 7 | Cree un grupo de dispositivos principal y una pila de plantillas.

Debe crear una pila de plantillas y un grupo de dispositivos, hará referencia a esta pila de plantillas y grupo de dispositivos más adelante cuando edite el archivo YAML para implementar los pods CN-MGMT. El complemento de Kubernetes en Panorama crea una plantilla llamada K8S-Network-Setup, y esta plantilla será parte de la pila de plantillas que defina aquí.

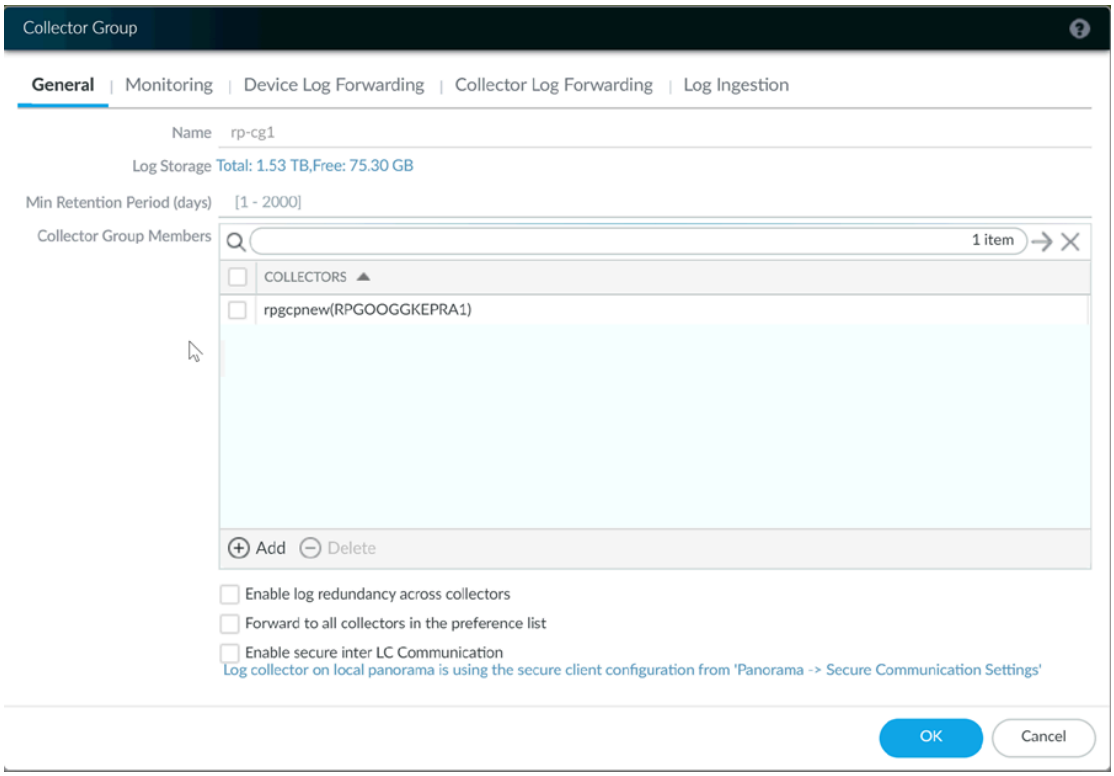
1. Cree una pila de plantillas y añada la plantilla K8S-Network-Setup a la pila de plantillas.
   1. Seleccione **Panorama** > **Templates (Plantillas)** y **Add Stack (Añadir pila)**.
   2. Introduzca un nombre único en **Name (Nombre)** para identificar la pila.
   3. Añada y seleccione la plantilla **K8S-Network-Setup** para daemonset, **K8S-Network-Setup-V2** para kubernetes como implementación de servicio, **K8S-Network-Setup-V3** para

implementación independiente de CNF o **K8S-Network-Setup-V3-HA** para implementación de CNF de HA.

4. Haga clic en **OK (Aceptar)**.

2. Cree un grupo de dispositivos.
   1. Vaya a **Panorama** > **Device Groups (Grupos de dispositivos)** y haga clic en **Add (Añadir)**.
   2. Introduzca un **Name (Nombre)** y una **Description (Descripción)** exclusivos para identificar el grupo de dispositivos.
   3. Seleccione **Parent Device Group (Grupo de dispositivos primario)** (de manera predeterminada, **Shared** [Compartido]) que estará justo por encima del grupo de dispositivos que está creando en la jerarquía del grupo de dispositivos.
   4. Haga clic en **OK (Aceptar)**.
3. Si está utilizando un dispositivo virtual de Panorama, puede crear un colector de logs y añádalo a un grupo de colectores de logs.
   1. Vaya a **Panorama** > **Collector Groups (Grupos de colectores)** y haga clic en **Add (Añadir)** para añadir un grupo de colectores.
   2. Introduzca un nombre en **Name (Nombre)** para el grupo de recopiladores.
   3. Introduzca el **Minimum Retention Period (Período de retención mínimo)** en días (de 1 a 2000) que el grupo de recopiladores conservará los logs del cortafuegos.

      De forma predeterminada, el campo está en blanco, lo que significa que el grupo de recopiladores conserva los logs indefinidamente.
   4. Seleccione **Add (Añadir)** recopiladores de logs (1 a 16) a la lista de Miembros del grupo de recopiladores.



5. Seleccione **Commit (Confirmar)** > **Commit and Push (Confirmar y enviar)** y luego haga clic en **Commit and Push (Confirmar y enviar)** para confirmar y enviar sus cambios a Panorama y al grupo de recopiladores que configuró.

4. Si está utilizando Enrutamiento avanzado, actívelo.

   1. Vaya a **Panorama** > **Templates (Plantillas) > Device (Dispositivo)**.
   2. En la pestaña **Management (Gestión)**, seleccione **Advanced Routing (Enrutamiento avanzado)** (Esto solo se aplica al modo de implementación CNF de Kubernetes).

STEP 8 | Configure el complemento de Kubernetes para supervisar los clústeres.

El siguiente paso en el proceso es añadir información de clúster de Kubernetes a Panorama para garantizar que los dos pueden comunicarse entre sí.

Panorama admite hasta 32 clústeres de Kubernetes.

Para asegurarse de que el complemento y los clústeres de Kubernetes estén sincronizados, el complemento sondea el servidor de la API de Kubernetes en un intervalo configurado y escucha las notificaciones de la API de Watch de Kubernetes en un intervalo predefinido.

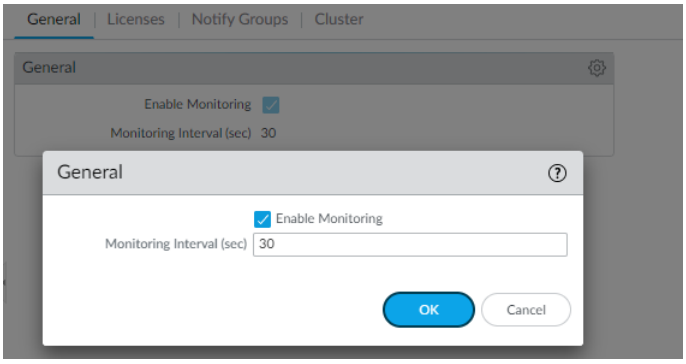
Después de añadir la información del clúster, Panorama siempre recupera el servicio, el nodo, el conjunto de réplicas y luego crea etiquetas para que pueda obtener visibilidad y controlar el tráfico hacia y desde estos clústeres. De forma opcional, puede especificar si desea que Panorama recupere

información en las etiquetas de Kubernetes y crear etiquetas para estas también. Consulte Asignación de dirección IP a etiqueta de atributos de Kubernetes para obtener una lista de los atributos compatibles.

1. Compruebe el intervalo de supervisión.

   El intervalo predeterminado en el que Panorama sondea el endpoint del servidor de la API de Kubernetes es de 30 segundos.

   1. Seleccione **Panorama** > **Plugins (Complementos)** > **Kubernetes** > **Setup (Configuración)** > **General**.
   2. Verifique que **Enable Monitoring (Habilitar supervisión)** esté seleccionado.
   3. Haga clic en el icono de engranaje para editar el **Monitoring Interval (Intervalo de supervisión)** y cambie a un intervalo de 30 a 300 segundos.



2. Seleccione **Panorama** > **Plugins (Complementos)** > **Kubernetes** > **Setup (Configuración)** > **Cluster (Clúster)** y **Add (Añadir)**.

   Asegúrese de no añadir el mismo clúster de Kubernetes a más de un dispositivo Panorama (instancia única o par de HA) porque puede ver incoherencias en la forma en que las asignaciones de direcciones IP a se registran en los grupos de dispositivos.

3. Introduzca un **Name (Nombre)** y la **API Server Address (Dirección del servidor API)**.

   Esta es la dirección IP del endpoint para el clúster que debe obtener de su implementación de Kubernetes. Introduzca un nombre, de hasta 20 caracteres, para identificar de manera única el nombre del clúster. No puede modificar este nombre porque Panorama usa el nombre del clúster cuando crea etiquetas para los pods, nodos y servicios que descubre dentro del clúster.

   El formato de la dirección del servidor API puede ser un nombre de host o una dirección IP: número de puerto, y no es necesario que especifique el puerto si está utilizando el puerto 443, el puerto predeterminado.

4. Seleccione el **Type (Tipo)** de entorno en el que se implementa su clúster.

   Las opciones disponibles son AKS, EKS, GKE, Native Kubernetes, OpenShift y otras.

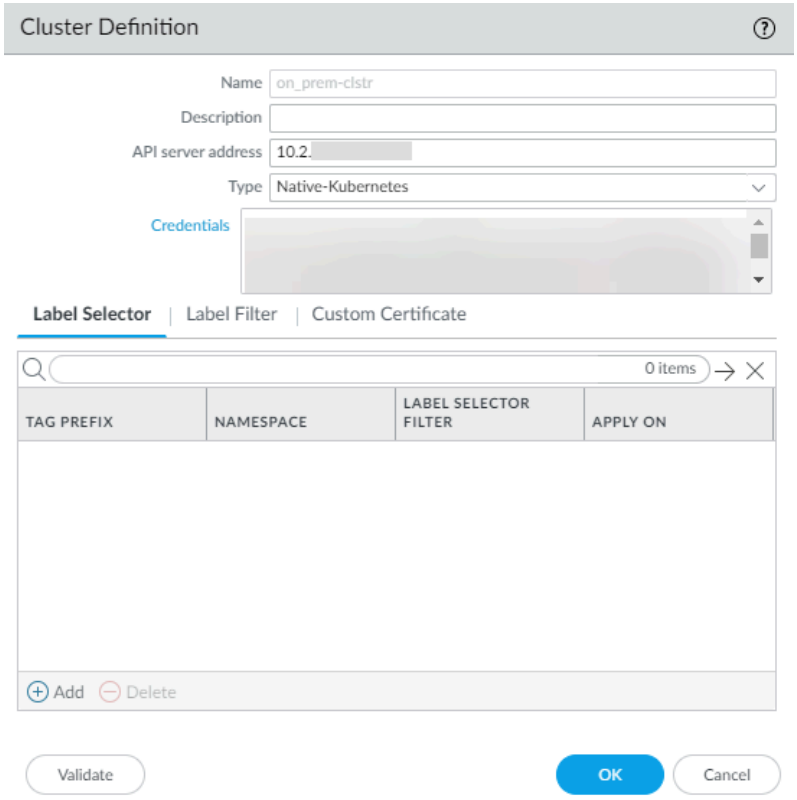
5. Cargue la **Credential (Credencial)** de la cuenta de servicio que Panorama requiere para comunicarse con el clúster. Como se describe en el flujo de trabajo Creación de cuentas de

servicio para la autenticación de clúster, el nombre de archivo de esta cuenta de servicio es `plugin-svc-acct.json`.

Si está cargando las credenciales de servicio mediante CLI/API, entonces tiene más de 10 KB, debe comprimir con gzip el archivo y luego realizar una codificación base64 del archivo comprimido antes de cargar o pegar el contenido del archivo en la CLI o API de Panorama. Estos pasos no son necesarios si va a cargar el archivo de credenciales de servicio en la GUI.

6. Haga clic en **OK (Aceptar)**.

   Puede dejar la configuración de Filtro de etiquetas y Selector de etiquetas para más adelante. Esta es una tarea opcional que le permite recuperar cualquier etiqueta personalizada o definida por el usuario para la que desea que Panorama cree etiquetas.

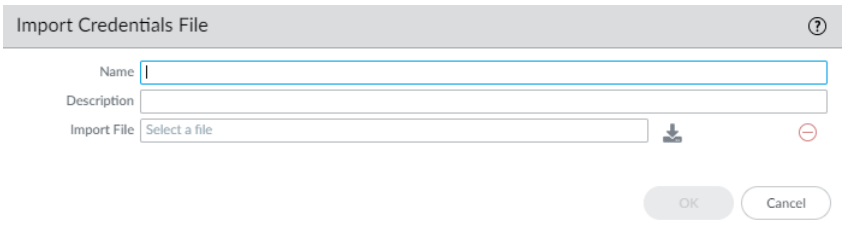


STEP 9 | (Opcional) Si el certificado del servidor API del clúster de Kubernetes está firmado por una cadena de certificados, la autenticación del complemento de Kubernetes para Panorama requiere todos los

certificados en la cadena. Si su servidor API utiliza una cadena de certificados, debe combinar todos los certificados de la cadena en un solo archivo .crt y añadirlo al complemento.

El complemento de Kubernetes admite hasta cuatro certificados.

1. Seleccione **Panorama** > **Kubernetes** > **Setup (Configuración)** > **Cluster (Clúster)** > **Add (Añadir)** > **Custom Certificate (Certificado personalizado)** > **Add (Añadir)** para importar un archivo de credenciales.
2. Introduzca un **Name (Nombre)** descriptivo.
3. (Opcional) Introduzca una **descripción**.
4. Haga clic en el icono de importación y desplácese hasta el archivo de certificado.
5. Haga clic en **OK (Aceptar)**.



STEP 10 | (Opcional) Configure un proxy para cada clúster.

A diferencia de los otros complementos, el complemento de Kubernetes no utiliza el proxy configurado en **Panorama** > **Setup (Configuración)** > **Services (Servicios)**. En cambio, si desea habilitar u omitir un proxy, debe introducir el proxy para cada clúster. Cuando se ha configurado, el complemento de Kubernetes utiliza esta dirección IP del servidor proxy para realizar todas las llamadas de API al servidor de API para este clúster.

1. Inicie sesión en la CLI de Panorama.
2. Introduzca los siguientes comandos de la CLI para configurar el servidor proxy para este clúster de 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>

*** el nombre de usuario y la contraseña son opcionales ***
```

STEP 11 | Siguientes pasos:

1. Obtención de las imágenes y los archivos para la implementación del CN-Series
2. Implementación del cortafuegos cn-series.
3. Configuración de Panorama para proteger una implementación de Kubernetes

Obtención de las imágenes y los archivos para la implementación del CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• Implementación de CN-Series	• CN-Series 10.1.x or above Container Images • Panorama con PAN-OS 10.1.x o versión superior • Helm 3.6 or above version client para la implementación de CN-Series utilizando Helm

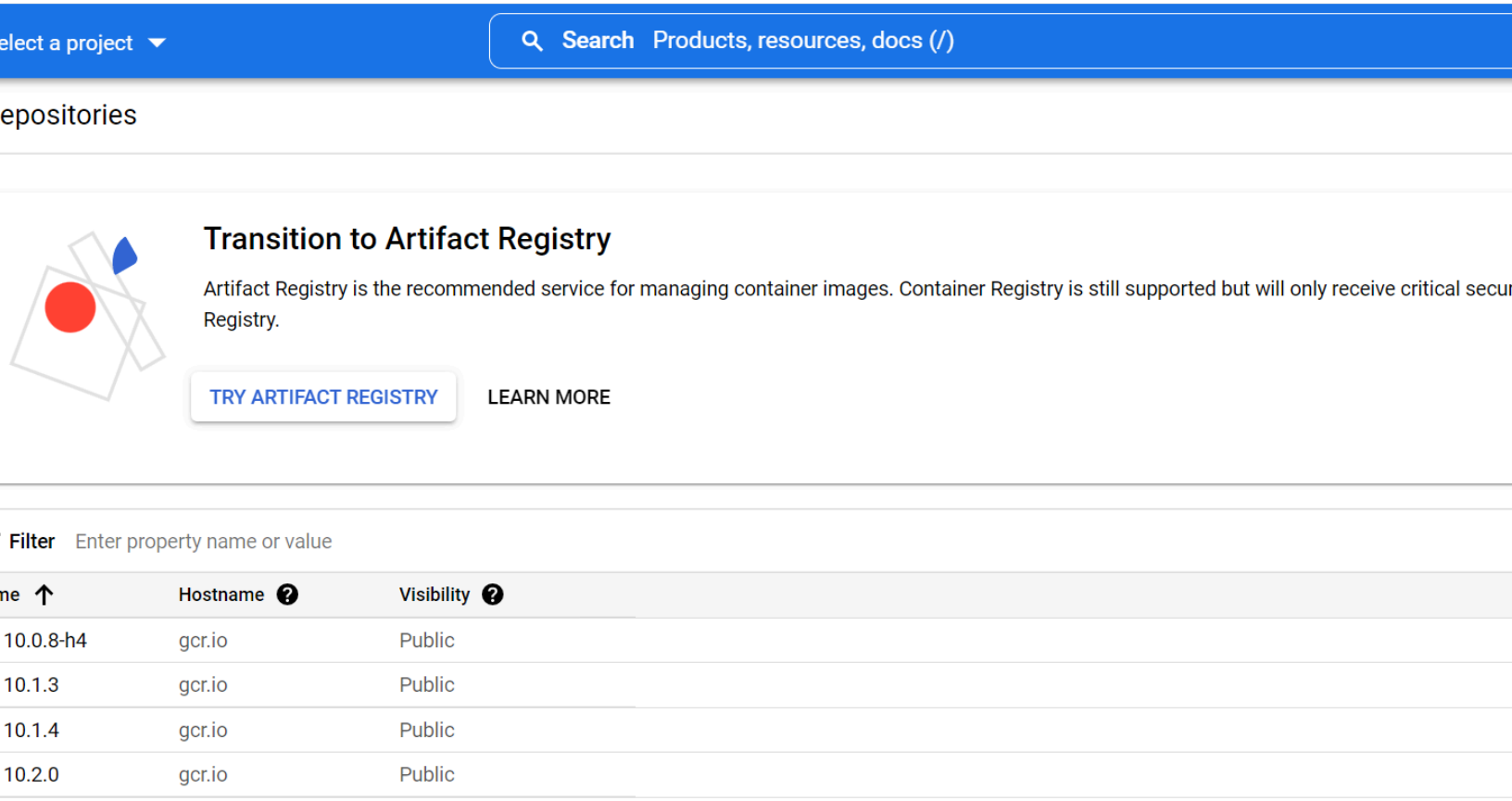
Consulte la tabla siguiente antes de comenzar la implementación para asegurarse de que ha descargado los archivos compatibles.

Versión de PAN-OS	Versión de YAML	Versión CNI	Versión 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

Siga los siguientes pasos para extraer las imágenes de docker del registro de contenedores públicos de Google Cloud Platform y, a continuación, continúe a implementar el cortafuegos CN-Series:

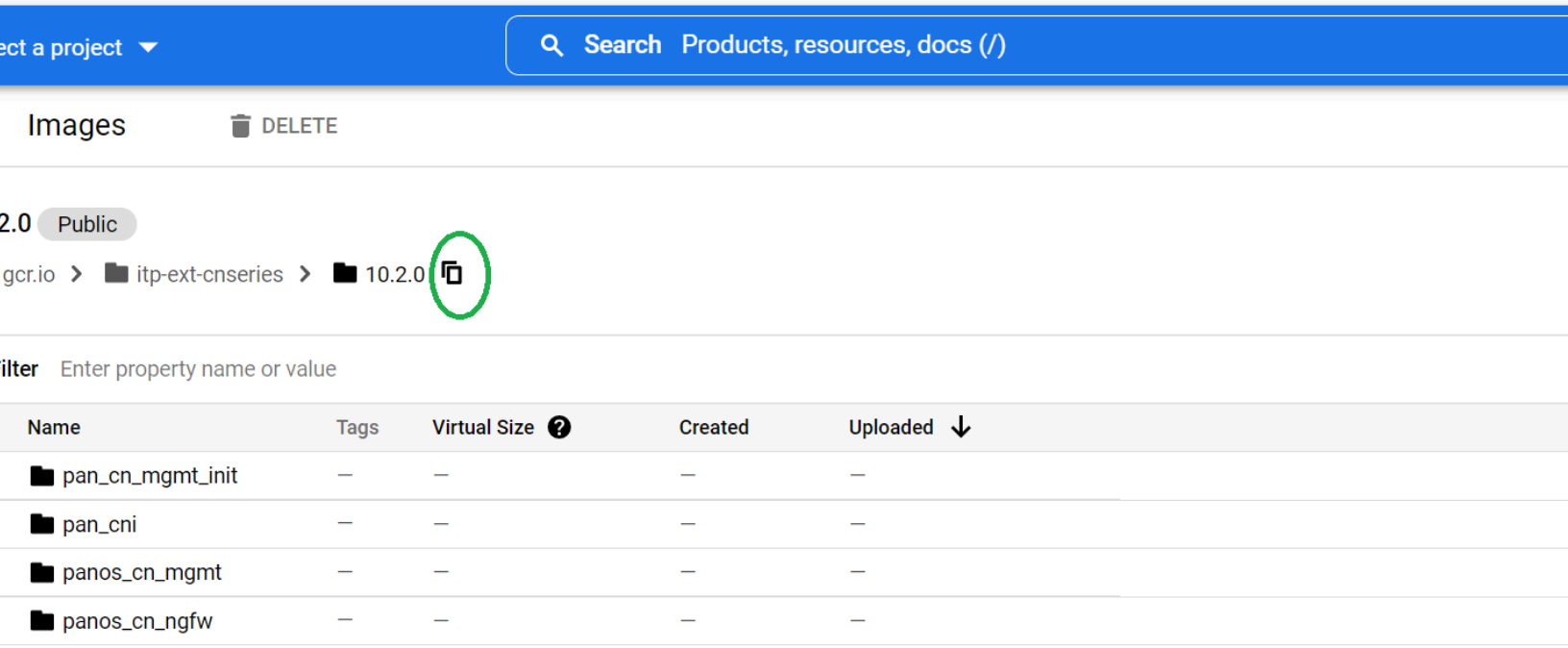
Imágenes de Docker del registro de contenedores públicos:

1. Según su versión de PAN-OS, extraiga las imágenes de Docker necesarias del repositorio de nube pública.



2. Seleccione la versión de PAN-OS requerida.

3. Copie el vínculo de cada ruta de imagen en la ubicación adecuada de los archivos YAML de implementación.



Haga lo siguiente para obtener los archivos YAML de GitHub:

1. Abra la carpeta del método de implementación, DaemonSet, Kubernetes Service o Kubernetes CNF que planifica utilizar.
2. Descargue los archivos yaml de la carpeta que corresponde a su entorno.

   Obtenga los archivos de la carpeta Native-k8s para usarlos con implementaciones nativas de Kubernetes locales o en la nube.

   Obtenga los archivos de la carpeta Kubernetes Gestionado correspondiente para GKE.

Imágenes de Docker del CSP de Palo Alto Networks:

Utilice los siguientes pasos para obtener los archivos YAML de GitHub y descargar las imágenes de docker del CSP de Palo Alto Networks y enviarlas a su registro privado antes de continuar con la implementación del cortafuegos CN-Series.

STEP 1 | Descargue las imágenes de docker y los archivos YAML.

1. Obtenga los archivos tar comprimidos del Portal de atención al cliente (CSP) de Palo Alto Networks.
   1. Inicie sesión en el CSP con su cuenta de asistencia técnica.
   2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.
   3. Seleccione **PAN-OS Container Images (Imágenes de contenedor de PAN-OS)** en el menú desplegable **Please Select (Seleccionar)**.
   4. Descargue los siguientes archivos para la versión de PAN-OS que desea implementar.

      PanOS_cn-X.X.X.tgz - para los pods CN-MGMT y CN-NGFW Pods.

      Pan_cn_mgmt_init-X.X.X.tgz - para el contenedor de inicialización que se ejecuta como parte del Pod CN-MGMT.

      Pan_cni-2.0.0.tgz - para el pod PAN-CNI.
2. Obtenga los archivos YAML de GitHub.
   1. Abra la carpeta del método de implementación,DaemonSet, Kubernetes Service o Kubernetes CNF que planifica utilizar.
   2. Descargue los archivos yaml de la carpeta que corresponde a su entorno.

      Obtenga los archivos de la carpeta Native-k8s para usarlos con implementaciones nativas de Kubernetes locales o en la nube.

      Obtenga los archivos de la carpeta de Kubernetes gestionado correspondiente para AKS, EKS o GKE.

STEP 2 | Recupere las imágenes de docker y envíelas a su registro de contenedores.

Por ejemplo, en una implementación de GKE, subirá las imágenes a un Registro de contenedores en GKE y obtendrá la ruta de la imagen para hacer referencia en los archivos YAML. Utilice los siguientes comandos en un sistema cliente que ejecute el motor de docker.

Reemplace las variables x en los siguientes pasos con los valores que coincidan con la versión de imagen que está utilizando. Por ejemplo, Pan_cn_mgmt-init-2.0.0.tgz o pan_cni:2.0.0.

1. Cargue las imágenes.

   ```
   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
   ```

   Después de estos pasos, "imágenes de docker" mostrará la imagen, por ejemplo, "paloaltonetworks/panos_cn_mgmt:x.x.x".

2. Etiquete estas imágenes para incluir su detalle de registro privado.

   ```
   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. Envíe estas imágenes a su registro privado.

   ```
   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
   ```


Servicio de creación de logs de Strata con cortafuegos CN-series

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Logging Service con cortafuegos CN-series	• Panorama con la versión PAN-OS 11.1 como mínimo • Licencia de Strata Logging Service

Strata Logging Service permite innovaciones basadas en IA para la ciberseguridad con el único enfoque del sector para normalizar y unir los datos de su empresa. Para obtener más información, consulte Introducción a Strata Logging Service y Strata Logging Service para cortafuegos gestionados por Panorama. Strata Logging Service ahora puede recopilar datos de logs del cortafuegos de nueva generación CN-Series. Cuando compra una licencia de Strata Logging Service, todos los cortafuegos registrados en su cuenta de soporte reciben una licencia de Strata Logging Service. También recibirá un enlace mágico que deberá utilizar para activar su instancia de Strata Logging Service.

Para comenzar con el registro de logs de Strata Logging Service para cortafuegos CN-series, debe asegurarse de que Instale el complemento de Kubernetes y configure Panorama para su cortafuegos CN-series. Proporcione el certificado del dispositivo al pod CN-MGMT para la conectividad de Strata Logging Service. Es importante registrar el pod CN-MGMT con una cuenta CSP para asegurarse de que el pod CN-MGMT se refleje en la instancia de Strata Logging Service. Añada el ID de PIN válido y el valor de PIN al archivo `pan-cn-mgmt-secret.yaml` para instalar correctamente el certificado del dispositivo. El cortafuegos CN-series requiere un certificado de dispositivo que autorice el acceso seguro a Strata Logging Service. Para obtener más información, consulte Instalación de un certificado de dispositivo en el cortafuegos CN-Series.

Después de que usted implemente su cortafuegos CN-series, verifique que su pod CN-MGMT esté visible en su cuenta del portal de atención al cliente, en **Dispositivos registrados**. Para obtener más información, consulte Registrar el cortafuegos. Asegúrese de Configurar su cortafuegos CN-Series con Panorama y Crear un perfil de implementación CN-Series en su cuenta CSP, y utilizar el código de autenticación para enviar licencias de Panorama a su cortafuegos CN-Series.

Configuración de Strata Logging Service para el cortafuegos CN-series

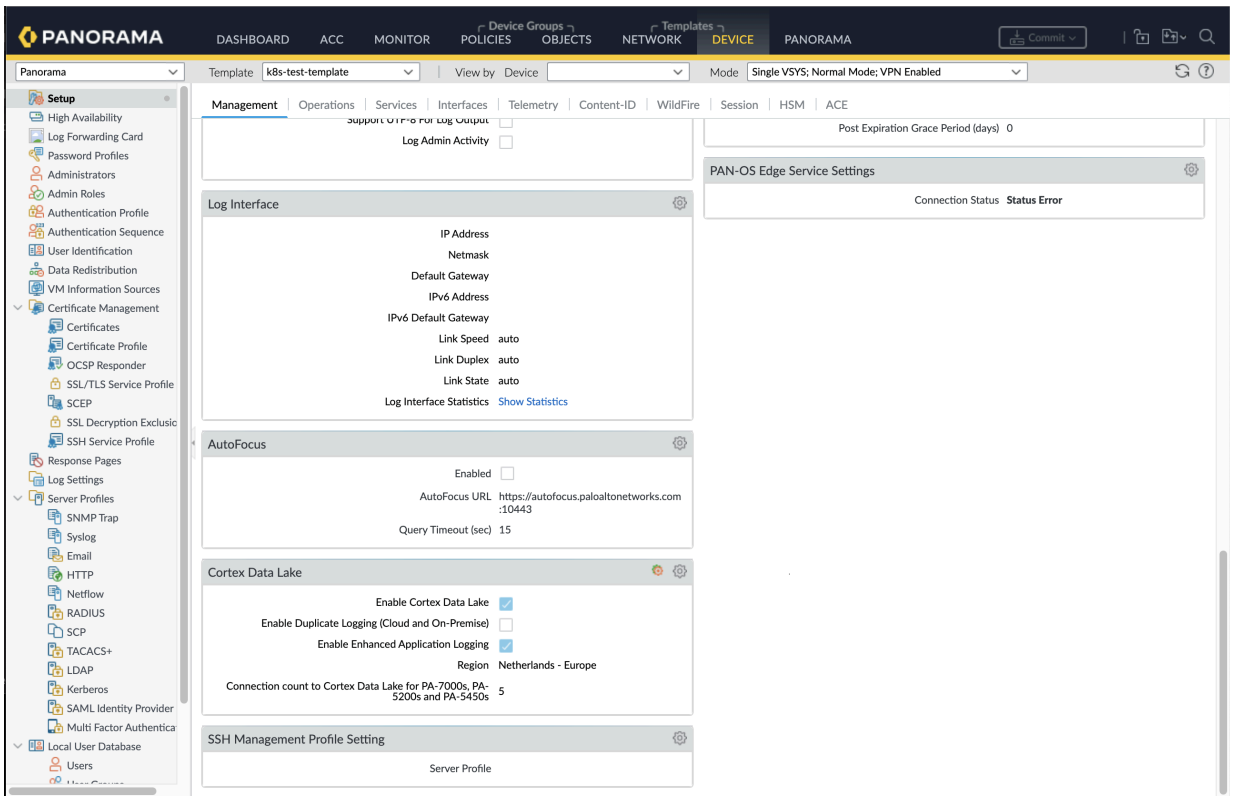
Strata Logging Service proporciona almacenamiento y agregación de logs centralizados y basados en la nube para servicios y aplicaciones proporcionados en la nube.

Asegúrese de que tiene una licencia de registro de logs y una instancia de Strata Logging Service creada en su cuenta de CSP. Para obtener más información, consulte Strata Logging Service.

Complete los siguientes pasos para configurar los ajustes de Strata Logging Service en Panorama y enviarlos al cortafuegos:

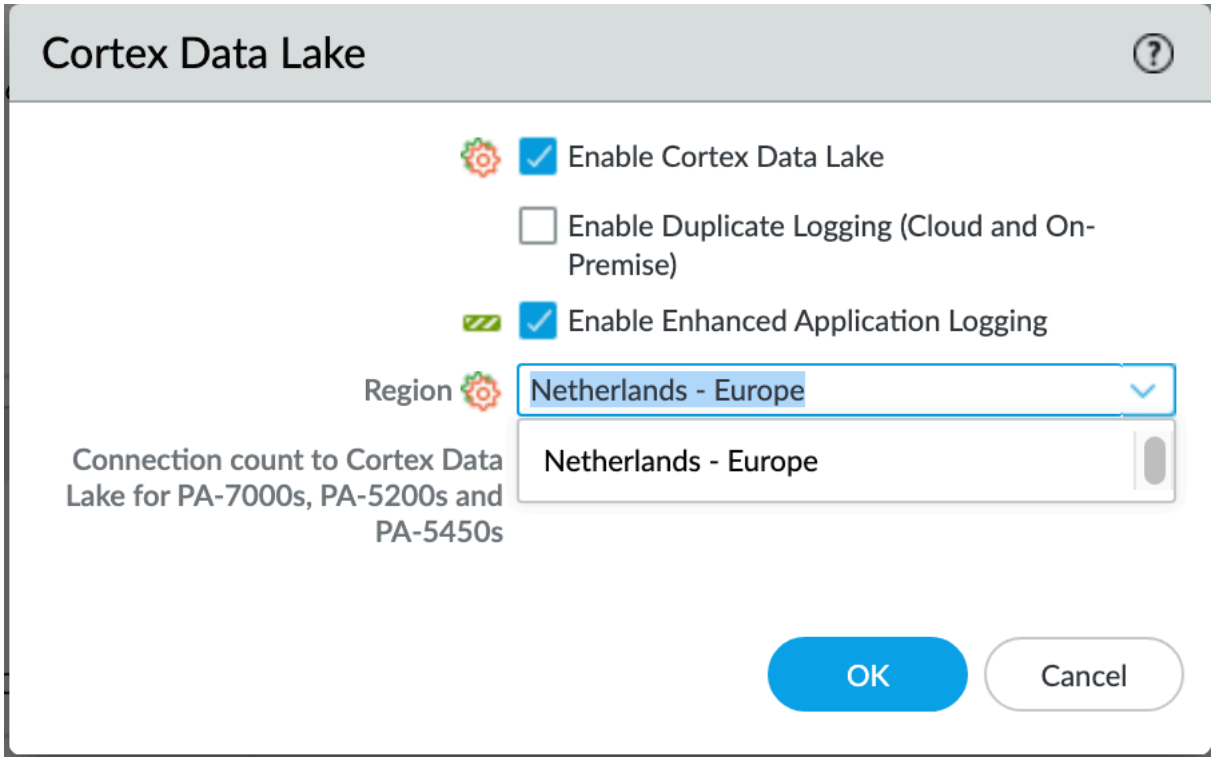
1. Incorpore su Panorama al servicio de Strata Logging Service para habilitar los ajustes de las configuraciones de Strata Logging Service en el dispositivo.
2. Incorporación de su cortafuegos CN-Series a la instancia del Strata Logging Service.

3. En su panorama, vaya a la pestaña**Device (Dispositivo)** y, a continuación, haga clic en **Settings (Configuración)** en el panel **Strata Logging Service**.



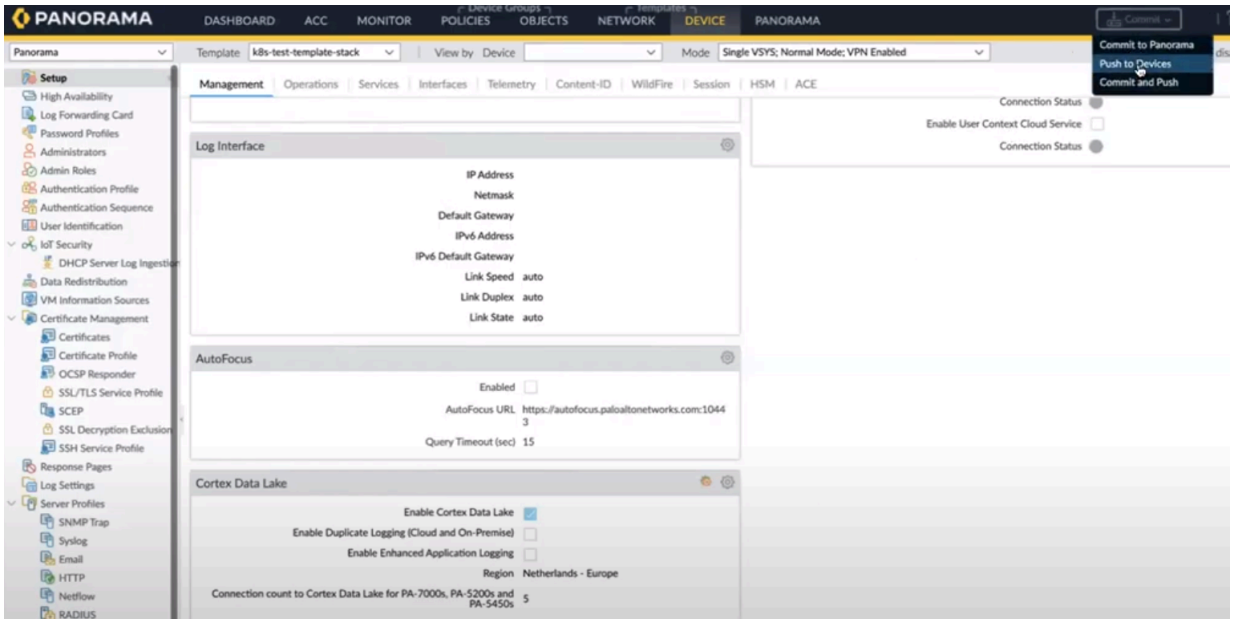
Ahora puede ver que la **Region (Región)** se rellena.

4. Haga clic en **Habilitar Strata Logging Service.** .



5. Haga clic en **OK (Aceptar)**.

6. Vaya a **Confirmar** > **Enviar a dispositivos**.



7. Seleccione su pod de **CN-MGMT**.
8. Haga clic en **Aceptar**.

   La configuración de Strata Logging Service para el pod CN-MGMT ahora se envía. El pod CN-MGMT ahora iniciará su conexión con la instancia de Strata Logging Service.

Una vez que el cortafuegos incorporado esté en un estado **conectado**, puede comenzar a enviar logs a su instancia de Strata Logging Service. Para obtener más información, consulte Comenzar a enviar logs a Strata Logging Service (gestionado por Panorama).

Compatibilidad de IoT Security con el cortafuegos CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• IOT Security para cortafuegos CN-Series	• Licencia de Strata Logging Service para suscripción al IoT que almacena datos en el servicio de strata logging service • Panorama con la versión PAN-OS 11.1 como mínimo

Para el cortafuegos CN-Series de nueva generación de Palo Alto Networks, la solución de IoT Security utiliza el aprendizaje automático (ML) para proporcionar visibilidad de los dispositivos IoT detectados en función de los metadatos de los logs que recibe del cortafuegos. IoT Security también identifica las vulnerabilidades y evalúa el riesgo en los dispositivos en función del comportamiento de su tráfico de red y las fuentes de amenazas actualizadas dinámicamente.

Puede usar las recomendaciones de reglas de políticas que genera IoT Security como referencia al añadir manualmente reglas al cortafuegos CN-Series. IoT Security siempre genera recomendaciones de reglas de políticas de seguridad, independientemente de la versión de PAN-OS.

*Al utilizar la **suscripción de IoT Security**, que almacena datos en Strata Logging Service, necesita una licencia de Strata Logging Service por cuenta y debe asegurarse de que la configuración de* Strata Logging Service *para su cortafuegos CN-series esté completa.*

Para obtener más información, consulte Requisitos previos de IoT Security.

Configurar la compatibilidad de IOT para cortafuegos CN-Series

Debe asegurarse de que su entorno cumple todos los requisitos previos para implementar IoT Security con el cortafuegos CN-Series. Para obtener más información, consulte Requisitos previos de IoT Security.

Para configurar la suscripción de **IoT - Requiere Data Lake** para el cortafuegos CN-series, debe completar los siguientes pasos:

Debe asegurarse de incorporar su Panorama en la instancia del servicio strata logging service. Para obtener más información, consulte Incorporación de cortafuegos con Panorama.

1. Crear un grupo de servicio de inquilinos (TSG). Para obtener más información, consulte el **Paso 3** en Activar suscripciones de IoT Security mediante servicios comunes.
2. Incorporación del inquilino de strata logging service al TSG. Debe asegurarse de comprar el servicio de strata logging service y activarlo mediante Magic link antes de usarlo en TSG.
3. Cree un perfil de implementación de la serie CN-Series con la opción **IoT: requiere Data Lake**.
4. Haga clic en **Finalizar configuración**. Una vez que asocie el perfil de implementación al TSG y haga clic en **Activar**, se creará un inquilino de IoT si aún no existe.

A continuación, puede reenviar los metadatos recopilados al servicio de registro de logs basado en la nube, donde IoT Security los utiliza para identificar varios dispositivos IoT en la red.

5. Aprovisione Panorama y genere un número de serie. Para obtener más información, consulte Registrar Panorama e instalar licencias.
6. Configure su cortafuegos CN-Series con Panorama usando el código de autenticación para enviar licencias de Panorama al cortafuegos CN-Series usando el complemento de kubernetes. Para obtener más información, consulte Configuración de Panorama para proteger una implementación de Kubernetes.

   Aplicar código de autenticación de implementación al complemento de Kubernetes en Panorama.

   Ahora puede ver su cortafuegos CN-series incorporado en un inquilino de IoT.
7. Configure el vwire de plantilla para permitir y habilitar la identificación del dispositivo en la zona.

   Puede utilizar la plantilla predeterminada **K8S-Network-Setup-V2** y realizar los siguientes cambios en dicha plantilla:

   - Habilite el pass-through del estado de enlace y el cortafuegos de multidifusión para el vwire predeterminado.
   - Habilite la identificación del dispositivo para la zona predeterminada.

   Para obtener más información, consulte Configuración de cables virtuales.
8. Configure la opción **Habilitar Cortex Data Lake** y **Habilitar creación mejorada de logs de aplicación** Panorama a cortafuegos CN-Series Para obtener más información, consulte Configuración de Strata Logging Service para el cortafuegos CN-series.

Para configurar la suscripción **IoT Security, no requiere Data Lake** para el cortafuegos CN-Series, debe completar los siguientes pasos:

Nota: Debe asegurarse de incorporar su Panorama en la instancia de strata logging service. Al usar IoT Security, no requiere suscripción a Data Lake, debe registrar su Panorama en el portal de IoT después de añadir el cortafuegos CN-Series. Para obtener más información, consulte el **Paso 2** en Preparación de su cortafuegos para IoT Security.

1. Crear un grupo de servicio de inquilinos (TSG). Para obtener más información, consulte el **Paso 3** en Activar suscripciones de IoT Security mediante servicios comunes.
2. Crear un perfil de implementación de la serie CN-Series con la opción **IoT: no requiere Data Lake**.
3. Configure la instancia de IOT y seleccione la opción **Finalizar configuración**y para asociar el perfil de implementación con el grupo de servicios de inquilino (TSG) para habilitar el servicio de registro de logs en el cortafuegos CN-Series y configurarlo para obtener y registrar metadatos de tráfico de red. Para obtener más información, consulte Preparación de su cortafuegos para IoT Security.

   A continuación, puede reenviar los metadatos recopilados al servicio de registro de logs basado en la nube, donde IoT Security los utiliza para identificar varios dispositivos IoT en la red.
4. Aprovisione Panorama y genere un número de serie. Para obtener más información, consulte Registrar Panorama e instalar licencias.
5. Configure su cortafuegos CN-Series con Panorama usando el código de autenticación para enviar licencias de Panorama al cortafuegos CN-Series usando el complemento de kubernetes. Para obtener

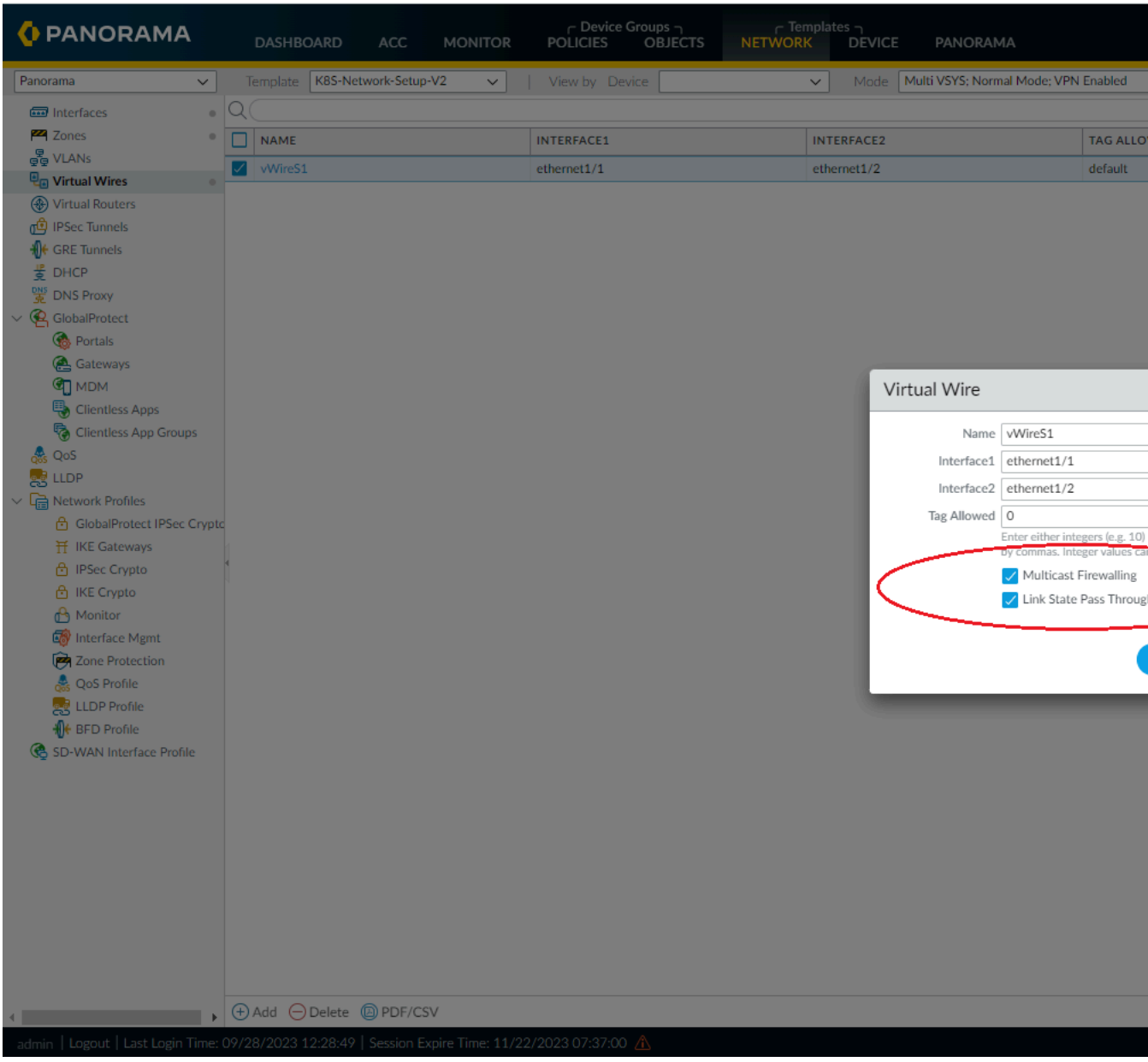
más información, consulte Configuración de Panorama para proteger una implementación de Kubernetes.

Aplicar código de autenticación de implementación al complemento de Kubernetes en Panorama. Ahora puede ver su cortafuegos CN-series incorporado en un inquilino de IoT.

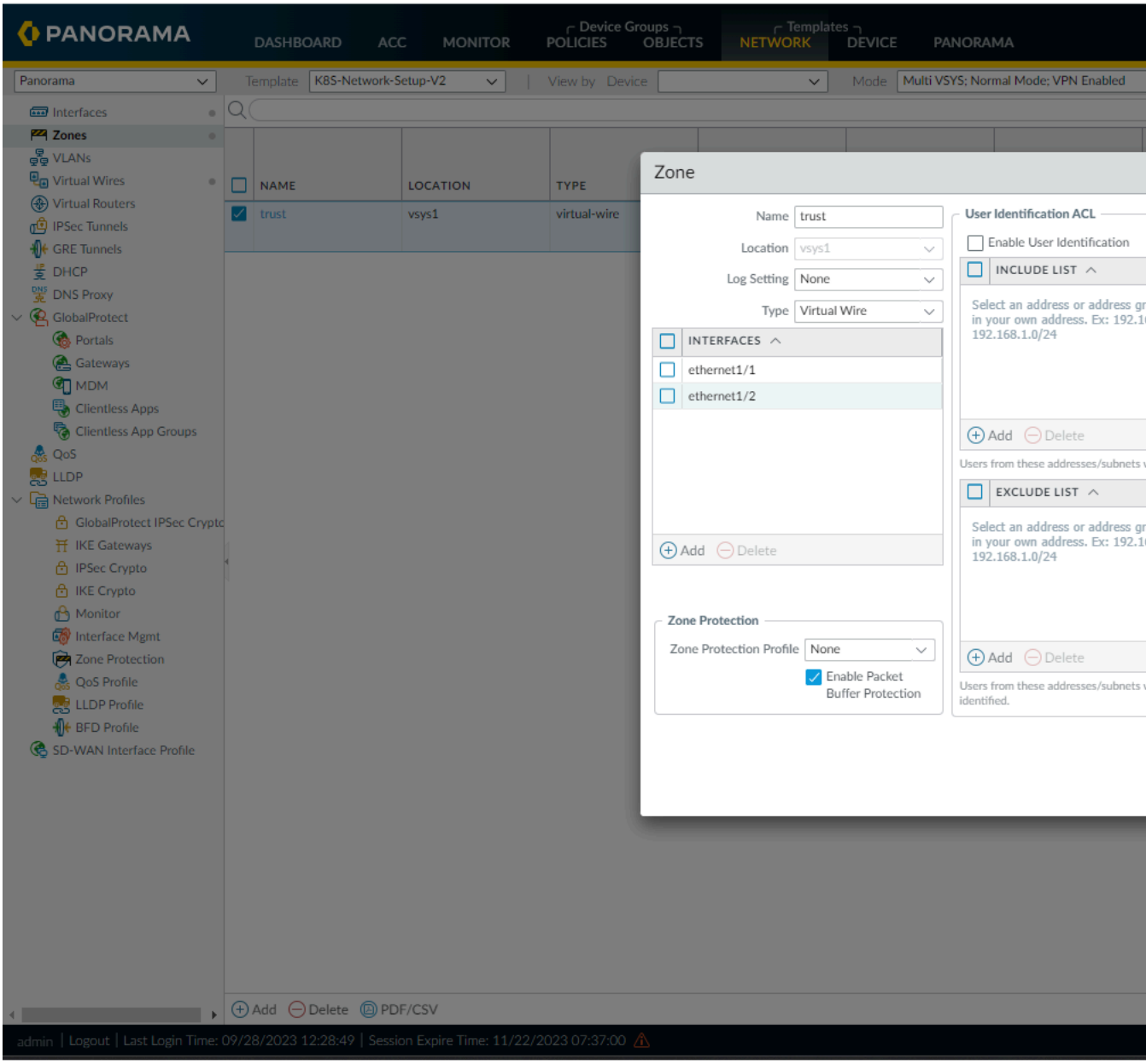
6. Configure el vwire de plantilla para permitir y habilitar la identificación del dispositivo en la zona. Para obtener más información, consulte Configuración de cables virtuales.

   Puede utilizar la plantilla predeterminada **K8S-Network-Setup-V** y realizar los siguientes cambios en dicha plantilla:

   - Habilite el pass-through del estado de enlace y el cortafuegos de multidifusión para el vwire predeterminado.



   - Habilite la identificación del dispositivo para la zona predeterminada.



Para obtener más información, consulte Configuración de cables virtuales.

Vwire configurado en k8s-template-v2 permite el paso del estado del enlace y el cortafuegos multidifusión. La configuración de zona de k8s-template-v2 permite la identificación de dispositivos

7. Configure la opción **Habilitar Cortex Data Lake** y **Habilitar creación mejorada de logs de aplicación** Panorama a cortafuegos CN-Series Para obtener más información, consulte Configuración de Strata Logging Service para el cortafuegos CN-series

Una vez que haya incorporado correctamente Panorama y el cortafuegos CN-Series en el servicio de registro de logging basado en la nube, vaya a la instancia de IoT.

Una vez que IoT Security tiene suficiente información para identificar los dispositivos a partir de su comportamiento de red, proporciona al cortafuegos CN-Series asignaciones de direcciones IP a

dispositivos y a Panorama recomendaciones de políticas que el administrador de Panorama puede importar y, a continuación, enviar al cortafuegos CN-Series para aplicar la política en el tráfico de dispositivos IoT.

Haga clic en **Gestión** > **Sitios y cortafuegos** > **Cortafuegos** en el portal de IoT Security para ver el estado de los logs que el servicio de registro de logs está transmitiendo a la aplicación de IoT Security. Para obtener más información, consulte Estado de la integración de IoT Security con el cortafuegos.

Descarga basada en software de corte en cortafuegos CN-Series

¿Dónde puedo usar esto?	¿Qué necesito?
• CN-Series como implementación de CNF de Kubernetes	• CN-Series 10.1.x or above Container Images • Para Panorama gestionado, cortafuegos CN-Series, Panorama con PAN-OS 11.0.4 o versión superior

Descripción general

Con el servicio de descarga inteligente de tráfico (ITO) basado en el software de corte, el cortafuegos CN-Series elimina el compromiso entre el rendimiento, la seguridad y el coste de la red. Para cada nuevo flujo en la red, el servicio ITO determina si el flujo puede beneficiarse o no de la inspección de seguridad. El servicio ITO enruta los primeros paquetes del flujo al cortafuegos para su inspección y este determina si inspeccionar o descargar el resto de los paquetes en el flujo. Esta determinación se basa en la política o en la incapacidad del flujo para inspeccionar. Al inspeccionar únicamente los flujos que se pueden beneficiar de la inspección de seguridad, la carga general en el cortafuegos se reduce y el rendimiento aumenta sin sacrificar la postura de seguridad.

Para las infraestructuras que carecen de DPU, el ITO basado en el software de corte puede funcionar aprovechando las NIC disponibles. Consulte Hypervisor Support Matrix para obtener información sobre las NIC y los hipervisores compatibles.

La descarga basada en software de corte es compatible con el protocolo de túnel GTP-U. Dentro de un GTP-U con Universal Time-through coordinado de software de sesión interna GTPU coordinado, después de que la sesión interna de GTPU complete la inspección de capa 7, el paquete de GTPU seguirá la ruta de datos de corte de software existente, evitará las operaciones innecesarias, aprovechará una caché FIB/MAC y se ejecutará hasta su finalización. El cortafuegos CN-Series es compatible con la función de software de corte de PAN-OS para la descarga de tráfico específica de GTP-U al implementar el cortafuegos CN-Series como un servicio CNF de Kubernetes.

Descarga de tráfico específica de GTP-U en cortafuegos CN-series

GTP comprende un plano de control (GTP-C), plano de usuario (GTP-U) y tráfico de tarificación (GTP' derivado de GTP-C) transferido en UDP/IP. Consulte las versiones de PAN-OS por modelo compatible con GTP y los estándares técnicos 3GPP que admiten GTPv1-C, GTPv2-C y GTP-U. Habilitar la seguridad GTP en cortafuegos Palo Alto Networks® le permite proteger la infraestructura de la red central móvil de paquetes GTP mal formados, ataques de denegación de servicio y mensajes GTP de fuera del estado, y también le permite proteger a los suscriptores móviles de paquetes IP falsos y ataques de sobrefacturación.

GTP-U se define en 3GPP TS 29.281. Este encapsula y enruta el tráfico del plano de usuario a través de múltiples interfaces de señalización como S1, S5 y S8. Los mensajes GTP-U son planos de usuario o mensajes de señalización. El número de puerto registrado para GTP-U es 2152. Para obtener más información, consulte Perfil de protección GTP.

La descarga basada en software de corte en la serie CN-Series también admite descargas de tráfico GTP-U. Ahora puede utilizar la suscripción de descarga de tráfico inteligente en la serie CN-Series como modo CNF de Kubernetes para desbloquear más rendimiento y proteger las redes móviles que aprovechan la seguridad GTP. Para cada paquete GTP-U que inspeccionará el CN-Series como modo CNF de Kubernetes, se completará una inspección completa de Capa 7 en las sesiones internas. Si el cortafuegos determina que las sesiones internas de este paquete GTP-U cualifican para descargarse, entonces todos los paquetes GTP-U posteriores que pertenecen a esta sesión se descargarán.

Los siguientes son los puntos importantes a considerar antes de configurar la descarga basada en software de corte en un cortafuegos CN-series:

- De forma predeterminada, las configuraciones ITO basadas en software de corte están deshabilitadas.
- Puede habilitar esta función solo con bootstrap/CLI.
- Puede usar el ITO basado en software de corte para tráfico plano y descarga de GTP-U dentro del ITO basado en software de corte de forma simultánea.
- Para actualizaciones de la versión actual con ITO habilitado, habilite la descarga de sesiones mediante la actualización de publicaciones de CLI.

En la serie CN-Series, solo el modo de implementación CNF de CN-series como Kubernetes admite ITO basadas en software de corte.

Habilitar las descargas de sesiones internas de GTP-U en el cortafuegos CN-series

Para habilitar las descargas de sesiones internas de GTP-U en el cortafuegos CN-series, los siguientes son los requisitos previos para habilitar GTP Security o 5G Security.

Debe editar el archivo **`pan-cn-mgmt-configmap.yaml`** con los siguientes cambios:

En el archivo `pan-cn-mgmt-configmap.yaml`, el valor de parámetro `PAN_GTP_ENABLED, PAN_GTP_CUT_THRU y PAN_SW_CUT_THRU` debe ser `verdadero` para habilitar las descargas internas de sesión de GTP-U.

Este es un ejemplo de un archivo `pan-cn-mgmt-configmap.yaml` actualizado:

```
# Start MGMT pod with GTP enabled. For complete functionality, need
 GTP # enabled at Panorama as well. 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"
```

