



OpenStack 向け Cisco Firepower Threat Defense Virtual スタートアップガイド

初版：2021年5月28日

最終更新：2021年10月27日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



第 1 章

Firepower Threat Defense Virtual と OpenStack のスタートアップガイド

OpenStack 環境のコンピューティングノードで実行しているカーネルベースの仮想マシン (KVM) ハイパーバイザに Firepower Threat Defense Virtual (FTDv) を展開できます。

- [OpenStack への FTDv 展開について \(1 ページ\)](#)
- [FTDv と OpenStack の前提条件 \(2 ページ\)](#)
- [FTDv と OpenStack のガイドラインと制限事項 \(3 ページ\)](#)
- [Firepower 展開での OpenStack の要件 \(4 ページ\)](#)
- [OpenStack での FTDv のネットワークトポロジの例 \(5 ページ\)](#)

OpenStack への FTDv 展開について

このガイドでは、OpenStack 環境で FTDv を展開する方法について説明します。OpenStack は無料のオープンな標準規格のクラウド コンピューティング プラットフォームであり、ほとんどの場合は、ユーザーが仮想サーバーやその他のリソースを利用できるように Infrastructure-as-a-Service (IaaS) としてパブリッククラウドとプライベートクラウドの両方に展開します。

この展開では、KVM ハイパーバイザを使用して仮想リソースを管理します。KVM は、仮想化拡張機能 (Intel VT など) を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネルモジュール (kvm.ko) と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。

KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワークカード、ディスク、グラフィックアダプタなどのプライベートな仮想化ハードウェアが搭載されています。

Firepower デバイスは KVM ハイパーバイザですでにサポートされているため、OpenStack サポートを有効にするために必要な追加のカーネルパッケージやドライバはありません。



(注) OpenStack の FTDv は、最適化されたマルチノード環境にインストールできます。

FTDv と OpenStack の前提条件

- software.cisco.com から qcow2 FTDv イメージを取得します。
- FTDv は、オープンソースの OpenStack 環境と Cisco VIM 管理対象 OpenStack 環境での展開をサポートします。
OpenStack のガイドラインに従って OpenStack 環境をセットアップします。
 - オープンソースの OpenStack ドキュメントを参照してください。
Stein リリース : <https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html>
Queens リリース : <https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/overview.html>
 - Cisco Virtualized Infrastructure Manager (VIM) OpenStack のドキュメント (Cisco Virtualized Infrastructure Manager のマニュアル、3.4.3 ~ 3.4.5) を参照してください。
- Cisco スマートアカウント。Cisco Software Central で作成できます。
- Firepower Threat Defense Virtual のライセンス。
 - Firepower Management Center からセキュリティサービスのすべてのライセンス資格を設定します。
 - ライセンスを管理する方法の詳細については、『*Firepower Management Center Configuration Guide*』の「Licensing the Firepower System」を参照してください。
- インターフェイスの要件：
 - 管理インターフェイス (2) : 1つは Firepower Threat Defense Virtual を Firepower Management Center に接続するために使用されます。もう1つは診断目的に使用され、通過トラフィックには使用できません。
 - 内部インターフェイスと外部インターフェイス : Firepower Threat Defense Virtual を内部のホストとパブリックインターフェイスに接続するために使用します。
- 通信パス：
 - Firepower Threat Defense Virtual にアクセスするためのフローティング IP。
- サポートされている FTDv の最小バージョン：
 - バージョン 7.0
- OpenStack の要件については、[Firepower 展開での OpenStack の要件 \(4 ページ\)](#) を参照してください。

- FTDv システムの要件については、『Cisco Firepower Compatibility』 [英語] を参照してください。

FTDv と OpenStack のガイドラインと制限事項

サポートされる機能

OpenStack の FTDv は次の機能をサポートしています。

- OpenStack 環境のコンピューティングノードで実行されている KVM ハイパーバイザへの FTDv の展開
- OpenStack CLI
- Heat テンプレートベースの展開
- OpenStack Horizon ダッシュボード
- ルーテッドモード (デフォルト)
- ライセンス : BYOL のみをサポート
- FMC を使用した FTDv 管理
- ドライバ : VIRTIO、VPP、および SRIOV

FTDv スマートライセンスのパフォーマンス階層

FTDv は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

表 1: FTDv 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様 (コア/RAM)	レート制限 (Rate Limit)	RA VPN セッション制限
FTDv5	4 コア/8 GB	100Mbps	50
FTDv10	4 コア/8 GB	1Gbps	250
FTDv20	4 コア/8 GB	3Gbps	250
FTDv30	8 コア/16 GB	5Gbps	250
FTDv50	12 コア/24 GB	10Gbps	750
FTDv100	16 コア/32 GB	16Gbps	10,000

FTDv デバイスのライセンスを取得する場合のガイドラインについては、『Firepower Management Center Configuration Guide』の「Firepower システムのライセンス」の章を参照してください。

サポートされない機能

OpenStack の FTDv は、以下をサポートしていません。

- 自動スケール
- OpenStack Stein リリースと Queens リリース以外の OpenStack リリース
- Ubuntu 18.04 バージョンと Red Hat Enterprise Linux (RHEL) 7.6 以外のオペレーティングシステム

Firepower 展開での OpenStack の要件

OpenStack 環境は、サポートされているハードウェアとソフトウェアの次の要件に準拠している必要があります。

表 2: ハードウェアおよびソフトウェアの要件

カテゴリ	サポートされるバージョン	注記
サーバ ハードウェア	UCS C240 M5	2 台の UCS サーバーを推奨します。os-controller ノードと os-compute ノードに 1 台ずつです。
ドライバ	VIRTIO、IXGBE、I40E	サポートされているドライバは次のとおりです。
オペレーティング システム	Ubuntu Server 18.04	これは、UCS サーバーで推奨されている OS です。
OpenStack バージョン	Stein リリース	さまざまな OpenStack リリースの詳細については、次の URL を参照してください。 https://releases.openstack.org/

表 3: Cisco VIM Managed OpenStack のハードウェアとソフトウェアの要件

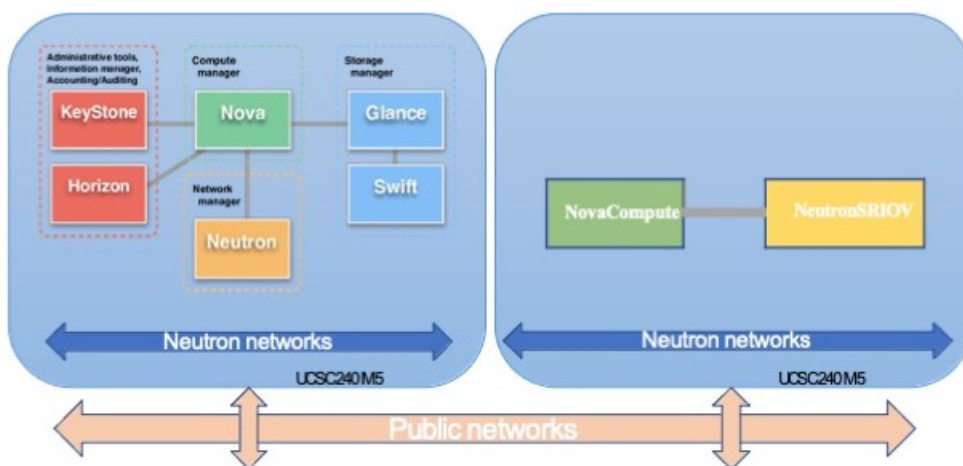
カテゴリ (Category)	サポートされるバージョン	注記 (Notes)
サーバ ハードウェア	UCS C220-M5/UCS C240-M4	os-controller ノードごとに 3 台、os-compute ノードに 2 台以上で、5 台の UCS サーバーを推奨します。
ドライバ (Drivers)	VIRTIO、SRIOV、および VPP	サポートされているドライバは次のとおりです。

カテゴリ (Category)	サポートされるバージョン	注記 (Notes)
オペレーティング システム	Red Hat Enterprise Linux 7.6	これが推奨 OS です。
OpenStack バージョン	OpenStack 13.0 (Queens リリース)	さまざまな OpenStack リリースの詳細については、次の URL を参照してください。 https://releases.openstack.org/
Cisco VIM バージョン	Cisco VIM 3.4.4	Cisco VIM OpenStack のドキュメントを参照してください。

OpenStack プラットフォームトポロジ

次の図に、2 台の UCS サーバーを使用して OpenStack での Firepower の展開をサポートするための推奨トポロジを示します。

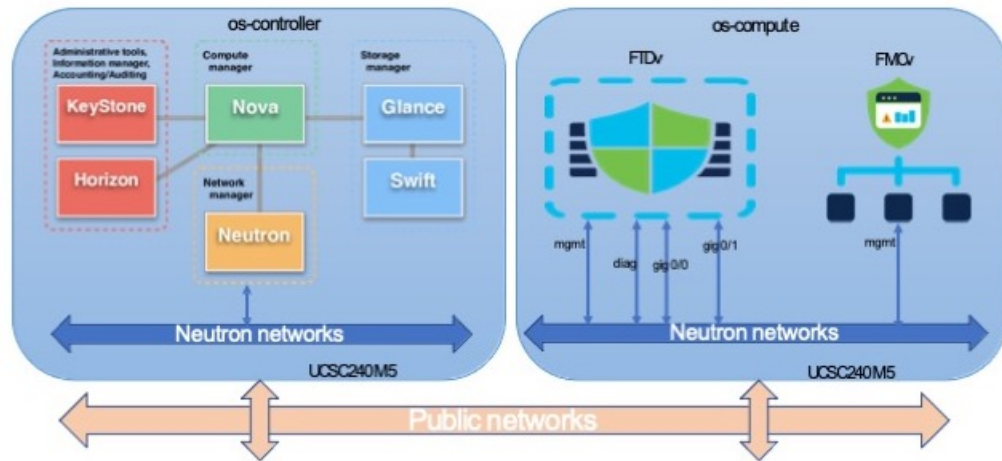
図 1: OpenStack プラットフォームトポロジ



OpenStack での FTDv のネットワークトポロジの例

次の図に、FTDv 用の OpenStack に設定された 4 つのサブネット（管理、診断、内部、および外部）を備えたルーテッドファイアウォールモードの FTDv のネットワークトポロジの例を示します。

図 2: OpenStack で FTDv と FMCv を使用したトポロジの例





第 2 章

OpenStack への Firepower Threat Defense Virtual の展開

- [展開の概要 \(7 ページ\)](#)
- [OpenStack への FTDv イメージのアップロード \(8 ページ\)](#)
- [OpenStack と FTDv のネットワーク インフラストラクチャの作成 \(9 ページ\)](#)
- [OpenStack での FTDv インスタンスの作成 \(9 ページ\)](#)

展開の概要

シスコでは、FTDvを展開するためのサンプルのHeatテンプレートを提供しています。OpenStackインフラストラクチャのリソースを作成する手順は、ネットワーク、サブネット、およびルーターインターフェイスを作成するために、Heatテンプレート (`deploy_os_infra.yaml`) ファイルで結合されます。FTDvの展開手順は大まかに次の部分に分類されます。

- FTDv qcow2 イメージを OpenStack Glance サービスにアップロードします。
- ネットワーク インフラストラクチャを作成します。
 - ネットワーク
 - サブネット
 - ルーター インターフェイス
- FTDv インスタンスを作成します。
 - フレーバ
 - セキュリティ グループ
 - フローティング IP
 - インスタンス

次の手順を使用して、OpenStack に FTDv を展開できます。

OpenStack への FTDv イメージのアップロード

FTDv qcow2 イメージを OpenStack コントローラノードにコピーし、イメージを OpenStack Glance サービスにアップロードします。

始める前に

Cisco.com から FTDv qcow2 ファイルをダウンロードし、Linux ホストに格納します。

<https://software.cisco.com/download/navigator.html>



(注) Cisco.com のログインおよびシスコ サービス契約が必要です。

ステップ 1 qcow2 イメージファイルを OpenStack コントローラノードにコピーします。

ステップ 2 FTDv イメージを OpenStack Glance サービスにアップロードします。

```
root@ucs-os-controller:~$ openstack image create <image_name> --public --disk-format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

ステップ 3 FTDv イメージが正常にアップロードされたことを確認します。

```
root@ucs-os-controller:~$ openstack image list
```

例 :

```
root@ucs-os-controller:~$ openstack image list
list+-----+
| ID | Name | Status |
+-----+-----+-----+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image | active |
+-----+-----+-----+
```

アップロードしたイメージとそのステータスが表示されます。

次のタスク

deploy_os_infra.yaml テンプレートを使用してネットワーク インフラストラクチャを作成します。

OpenStack と FTDv のネットワーク インフラストラクチャの作成

始める前に

Heat テンプレートファイルは、フレーバー、ネットワーク、サブネット、ルーティングインターフェイス、セキュリティグループルールなど、ネットワーク インフラストラクチャと FTDv に必要なコンポーネントを作成するために必要です。

- `deploy_os_infra.yaml`
- `env.yaml`

FTDv バージョンのテンプレートは次の GitHub リポジトリから入手できます。

- <https://github.com/CiscoDevNet/cisco-ftdv/tree/Release-7.0.0/deployment-templates/openstack>



重要 シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

ステップ 1 インフラストラクチャ Heat テンプレートファイルを展開します。

```
root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>
```

例 :

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

ステップ 2 インフラストラクチャ スタックが正常に作成されたかどうかを確認します。

```
root@ucs-os-controller:$ openstack stack list
```

次のタスク

OpenStack で FTDv インスタンスを作成します。

OpenStack での FTDv インスタンスの作成

FTDv Heat テンプレートのサンプルを使用して、OpenStack に FTDv を展開します。

始める前に

OpenStack で FTDv を展開するには、Heat テンプレートが必要です。

- `deploy_ftdv.yaml`

FTDv バージョンのテンプレートは次の GitHub リポジトリから入手できます。

- <https://github.com/CiscoDevNet/cisco-ftdv/tree/Release-7.0.0/deployment-templates/openstack>



重要 シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。更新と ReadMe の手順については、GitHub を定期的に確認してください。

ステップ 1 FTDv Heat テンプレートファイル (`deploy_ftdv.yaml`) を展開して、ASA v インスタンスを作成します。

```
root@ucs-os-controller:~$ openstack stack create ftdv-stack -e env.yaml -t deploy_ftdv.yaml
```

例:

```

+-----+-----+
| Field          | Value                               |
+-----+-----+
| id             | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name     | ftdv-stack                          |
| description    | FTDvtemplate                        |
| creation_time  | 2020-12-07T14:55:05Z                |
| updated_time   | None                                  |
| stack_status   | CREATE_IN_PROGRESS                  |
| stack_status_reason | Stack CREATE started                |
+-----+-----+

```

ステップ 2 FTDv スタックが正常に作成されたことを確認します。

```
root@ucs-os-controller:~$ openstack stack list
```

例:

```

+-----+-----+-----+-----+-----+-----+
| ID              | Stack Name | Project | Stack |
+-----+-----+-----+-----+-----+-----+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-07T14:55:05Z | None |
+-----+-----+-----+-----+-----+-----+
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-03T10:46:50Z | None |
+-----+-----+-----+-----+-----+-----+

```



第 3 章

Firepower Management Center を使用した Firepower Threat Defense Virtual の管理

この章では、FMCを使用して管理されるスタンドアロンのFTDvデバイスを展開する方法について説明します。



(注) このドキュメントでは、最新のFTDvバージョンの機能について説明します。古いバージョンのソフトウェアを使用している場合は、お使いのバージョンのFMCコンフィギュレーションガイドの手順を参照してください。

- [Firepower Management Center を使用した Firepower Threat Defense Virtual について](#) (11 ページ)
- [Firepower Management Center へのログイン](#) (12 ページ)
- [Firepower Management Center へのデバイスの登録](#) (12 ページ)
- [基本的なセキュリティポリシーの設定](#) (14 ページ)
- [Firepower Threat Defense CLI へのアクセス](#) (25 ページ)

Firepower Management Center を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense Virtual (FTDv) は、Cisco NGFW ソリューションの仮想化コンポーネントです。FTDv は、ステートフルファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System (NGIPS)、Application Visibility and Control (AVC)、URL フィルタリング、高度なマルウェア防御 (AMP) などの次世代ファイアウォールサービスを提供します。

FTDv を管理するには、別のサーバー上で実行されるフル機能のマルチデバイスマネージャである Firepower Management Center (FMC) を使用します。FMC のインストールの詳細については、『[FMCgetting started guide](#)』[英語] を参照してください。

FTDv は、FTDv 仮想マシンに割り当てた管理インターフェイス上の FMC を登録して通信します。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して FTD CLI にアクセスすることも、Firepower CLI から FTD に接続することもできます。

Firepower Management Center へのログイン

FMC を使用して、FTD を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート (<https://www.cisco.com/go/firepower-notes>) を参照してください。

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

`https://fmc_ip_address`

`fmc_ip_address` は、FMC の IP アドレスまたはホスト名を指定します。

ステップ 2 ユーザー名とパスワードを入力します。

ステップ 3 [ログイン (Log In)] をクリックします。

Firepower Management Center へのデバイスの登録

始める前に

FTDv 仮想マシンが、正常に展開されていて、電源がオンになっており、最初のブート手順を実行済みであることを確認してください。



(注) この手順では、`day0/bootstrap` スクリプトを使用して、FMC の登録情報が指定されていることを前提としています。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。[FTD のコマンドリファレンス](#)を参照してください。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 2 [追加 (Add)] ドロップダウンリストから、[デバイスの追加 (Add Device)] を選択し、次のパラメータを入力します。

Add Device ? X

Host:†

Display Name:

Registration Key:™

Group: ▼

Access Control Policy:™ ▼

Smart Licensing

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

- [ホスト (Host)] : 追加するデバイスの IP アドレスを入力します。
- [表示名 (Display Name)] : FMC に表示するデバイスの名前を入力します。
- [登録キー (Registration key)] : FTDv ブートストラップ設定で指定したものと同一登録キーを入力します。
- [ドメイン (Domain)] : マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。
- [グループ (Group)] : グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー (Access Control Policy)] : 初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成 (Create new policy)]を選択し、[すべてのトラフィックをブロック (Block all traffic)]を選択します。後でこれを変更してトラフィックを許可することができます。「[アクセス制御の設定 \(23 ページ\)](#)」を参照してください。

New Policy ? X

Name:

Description:

Select Base Policy: ▼

Default Action: Block all traffic Intrusion Prevention Network Discovery

- [スマートライセンス (Smart Licensing)] : 展開する機能に必要なスマートライセンスとして、[マルウェア (Malware)] (AMP マルウェアインスペクションを使用する予定の場合)、[脅威 (Threat)] (侵入防御を使用する予定の場合)、および [URL] (カテゴリベースの URL フィルタリングを実装する予定の場合) を割り当てます。
- [一意の NAT ID (Unique NAT ID)] : FTDv ブートストラップ設定で指定した NAT ID を指定します。
- [パケットの転送 (Transfer Packets)] : デバイスから FMC へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを FMC に送信します。このオプションを無効にした場合は、イベント情報だけが FMC に送信され、パケットデータは送信されません。

ステップ 3 [登録 (Register)] をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されません。FTDv が登録に失敗した場合は、次の項目を確認してください。

- ping : FTD CLI (「[Firepower Threat Defense CLI へのアクセス \(25 ページ\)](#)」) にアクセスし、次のコマンドを使用して FMC IP アドレスへの ping を実行します。

```
ping system ip_address
```

ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。FTD IP アドレスを変更する必要がある場合は、**configure network {ipv4|ipv6} manual** コマンドを実行します。

- NTP : NTP サーバーが [システム (System)] > [設定 (Configuration)] > [時刻の同期 (Time Synchronization)] ページの FMC サーバーセットと一致することを確認します。
- 登録キー、NAT ID、および FMC IP アドレス : 両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、FTDv で登録キーと NAT ID を設定することができます。また、このコマンドで FMC IP アドレスを変更することもできます。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス : 内部インターフェイスにスタティック IP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバー : クライアントの内部インターフェイスで DHCP サーバーを使用します。
- デフォルトルート : 外部インターフェイスを介してデフォルトルートを追加します。
- NAT : 外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール : 内部から外部へのトラフィックを許可します。

- ステップ1 インターフェイスの設定 (15 ページ)
- ステップ2 DHCP サーバーの設定 (18 ページ)
- ステップ3 デフォルトルートの追加 (19 ページ)
- ステップ4 NAT の設定 (21 ページ)
- ステップ5 アクセス制御の設定 (23 ページ)
- ステップ6 設定の展開 (25 ページ)

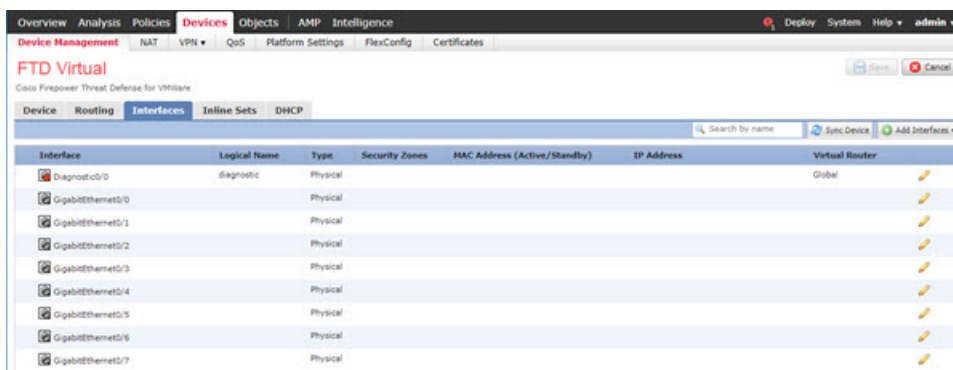
インターフェイスの設定

FTDv インターフェイスを有効にし、それらをセキュリティゾーンに割り当て、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」(DMZ) となる場合があります。

一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

- ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスをクリックします。
- ステップ2 [インターフェイス (Interfaces)] をクリックします。



- ステップ3 「内部」に使用するインターフェイスをクリックします。
[全般 (General)] タブが表示されます。

The screenshot shows the 'Edit Physical Interface' dialog box with the following configuration:

- Name: inside
- Description: (empty)
- Mode: None
- Security Zone: inside_zone
- Interface ID: GigabitEthernet0/0
- MTU: 1500 (64 - 9000)
- Enabled: Management Only:

- 48 文字までの [名前 (Name)] を入力します。
たとえば、インターフェイスに **inside** という名前を付けます。
- [有効 (Enabled)] チェックボックスをオンにします。
- [モード (Mode)] は [なし (None)] に設定したままにします。
- [セキュリティゾーン (Security Zone)] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規 (New)] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできませんが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

- [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

(注) Google Cloud Platform 上の VPC ネットワークは IPv6 をサポートしていません。

- [IPv4] : ドロップダウンリストから [スタティックIPを使用する (Use Static IP)] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

たとえば、**192.168.1.1/24** などと入力します。

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- [IPv6] : ステータス自動設定の場合は [自動設定 (Autoconfiguration)] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスをクリックします。

[全般 (General)] タブが表示されます。

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

a) 48 文字までの [名前 (Name)] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効 (Enabled)] チェックボックスをオンにします。

c) [モード (Mode)] は [なし (None)] に設定したままにします。

d) [セキュリティゾーン (SecurityZone)] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規 (New)] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「outside_zone」という名前のゾーンを追加します。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

(注) Google Cloud Platform 上の VPC ネットワークは IPv6 をサポートしていません。

- [IPv4] : [DHCPの使用 (Use DHCP)] を選択し、次のオプションのパラメータを設定します。
 - [DHCP を使用してデフォルト ルートを取得 (Obtain default route using DHCP)] : DHCP サーバーからデフォルト ルートを取得します。
 - [DHCPルートメトリック (DHCP route metric)] : アドミニストレーティブ ディスタンスを学習したルートに割り当てます (1 ~ 255) 。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is active. Under 'IP Type', 'Use DHCP' is selected. The 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1'.

- [IPv6] : ステートレス自動設定の場合は [自動設定 (Autoconfiguration)] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存 (Save)] をクリックします。

DHCP サーバーの設定



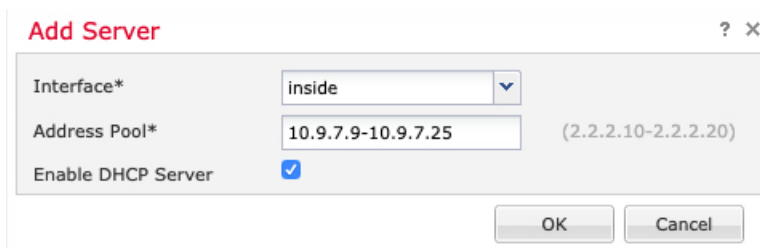
(注) AWS、Azure、GCP、OCIなどのパブリッククラウド環境に展開する場合は、この手順をスキップします。

クライアントで DHCP を使用して FTDv から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスをクリックします。

ステップ 2 [DHCP] > [DHCPサーバー (DHCP Server)] を選択します。

ステップ 3 [サーバー (Server)] ページで、[追加 (Add)] をクリックして、次のオプションを設定します。



- [インターフェイス (Interface)] : ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール (Address Pool)] : DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があるため、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする (Enable DHCP Server)] : 選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存 (Save)] をクリックします。

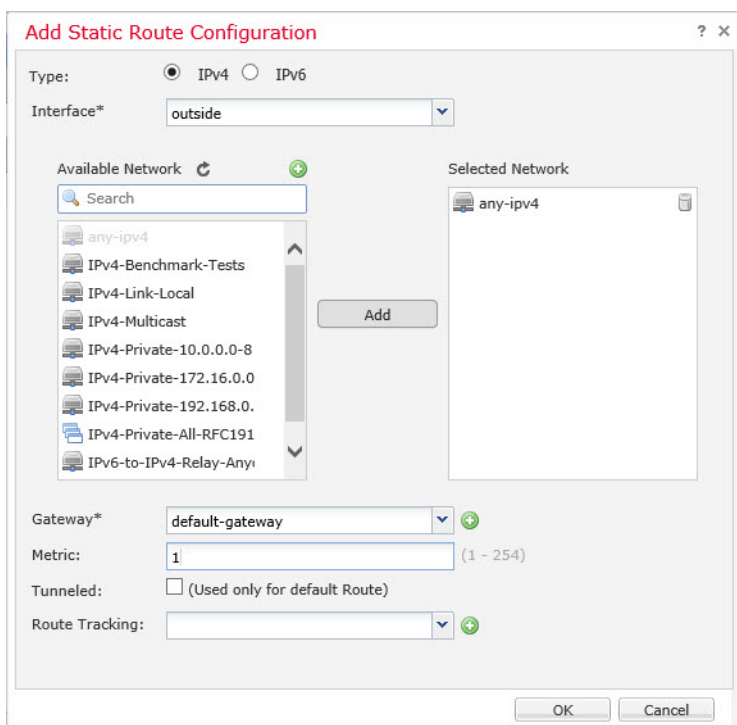
デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。外部インターフェイスに DHCP を使用する場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。DHCP サーバーからデフォルトルートを受信した場合は、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [ルーティング (Routing)] > [スタティックルート (Static Route)] ページの [IPv4 ルート (IPv4 Routes)] または [IPv6 ルート (IPv6 Routes)] テーブルに表示されます。

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスをクリックします。

ステップ 2 [ルーティング (Routing)] > [スタティックルート (Static route)] を選択し、[ルートを追加 (Add route)] をクリックして、次のように設定します。

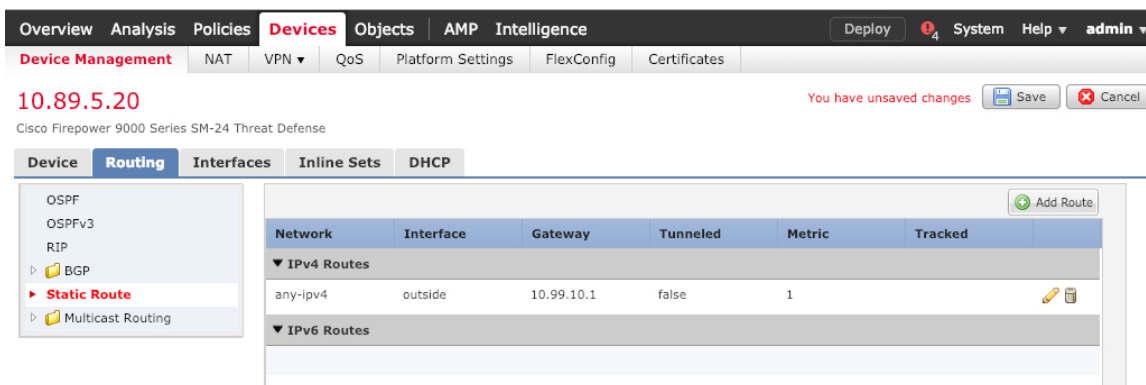
デフォルトルートの追加



- [タイプ (Type)] : 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス (Interface)] : 出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク (Available Network)] : IPv4 デフォルトルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- [ゲートウェイ (Gateway)] または [IPv6ゲートウェイ (IPv6 Gateway)] : このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。
- [メトリック (Metric)] : 宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ~ 255 で、デフォルト値は 1 です。

ステップ 3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。



ステップ 4 [保存 (Save)] をクリックします。

NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポートアドレス変換 (PAT) と呼びます。

ステップ 1 [デバイス (Devices)] > [NAT] をクリックし、[新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存 (Save)] をクリックします。



ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

NAT の設定

ステップ3 [ルール of 追加 (Add Rule)] をクリックします。

[NATルールの追加 (Add NAT Rule)] ダイアログボックスが表示されます。

ステップ4 基本ルールのオプションを設定します。

- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

ステップ5 [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。

ステップ6 [変換 (Translation)] ページで、次のオプションを設定します。

- [元の送信元 (Original Source)] : をクリックして、すべての IPv4 トラフィック (0.0.0.0/0) のネットワークオブジェクトを追加します。

(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元 (Translated Source)] : [宛先インターフェイス IP (Destination Interface IP)] を選択します。

ステップ 7 [保存 (Save)] をクリックしてルールを追加します。

ルールが [ルール (Rules)] テーブルに保存されます。

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
▼ Auto NAT Rules											
#	→	Dynamic	any	outside_zone	all-ipv4			Interface			Ons:false
▼ NAT Rules After											

ステップ 8 NAT ページで [保存 (Save)] をクリックして変更を保存します。

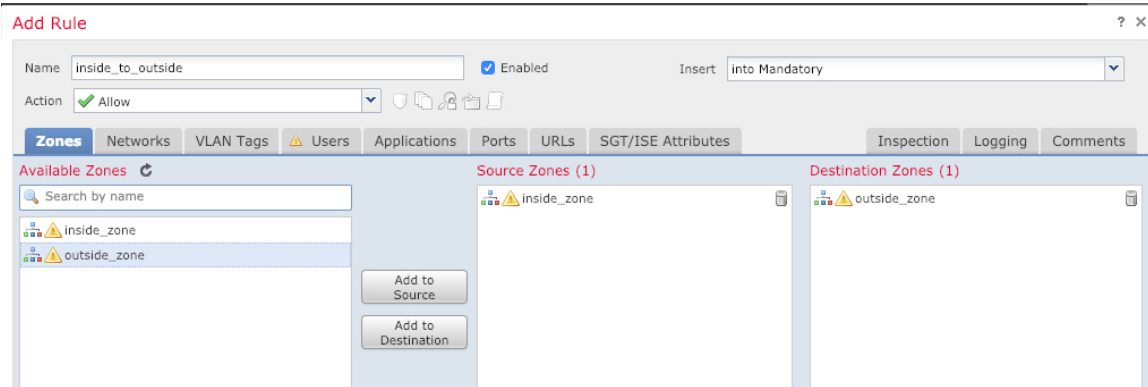
アクセス制御の設定

FTDv を FMC に登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

より高度なセキュリティ設定とルールを設定する場合は、FMC のコンフィギュレーション ガイドを参照してください。

ステップ 1 [ポリシー (Policy)] > [アクセスポリシー (Access Policy)] > [アクセスポリシー (Access Policy)] を選択し、FTD に割り当てられているアクセス コントロール ポリシーのをクリックします。

ステップ 2 [ルールを追加 (Add Rule)] をクリックし、次のパラメータを設定します。

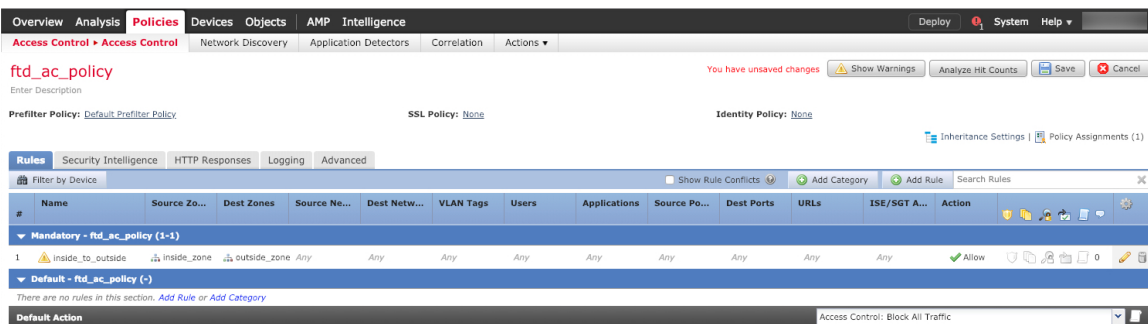


- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside_to_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加 (Add)] をクリックします。

ルールが [ルール (Rules)] テーブルに追加されます。

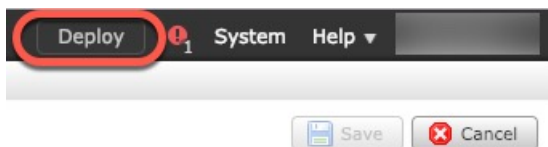


ステップ 4 [保存 (Save)] をクリックします。

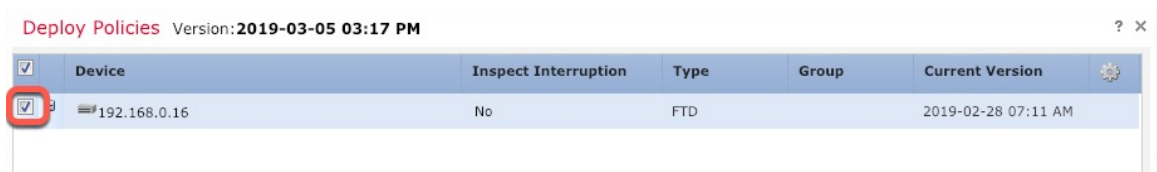
設定の展開

設定の変更を FTDv に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

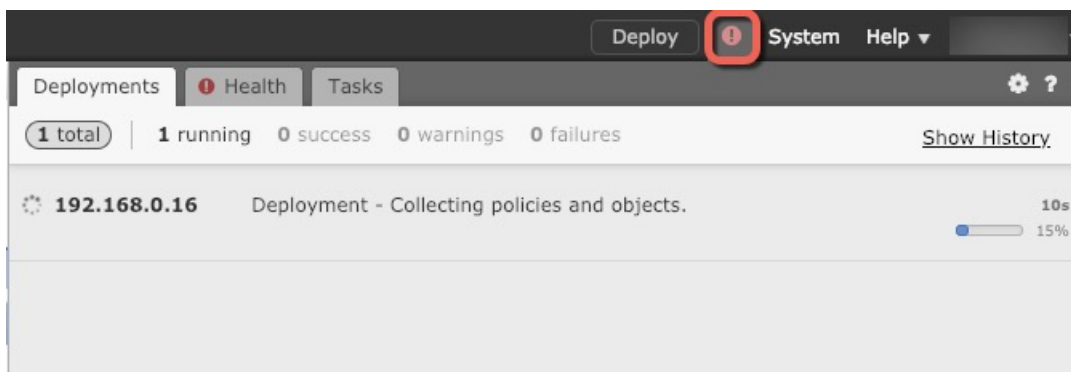
ステップ 1 右上の [展開 (Deploy)] をクリックします。



ステップ 2 [ポリシーの展開 (Deploy Policies)] ダイアログボックスでデバイスを選択し、[展開 (Deploy)] をクリックします。



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開 (Deploy)] ボタンの右側にあるアイコンをクリックします。



Firepower Threat Defense CLI へのアクセス

FTDv CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLI にアクセスするには、管理インターフェイスへの SSH を使用するか、VMware コンソールから接続します。

ステップ 1 (オプション 1) FTDv 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、仮想マシンを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して FTDv にログインします。

ステップ 2 (オプション 2) VMware コンソールを開き、初期展開時に設定したデフォルトのユーザー名「admin」アカウントとパスワードを使用してログインします。
