paloalto TECHDOCS

CN-Series 使用入门

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

适用于 Kubernetes 的 CN-Series 防火墙

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

Palo Alto Networks 容器本机防火墙 (CN-Series) 可原生集成到 Kubernetes (k8s)，以提供完整的 L7 可见性、应用程序级别分段、DNS 安全，并为跨公共云或数据中心环境中受信任区域的流量预防高级威胁。它能够让您隔离和保护工作负载、应用程序堆栈和服务，甚至作为单个容器进行扩展、缩减或跨主机，并且可以始终应用基于 Kubernetes 标签的安全策略。

Kubernetes 环境中的应用程序部署是动态的，以下团队通常会参与容器生命周期：

- **Platform (PAAS) Admin**（平台 **(PAAS)** 管理员）— 在公共云和数据中心中管理 Kubernetes 集群和其他基础架构组件。
- **App Teams**（应用团队）— 在 PAAS 管理员提供的 Kubernetes 命名空间/项目中部署其各自的容器化应用程序和其他应用程序。
- **Security Admin**（安全管理员）— 为整个部署配置安全保护，包括 Kubernetes 集群和单个容器化应用程序。

在此动态场景中并与多个团队互动时，安全管理和监控都可能会带来挑战。使用 CN-Series 防火墙，安全管理员可为各种环境中的容器化应用程序配置安全保护，包括云提供商托管的 k8s（例如 GKE、EKS、AKS）、客户托管的 k8s（例如 Openshift）和公共云或本地数据中心中的 Native k8s。CN-Series 防火墙使用 Kubernetes 结构体和元数据驱动型策略，以便各个团队可以自动化部署并有效实施安全策略，从而始终如一地预防已知和未知的威胁。

使用 CN-Series 防火墙保护 Kubernetes 工作负载

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

CN-Series 防火墙部署为两组 Pod：一组用于管理平面 (CN-MGMT)，另一组用于防火墙数据平面 (CN-NGFW)。防火墙数据平面作为 DaemonSet 运行，允许 Kubernetes 内部的单个命令同时在 Kubernetes 集群的所有节点上部署防火墙。管理平面作为 Kubernetes 服务运行。

CN-Series 防火墙通过 Panorama 控制台进行管理。Panorama 中的 Kubernetes 插件提供有关环境中容器的上下文信息，从而无缝地实现基于上下文的网络安全策略。

例如，Kubernetes 命名空间可用于定义防火墙策略中的流量源。您可以在本地或公共云托管的 Kubernetes 环境中部署 CN-Series 防火墙。

CN-Series 防火墙还可以部署到云托管的 Kubernetes 产品中，包括 Google Kubernetes Engine (GKE®)、Azure Kubernetes 服务 (AKS)、Alibaba Cloud (ACK) 和 Amazon Elastic Kubernetes 服务 (EKS)。您还可以通过 Kubernetes 包管理器（例如 Helm）进行部署。

CN-Series 可为容器信任区域和其他工作负载类型之间的入站、出站和东向西流量提供威胁防护，而不会减慢开发速度。

将 CN-Series 部署到第 7 层可查看容器流量，并使用预防威胁配置文件实施安全策略，以保护跨 Kubernetes 命名空间边界的允许流量，以及与硬件和 VM 系列防火墙共享该上下文，以确保在整个混合云环境中使用一致的策略实施模型。

防止 **Kubernetes** 环境数据泄露：

CN-Series 防火墙提供多种安全功能，以防止敏感数据从 Kubernetes 环境中泄露。流量内容检查（包括 TLS/SSL 加密流量的检查）可确保识别并修复包含恶意负载的数据包。URL 过滤禁止与潜在恶意网站（包括恶意代码存储库）的出站连接。

防止威胁跨越 **Kubernetes** 命名空间边界的横向传播：

应用程序之间的信任边界是实施分段策略以防止威胁横向移动的逻辑位置。在许多 Kubernetes 环境中，Kubernetes 命名空间是信任边界。CN-Series 防火墙可以在 Kubernetes 命名空间之间以及 Kubernetes 命名空间与其他工作负载类型（例如虚拟机和裸机服务器）之间实施威胁预防策略，以阻止威胁在您的云原生应用程序和您的传统基础设施之间移动。

CN-Series 密钥概念

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

CN-Series 防火墙旨在提供保护容器化环境中的应用程序所需的工具。要了解 CN-Series 如何适应容器化网络，理解一些关键概念非常重要。

- 集群 — 容器化环境的基础；所有容器化应用程序都在集群上运行。
- 节点 — 根据集群，节点可能是虚拟机或物理机，其中包含 Pod 所需的必要服务。
- **Pod** — 可在 Kubernetes 中部署和管理的最小的可部署计算单元。CN-Series 防火墙作为两个 Pod 部署在分布式 PAN-OS 架构中：CN-MGMT 和 CN-NGFW。有关更多信息，请参阅 CN-Series 核心构建块。
- 命名空间 — 命名空间是一个由物理集群支持的虚拟集群。在许多用户分布在多个团队和职能部门的环境中，可以使用命名空间将他们分在一个集群上。
- 容器网络接口 **(CNI)** — 一个为容器配置网络接口的插件。此外，删除容器时，CNI 会删除分配的用于网络的资源。
- **DaemonSet** — 在 Kubernetes 部署中，DaemonSet 确保部分或所有节点运行特定 Pod 的副本。随着将节点添加到 Kubernetes 集群，DaemonSet 定义的 Pod 的副本也会添加到每个新节点。将 CN-Series 防火墙部署为 DaemonSet 时，CN-NGFW Pod 的副本会部署在集群中的每个节点上（每个 CN-MGMT 对最多 30 个）。
- **Kubernetes** 服务 — 一种抽象，将在一组 Pod 上运行的应用程序公开为网络服务。将 CN-Series 部署为服务时，部署的 CN-NGFW Pod 的数量由您在设置 yaml 文件时定义。
- **Kuberenetes CNF** — 部署 CN-series-as-a-kubernetes-CNF 解决了通过外部实体（例如云提供商的本机路由、vRouters 和架顶式 (TOR) 交换机等）使用服务功能链 (SFC) 的流量所面临的这些挑战。CN-series-as-a-kubernetes-CNF 部署模式不会影响应用程序 Pod。
- **Horizontal Pod Autoscaler (HPA)** — 根据各种指标（例如 CPU 利用率或会话利用率）自动扩展部署、副本集或状态集中的 Pod 数量。

  HPA 仅在作为 *Kubernetes* 服务的 *CN-Series* 上受支持。

- **HSF** — Palo Alto Networks CN-Series Hyperscale Security Fabric (HSF) 1.0 是新一代容器化防火墙集群，可为部署 5G 网络的移动服务提供商提供高度可扩展且具有弹性的新一代防火墙解决方案。

CN-Series 核心构建块

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN-Series 的 Helm 3.6 or above version client

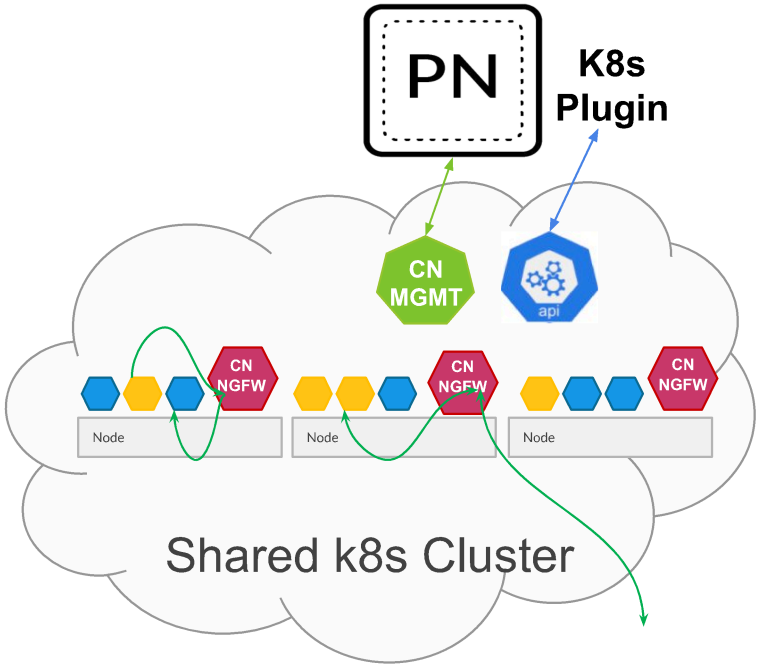
CN-Series 防火墙是容器化的下一代防火墙，可为 Kubernetes 集群中的容器化应用程序工作负载提供更好的可见性和安全性。CN-Series 防火墙使用 Native Kubernetes (K8s) 构造和 Palo Alto Networks 组件使之成为可能。

部署 CN-Series 防火墙的核心构建块是：

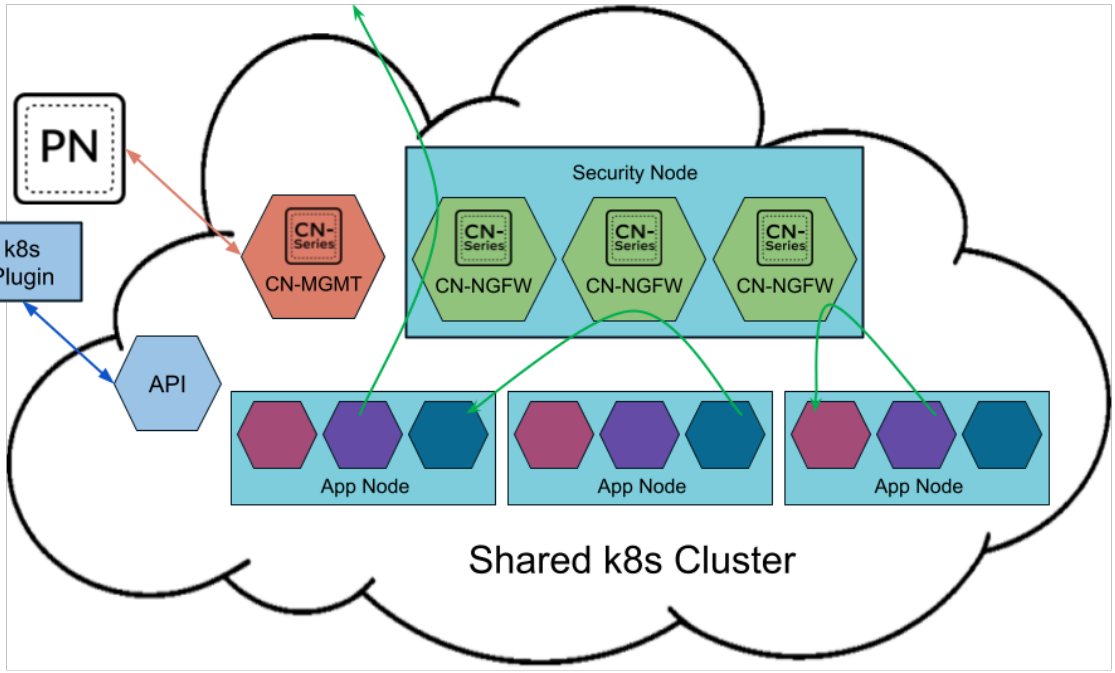
- **CN-Series Deployment Files**（**CN-Series** 部署文件）— 要在容器化环境中部署 CN-Series，您必须下载并部署各种 CN-Series 部署文件。
  - PAN-CN-MGMT— Init 容器将生成证书，这些证书可用于保护 CN-MGMT Pod 的实例之间以及 CN-MGMT Pod 和 CN-NGFW Pod 之间的通信。
  - PAN-CN-MGMT-CONFIGMAP
  - PAN-CN-MGMT-SECRET — 允许 Panorama 对防火墙进行验证，以便将每个防火墙添加为托管设备。部署生命周期必须提供 VM 身份验证密钥。如果连接请求中没有有效密钥，则 CN-Series 防火墙将无法注册到 Panorama。
  - PAN-CN-NGFW
  - PAN-CN-NGFW-CONFIGMAP
  - PAN-CNI
  - PAN-CNI-CONFIGMAP
  - PAN-CNI-MULTUS
- **Distributed PAN-OS architecture with CN-MGMT and CN-NGFW Pod**（具有 **CN-MGMT** 和 **CN-NGFW Pod** 的分布式 **PAN-OS** 基础架构）— 容器化防火墙的管理平面 (CN-MGMT) 和数据平面 (CN-NGFW) 是独立的，可为应用程序启用更好的运行时保护并支持更小的占用空间。使用具有 ConfigMap 对象的容器映像和 YAML 清单文件部署 CN-MGMT 和 CN-NGFW。
- 将 **CN-MGMT** 作为 StatefulSet 运行可确保具有持久卷，并作为可在 Kubernetes 环境中使用 DNS 发现的 K8s 服务公开。CN-MGMT 可提供容错功能，并且在 CN-MGMT Pod 重新启动或发生故障时单个 CN-MGMT Pod 可管理现有的 CN-NGFW Pod。

- **CN-NGFW** 可以部署为 DaemonSet 或 Kubernetes Service。DaemonSet 部署适用于具有较大节点且需要低延迟和/或需要高防火墙容量的 Kubernetes 环境。作为 Kubernetes 服务的 CN-Series 适用于具有较小节点和/或需要更动态的防火墙的 Kubernetes 环境。
  - 当部署为 **DaemonSet** 时，CN-NGFW Pod 的每个实例可以保护在同一节点上运行的 30 个应用程序 Pod。使用该基础架构，您可以将 CN-NGFW DaemonSet Pod 放置在要保护集群中

工作负载的每个节点上，一对 CN-MGMT Pod 可以连接到并最多管理集群中的 30 个 CN-NGFW Pod。有关限制的详细信息，请参阅CN-Series 的性能和扩展性。



- 当部署为 **Kubernetes** 服务时，CN-NGFW 的实例可以部署在安全节点上，而应用程序 Pod 流量将被重定向到可用的 CN-NGFW 实例以进行检查和实施。



- **PAN-CNI plugin for network insertion**（适用于网络插入的 **PAN-CNI** 插件）— PAN-CNI 插件负责在每个 Pod 上分配网络接口，从而启用与 CN-NGFW Pod 的网络连接。使用 YAML 文件可以部署包含 PAN-CNI DaemonSet 的 CN-Series，从而将 PAN-CNI 插件插入集群中每个节点上的 CNI 插件链。该插件将在每个应用程序 Pod 出现时读取其注释，以确定是否启用安全性，并在流量进出 Pod 时将其重定向到 CN-NGFW Pod 进行检查。

- **Panorama for centralized management**（用于集中管理的 **Panorama**）— Panorama 可用作管理容器化防火墙的配置和许可的中心。同时，还可托管 Kubernetes 插件，从而启用对 Kubernetes 集群的监控，并进行集中式安全策略管理。您可以使用物理或虚拟 Panorama 设备，并将其部署在本地或公共云环境中。Panorama 必须与防火墙管理平面 Pod (CN-MGMT) 建立网络连接，以确保可以许可 (CN-NGFW) 防火墙，并使用 Panorama 模板和设备组推送配置和策略。Palo Alto Networks 建议您在高可用性配置中部署 Panorama。

  您需要标准 Kubernetes 工具（例如 kubectl 或 Helm）部署和管理 Kubernetes 集群、应用程序和防火墙服务。Panorama 并非旨在成为 Kubernetes 集群部署和管理的 Orchestrator。托管 Kubernetes 提供商已提供用于集群管理的模板。您还可以使用社区支持的模板部署具有 Helm 和 Terraform 的 CN-Series 。

- **Kubernetes Plugin on Panorama**（**Panorama** 上的 **Kubernetes** 插件）— Kubernetes 插件可管理 CN-Series 防火墙的许可证。许可基于您选择分配给 CN-NGFW Pod 的内核数量。每个 CN-NGFW Pod 都使用许可证令牌，并且在激活授权代码并从 Palo Alto Networks 许可证服务器检索指定数量的令牌后，将在 Panorama 上本地管理令牌。当每个 CN-NGFW 出现在 Kubernetes 节点上时，Panorama 将在本地分发许可证令牌。

  使用 Panorama 上的 Kubernetes 插件还可监控并利用用于组织 Kubernetes 对象（例如 Pod、服务、部署和关联标识属性）的 Kubernetes 标签，以便创建上下文感知的安全策略规则。Kubernetes 插件近实时地与 API 服务器通信并检索元数据，以了解集群中运行的应用程序。Kubernetes 插件可从 Kubernetes 集群收集命名空间、服务和标签，为集群中关联对象的 IP 地址到标签映射创建标签，然后可将其用于安全策略。有关详细信息，请参阅 Kubernetes 属性的 IP 地址到标签映射。

  同时，该插件还会在应用程序 YAML 文件中指定的端口上收集信息，并创建服务对象。

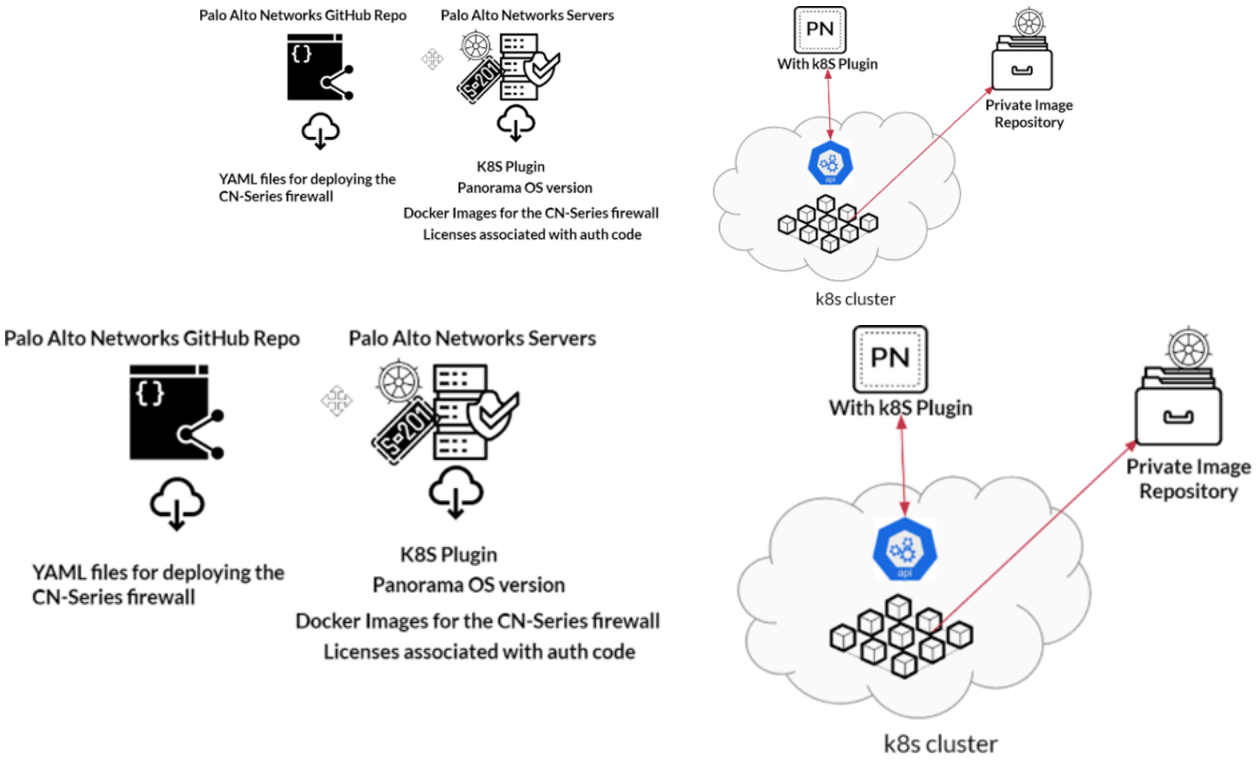
  当这些标签和服务对象自动与每个集群中的 CN-NGFW Pod 共享时，您还可以启用与基于硬件或 VM 系列防火墙共享的标签和服务对象。这些标签可用作动态地址组中的匹配条件，然后您可以用于保护 Pod 或命名空间与 Internet 公开的服务或出站连接之间的流量。

  Palo Alto Networks 建议在高可用性配置中部署 Panorama，以便 Panorma 对等在发生故障时可继续接收 IP 地址更新。如果部署单个 Panorama 实例，则在发生故障时不会影响来自任何现有应用程序 Pod 的流量，并且会在 CN-NGFW Pod 上执行当前策略。当出现新的 Pod 时，所有带有“任何”源的规则都将与此新 Pod 匹配，并且将根据策略规则允许或阻止来自此新 Pod 的流量。例如，如果有防间谍软件策略规则阻止从任何源到外界的出站访问，则会将此规则应用于新 Pod，并且配置文件可以保护流量。如果有默认的拒绝规则，则将拒绝来自此新 Pod 的流量。

  您可以使用 *Kubernetes* 插件将 *Kubernetes* 集群中部署的 *Pod*、节点、命名空间和服务的 *IP* 地址到标签映射分发到物理或 *VM* 系列防火墙，即使在该集群中未部署 *CN-Series* 防火墙。

使用 CN-Series 防火墙保护 Kubernetes 集群所需的组件

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN-Series 的 Helm 3.6 or above version client



以下是部署 CN-Series 防火墙和保护 Kubernetes 集群中部署的应用程序所需资源的列表。

- **Panorama** — 可以连接到 Kubernetes 集群的基于硬件的设备或虚拟设备，该集群中已部署应用程序和 CN-Series 防火墙。CN-Series 防火墙的许可证管理和配置管理需要使用 Panorama。有关详细信息，请参阅CN-Series 核心构建块。
- **Kubernetes Plugin on Panorama**（**Panorama** 上的 **Kubernetes** 插件）— 由于容器化应用程序的更改速度，因此查看集群中的容器活动，以及管理集群中每个节点上部署的防火墙的许可证令牌分配需要使用该插件。

  Kubernetes 插件使用服务帐户凭据连接到 Kubernetes 集群。使用该插件可检索资源属性和标签，并创建标签和服务对象。这些标签可用于创建动态地址组，并在 IP 流量实施的安全策略中

加以引用。您还可以使用安全策略中的服务对象，根据端口和 IP 地址允许或拒绝流量。这些标签和服务对象可用于查看并更好地控制 Kubernetes 集群中的流量实施。

- **Docker Images**（**Docker** 映像）— 为了支持分布式基础架构，CN-Series 防火墙具有 Palo Alto Networks 门户提供的四个 Docker 映像。这些映像作为三个压缩的 tar 存档文件（tar.gz 格式）发布，您必须解压缩这些映像并通过 Docker 将其推送到映像注册表。

  注意：确保映像和 YAML 文件版本兼容。压缩的文件包括：

  - **PanOS_cn-10.1.0.tgz** — 该存档文件包括防火墙管理平面 (CN-MGMT) 和防火墙数据平面 (CN-NGFW) 映像。

    例如，解压缩后的映像名称为：`panos_cn_ngfw:10.1.0-b7` 和 `panos_cn_mgmt:10.1.0-b7`

    - **Pan_cn_mgmt_init-2.0.0.tgz** — 该存档文件包括 init 容器 (CN-INIT)，其中包含防火墙上部署管理平面所需的实用程序。使用 init 容器可保护 CN-MGMT 和 CN-NFGW Pod 之间的 IPSec 通信。例如，解压缩后的映像名称为：`pan_cn_mgmt_init:1.0.0-b1-c1`。
    - **Pan_cni-2.0.0-<xn>.tgz** — 该存档文件包括 CNI 插件，使用该插件可在 CN-MGMT 和 CN-NFGW 之间建立连接，并重新配置应用程序 Pod 上的网络接口，以将流量重定向到每个节点上的 CN-NGFW Pod。例如，解压缩后的映像名称为：`pan_cni:2.0.0`。

上面列出的映像名称只是示例，在最新版本中将发生变化。您可以在 Palo Alto Networks 门户上找到最新的映像。

- **YAML Files**（**YAML** 文件）— YAML 文件在 GitHub 上发布，其中包含用于在 Kubernetes 集群中部署资源的必填字段和对象规范。

  为方便起见，将支持环境（例如 Native Kubernetes 或 GKE）所需的所有 YAML 文件合并且压缩在一个文件夹中。

  YAML 文件通过 *HELM* 图表自动部署，这是部署 *CN-Series* 防火墙的推荐方法。

  - CN-MGMT 有三个 YAML 文件 — `pan-cn-mgmt.yaml`、`pan-cn-mgmt-configmap.yaml`、`pan-cn-mgmt-secret.yaml`、`pan-cn-mgmt-slot-cr.yaml` 和 `pan-cn-mgmt-slot-crd.yaml`。
  - CN-NGFW 包含两个 YAML 文件 — `pan-cn-ngfw.yaml` 和 `pan-cn-ngfw-configmap.yaml`。除了前面提到的文件，作为 Kubernetes 服务的 CN-NGFW 还有 `pan-cn-ngfw-svc.yaml`。
  - CNI 插件包含三个 YAML 文件 — `pan-cni-configmap.yaml`、`pan-cni.yaml` 或 `pan-cni-multus.yaml`。

    如果要在具有作为元插件的 Multus CNI 的环境中部署 CN-Series，并调用其他 CNI 插件，则必须选择 `pan-cni.yaml` 或 `pan-cni-multus.yaml` 文件。

    在 OpenShift 上部署 CN-Series 时，默认启用 Multus，因此使用 pan-cni.yaml 已足够。但是，如果在支持 Multus CNI 但为可选的环境中部署 CN-Series，请使用 pan-cni-multus.yaml 而不是 pan-cni.yaml。

    - 在下面的服务帐户创建部分中还可引用 *`pan-cni-serviceaccount.yaml`* 文件。
    - 对于 *OpenShift* 部署，可使用其他 *`pan-cni-net-attach-def.yaml`* 文件。

- **Service Account Creation**（服务帐户创建）— 三个 YAML 文件：`pan-mgmt-serviceaccount.yaml`、`pan-cni-serviceaccount.yaml` 和 `plugin-serviceaccount.yaml`。

  `pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml` 文件用于 CN-MGMT 和 CN-NGFW Pod，以对集群进行身份验证。

  `plugin-serviceaccount.yaml` 文件用于 Panorama 上的 Kubernetes 插件，以对集群进行身份验证。

- **Persistent volume YAML for Native Kubernetes deployments**（适用于 **Native Kubernetes** 部署的持久卷 **YAML**）— `pan-cn-pv-manual.yaml` 和 `pan-cn-pv-local.yaml` 文件。

  `pan-cn-pv-manual.yaml` 文件仅为具有单个节点集群的 PoC 提供。Palo Alto Networks 强烈建议使用动态配置的持久卷存储 `pan-cn-mgmt.yaml` 文件中引用的 CN-MGMT Pod 的配置和日志。确保在集群中为两个 CN-MGMT Pod 设置一个持久卷。

- **License auth code**（许可证授权代码）— 授权代码用于许可在集群中每个节点上部署的每个 CN-NGFW Pod 实例。

  许可证身份验证代码与在 Palo Alto Network CSP 上创建的 CN-Series 部署配置文件相关联。此外，它还会启用创建部署配置文件时选择的任何安全订阅。

其他 CN-Series 资源

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

您可以使用以下资源详细来了解 CN-Series 防火墙以及它如何帮助保护容器化网络。

- CN-Series 防火墙 — 观看这些视频以了解 CN-Series 防火墙。
- CN-Series 的原因、内容和方式 — Palo Alto Networks 直播社区上的三部分博客系列（带有嵌入式视频），描述了 CN-Series 防火墙的原因、内容和方式。
- Palo Alto Networks Qwiklabs — 使用 alo Alto Networks Qwiklab 进行实验练习，然后在 AWS 或 GCP 中尝试 CN-Series 防火墙。
- 适用于 Kubernetes 的 Panorama 插件发行说明 — 阅读发行说明，了解最新版本的 Kubernetes Panorama 插件中引入的功能和增强功能。
- PAN-OS 发行说明 — 查看 PAN-OS 发行说明，了解有关最新版本的 PAN-OS 中引入的 CN-Series 功能和增强功能的更多信息。
- Panorama 管理员指南 — Panorama 是用于连接 Kubernetes 环境，管理部署的 CN-Series 防火墙以及定义安全策略的界面。

CN-Series 系统要求

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

本节介绍在 Kubernetes 群集和内部部署环境中部署 CN-Series 防火墙的建议系统要求。

本部分包含以下主题：

Kubernetes 集群的 CN-Series 系统要求

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

以下是我们推荐的跨多种支持模式部署 CN-Series 防火墙的系统要求。

- PAN-OS 10.1
- PAN-OS 10.2 及更高版本

PAN-OS 10.1

下表显示了部署 CN-Series 的群集的系统要求。这些值是 CPU、内存和磁盘存储空间的一般指示；您部署的资源数量可能会因需求而异。

CN-Series 中型不可用于 *CN-Series* 即 *DaemonSet*。

资源	**CN-MGMT** - 小型	**CN-NGFW** - 小型	**CN-MGMT** - 中型	**CN-NGFW** - 中型	**CN-MGMT** - 大型	**CN-NGFW** - 大型
内存（最小）	3GB	• 2GB (Daemonset) • 2.5GB（K8s 服务）	3GB	6GB	4GB	48GB
CPU（最少）	2（推荐）	2（推荐）	2（推荐）	4（推荐）	4（推荐）	12（推荐）
CPU（最多）	N/A	31	N/A	31	N/A	31
磁盘	50GB	N/A	50GB	N/A	50GB	N/A

PAN-OS 10.2 及更高版本

5G-Native Security 仅在 Daemonset 和 Kubernetes CNF 模式下受支持。

CN-MGMT 和 *CN-NGFW* 的内存和核心组合分别适用于小型、中型和大型部署。与 *CN-MGMT* 相关的小型、中型和大型部署的组合直接映射到相应的 *CN-NGFW*。

表 **1:** 推荐的 **CN-Series** 系统和容量矩阵

CN 模式	资源	小	中	中	中	大	大
Daemonset	最小 CN-MGMT 内存	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 内存	2G	6.5G	16G	32G	48G	56G
	推荐的 CN-MGMT 内核数	2	2	2	4	8	12
	CN-NGFW 核心数上限	2	4	8	16	31	47
	磁盘	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 大页面大小	N/A	N/A	N/A	N/A	N/A	N/A
Kubernetes 服务	最小 CN-MGMT 内存	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 内存	4G	6.5G	16G	32G	48G	56G
	推荐的 CN-MGMT 内核数	2	2	2	4	8	12
	CN-NGFW 核心数上限	2	4	8	16	31	47

CN 模式	资源	小	中	中	中	大	大
	磁盘	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 大页面大小	N/A	N/A	N/A	N/A	N/A	N/A
Kubernetes CNF	最小 CN-MGMT 内存	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 内存	2G	6.5G	16G	32G	48G	56G
	推荐的 CN-MGMT 内核数	2	2	2	4	8	12
	CN-NGFW 核心数上限	2	4	8	16	31	47
	磁盘	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 大页面大小	1G	1G	2G	2G	4G	4G

Kubernetes 本地部署的 CN-Series 系统要求

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

查看本地部署的以下先决条件：

- 确保 Kubernetes 集群中的所有节点都可访问容器映像。
- 在集群中为两个 CN-MGMT Pod 设置一个持久卷。由于 CN-MGMT Pod 作为 StatefulSet 部署，从而主动管理 CN-NGFW Pod，因此两个实例都必须有权访问持久卷。

要获得 *Rancher* 集群的 *SSH* 访问权限，您必须确保将 *kubeconfig* 文件的内容复制到 `/.kube/config` 下，这样就只有您可以为集群运行 *kubectl* 命令。

另外，您要确保在系统上安装 *Kubernetes* 命令行工具 *kubectl*。有关详细信息，请参阅安装工具。

对于支持 *Rancher* 的 *CN-Series*，请在主节点 *Ubuntu 18.0.4 LTS* 虚拟机（配备 *8* 个 *vCPU* 和 *32G* 内存，磁盘最小为 *200G*）上安装 *Docker*。有关更多信息，请参阅在 Ubuntu 上安装 Docker 18.04。

对于 *Ubuntu 18.0.4*，应使用以下命令将计算机上的内核更新为最新内核：

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

CN-Series 的性能和扩展性

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

以下部分列出了 使用 CN-Series 防火墙保护 Kubernetes 工作负载所需的不同组件的规模数量：

- CN-Series 组件支持的规模
- Panorama 上的 Kubernetes 插件支持的规模
- CN-Series 关键性能指标

CN-Series 组件支持的规模

有关 CN-Series CPU、内存和磁盘存储定义的信息，请参见 Kubernetes 集群的 CN-Series 系统要求。

下表按 CN-Series 大小（小型、中型和大型）分别列出了一些数据。这些 CN-Series 大小具有以下内存值：

- **CN-Series** 小型版 — 最低 2.5G CN-NGFW 和 3G CN-MGMT
- **CN-Series** 中型版 — 最低 6G CN-NGFW 和 3G CN-MGMT
- **CN-Series** 大型版 — 最低 42G CN-NGFW 和 4G CN-MGMT

属性	**CN-Series** 规模 **(DaemonSet)**	**CN-Series** 规模（**K8s** 服务）	**CN-Series** 规模 **(K8s-CNF)**
每个 K8s 集群的最多 CN-MGMT 对	主动/被动高可用性模式下的 4CN-MGMT 对	主动/被动高可用性模式下的 4CN-MGMT 对	主动/被动高可用性模式下的 4CN-MGMT 对
每个 CN-MGMT 对的最多 CN-NGFW Pod	30	30	30
由 CN-NGFW 保护的 Kubernetes Pod（每个 K8s 节点）	30（PAN-OS 10.1.8 或更低版本）	N/A	N/A

属性	CN-Series 规模 (DaemonSet)	CN-Series 规模（K8s 服务）	CN-Series 规模 (K8s-CNF)
	125（安装了 k8s 2.0.2 的 PAN-OS 10.1.9 及以上版本）	此部署模式与 *K8s* 节点上的应用程序 *Pod* 数量无关。	此部署模式与 *K8s* 节点上的应用程序 *Pod* 数量无关。
每个 CN-NGFW 的最大 TCP/IP 会话数	CN-Series 小型：20,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000	CN-Series 小型：250,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000	CN-Series 小型：250,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000
每个 CN-MGMT 对的最大动态地址组 IP 地址数*	CN-Series 小型：2500（PAN-OS 10.0.6 及更低版本） 10,000（PAN-OS 10.0.7 及更高版本）	CN-Series 小型：2500（PAN-OS 10.0.6 及更低版本） 10,000（PAN-OS 10.0.7 及更高版本） CN-Series 中型：200，000 CN-Series 大型：300，000	CN-Series 小型：2500（PAN-OS 10.0 及更低版本） 10,000（PAN-OS 10.0.7 及更高版本） CN-Series 中型：200，000 CN-Series 大型：300，000
每个 CN-MGMT 对的每个 IP 地址标签数*	32	32	32
最大安全区域	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200
安全配置文件	CN-Series 小型：38 CN-Series 中型：375 CN-Series 大型：750	CN-Series 小型：375 CN-Series 中型：375 CN-Series 大型：750	CN-Series 小型：375 CN-Series 中型：375 CN-Series 大型：750

属性	**CN-Series** 规模 **(DaemonSet)**	**CN-Series** 规模（**K8s** 服务）	**CN-Series** 规模 **(K8s-CNF)**
最大接口数	对于 **PAN OS 10.1.8** 或更低版本： CN-Series 小型：30 CN-Series 中型：30 CN-Series 大型：30 对于安装了 **k8s 2.0.2** 的 **PAN-OS 10.1.9** 及更高版本： CN-Series 小型：250 CN-Series 中型：250 CN-Series 大型：250	CN-Series 小型：2 CN-Series 中型：2 CN-Series 大型：2	CN-Series 小型：60 CN-Series 中型：60 CN-Series 大型：60

*请参阅防火墙比较工具。

数量	**CN-Series** 小型（最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型（最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型（最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
安全规则	1500	10,000	20,000
安全规则计划	256	256	256
NAT 规则 *CNF* 模式支持 *NAT* 规则。	N/A	N/A	N/A
解密规则	1000	1000	2000
应用覆盖规则	1000	1000	2000
隧道内容检测规则	100	500	2000

数量	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
SD-WAN 规则	N/A	N/A	N/A
基于策略的转发规则 *CNF* 模式支持基于策略的转发规则。	N/A	N/A	N/A
强制网络门户模式	N/A	N/A	N/A
DoS 保护规则	• 100 (DaemonSet) • 1000（K8s 服务）	1000	1000

对象（地址和服务）	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
地址对象	10,000	10,000	40,000
地址组	1000	1000	4000
每个地址组的成员数	2500	2500	2500
服务对象	2000	2000	5000
服务组	500	500	500
每个服务组的成员数	500	500	500
FQDN 地址对象	2000	2000	2000
最大动态地址组 IP 地址	2500	200，000	300，000

对象（地址和服务）	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
每个 IP 地址的标签	32	32	32

App-ID	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
自定义 App-ID 签名	6000	6000	6000
共享的自定义 App-ID	512	512	512
自定义 App-ID（特定于虚拟系统）	6416	6416	6416

SSL 解密	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
最大 SSL 入站证书	1000	1000	1000
SSL 证书缓存（转发代理）	128	2000	8000
最大并发解密会话数	• 1024 (DaemonSet) • 6400（K8s 服务）	15,000	100，000
SSL 端口镜像	否	否	否
SSL 解密代理	否	否	否
HSM 支持	否	否	否

URL 筛选	CN-Series 小型 （最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型 （最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型 （最低 42G CN-NGFW 和最低 4G CN-MGMT）
允许列表、阻止列表和自定义类别的条目总数	25,000	25,000	100，000
最大自定义类别	• 500 (DaemonSet) • 2849（K8s 服务）	2849	2849
用于 URL 过滤的 Dataplane 缓存大小	• 5000 (DaemonSet) • 90,000（K8s 服务）	90,000	250,000
管理平面动态缓存大小	100，000	100，000	600,000

EDL	CN-Series 小型 （最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型 （最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型 （最低 42G CN-NGFW 和最低 4G CN-MGMT）
自定义列表的最大数量	30	30	30
每个系统的最大 IP 数	50,000	50,000	50,000
每个系统的最大 DNS 域数	50,000	500，000	2,000,000
每个系统的最大 URL 数	50,000	100，000	100，000
最短检查间隔（分钟）	5	5	5

地址分配	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
DHCP 服务器	3	10	125
DHCP 中继	否	否	否
已分配地址的最大数量	64,000	64,000	64,000

接口	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
最大接口数（逻辑和物理接口）	• 60 (DaemonSet) • 2（K8s 服务） • 2 (K8s-CNF)	• 60 (DaemonSet) • 2（K8s 服务） • 2 (K8s-CNF)	• 60 (DaemonSet) • 2（K8s 服务） • 2 (K8s-CNF)
管理 - 带外	N/A	N/A	N/A
管理 - 10/100/1000 高可用性	N/A	N/A	N/A
管理 - 40G 高可用性	N/A	N/A	N/A
管理 - 10G 高可用性	N/A	N/A	N/A
流量 - 10/100/1000	N/A	N/A	N/A
流量 - 100/1000/10000	N/A	N/A	N/A
流量 - 1G SFP	N/A	N/A	N/A
流量 - 10G SFP+	N/A	N/A	N/A
流量 - 40/100G QSFP+/QSFP28	N/A	N/A	N/A

接口	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
每台设备的 802.1q 标签	N/A	N/A	N/A
每个物理接口的 802.1q 标签	N/A	N/A	N/A
最大聚合接口	N/A	N/A	N/A
最大 SD-WAN 虚拟接口	N/A	N/A	N/A

NAT	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
NAT 规则总容量	N/A	N/A	N/A
最大 NAT 规则（静态）	N/A	N/A	N/A
最大 NAT 规则 (DIP)	N/A	N/A	N/A
最大 NAT 规则 (DIPP)	N/A	N/A	N/A
最大翻译 IP 数 (DIP)	N/A	N/A	N/A
最大翻译 IP 数 (DIPP)	N/A	N/A	N/A
默认 DIPP 池超额订阅	N/A	N/A	N/A

User-ID	CN-Series 小型（最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型（最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型（最低 42G CN-NGFW 和最低 4G CN-MGMT）
IP 用户映射（管理平面）	N/A	N/A	N/A
IP 用户映射（数据平面）	N/A	N/A	N/A
策略中使用的活动组和唯一组	N/A	N/A	N/A
用户 ID 代理的数量	N/A	N/A	N/A
用户 ID 的受监控服务器	N/A	N/A	N/A
终端服务器代理	N/A	N/A	N/A
每位用户的标签	N/A	N/A	N/A

路由	CN-Series 小型（最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型（最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型（最低 42G CN-NGFW 和最低 4G CN-MGMT）
IPv4 转发表大小	N/A	N/A	N/A
IPv6 转发表大小	N/A	N/A	N/A
系统总转发表大小	N/A	N/A	N/A
最大路由对端数（取决于协议）	N/A	N/A	N/A
静态条目 - DNS 代理	N/A	N/A	N/A
双向转发检测 (BFD) 会话数	N/A	N/A	N/A

L2 转发	CN-Series 小型（最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型（最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型（最低 42G CN-NGFW 和最低 4G CN-MGMT）
每台设备的 ARP 表大小	N/A	N/A	N/A
IPv6 相邻表大小	N/A	N/A	N/A
每台设备的 MAC 表大小	N/A	N/A	N/A
每个广播域的最大 ARP 条目数	N/A	N/A	N/A
每个广播域的最大 MAC 条目数	N/A	N/A	N/A

QoS	CN-Series 小型（最低 2.5G CN-NGFW 和最低 3G CN-MGMT）	CN-Series 中型（最低 6G CN-NGFW 和最低 2G CN-MGMT）	CN-Series 大型（最低 42G CN-NGFW 和最低 4G CN-MGMT）
QoS 策略的数量	N/A	N/A	N/A
支持 QoS 的物理接口	N/A	N/A	N/A
每个物理接口的明文节点	N/A	N/A	N/A
按策略标记 DSCP	N/A	N/A	N/A
支持的子接口	N/A	N/A	N/A

IPsec VPN	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
Max IKE 对端	N/A	N/A	N/A
站点到站点（使用代理 ID）	N/A	N/A	N/A
SD-WAN IPsec 隧道	N/A	N/A	N/A

GlobalProtect	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
GlobalProtect 客户端 **VPN** 最大隧道数（SSL、IPsec、带 XAUTH 的 IKE）	N/A	N/A	N/A
GlobalProtect 无客户端 **VPN** 最大 SSL 隧道数	N/A	N/A	N/A

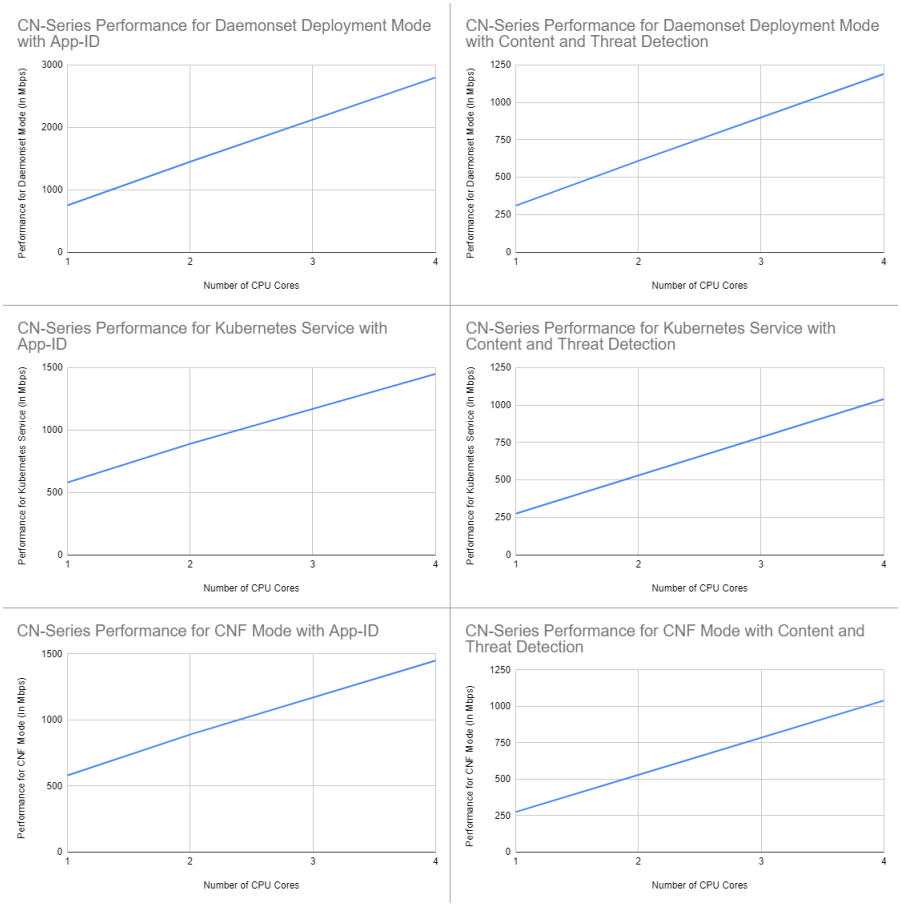
多播	**CN-Series** 小型 （最低 **2.5G CN-NGFW** 和最低 **3G CN-MGMT**）	**CN-Series** 中型 （最低 **6G CN-NGFW** 和最低 **2G CN-MGMT**）	**CN-Series** 大型 （最低 **42G CN-NGFW** 和最低 **4G CN-MGMT**）
复制（传出接口）	N/A	N/A	N/A
路由	N/A	N/A	N/A

Panorama 上的 Kubernetes 插件支持的规模

属性	**Kubernetes** 插件规模
K8s Panorama 插件上的最大集群数	32（在所有支持的环境中，例如 Native K8s、AKS、EKS、GKE）

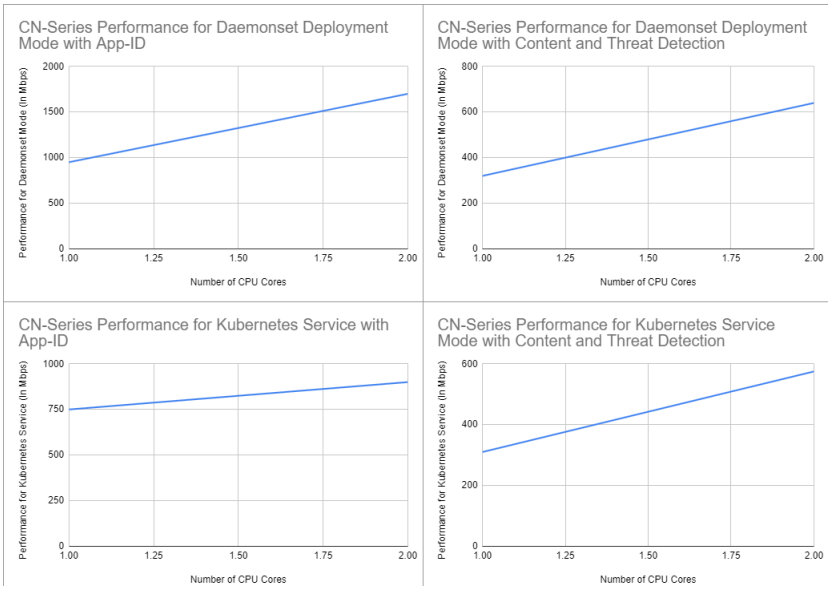
CN-Series 关键性能指标

AWS EKS 上的 **CN-Series**				
	CPU 核心数	**CN-Series** 即 **DaemonSet (MMAP)**	**CN-Series** 即 **Kubernetes** 服务 **(MMAP)**	**CN-Series** 即 **Kubernetes CNF (MMAP)**
App-ID	1	750 Mbps	580 Mbps	580 Mbps
内容和威胁检测	1	310 Mbps	275 Mbps	275 Mbps
App-ID	2	1.45 Gbps	890 Mbps	890 Mbps
内容和威胁检测	2	610 Mbps	530 Mbps	530 Mbps
App-ID	4	2.8 Gbps	1.45 Gbps	1.45 Gbps
内容和威胁检测	4	1.19 Gbps	1.04 Gbps	1.04 Gbps



Google Cloud GKE 上的 CN-Series （已启用 XDP）			
	CPU 核心数	**CN-Series 即 DaemonSet**	**CN-Series 即 Kubernetes 服务**
App-ID	1	950 Mbps	750 Mbps
内容和威胁检测	1	320 Mbps	310 Mbps
App-ID	2	1.7 Gbps	900 Mbps
内容和威胁检测	2	640 Mbps	575 Mbps

下表中的信息是在 *Google Kubernetes Engine (GKE)* 上进行的测试，其中流量在同一集群中同一节点上的节点之间和 *Pod* 之间转发



功能/属性	**CN-Series** 小型	**CN-Series** 中型	**CN-Series** 大型
CN-NGFW 的每个 vCPU 的防火墙吞吐量（已启用 App-ID）	500 Mbps	500 Mbps	500 Mbps
CN-NGFW 的每个 vCPU 的威胁防护吞吐量	250 Mbps	250 Mbps	250 Mbps
最大会话数	• 20,000 (DaemonSet) • 250,000（K8s 服务） • 250,000 (K8s-CNF)	819,200	10,000,000
CN-NGFW 的每个 vCPU 的 IPsec VPN 吞吐量	N/A	N/A	N/A
每秒连接数	N/A	N/A	N/A

CN-Series 部署 — 支持的环境

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 图表部署 CN-Series 的 Helm 3.6 or above version client

本章提供有关 CN-Series 防火墙的兼容性和版本要求的信息。

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

PAN-OS 10.1

您可以在以下环境中部署 CN-Series 防火墙：

产品	版本
容器运行时	Docker CRI-O Containerd
Kubernetes 版本	1.17 至 1.27
云提供商托管 Kubernetes	• AWS EKS（1.17 至 1.27，用于 CN-Series 即 DaemonSet 和 CN-Series 即服务部署模式。） • EKS on AWS Outpost（1.17 至 1.25） *AWS Outpost 上 EKS 的 CN-Series 不支持 SR-IOV 或Multus。* • Azure AKS（1.17 至 1.27） 在 *Azure AKS* 中，*PAN-OS 10.1.10h1* 是支持 *Kubernetes 1.25* 及更高版本所需的最低版本。

产品	版本
	• AliCloud ACK (1.26) • GCP GKE（1.17 至 1.27）  包括 *GKE Dataplane V2*。
客户托管 Kubernetes	在公共云或本地数据中心上。 确保此表中已列出 Kubernetes 版本、CNI 类型和 Host VM OS 版本。 VMware TKG+ 版本 1.1.2 • 基础架构平台 — vSphere 7.0 • Kubernetes Host VM OS — Photon OS
Kubernetes 主机虚拟机	操作系统 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 及更高版本 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux 内核版本： • 4.18 或更高版本（仅限 K8s 服务模式） • 5.4 或更新版本需要启用 AF_XDP 模式。有关详细信息，请参见 CN-Series 部署 YAML文件中的可编辑参数。
	Linux Kernel Netfilter：Iptables
CNI 插件	CNI Spec 0.3 及更高版本： • AWS-VPC • Azure • Calico • Flannel • Weave • 适用于 AliCloud、Terway

产品	版本

	• 适用于 Openshift、OpenshiftSDN
	• 作为 DaemonSet，CN-Series 防火墙支持以下内容。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	**CN-Series** 即 **DaemonSet**： 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 **CN-Series** 即 **K8s** 服务： （PAN-OS 10.1.2 及更高版本） 4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 *PAN-OS 10.1.10h1* 是支持 *4.12* 及更高版本所需的最低版本。

在部署 CN-Series 防火墙之前，另请参阅Kubernetes 集群的 CN-Series 系统要求。

PAN-OS 10.2

您可以在以下环境中部署 CN-Series 防火墙：

产品	版本
容器运行时	Docker CRI-O Containerd
Kubernetes 版本	1.17 至 1.27
云提供商托管 Kubernetes	• AWS EKS（1.17 至 1.27，用于 CN-Series 即 DaemonSet 和 CN-Series 即服务部署模式。） • AWS EKS（1.17 至 1.22，适用于 CN-Series 即 CNF 部署模式。）

产品	版本
	• EKS on AWS Outpost（1.17 至 1.22） 适用于 *EKS on AWS Outpost* 的 *CN-Series* 不支持 *SR-IOV* 或 *Multus*。 • Azure AKS（1.17 至 1.28） 在 *Azure AKS* 中，*PAN-OS 10.2.4h3* 是支持 *Kubernetes 1.25* 及更高版本所需的最低版本。 • GCP GKE（1.17 至 1.27） 在 *GCP GKE* 中，*PAN-OS 10.2.4h3* 是支持 *kubernetes 1.25* 及更高版本所需的最低版本。 包括 *GKE Dataplane V2*。 • Google Anthos 1.12.3 • OCI OKE (1.23)
客户托管 Kubernetes	在公共云或本地数据中心上。 确保此表中已列出 Kubernetes 版本、CNI 类型和 Host VM OS 版本。 VMware TKG+ 版本 1.1.2 • 基础架构平台 — vSphere 7.0 • Kubernetes Host VM OS — Photon OS
Kubernetes 主机虚拟机	操作系统 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 及更高版本 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux 内核版本： • 4.18 或更高版本（仅限 K8s 服务模式）

产品	版本
	• 5.4 或更新版本需要启用 AF_XDP 模式。有关详细信息，请参见 CN-Series 部署 YAML文件中的可编辑参数。
	Linux Kernel Netfilter：Iptables

CNI 插件	CNI Spec 0.3 及更高版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 适用于 Openshift、OpenshiftSDN、OVN Kubernetes
	• 作为 DaemonSet，CN-Series 防火墙支持以下内容。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• 版本 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 *OpenShift 4.7* 在 *CN-Series* 上仅作为 *DaemonSet*。 • AWS 上的 OpenShift *PAN-OS 10.2.4h3* 是支持 *4.12* 及更高版本所需的最低版本。

在部署 CN-Series 防火墙之前，另请参阅Kubernetes 集群的 CN-Series 系统要求。

PAN-OS 11.0

您可以在以下环境中部署 CN-Series 防火墙：

产品	版本
容器运行时	Docker CRI-O Containerd
Kubernetes 版本	1.17 至 1.27
云提供商托管 Kubernetes	• AWS EKS（1.17 至 1.27，用于 CN-Series 即 DaemonSet 和 CN-Series 即服务部署模式。） • AWS EKS（1.17 至 1.22，适用于 CN-Series 即 CNF 部署模式。） • EKS on AWS Outpost（1.17 至 1.25） *AWS Outpost* 上 *EKS* 的 *CN-Series* 不支持 *SR-IOV* 或*Multus*。 • Azure AKS（1.17 至 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支持 *kubernetes 1.25* 及更高版本所需的最低版本。 • GCP GKE（1.17 至 1.27） 包括 *GKE Dataplane V2*。 • OCI OKE (1.23)
客户托管 Kubernetes	在公共云或本地数据中心上。 确保此表中已列出 Kubernetes 版本、CNI 类型和 Host VM OS 版本。 VMware TKG+ 版本 1.1.2 • 基础架构平台 — vSphere 7.0 • Kubernetes Host VM OS — Photon OS
Kubernetes 主机虚拟机	操作系统 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 及更高版本 • CoreOS 21XX、22XX

产品	版本
	• Container-Optimized OS
	Linux 内核版本： • 4.18 或更高版本（仅限 K8s 服务模式） • 5.4 或更新版本需要启用 AF_XDP 模式。有关详细信息，请参见 CN-Series 部署 YAML文件中的可编辑参数。
	Linux Kernel Netfilter：Iptables

CNI 插件	CNI Spec 0.3 及更高版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 适用于 Openshift、OpenshiftSDN、OVN Kubernetes
	• 作为 DaemonSet，CN-Series 防火墙支持以下内容。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• 版本 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13。 *OpenShift 4.7* 在 *CN-Series* 上仅作为 *DaemonSet*。 *PAN-OS 11.0.2* 是支持 *4.12* 及更高版本所需的最低版本。 • AWS 上的 OpenShift

在部署 CN-Series 防火墙之前，另请参阅Kubernetes 集群的 CN-Series 系统要求。

PAN-OS 11.1

您可以在以下环境中部署 CN-Series 防火墙：

产品	版本
容器运行时	Docker CRI-O Containerd
Kubernetes 版本	1.17 至 1.27
云提供商托管 Kubernetes	• AWS EKS（1.17 至 1.27，用于 CN-Series 即 DaemonSet 和 CN-Series 即服务部署模式。） • AWS EKS（1.17 至 1.22，适用于 CN-Series 即 CNF 部署模式。） • EKS on AWS Outpost（1.17 至 1.25） *AWS Outpost* 上 *EKS* 的 *CN-Series* 不支持 *SR-IOV* 或*Multus*。 • Azure AKS（1.17 至 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支持 *kubernetes 1.25* 及更高版本所需的最低版本。 • GCP GKE（1.17 至 1.27） 包括 *GKE Dataplane V2*。 • OCI OKE (1.23)
客户托管 Kubernetes	在公共云或本地数据中心上。 确保此表中已列出 Kubernetes 版本、CNI 类型和 Host VM OS 版本。 VMware TKG+ 版本 1.1.2 • 基础架构平台 — vSphere 7.0 • Kubernetes Host VM OS — Photon OS
Kubernetes 主机虚拟机	操作系统 • Ubuntu 16.04 • Ubuntu 18.04

产品	版本
	• Ubuntu 22.04 • RHEL/Centos 7.3 及更高版本 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux 内核版本： • 4.18 或更高版本（仅限 K8s 服务模式） • 5.4 或更新版本需要启用 AF_XDP 模式。有关详细信息，请参见 CN-Series 部署 YAML文件中的可编辑参数。
	Linux Kernel Netfilter：Iptables

CNI 插件	CNI Spec 0.3 及更高版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 适用于 Openshift、OpenshiftSDN、OVN Kubernetes
	• 作为 DaemonSet，CN-Series 防火墙支持以下内容。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• 版本 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13。  *OpenShift 4.7* 在 *CN-Series* 上仅作为 *DaemonSet*。 *PAN-OS 11.0.2* 是支持 *4.12* 及更高版本所需的最低版本。 • AWS 上的 OpenShift

在部署 CN-Series 防火墙之前，另请参阅Kubernetes 集群的 CN-Series 系统要求。

PAN-OS 11.2

您可以在以下环境中部署 CN-Series 防火墙：

产品	版本
容器运行时	Docker CRI-O Containerd
Kubernetes 版本	1.17 至 1.27
云提供商托管 Kubernetes	• AWS EKS（1.17 至 1.27，用于 CN-Series 即 DaemonSet 和 CN-Series 即服务部署模式。） • AWS EKS（1.17 至 1.22，适用于 CN-Series 即 CNF 部署模式。） • EKS on AWS Outpost（1.17 至 1.25） *AWS Outpost 上 EKS 的 CN-Series 不支持 SR-IOV 或Multus。* • Azure AKS（1.17 至 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支持 *kubernetes 1.25* 及更高版本所需的最低版本。 • GCP GKE（1.17 至 1.27） 包括 *GKE Dataplane V2*。 • OCI OKE (1.23)
客户托管 Kubernetes	在公共云或本地数据中心上。 确保此表中已列出 Kubernetes 版本、CNI 类型和 Host VM OS 版本。 VMware TKG+ 版本 1.1.2 • 基础架构平台 — vSphere 7.0 • Kubernetes Host VM OS — Photon OS
Kubernetes 主机虚拟机	操作系统

产品	版本
	• Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 及更高版本 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux 内核版本： • 4.18 或更高版本（仅限 K8s 服务模式） • 5.4 或更新版本需要启用 AF_XDP 模式。有关详细信息，请参见 CN-Series 部署 YAML文件中的可编辑参数。
	Linux Kernel Netfilter：Iptables

CNI 插件	CNI Spec 0.3 及更高版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 适用于 Openshift、OpenshiftSDN、OVN Kubernetes
	• 作为 DaemonSet，CN-Series 防火墙支持以下内容。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

产品	版本
OpenShift	• 版本 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13。 *OpenShift 4.7* 在 *CN-Series* 上仅作为 *DaemonSet*。 *PAN-OS 11.0.2* 是支持 *4.12* 及更高版本所需的最低版本。 • AWS 上的 OpenShift

在部署 CN-Series 防火墙之前，另请参阅Kubernetes 集群的 CN-Series 系统要求。

CN-Series 部署先决条件

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

要部署 CN-Series 防火墙，必须确保满足以下先决条件：

- 授予 CN-Series 防火墙许可证
- 在 CN-Series 防火墙上安装设备证书
- 创建用于集群身份验证的服务帐户
- 为 CN-Series 安装 Kubernetes 插件并设置 Panorama
- 获取用于 CN-Series 部署的映像和文件

授予 CN-Series 防火墙许可证

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

CN-Series 防火墙许可由 Panorama 上的 Kubernetes 插件管理。CN-Series 防火墙的许可基于部署在 Kubernetes 环境中的 CN-NGFW Pod 使用的 vCPU（核心）总数。每个使用 CN-NGFW 的 vCPU 消耗一个令牌。

- 激活积分 — 首先激活积分。激活后，您可以将积分池中的积分应用于 CN-Series 部署配置文件。
- 创建 CN-Series 部署配置文件 — 在部署配置文件中，您将指定分配给生成身份验证代码的 vCPU 数量。然后，您将使用与 CN-Series 部署配置文件关联的身份验证来授予 Kubernetes 集群中的 CN-Series 防火墙许可证。部署配置文件可用于根据分配的 vCPU 数量授予 CN-NGFW Pod 许可证。部署配置文件中的单个身份验证代码可用于跨不同 Kubernetes 环境、不同集群或不同 Panorama 实例为 CN-Series 授予许可。

  在 CN-Series 即 Kubernetes 服务部署中，如果在您的环境中部署的 CN-NGFW Pod 的数量超出分配的 vCPU 数量，您有 30 天宽限期来将更多 vCPU 添加到您的部署配置文件中，或者删除多出的 CN-NGFW Pod。如果您在 30 天宽限期内不分配额外的 vCPU 或删除未授权的 Pod，则集群中的所有 CN-Series 防火墙都将被取消授权。

  如果部署的 Pod 超出分配的 vCPU 数量，您将有四小时宽限期来将更多 vCPU 添加到您的部署配置文件中，或者删除多余的 CN-NGFW Pod。如果您未在四小时宽限期内分配额外的 vCPU 或删除未许可的 Pod，则未许可的 Pod 将停止处理流量。已获得许可的 Pod 将保持许可状态。

  在创建 CN-Series 部署配置文件时，您还可以选择配置虚拟 Panorama 设备。
- 管理部署配置文件 — 您可以根据 CN-Series 部署的要求编辑、克隆或删除 CN-Series 部署配置文件。此外，您可以在创建部署配置文件后添加或删除订阅。

许可证适用于集群级别的 *CN-Series* 。单个 *CN-NGFW* 可能显示为未许可，但是，在整个集群被取消许可之前，集群中的所有 *Pod* 都已获得许可。

激活积分

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

在贵组织内，您可以创建多个帐户，每个帐户都有不同的用途。在激活过程中，您只能为每个默认积分池选择一个帐户。一旦积分池处于活动状态，则授予积分管理员角色的用户就可以为部署分配积分，甚至可以将积分传输到其他积分池。

如果您有现有 CSP 帐户并且是超级用户或管理员，系统会自动将积分管理员角色添加到您的配置文件中。如果您没有现有帐户，CSP 会自动为您创建一个帐户，并将积分管理员角色添加到您的配置文件中。

您（购买者）会收到一封电子邮件，其中详细说明了订阅、积分池 ID、订阅的开始和结束日期、购买的积分金额以及默认积分池（激活积分时创建的积分池）的描述。

保护此电子邮件以备将来参考。

STEP 1 | 在电子邮件中，单击 **Start Activation**（开始激活）以查看可用的积分池。

STEP 2 | 选择要激活的积分池。您可以使用搜索字段按帐号或用户名筛选帐户列表。

如果您已购买多个积分池，系统会自动将其选定。复选标记表示登录积分的激活链接。

系统会提示您进行身份验证或登录。

如果您取消选择积分池，您会看到一个提醒，提示您如果要激活这些积分，则必须返回电子邮件并单击 ***Start Activation***（开始激活）链接。

STEP 3 | 选择 **Start Activation**（开始激活）。

STEP 4 | 选择支持帐户（您可以按帐号或姓名进行搜索）。

STEP 5 | 选择默认积分池。

STEP 6 | 选择 **Deposit Credits**（存款积分）。

您会看到一条提示存款成功的消息。

STEP 7 | （可选）如果这是您第一次激活积分，则系统会显示 **Create Deployment Profile**（创建部署配置文件）对话框。

继续阅读创建 CN-Series 部署配置文件。

创建 CN-Series 部署配置文件

在何处可以使用？	需要什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署适用于 CN-Series 的 Helm 3.6 or above version client

按照以下过程创建 CN-Series 部署配置文件。

STEP 1 | 如果您已有积分池，请登录该帐户，然后从指示板中选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分） > **Prisma NGFW Credits**（**Prisma NGFW** 积分） > **Create New Profile**（新建配置文件）。

如果您刚才已激活积分池，则会看到 **Create Deployment Profile**（创建部署配置文件）表单。

1. 选择 **CN-Series**（**CN-Series** ）防火墙类型。
2. 选择 **PAN-OS 10.2 and above**（**PAN-OS 10.2** 及更高版本）。
3. 单击 **Next**（下一步）。

STEP 2 | CN-Series 配置文件。

1. **Profile Name**（配置文件名称）。

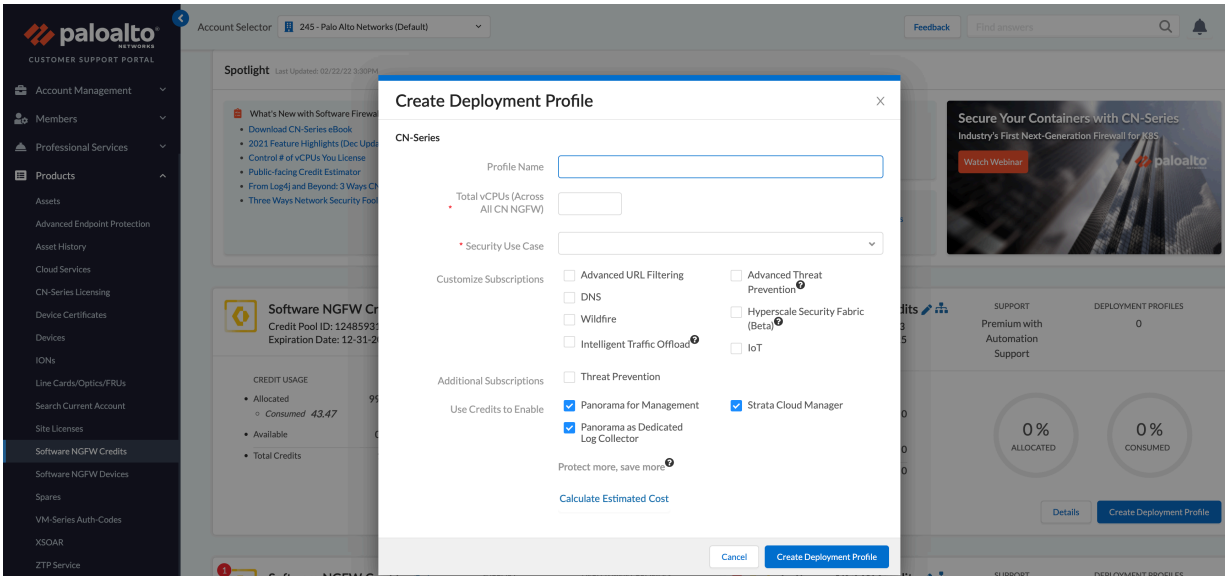
   为配置文件命名。
2. 总 **vCPU** 数量

   输入所有 CN-NGFW 中的 vCPU 总数。
3. 从下拉列表中选择一个安全用例。下拉列表中的每个安全用例都会自动选择一些建议用于所选用例的描述。如果选择自定义，则可以指定要在部署中使用的订阅。
4. （可选）使用积分启用 **VM Panorama** — **For Management**（用于管理）或 **Dedicated Log Collector**（专用日志收集器）。

STEP 3 | （可选）将鼠标悬停在 **Protect More, Save More**（更完善的保护，更优惠的价格）上，以查看您的积分分配如何影响节省金额。

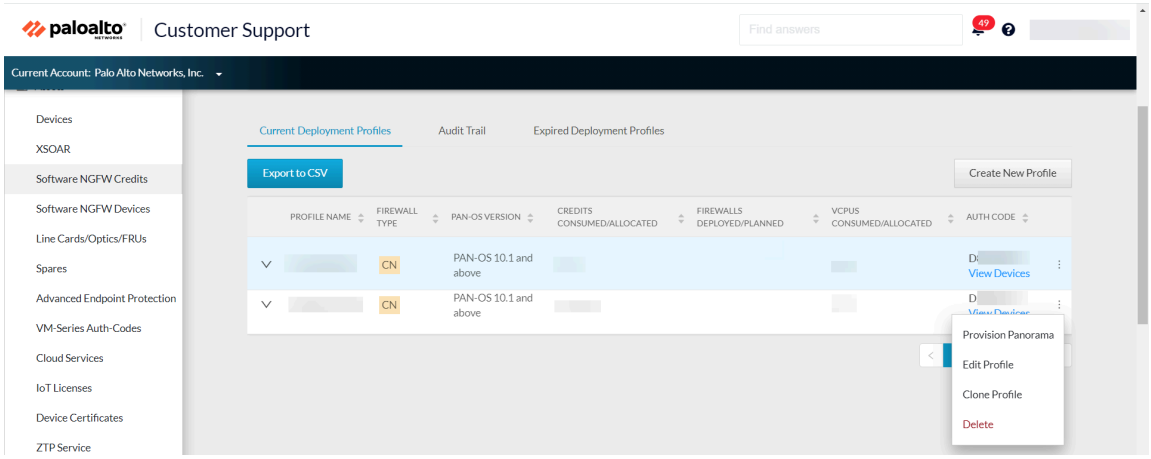
STEP 4 | 单击 **Calculate Estimated Cost**（计算估计成本）以查看积分总数和部署前可用的积分数量。

（可选）将鼠标悬停在估计值后面的问号上方以查看每个组成部分的积分明细。

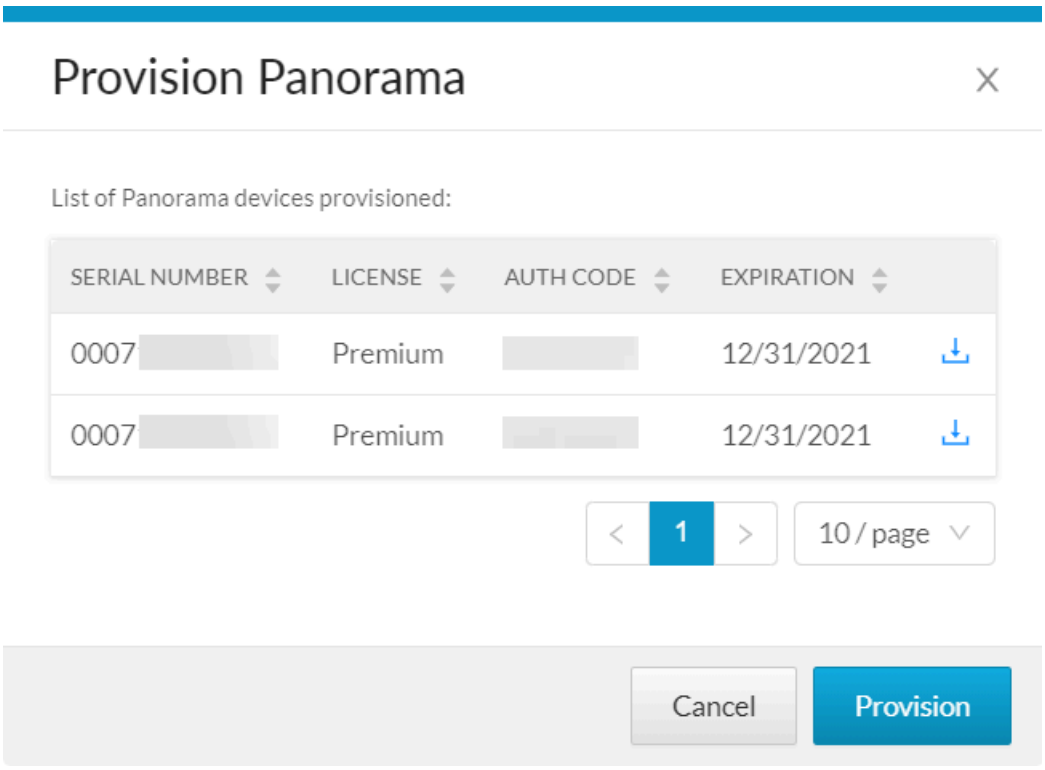


STEP 5 | （可选）配置 Panorama。如果您使用积分来启用虚拟机 Panorama，请完成以下步骤以配置 Panorama 并生成序列号。管理 CN-Series 部署需要 Panorama。将序列号应用于 Panorama 后，Panorama 将联系许可更新服务器并检索许可证。

1. 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分） > **Prisma NGFW Credits**（**Prisma NGFW** 积分）并找到部署配置文件。
2. 在最右侧选择垂直省略号，然后选择 **Provision Panorama**（配置 **Panorama**）。



3. 单击“配置 Panorama”以生成序列号。
4. 记录或复制序列号以应用于 Panorama 实例。



5. 注册 Panorama。

管理部署配置文件

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN 系列的 Helm 3.6 or above version client

您可以使用以下过程管理现有部署配置文件。

- 编辑部署配置文件
- 克隆部署配置文件
- 删除部署配置文件
- 将积分转移到同一帐户中的池
- 将积分转移到不同的 CSP 帐户

编辑部署配置文件

您可以修改现有部署配置文件以添加更多积分或为您的部署分配额外的 vCPU。与要修改的部署配置文件关联的身份验证代码不得在 Panorama 上使用。

STEP 1 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后选择一个配置文件（选定一行）。

STEP 2 | 在最右侧选择垂直省略号（更多选项），然后选择 **Edit Profile**（编辑配置文件）。

STEP 3 | 执行更改，然后选择 **Update Deployment Profile**（更新部署配置文件）。

克隆部署配置文件

完成以下过程可克隆现有部署配置文件。

STEP 1 | 转到 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分）并选择配置文件（选定一行）。

STEP 2 | 在最右侧，选择垂直省略号（“更多”选项），然后选择 **Clone Profile**（克隆配置文件）。

STEP 3 | 更改配置文件名称，进行任何其他更改，然后选择 **Create Deployment Profile**（创建部署配置文件）。

删除部署配置文件

在删除部署配置文件之前，您必须删除使用该配置文件的所有防火墙。与要删除的部署配置文件关联的身份验证代码不得在 Panorama 上使用。

STEP 1 | 在 CSP 中，选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分），然后选择一个配置文件（选定一行）。

STEP 2 | 在最右侧，选择垂直省略号（更多选项）并选择 **Delete**（删除）。

将积分转移到同一帐户中的池

您可以将积分转移到您可以访问的不同帐户的积分池。

STEP 1 | 登录到您的 CSP 帐户。

STEP 2 | 选择 **Assets**（资产） > **Software NGFW Credits**（软件 **NGFW** 积分）。

- 识别源积分池并记下积分池 ID。
- 识别目标积分池并记下积分池 ID。

STEP 3 | 转到源积分池，然后选择左下角的 **Transfer Credits**（传输积分）。

STEP 4 | 选择 **Different CSP account**（不同的 **CSP** 帐户）。

1. **New credit type**（新积分类型）— 选择积分类型。此时，源类型和目标类型必须相同。
2. **Credit Pool ID#**（积分池 **ID** 号）— 选择积分池 ID 号。如果目标帐户没有任何所选类型的积分池，则 CSP 会提示您创建积分池。
3. **Amount to transfer**（传输数量）— 输入传输数量。

STEP 5 | 选择 **Update Credits**（更新积分）。

将积分转移到不同的 CSP 帐户

您可以将积分转移到同一帐户中的积分池。

STEP 1 | 登录您的 CSP 帐户。

STEP 2 | 选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分）。

- 识别源积分池并记下积分池 ID。
- 识别目标积分池并记下积分池 ID。

  如果目标在不同帐户中，请从左上角的 **Current Account**（当前帐户）下拉列表中选择，然后选择 **Assets**（资产）> **Software NGFW Credits**（软件 **NGFW** 积分）。找到目标并记录积分类型和积分池 ID。

STEP 3 | 转到源积分池，然后单击左下角的 **Transfer Credits**（传输积分）。

STEP 4 | 选择不同的 CSP 帐户。

1. **Transfer to**（传输到）— 选择帐户名称。
2. **As credit type**（作为积分类型）— 选择积分类型。此时，源类型和目标类型必须相同。
3. **Credit Pool ID#**（积分池 **ID** 号）— 选择积分池 ID 号。如果目标帐户没有任何所选类型的积分池，则 CSP 会提示您创建积分池。
4. **Amount to transfer**（传输数量）— 输入传输数量。

STEP 5 | 选择 **Update Credits**（更新积分）。

在 CN-Series 防火墙上安装设备证书

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN-Series 的 Helm 3.6 or above version client

防火墙需要设备证书，以授权安全访问 Palo Alto 云交付的安全服务 (CDSS)，例如 WildFire、AutoFocus 和 Strata 日志记录服务。您必须应用自动注册 PIN 才能将 CDSS 许可证应用于 CN-Series 防火墙部署。每个密码或 PIN 都是在客户支持门户 (CSP) 上生成的，并且对于 Palo Alto Networks 支持帐户来说都是唯一的。要成功安装设备证书，CN-Series 管理平面 Pod (CN-MGMT) 必须具有出站互联网连接，并且必须允许在您的网络上使用以下完全限定域名 (FQDN) 和端口。

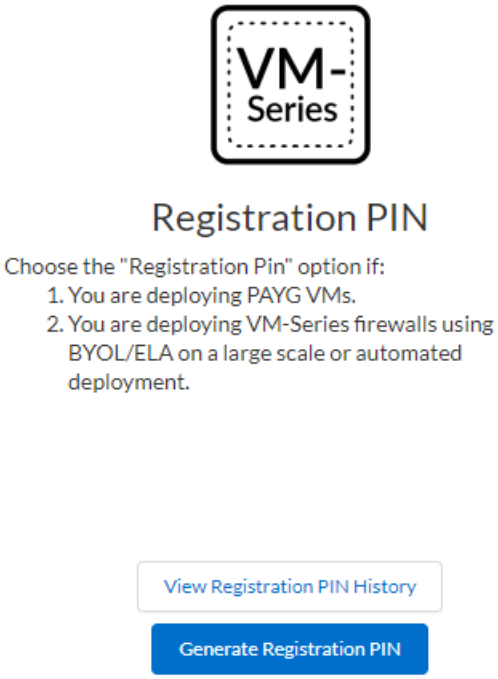
FQDN	端口
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 和 TCP 443

要将设备证书添加到没有现有设备证书的现有部署中，必须在 `pan-cn-mgmt-secret.yaml` 中添加有效的 *PIN ID* 和值后，重新部署 *CN-Series* 防火墙。对于公有云 *CN-Series* 部署，必须在重新部署之前删除永久容量声明。对于静态/原生 *Kubernetes* 部署，在重新部署之前，必须删除永久卷声明和永久卷。

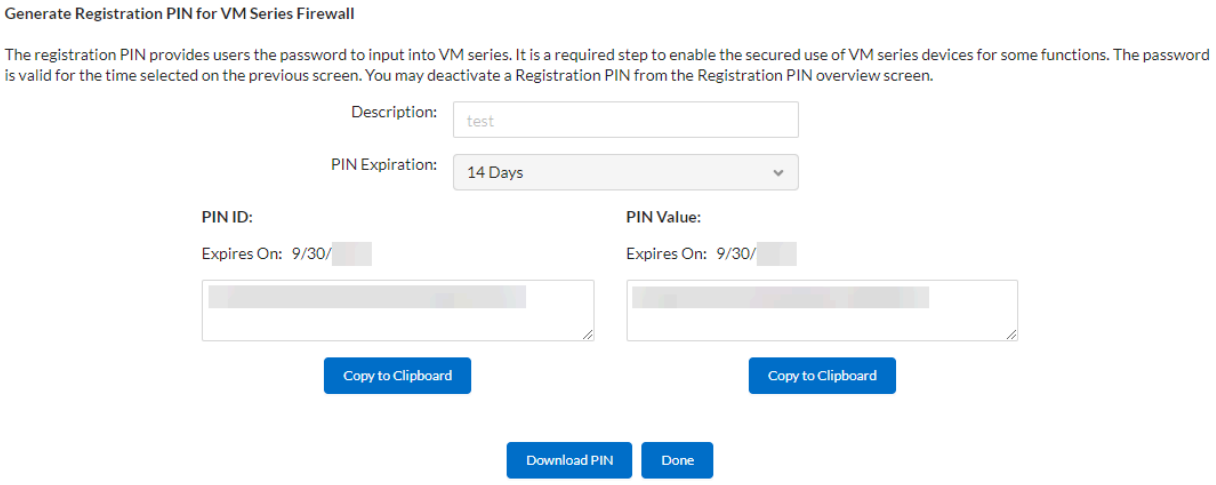
STEP 1 | 请使用您的帐户凭据登录到 Palo Alto Networks 客户支持门户。

如果需要新帐户，请参阅如何创建新的客户支持门户用户帐户。

STEP 2 | 选择 **Assets**（资产） > **Device Certificates**（设备证书） > **Generate Registration PIN**（生成注册 **PIN**）。



STEP 3 | 输入描述，然后从下拉列表中选择 **PIN Expiration**（**PIN** 过期日期）。



STEP 4 | 保存 PIN ID 和值。

保存 PIN ID 和值。此 PIN ID 和值是 `pan-cn-mgmt-secret.yaml` 文件中的输入，该文件用于部署 CN-Series 防火墙。确保在 PIN 过期之前启动防火墙。

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

创建用于集群身份验证的服务帐户

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 图表部署适用于 CN-Series 的 Helm 3.6 or above version client

CN-Series 防火墙需要三个具有最低权限的服务帐户，这些帐户授权防火墙与 Kubernetes 集群资源进行通信。利用 `plugin-serviceaccount.yaml` 创建的服务帐户 (pan-plugin-user) 使用 Panorama 上的 Kubernetes 插件，通过 Kubernetes 集群进行身份验证以检索 Pod 上的元数据。其他两个 yaml 文件：`pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml`，用于创建 pan-mgmt-sa 和 pan-cni-sa 服务帐户，在具有容错功能的 CN-Mgmt Pod 之间以及在 CN-MGMT Pod 和 CN-NGFW Pod 之间启用身份验证。

默认情况下，*YAML* 文件在 *kube-system* 命名空间中创建服务帐户和密钥；*Kubernetes* 插件仅在 *kube-system* 命名空间中查找密钥。

要创建服务帐户，Kubernetes 集群应该准备就绪。

STEP 1 | 为 `plugin-serviceaccount.yaml` 文件运行服务帐户的 YAML 文件。

该服务帐户可启用 Panorama 要求对 GKE 集群进行身份验证所需的权限，以检索 Kubernetes 标签和资源信息。默认情况下，将该服务帐户命名为 pan-plugin-user。

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

   查看与该服务帐户相关联的密钥。

   如果您使用的是 *Kubernetes* 版本 *1.24* 或更高版本，请运行以下命令以查看与此服务帐户关联的密钥：

   `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`**

   在本例中，创建一个凭据文件，将其命名为 cred.json，其中包括密钥，然后保存该文件。您需要将此文件上传到 Panorama，以设置用于监控为 CN-Series 安装 Kubernetes 插件并设置 Panorama中的集群的 Kubernetes 插件。

STEP 2 | 运行 `pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml` 文件。

`pan-mgmt-serviceaccount.yaml` 文件用于创建一个服务帐户，将其命名为 pan-sa，并且启用 CN-MGMT 和 CN-NGFW Pod 进行相互通信，以及与 PAN-CNI 和 Kubernetes API 服务器进行通信需要此帐户。如果修改此服务帐户名称，则还必须更新用于部署 CN-MGMT 和 CN-NFGW Pod 的 YAML 文件。`pan-cni-serviceaccount.yaml` 文件用于创建一个服务帐户，将其命名为 pan-cni-sa。

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

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

STEP 3 | 验证服务帐户。

```
kubectl get serviceaccounts -n kube-system
```

如果使用的是 *HELM* 图标，则步骤 *2*、*3* 由 *HELM* 图标自动执行，不需要手动执行。

为 CN-Series 安装 Kubernetes 插件并设置 Panorama

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN-Series 的 Helm 3.6 or above version client

只要 Panorama 设备可与要在其中部署 CN-Series 防火墙的 Kubernetes 集群连接，您就可在本地或云中部署 Panorama 应用程序。该工作流将指导您完成安装 Kubernetes 插件，激活授权代码并设置 Kubernetes 插件以监控集群的过程。

您必须仔细计划要分配给 *Panorama* 的积分数量。更改积分数量后，无需在 *Panorama OS 11.0* 上重新部署 *CN-Series* 防火墙。

有关详细信息，请参阅授予 CN-Series 防火墙许可证和软件 NGFW 积分估算器。

STEP 1 | 部署软件版本为 11.0 的 Panorama，并安装最低内容版本。

1. 有关 PAN-OS 11.0 上的最低内容发布版本，请转到 **Panorama** > **Dynamic Updates**（动态更新）。

   请参阅 PAN-OS 发行说明。

2. 转到 **Panorama** > **Software**（软件）。

   找到并下载您正在升级的发行版本的型号特定文件。例如，要将 M 系列设备升级到 Panorama 11.0，请下载 Panorama_m-11.0.0 映像；要将 Panorama 虚拟设备升级到 Panorama 11.0.0，请下载 Panorama_pc-11.0.0 映像。

   成功下载后，已下载映像的 **Action**（操作）列将从 Download（下载）更改为 Install（安装）。

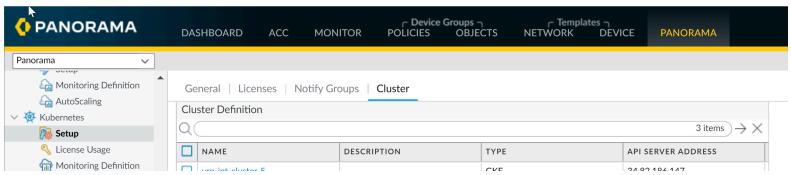
STEP 2 | 如果您希望 Panorama 收集防火墙日志，请验证 Panorama 是否处于 Panorama 模式。

STEP 3 | 安装 Panorama 上的 Kubernetes 插件。如果 Panorama 设备部署为 HA 对，则必须先在主要（活动）对端上安装 Kubernetes 插件。

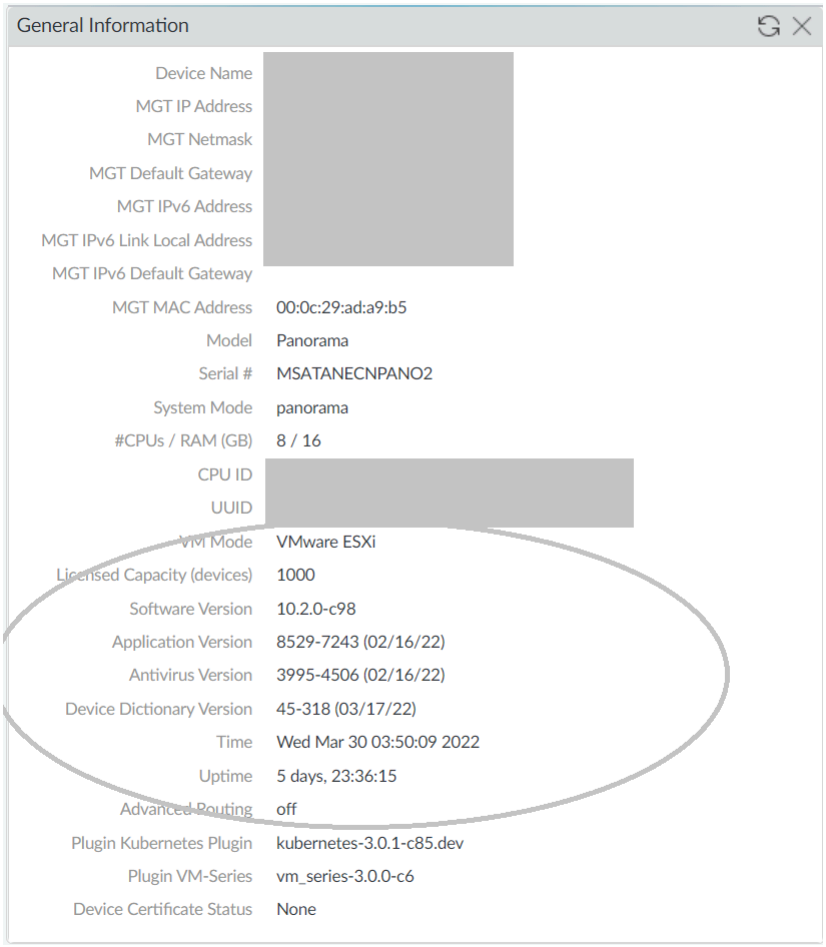
1. 登录到 Panorama Web 界面，选择 **Panorama** > **Plugins**（插件），然后单击 **Check Now**（立即检查）以获取可用的插件列表。
2. 选择 **Download**（下载），然后 **Install**（安装）Kubernetes 插件。

   安装成功后，Panorama 将刷新，**Panorama** 选项卡上会显示 Kubernetes 插件。

如果 Panorama 部署在 HA 对中，请按步骤 3 中所述的以上步骤在辅助（被动）Panorama 上安装 Kubernetes 插件。



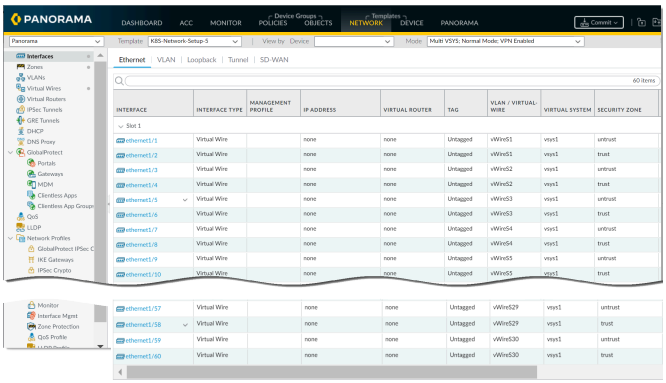
您还可以在 Panorama **Dashboard**（指示板）上验证 General Information（常规信息）小部件。



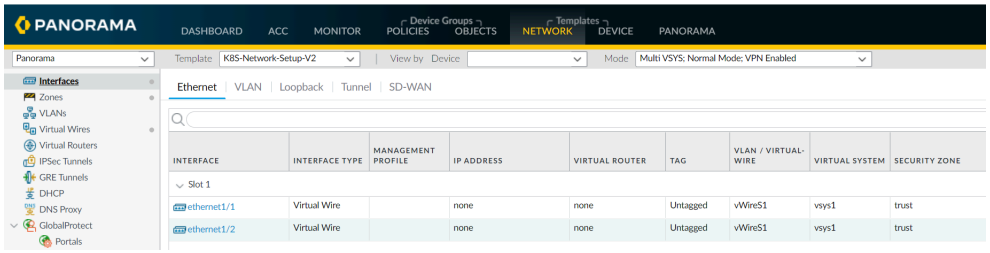
STEP 4 | 在 Panorama 上提交更改。

单击 **Commit to Panorama**（提交到 **Panorama**）。该提交将创建四个模板 — **K8S-Network-Setup**、**K8S-Network-Setup-V2**、**K8S-Network-Setup-V3** 和 **K8S-Network-Setup-V3-HA**。这些接口显示在 Panorama 上最多可能需要一分钟的时间。

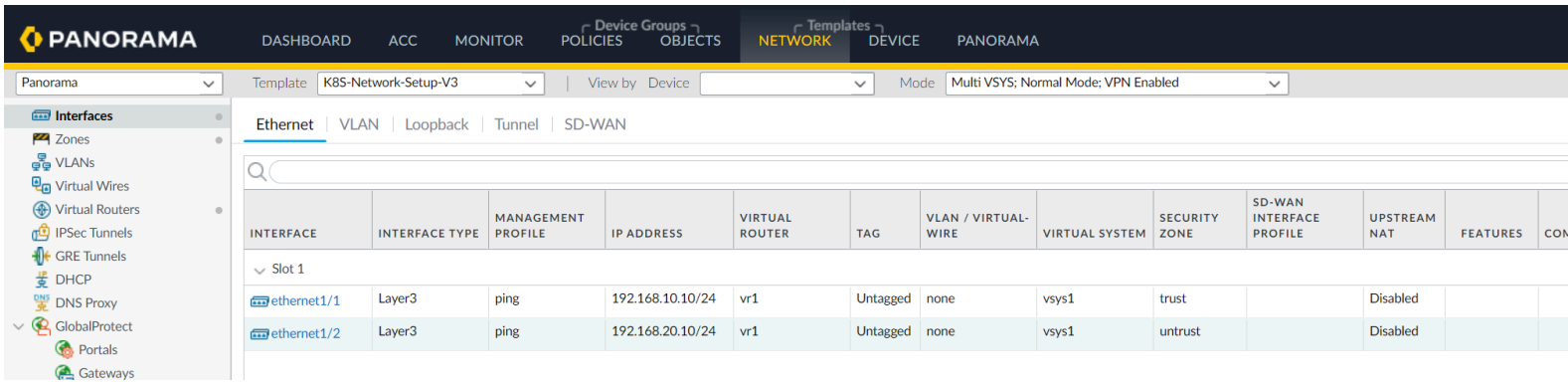
- **K8S-Network-Setup** 与 CN-Series 即 DaemonSet 一起使用，并且有 30 条虚拟线路，以及一对用于保护应用程序的接口（虚拟线路的一部分）。因此，CN-NGFW 在一个节点上可以最多保护 30 个应用程序 Pod。



- **K8S-Network-Setup-V2** 旨在与 CN-Series 即 Kubernetes 服务搭配使用，并具有一条虚拟线路，以及一对用于保护应用程序的接口（虚拟线路的一部分）。

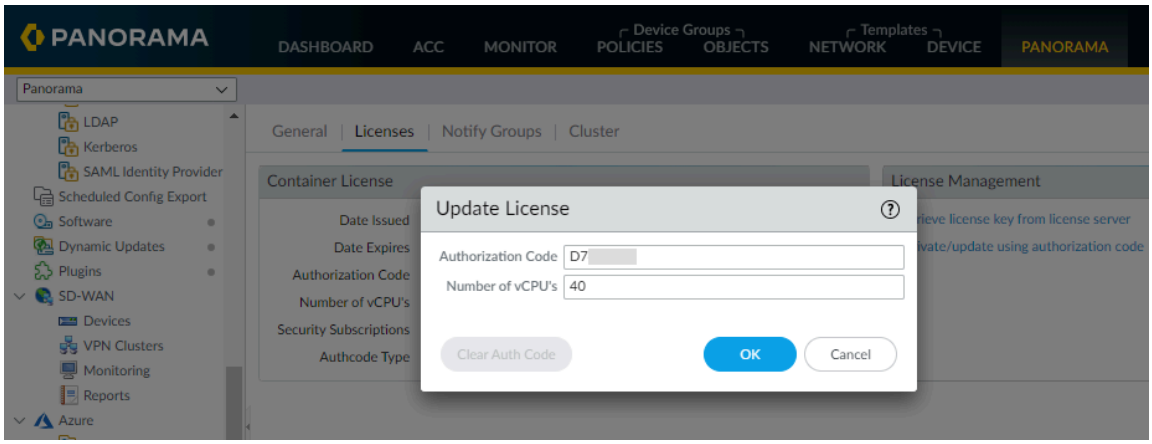


- **K8S-Network-Setup-V3** 模板有一个示例配置，您可以克隆该配置，也可以对其进行修改以匹配所需的配置。Kubernetes CNF 部署模式可保护容器和非容器工作负载。您可以将其部署为独立的第 3 层部署。



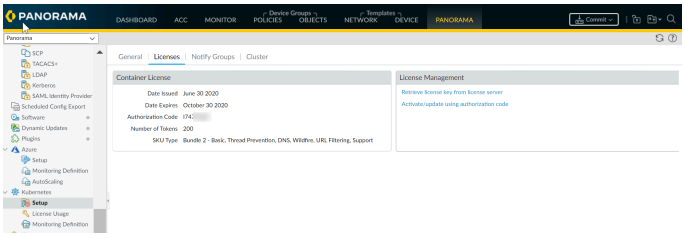
STEP 5 | 在 Panorama 上获取 CN-Series 许可证积分。

1. 选择 **Panorama** > **Plugins**（插件） > **Kubernetes** > **Setup**（设置） > **Licenses**（许可证）。
2. 选择**Activate/update using authorization code**（使用授权代码激活/更新），然后输入授权代码和所需的 vCPU 总数。您必须创建 CN-Series 部署配置文件才能获得 CN-Series 授权代码。



如果在不激活许可证的情况下部署 CN-Series 防火墙，则将会有 4 个小时的宽限期，此后防火墙将停止处理流量。宽限期过后，CN-NGFW 实例将根据 `pan-cn-ngfw-configmap.yaml` 中定义的 (FAILOVER_MODE) 进入 failopen（默认）或 failclosed 模式。在 failopen 模式下，防火墙将接收数据包并将其发送出去，而不应用任何安全策略。转换为 failopen 模式将需要重新启动，并且在重新启动过程中可能会导致流量短暂中断（预计大约 10 至 30 秒）。在 failclosed 模式下，防火墙将丢弃收到的所有数据包。fail-close 模式可能会导致关闭 CN-NGFW Pod，并将积分释放到可用积分池以许可新的 CN-NGFW Pod。

3. 确认已更新可用许可证积分数量。



STEP 6 | 生成 VM 身份验证密钥。

1. 请确保符合以下前提条件：
   - 您有可访问 Panorama 网络的计算机。
   - 您知道 Panorama IP 地址。
   - 管理接口支持 SSH，这是默认设置。如果管理员已禁用 SSH，但您要重新启用它：选择 **Panorama** > **Setup**（设置） > **Interfaces**（接口），单击 **Management**（管理），选择 **SSH**，单击 **OK**（确定），选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），然后将更改 **Commit**（提交）到 Panorama 配置。
2. 要使用 SSH 访问 CLI：
   1. 在 SSH 客户端中输入 Panorama IP 地址并使用端口 22。
   2. 在出现提示时，输入您的管理访问凭据。登录后，会显示当日消息，之后是处于操作模式的 CLI 提示符。例如：

      ```
      admin@ABC_Sydney>
      ```
3. 使用以下操作命令：

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

   举例来说，若要生成一个有效期为 24 小时的密钥，则输入以下命令：

   request bootstrap vm-auth-key generate lifetime 24

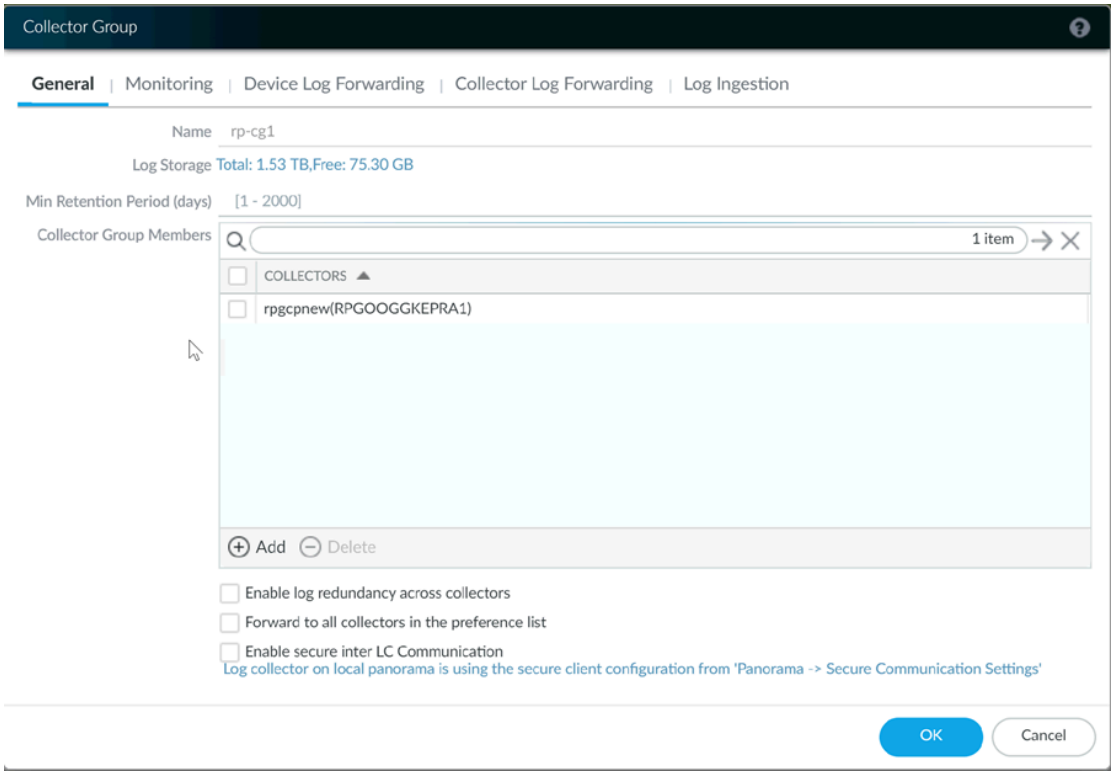
   ```
    VM auth key 755036225328715 generated.  Expires
   at:2020/01/29 12:03:52
   ```
4. 您要确保将 VM 身份验证密钥保存在某个位置，因为后续步骤需要。

STEP 7 | 创建父设备组和模板堆栈。

您必须创建模板堆栈和设备组，稍后在编辑 YAML 文件以部署 CN-MGMT Pod 时将会引用此模板堆栈和设备组。Panorama 上的 Kubernetes 插件将创建一个名为 K8S-Network-Setup 的模板，该模板将成为您在此处定义的模板堆栈的一部分。

1. 创建一个模板堆栈，然后将 K8S-Network-Setup 模板添加到该模板堆栈。
   1. 选择 **Panorama** > **Templates**（模板），然后 **Add Stack**（添加堆栈）。
   2. 输入唯一的**Name**（名称）以标识该堆栈。
   3. 添加并选择 **K8S-Network-Setup** 模板（用于 DaemonSet）、**K8S-Network-Setup-V2**（用于 Kubernetes 即服务部署）、**K8S-Network-Setup-V3**（用于独立 CNF 部署）或 **K8S-Network-Setup-V3-HA**（用于 CNF HA 部署）。
   4. 单击 **OK**（确定）。
2. 创建设备组。
   1. 转到 **Panorama** > **Device Groups**（设备组），然后单击 **Add**（添加）。
   2. 输入唯一的 **Name**（名称）和 **Description**（说明），以标识设备组。
   3. 选择将处于您在设备组层次结构中所创建的设备组正上方的 **Parent Device Group**（父设备组）（默认为 **Shared**（共享））。
   4. 单击 **OK**（确定）。
3. 如果使用 Panorama 虚拟设备，则可以创建一个日志收集器，并将其添加到日志收集器组。
   1. 转到 **Panorama** > **Collector Groups**（收集器组），然后 **Add**（添加）收集器组。
   2. 输入日志收集器的 **Name**（名称）。
   3. 输入收集器组将保留防火墙日志的**Minimum Retention Period**（最小保留期）天数（范围为 1 至 2,000）。

      默认情况下，该字段为空，这表示收集器组无限期地保留日志。
   4. 将日志收集器（1 至 16 个）**Add**（添加）到收集器组成员列表。



5. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后将更改 **Commit and Push**（提交并推送）到 Panorama 和配置的收集器组。

4. 如果您正在使用高级路由，请启用它。

   1. 转到 **Panorama** > **Templates**（模板）> **Device**（设备）。
   2. 在 **Management**（管理）选项卡中，选择 **Advanced Routing**（高级路由）（这仅适用于 Kubernetes CNF 模式的部署）。

STEP 8 | 设置 Kubernetes 插件以监控集群。

该过程的下一步是将 Kubernetes 集群信息添加到 Panorama 中，以确保两者可以相互通信。

Panorama 最多支持 *32* 个 *Kubernetes* 集群。

为确保插件和 Kubernetes 集群同步，该插件会以配置的间隔轮询 Kubernetes API 服务器，并以预定义的间隔监听来自 Kubernetes Watch API 的通知。

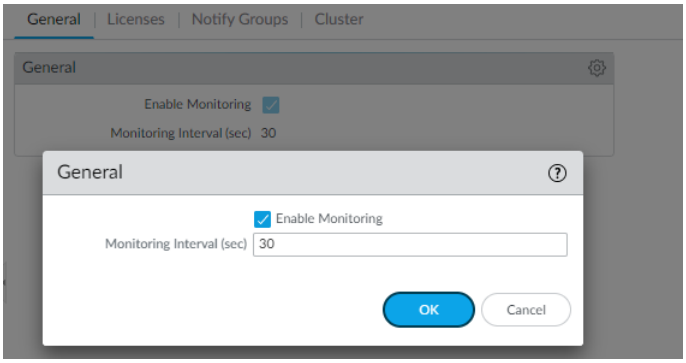
添加集群信息后，Panorama 将始终检索服务、节点和副本集等内容并为其创建标记，以查看并控制往返于这些集群之间的流量。（可选）您还可以指定是否希望 Panorama 检索有关

Kubernetes 标签的信息并为其创建标签。有关支持的属性列表，请参阅 Kubernetes 属性的 IP 地址到标签映射。

1. 检查监控间隔。

   Panorama 轮询 Kubernetes API 服务器端点的默认间隔为 30 秒。

   1. 选择 **Panorama** > **Plugins**（插件） > **Kubernetes** > **Setup**（设置） > **General**（常规）。
   2. 确认已选中 **Enable Monitoring**（启用监控）。
   3. 单击齿轮图标以编辑 **Monitoring Interval**（监控间隔），并将其更改为 30 至 300 秒的范围。

2. 选择 **Panorama** > **Plugins**（插件） > **Kubernetes** > **Setup**（设置） > **Cluster**（集群），然后 **Add Cluster**（添加集群）。

   确保不要将同一 Kubernetes 集群添加到多个 Panorama（单个实例或 HA 对）设备，因为将 IP 地址到映射注册到设备组的方式不一致。

3. 输入 **Name**（名称）和 **API Server Address**（**API** 服务器地址）。

   这是必须从 Kubernetes 部署中获取的集群的端点 IP 地址。输入一个名称（最多 20 个字符），以唯一标识集群的名称。您无法修改此名称，因为 Panorama 在为集群中所发现的 Pod、节点和服务创建标签时会使用该集群名称。

   API 服务器地址的格式可以是主机名或 IP 地址:端口号，如果使用端口 443（默认端口），则无需指定端口。

4. 选择要在其中部署集群的环境的 **Type**（类型）。

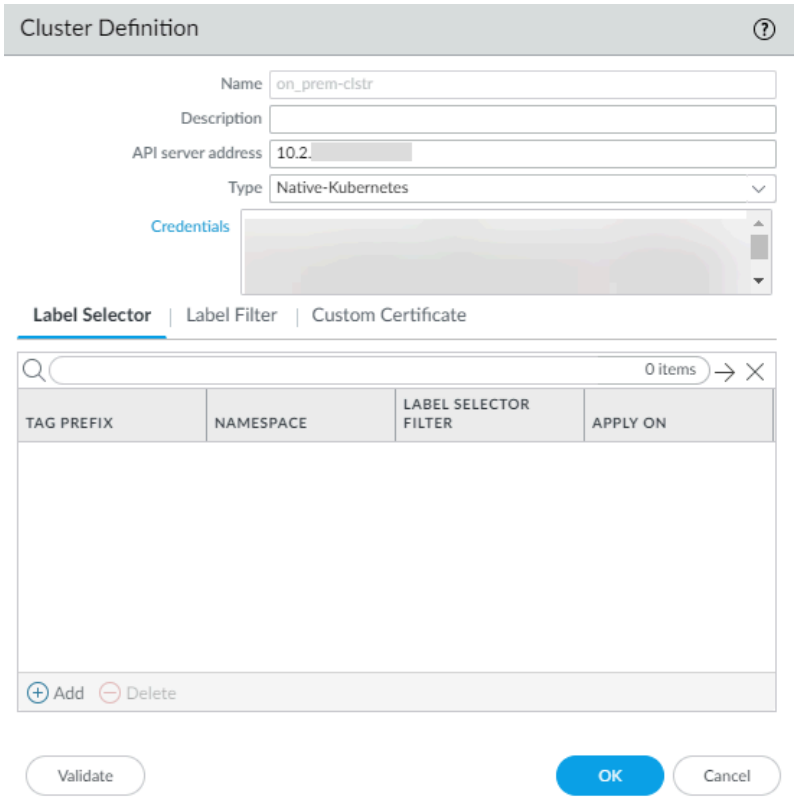
   可用选项为 AKS、EKS、GKE、Native Kubernetes、OpenShift 和其他。

5. 上传 Panorama 与集群进行通信所需的服务帐户 **Credential**（凭据）。如创建用于集群身份验证的服务帐户工作流程中所述，此服务帐户的文件名为 `plugin-svc-acct.json`。

   如果通过 *CLI/API* 上传服务凭据，则必须将文件 *gzip*，并对压缩文件进行 *base64* 编码，然后将文件内容上传或粘贴到 *Panorama CLI* 或 *API* 中。如果要在 *GUI* 上上传服务凭据文件，则不需要执行这些步骤。

6. 单击 **OK**（确定）。

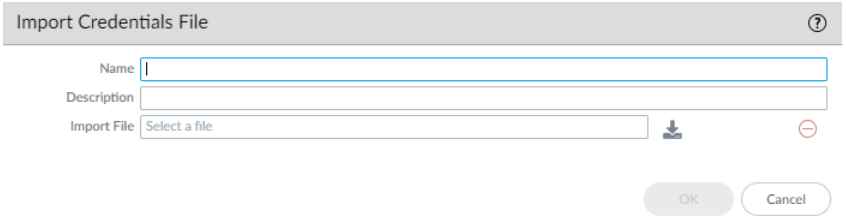
您可以保留标签筛选器和标签选择器配置以备后用。这是一项可选任务，能让您检索希望 Panorama 为其创建标签的任何自定义标签或用户定义的标签。



STEP 9 | （可选）如果您的 Kubernetes 集群 API 服务器证书由证书链签名，则来自 Panorama 的 Kubernetes 插件的身份验证需要链中的每个证书。如果 API 服务器使用证书链，则必须将链中的所有证书合并为一个 .crt 文件，并将其添加到插件中。

Kubernetes 插件最多支持四个证书。

1. 选择 **Panorama** > **Kubernetes** > **Setup**（设置） > **Cluster**（集群） > **Add**（添加） > **Custom Certificate**（自定义证书） > **Add**（添加）以导入证书文件。
2. 输入描述性的 **Name**（名称）。
3. （可选）输入 **Description**（说明）。
4. 单击导入图标并导航到证书文件。
5. 单击 **OK**（确定）。



STEP 10 | （可选）为每个集群配置代理。

与其他插件不同，Kubernetes 插件不使用在 **Panorma** > **Setup**（设置） > **Services**（服务）下配置的代理。相反，如果要启用或绕过代理，则必须为每个集群输入代理。配置后，Kubernetes 插件将使用此代理服务器 IP 地址对该集群的 API 服务进行所有 API 调用。

1. 登录到 Panorama 命令行界面。
2. 输入以下 CLI 命令为此 Kubernetes 集群配置代理服务器。

   ```
   > 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>
   *** username and password are optional ***
   ```

STEP 11 | 后续步骤：

1. 获取用于 CN-Series 部署的映像和文件
2. 部署 CN-Series 防火墙。
3. 配置 Panorama 以保护 Kubernetes 部署

获取用于 CN-Series 部署的映像和文件

在何处可以使用？	需要提供什么？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • 运行 PAN-OS 10.1.x 或更高版本的 Panorama • 使用 Helm 部署 CN-Series 的 Helm 3.6 or above version client

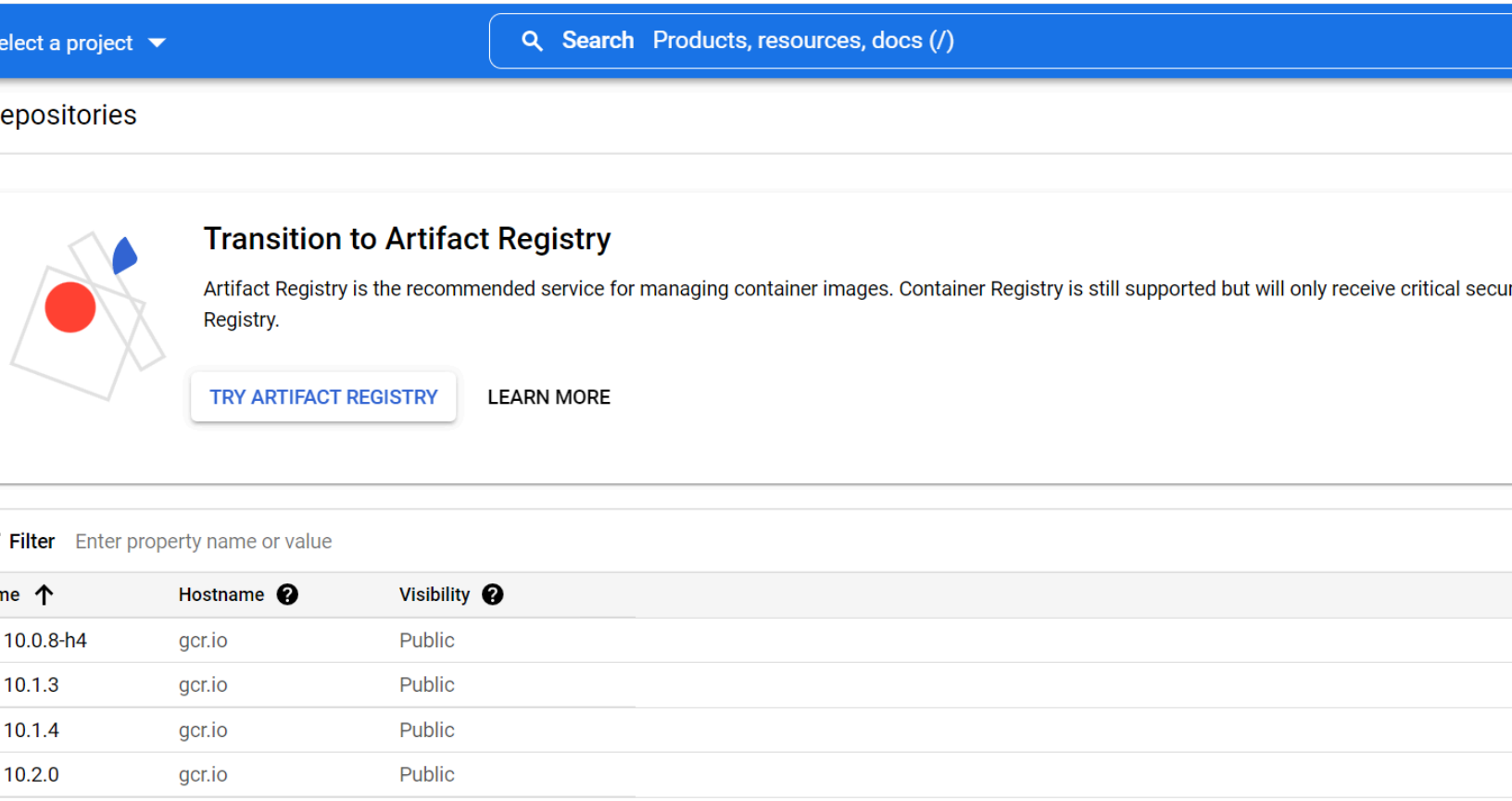
开始部署之前，请参阅下表以确保已下载兼容文件。

PAN-OS 版本	**YAML** 版本	**CNI** 版	**MGMT-INIT** 版本
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

按照以下步骤从 Google Cloud Platform 上的公共容器注册表中提取 Docker 镜像，然后继续部署 CN-Series 防火墙：

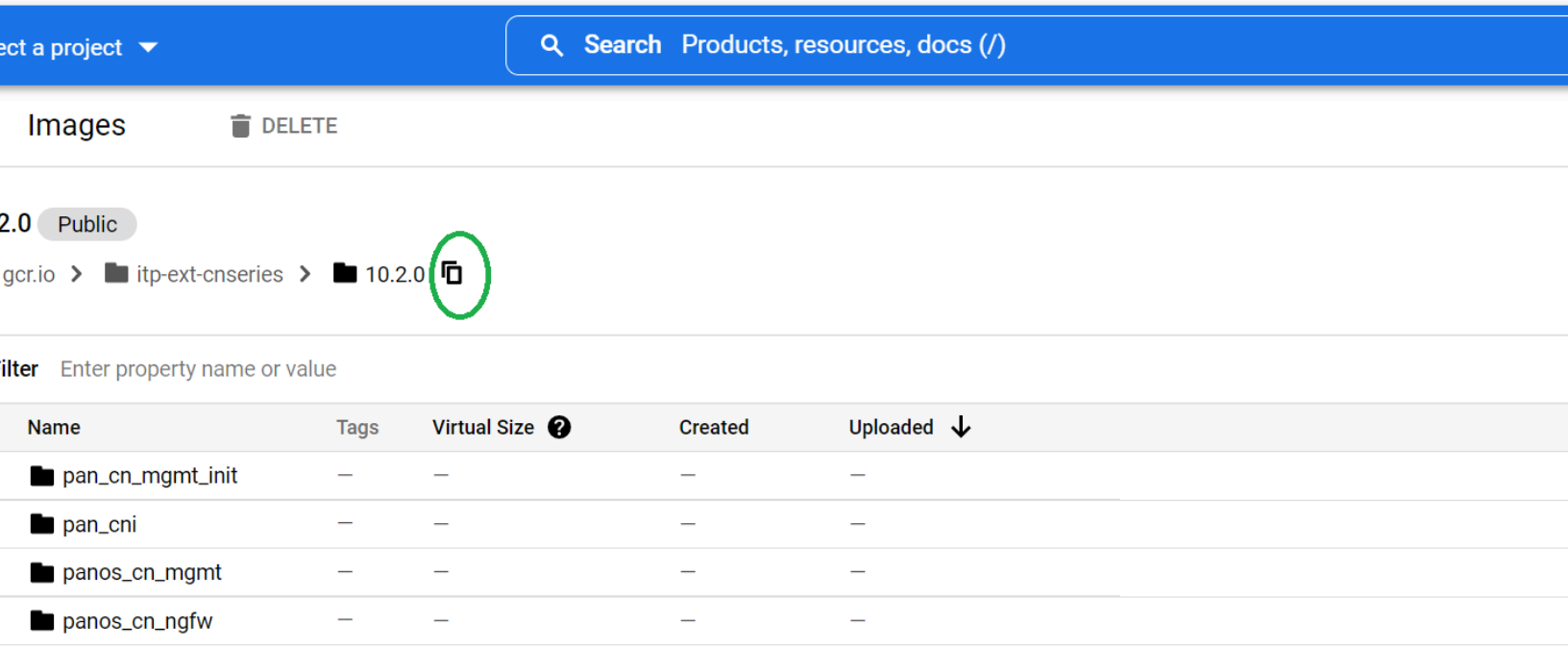
来自公共容器注册表的 **Docker** 映像：

1. 根据 PAN-OS 版本，从公共云存储库中提取所需的 Docker 映像。



2. 选择所需的 PAN OS 版本。

3. 将每个映像路径的链接复制到部署 YAML 文件中的适当位置。



执行以下操作以从 GitHub 获取 YAML 文件：

1. 打开部署方法的文件夹 - DaemonSet、Kubernetes 服务或 Kubernetes CNF。
2. 从与您的环境对应的文件夹下载 yaml 文件。

   从 Native-k8s 文件夹获取文件，以用于本机 Kubernetes 本地部署或云部署。

   从 AKS、EKS 或 GKE 的相应托管 Kubernetes 文件夹获取文件。

来自 **Palo Alto Networks CSP** 的 **Docker** 图像：

按照以下说明从 GitHub 获取 YAML 文件，并从 Palo Alto Networks CSP 下载 Docker 映像，然后将其推送到私有注册表，再继续部署 CN-Series 防火墙。

STEP 1 | 下载 Docker 映像和 YAML 文件。

1. 从 Palo Alto Networks 客户支持门户 (CSP) 获取压缩的 tar 存档文件。
   1. 使用支持帐户登录 CSP。
   2. 选择 **Updates**（更新） > **Software Updates**（软件更新）。
   3. 从 **Please Select**（请选择）下拉列表中选择 **PAN-OS Container Images**（**PAN-OS** 容器映像）。
   4. 为要部署的 PAN-OS 版本下载以下文件。

      PanOS_cn-X.X.X.tgz - for CN-MGMT and CN-NGFW Pods.

      Pan_cn_mgmt_init-X.X.X.tgz - for the init container that runs as a part of the CN-MGMT Pod.

      Pan_cni-2.0.0.tgz - for the PAN-CNI Pod.
2. 从 GitHub 获取 YAML 文件。
   1. 打开部署方法（DaemonSet、Kubernetes 服务或 Kubernetes CNF）的文件夹。
   2. 从与您的环境对应的文件夹下载 yaml 文件。

      从 Native-k8s 文件夹获取文件，以用于 Native Kubernetes 本地部署或云部署。

      从 AKS、EKS 或 GKE 的各自托管 Kubernetes 文件夹获取文件。

STEP 2 | 检索 Docker 映像并将其推送到容器注册表。

例如，在 GKE 部署中，您可将映像上传到 GKE 上的容器注册表，并在 YAML 文件中获取要引用的映像路径。在运行 Docker 引擎的客户端系统中使用以下命令。

将以下步骤中的 *x* 变量替换为与您正在使用的映像版本匹配的值。例如，*Pan_cn_mgmt-init-2.0.0.tgz* 或 *pan_cni:2.0.0*。

1. 加载映像。

   ```
   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
   ```

   完成这些步骤后，“docker images”将显示映像，例如“paloaltonetworks/panos_cn_mgmt:x.x.x”。

2. 为这些映像添加标签以包括专用注册表详细信息。

   ```
   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. 将这些映像推送到专用注册表。

   ```
   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
   ```

使用 CN-Series 防火墙的 Strata 日志记录服务

在何处可以使用？	需要提供什么？
• 具有 CN-Series 防火墙的 Strata 日志记录服务	• 最低运行 PAN-OS 11.1 版本的 Panorama • Strata 日志记录服务许可证

Strata 日志记录服务支持基于 AI 的网络安全创新，采用业界唯一的方法将企业数据标准化并拼接到一起。有关详细信息，请参阅 Strata 日志记录服务简介和适用于 Panorama-Managed 防火墙的 Strata 日志记录服务。Strata 日志服务现在可以从 CN-Series 新一代防火墙收集日志数据。当您购买 Strata 日志记录服务许可证时，所有注册到您的支持帐户的防火墙都会收到 Strata 日志记录服务许可证。您还将收到一个 Magic 链接，您需要使用它来激活 Strata 日志记录服务实例。

要开始使用 CN-Series 防火墙 Strata 日志记录服务记录日志，您必须确保为 CN-Series 防火墙安装 Kubernetes 插件并设置 Panorama。向 CN-MGMT Pod 提供设备证书，以连接 Strata 日志记录服务连接。使用 CSP 帐户注册 CN-MGMT Pod 非常重要，这样才能确保 CN-MGMT Pod 反映在 Strata 日志记录服务实例中。将有效的 PIN-ID 和 PIN 值添加到 `pan-cn-mgmt-secret.yaml` 文件中以成功安装设备证书。CN-Series 防火墙需要一个设备证书来授权对 Strata 日志记录服务的安全访问。有关详细信息，请参阅在 CN-Series 防火墙上安装设备证书。

在部署 CN-Series 防火墙后，请验证您的 CN-MGMT Pod 是否在客户支持门户帐户上的已注册设备下可见。有关详细信息，请参阅注册防火墙。请确保使用 Panorama 配置 CN-Series 防火墙，并在您的 CSP 帐户上创建 CN-Series 部署配置文件，然后使用身份验证代码将许可证从 Panorama 推送到 CN-Series 防火墙。

为 **CN-Series** 防火墙配置 **Strata** 日志记录服务

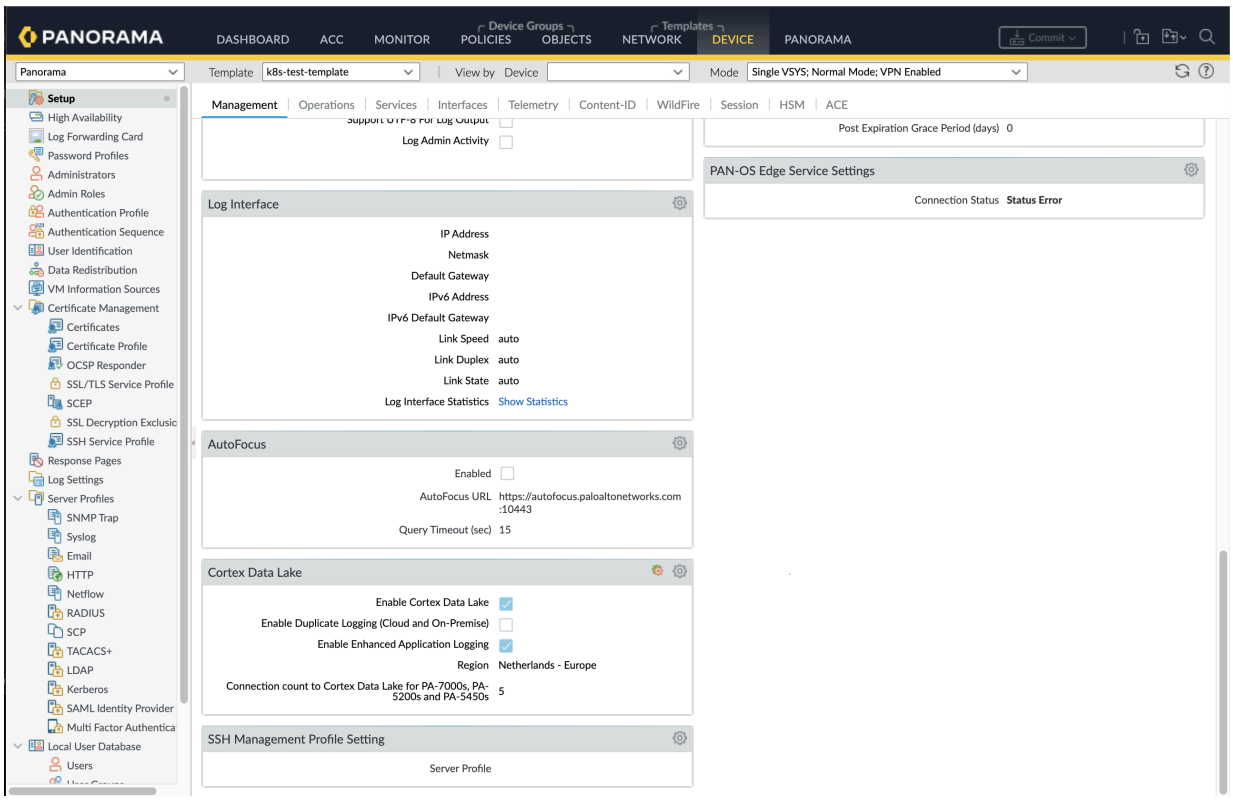
Strata 日志记录服务为云交付的服务和应用程序提供基于云的集中式日志存储和聚合。

确保您有一个日志许可证和一个在 *CSP* 帐户中创建的 *Strata* 日志服务实例。有关详细信息，请参阅 Strata 日志记录服务。

完成以下步骤以在 Panorama 上配置 Strata 日志记录服务设置并将其推送到防火墙：

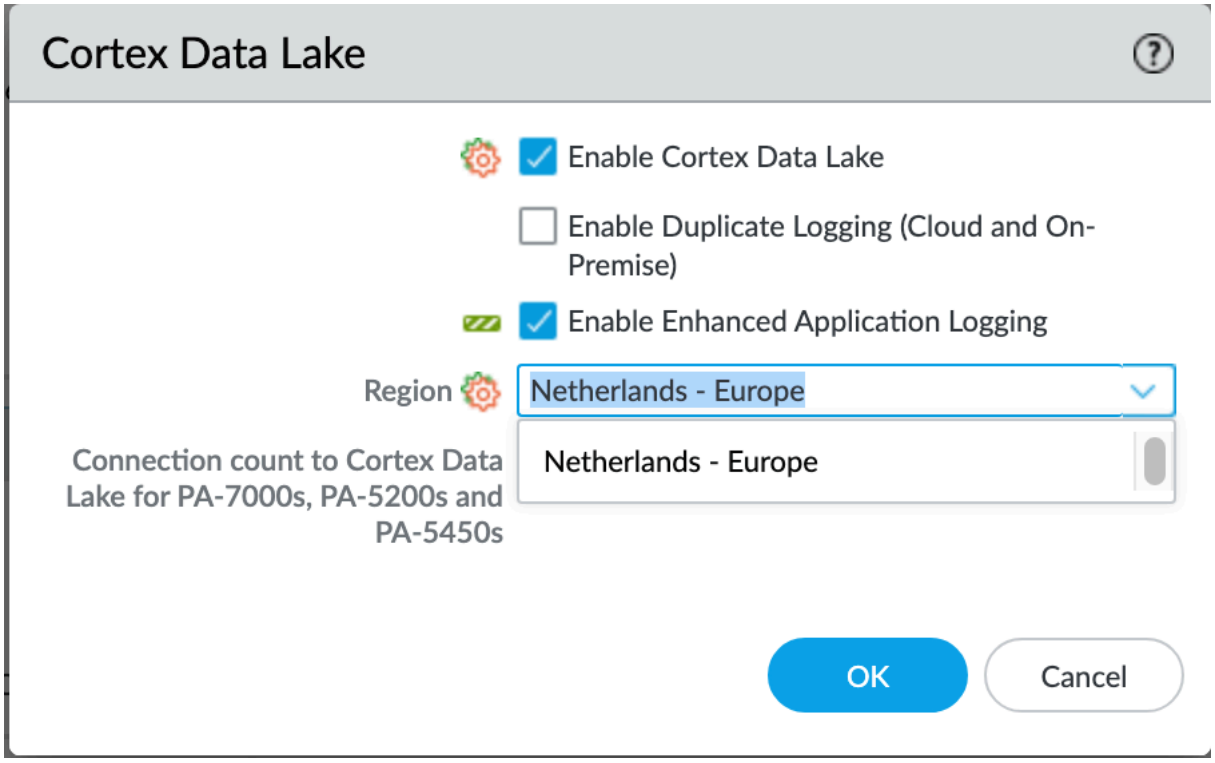
1. 将您的 Panorama 加入 Strata 日志记录服务，以在设备上启用 Strata 日志记录服务配置的设置。
2. 将 CN-Series 防火墙加入 Strata 日志记录服务实例。

3. 在 Panorama 中，转到设备选项卡，然后在 **Strata** 日志记录服务窗格中单击设置。



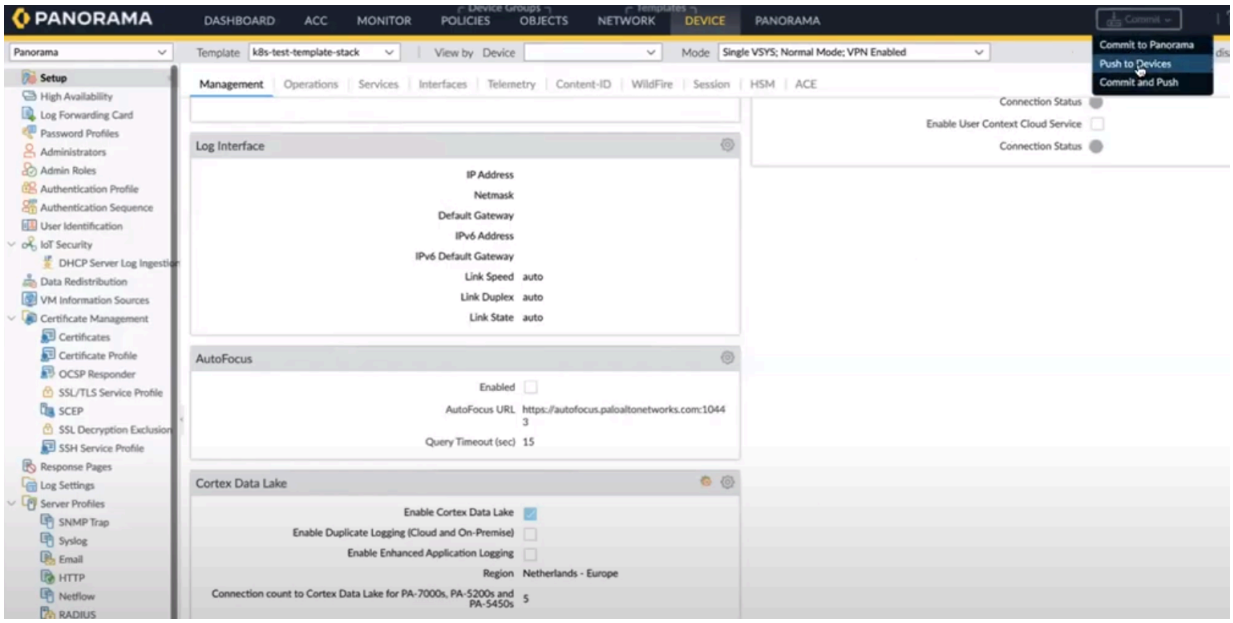
现在，您会看到已填写该区域。

4. 单击启用 **Strata** 日志记录服务。



5. 单击 **OK**（确定）。

6. 转至 > 推送到设备。



7. 选择 **CN-MGMT** Pod。

8. 点击确定。

   现在已推送 CN-MGMT Pod 的 Strata 日志记录服务配置。CN-MGMT Pod 现在将启动与 Strata 日志记录服务实例的连接。

一旦已加入的防火墙处于连接状态，您就可以开始向 Strata 日志服务实例发送日志。有关更多信息，请参阅开始将日志发送到 Strata 日志记录服务 (Panorama-Managed)。

适用于 CN-Series 防火墙的 IoT Security 支持

在何处可以使用？	需要提供什么？
• 适用于 CN-Series 防火墙的 IoT Security	• 适用于 IoT 订阅的 Strata 日志记录服务许可证，用于将数据存储在 Strata 日志记录服务中 • 最低运行 PAN-OS 11.1 版本的 Panorama

对于 Palo Alto Networks 下一代 CN 系列防火墙，IoT Security 解决方案根据从防火墙接收的日志中的元数据，使用机器学习 (ML) 提供已发现的 IoT 设备的可见性。IoT Security 还会根据设备的网络流量行为和动态更新的威胁源来识别设备的漏洞并评估风险。

手动向 CN-Series 防火墙添加规则时，可以使用 IoT Security 生成的策略规则建议作为参考。无论 PAN-OS 版本如何，IoT Security 始终会生成安全策略规则建议。

当使用将数据存储在 *Strata* 日志记录服务中的 ***IoT Security*** 订阅时，每个帐户需要一个 *Strata* 日志记录服务许可证，并且必须确保已完成 CN-Series 防火墙的 Strata 日志记录服务配置。

有关更多信息，请参阅 IoT Security 先决条件。

为 **CN-Series** 防火墙配置 **IoT** 支持

您必须确保环境满足使用 CN-Series 防火墙部署 IoT Security 的所有先决条件。有关更多信息，请参阅 IoT Security 先决条件。

要为 CN-Series 防火墙配置 **IoT -** 需要数据湖订阅，您必须完成以下步骤：

必须确保将 *Panorama* 加入 *Strata* 日志记录服务实例中。有关详细信息，请参阅使用 Panorama 加入防火墙。

1. 创建租户服务组 (TSG)。有关详细信息，请参阅通过常用服务激活 IoT Security 订阅中的步骤 **3**。
2. 将 Strata 日志记录服务租户加入 TSG。您必须确保购买 Strata 日志记录服务并使用 Magic 链接将其激活，然后才能在 TSG 中使用。
3. 使用 **IoT -** 需要数据湖选项创建 CN-Series 部署配置文件。
4. 单击完成设置。将部署配置文件关联到 TSG 并单击激活后，如果不存在 IoT 租户，则会创建一个。

然后，您可以将收集到的元数据转发到基于云的日志记录服务，IoT Security 会使用它来识别网络上的各种 IoT 设备。

5. 配置 Panorama 并生成序列号。有关更多信息，请参阅注册 Panorama 并安装许可证。
6. 使用身份验证代码通过 Panorama 配置您的 CN-Series 防火墙，以使用 Kubernetes 插件将许可证从 Panorama 推送到 CN-Series 防火墙。有关详细信息，请参阅配置 Panorama 以保护 Kubernetes 部署。

   将部署身份验证代码应用于 Panorama 中的 Kubernetes 插件。

   您现在可以看到 CN-Series 防火墙已加入 IoT 租户。
7. 配置模板 vwire 以允许并启用区域中的 Device-ID。

   您可以使用默认模板 **K8S-Network-Setup-V2**，并在该模板中进行以下更改：

   - 为默认 vwire 启用链路状态直通和多播防火墙。
   - 为默认区域启用设备识别。

   有关详细信息，请参阅配置虚拟线路。
8. 将 Panorama 的启用 **Cortex Data Lake** 和启用增强应用程序日志记录选项配置为 CN-Series 防火墙。有关更多信息，请参阅 CN-Series 防火墙的 Strata 日志记录服务配置。

对于 CN-Series 防火墙，要配置 **IoT Security**，不需要数据湖订阅，您必须完成以下步骤：

注意：您必须确保将 Panorama 加入 Strata 日志记录服务实例中。使用“IoT Security 时，不需要数据湖”订阅时，在添加 CN-Series 防火墙后，您必须在 IoT 门户中注册 Panorama。有关更多信息，请参阅为 IoT Security 准备防火墙中的步骤 **2**。

1. 创建租户服务组 (TSG)。有关详细信息，请参阅通过常用服务激活 IoT Security 订阅中的步骤 **3**。
2. 使用 **IoT -** 不需要数据湖选项创建 CN-Series 部署配置文件。
3. 设置您的 IoT 实例并选择完成设置选项，将您的部署配置文件与租户服务组 (TSG) 相关联，以便在您的 CN-Series 防火墙上启用日志记录服务，并将其配置为获取和记录网络流量元数据。有关更多信息，请参阅为 IoT Security 准备防火墙。

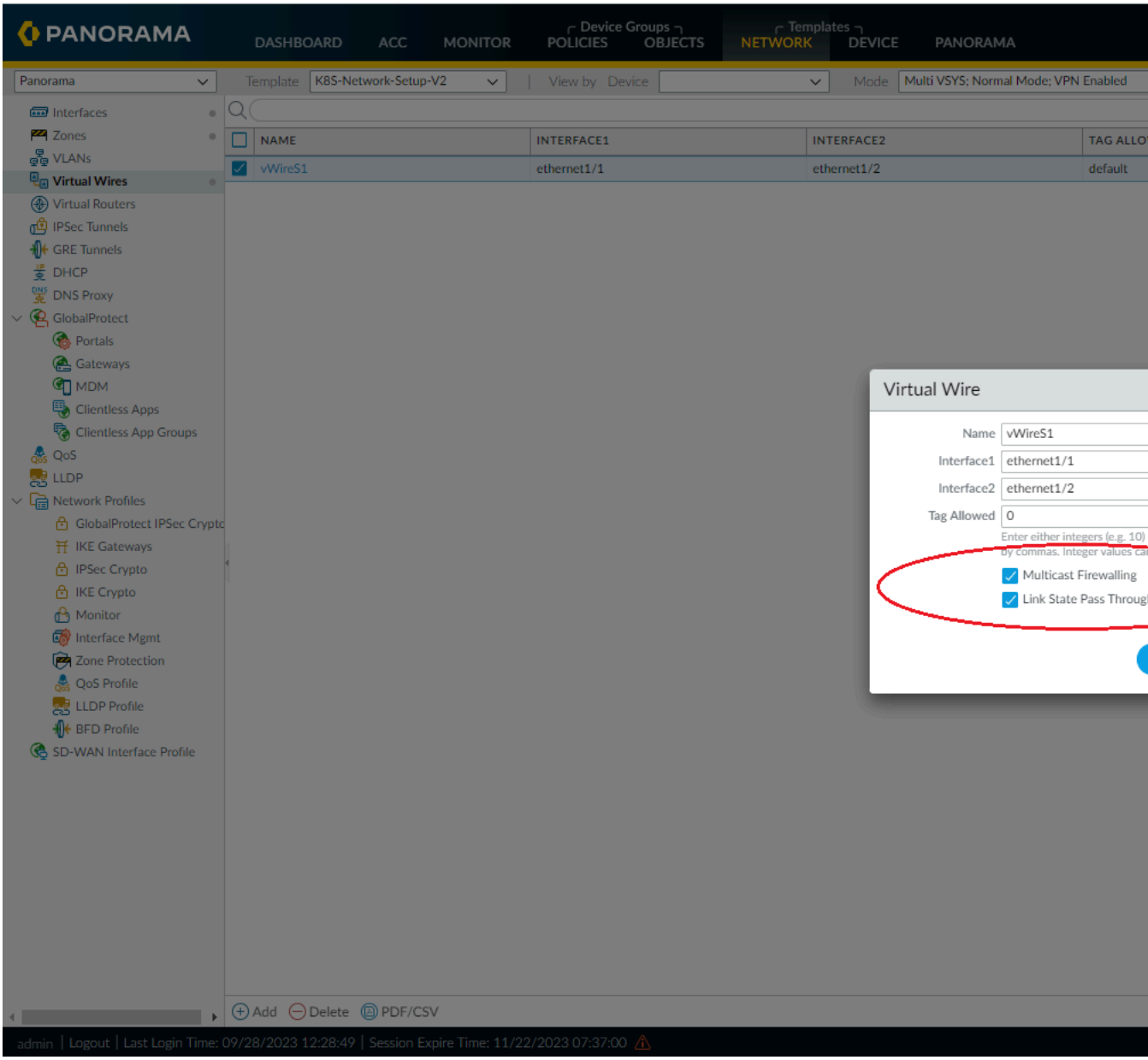
   然后，您可以将收集到的元数据转发到基于云的日志记录服务，IoT Security 会使用它来识别网络上的各种 IoT 设备。
4. 配置 Panorama 并生成序列号。有关更多信息，请参阅注册 Panorama 并安装许可证。
5. 使用身份验证代码通过 Panorama 配置您的 CN-Series 防火墙，以使用 Kubernetes 插件将许可证从 Panorama 推送到 CN-Series 防火墙。有关详细信息，请参阅配置 Panorama 以保护 Kubernetes 部署。

   将部署身份验证代码应用于 Panorama 中的 Kubernetes 插件。您现在可以看到 CN-Series 防火墙已加入 IoT 租户。

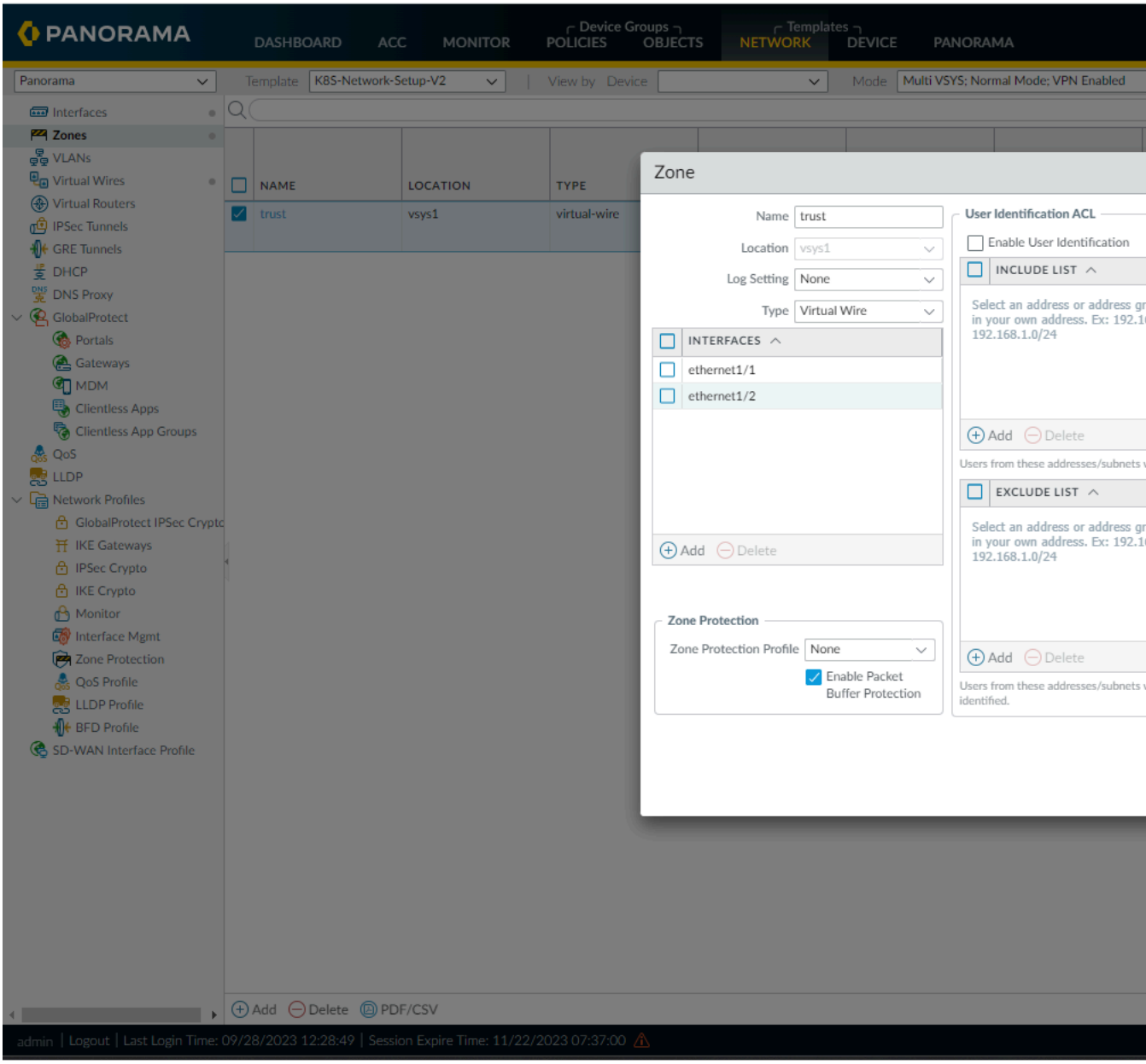
6. 配置模板 vwire 以允许并启用区域中的 Device-ID。有关详细信息，请参阅配置虚拟线路。

   您可以使用默认模板 **K8S-Network-Setup-V** 并在该模板中进行以下更改：

   - 为默认 vwire 启用链路状态直通和多播防火墙。



   - 为默认区域启用设备识别。



有关详细信息，请参阅配置虚拟线路。

k8s-template-v2 中配置的 vwire 允许链路状态直通和多播防火墙。k8s-template-v2 的区域配置可以实现设备识别

7. 将 Panorama 的启用 **Cortex Data Lake** 和启用增强应用程序日志记录选项配置为 CN-Series 防火墙。有关详细信息，请参阅适用于 CN-Series 防火墙的 Strata 日志记录服务配置

在成功将 Panorama 和 CN-Series 防火墙加入基于云的日志记录服务后，请转到您的 IoT 实例。

当 IoT Security 拥有足够的信息，可从网络行为中识别设备后，它会为 CN-Series 防火墙提供 IP 地址到设备的映射，并为 Panorama 提供策略建议，Panorama 管理员可以导入这些建议，然后将其推送到 CN-Series 防火墙以对 IoT 设备流量执行策略。

单击 IoT Security 门户中的管理 > 站点和防火墙 > 防火墙，查看日志记录服务传输到 IoT Security 应用程序的日志的状态。有关更多信息，请参阅 IoT Security 与防火墙的集成状态。

CN-Series 防火墙上基于软件直通的卸载

在何处可以使用？	需要提供什么？
• CN-Series Kubernetes CNF 部署	• CN-Series 10.1.x or above Container Images • 对于 Panorama 托管的 CN-Series 防火墙，运行 PAN-OS 11.0.4 或更高版本的 Panorama

概述

借助基于软件直通的智能流量卸载 (ITO) 服务，CN-Series 防火墙消除了网络性能、安全性和成本之间的权衡。对于网络中的每个新流，ITO 服务都会确定该流是否可以从安全检查中受益。ITO 服务将流的前几个数据包路由到防火墙进行检查，以确定是否检查或卸载流中的其余数据包。此决定基于无法检查的政策或流程。通过仅检查可以从安全检查中受益的流量，防火墙的总体负载会减少，性能会提高，而不会牺牲安全态势。

对于缺少 DPU 的基础设施，基于软件直通的 ITO 能够利用可用的 NIC 来发挥作用。请参阅虚拟机管理程序支持矩阵以了解支持的 NIC 和虚拟机管理程序。

基于软件直通的卸载支持 GTP-U 隧道协议。在 GTP-U 中，通过 GTPU 内部会话软件协调通用时间直通，在 GTPU 内部会话完成第 7 层检查后，GTPU 数据包将遵循现有的软件直通数据路径，绕过不必要的操作，利用 FIB/MAC 缓存，并运行至完成。将 CN-Series 防火墙部署为 Kubernetes CNF 服务时，CN-Series 防火墙支持 PAN-OS 软件直通功能，以用于 GTP-U 特定流量卸载。

CN-Series 防火墙上的 **GTP-U** 特定流量卸载

GTP 包括控制平面 (GTP-C)、用户平面 (GTP-U) 和在 UDP/IP 上传输的计费（源自 GTP-C 的 GTP）。查看支持 GTP 的 PAN-OS 版本型号以及 GTPv1-C、GTPv2-C 和 GTP-U 支持的 3GPP 技术标准。在 Palo Alto Networks® 防火墙上启用 GTP Security 可让您保护移动核心网络基础设施免受格式错误的 GTP 数据包、拒绝服务攻击和错误状态 GTP 消息的侵害，还可让您保护移动用户免受欺骗 IP 数据包和超额计费攻击。

GTP-U 在 3GPP TS 29.281 中定义。它封装并路由跨多个信令接口（例如 S1、S5 和 S8）的用户平面流量。GTP-U 消息可以是用户平面消息，也可以是信令消息。GTP-U 的注册端口号是 2152。有关更多信息，请参阅 GTP 保护配置文件。

CN-Series 上基于软件直通的卸载也支持 GTP-U 流量卸载。您现在可以将 CN-Series 上的智能流量卸载订阅用作 Kubernetes CNF 模式，以解锁更高的性能并利用 GTP Security 保护移动网络。对于 CN-Series 即 Kubernetes CNF 模式将检查的每个 GTP-U 数据包，都将在内部会话上完成完整的第 7

层检查。如果防火墙确定此 GTP-U 数据包的内部会话符合卸载条件，则会卸载属于此会话的所有后续 GTP-U 数据包。

以下是在 CN-Series 防火墙上配置基于软件直通的卸载之前需要考虑的重要事项：

- 默认情况下，基于软件直通的 ITO 配置是禁用的。
- 您只能使用 bootstrap/CLI 启用此功能。
- 您可以同时使用基于软件直通的 ITO 进行普通流量传输，并在基于软件直通的 ITO 内进行 GTP-U 卸载。
- 要升级到启用 ITO 的当前版本，请在升级后使用 CLI 启用会话卸载。

在 *CN-Series* 中，只有 *CN-Series* 即 *Kubernetes CNF* 部署模式支持基于软件直通的 *ITO*。

在 **CN-Series** 防火墙上启用 **GTP-U** 内部会话卸载

要在 CN-Series 防火墙上启用 GTP-U 内部会话卸载，以下是启用 GTP 安全或 5G 安全的先决条件。

您必须编辑 **`pan-cn-mgmt-configmap.yaml`** 文件并进行以下更改：

在 `pan-cn-mgmt-configmap.yaml` 文件中，`PAN_GTP_ENABLED`、`PAN_GTP_CUT_THRU` 和 `PAN_SW_CUT_THRU` 参数值必须为 `true` 才能启用 GTP-U 内部会话卸载。

以下是更新后的 `pan-cn-mgmt-configmap.yaml` 文件的示例：

```
# 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"
```