paloalto TECHDOCS

CNシリーズ スタート ガイド

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

Kubernetes 用 CN-Series ファイアウォール

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

Palo Alto Networks Container Native Firewalls(CN-Series)は、Kubernetes(k8s)にネイティブに統合され、パブリック クラウドまたはデータセンター環境のトラスト ゾーンを行き来するトラフィックに対して完全なL7の可視性、アプリケーション レベル セグメンテーション、DNSセキュリティ、および高度な脅威に対する保護を提供します。このファイアウォールを使用すれば、個々のコンテナがスケールアップ、ダウン、またはホストをまたがってスケーリングした場合でも、ワークロード、アプリケーション スタック、およびサービスを分離して保護し、Kubernetesラベルに基づくセキュリティ ポリシーを一貫して適用することができます。

Kubernetes環境でのアプリケーションのデプロイメントは動的であり、多くの場合、以下のチームがコンテナのライフサイクルに関わります。

- プラットフォーム **(PAAS)** 管理者 - パブリック クラウドとデータ センターで Kubernetes クラスタとその他のインフラストラクチャ コンポーネントを管理します。
- アプリケーション チーム - PAAS 管理者から提供されるKubernetes名前空間/プロジェクトで個々のコンテナ化されたアプリケーションやその他のアプリケーションをデプロイします。
- セキュリティ管理者 - Kubernetesクラスタと個々のコンテナ化されたアプリケーションを含むデプロイメント全体でセキュリティをプロビジョニングします。

この動的シナリオと複数のチームとの相互作用では、セキュリティの管理と監視が課題になります。CN-Seriesを使用すれば、セキュリティ管理者は、GKE、EKS、AKS、AliCloud ACKなどのクラウド プロバイダ管理のk8sや、パブリック クラウドまたはオンプレミス データセンターでのOpenshiftやネイティブk8sなどの顧客管理のk8sを含む様々な環境で、コンテナ化されたアプリケーションに対するセキュリティをプロビジョニングすることができます。CN-Seriesは、Kubernetesコンストラクトとメタデータ駆動型ポリシーを使用して、チームがデプロイメントを自動化し、セキュリティ ポリシーを効率的に適用して、既知の脅威と未知の脅威から一貫して保護できるようにします。

CNシリーズ ファイアウォールを使用してKubernetes ワークロードを保護する

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CNシリーズ ファイアウォールは、management plane(管理プレーン - MP)用(CN-MGMT)とファイアウォール データプレーン用(CN-NGFW)の2セットのポッドとしてデプロイされます。ファイアウォール データプレーンはデーモンセットとして実行されるため、Kubernetes内から1つのコマンドでKubernetesクラスタ内のすべてのノードにファイアウォールを一度にデプロイできます。management plane (管理プレーン - MP)はKubernetesサービスとして実行されます。

CNシリーズのファイアウォールはPanoramaコンソールで管理されます。Panorama内のKubernetesプラグインは、環境内のコンテナに関するコンテキスト情報を提供し、これによりコンテキストベースのネットワーク セキュリティ ポリシーをシームレスに実現できます。

たとえば、Kubernetes名前空間を使用して、ファイアウォール ポリシーでトラフィックの送信元を定義できます。CNシリーズのファイアウォールは、オンプレミスまたはパブリック クラウドでホストされるKubernetes環境にデプロイできます。

CNシリーズのファイアウォールは、Google Kubernetes Engine(GKE®)、 Azure Kubernetes Service(AKS)、 Alibaba Cloud(ACK)、 Amazon Elastic Kubernetes Service(EKS)など、クラウドで管理されるKubernetes製品にもデプロイできます。HelmなどのKubernetesパッケージ マネージャーを介してデプロイすることもできます。

CN-Series は、開発速度を落とすことなく、コンテナ トラスト ゾーンとその他のワークロード タイプ間のインバウンド、アウトバウンド、および East-West トラフィックの脅威防御を提供します。

CN-Series をデプロイしてコンテナ トラフィックに対するレイヤー 7 の可視性を確保し、脅威防御プロファイルを含むセキュリティ ポリシーを適用して Kubernetes 名前空間境界を越えて許可されたトラフィックを保護し、そのコンテキストをハードウェアや VM-Series ファイアウォールと共有してハイブリッド クラウド環境全体での一貫したポリシー適用モデルを確保します。

Kubernetes環境からのデータの流出を防ぐ:

CNシリーズ ファイアウォールは、Kubernetes環境からの機密データの流出を防ぐため、さまざまなセキュリティ機能を提供しています。TLS/SSLで暗号化されたトラフィックの検査を含むトラフィック コンテンツ検査により、悪意のあるペイロードを含むパケットが確実に特定され、

修正されます。URLフィルタリングは、悪意のあるコード リポジトリを含む潜在的に悪意のあるウェブサイトへのアウトバウンド接続を遮断します。

Kubernetes名前空間の境界を越えた脅威の横断的な拡散の防止:

アプリケーション間で信頼できる境界は、脅威の横方向の動きを防止するセグメンテーション ポリシーを適用するための論理的な場所です。多くのKubernetes環境では、Kubernetes名前空間が信頼できる境界となります。CNシリーズのファイアウォールは、Kubernetes名前空間同士だけでなく、Kubernetes名前空間と他のワークロードタイプ(VMやベアメタルサーバーなど)の間でも脅威防御ポリシーを適用できるため、クラウド ネイティブ アプリケーションとレガシー インフラストラクチャ間の移動による脅威を抑止できます。

CN-Series の主要概念

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォールは、コンテナ化された環境でアプリケーションを保護するために必要なツールを提供するように設計されています。CN シリーズがコンテナ化されたネットワークにどのように適合するかを理解するには、いくつかの重要な概念を理解することが重要です。

- クラスター— コンテナ化された環境の基盤であり、すべてのコンテナ化されたアプリケーションはクラスターの上で実行されます。
- ノード—クラスターによっては、ポッドに必要なサービスを含む仮想マシンまたは物理マシンがノードになる場合があります。
- **Pod**-Kubernetes でデプロイおよび管理できる最小のデプロイ可能なコンピューティング ユニット。CN-Series ファイアウォールは、分散 PAN-OS アーキテクチャに CN-MGMT および CN-NGFW の 2 つのポッドとしてデプロイされます。詳細については、CN-Series コアビルディングブロックを参照してください。
- 名前空間- 名前空間は、物理クラスターに裏付けられた仮想クラスターです。複数のチームや機能に多くのユーザーが分散している環境では、名前空間を使用して 1 つのクラスター上でユーザーを分離できます。
- コンテナネットワークインターフェース**(CNI)**- コンテナのネットワークインターフェースを設定するプラグイン。さらに、CNI は、コンテナが削除されるときに、ネットワークに使用される割り当て済みリソースを削除します。
- **DaemonSet**-Kubernetes デプロイメントでは、一部またはすべてのノードが特定のポッドのコピーを実行することを DaemonSet が保証します。ノードが Kubernetes クラスターに追加されると、DaemonSet によって定義されたポッドのコピーが新しい各ノードに追加されます。CN-Series ファイアウォールを DaemonSet として展開すると、CN-NGFW ポッドのコピーがクラスタ内の各ノード(CN-MGMT ペアあたり最大 30 個)にデプロイされます。
- **Kubernetes** サービス- ネットワーク サービスとして、一連のポッドで実行されているアプリケーションを公開する抽象化です。CN-Series をサービスとしてデプロイする場合、デプロイされる CN-NGFW ポッドの数は、yaml ファイルをセットアップするときにユーザーが定義します。
- **Kuberenetes CNF** - CN-series-as-a-kubernetes-CNFをデプロイすると、クラウドプロバイダーのネイティブルーティング、vRouters、Top of Rack(TOR)スイッチなどの外部エンティティを

介してService Function Chaining(SFC)を使用するトラフィックに関連する課題が解決されます。CN-series-as-a-kubernetes-CNFのデプロイメントモードは、アプリケーションポッドに影響を与えません。

- 水平ポッド自動スケーラ**(HPA)**—CPU使用率やセッション使用率などのさまざまなメトリックに基づいて、デプロイメント、レプリカ セット、ステートフル セット内のポッド数を自動的にスケーリングします。

  HPA は、*CN-Series* で *Kubernetes* サービスとしてのみサポートされています。

- **HSF** - Palo Alto Networks CN-Series Hyperscale Security Fabric(HSF)1.0は、コンテナ化された次世代ファイアウォールのクラスタであり、5Gネットワークを展開するモバイル サービス プロバイダー向けに高度にスケーラブルで回復力のある次世代ファイアウォール ソリューションを配信します。

CN-Series の中核となる構成単位

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

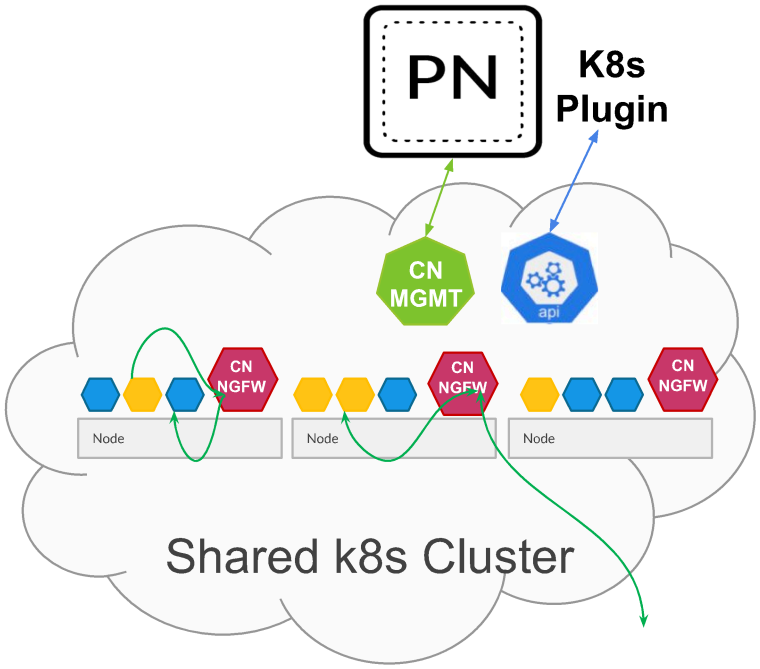
CN-Series ファイアウォールは、Kubernetes クラスタ上のコンテナ化されたアプリケーション ワークロードの可視化とセキュリティを提供する、コンテナ化された次世代ファイアウォールです。これを実現するために、Kubernetes (K8s) コンストラクトと Palo Alto Networks コンポーネントが使用されます。

CNシリーズ ファイアウォールをデプロイするための中核となる構成単位を以下に示します。

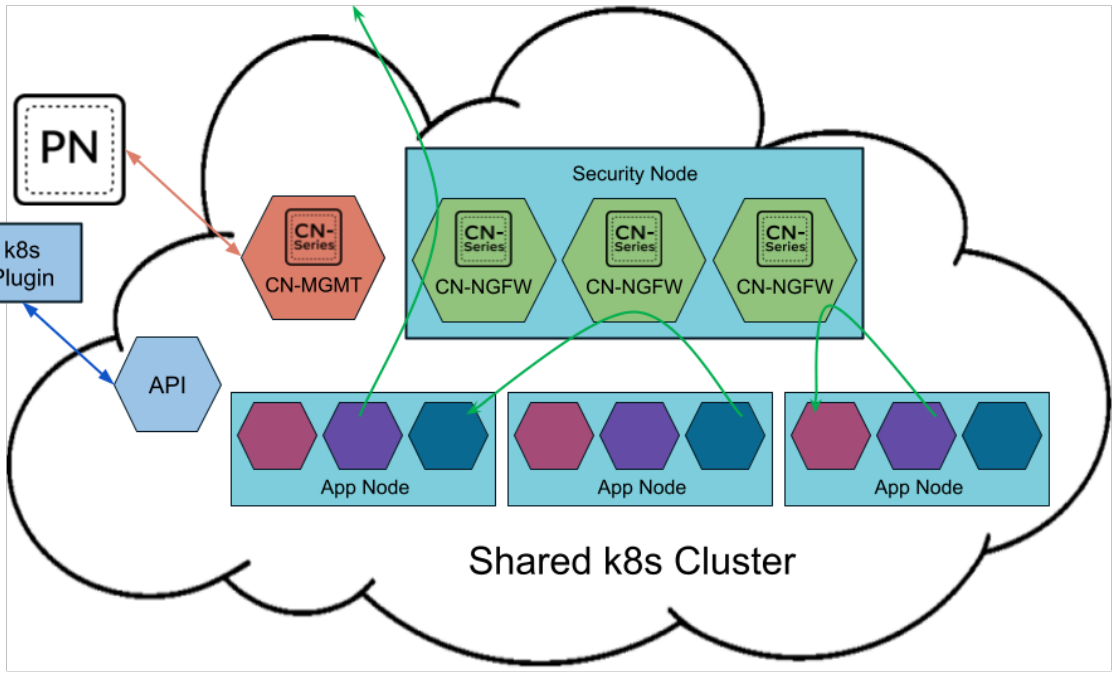
- **CN-Series** デプロイメントファイル — コンテナ化された環境に CN シリーズを展開するには、さまざまな CN シリーズ展開ファイルをダウンロードして展開する必要があります。
  - PAN-CN-MGMT — 初期コンテナは、CN-MGMT ポッドのインスタンス間、および CN-MGMT ポッドと CN-NGFW ポッド間の通信を保護するために使用される証明書を生成します。
  - PAN-CN-MGMT-CONFIGMAP
  - PAN-CN-MGMT-SECRET — Panorama がファイアウォールを認証して、各ファイアウォールを管理対象デバイスとして追加できるようにします。VM 認証キーは、デプロイメントの有効期限が切れるまで必要になります。接続リクエストに有効なキーがない場合、CN-Series ファイアウォールを Panorama に登録できません。
  - PAN-CN-NGFW
  - PAN-CN-NGFW-CONFIGMAP
  - PAN-CNI
  - PAN-CNI-CONFIGMAP
  - PAN-CNI-MULTUS
- **CN-MGMT** ポッドと **CN-NGFW** ポッドを使用した分散 **PAN-OS** アーキテクチャ - コンテナ化されたファイアウォールの管理プレーン (CN-MGMT) とデータ プレーン (CN-NGFW) は分離しており、アプリケーションのより良いランタイム保護を可能にし、より小さいフットプリントに対応します。CN-MGMT と CN-NGFW は、コンテナ イメージと、ConfigMap オブジェクトを含む YAML マニフェスト ファイルを使用してデプロイされます。
- **CN-MGMT** は、StatefulSet として動作し、永続ボリュームを備え、Kubernetes 環境で DNS を使用して検出可能な K8s サービスとして公開されます。CN-MGMT は耐障害性を備えてお

り、CN-MGMT ポッドの再起動や故障が発生した場合は 1 つの CN-MGMT ポッドで既存の CN-NGFW ポッドを管理することができます。

- **CN-NGFW** は、DaemonSet または Kubernetes サービスとしてデプロイできます。DaemonSet のデプロイメントは、より大きなノード、低レイテンシを必要とするポッド、および/または高いファイアウォール容量を必要とするポッドを備えたKubernetes環境に適しています。Kubernetes サービスとしての CN-Series は、ノードが小さい、またはより動的なファイアウォールを必要とする Kubernetes 環境 に適しています。
  - **DaemonSet** としてデプロイすると、CN-NGFW ポッドの各インスタンスは、同じノードで実行されている 30 のアプリケーションポッドを保護できます。このアーキテクチャを使用すれば、クラスタ内のワークロードを保護するノードごとに CN-NGFW DaemonSet ポッドを配置し、CN-MGMT ポッドのペアをクラスタ内の最大 30 個の CN-NGFW ポッドに接続し、管理させることができます。制限の詳細は、「CN-Series のパフォーマンスとスケーリング」を参照してください。



- **Kubernetes** サービスとしてデプロイすると、CN-NGFW のインスタンスをセキュリティ ノードにデプロイでき、アプリケーションポッドトラフィックは、検査と実施のために利用可能な CN-NGFW インスタンスにリダイレクトされます。



- ネットワーク挿入用の **PAN-CNI** プラグイン - PAN-CNI プラグインは、すべてのポッド上のネットワーク インターフェースの割り当てを担当し、CN-NGFW ポッドへのネットワーク接続を可能にします。CN シリーズの導入を可能にする YAML ファイルには、クラスタ内の各

ノードの CNI プラグイン チェーンに PAN-CNI プラグインを挿入する PAN-CNI DaemonSet が含まれています。このプラグインは、起動した各アプリケーション ポッドのアノテーションを読み取り、そのポッドを出入りするときに、セキュリティを有効にして、トラフィックを検査のために CN-NGFW ポッドにリダイレクトするかどうかを判断します。

- 集中管理用の **Panorama** - Panorama は、コンテナ化されたファイアウォールの設定とライセンスを管理するためのハブとして機能します。また、Kubernetes クラスタの監視と集中型セキュリティ ポリシー管理を可能にする Kubernetes プラグインをホストします。物理または仮想 Panorama アプライアンスを使用し、それをオンプレミスまたはパブリック クラウド環境でデプロイできます。Panorama が (CN-NGFW) ファイアウォールをライセンスし、Panorama テンプレートとデバイス グループを使用して設定とポリシーをプッシュできるようにするには、Panorama がファイアウォール管理プレーン ポッド (CN-MGMT) にネットワーク接続できる必要があります。Palo Alto Networks は HA 設定で Panorama をデプロイすることをお勧めします。

  Kubernetes クラスタ、アプリケーション、およびファイアウォール サービスをデプロイして管理するためには、kubectl や Helm などの標準の Kubernetes ツールが必要です。Panorama は、Kubernetes クラスタのデプロイメントと管理用のオーケストレーターになるようには設計されていません。クラスタ管理用のテンプレートがマネージド Kubernetes プロバイダから提供されています。Helm や Terraform を使用して CN-Series をデプロイするときに、コミュニティ サポート テンプレートを使用することもできます。

- **Kubernetes Plugin on Panorama** - この Kubernetes プラグインは、CN-Series ファイアウォールのライセンスを管理します。ライセンスは、CN-NGFW ポッドに割り当てることを選択したコアの数に基づいています。各 CN-NGFW ポッドが 1 つずつのライセンス トークンを使用し、トークンは、認証コードがアクティブにされ、Palo Alto Networks のライセンス サーバーから指定された数のトークンが取得されてから、Panorama 上でローカルに管理されます。各 CN-NGFW が Kubernetes ノード上で起動すると、Panorama がローカルにライセンス トークンを配布します。

  Panoram 上の Kubernetes plugin を使用すれば、クラスタを監視したり、Kubernetes ラベルを利用してポッド、サービス、デプロイメント、関連識別属性などの Kubernetes オブジェクトを整理したりすることもできるため、コンテキストを意識したセキュリティ ポリシー ルールを作成できます。Kubernetes プラグインは API サーバーと通信し、ほぼリアルタイムでメタデータを取得して、クラスター内で実行されているアプリケーションを可視化します。Kubernetes プラグインは、Kubernetes クラスタから名前空間、サービス、およびラベルを収集し、クラスタ内の関連オブジェクトに関する IP アドレス/タグ マッピング用のタグを作成します。このタグは、セキュリティ ポリシーで使用できます。詳細についてはKubernetes属性のIPアドレスからタグへのマッピングを参照してください。

  また、アプリケーション YAML で指定されたポートに関する情報を収集し、サービス オブジェクトを作成します。

  これらのタグとサービス オブジェクトは自動的に各クラスタ内の CN-NGFW ポッドと共有されますが、ハードウェアベースまたは VM-Series ファイアウォールを使用してタグとサービス オブジェクトを共有することもできます。タグは、ダイナミック アドレス グループ内の一

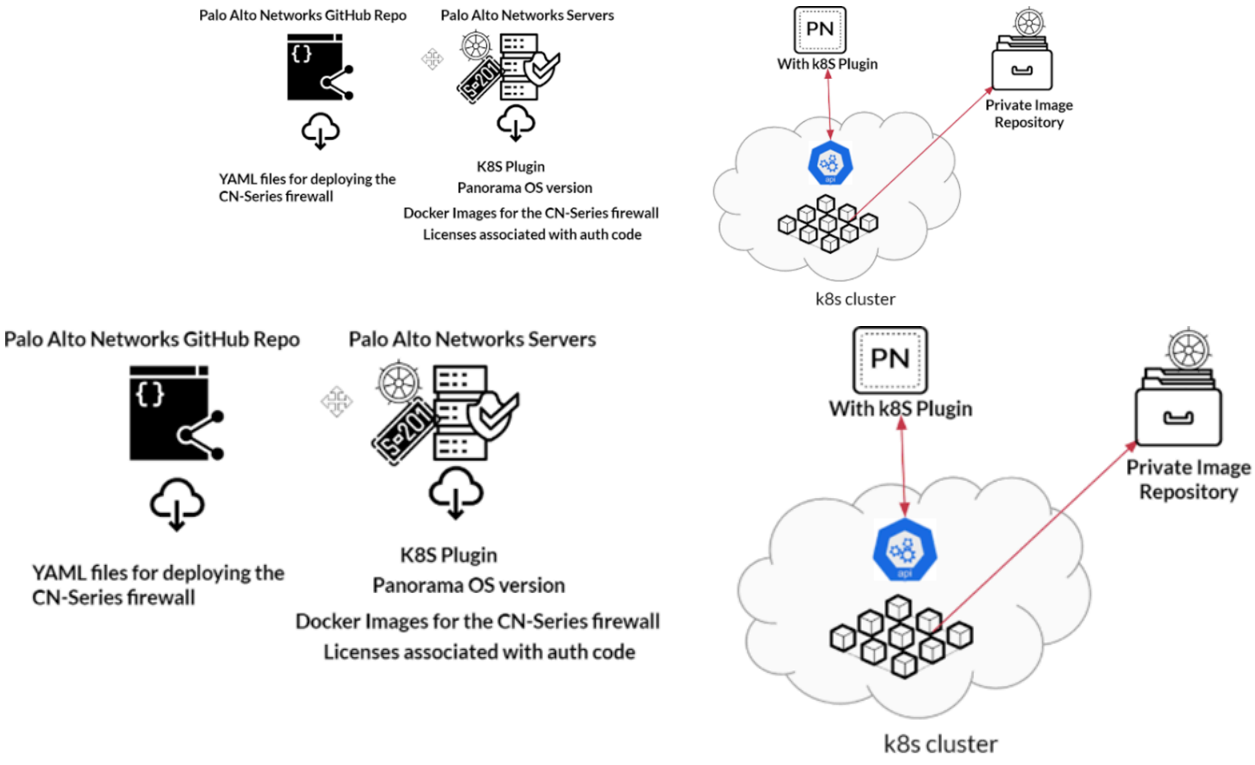
致条件として使用できます。そうすれば、ポッド間や名前空間間のトラフィック、インターネット公開サービスへのトラフィック、またはアウトバウンド接続を保護するために使用できます。

Palo Alto Networks では、障害が発生した場合でも Panorama ピアが IP アドレスの更新を継続的に受信できるように、Panorama を HA 構成で展開することをお勧めします。Panorama の 1 つのインスタンスをデプロイした場合、障害が発生しても、既存のアプリケーション ポッドからのトラフィックは影響を受けず、現行のポリシーが CN-NGFW ポッドに適用されます。新しいポッドが起動すると、ソースが "ANY" になっているすべてのルールがこの新しいポッドに適用され、この新しいポッドからのトラフィックがポリシー ルールに基づいて許可またはブロックされます。たとえば、任意のソースから外部へのアウトバウンド アクセスをブロックするためのアンチスパイウェア ポリシー ルールがある場合は、このルールが新しいポッドに適用され、プロファイルでトラフィックを保護することができます。デフォルトの拒否ルールがある場合は、この新しいポッドからのトラフィックが拒否されます。

*Kubernetes*プラグインを使用して、*Kubernetes*クラスタ内にデプロイされたポッド、ノード、ネームスペース、およびサービスの*IP*アドレスからタグへのマッピングを、そのクラスタに*CN*シリーズファイアウォールをデプロイしていなくても、物理ファイアウォールまたは*VM*シリーズファイアウォールに配布できます。

CN-Series ファイアウォールを使用して Kubernetes クラスタをセキュリティで保護するために必要なコンポーネント

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用



CNシリーズ ファイアウォールをデプロイし、Kubernetesクラスタ内にデプロイされたアプリケーションを保護するために必要なものは、以下のとおりです。

- **Panorama** — アプリケーションと CN-Series ファイアウォールがデプロイされている Kubernetes クラスタに接続できるハードウェア ベースのアプライアンスまたはバーチャル アプライアンスです。Panorama は、CN-Series ファイアウォールのライセンス管理と設定の管理のために必要です。詳細については、CN-Series の中核となる構成単位を参照してください。

- **Kubernetes Plugin on Panorama** — コンテナ化されたアプリケーションは変化が早いので、クラスタ内のコンテナ アクティビティを可視化するためと、クラスタ内の各ノードにデプロイされたファイアウォールのライセンス トークン割り当てを管理するために、このプラグインが必要になります。

  Kubernetes プラグインは、サービス アカウント資格情報を使用して Kubernetes クラスタに接続します。そこから、リソース属性とラベルを取得し、タグとサービス オブジェクトを作成します。タグは、Dynamic Address Group (ダイナミック アドレス グループ) を作成し、IP トラフィックの適用のためにそれらをセキュリティ ポリシー内で参照するために使用できます。また、セキュリティ ポリシー内でサービス オブジェクトを使用して、IP アドレスだけでなくポートに基づいてトラフィックを許可または拒否することもできます。タグとサービス オブジェクトを使用すると、Kubernetes クラスタ内でトラフィックの適用が可視化され、それを細かく制御することができます。

- **Docker** イメージ — 分散アーキテクチャをサポートするため、CN-Series ファイアウォールでは、Palo Alto Networks ポータル上で 4 つの Docker イメージを利用可能です。これらのイメージは 3 つの圧縮された tar アーカイブ (tar.gz 形式) として発行されており、これらのイメージを解凍し、イメージ レジストリに対して Docker プッシュを行う必要があります。

  注:イメージと YAML ファイルのバージョンに互換性があることを確認してください。圧縮ファイルは次のとおりです。

  - **PanOS_cn-10.1.0.tgz** — このアーカイブには、ファイアウォール管理プレーン (CN-MGMT) およびファイアウォール データプレーン (CN-NGFW) イメージが含まれています。

    解凍されるイメージ名は、たとえば、`panos_cn_ngfw:10.1.0-b7` および `panos_cn_mgmt:10.1.0-b7` になります

    - **Pan_cn_mgmt_init-2.0.0.tgz** — このアーカイブには、ファイアウォールに管理プレーンをデプロイするために必要なユーティリティが入った初期化コンテナ (CN-INIT) が含まれています。初期化コンテナを使用すると、CN-MGMT および CN-NFGW ポッド間で、セキュリティで保護された IPSec 通信が有効になります。解凍されるイメージ名は、たとえば、`pan_cn_mgmt_init:1.0.0-b1-c1` になります。
    - **Pan_cni-2.0.0.tgz** — このアーカイブには、CN-MGMT と CN-NFGW の間の接続を有効にし、トラフィックを各ノード上の CN-NGFW ポッドにリダイレクトするようにアプリケーション ポッド上のネットワーク インターフェースを再設定する CNI プラグインが含まれています。解凍されるイメージ名は、たとえば、`pan_cni:2.0.0` になります。

上記のイメージ名は一例であり、最新リリースを反映して変更されます。Palo Alto Networks ポータルで最新のイメージを見つけることができます。

- **YAML** ファイル — リソースを Kubernetes クラスタにデプロイするために必要なフィールドとオブジェクト仕様が含まれた YAML ファイルで、GitHub で公開されています。

  ネイティブ Kubernetes または GKE などのサポートされている環境に必要なすべての YAML ファイルが、使いやすいように 1 つのフォルダにまとめて圧縮されています。

  YAML ファイルは *HELM* チャートを介して自動的にデプロイされます。これは、*CN-Series* ファイアウォールのデプロイに推奨される方法です。

  - CN-MGMTには、`pan-cn-mgmt.yaml`、`pan-cn-mgmt-configmap.yaml`、`pan-cn-mgmt-secret.yaml`、`pan-cn-mgmt-slot-cr.yaml`、`pan-cn-mgmt-slot-crd.yaml`の3つのYAMLファイルがあります。
  - DaemonSet としての CN-NGFW には、次の 2 つの YAML ファイルがあります — `pan-cn-ngfw.yaml`、`pan-cn-ngfw-configmap.yaml`。Kubernetes サービスとして のCN-NGFW には、前述のファイルに加えて、`pan-cn-ngfw-svc.yaml` があります。
  - CNI プラグインには、次の 3 つの YAML ファイルがあります — `pan-cni-configmap.yaml`、`pan-cni.yaml` または `pan-cni-multus.yaml`。

    メタ プラグインとして機能し、他の CNI プラグインを呼び出す Multus CNI のある環境に CN-Series をデプロイしている場合は、`pan-cni.yaml` または `pan-cni-multus.yaml` のいずれかを選ぶ必要があります。

    CN-Series を OpenShift 上にデプロイしている場合は、デフォルトで Multus が有効にされるため、pan-cni.yaml が適切です。一方、Multus CNI がサポートされていてもそれが省略可能な環境 (自己管理型の (ネイティブ) 環境など) に CN-Series をデプロイしている場合は、pan-cni.yaml の代わりに pan-cni-multus.yaml を使用してください。

    - 下のサービス アカウント作成セクションで参照されている *`pan-cni-serviceaccount.yaml`* もあります。
    - *OpenShift* デプロイメントの場合は、追加の *`pan-cni-net-attach-def.yaml`* があります。
  - サービス アカウント作成 — 3 つの YAML ファイルがあります。`pan-mgmt-serviceaccount.yaml`、`pan-cni-serviceaccount.yaml`、`plugin-serviceaccount.yaml`。

    `pan-mgmt-serviceaccount.yaml` と `pan-cni-serviceaccount.yaml` は、CN-MGMT および CN-NGFW ポッドがクラスタに対して認証するためものです。

    `plugin-serviceaccount.yaml` は、Kubernetes plugin on Panorama がクラスタに対して認証するためのものです。
  - ネイティブ **Kubernetes** デプロイメント用の永続ボリューム **YAML** — `pan-cn-pv-manual.yaml` および `pan-cn-pv-local.yaml`。

    `pan-cn-pv-manual.yaml` は、単一ノード クラスタを使用した PoC 用にのみ提供されています。Palo Alto Networks では、`pan-cn-mgmt.yaml` 内で参照されている CN-MGMT

ポッド用の設定とログを格納するために、動的にプロビジョニングされた永続ボリュームを使用することを強くお勧めします。両方の CN-MGMT ポッドについて、クラスタ内に永続ボリュームをセットアップしたことを確認してください。

- ライセンス認証コード — 認証コードを使用すると、クラスタ内の各ノードにデプロイされた CN-NGFW ポッドの各インスタンスにライセンスを付与できます。

  ライセンス認証コードは、Palo Alto Network CSP で作成した CN-Series デプロイメントプロファイルに関連付けられています。さらに、デプロイメントプロファイルの作成時に選択したセキュリティサブスクリプションが有効になります。

CN-Series に関するその他のリソース

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

以下のリソースを使用して、CN-Series ファイアウォールの詳細と、コンテナ化されたネットワークの保護にどのように役立つかを確認できます。

- CN-Series ファイアウォール — CN-Series ファイアウォールについては、これらのビデオをご覧ください。
- CN Series の利点、概要、および使用法—Palo Alto Networks ライブコミュニティに関する3部構成のブログシリーズ（ビデオが埋め込まれています）。CNシリーズファイアウォールの利点、概要、および使用法について説明しています。
- Palo Alto Network Qwiklabs-Palo Alto Networks Qwiklab を使用してラボの演習を行い、AWS または GCPで CN-Series ファイアウォールを試すことができます。
- Kubernetes 用 Panorama プラグインのリリースノート-このリリースノートを読むと、Kubernetes 用 Panorama プラグインの最新バージョンで導入された機能と拡張機能について学習できます。
- PAN-OS リリースノート-PAN-OSリリースノートを表示して、最新バージョンの PAN-OS で導入されたCN-Series の機能と拡張機能の詳細を確認できます。
- Panorama 管理者ガイド—Panorama は、Kubernetes 環境への接続、デプロイされた CN-Series ファイアウォールの管理、セキュリティ ポリシーの定義に使用されるインターフェースです。

CN-Series のシステム要件

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

このセクションでは、Kubernetesクラスターおよびオンプレミス環境にCNシリーズ ファイアウォールを導入するための推奨システム要件について説明します。

このセクションでは、以下のトピックについて説明します。

- Kubernetesクラスタを想定したCNシリーズ システム要件
- オンプレミスKubernetesデプロイメントを想定したCNシリーズ ファイアウォールのシステム要件
- CN-Series のパフォーマンスとスケーリング
- CN-Series のデプロイメント — サポートされる環境

Kubernetesクラスタを想定したCNシリーズ システム要件

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

サポートされている複数のモードにわたって CN-Series ファイアウォールをデプロイするための推奨システム要件は次のとおりです。

- PAN-OS 10.1
- PAN-OS 10.2以降

PAN-OS 10.1

以下の表に、CN-Series がデプロイされるクラスターのシステム要件を示します。これらの値は、CPU、メモリ、およびディスクストレージの一般的なガイドラインです。デプロイするリソースの量は、ニーズに応じて異なる場合があります。

CN-Series ミディアムは、*Daemonset* として *CN-Series* では使用できません。

リソース	CN-MGMT-スモール	CN-NGFW-スモール	CN-MGMT-ミディアム	CN-NGFW-ミディアム	CN-MGMT-ラージ	CN-NGFW-ラージ
メモリ (最小)	3GB	• 2GB (Daemonset) • 2.5GB (K8s サービス)	3GB	6GB	4GB	48GB
CPU (最小)	2 (推奨)	2 (推奨)	2 (推奨)	4 (推奨)	4 (推奨)	12 (推奨)

リソース	CN-MGMT-スモール	CN-NGFW-スモール	CN-MGMT-ミディアム	CN-NGFW-ミディアム	CN-MGMT-ラージ	CN-NGFW-ラージ
CPU (最大)	該当なし	31	該当なし	31	該当なし	31
ディスク	50GB	該当なし	50GB	該当なし	50GB	該当なし

PAN-OS 10.2以降

5G-ネイティブセキュリティは、Daemonset および Kubernetes CNF モードでのみサポートされます。

CN-MGMT と *CN-NGFW* のメモリとコアの組み合わせは、それぞれ*small*、*Medium*、*Large*に適用されます。*CN-MGMT* マップに関連する*Small*、*Medium*、*Large*の組み合わせは、それぞれの *CN-NGFW* に直接マップされます。

表 **1 :** 推奨される **CN-Series** システムと能力のマトリックス

CN モード	リソース	小	中	中	中	大	大
DaemonSet	最小 CN-MGMT メモリ	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW メモリ	2G	6.5G	16G	32G	48G	56G
	推奨されるCN-MGMTコア	2	2	2	4	8	12
	最大CN-NGFW コア	2	4	8	16	31	47
	ディスク	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi

CN モード	リソース	小	中	中	中	大	大
	DPDK Hugepageサイズ	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし
Kubernetesサービス	最小 CN-MGMT メモリ	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW メモリ	4G	6.5G	16G	32G	48G	56G
	推奨されるCN-MGMTコア	2	2	2	4	8	12
	最大CN-NGFW コア	2	4	8	16	31	47
	ディスク	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK Hugepageサイズ	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし
Kubernetes CNF	最小 CN-MGMT メモリ	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW メモリ	2G	6.5G	16G	32G	48G	56G
	推奨されるCN-MGMTコア	2	2	2	4	8	12

CN モード	リソース	小	中	中	中	大	大
	最大CN-NGFW コア	2	4	8	16	31	47
	ディスク	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK Hugepageサイズ	1G	1G	2G	2G	4G	4G

オンプレミスKubernetesデプロイメントを想定したCNシリーズ ファイアウォールのシステム要件

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

オンプレミス デプロイメントに関する以下の前提条件を確認してください。

- コンテナ イメージが Kubernetes クラスタ内のすべてのノードからアクセスできることを確認します。
- 両方の CN-MGMT ポッド用のクラスタ内に永続ボリュームをセットアップします。CN-MGMT ポッドは CN-NGFW ポッドをアクティブに管理する StatefulSet としてデプロイされるため、両方のインスタンスが永続ボリュームにアクセスできる必要があります。

Rancher クラスタの *SSH* アクセスを取得するには、*kubeconfig* ファイルの内容が `/.kube/config` の場所にコピーされていることを確認する必要があります。これにより、クラスターに対して *kubectl* コマンドを実行できるようになります。

また、*Kubernetes* コマンドライン ツール *kubectl* がシステムにインストールされていることを確認します。詳細については、ツールのインストールを参照してください。

Rancher サポート付き *CN-Series* の場合は、マスターノード *Ubuntu 18.0.4 LTS VM* に *Docker* をインストールし、*8 vCPU* と *32G* メモリ*(*最小 *200G* ディスク*)* を搭載します。詳細については、Ubuntu 18.04 に Docker をインストールするを参照してください。

Ubuntu 18.0.4 の場合、マシン上のカーネルは、以下のコマンドを使用して最新のカーネルに更新する必要があります。

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

CN-Series のパフォーマンスとスケーリング

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

各種コンポーネントでCNシリーズ ファイアウォールを使用してKubernetes ワークロードを保護するのために必要なスケール数を以下のセクションに示します。

- CN-Series コンポーネントでサポートされるスケール
- Kubernetes Plugin on Panorama でサポートされるスケール
- CN-Series の主要パフォーマンス メトリック

CN-Series コンポーネントでサポートされるスケール

CN-Series のCPU、メモリ、およびディスクストレージの定義についての情報は、Kubernetesクラスタを想定したCNシリーズ システム要件を参照してください。

次の表は、CN-Series のサイズ (小、中、大) ごとにデータを分けています。これらの CN-Seriesのサイズには、次のメモリ値があります。

- **CN-Series Small** — 最小 2.5G CN-NGFW および 3G CN-MGMT
- **CN-Series Medium** — 最小6Gの CN-NGFWおよび3G CN-MGMT
- **CN-Series Large** — 最小 42G の CN-NGFW および 4G CN-MGMT

属性	**CN-Series** スケール **(DaemonSet)**	**CN-Series** スケール **(K8s** サービス**)**	**CN-Series** スケール **(K8s-CNF)**
K8s クラスタあたりの最大 CN-MGMT ペア数	アクティブ/パッシブ HA モードの 4 つの CN-MGMT ペア	アクティブ/パッシブ HA モードの 4 つの CN-MGMT ペア	アクティブ/パッシブ HA モードの 4 つの CN-MGMT ペア
CN-MGMT ペアあたりの最大 CN-NGFW ポッド数	30	30	30

属性	CN-Series スケール (DaemonSet)	CN-Series スケール (K8s サービス)	CN-Series スケール (K8s-CNF)
CN-NGFW によって保護される Kubernetes ポッド数 (K8s ノードあたり)	30 (PAN-OS 10.1.8 以前のバージョン) 125 (k8s 2.0.2 がインストールされた PAN-OS 10.1.9 以降のバージョン)	該当なし このデプロイメントモードは、*K8s* ノード上のアプリケーションポッドの数には依存しません。	該当なし このデプロイメントモードは、*K8s* ノード上のアプリケーションポッドの数には依存しません。
CN-NGFW あたりの最大 TCP/IP セッション数	CN-Series スモール：20,000 CN-Series ミディアム：819,200 CN-Series ラージ：10,000,000	CN-Series スモール：250,000 CN-Series ミディアム：819,200 CN-Series ラージ：10,000,000	CN-Series スモール：250,000 CN-Series ミディアム：819,200 CN-Series ラージ：10,000,000
CN-MGMT ペアあたりの最大ダイナミック アドレス グループ IP アドレス数*	CN-Series スモール：2500（PAN-OS 10.0.6 以下） 10,000 (PAN-OS 10.0.7 以上)	CN-Series スモール：2500（PAN-OS 10.0.6 以下） 10,000 (PAN-OS 10.0.7 以上) CN-Series ミディアム：200,000 CN-Series ラージ：300,000	CN-Series スモール：2500（PAN-OS 10.0.6 以下） 10,000 (PAN-OS 10.0.7 以上) CN-Series ミディアム：200,000 CN-Series ラージ：300,000
IP アドレス*および CN-MGMT ペアあたりのタグ数	32	32	32

属性	**CN-Series** スケール **(DaemonSet)**	**CN-Series** スケール **(K8s** サービス**)**	**CN-Series** スケール **(K8s-CNF)**
最大セキュリティ ゾーン	CN-Series スモール：2 CN-Series ミディアム：40 CN-Series ラージ：200	CN-Series スモール：2 CN-Series ミディアム：40 CN-Series ラージ：200	CN-Series スモール：2 CN-Series ミディアム：40 CN-Series ラージ：200
セキュリティ プロファイル	CN-Series スモール：38 CN-Series ミディアム：375 CN-Series ラージ：750	CN-Series スモール：375 CN-Series ミディアム：375 CN-Series ラージ：750	CN-Series スモール：375 CN-Series ミディアム：375 CN-Series ラージ：750
最大インターフェイス	**PAN-OS 10.1.8** 以前のバージョンの場合**:** CN-Series スモール：30 CN-Series ミディアム：30 CN-Series ラージ：30 **k8s 2.0.2** がインストールされた **PAN-OS 10.1.9** 以降のバージョンの場合**:** CN-Series スモール：250 CN-Series ミディアム：250 CN-Series ラージ：250	CN-Series スモール：2 CN-Series ミディアム：2 CN-Series ラージ：2	CN-Series スモール：60 CN-Series ミディアム：60 CN-Series ラージ：60

*「ファイアウォール比較ツール」を参照してください。

ポリシー	**CN-Series** スモール **(**最小 **2.5G CN-NGFW** および最小 **3G CN-MGMT)**	**CN-Series** ミディアム **(**最小 **6G CN-NGFW** および最小 **2G CN-MGMT)**	**CN-Series** ラージ **(**最小 **42G CN-NGFW** および最小 **4G CN-MGMT)**
セキュリティルール数	1500	10,000	20,000
セキュリティルールスケジュール	256	256	256
NATルール *NAT* ルールは *CNF* モードでサポートされています。	該当なし	該当なし	該当なし
復号ルール	1000	1000	2000
アプリケーションオーバーライドルール	1000	1000	2000
トンネルコンテンツ検査ルール	100	500	2000
SD-WAN ルール	該当なし	該当なし	該当なし
ポリシー ベース フォワーディング ルール	該当なし	該当なし	該当なし

ポリシー	**CN-Series** スモール **(**最小 **2.5G CN-NGFW** および最小 **3G CN-MGMT)**	**CN-Series** ミディアム **(**最小 **6G CN-NGFW** および最小 **2G CN-MGMT)**	**CN-Series** ラージ **(**最小 **42G CN-NGFW** および最小 **4G CN-MGMT)**
ポリシーベースの転送ルールは、*CNF* モードでサポートされています。			
キャプティブポータルルール	該当なし	該当なし	該当なし
DoS プロテクションルール	• 100 (DaemonSet) • 1000 (K8s サービス)	1000	1000

オブジェクト (アドレスとサービス)	**CN-Series** スモール **(**最小 **2.5G CN-NGFW** および最小 **3G CN-MGMT)**	**CN-Series** ミディアム **(**最小 **6G CN-NGFW** および最小 **2G CN-MGMT)**	**CN-Series** ラージ **(**最小 **42G CN-NGFW** および最小 **4G CN-MGMT)**
アドレス オブジェクト	10,000	10,000	40,000
アドレス グループ	1000	1000	4000
アドレス グループごとのメンバー	2500	2500	2500
サービスオブジェクト	2000	2000	5000

オブジェクト (アドレスとサービス)	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
サービス グループ	500	500	500
サービス グループごとのメンバー	500	500	500
FQDN アドレス オブジェクト	2000	2000	2000
ダイナミック アドレス グループ IP アドレスの最大数	2500	200,000	300,000
IP アドレスあたりのタグ数	32	32	32

App-ID	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
カスタム App-ID シグネチャ	6000	6000	6000
共有カスタム App-ID	512	512	512
カスタム App-ID (仮想システム固有)	6416	6416	6416

SSL復号化	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
SSL インバウンド証明書の最大数	1000	1000	1000

SSL復号化	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
SSL 証明書キャッシュ (転送プロキシ)	128	2000	8000
同時復号化セッションの最大数	• 1024 (DaemonSet) • 6400 (K8s サービス)	15,000	100,000
SSL ポートミラー	いいえ	いいえ	いいえ
SSL 復号化ブローカー	いいえ	いいえ	いいえ
サポートされる HSM	いいえ	いいえ	いいえ

URL フィルタリング	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
許可リスト、ブロックリスト、およびカスタムカテゴリの合計エントリ数	25,000	25,000	100,000
カスタムカテゴリの最大数	• 500 (DaemonSet) • 2849 (K8s サービス)	2849	2849
URL フィルタリング用のデータプレーンキャッシュサイズ	• 5000 (DaemonSet) • 90,000 (K8s サービス)	90,000	250,000
管理プレーンの動的キャッシュサイズ	100,000	100,000	600,000

EDL	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
カスタムリストの最大数	30	30	30
システムあたりの IP の最大数	50,000	50,000	50,000
システムあたりの DNS ドメインの最大数	50,000	500,000	2,000,000
システムあたりの URL の最大数	50,000	100,000	100,000
最短チェック間隔 (分)	5	5	5

アドレス割り当て	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
DHCP サーバー	3	10	125
DHCP リレー	いいえ	いいえ	いいえ
割り当てられるアドレスの最大数	64,000	64,000	64,000

インターフェイス	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
最大インターフェース数 (論理および物理)	• 60 (DaemonSet) • 2 (K8s サービス) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (K8s サービス) • 2 (K8s-CNF)	• 60 (DaemonSet) • 2 (K8s サービス) • 2 (K8s-CNF)

インターフェイス	**CN-Series** スモール **(**最小 **2.5G CN-NGFW** および最小 **3G CN-MGMT)**	**CN-Series** ミディアム **(**最小 **6G CN-NGFW** および最小 **2G CN-MGMT)**	**CN-Series** ラージ **(**最小 **42G CN-NGFW** および最小 **4G CN-MGMT)**
管理-範囲外	該当なし	該当なし	該当なし
管理-10/100/1000 高可用性	該当なし	該当なし	該当なし
管理-40G 高可用性	該当なし	該当なし	該当なし
管理-10G 高可用性	該当なし	該当なし	該当なし
トラフィック-10/100/1000	該当なし	該当なし	該当なし
トラフィック-100/1000/10000	該当なし	該当なし	該当なし
トラフィック-1G SFP	該当なし	該当なし	該当なし
トラフィック-10G SFP+	該当なし	該当なし	該当なし
トラフィック-40/100G QSFP+/QSFP28	該当なし	該当なし	該当なし
デバイスごとの 802.1q タグ	該当なし	該当なし	該当なし
物理インターフェースあたりの 802.1q タグ	該当なし	該当なし	該当なし
集約インターフェースの最大数	該当なし	該当なし	該当なし
SD-WAN 仮想インターフェースの最大数	該当なし	該当なし	該当なし

NAT	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
NAT ルールキャパシティの合計	該当なし	該当なし	該当なし
最大 NAT ルール（スタティック）	該当なし	該当なし	該当なし
最大 NAT ルール (DIP)	該当なし	該当なし	該当なし
最大 NAT ルール (DIPP)	該当なし	該当なし	該当なし
最大変換済み IP 数（DIP）	該当なし	該当なし	該当なし
最大変換済み IP 数 (DIPP)	該当なし	該当なし	該当なし
デフォルトの DIPP プールオーバーサブスクリプション	該当なし	該当なし	該当なし

User-ID	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
IP ユーザー マッピング（管理プレーン）	該当なし	該当なし	該当なし
IP ユーザー マッピング (データプレーン)	該当なし	該当なし	該当なし
ポリシーで使用されるアクティブで一意のグループ	該当なし	該当なし	該当なし

User-ID	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
User-ID エージェントの数	該当なし	該当なし	該当なし
User-ID の監視対象サーバー	該当なし	該当なし	該当なし
ターミナルサーバーエージェント	該当なし	該当なし	該当なし
ユーザーごとのタグ	該当なし	該当なし	該当なし

routing	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
IPv4 転送テーブル サイズ	該当なし	該当なし	該当なし
IPv6転送テーブル サイズ	該当なし	該当なし	該当なし
システムの転送テーブル サイズの合計	該当なし	該当なし	該当なし
ルーティングピアの最大数（プロトコル依存）	該当なし	該当なし	該当なし
スタティック エントリ - DNS プロキシ	該当なし	該当なし	該当なし
双方向転送検出（BFD）セッション	該当なし	該当なし	該当なし

L2 転送	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
デバイスごとの ARP テーブルサイズ	該当なし	該当なし	該当なし
IPv6 隣接テーブル サイズ	該当なし	該当なし	該当なし
デバイスごとの MAC テーブルサイズ	該当なし	該当なし	該当なし
ブロードキャストドメインあたりの最大 ARP エントリ数	該当なし	該当なし	該当なし
ブロードキャストドメインあたりの最大 MAC エントリ数	該当なし	該当なし	該当なし

QoS	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
QoS ポリシーの数	該当なし	該当なし	該当なし
QoS をサポートする物理インターフェース	該当なし	該当なし	該当なし
物理インターフェースあたりのクリアテキストノード	該当なし	該当なし	該当なし
ポリシーによる DSCP マーキング	該当なし	該当なし	該当なし

QoS	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
サポートされるサブインターフェース	該当なし	該当なし	該当なし

IPsec VPN	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
IKE ピアの最大数	該当なし	該当なし	該当なし
サイト間 (プロキシ ID 付き)	該当なし	該当なし	該当なし
SD-WAN IPsec トンネル	該当なし	該当なし	該当なし

グローバルプロテクト	CN-Series スモール (最小 2.5G CN-NGFW および最小 3G CN-MGMT)	CN-Series ミディアム (最小 6G CN-NGFW および最小 2G CN-MGMT)	CN-Series ラージ (最小 42G CN-NGFW および最小 4G CN-MGMT)
GlobalProtect クライアント **VPN** 最大トンネル（SSL、IPsec、IKE と XAUTH）	該当なし	該当なし	該当なし
GlobalProtect クライアントレス **VPN** SSL トンネルの最大数	該当なし	該当なし	該当なし

マルチキャスト	**CN-Series** スモール **(**最小 **2.5G CN-NGFW** および最小 **3G CN-MGMT)**	**CN-Series** ミディアム **(**最小 **6G CN-NGFW** および最小 **2G CN-MGMT)**	**CN-Series** ラージ **(**最小 **42G CN-NGFW** および最小 **4G CN-MGMT)**
レプリケーション (出口インターフェース)	該当なし	該当なし	該当なし
ルート	該当なし	該当なし	該当なし

Kubernetes Plugin on Panorama でサポートされるスケール

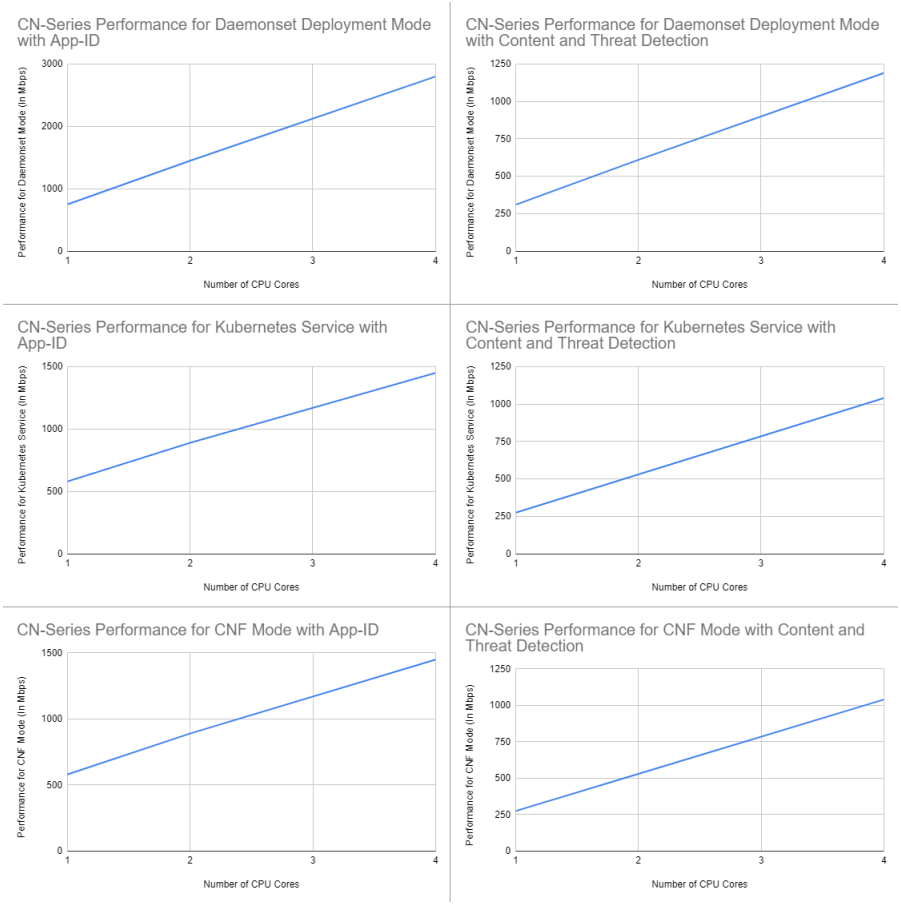
属性	**Kubernetes** プラグイン スケール
K8s Panorama プラグイン上の最大クラスタ数	32(ネイティブK8s、AKS、EKS、GKEなどのサポートされているすべての環境全体で)

CN-Series の主要パフォーマンス メトリック

AWS EKS での **CN-Series**				
	CPU コア	**DaemonSet** としての **CN-Series (MMAP)**	**Kubernetes** サービスとしての **CN-Series (MMAP)**	**Kubernetes CNF**としての **CN-Series (MMAP)**
App-ID	{{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}>{{防御>防御<防御}>{防御>防御<防	750 Mbps	580 Mbps	580 Mbps

AWS EKS での CN-Series				
	CPU コア	DaemonSet としての CN-Series (MMAP)	Kubernetes サービスとしての CN-Series (MMAP)	Kubernetes CNFとしての CN-Series (MMAP)
	御}<{防 御>防 御<防 御}}<{{防 御>防 御<防 御}>{防 御>防 御<防 御}<{防 御>防 御<防 御}}}			
コンテンツと脅威の検出	{{{防 御>防 御<防 御}>{防 御>防 御<防 御}<{防 御>防 御<防 御}}>{{防 御>防 御<防 御}>{防 御>防 御<防 御}<{防 御>防 御<防 御}}<{{防 御>防 御<防 御}>{防 御>防	310 Mbps	275 Mbps	275 Mbps

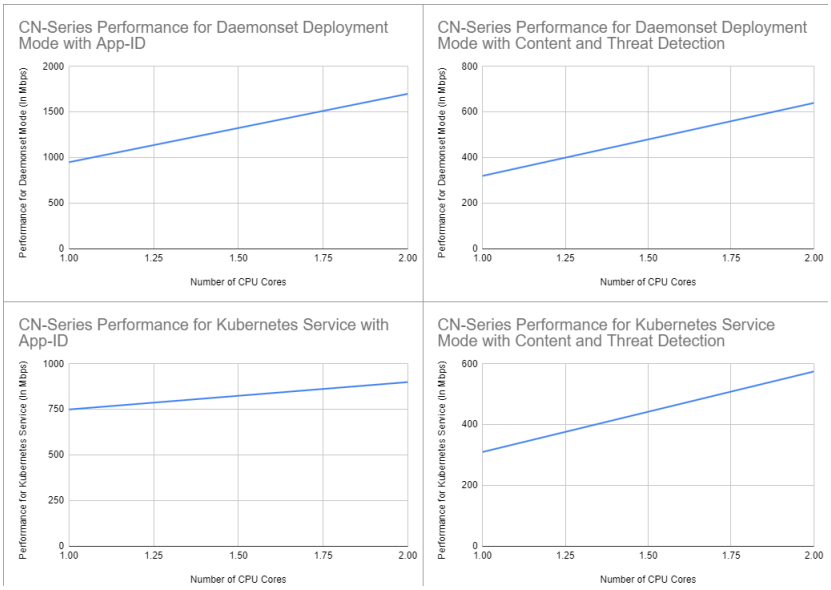
AWS EKS での CN-Series				
	CPU コア	DaemonSet としての CN-Series (MMAP)	Kubernetes サービスとしての CN-Series (MMAP)	Kubernetes CNFとしての CN-Series (MMAP)
	御<防御}<{防御>防御<防御}}}			
App-ID	2	1.45 Gbps	890 Mbps	890 Mbps
コンテンツと脅威の検出	2	610 Mbps	530 Mbps	530 Mbps
App-ID	4	2.8 Gbps	1.45 Gbps	1.45 Gbps
コンテンツと脅威の検出	4	1.19 Gbps	1.04 Gbps	1.04 Gbps



Google Cloud GKE の CN-Series (XDP 有効)			
	CPU コア	**DaemonSet としての CN-Series**	**Kubernetes サービスとしての CN-Series**
App-ID	{{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}>{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}<{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}}	950 Mbps	750 Mbps
コンテンツと脅威の検出	{{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御	320 Mbps	310 Mbps

Google Cloud GKE の CN-Series (XDP 有効)			
	CPU コア	**DaemonSet としての CN-Series**	**Kubernetes サービスとしての CN-Series**
	御}}>{{防 御>防 御<防 御}>{防 御>防 御<防 御}<{防 御>防 御<防 御}}<{{防 御>防 御<防 御}>{防 御>防 御<防 御}<{防 御>防 御<防 御}}}		
App-ID	2	1.7 Gbps	900 Mbps
コンテンツと脅威の検出	2	640 Mbps	575 Mbps

以下の表の情報のテストは、*Google Kubernetes Engine*（*GKE*）上で、同じクラスタ内の同じノード上のノード間およびポッド間のトラフィックで実行されました。



機能/属性	**CN-Series** スモール	**CN-Series** ミディアム	**CN-Series** ラージ
CN-NGFW の vCPU あたりのファイアウォールスループット（App-ID対応）	500 Mbps	500 Mbps	500 Mbps
CN-NGFW の vCPU あたりの脅威防御スループット	250 Mbps	250 Mbps	250 Mbps
最大セッション数	• 20,000 (DaemonSet) • 250,000 (K8s サービス) • 250,000 (k8s-CNF)	819,200	10,000,000
CN-NGFW の vCPU ごとの IPsec VPN スループット	該当なし	該当なし	該当なし
Connections per Second（接続数/秒）	該当なし	該当なし	該当なし

CN-Series のデプロイメント — サポートされる環境

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmチャートを使用したCNシリーズのデプロイメント用

この章では、CN シリーズ ファイアウォールの互換性とバージョン要件について説明します。

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

PAN-OS 10.1

CN-Series ファイアウォールは次の環境でデプロイできます。

製品	バージョン
コンテナ ランタイム	Docker CRI-O Containerd
Kubernetes のバージョン	1.17～1.27
クラウド プロバイダが管理する Kubernetes	• AWS EKS(DaemonSetとしてのCNシリーズおよびデプロイメントのサービス モードとしてのCNシリーズの場合は 1.17～1.27) • AWS Outpost（1.17～1.25）のEKS *AWS Outpost の EKS 用 CN-Series は SR-IOV または Multus* をサポートしていません。

製品	バージョン
	• Azure AKS（1.17～1.27） *Azure AKS*では、*Kubernetes 1.25*以降をサポートするために最低限必要なバージョンは*PAN-OS 10.1.10h1*です。 • AliCloud ACK (1.26) • GCP GKE（1.17～1.27） *GKE* データプレーン *V2* が含まれています。
顧客が管理する Kubernetes	パブリック クラウドまたはオンプレミス データセンター。 Kubernetes のバージョン、CNI のタイプ、およびホスト VM OS のバージョンがこの表のとおりであることを確認してください。 VMware TKG+ バージョン 1.1.2 • インフラストラクチャ プラットフォーム - vSphere 7.0 • Kubernetes ホスト VM OS - Photon OS
Kubernetes ホスト VM	オペレーティングシステム： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 以降 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux カーネルバージョン： • 4.18以降（K8s サービスモードのみ） • AF_XDP モードを有効にするには 5.4 以降が必要です。詳細については、CN-Series デプロイメント YAML ファイルの編集可能なパラメーターを参照してください。

製品	バージョン
	Linux カーネル Netfilter：Iptables

CNI プラグイン	CNI Spec 0.3 以降:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• AliCloud、Terway用
	• Openshift の場合、OpenshiftSDN
	• 以下は、CN-Series ファイアウォールで DaemonSet としてサポートされています。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	**DaemonSet** としての **CN-Series:** 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12、および4.13 **K8s** サービスとしての **CN-Series:** (PAN-OS 10.1.2以降) 4.7、4.8、4.9、4.10、4.11、4.12、および4.13 *4.12*以上をサポートするために最低限必要なバージョンは*PAN-OS 10.1.10h1*です。

また、CNシリーズ ファイアウォールをデプロイする前にKubernetesクラスタを想定したCNシリーズ システム要件も確認してください。

PAN-OS 10.2

CN-Series ファイアウォールは次の環境でデプロイできます。

製品	バージョン
コンテナ ランタイム	Docker CRI-O Containerd
Kubernetes のバージョン	1.17～1.27
クラウド プロバイダが管理する Kubernetes	• AWS EKS(DaemonSetとしてのCNシリーズおよびデプロイメントのサービス モードとしてのCNシリーズの場合は 1.17～1.27) • AWS EKS (CNF デプロイメント モードとしてのCNシリーズの場合は 1.17～1.22) • AWS Outpost （1.17～1.22） の EKS *AWS Outpost の EKS 用 CN-Series は SR-IOV または Multus をサポートしていません。* • Azure AKS（1.17～1.28） *Azure AKSでは、Kubernetes 1.25以降をサポートするために最低限必要なバージョンはPAN-OS 10.2.4h3です。* • GCP GKE（1.17～1.27） *GCP GKEでは、Kubernetes 1.25以上をサポートするために最低限必要なバージョンはPAN-OS 10.2.4h3です。* *GKE データプレーン V2 が含まれています。* • Google Anthos 1.12.3 • OCI OKE (1.23)
顧客が管理する Kubernetes	パブリック クラウドまたはオンプレミス データセンター。 Kubernetes のバージョン、CNI のタイプ、およびホスト VM OS のバージョンがこの表のとおりであることを確認してください。

製品	バージョン
	VMware TKG+ バージョン 1.1.2 • インフラストラクチャ プラットフォーム - vSphere 7.0 • Kubernetes ホスト VM OS - Photon OS
Kubernetes ホスト VM	オペレーティングシステム： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 以降 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux カーネルバージョン： • 4.18以降（K8s サービスモードのみ） • AF_XDP モードを有効にするには 5.4 以降が必要です。詳細については、CN-Series デプロイメント YAML ファイルの編集可能なパラメーターを参照してください。
	Linux カーネル Netfilter：Iptables

CNI プラグイン	CNI Spec 0.3 以降:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Openshift、OpenshiftSDN、OVN Kubernetes向け
	• 以下は、CN-Series ファイアウォールで DaemonSet としてサポートされています。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

製品	バージョン
OpenShift	• バージョン 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12、および4.13 *OpenShift 4.7* は、*CN-Series* で *DaemonSet* としてのみ認定されています。 • AWS上のOpenShift では、 *4.12*以降をサポートするために最低限必要なバージョンは*PAN-OS 10.2.4h3*です。

また、CNシリーズ ファイアウォールをデプロイする前にKubernetesクラスタを想定したCNシリーズ システム要件も確認してください。

PAN-OS 11.0

CN-Series ファイアウォールは次の環境でデプロイできます。

製品	バージョン
コンテナ ランタイム	Docker CRI-O Containerd
Kubernetes のバージョン	1.17～1.27
クラウド プロバイダが管理する Kubernetes	• AWS EKS(DaemonSetとしてのCNシリーズおよびデプロイメントのサービス モードとしてのCNシリーズの場合は 1.17～1.27) • AWS EKS (CNF デプロイメント モードとしてのCNシリーズの場合は 1.17～1.22) • AWS Outpost（1.17～1.25）のEKS *AWS Outpost* の *EKS* 用 *CN-Series* は *SR-IOV* または *Multus* をサポートしていません。

製品	バージョン
	• Azure AKS（1.17～1.27） *Azure AKS*では、*Kubernetes 1.25*以降をサポートするために最低限必要なバージョンは*PAN-OS 11.0.2*です。 • GCP GKE （1.17～1.27） *GKE* データプレーン *V2* が含まれています。 • OCI OKE (1.23)
顧客が管理する Kubernetes	パブリック クラウドまたはオンプレミス データセンター。 Kubernetes のバージョン、CNI のタイプ、およびホスト VM OS のバージョンがこの表のとおりであることを確認してください。 VMware TKG+ バージョン 1.1.2 • インフラストラクチャ プラットフォーム - vSphere 7.0 • Kubernetes ホスト VM OS - Photon OS
Kubernetes ホスト VM	オペレーティングシステム： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 以降 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux カーネルバージョン： • 4.18以降（K8s サービスモードのみ） • AF_XDP モードを有効にするには 5.4 以降が必要です。詳細については、CN-Series デプロイメント YAML ファイルの編集可能なパラメーターを参照してください。

製品	バージョン
	Linux カーネル Netfilter：Iptables

CNI プラグイン	CNI Spec 0.3 以降:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Openshift、OpenshiftSDN、OVN Kubernetes向け
	• 以下は、CN-Series ファイアウォールで DaemonSet としてサポートされています。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• バージョン 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12、および4.13。 *OpenShift 4.7* は、*CN-Series* で *DaemonSet* としてのみ認定されています。 *4.12*以上をサポートするために最低限必要なバージョンは*PAN-OS 11.0.2*です。 • AWS での OpenShift

また、CNシリーズ ファイアウォールをデプロイする前にKubernetesクラスタを想定したCNシリーズ システム要件も確認してください。

PAN-OS 11.1

CN-Series ファイアウォールは次の環境でデプロイできます。

製品	バージョン
コンテナ ランタイム	Docker CRI-O Containerd
Kubernetes のバージョン	1.17～1.27
クラウド プロバイダが管理する Kubernetes	• AWS EKS(DaemonSetとしてのCNシリーズおよびデプロイメントのサービス モードとしてのCNシリーズの場合は 1.17～1.27) • AWS EKS (CNF デプロイメント モードとしてのCNシリーズの場合は 1.17～1.22) • AWS Outpost（1.17～1.25）のEKS *AWS Outpost の EKS 用 CN-Series は SR-IOV または Multus をサポートしていません。* • Azure AKS（1.17～1.27） *Azure AKSでは、Kubernetes 1.25以降をサポートするために最低限必要なバージョンはPAN-OS 11.0.2です。* • GCP GKE （1.17～1.27） *GKE データプレーン V2 が含まれています。* • OCI OKE (1.23)
顧客が管理する Kubernetes	パブリック クラウドまたはオンプレミス データセンター。 Kubernetes のバージョン、CNI のタイプ、およびホスト VM OS のバージョンがこの表のとおりであることを確認してください。 VMware TKG+ バージョン 1.1.2 • インフラストラクチャ プラットフォーム - vSphere 7.0 • Kubernetes ホスト VM OS - Photon OS

製品	バージョン
Kubernetes ホスト VM	オペレーティングシステム： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 以降 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux カーネルバージョン： • 4.18以降（K8s サービスモードのみ） • AF_XDP モードを有効にするには 5.4 以降が必要です。詳細については、CN-Series デプロイメント YAML ファイルの編集可能なパラメーターを参照してください。
	Linux カーネル Netfilter：Iptables

CNI プラグイン	CNI Spec 0.3 以降:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Openshift、OpenshiftSDN、OVN Kubernetes向け
	• 以下は、CN-Series ファイアウォールで DaemonSet としてサポートされています。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

製品	バージョン
OpenShift	• バージョン 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12、および4.13。 *OpenShift 4.7* は、*CN-Series* で *DaemonSet* としてのみ認定されています。 *4.12*以上をサポートするために最低限必要なバージョンは*PAN-OS 11.0.2*です。 • AWS での OpenShift

また、CNシリーズ ファイアウォールをデプロイする前にKubernetesクラスタを想定したCNシリーズ システム要件も確認してください。

PAN-OS 11.2

CN-Series ファイアウォールは次の環境でデプロイできます。

製品	バージョン
コンテナ ランタイム	Docker CRI-O Containerd
Kubernetes のバージョン	1.17～1.27
クラウド プロバイダが管理する Kubernetes	• AWS EKS(DaemonSetとしてのCNシリーズおよびデプロイメントのサービス モードとしてのCNシリーズの場合は 1.17～1.27) • AWS EKS (CNF デプロイメント モードとしてのCNシリーズの場合は 1.17～1.22) • AWS Outpost（1.17～1.25）のEKS *AWS Outpost* の *EKS* 用 *CN-Series* は *SR-IOV* または *Multus* をサポートしていません。

製品	バージョン
	• Azure AKS（1.17～1.27） *Azure AKS*では、*Kubernetes 1.25*以降をサポートするために最低限必要なバージョンは*PAN-OS 11.0.2*です。 • GCP GKE（1.17～1.27） *GKE* データプレーン *V2* が含まれています。 • OCI OKE (1.23)
顧客が管理する Kubernetes	パブリック クラウドまたはオンプレミス データセンター。 Kubernetes のバージョン、CNI のタイプ、およびホスト VM OS のバージョンがこの表のとおりであることを確認してください。 VMware TKG+ バージョン 1.1.2 • インフラストラクチャ プラットフォーム - vSphere 7.0 • Kubernetes ホスト VM OS - Photon OS
Kubernetes ホスト VM	オペレーティングシステム： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 以降 • CoreOS 21XX、22XX • Container-Optimized OS
	Linux カーネルバージョン： • 4.18以降（K8s サービスモードのみ） • AF_XDP モードを有効にするには 5.4 以降が必要です。詳細については、CN-Series デプロイメント YAML ファイルの編集可能なパラメーターを参照してください。

製品	バージョン
	Linux カーネル Netfilter：Iptables

CNI プラグイン	CNI Spec 0.3 以降:
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• Openshift、OpenshiftSDN、OVN Kubernetes向け
	• 以下は、CN-Series ファイアウォールで DaemonSet としてサポートされています。
	  • Multus
	  • Bridge
	  • SR-IOV
	  • Macvlan

OpenShift	• バージョン 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12、および4.13。 *OpenShift 4.7* は、*CN-Series* で *DaemonSet* としてのみ認定されています。 *4.12*以上をサポートするために最低限必要なバージョンは*PAN-OS 11.0.2*です。 • AWS での OpenShift

また、CNシリーズ ファイアウォールをデプロイする前にKubernetesクラスタを想定したCNシリーズ システム要件も確認してください。

CNシリーズ デプロイメントの前提条件

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN シリーズ ファイアウォールをデプロイするには、以下の前提条件が満たされていることを確認する必要があります。

- CN-Series ファイアウォールのライセンス取得
- CNシリーズ ファイアウォールへのデバイス証明書のインストール
- クラスタ認証用にサービス アカウントを作成する
- Kubernetes プラグインをインストールし、CN-Series 用 Panorama をセットアップする
- CN-Series デプロイメント用にイメージとファイルを取得する

CN-Series ファイアウォールのライセンス取得

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォール ライセンス割り当ては、Kubernetes plugin on Panorama によって管理されます。CN-Series ファイアウォールは、Kubernetes環境にデプロイされた CN-NGFW ポッドによって使用される vCPU（コア）の総数に基づいてライセンス付与されます。CN-NGFW を使用する vCPU ごとに 1 つのトークンが消費されます。

- クレジットのアクティベート—まずクレジットをアクティベートします。アクティベートすると、クレジットプールから CN-Series デプロイメント プロファイルにクレジットを適用できます。
- CN-Series デプロイメントプロファイルの作成-デプロイメント プロファイルで、生成された認証コードに割り当てる vCPU の数を指定します。次に、CN-Series デプロイメントプロファイルに関連付けられた認証コードを使用して、Kubernetes クラスター内のCN-Series ファイアウォールのライセンスを取得します。デプロイメント プロファイルは、割り当てられた vCPU の数に基づいて CN-NGFW ポッドのライセンスを取得するために使用できます。異なる Kubernetes 環境、異なるクラスター、または異なる Panorama インスタンス間で CN-Series ライセンスを取得するには、1 つのデプロイメント プロファイルから 1 つの認証コードを使用します。

  CN-Series-as-a-Kubernetes-Service デプロイメントでは、ご使用の環境にデプロイされた CN-NGFW ポッドの数が、割り当てられた vCPU の数を超えている場合、デプロイメント プロファイルに vCPU を追加するか、十分な CN-NGFW ポッドを削除するまで 30 日間の猶予期間があります。30日間の猶予期間内に追加のvCPUを割り当てるか、ライセンスのないポッドを削除しない場合、クラスター内のすべての CN-Series ファイアウォールのライセンスが解除されます。

  CN-Series が DaemonSet としてデプロイされる際に、デプロイされた CN-NGFW ポッドの数が、割り当てられた vCPU の数を超えている場合、デプロイメントプロファイルに vCPU を追加するか、十分なCN-NGFWポッドを削除するまで 4 時間の猶予期間があります。4時間の猶予期間内に追加の vCPU を割り当てないか、ライセンスのないポッドを削除しない場合、

ライセンスのないポッドはトラフィックの処理を停止します。すでにライセンスを付与されたポッドはライセンスを付与されたままです。

CN-Series のデプロイメント プロファイルを作成するときに、仮想 Panorama アプライアンスをプロビジョニングするオプションもあります。

- デプロイメントプロファイルの管理-CN-Series デプロイメントの要件に基づいて、CN-Series デプロイメント プロファイルを編集、複製、または削除できます。さらに、サブスクリプションを作成した後、デプロイメント プロファイルにサブスクリプションを追加したり、デプロイメント プロファイルからサブスクリプションを削除したりできます。

ライセンスは、クラスターレベルで *CN-Series* に適用されます。個々の *CN-NGFW* にライセンスが付与されていないように見える場合がありますが、クラスター全体がライセンス解除されるまで、クラスター内のすべてのポッドにはライセンスが付与されています。

クレジットのアクティベート

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

組織内では、それぞれが異なる目的を持つ多くのアカウントを作成できます。アクティベーション中は、デフォルトのクレジットプールごとに 1 つのアカウントのみを選択できます。クレジット プールがアクティブになると、クレジット管理者ロールを付与されたユーザーは、クレジットをデプロイメントに割り当て、クレジットを他のプールに転送することもできます。

既存の CSP アカウントがあり、スーパーユーザーまたは管理者である場合、システムは自動的にクレジット管理者ロールをプロファイルに追加します。既存のアカウントがない場合、CSP は自動的にアカウントを作成し、クレジット管理者ロールをプロファイルに追加します。

お客様 (購入者) は、サブスクリプション、クレジット プール ID、サブスクリプションの開始日と終了日、購入したクレジットの金額、およびデフォルトのクレジット プール (クレジットをアクティベートしたときに作成されたクレジット プール) の説明が記載された電子メールを受信します。

後で参照できるように、このメールを保存してください。

STEP 1 | 電子メールで、[アクティベーションの開始]をクリックして、使用可能なクレジットプールを表示します。

STEP 2 | アクティベートするクレジットプールを選択します。検索フィールドを使用して、アカウントリストを番号または名前でフィルタリングできます。

複数のクレジット プールを購入した場合は、両方が自動的に選択されます。チェックマークは、オンボーディングクレジットのアクティベーションリンクを表します。

認証またはサインインするように求められます。

クレジットプールの選択を解除すると、それらのクレジットをアクティベートするには、電子メールに戻って*[アクティベーションの開始]*リンクをクリックする必要があるというリマインダーが表示されます。

STEP 3 | [アクティベーションの開始]を選択します。

STEP 4 | サポートアカウントを選択します（アカウント番号または名前で検索できます）。

STEP 5 | デフォルトのクレジットプールを選択します。

STEP 6 | [デポジットクレジット]を選択します。

デポジットが正常に完了したというメッセージが表示されます。

STEP 7 | (オプション)これが初めてのクレジットアクティベーションである場合は、[デプロイメントプロファイルの作成]ダイアログが表示されます。

CN-Series デプロイメントプロファイルの作成に進みます。

CN-Series デプロイメントプロファイルの作成

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaHelm 3.6 or above version clientHelmを使用したCNシリーズデプロイメントのためにPAN-OS 10.1.x以降のバージョンを実行している

CNシリーズ デプロイメント プロファイルを作成するには、以下の手順を実行します。

STEP 1 | すでにクレジットプールがある場合は、アカウントにログインし、ダッシュボードからアセット > ソフトウェア **NGFW** クレジット > **Prisma NGFW** クレジット > 新規プロファイルの作成 を選択します。

クレジットプールをアクティベートしたばかりの場合は、デプロイメント プロファイルの作成フォームが表示されます。

1. **CN-Series** ファイアウォールタイプを選択します。
2. **PAN-OS10.2** 以降を選択します。
3. **Next**（次へ）をクリックします。

STEP 2 | CN-Series プロファイル。

1. プロファイル名。

   プロファイルに名前を付けます。

2. 合計 **vCPU** 数。

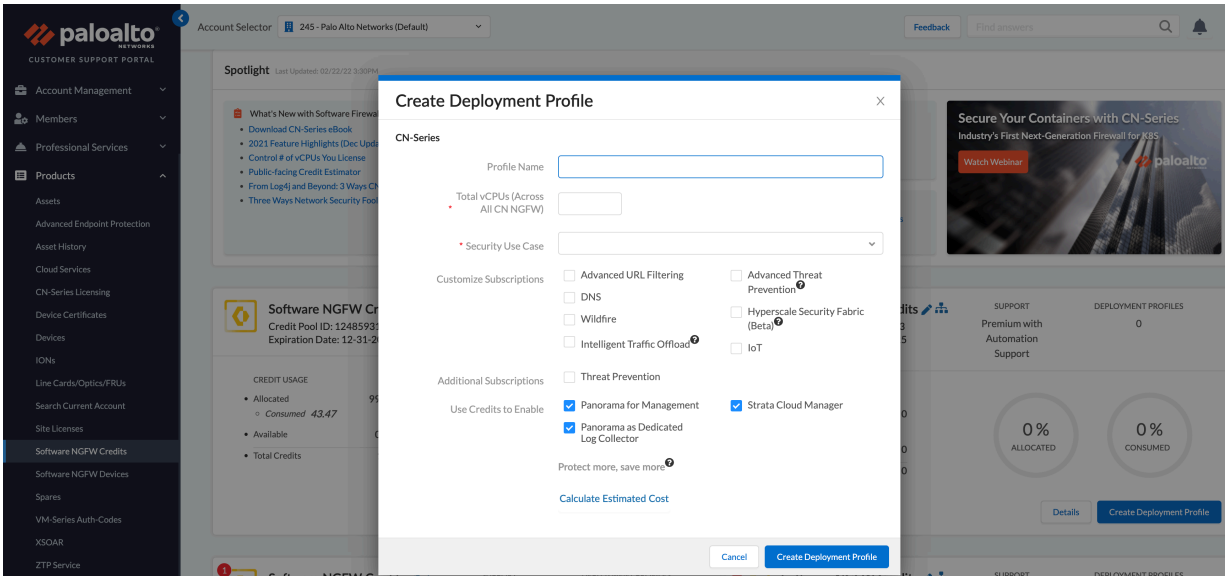
   すべての CN-NGFW にわたる vCPU の総数を入力します。

3. ドロップダウンからセキュリティのユースケースを選択します。ドロップダウンの各セキュリティユースケースは、選択したユースケースに推奨されるいくつかの説明を自動的に選択します。[カスタム]を選択すると、デプロイメントで使用するサブスクリプションを指定できます。
4. （任意）クレジットを使用して **VM Panorama** を有効にする—管理または専用のログコレクタの場合。

STEP 3 | （任意）[さらに保護、さらに保存]の後にある疑問符にカーソルを合わせると、クレジットの割り当てが節約にどのように影響するかを確認できます。

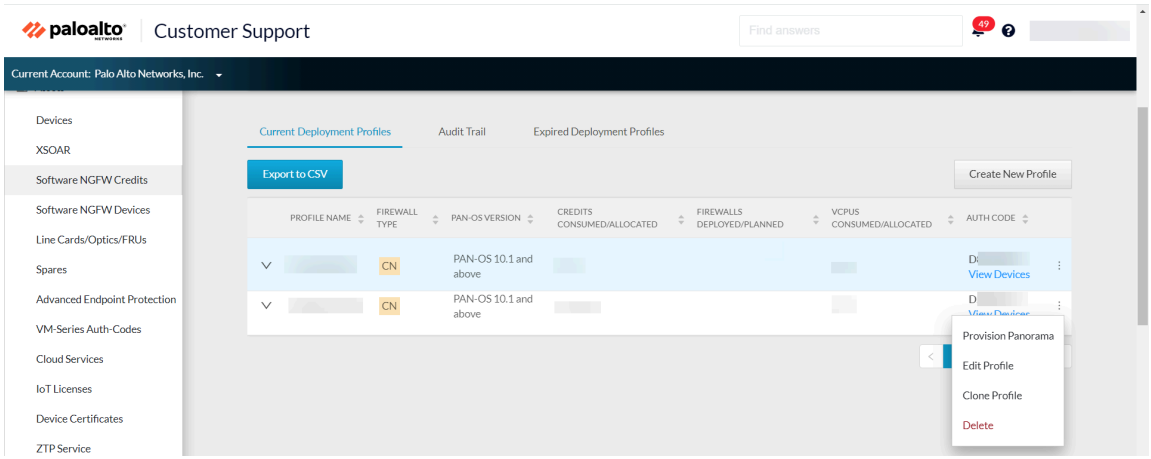
STEP 4 | [見積もりコストの計算]をクリックすると、クレジットの合計と、デプロイメント前に使用可能なクレジットの数が表示されます。

（任意）見積もりの後にある疑問符にカーソルを合わせると、各コンポーネントのクレジットの内訳が表示されます。



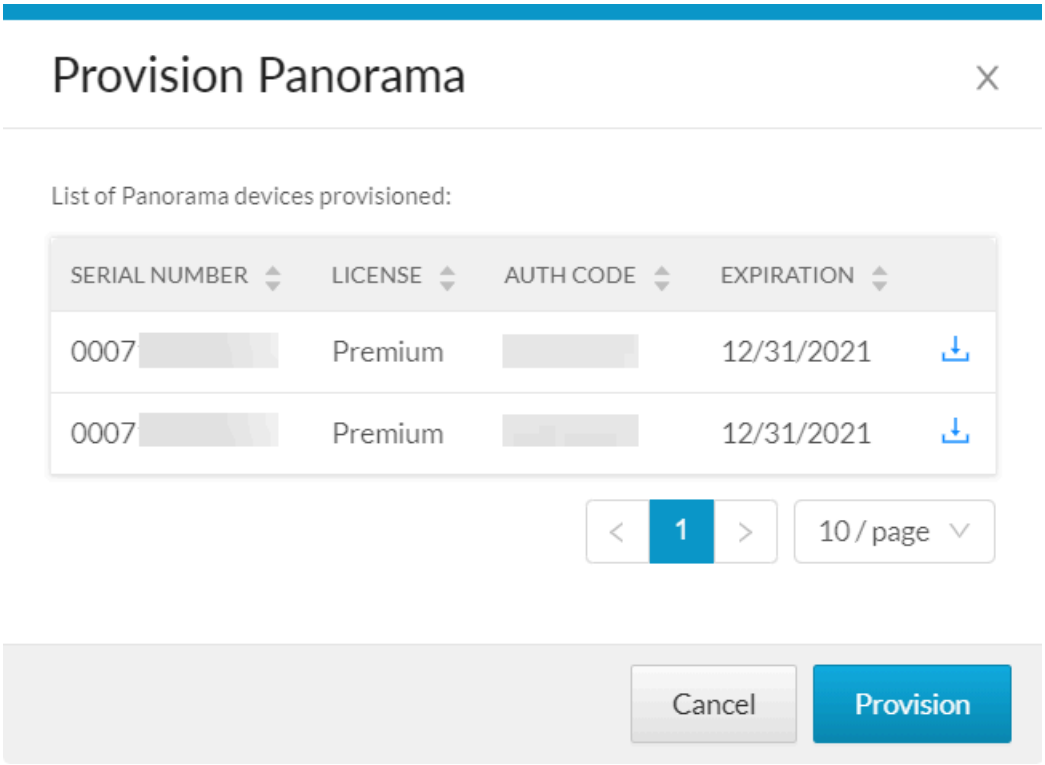
STEP 5 | (任意)Panorama をプロビジョニングします。クレジットを使用して VM Panorama を有効にした場合は、以下の手順を実行して Panorama をプロビジョニングし、シリアル番号を生成します。CNシリーズのデプロイメントを管理するにはパノラマが必要です。シリアル番号を Panorama に適用すると、Panorama はライセンス更新サーバーに接続してライセンスを取得します。

1. アセット > ソフトウェア **NGFW** クレジット > **Prisma NGFW** クレジットを選択し、デプロイメント プロファイルを見つけます。
2. 右端で、縦の省略記号を選択し、[**Panorama** のプロビジョニング]を選択します。



3. [Panorama のプロビジョニング]をクリックして、シリアル番号を生成します。

4. シリアル番号を記録またはコピーして、Panorama インスタンスに適用します。



5. Panorama を登録します。

デプロイメントプロファイルの管理

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

以下の手順を使用して、既存のデプロイメントプロファイルを管理できます。

- デプロイメントプロファイルの編集
- デプロイメントプロファイルのクローン作成
- デプロイメントプロファイルの削除
- 同じアカウントのプールにクレジットを転送する
- クレジットを別の CSP アカウントに転送する

デプロイメントプロファイルの編集

既存のデプロイメントプロファイルを変更して、クレジットを追加したり、デプロイメントに vCPU を追加したりできます。変更するデプロイメントプロファイルに関連付けられている認証コードは、Panorama で使用してはなりません。

STEP 1 | アセット > ソフトウェア **NGFW** クレジット を選択し、プロファイルを選択します(行を選択)。

STEP 2 | 右端で、縦の省略記号（[その他のオプション]）を選択し、[プロファイルの編集]を選択します。

STEP 3 | 変更を加えて、[デプロイメントプロファイルの更新]を選択します。

デプロイメントプロファイルのクローン作成

以下の手順を実行して、既存のデプロイメント プロファイルのクローンを作成します。

STEP 1 | [アセット > ソフトウェア **NGFW** クレジット]に移動し、プロファイルを選択します(行を選択)。

STEP 2 | 右端で、縦の省略記号([その他のオプション])を選択し、[プロファイルのクローン作成]を選択します。

STEP 3 | プロファイル名を変更し、その他の変更を加えて、[デプロイメントプロファイルの作成]を選択します。

デプロイメントプロファイルの削除

デプロイメント プロファイルを削除する前に、プロファイルを使用するファイアウォールをすべて削除する必要があります。削除するデプロイメントプロファイルに関連付けられている認証コードは、Panorama で使用してはなりません。

STEP 1 | CSP で[アセット > ソフトウェア **NGFW** クレジット]を選択し、プロファイルを選択します(行を選択)。

STEP 2 | 右端で、縦の省略記号（[その他のオプション]）を選択し、[削除]を選択します。

同じアカウントのプールにクレジットを転送する

アクセスできる別のアカウントのクレジットプールにクレジットを転送できます。

STEP 1 | CSP アカウントにログインします。

STEP 2 | アセット > ソフトウェア **NGFW** クレジットを選択します。

- 送信元クレジットプールを特定し、クレジットプール ID をメモします。
- 宛先クレジットプールを特定し、クレジットプール ID をメモします。

STEP 3 | 送信元クレジットプールに移動し、左下の[クレジットの転送]を選択します。

STEP 4 | 別の **CSP** アカウントを選択します。

1. 新しいクレジットタイプ - クレジットタイプを選択します。このとき、送信元と宛先のタイプは同じである必要があります。
2. クレジットプール **ID** 番号 - クレジットプール ID 番号を選択します。選択したタイプのクレジットプールが宛先アカウントにない場合、CSP はクレジットプールを作成するように指示します。
3. 送金金額 - 送金金額を入力します。

STEP 5 | [クレジットの更新]を選択します。

クレジットを別の **CSP** アカウントに転送する

同じアカウントのクレジットプールにクレジットを転送できます。

STEP 1 | CSP アカウントにログインします。

STEP 2 | アセット > ソフトウェア **NGFW** クレジットを選択します。

- 送信元クレジットプールを特定し、クレジットプール ID をメモします。
- 宛先クレジットプールを特定し、クレジットプール ID をメモします。

  宛先が別のアカウントにある場合は、左上の[現在のアカウント]ドロップダウンからその宛先を選択し、[アセット > ソフトウェア **NGFW** クレジット]を選択します。宛先を見つけて、クレジットタイプとクレジットプール ID をメモします。

STEP 3 | 送信元クレジットプールに移動し、左下の[クレジットの転送]をクリックします。

STEP 4 | 別の CSP アカウントを選択します。

1. 転送先 - アカウント名を選択します。
2. クレジットタイプとして - クレジットタイプを選択します。このとき、送信元と宛先のタイプは同じである必要があります。
3. クレジットプール **ID** 番号 - クレジットプール ID 番号を選択します。選択したタイプのクレジットプールが宛先アカウントにない場合、CSP はクレジットプールを作成するように指示します。
4. 送金金額 - 送金金額を入力します。

STEP 5 | [クレジットの更新]を選択します。

CNシリーズ ファイアウォールへのデバイス証明書のインストール

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

ファイアウォールには、WildFire、AutoFocus、Strata Logging ServiceなどのPalo Altoクラウド配信セキュリティサービス(CDSS)への安全なアクセスを許可するデバイス証明書が必要です。CNシリーズ ファイアウォール デプロイメントにCDSSライセンスを適用するには、自動登録PINを適用する必要があります。各PINは、カスタマーサポートポータル(CSP)上で生成され、ご自分のPalo Alto Networksサポートアカウント固有のものになります。デバイス証明書を正常にインストールするには、CNシリーズmanagement plane(管理プレーン - MP)ポッド(CN-MGMT)にアウトバウンドインターネット接続があり、以下のfully qualified domain name(完全修飾ドメイン名 - FQDN)とポートがネットワークで許可されている必要があります。

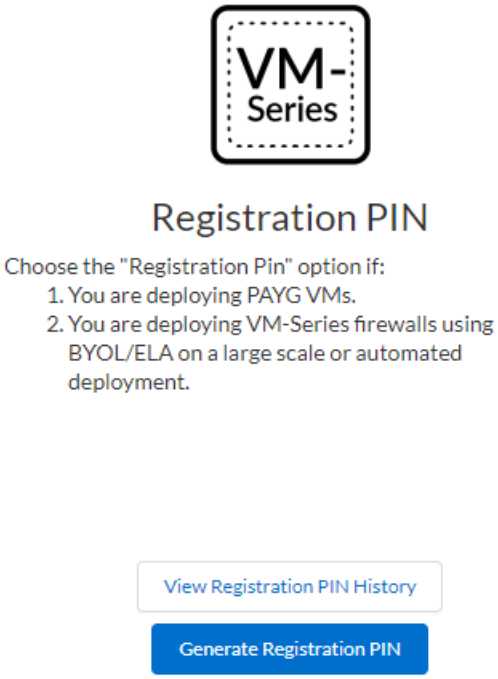
FQDN	ポート
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 および TCP 443

デバイス証明書のない既存のデプロイメントにデバイス証明書を追加するには、有効な*PIN ID*と値を`pan-cn-mgmt-secret.yaml`に追加した後に、*CN*シリーズ ファイアウォールを再デプロイする必要があります。パブリック クラウドの*CN*シリーズのデプロイメントの場合、再デプロイする前に永続ボリューム要求を削除する必要があります。スタティック/ネイティブ*Kubernetes*デプロイメントの場合、再デプロイする前に永続ボリューム要求と永続ボリュームを削除する必要があります。

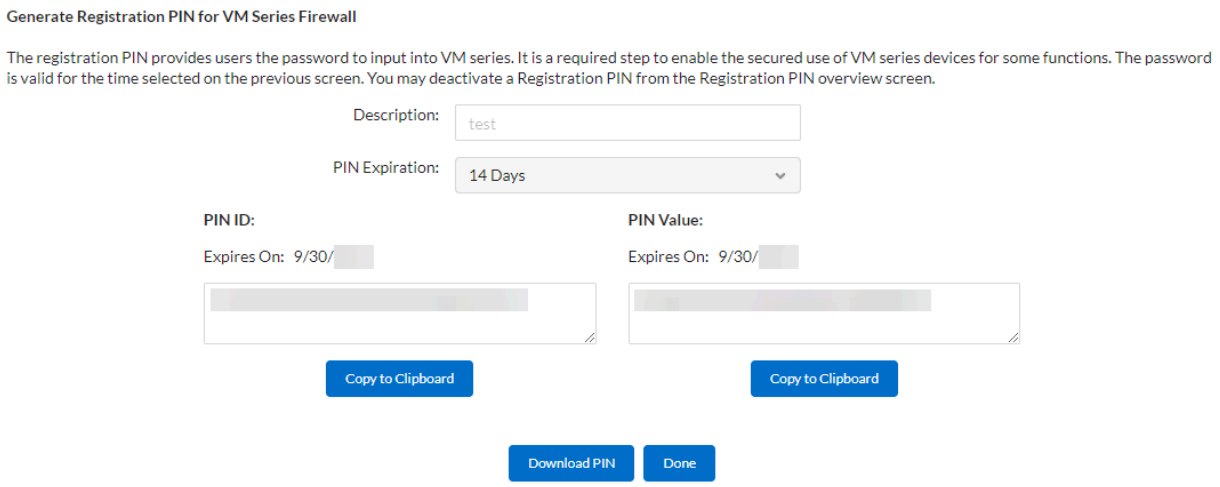
STEP 1 | ご自身のアカウント情報を使用して Palo Alto Networks カスタマーサポート ポータルにログインします。

新しいアカウントが必要な場合は、「新しいカスタマー サポート ポータル ユーザー アカウントを作成する方法」を参照してください。

STEP 2 | **Assets**（アセット） > **Device Certificates**（デバイス証明書） > **Generate Registration PIN**（登録**PIN**の生成）を選択します。



STEP 3 | [説明] を入力し、ドロップダウンから [**PIN** の有効期限] を選択します。



STEP 4 | PIN IDと値を保存します。

PIN IDと値を保存します。このPIN IDと値は、CNシリーズ ファイアウォールのデプロイメントに使用される `pan-cn-mgmt-secret.yaml`ファイルへの入力です。PINが失効する前に、忘れずにファイアウォールを起動してください。

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

クラスタ認証用にサービス アカウントを作成する

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmチャートを使用したCNシリーズのデプロイメント用

CN-Series ファイアウォールには、Kubernetes クラスタ リソースと通信することを許可する最小権限を備えた 3 つのサービス アカウントが必要です。`plugin-serviceaccount.yaml` を使用して作成されたサービス アカウント (pan-plugin-user) を使用すれば、Kubernetes plugin on Panorama で Kubernetes クラスタによるポッド上のメタデータの取得を認証することができます。他の 2 つの yaml ファイル (`pan-mgmt-serviceaccount.yaml` と `pan-cni-serviceaccount.yaml`) は、耐障害性のある CN-Mgmt ポッド間の認証と、CN-MGMT ポッドと CN-NGFW ポッド間の認証を有効にする pan-mgmt-sa サービス アカウントと the pan-cni-sa サービス アカウントを作成します。

デフォルトで、*YAML* ファイルは、*kube-system* 名前空間でサービス アカウントとシークレットを作成します。*Kubernetes* プラグインは、*kube-system* 名前空間でシークレットを検索するだけです。

サービス アカウントを作成するには、Kubernetes クラスタの準備が整っている必要があります。

STEP 1 | `plugin-serviceaccount.yaml` に対してサービス アカウント YAML を実行します。

このサービス アカウントは、Panorama で GKE クラスタによる Kubernetes ラベルとリソース情報の取得を認証するために必要な権限を有効にします。このサービス アカウントには、デフォルトで、pan-plugin-user という名前が付けられています。

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

   このサービス アカウントに関連付けられたシークレットを表示するには、以下の手順を実行します。

   *Kubernetes*のバージョン*1.24*以降を使用している場合は、以下のコマンドを実行して、このサービス アカウントに関連付けられているシークレットを表示します:

   `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`**

   シークレットを含む認証情報ファイル (この例では cred.json という名前が付けられている) を作成し、保存します。このファイルを Panorama にアップロードして、Kubernetes プラグインをインストールし、CN-Series 用 Panorama をセットアップする 内のクラスタを監視するように Kubernetes プラグインをセットアップする必要があります。

STEP 2 | `pan-mgmt-serviceaccount.yaml` と `pan-cni-serviceaccount.yaml` を実行します。

`pan-mgmt-serviceaccount.yaml` は、pan-sa という名前のサービス アカウントを作成し、CN-MGMT ポッドと CN-NGFW ポッドが相互に通信したり、PAN-CNI や Kubernetes API サーバーと通信できるようにするために必要です。このサービス アカウント名を変更した場合は、CN-MGMT ポッドと CN-NFGW ポッドのデプロイに使用する YAML ファイルも更新する必要があります。`pan-cni-serviceaccount.yaml` は、pan-cni-sa という名前のサービス アカウントを作成します。

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

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

STEP 3 | サービス アカウントを確認します。

`kubectl get serviceaccounts -n kube-system`

HELM チャートを使用している場合、ステップ *2* と *3* は *HELM* チャートによって自動化されているため、手動で実行する必要はありません。

Kubernetes プラグインをインストールし、CN-Series 用 Panorama をセットアップする

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

Panorama アプライアンスが CN-Series ファイアウォールのデプロイ先である Kubernetes クラスタと接続できる限り、オンプレミスまたはクラウド内で Panorama アプライアンスをデプロイできます。このワークフローでは、Kubernetes プラグインをインストールして、認証コードをアクティブにし、クラスタを監視するように Kubernetes プラグインをセットアップするプロセスを示します。

Panorama に割り当てるクレジット数は慎重に計画する必要があります。クレジット数を変更した後、*Panorama OS 11.0* に *CN* シリーズ ファイアウォールを再展開する必要はありません。

詳細については、 CN-Series ファイアウォールのライセンス取得 および Software NGFW Credit Estimatorを参照してください。

STEP 1 | ソフトウェア バージョン 11.0 で Panorama をデプロイし、最小のコンテンツ バージョンをインストールします。

1. PAN-OS 11.0 の最小のコンテンツ リリース バージョンについては、**Panorama** > ダイナミック更新に移動します。

   「PAN-OS リリース ノート」を参照してください。

2. ソフトウェアバージョンについては、**Panorama** > ソフトウェアに移動します。

   アップグレードしているリリース バージョンのモデル固有のファイルを特定してダウンロードします。たとえば、M シリーズ アプライアンスを Panorama 11.0 にアップグレードするには、Panorama_m-11.0.0 イメージをダウンロードします。 Panorama 仮想アプライアンスを Panorama 11.0.0 にアップグレードするには、Panorama_pc-11.0.0 イメージをダウンロードします。

   正常にダウンロードが完了すると、ダウンロードしたイメージの **[アクション]** 列が [ダウンロード] から [インストール] に変わります。

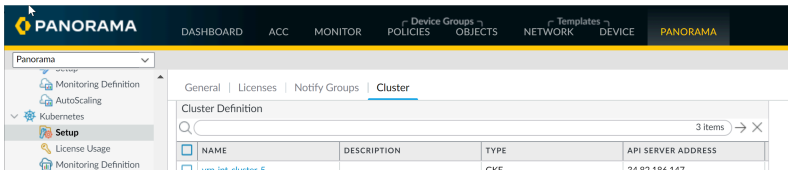
STEP 2 | Panorama でファイアウォール ログを収集する場合は、Panorama が [Panoramaモード] になっていることを確認します。

STEP 3 | Kubernetes plugin on Panorama をインストールします。Panorama アプライアンスが HA ペアとしてデプロイされている場合は、まずプライマリ（アクティブ）ピアに Kubernetes プラグインをインストールする必要があります。

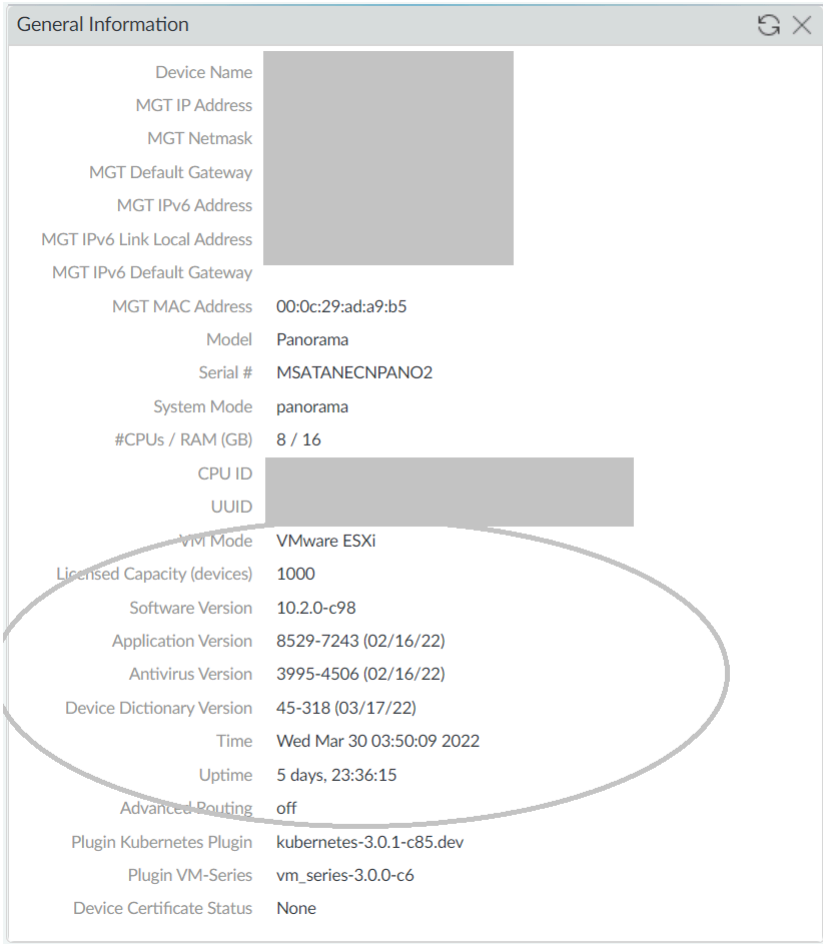
1. Panorama Web インターフェイスにログインし、**Panorama** > **Plugins**（プラグイン）を選択して**Check Now**（今すぐチェック）をクリックし、利用できるプラグインのリストを入手します。
2. **[ダウンロード]** を選択して、Kubernetes プラグインをインストールします。

   インストールが正常に完了したら、Panorama が更新され、**[Panorama]** タブに Kubernetes プラグインが表示されます。

パノラマが HA ペアでデプロイされている場合は、手順 3 で説明した上記の手順に従って、セカンダリ（パッシブ）パノラマに Kubernetes プラグインをインストールします。



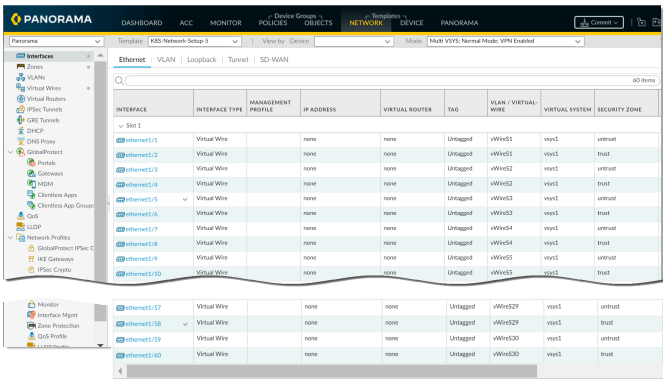
Panorama ダッシュボードで、一般的な情報ウィジェットを確認することもできます。



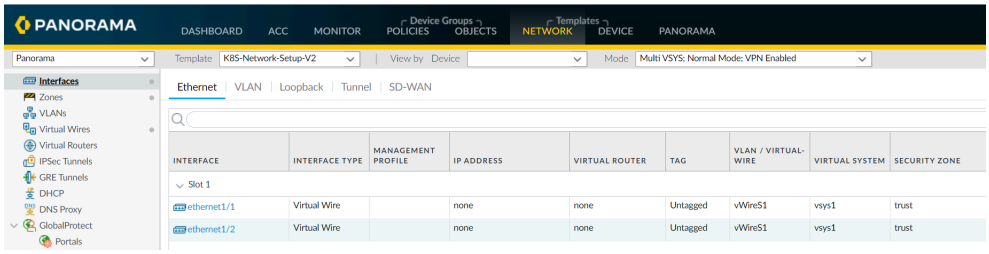
STEP 4 | Panorama 上の変更内容をコミットします。

[Panorama へのコミット**]** をクリックします。コミットにより、**K8S-Network-Setup**、**K8S-Network-Setup-V2**、**K8S-Network-Setup-V3**、および**K8S-Network-Setup-V3-HA**の4つのテンプレートが作成されます。Panorama にインターフェースが表示されるまでに最大 1 分かかります。

- **K8S-Network-Setup** は DaemonSet としての CN-Series で使用するためのものであり、30 本のバーチャル ワイヤを備えています。これは、アプリケーションを保護するためのバーチャル ワイヤの一部であるインターフェースのペアです。そのため、DaemonSet としての CN-NGFW は、ノード上の最大 30 個のアプリケーション ポッドを保護できます。

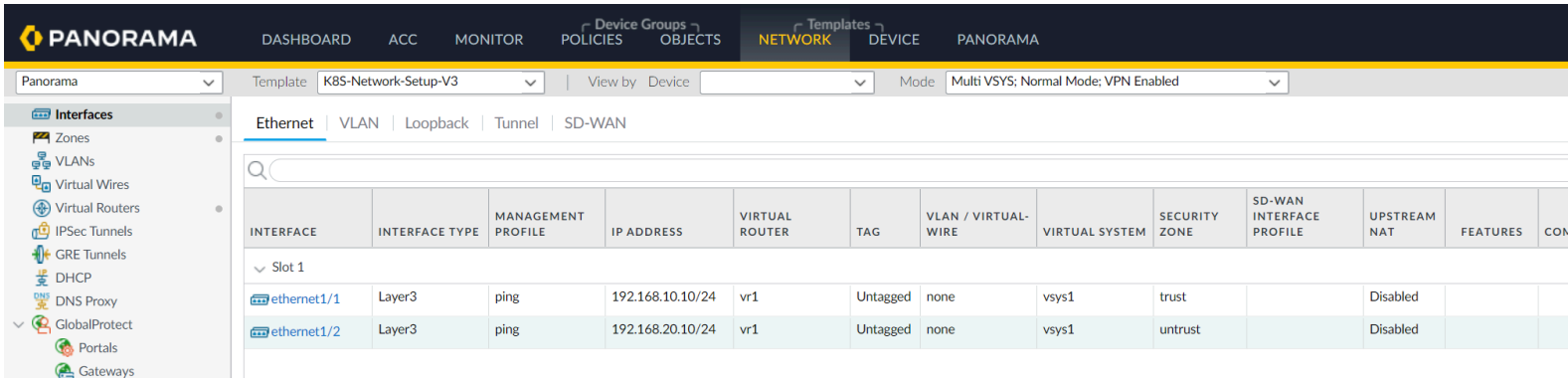


- **K8S-Network-Setup-V2**は、KubernetesサービスとしてのCNシリーズで使用するためのものであり、バーチャル ワイヤを1つ備えています。これは、ポッド アプリケーションを保護するためのバーチャル ワイヤの一部であるインターフェースのペアです。



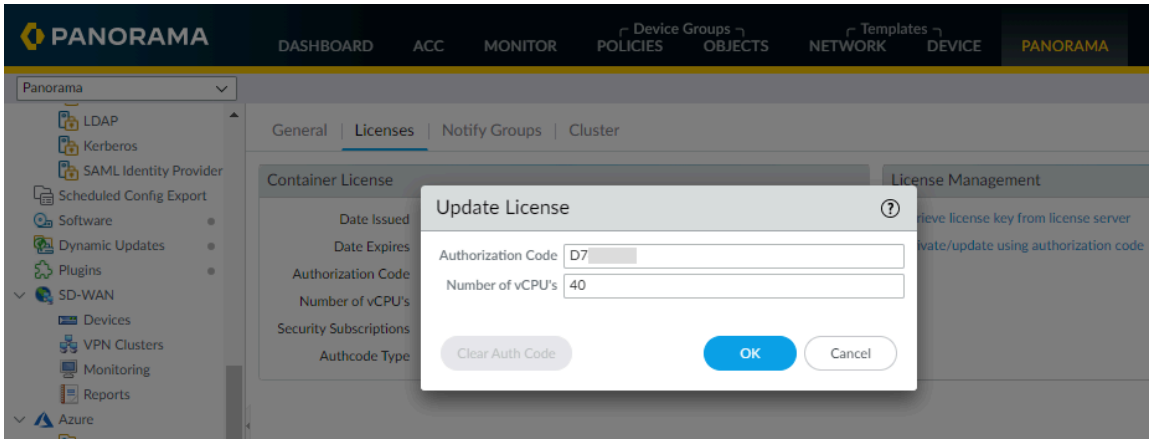
- **K8S-Network-Setup-V3** テンプレートには、複製できるサンプル構成があり、目的の構成に合わせて変更できます。Kubernetes CNFモードは、コンテナと非コンテナの両方のワー

クロードを保護します。スタンドアロンのレイヤー3デプロイメントとしてデプロイできます。



STEP 5 | パノラマで CN-Series のライセンスクレジットを取得します。

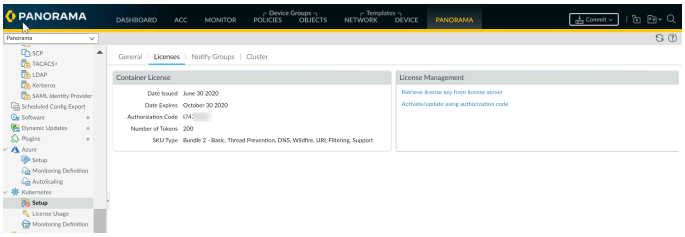
1. **[Panorama]** > **[プラグイン]** > **[Kubernetes]** > **[セットアップ]** > **[ライセンス]** を選択します。
2. 認証コードを使用してアクティベート/更新 を選択し、認証コードと必要なデータプレーン vCPU の総数を入力します。CN-Series の認証コードを取得するためにCN-Series デプロイメントプロファイルの作成をする必要があります。



ライセンスをアクティブにせずに CN-Series ファイアウォールをデプロイする場合は、ファイアウォールがトラフィック処理を停止してから 4 時間の猶予期間が与えられます。猶予期間が過ぎると、CN-NGFW インスタンスが `pan-cn-ngfw-configmap.yaml` で定義された (FAILOVER_MODE) に基づいて、failopen (デフォルト) または failclose します。fail-open モードでは、ファイアウォールがパケットを受信して、セキュリティ ポリシーを適用せずに送信します。fail-open に移行するには、再起動が必要であり、その間はトラフィックが短時間中断します (約 10 ～ 30 秒)。fail-closed モードでは、ファイアウォールが受信したすべてのパケットをドロップしま

す。fail-close は、CN-NGFW ポッドをダウンさせ、新しい CN-NGFW ポッドにライセンス供与するためにクレジットを使用可能なクレジットプールに解放します。

3. 使用可能なライセンス クレジットの数が更新されていることを確認します。



STEP 6 | VM 認証キーを生成します。

1. 以下の前提条件が満たされることを確認します。
   - Panorama にネットワーク アクセスできるコンピュータがあること。
   - PanoramaのIPアドレスが分かること。
   - 管理インターフェイスが、デフォルト設定であるSSHをサポートしていること。管理者が SSH を無効にしたが、再び有効にしたい場合は、**Panorama** > **Setup**（セットアップ） > **Interfaces**（インターフェース）の順に選択します。次に、**Management**（管理）をクリックし、**SSH** を選択して **OK** をクリックします。続いて、**Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、Panorama 設定に対して、変更内容を **Commit**（コミット）します。
2. SSH を使用して CLI にアクセスするには、以下の手順を実行します。
   1. SSH クライアントで Panorama IP アドレスを入力し、ポート 22 を使用します。
   2. 管理アクセス認証情報を指示に従って入力します。ログイン後は message of the day（本日のメッセージ）が表示され、次にCLIのプロンプトが操作モードで表示されます。以下に例を示します。

      ```
      admin@ABC_Sydney>
      ```
3. 以下の操作コマンドを実行します：

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

   次は、24 時間有効なキーを生成する例です。

   request bootstrap vm-auth-key generate lifetime 24

   ```
   VM 認証キー 755036225328715 が生成されました。 有効期限：2020/01/29 12:03:52
   ```
4. 後の手順で必要になるため、VM 認証キーを必ずどこかに保存しておく必要があります。

STEP 7 | 親デバイス グループとテンプレート スタックを作成します。

テンプレート スタックとデバイス グループを作成する必要があります。後で、CN-MGMT ポッドをデプロイするために YAML ファイルを編集するときに、このテンプレート スタックとデバイス グループを参照します。Kubernetes plugin on Panorama が K8S-Network-Setup という名前のテンプレートを作成します。このテンプレートは、ここで定義したテンプレート スタックの一部になります。

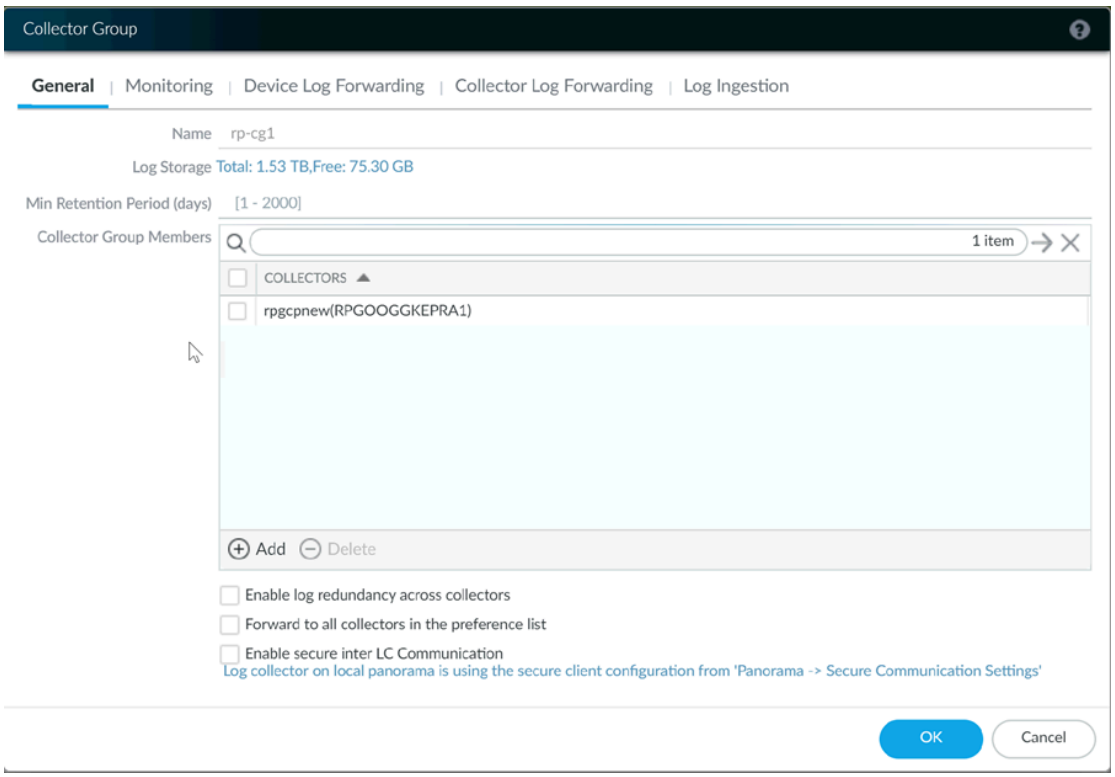
1. テンプレート スタックを作成して、K8S-Network-Setup テンプレートをテンプレート スタックに追加します。
   1. **[Panorama]** > **[**テンプレート**]** を選択し、**[**スタックの追加**]** を選択します。
   2. スタックの識別に使用する一意の **Name**（名前）を入力します。
   3. デーモンセット用の **K8S-Network-Setup** テンプレート、kubernetesのサービスデプロイメントとしての **K8S-Network-Setup-V2**、スタンドアロン CNF デプロイメント

用の **K8S-Network-Setup-V3**、または CNF HA デプロイメント用の **K8S-Network-Setup-V3-HA** を追加して選択します。

4. **OK** をクリックします。

2. デバイス グループを作成します。
   1. **Panorama** > デバイス グループ を選択し、追加 をクリックします。
   2. デバイス グループを識別するために、一意の **Name**（名前）と **Description**（内容）を入力します。
   3. デバイス グループの階層構造で現在作成しようとしているデバイス グループの直接の親にあたる **Parent Device Group**（親デバイス グループ）（デフォルトは **Shared**（共有））を選択します。
   4. **OK** をクリックします。
3. Panorama 仮想 アプライアンスを使用している場合、ログコレクタを作成して、ログコレクタ グループに追加できます。
   1. **Panorama** > **Collector Groups** （コレクタ グループ）の順に選択し、コレクタ グループを 追加します。
   2. コレクタ グループの名前を入力します。
   3. コレクタ グループがファイアウォール ログを保持する **Minimum Retention Period**（最小保持期間）の日数（1 ～ 2,000）を入力します。

      デフォルトでは、このフィールドは空白（コレクタ グループが無期限にログを保持する）です。
   4. ログ コレクタ（1 ～ 16 個）を Collector Group Members（コレクタ グループ メンバー）リストに **Add**（追加）します。



5. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）の順に選択し、変更を Panorama および設定したコレクタ グループに **Commit and Push**（コミットしてプッシュ）します。

4. 高度なルーティングを使用している場合は、有効にしてください。

   1. **Panorama** > テンプレート > ［デバイス に移動します。
   2. 管理タブで、高度なルーティングを選択します。(これは、デプロイメントのKubernetes CNFモードにのみ適用されます)。

STEP 8 | クラスタを監視するための Kubernetes プラグインをセットアップします。

プロセスの次のステップは、Kubernetes クラスタ情報を Panorama に追加して、2 つが相互に通信できるようにすることです。

パノラマは最大*32*個の*Kubernetes*クラスタをサポートします。

プラグインと Kubernetes クラスタが確実に同期されるようにするために、プラグインは構成された間隔でKubernetes API サーバーをポーリングし、 事前定義された間隔で Kubernetes Watch API からの通知を受けます。

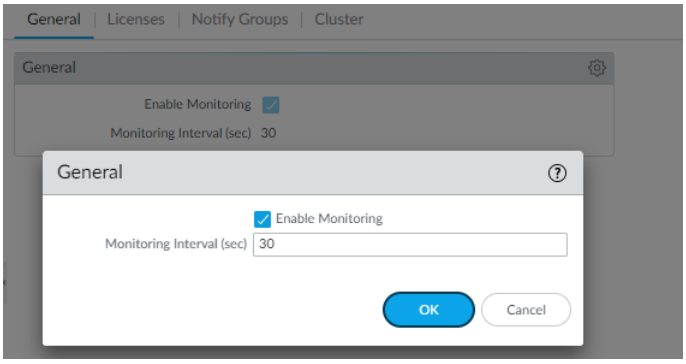
クラスタ情報を追加すると、Panorama は常に、サービス、ノード、レプリカ セットなどを取得して、それら用のタグを作成し、可視性を高め、これらのクラスタとの間でやり取りされるトラフィックを制御できるようにします。必要に応じて、Panorama で Kubernetes ラベルに関する情報を取得し、それらのタグも作成するかどうかを指定できます。詳細にサポートさ

れている属性の一覧については、Kubernetes属性のIPアドレスからタグへのマッピングを参照してください。

1. モニタリング間隔をチェックします。

   Panorama が Kubernetes API サーバー エンドポイントをポーリングするデフォルト間隔は 30 秒です。

   1. **[Panorama]** > **[プラグイン]** > **[Kubernetes]** > **[セットアップ]** > **[一般]** を選択します。
   2. **[Enable Monitoring (モニタリングの有効化)]** が選択されていることを確認します。
   3. 歯車アイコンをクリックして、**[Monitoring Interval (モニタリング間隔)]** を編集し、30 ～ 300 秒の範囲に変更します。



2. **[Panorama]** > **[プラグイン]** > **[Kubernetes]** > **[セットアップ]** > **[クラスタ]** を選択して、**[Add Cluster (クラスタの追加)]** を選択します。

   同じ Kubernetes クラスタが複数の Panorama (単一のインスタンスまたは HA ペア) アプライアンスに追加されていないことを確認します。これは、IP アドレスとのマッピングがデバイス グループに登録される方法への一貫性が失われる場合があるためです。

3. 名前と **API** サーバー アドレスを入力します。

   これは、Kubernetes デプロイメントから取得する必要のあるクラスタのエンドポイント IP アドレスです。クラスタの名前を一意に識別するための名前を最大 20 文字で入力します。この名前は変更することができません。これは、Panorama がクラスタ内で検出したポッド、ノード、およびサービス用のタグを作成するときにクラスタ名を使用するためです。

   API サーバー アドレスの形式は、ホスト名または IP アドレス:ポート番号にすることができます。デフォルト ポートのポート 443 を使用している場合は、ポートを指定する必要がありません。

4. クラスタがデプロイされる環境の **[タイプ]** を選択します。

   使用可能なオプションは、AKS、EKS、GKE、ネイティブ Kubernetes、OpenShift、およびその他です。

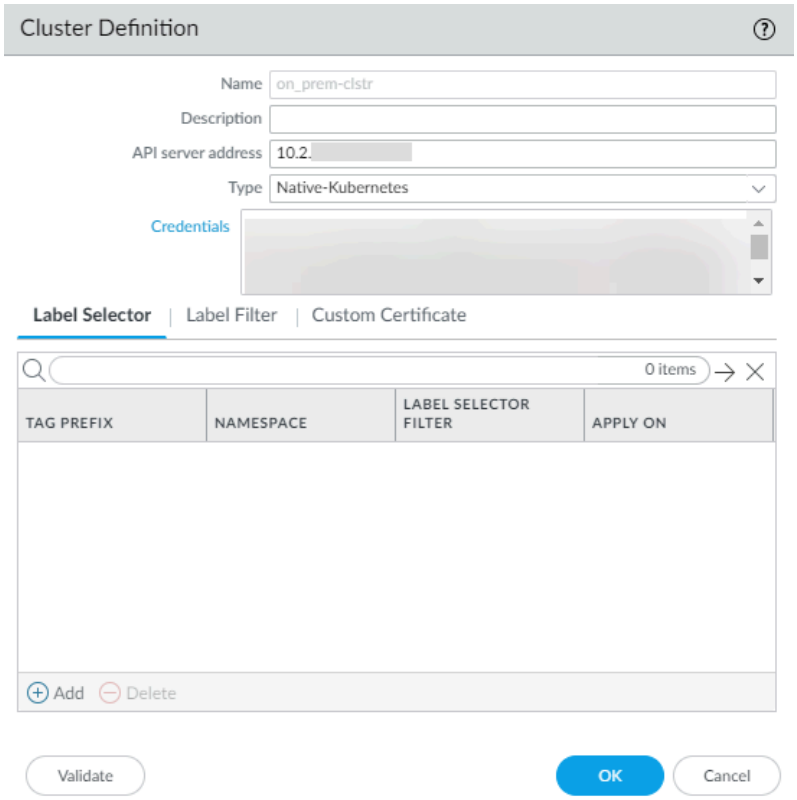
5. Panorama がクラスタと通信するために必要なサービス アカウント認証情報をアップロードします。クラスタ認証用にサービス アカウントを作成するワークフロー

で説明されているように、このサービスアカウントのファイル名は`plugin-svc-acct.json`です。

サービスの資格情報を *CLI/APLI* を介してアップロードする場合は、ファイルを *gzip* で圧縮し、圧縮したファイルの *base64* エンコーディングを実施してから、ファイルの内容を *Panorama* の *CLI* や *API* にアップロードまたは貼り付けを行う必要があります。*GUI* でサービスクレデンシャルファイルをアップロードする場合、これらの手順は必要ありません。

6. **OK** をクリックします。

後で使用するために、ラベル フィルタとラベル セレクタの設定をそのままにしておくことができます。これは、Panorama でタグを作成するカスタム ラベルまたはユーザー定義ラベルを取得できるようにするためのオプション タスクです。

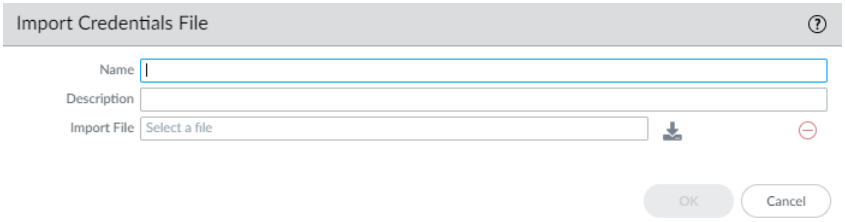


STEP 9 | (任意) Kubernetes クラスタ API サーバー証明書が証明書チェーンによって署名されている場合、Panorama 用の Kubernetes プラグインからの認証には、チェーン内のすべての証明書が

必要です。API サーバーが証明書チェーンを使用している場合は、チェーン内のすべての証明書を 1 つの .crt ファイルに結合し、プラグインに追加する必要があります。

Kubernetes プラグインは最大 *4* つの証明書をサポートします。

1. **Panorama** > **Kubernetes** > セットアップ > クラスタ > 追加 > カスタム証明書 > 追加 を選択して、認証情報ファイルをインポートします。
2. 分かりやすい **Name**（名前）を入力します。
3. （任意）**Description (**内容**)** を入力します。
4. [インポート] アイコンをクリックし、証明書ファイルに移動します。
5. **OK** をクリックします。



STEP 10 | (任意) クラスタごとに 1 つのプロキシを設定します。

他のプラグインとは異なり、Kubernetesプラグインは、**Panorma** > セットアップ > サービスで設定されたプロキシを使用しません。代わりに、プロキシを有効化またはバイパスする場合は、各クラスタのプロキシを入力する必要があります。設定されていれば、Kubernetes プラグインが、このプロキシ サーバーの IP アドレスを使用して、このクラスタの API サーバーに対するすべての API 呼び出しを実行します。

1. Panorama で CLI にログインします。
2. 以下の CLI コマンドを入力して、この Kubernetes クラスタのプロキシ サーバーを設定します。

   ```
   > 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 と password は任意 ***
   ```

STEP 11 | 次のステップ

1. CN-Series デプロイメント用にイメージとファイルを取得する
2. CNシリーズ ファイアウォールをデプロイします。
3. Panorama を設定して Kubernetes デプロイメントをセキュリティで保護する

CN-Series デプロイメント用にイメージとファイルを取得する

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している • Helm 3.6 or above version clientHelmを使用したCNシリーズのデプロイメント用

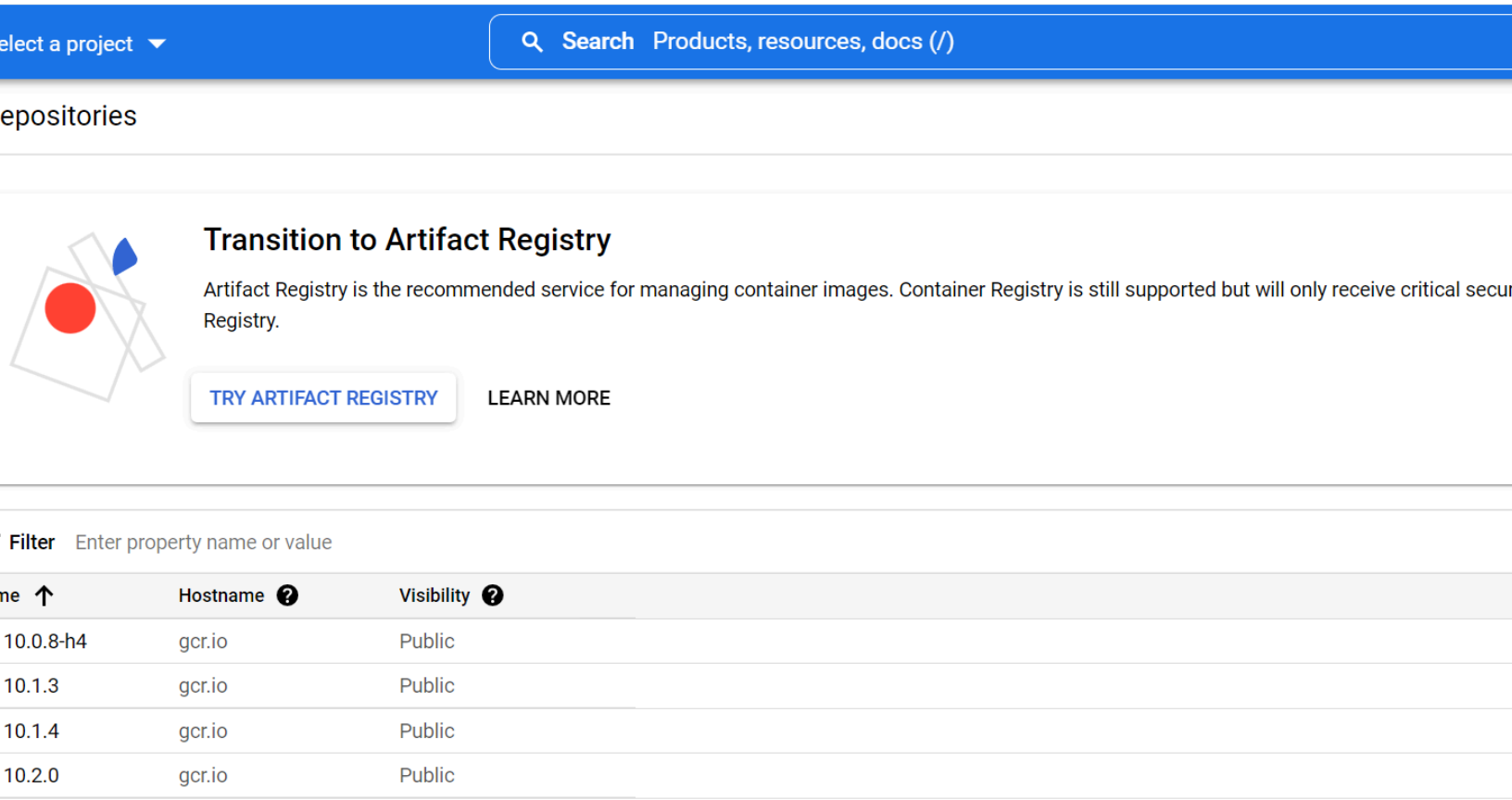
デプロイメントを開始する前に以下の表を参照して、互換性のあるファイルをダウンロードしていることを確認してください。

PAN-OS バージョン	YAML バージョン	CNI バージョン	MGMT-INITバージョン
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

以下の手順に沿って、Google Cloud Platform のパブリック コンテナー レジストリからDocker イメージを取得し、CNシリーズ ファイアウォールをデプロイするに進みます 。

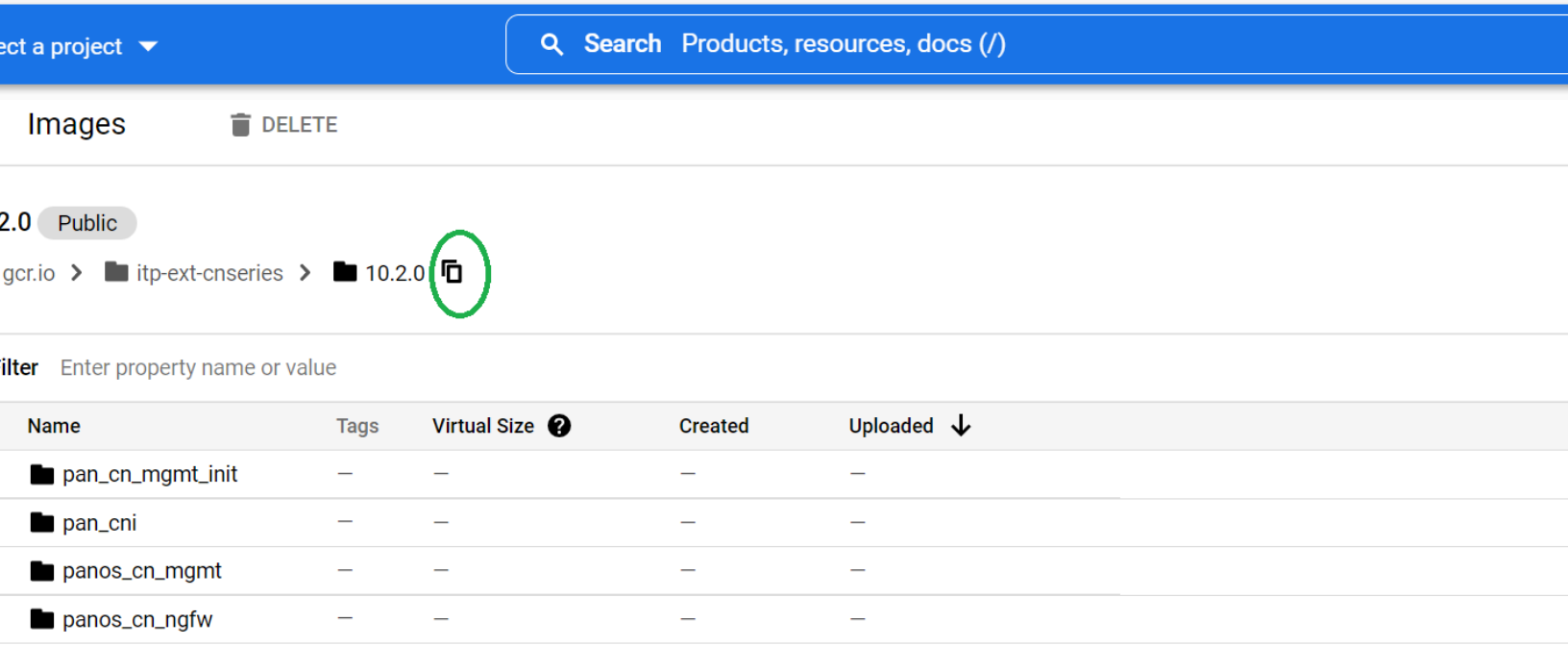
パブリック コンテナ レジストリからの**Docker** イメージ**:**

1. PAN-OS のバージョンに基づいて、パブリッククラウドリポジトリから 必要なDockerイメージを取得します。



2. 必要な PAN-OS バージョンを選択します。

3. 各イメージ パスのリンクを、展開 YAML ファイル内の適切な場所にコピーします。



GitHubからYAMLファイルを取得するには、以下の手順を実行します。

1. 使用する予定のデプロイメント方法 (DaemonSet、Kubernetes Service、または Kubernetes CNF) のフォルダーを開きます。
2. 環境に対応するフォルダから yaml ファイルをダウンロードします。

   ネイティブ Kubernetes オンプレミスまたはクラウド デプロイメントで使用するためのファイルを Native-k8s フォルダから取得します。

   GKE 用のそれぞれのマネージド Kubernetes フォルダからファイルを取得します。

Palo Alto Networks CSP の Docker イメージ:

以下の手順を使用して、GitHubからYAMLファイルを取得し、Palo Alto Networks CSPからDockerイメージをダウンロードして、ユーザーのプライベート レジストリにプッシュしてから、CNシリーズ ファイアウォールをデプロイするに進みます。

STEP 1 | Docker イメージと YAML ファイルをダウンロードします。

1. Palo Alto Networks カスタマー サポート ポータル (CSP) から、圧縮された tar アーカイブを取得します。
   1. サポートアカウントを使用して CSP にログインします。
   2. **Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択します。
   3. [選択してください] ドロップダウンから [**PAN-OS** コンテナイメージ] を選択します。
   4. デプロイしたい PAN-OS バージョンの以下のファイルをダウンロードします。

      PanOS_cn-X.X.X.tgz - CN-MGMT ポッドと CN-NGFW ポッド用。

      Pan_cn_mgmt_init-X.X.X.tgz - CN-MGMT ポッドの一部として動作する初期コンテナ用。

      Pan_cni-2.0.0.tgz-PAN-CNI ポッド用。
2. GitHub から YAML ファイルを取得します。
   1. 使用する予定のデプロイメント方法 (DaemonSet、Kubernetes Service、またはKubernetes CNF) のフォルダを開きます。
   2. 環境に対応するフォルダから yaml ファイルをダウンロードします。

      ネイティブ Kubernetes オンプレミスまたはクラウド デプロイメントで使用するためのファイルを Native-k8s フォルダから取得します。

      AKS、EKS、または GKE 用のそれぞれのマネージド Kubernetes フォルダからファイルを取得します。

STEP 2 | Docker イメージを取得して、コンテナ レジストリにプッシュします。

たとえば、GKE デプロイメント上では、GKE 上のコンテナ レジストリにイメージをアップロードして、YAML ファイルで参照するためのイメージ パスを取得します。Docker エンジンを実行しているクライアント システム上で以下のコマンドを使用します。

以下の手順の *x* 変数を、使用しているイメージ バージョンと一致する値に置き換えます。たとえば、*pan_cn_mgmt-init-2.0.0.tgz* または *pan_cni:2.0.0*。

1. イメージをロードします。

   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

   これらのステップの後で、"docker images" にイメージ ("paloaltonetworks/panos_cn_mgmt:x.x.x" など) が表示されます。

2. これらのイメージにタグを付けて、プライベート レジストリの詳細を含めます。

   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. これらのイメージをプライベート レジストリにプッシュします。

   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

CNシリーズ ファイアウォールを使用したStrata Logging Service

どこで使用できますか?	何が必要ですか?
• CNシリーズ ファイアウォールを使用したStrata Logging Service	• PanoramaPAN-OS 11.1バージョン以上で動作している • Strata Logging Serviceライセンス

Strata Logging Serviceは、企業のデータを正規化してつなぎ合わせる業界唯一のアプローチにより、サイバーセキュリティのための AI ベースのイノベーションを実現します。詳細については、Strata Logging Service の概要およびPanoramaマネージドファイアウォール向けStrata Logging Serviceを参照してください。Strata Logging Serviceでは、CNシリーズ次世代ファイアウォールからログ データを収集できるようになりました。Strata Logging Service ライセンスを購入すると、サポート アカウントに登録されているすべてのファイアウォールに Strata Logging Service ライセンスが付与されます。また、Strata Logging Serviceインスタンスをアクティベートするために必要となるマジック リンクも受け取ります。

CNシリーズ ファイアウォールの Strata Logging Serviceロギングを開始するには、Kubernetesプラグインをインストールし、CNシリーズ ファイアウォール用に Panorama をセットアップする必要があります。Strata Logging Serviceへの接続のために、CN-MGMTポッドにデバイス証明書を提供します。CN-MGMTポッドをCSPアカウントに登録し、CN-MGMTポッドがStrata Logging Serviceインスタンスに反映されるようにすることが重要です。デバイス証明書を正常にインストールするには、有効なPIN-IDとPIN 値を`pan-cn-mgmt-secret.yaml`ファイルに追加します。CNシリーズ ファイアウォールには、Strata Logging Serviceへの安全なアクセスを許可するデバイス証明書が必要です。詳細については、CNシリーズ ファイアウォールにデバイス証明書をインストールするを参照してください。

CNシリーズ ファイアウォールをデプロイした後、CN-MGMTポッドがカスタマー サポート ポータル アカウントの登録済みデバイスに表示されていることを確認します。詳細については、ファイアウォールの登録を参照してください。CNシリーズ ファイアウォールをPanoramaで設定し、CSP アカウントでCNシリーズ デプロイメント プロファイルを作成し、認証コードを使用してPanoramaからCNシリーズ ファイアウォールにライセンスをプッシュするようにしてください。

CNシリーズファイアウォールの**Strata Logging Service**を設定する

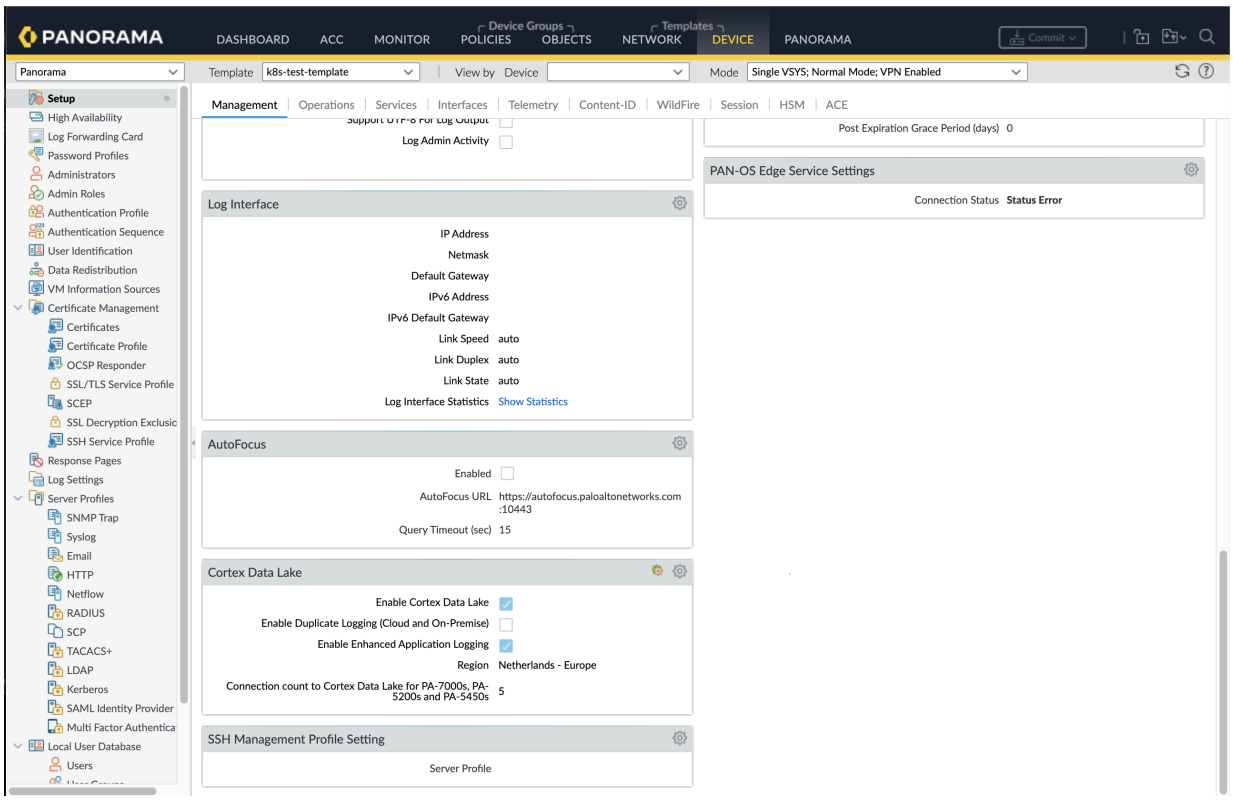
Strata Logging Serviceは、クラウド配信のサービスとアプリケーション向けに、クラウドベースの集中型ログ ストレージと集約機能を提供します。

*CSP*アカウントにロギング ライセンスと *Strata Logging Service*インスタンスが作成されていることを確認します。詳細については、Strata Logging Serviceを参照してください。

PanoramaでStrata Logging Serviceの設定を行い、ファイアウォールにプッシュするには、以下の手順を実行します。

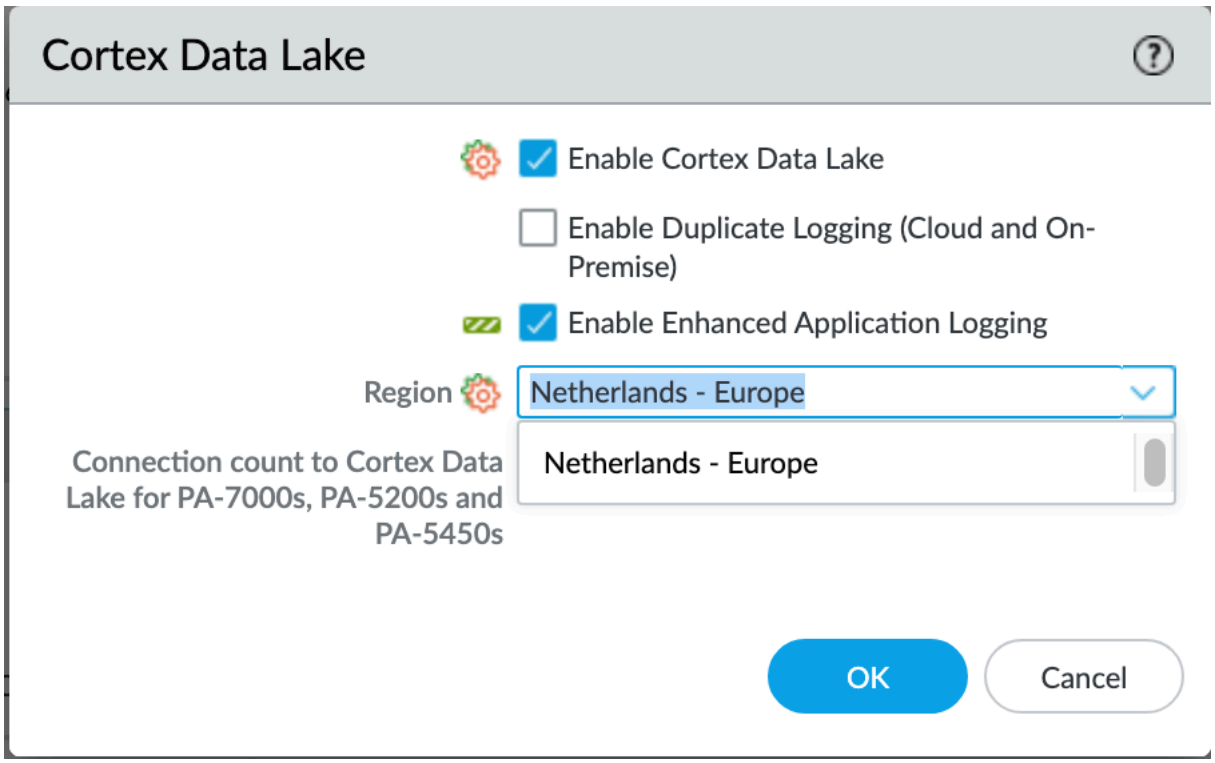
1. PanoramaをStrata Logging Serviceにオンボード化して、デバイス上で Strata Logging Service設定を有効にします。
2. CNシリーズ ファイアウォールを Strata Logging Service インスタンスにオンボード化します。

3. パノラマで、デバイスタブに移動し、**Strata Logging Service**ペインで設定をクリックします。



リージョンにデータが入力されていることがわかります。

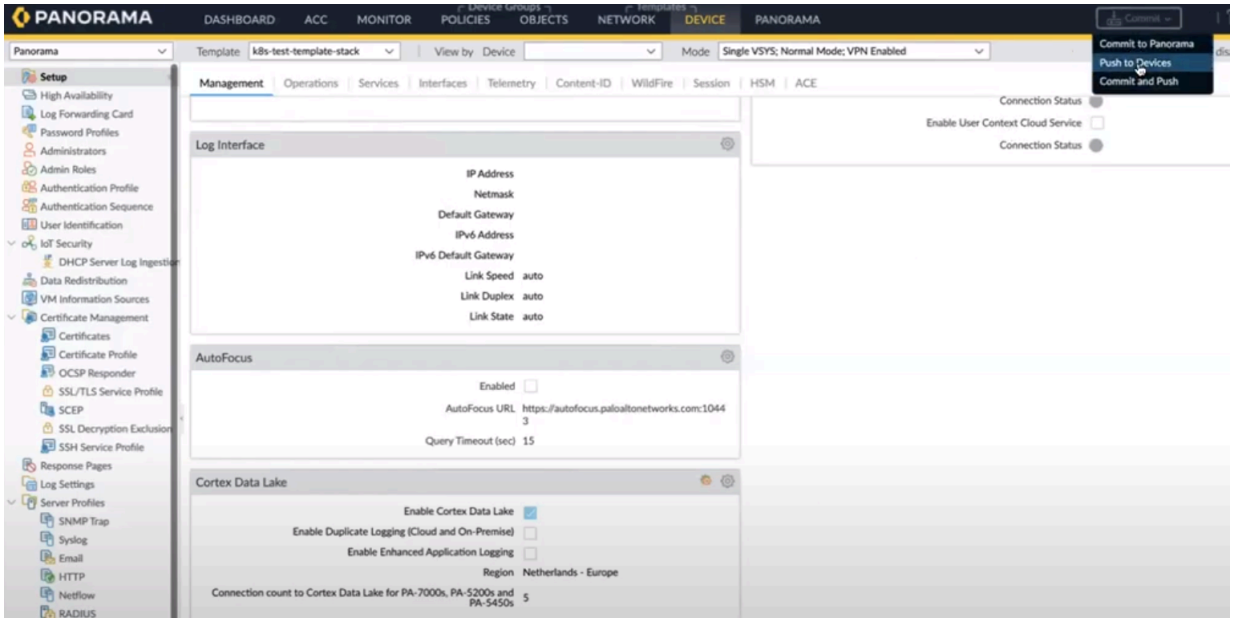
4. **Strata Logging Service**の有効化



をクリックします。

5. **OK** をクリックします。

6. コミット>デバイスにプッシュに移動します。



7. **CN-MGMT**ポッドを選択します。

8. **OK**をクリックします。

   CN-MGMT ポッドのStrata Logging Service設定がプッシュされました。CN-MGMTポッドは、Strata Logging Serviceインスタンスへの接続を開始します。

オンボード化されたファイアウォールが接続状態になると、Strata Logging Serviceインスタンスにログを送信できるようになります。詳細については、Strata Logging Service(Panorama管理)へのログ送信の開始を参照してください。

CNシリーズ ファイアウォールのIoTセキュリティ サポート

どこで使用できますか?	何が必要ですか?
• CNシリーズ ファイアウォールのIoTセキュリティ	• Strata Logging Serviceにデータを保存するIoTサブスクリプションのStrata Logging Serviceライセンス • PanoramaPAN-OS 11.1バージョン以上で動作している

Palo Alto Networksの次世代CNシリーズ ファイアウォールの場合、IoTセキュリティ ソリューションが機械学習(ML)を使用して、ファイアウォールから受信したログのメタデータに基づいて、検出されたIoTデバイスを可視化します。また、IoTセキュリティは、デバイスのネットワーク トラフィック動作とダイナミック更新による脅威フィードに基づいて、デバイスの脆弱性を特定し、リスクを評価します。

CNシリーズ ファイアウォールにルールを手動で追加する際に、IoTセキュリティが生成するポリシー ルールの推奨事項を利用できます。IoTセキュリティはPAN-OSのバージョンに関係なく、セキュリティ ポリシー ルールの推奨事項を常に生成します。

*Strata Logging Service*にデータを保存する***IoT*** セキュリティ サブスクリプションを使用する場合、アカウントごとに*1*つの*Strata Logging Service*ライセンスが必要であり、*CN*シリーズ ファイアウォールのStrata Logging Serviceの設定が完了している必要があります。

詳細については、IoTセキュリティの前提条件を参照してください。

CNシリーズ ファイアウォールの**IoT**サポートの設定

CNシリーズ ファイアウォールでIoTセキュリティをデプロイするには、環境がすべての前提条件を満たしていることを確認する必要があります。詳細については、IoTセキュリティの前提条件を参照してください。

CNシリーズ ファイアウォールの**IoT - Requires Data Lake**サブスクリプションを設定するには、以下の手順を完了する必要があります。

*Panorama*を*Strata Logging Service*インスタンスにオンボード化する必要があります。詳細については、Panoramaのオンボード ファイアウォールを参照してください。

1. TSG(テナント サービス グループ)を作成します。詳細については、共通サービスを通じたIoTセキュリティ サブスクリプションのアクティベートの手順**3**を参照してください。
2. Strata Logging Service テナントをTSGにオンボード化させる。TSGで使用する前に、必ずStrata Logging Serviceを購入し、Magicリンクを使用してアクティベートする必要があります。
3. **IoT - Requires Data Lake**オプションでCNシリーズ デプロイメント プロファイルを作成します。
4. セットアップの終了をクリックします。デプロイメント プロファイルをTSGに関連付けてアクティベートをクリックすると、IoTテナントがまだ作成されていない場合は作成されます。

   その後、収集したメタデータをクラウド ベースのロギング サービスに転送し、IoTセキュリティがそれを使用してネットワーク上のさまざまなIoTデバイスを識別することができます。
5. Panorama のプロビジョニング。シリアルナンバーを生成します。詳細については、パノラマの登録とライセンスのインストールを参照してください。
6. 認証コードを使ってPanoramaでCNシリーズファイアウォールを設定して、kubernetesプラグインを使用してPanoramaでCNシリーズ ファイアウォールにライセンスをプッシュします。詳細については、Panorama を設定して Kubernetes デプロイメントを保護するを参照してください。

   PanoramaのKubernetesプラグインにデプロイメント認証コードを適用します。

   CNシリーズのファイアウォールがIoTテナントにオンボード化されているのを確認できます。
7. テンプレートvwireを設定してゾーン内のデバイス ID を許可および有効にします。

   デフォルトテンプレート**K8S-Network-Setup-V2**を使用し、そのテンプレートで以下の変更を行うことができます。

   - デフォルトvwireのリンクステート パススルーとマルチキャスト ファイアウォールを有効にします。
   - デフォルト ゾーンのデバイス識別を有効にします。

   詳細については、バーチャル ワイヤの設定を参照してください。
8. CNシリーズ ファイアウォールに**Enable Cortex Data Lake**と**Enable Enhanced Application Logging**オプションPanoramaを設定します。詳細については、CN シリーズ ファイアウォールのStrata Logging Serviceの設定を参照してください。

CNシリーズ ファイアウォールの**IoT Security, Doesn't Require Data Lake**サブスクリプションを設定するには、以下の手順を完了する必要があります。

注:PanoramaをStrata Logging Serviceインスタンスにオンボード化する必要があります。IoT Security, Doesn't Require Data Lakeサブスクリプションを利用する場合は、CNシリーズ ファイアウォールを追加した後に、IoTポータルにPanoramaを登録する必要があります。詳細については、IoTセキュリティのためのファイアウォールの準備の手順**2**を参照してください。

1. TSG(テナント サービス グループ)を作成します。詳細については、共通サービスを通じたIoTセキュリティサブスクリプションのアクティベートの手順**3**を参照してください。

2. **IoT - Doesn’t Require Data Lake**オプションでCNシリーズ デプロイメント プロファイルを作成します。
3. IoTインスタンスをセットアップし、セットアップの終了オプションを選択してデプロイメント プロファイルをテナント サービス グループ(TSG)に関連付け、CNシリーズ ファイアウォールでロギング サービスを有効にし、ネットワーク トラフィックのメタデータを取得してログに記録するように設定します。詳細については、IoTセキュリティのためのファイアウォールの準備を参照してください。

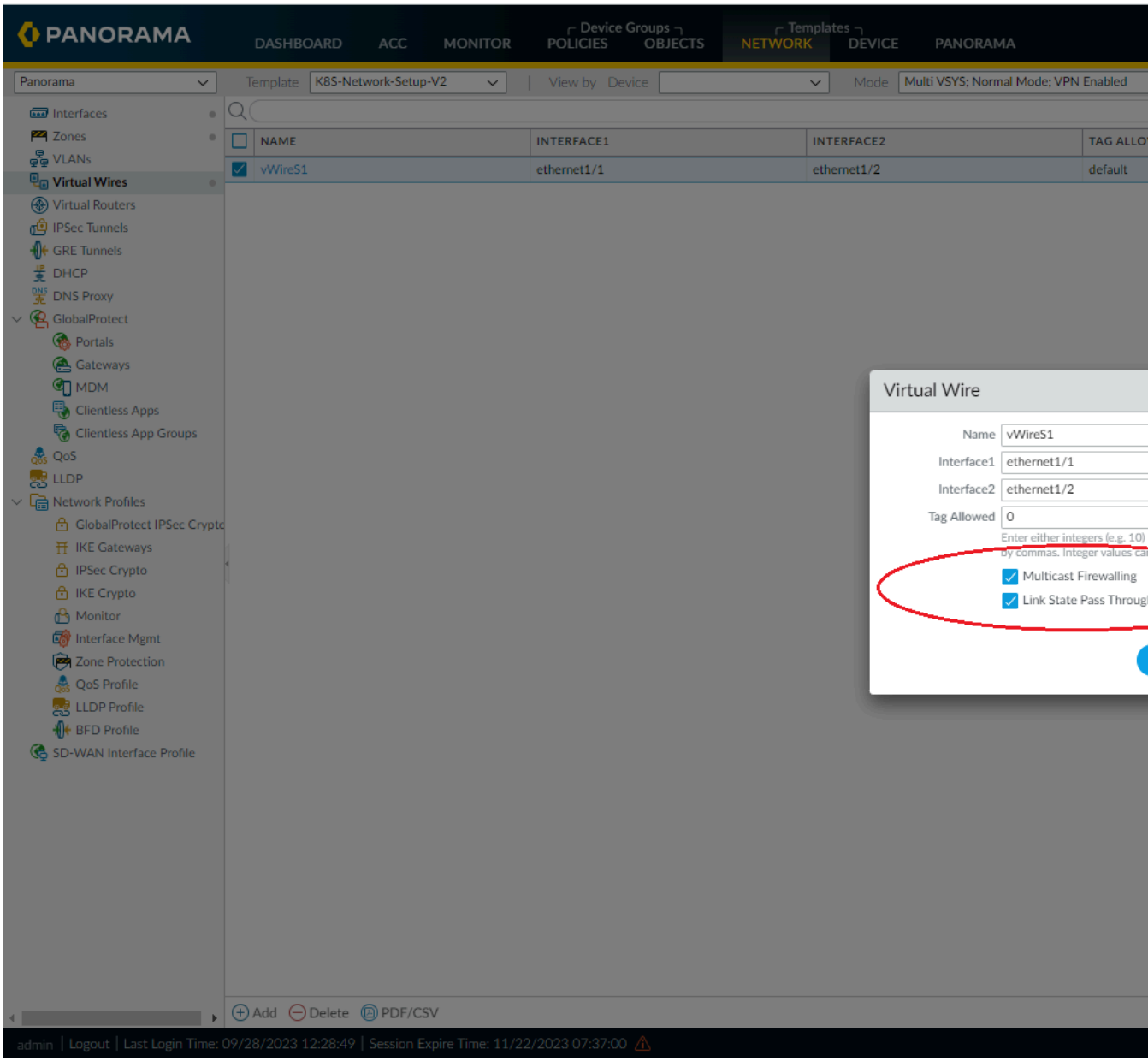
   その後、収集したメタデータをクラウド ベースのロギング サービスに転送し、IoTセキュリティがそれを使用してネットワーク上のさまざまなIoTデバイスを識別することができます。
4. Panorama のプロビジョニング。シリアルナンバーを生成します。詳細については、パノラマの登録とライセンスのインストールを参照してください。
5. 認証コードを使ってPanoramaでCNシリーズファイアウォールを設定して、kubernetesプラグインを使用してPanoramaでCNシリーズ ファイアウォールにライセンスをプッシュします。詳細については、Panorama を設定して Kubernetes デプロイメントを保護するを参照してください。

   PanoramaのKubernetesプラグインにデプロイメント認証コードを適用します。CNシリーズのファイアウォールがIoTテナントにオンボード化されているのを確認できます。

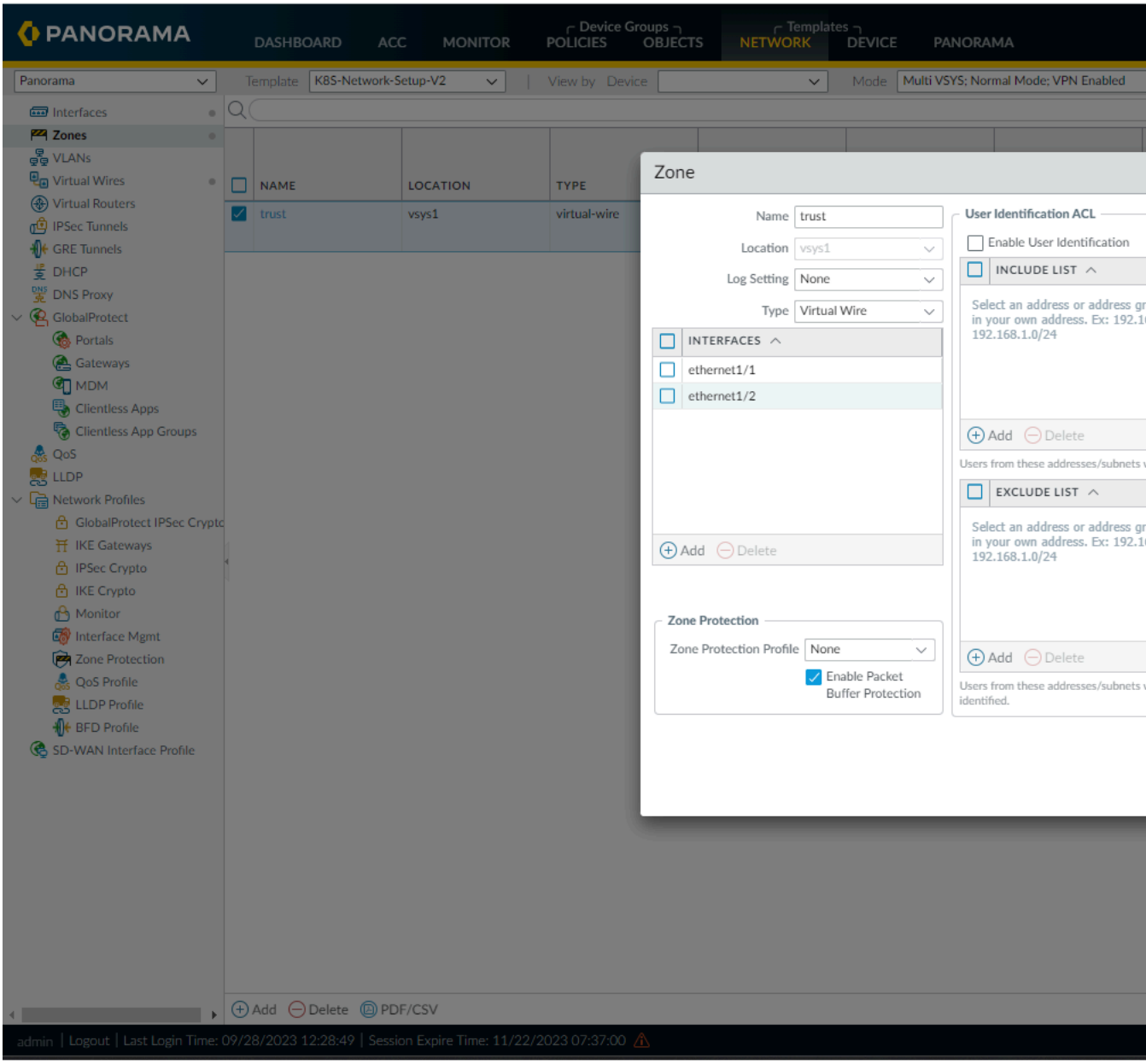
6. テンプレートvwireを設定してゾーン内のデバイス ID を許可および有効化します。詳細については、バーチャル ワイヤの設定を参照してください。

   デフォルトテンプレート**K8S-Network-Setup-V**を使用して、そのテンプレートで以下の変更を行うことができます。

   - デフォルトvwireのリンクステート パススルーとマルチキャスト ファイアウォールを有効にします。



   - デフォルト ゾーンのデバイス識別を有効にします。



詳細については、バーチャル ワイヤの設定を参照してください。

k8s-template-v2で設定されたVwireは、リンクステート パススルーとマルチキャスト ファイアウォールを可能にします。k8s-template-v2のゾーン設定により、デバイスの識別が可能になります

7. CNシリーズ ファイアウォールに**Enable Cortex Data Lake**と**Enable Enhanced Application Logging**オプションPanoramaを設定します。詳細については、CN シリーズ ファイアウォールのStrata Logging Serviceの設定を参照してください。

PanoramaとCNシリーズ ファイアウォールをクラウドベースのロギングサービスに正常にオンボード化したら、IoTインスタンスに移動します。

IoTセキュリティは、ネットワークの動作からデバイスを識別するのに十分な情報を得た後、IPアドレスとデバイスのマッピングを備えたCNシリーズ ファイアウォールと、Panorama管理者がインポートし、CNシリーズ ファイアウォールにプッシュしてIoTデバイスのトラフィックにポリシーを適用できるポリシー推奨事項を備えたPanoramaを提供します。

IoTセキュリティポータルの管理>サイトとファイアウォール>ファイアウォールをクリックして、ロギングサービスがIoTセキュリティ アプリケーションにストリーミングしているログのステータスを確認します。詳細については、ファイアウォールとIoTセキュリティの統合状況をご覧ください。

CNシリーズ ファイアウォールでのソフトウェア カットスルーを前提にしたオフロード

どこで使用できますか?	何が必要ですか?
• Kubernetes CNFデプロイメントとしてのCN-Series	• CN-Series 10.1.x or above Container Images • Panoramaマネージド、CNシリーズ ファイアウォール、PanoramaPAN-OS11.0.4以降のバージョンを実行している

概要

ソフトウェア カットスルー ベースのインテリジェント トラフィック オフロード(ITO)サービスにより、CNシリーズファイアウォールはネットワーク パフォーマンス、セキュリティ、コストのトレードオフを排除します。ITOサービスは、ネットワーク上の新しいフローごとに、そのフローがセキュリティ検査の恩恵を受けられるか否かを判断します。ITOサービスは、フローの最初の数パケットを検査のためにファイアウォールにルーティングします。ファイアウォールは、フローの残りのパケットを検査するかオフロードするかを決定します。この判定は、ポリシーまたはフローが検査できないことに基づいて行われます。セキュリティ検査の恩恵を受けることができるフローのみを検査することにより、ファイアウォールの全体的な負荷が軽減され、セキュリティ態勢を犠牲にすることなくパフォーマンスが向上します。

DPUのないインフラストラクチャでは、ソフトウェア カットスルー ベースのITOが利用可能なNICを利用して機能します。サポートされるNICとハイパーバイザの詳細については、ハイパーバイザ サポート マトリックスを参照してください。

ソフトウェア カットスルー ベースのオフロードは、GTP-Uトンネル プロトコルをサポートします。GTP-U With GTPU inner session software Coordinated Universal Time-throughでは、GTPUインナー セッションがレイヤー7の検査を完了した後、GTPUパケットは既存のソフトウェア カットスルー データパスに従い、不要な操作をバイパスし、FIB/MACキャッシュを利用し、完了まで実行されます。CNシリーズ ファイアウォールは、Kubernetes CNFサービスとしてCNシリーズファイアウォールをデプロイする場合、GTP-U固有のトラフィック オフロードのPAN-OSソフトウェアカットスルー機能をサポートします。

CNシリーズ ファイアウォールでの**GTP-U**固有のトラフィックオフロード

GTPは、UDP/IP上で転送されるコントロールプレーン(GTP-C)、ユーザープレーン(GTP-U)、および課金(GTP-Cから派生したGTP')トラフィックを構成します。GTP をサポートするモデル

別のPAN-OSリリースと、GTPv1-C、GTPv2-C、GTP-U がサポートする 3GPP技術基準を表示します。Palo Alto Networks®ファイアウォールでGTPセキュリティを有効にすると、不正な形式のGTPパケット、Denial-Of-Service(サービス拒否 - DOS)攻撃、ステート外GTPメッセージからモバイル コア ネットワーク インフラストラクチャを保護できます。また、なりすましIPパケットやオーバービリング攻撃からモバイル加入者を保護することもできます。

GTP-U は3GPP TS 29.281で定義されている。ユーザー プレーン トラフィックをカプセル化し、S1、S5、S8 などの複数のシグナリング インターフェースにわたってルーティングします。GTP-Uメッセージは、ユーザー プレーンまたはシグナリング メッセージのいずれかです。GTP-Uの登録ポート番号は2152です。詳細については、GTP保護プロファイルを参照してください。

CNシリーズのソフトウェア カットスルー ベースのオフロードは、GTP-Uトラフィック オフロードもサポートします。CNシリーズのIntelligent Traffic OffloadサブスクリプションをkubernetesのCNFモードとして使用し、GTPセキュリティを活用して、より多くのパフォーマンスを引き出し、モバイルネットワークを保護することができるようになりました。Kubernetes CNFモードとしてのCN-シリーズが検査するすべてのGTP-Uパケットについて、内部セッションで完全なレイヤー7検査が完了します。このGTP-Uパケットの内部セッションがオフロード対象であるとファイアウォールが判断した場合、このセッションに属する以降のすべてのGTP-U パケットがオフロードされます。

CNシリーズ ファイアウォールでソフトウェア カットスルー ベースのオフロードを設定する前に考慮すべき重要なポイントを以下に示します。

- デフォルトでは、ソフトウェア カットスルー ベースのITO設定は無効になっています。
- この機能を有効にするには、ブートストラップ/CLIのみを使用します。
- プレーン トラフィックのためのソフトウェア カットスルー ベースのITOとソフトウェアカットスルーベースのITO内のGTP-Uオフロードを同時に使用できます。
- ITOを有効にした状態で現行バージョンにアップグレードする場合は、CLIを使用してセッション オフロードを有効にします。

*CN*シリーズでは、デプロイメントにおける*Kubernetes*の*CNF*モードとして*CN*シリーズのみがソフトウェア カットスルー ベースの*ITO*をサポートしています。

CNシリーズ ファイアウォールで**GTP-U**インナー セッション オフロードを有効にする

CNシリーズ ファイアウォールでGTP-Uインナー セッション オフロードを有効にするために、GTPセキュリティまたは5Gセキュリティを有効にするための前提条件を以下に示します。

`pan-cn-mgmt-configmap.yaml`ファイルに以下の変更を加えて編集する必要があります。

GTP-U 内部セッションオフロードを有効にするには、`pan-cn-mgmt-configmap.yaml`ファイルで、`PAN_GTP_ENABLED`、`PAN_GTP_CUT_THRU`、および `PAN_SW_CUT_THRU`のパラメータ値を`true` にする必要があります。

更新された pan-cn-mgmt-configmap.yamlファイルの例は以下の通りです。

```
#GTPを有効にして MGMT ポッドを開始します。完全な機能を得るには、Panoramaで
もGTP#の有効化が必要PAN_GTP_ENABLED: "true" # GTP SWカットスルーを有効にし
てMGMTポッドを起動します。PAN_GTP_CUT_THRU: " true " # SWカットスルーを有効
にしてMGMTポッドを起動します。PAN_SW_CUT_THRU: "true"
```

