



Cisco Firepower Threat Defense Virtual スタートアップガイド (Google クラウドプラットフォーム向け)

初版：2020年10月19日

最終更新：2021年12月1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 Google Cloud Platform の利用開始

Firepower Threat Defense Virtual (FTDv) は、シスコの Firepower 次世代ファイアウォール機能を仮想化環境にもたらし、一貫性のあるセキュリティポリシーを実現して、物理、仮想、クラウドの各環境にわたって、またクラウド間で、ワークロードを把握します。

この章では、Google Cloud Platform (GCP) 環境内における Firepower Threat Defense Virtual の機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明します。また、この章では FTDv を管理するためのオプションについても説明します。

展開を開始する前に、管理オプションを理解しておくことが重要です。FTDv の管理と監視には Firepower Management Center を使用できます。

- [GCP への FTDv の展開について \(1 ページ\)](#)
- [FTDv と GCP の前提条件 \(3 ページ\)](#)
- [FTDv と GCP のガイドラインおよび制限事項 \(3 ページ\)](#)
- [GCP 上の FTDv のネットワークトポロジの例 \(4 ページ\)](#)

GCP への FTDv の展開について

Firepower Threat Defense Virtual (FTDv) は、物理的な Cisco FTD と同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。FTDv は、パブリック GCP に展開できます。その後設定を行うことで、時間の経過とともにロケーションを展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できます。

GCP マシンタイプのサポート

FTDv のニーズに合わせて Google 仮想マシンのタイプとサイズを選択します。現在、FTDv は、コンピューティング最適化された汎用マシンの標準タイプ、ハイメモリマシンタイプ、および高 CPU マシンタイプのいずれもサポートしています。



(注) サポートされるマシンタイプは、予告なく変更されることがあります。

表 1: サポートされるコンピューティング最適化マシンタイプ

コンピューティング最適化マシンタイプ	属性	
	vCPU	RAM (GB)
c2-standard-4	4	16 GB
c2-standard-8	8	32 GB
c2-standard-16	16	64 GB

表 2: サポートされる汎用マシンタイプ

汎用マシンタイプ	属性	
	vCPU	RAM (GB)
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-8	8	7.2
n1-highcpu-16	16	14.4
n2-highcpu-8	8	8
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- FTDv には、少なくとも 4 つのインターフェイスが必要です。
- サポートされる vCPU の最大数は 16 です。

ユーザーは、GCP でアカウントを作成し、GCP Marketplace の Cisco Firepower NGFW 仮想ファイアウォール (NGFWv) 製品を使用して VM インスタンスを起動し、GCP マシンタイプを選択します。

FTDv と GCP の前提条件

- <https://cloud.google.com> で GCP アカウントを作成します。
- GCP プロジェクトを作成します。Google ドキュメントの『[Creating Your Project](#)』を参照してください。
- Cisco スマートアカウント。Cisco Software Central (<https://software.cisco.com/>) で作成できます。
- Firepower Threat Defense Virtual へのライセンス付与。
 - 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。
 - トラフィック インターフェイス (2) : Firepower Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。
- 通信パス：
 - Firepower Threat Defense Virtual にアクセスするためのパブリック IP。
- FTDv のシステム要件については、『[Cisco Firepower Compatibility Guide](#)』を参照してください。

FTDv と GCP のガイドラインおよび制限事項

サポートされる機能

- GCP Compute Engine での展開
- インスタンスあたり最大 16 個の vCPU
- 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
- Firepower Management Center サポートのみ。

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 3: 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、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	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。



(注) vCPU/メモリの値を変更するには、最初にFTDv デバイスの電源をオフにする必要があります。

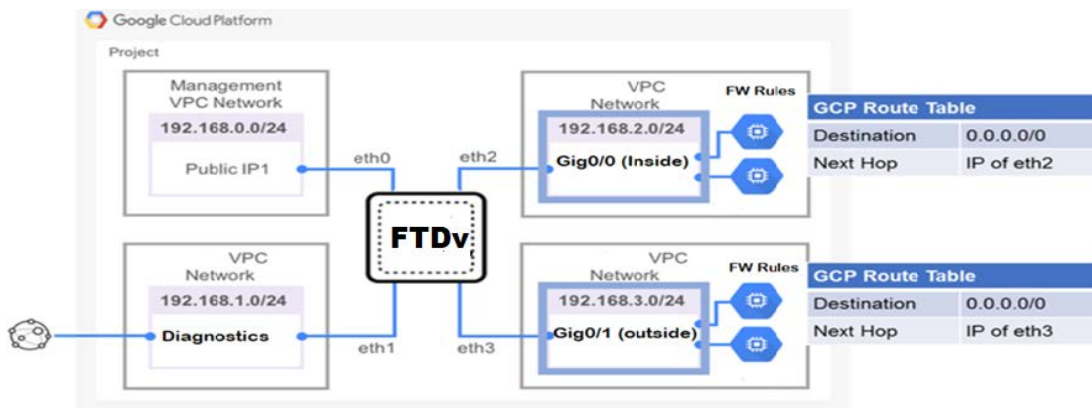
サポートされない機能

- IPv6
- FTDv ネイティブ HA
- 自動スケール
- トランスペアレント/インライン/パッシブ モード
- ジャンボ フレーム

GCP 上の FTDv のネットワークトポロジの例

次の図は、FTDv 用に4つのサブネット（管理、診断、内部、外部）がGCP内に設定されたルーテッドファイアウォールモードのFTDvの推奨トポロジを示しています。

図 1: GCP 展開での FTDv の例





第 2 章

GCP 上の Firepower Threat Defense Virtual の展開

Google Cloud Platform (GCP) 上で FTDv を展開できます。GCP は、Google が提供する可用性の高いホスト環境でアプリケーションを実行できるパブリッククラウドコンピューティングサービスです。

GCP コンソールの **[ダッシュボード (Dashboard)]** に GCP プロジェクト情報が表示されます。

- まだ選択していない場合は、**[ダッシュボード (Dashboard)]** で GCP プロジェクトを選択してください。
- ダッシュボードにアクセスするには、**[ナビゲーションメニュー (Navigation menu)]** > **[ホーム (Home)]** > **[ダッシュボード (Dashboard)]** をクリックします。

GCP コンソールにログインし、GCP Marketplace で Cisco Firepower NGFW 仮想ファイアウォール (NGFWv) 製品を検索し、FTDv インスタンスを起動します。次の手順では、GCP 環境を準備し、FTDv インスタンスを起動して FTDv を展開する方法について説明します。

- [VPC ネットワークの作成 \(7 ページ\)](#)
- [ファイアウォールルールの作成 \(8 ページ\)](#)
- [GCP 上の FTDv インスタンスの作成 \(9 ページ\)](#)

VPC ネットワークの作成

FTDv の展開には、FTDv を展開する前に 4 つのネットワークを作成する必要があります。ネットワークは次のとおりです。

- 管理サブネットの管理 VPC。
- 診断 VPC または診断サブネット。
- 内部サブネットの内部 VPC。
- 外部サブネットの外部 VPC。

さらに、FTDv を通過するトラフィックフローを許可するようにルートテーブルと GCP ファイアウォールルールを設定します。ルートテーブルとファイアウォールルールは、FTDv 自体に設定されているものとは別になっています。関連するネットワークと機能に応じて、GCP ルートテーブルとファイアウォールルールに名前を付けます。ガイドとして、[GCP 上の FTDv のネットワークトポロジの例](#) を参照してください。

手順

- ステップ 1 GCP コンソールで、[VPC ネットワーク (VPC networks)] を選択し、[VPC ネットワークの作成 (Create VPC Network)] をクリックします。
- ステップ 2 [名前 (Name)] フィールドに、特定の名前を入力します。
- ステップ 3 サブネット作成モードで、[カスタム (Custom)] をクリックします。
- ステップ 4 新しいサブネットで [名前 (Name)] フィールドに、特定の名前を入力します。
- ステップ 5 [地域 (Region)] ドロップダウンリストから、展開に適した地域を選択します。4 つのネットワークはすべて同じリージョン内にある必要があります。
- ステップ 6 [IP アドレス範囲 (IP address range)] フィールドで、最初のネットワークのサブネットを CIDR 形式 (10.10.0.0/24 など) で入力します。
- ステップ 7 その他すべての設定はデフォルトのまま、[作成 (Create)] をクリックします。
- ステップ 8 ステップ 1〜7 を繰り返して、残りの 3 つの VPC ネットワークを作成します。

ファイアウォールルールの作成

FTDv インスタンスの展開中に、管理インターフェイスのファイアウォールルールを適用します (FMC との SSH および SFTunnel 通信を許可するため)。[GCP 上の FTDv インスタンスの作成 \(9 ページ\)](#) を参照してください。要件に応じて、内部、外部、および診断インターフェイスのファイアウォールルールを作成することもできます。

手順

- ステップ 1 GCP コンソールで、[ネットワーキング (Networking)] > [VPC ネットワーク (VPC network)] > [ファイアウォール (Firewall)] を選択し、[ファイアウォールルールの作成 (Create Firewall Rule)] をクリックします。
- ステップ 2 [名前 (Name)] フィールドに、ファイアウォールルールのわかりやすい名前を入力します (例: `vpc-asiasouth-inside-fwrule`)。
- ステップ 3 [ネットワーク (Network)] ドロップダウンリストから、ファイアウォールルールを作成する VPC ネットワークの名前を選択します (例: `ftdv-south-inside`)。
- ステップ 4 [ターゲット (Targets)] ドロップダウンリストから、ファイアウォールルールに適用可能なオプションを選択します (例: [ネットワーク内のすべてのインスタンス (All instances in the network)])。

ステップ5 [送信元 IP 範囲 (Source IP Ranges)] フィールドに、送信元 IP アドレスの範囲を CIDR 形式で入力します (例: 0.0.0.0/0)。

トラフィックは、これらの IP アドレス範囲内の送信元からのみ許可されます。

ステップ6 [プロトコルとポート (Protocols and ports)] の下で、[指定されたプロトコルとポート (Specified protocols and ports)] を選択します。

ステップ7 セキュリティルールを追加します。

ステップ8 [作成 (Create)] をクリックします。

GCP 上の FTDv インスタンスの作成

以下の手順に従って、GCP マーケットプレイスから提供される Cisco Firepower NGFW 仮想ファイアウォール (NGFWv) を使用して FTDv インスタンスを展開できます。

手順

ステップ1 [GCP コンソール](#) にログインします。

ステップ2 ナビゲーションメニューの > [マーケットプレイス (Marketplace)] をクリックします。

ステップ3 マーケットプレイスで「Cisco Firepower NGFW 仮想ファイアウォール (NGFWv) (Cisco Firepower NGFW virtual firewall (NGFWv))」を検索して、製品を選択します。

ステップ4 [作成 (Launch)] をクリックします。

- a) [展開名 (Deployment name)] : インスタンスの一意の名前を指定します。
- b) [ゾーン (Zone)] : FTDv を展開するゾーンを選択します。
- c) [マシンタイプ (Machine type)] : [GCP マシンタイプのサポート \(1 ページ\)](#) に基づいて正しいマシンタイプを選択します。
- d) [SSH キー (SSH key)] (オプション) : SSH キーペアから公開キーを貼り付けます。

キーペアは、GCP が保存する公開キーと、ユーザーが保存する秘密キーファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キーペアはインスタンスへの接続に必要となるため、必ず既知の場所に保存してください。

- e) このインスタンスにアクセスするためのプロジェクト全体の SSH キーを許可するかブロックするかを選択します。Google ドキュメント『[Allowing or blocking project-wide public SSH keys from a Linux instance](#)』を参照してください。
- f) [起動スクリプト (Startup script)] : インスタンスが起動するたびに自動化されたタスクを実行するために、FTDv インスタンスの起動スクリプトを作成できます。

次に、[起動スクリプト (Startup script)] フィールドにコピーして貼り付ける day0 構成の例を示します。

```
{
  "AdminPassword": "Cisco@123123",
  "Hostname": "ftdv-gcp",
```

```
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

ヒント 実行エラーを防ぐには、JSON 検証ツールを使用して Day0 構成を検証する必要があります。

- g) **[ネットワークインターフェイス (Network interfaces)]** : 1) 管理、2) 診断、3) 内部、4) 外部のインターフェイスを設定します。
- (注) インスタンスを作成した後では、インスタンスにインターフェイスを追加できません。不適切なインターフェイス構成でインスタンスを作成した場合は、インスタンスを削除し、適切なインターフェイス構成で再作成する必要があります。
1. **[ネットワーク (Network)]** ドロップダウンリストから、**[VPC network (VPC ネットワーク)]** (*vpc-asiasouth-mgmt* など) を選択します。
 2. **[外部 IP (External IP)]** ドロップダウンリストから、適切なオプションを選択します。
管理インターフェイスには、**[外部 IP からエフェメラルへ (External IP to Ephemeral)]** を選択します。内部および外部インターフェイスでは、これはオプションです。
 3. **[完了 (Done)]** をクリックします。
- h) **[ファイアウォール (Firewall)]** : ファイアウォールルールを適用します。
- **[インターネットからの TCP ポート 22 のトラフィックを許可する (SSH アクセス) (Allow TCP port 22 traffic from the Internet (SSH access))]** チェックボックスをオンにして、SSH を許可します。
 - **[インターネットからの HTTPS のトラフィックを許可する (FMC access) (Allow HTTPS traffic from the Internet (FMC access))]** チェックボックスをオンにして、FMC および管理対象デバイスが双方向の SSL 暗号化通信チャネル (SFTunnel) を使用して通信できるようにします。
- i) **[詳細 (More)]** をクリックしてビューを展開し、**[IP 転送 (IP Forwarding)]** が **[オン (On)]** に設定されていることを確認します。

ステップ 5 **[展開 (Deploy)]** をクリックします。

- (注) 起動時間は、リソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに 7~8 分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

次のタスク

GCP コンソールの [VM インスタンス (VM instance)] ページからインスタンスの詳細を表示します。インスタンスを停止および開始するための内部 IP アドレス、外部 IP アドレス、およびコントロールが表示されます。編集する場合は、インスタンスを停止する必要があります。



第 3 章

GCP 上の Firepower Threat Defense Virtual インスタンスへのアクセス

展開中に SSH（ポート 22 経由の TCP 接続）を許可するファイアウォールルールがすでに有効化されていることを確認します。詳細については、[GCP 上の FTDv インスタンスの作成（9 ページ）](#) を参照してください。

このファイアウォールルールにより、FTDv インスタンスへのアクセスが可能になり、次の方法を使用してインスタンスに接続できます。

- 外部 IP（External IP）
 - その他の SSH クライアントまたはサードパーティ製ツール
- シリアル コンソール
- Gcloud コマンドライン

詳細については、Google ドキュメントの『[Connecting to instances](#)』を参照してください。



(注) Day0 構成を追加しない場合は、デフォルトのログイン情報（ユーザー名：**admin**、パスワード：**Admin123**）を使用して FTDv インスタンスにログインできます。最初のログイン試行時にパスワードを設定するように求められます。

- [外部 IP を使用した FTDv インスタンスへの接続（13 ページ）](#)
- [シリアルコンソールを使用した FTDv インスタンスへの接続（15 ページ）](#)
- [Gcloud を使用した FTDv インスタンスへの接続（15 ページ）](#)

外部 IP を使用した FTDv インスタンスへの接続

FTDv インスタンスには、内部 IP と外部 IP が割り当てられます。外部 IP を使用して FTDv インスタンスにアクセスできます。

手順

- ステップ 1** GCP コンソールで、[コンピューティングエンジン (Compute Engine)] > [VM インスタンス (VM instances)] を選択します。
- ステップ 2** FTDv のインスタンス名をクリックすると、[VM インスタンスの詳細 (VM instance details)] ページが開きます。
- ステップ 3** [詳細 (Details)] タブで、[SSH] フィールドのドロップダウンメニューをクリックします。
- ステップ 4** [SSH] ドロップダウンメニューから、目的のオプションを選択します。

次の方法を使用して FTDv インスタンスに接続できます。

- その他の SSH クライアントまたはサードパーティ製ツール：詳細については、Google ドキュメントの「[Connecting using third-party tools](#)」を参照してください。
-

SSH を使用した FTDv インスタンスへの接続

UNIX スタイルのシステムから FTDv インスタンスに接続するには、SSH を使用してインスタンスにログインします。

手順

- ステップ 1** 次のコマンドを使用して、ファイルの権限を設定し、自分だけがファイルを読み取れるようにします。

```
$ chmod 400 <private_key>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

- ステップ 2** インスタンスにアクセスするには、次の SSH コマンドを使用します。

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、FTDv インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。

シリアルコンソールを使用したFTDvインスタンスへの接続

手順

- ステップ 1 GCP コンソールで、[コンピューティングエンジン (Compute Engine)] > [VM インスタンス (VM instances)] を選択します。
- ステップ 2 FTDv のインスタンス名をクリックすると、[VM インスタンスの詳細 (VM instance details)] ページが開きます。
- ステップ 3 [詳細 (Details)] タブで、[シリアルコンソールへの接続 (Connect to serial console)] をクリックします。

詳細については、Google ドキュメントの「[シリアルコンソールとのやり取り](#)」を参照してください。

Gcloud を使用した FTDv インスタンスへの接続

手順

- ステップ 1 GCP コンソールで、[コンピューティングエンジン (Compute Engine)] > [VM インスタンス (VM instances)] を選択します。
- ステップ 2 FTDv のインスタンス名をクリックすると、[VM インスタンスの詳細 (VM instance details)] ページが開きます。
- ステップ 3 [詳細 (Details)] タブで、[SSH] フィールドのドロップダウンメニューをクリックします。
- ステップ 4 [gcloud コマンドを表示 (View gcloud command)] > [Cloud Shell で実行 (Run in Cloud Shell)] をクリックします。

[Cloud Shell] ターミナルウィンドウが開きます。詳細については、Google ドキュメントの「[gcloud コマンドラインツールの概要](#)」、および「[gcloud compute ssh](#)」を参照してください。



第 4 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](#) (17 ページ)
- [Firepower Management Center へのログイン](#) (18 ページ)
- [Firepower Management Center へのデバイスの登録](#) (18 ページ)
- [基本的なセキュリティポリシーの設定](#) (21 ページ)
- [Firepower Threat Defense CLI へのアクセス](#) (33 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。

手順

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。

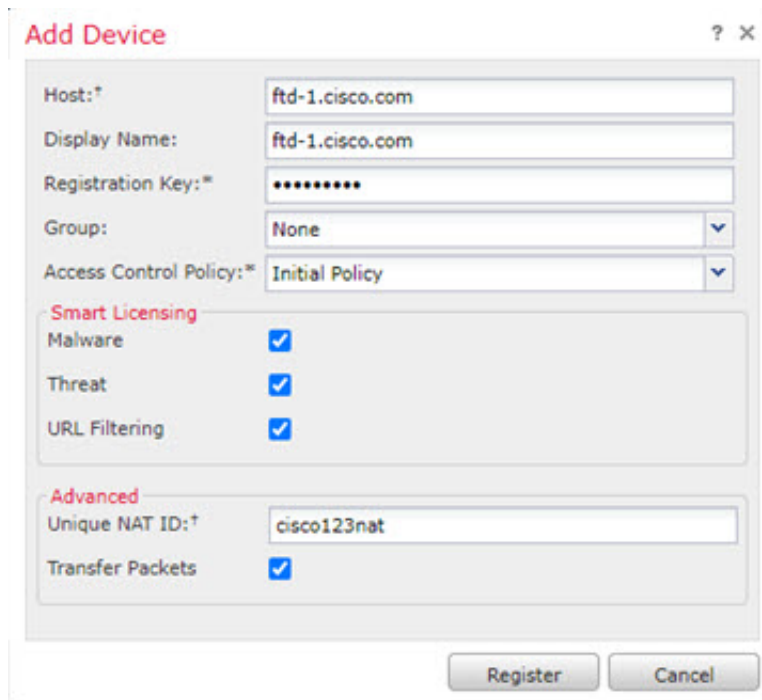


(注) この手順では、`day0/bootstrap` スクリプトを使用して、FMC の登録情報が指定されていることを前提としています。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。[FTD のコマンドリファレンス](#)を参照してください。

手順

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。



The screenshot shows the 'Add Device' dialog box with the following fields and options:

- Host: ftd-1.cisco.com
- Display Name: ftd-1.cisco.com
- Registration Key: *****
- Group: None
- Access Control Policy: Initial Policy
- Smart Licensing:
 - Malware:
 - Threat:
 - URL Filtering:
- Advanced:
 - Unique NAT ID: cisco123nat
 - Transfer Packets:

Buttons: Register, Cancel

- [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 \(31 ページ\)](#)」を参照してください。

- [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す。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 \(33 ページ\)](#)」) 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。

手順

-
- ステップ 1 [インターフェイスの設定 \(21 ページ\)](#)
 - ステップ 2 [DHCP サーバーの設定 \(25 ページ\)](#)
 - ステップ 3 [デフォルトルートの追加 \(26 ページ\)](#)
 - ステップ 4 [NAT の設定 \(28 ページ\)](#)
 - ステップ 5 [アクセス制御の設定 \(31 ページ\)](#)
 - ステップ 6 [設定の展開 \(32 ページ\)](#)
-

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。

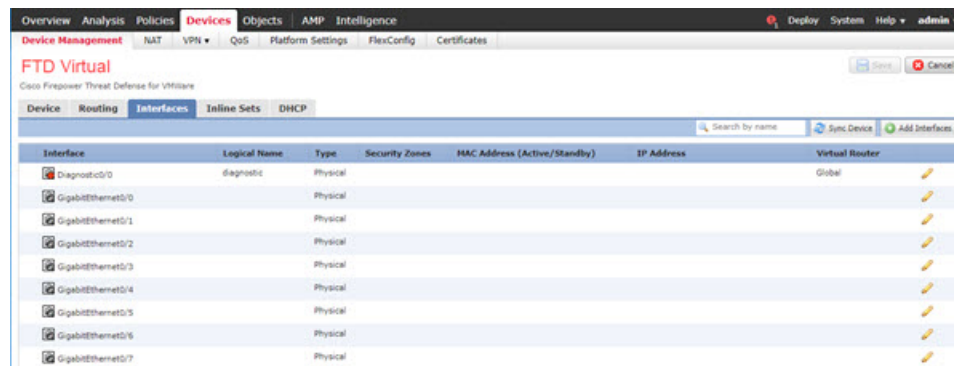
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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。

手順

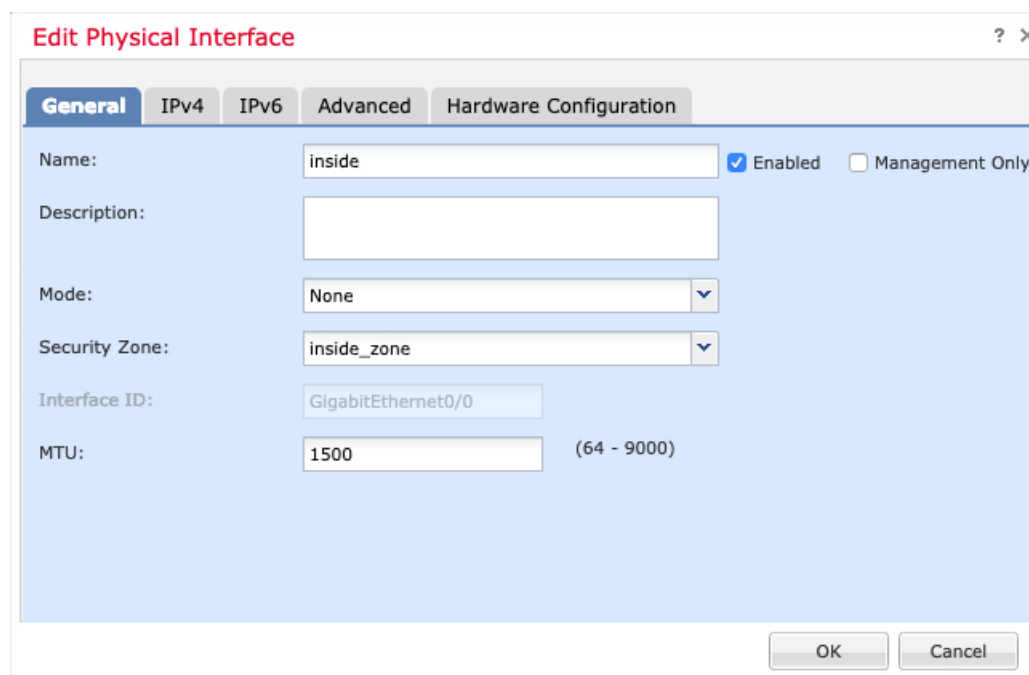
ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスをクリックします。

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。



- 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。

- 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。

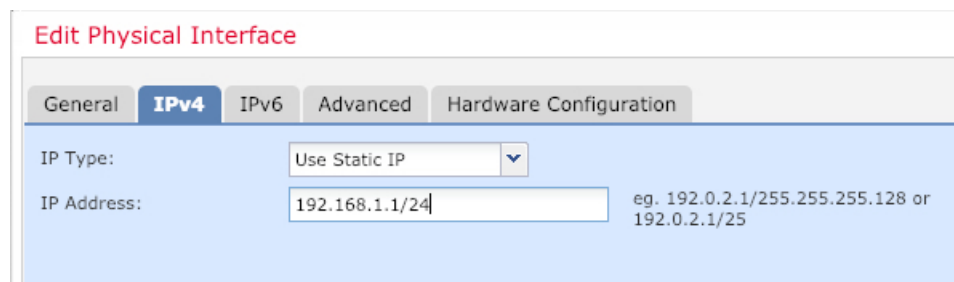
たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできませんが、外部から内部に向けて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

- 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] : 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。



The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is active. The 'IP Type' dropdown menu is set to 'Use Static IP'. The 'IP Address' field contains the text '192.168.1.1/24'. To the right of the IP address field, there is a small text example: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'. The window has tabs for 'General', 'IPv4', 'IPv6', 'Advanced', and 'Hardware Configuration'.

- [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 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: Enabled Management Only

Description:

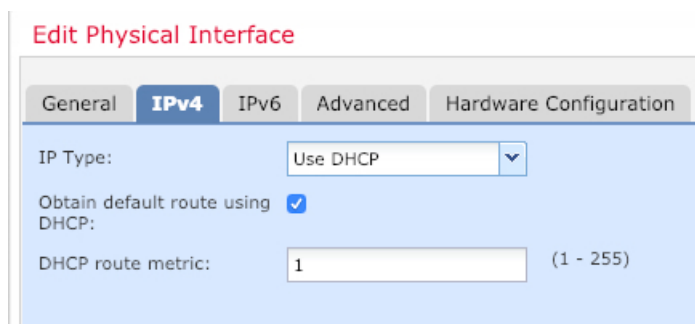
Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

- 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 (Security Zone)] 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。



Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use DHCP

Obtain default route using DHCP:

DHCP route metric: 1 (1 - 255)

- [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。

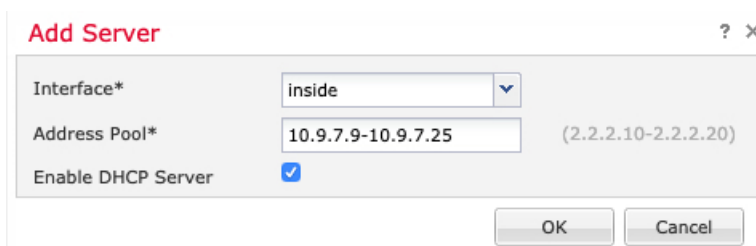
クライアントでDHCPを使用してFTDvからIPアドレスを取得するようにする場合は、DHCPサーバーを有効にします。

手順

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。



Add Server ? X

Interface* inside

Address Pool* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

- [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り、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。

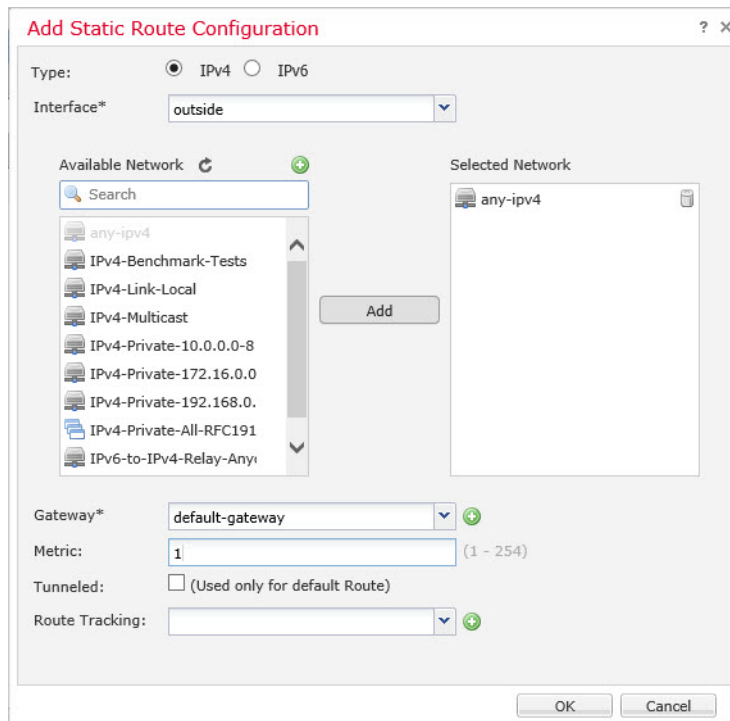
デフォルトルートの追加

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。

手順

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。



- [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。

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

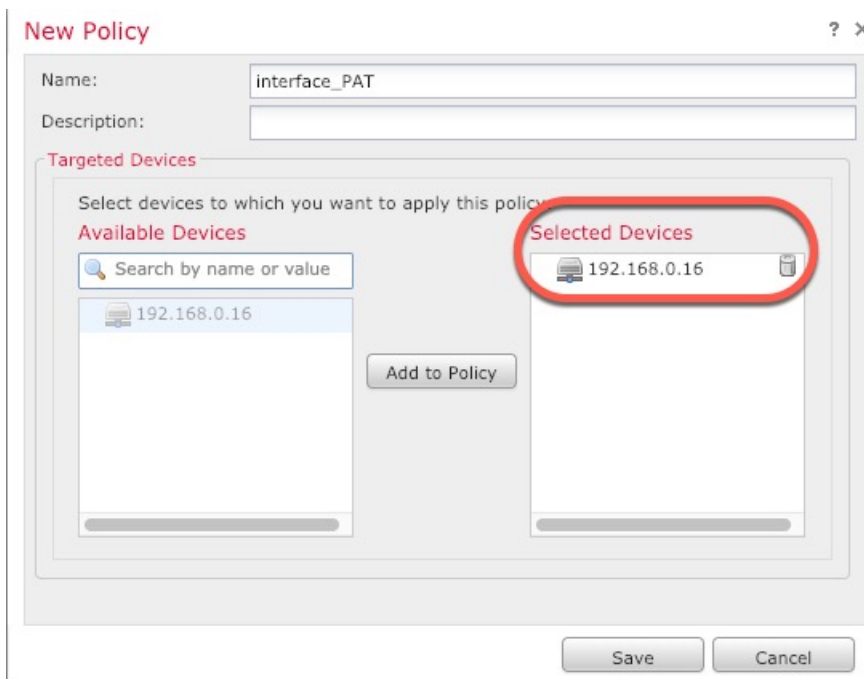
ステップ 4 [保存 (Save)] をクリックします。

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。

手順

- 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。

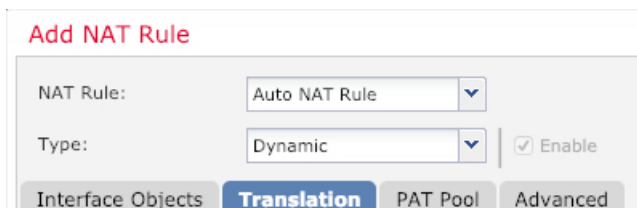


ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ 3 [ルールの追加 (Add Rule)] をクリックします。

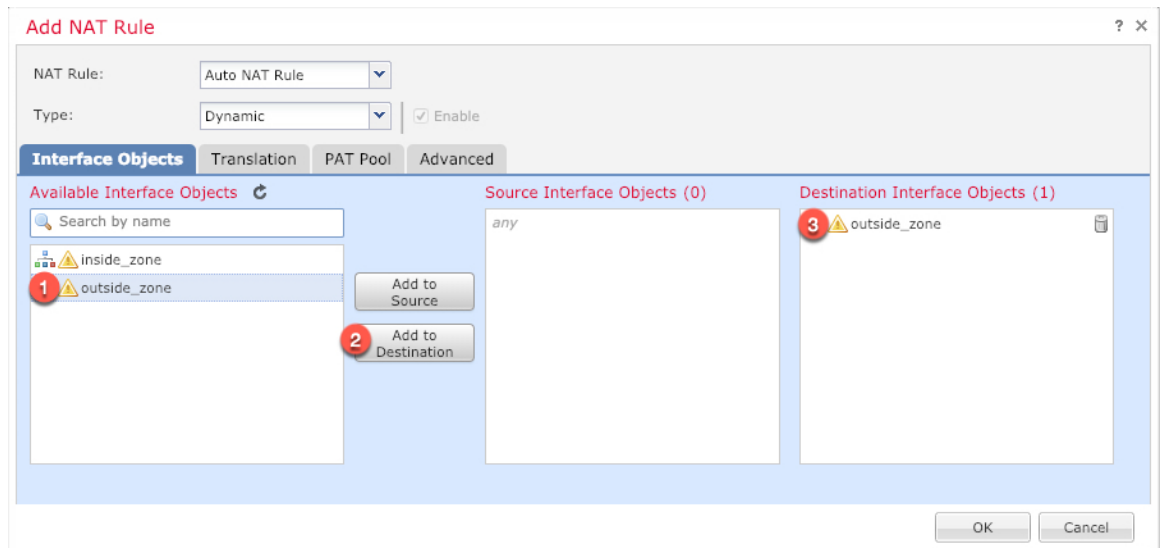
[NATルールの追加 (Add NAT Rule)] ダイアログボックスが表示されます。

ステップ 4 基本ルールのオプションを設定します。

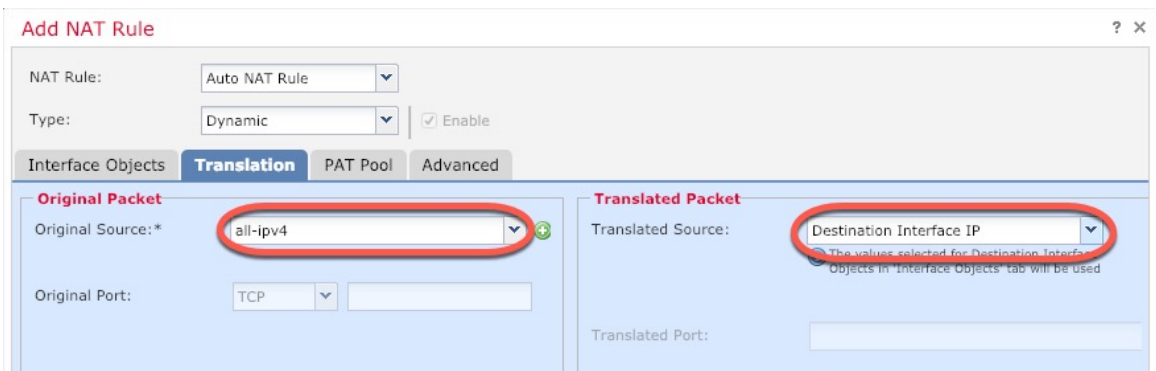


- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

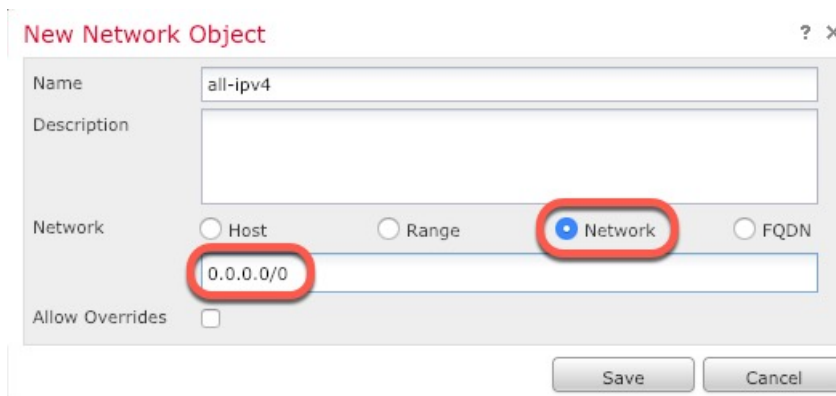
ステップ 5 [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。



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。

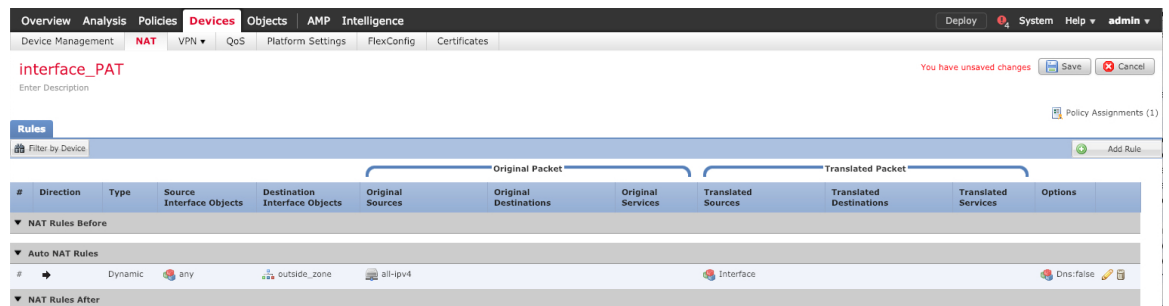


- (注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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。



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

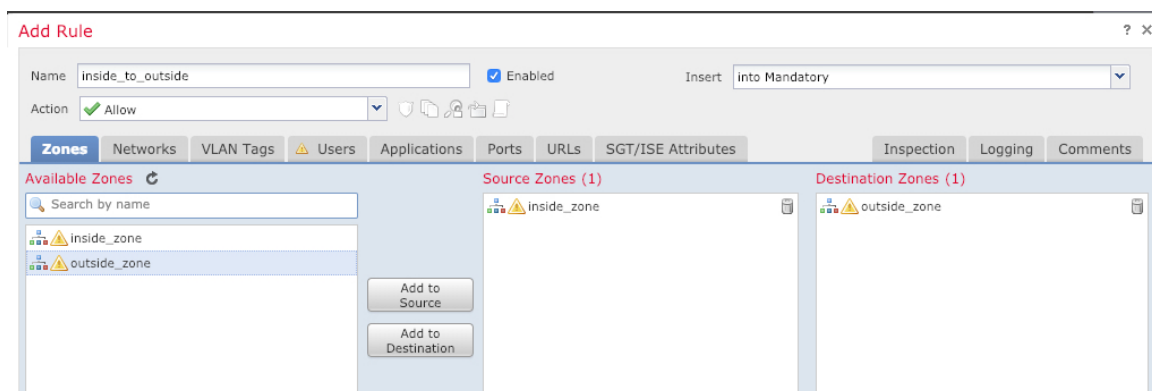
FTDv を FMC に登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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。

手順

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。

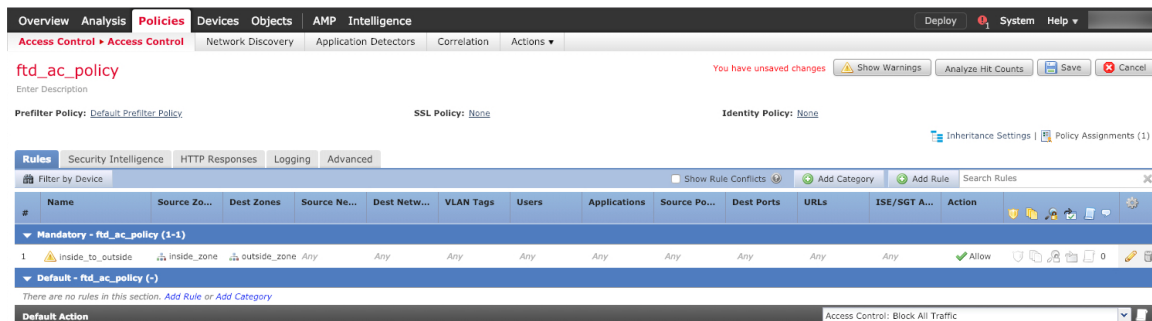


- [名前 (Name)] : このルールに名前を付けます (たとえば、 **inside_to_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

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。



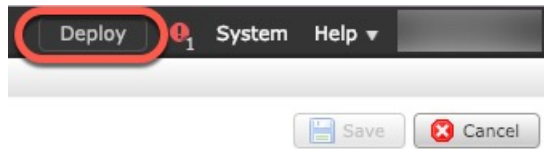
ステップ 4 [保存 (Save)] をクリックします。

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。

手順

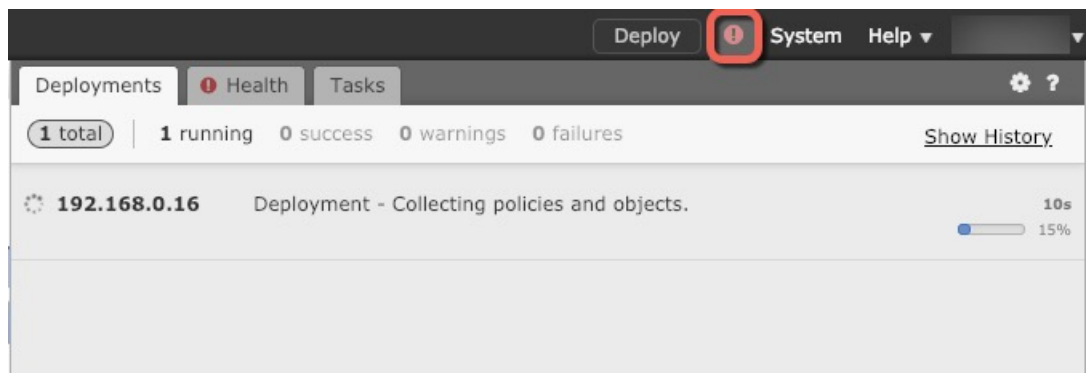
ステップ 1 右上の [展開 (Deploy)] をクリックします。



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。

手順

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。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2021 Cisco Systems, Inc. All rights reserved.

