



Cisco Firepower Threat Defense Virtual スタートアップガイド (AWS クラウド向け)

初版：2018年7月31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 AWS の 利用開始

Amazon Virtual Private Cloud (VPC) は、お客様が定義する仮想ネットワークで Amazon Web Services (AWS) のリソースを起動できるようにします。この仮想ネットワークは、お客様自身のデータセンターで運用されている可能性がある従来型のネットワークとよく似ているだけでなく、AWS のスケーラブルなインフラストラクチャを活用するというメリットがあります。

このドキュメントでは、AWS に Firepower Threat Defense Virtual を展開する方法について説明します。

- [FTDv および AWS クラウドについて \(1 ページ\)](#)
- [エンドツーエンドの手順 \(4 ページ\)](#)
- [Firepower デバイスの管理方法 \(5 ページ\)](#)
- [AWS ソリューションの概要 \(6 ページ\)](#)
- [Firepower Threat Defense Virtual の前提条件 \(7 ページ\)](#)
- [FTDv および AWS のガイドラインと制限事項 \(8 ページ\)](#)
- [AWS 環境の設定 \(10 ページ\)](#)

FTDv および AWS クラウドについて

AWS はパブリッククラウド環境です。Firepower Threat Defense Virtual は、次のインスタンスタイプの AWS 環境でゲストとして実行されます。



- (注) 次の表に示すように、FTD バージョン 6.6.0 では C5 インスタンスタイプのサポートが追加されています。インスタンスが大きくなるほど、AWS VM により多くの CPU リソースが提供され、パフォーマンスが向上し、さらに多くのネットワークインターフェイスが実現します。
-

表 1: FTDv の AWS サポートインスタンス

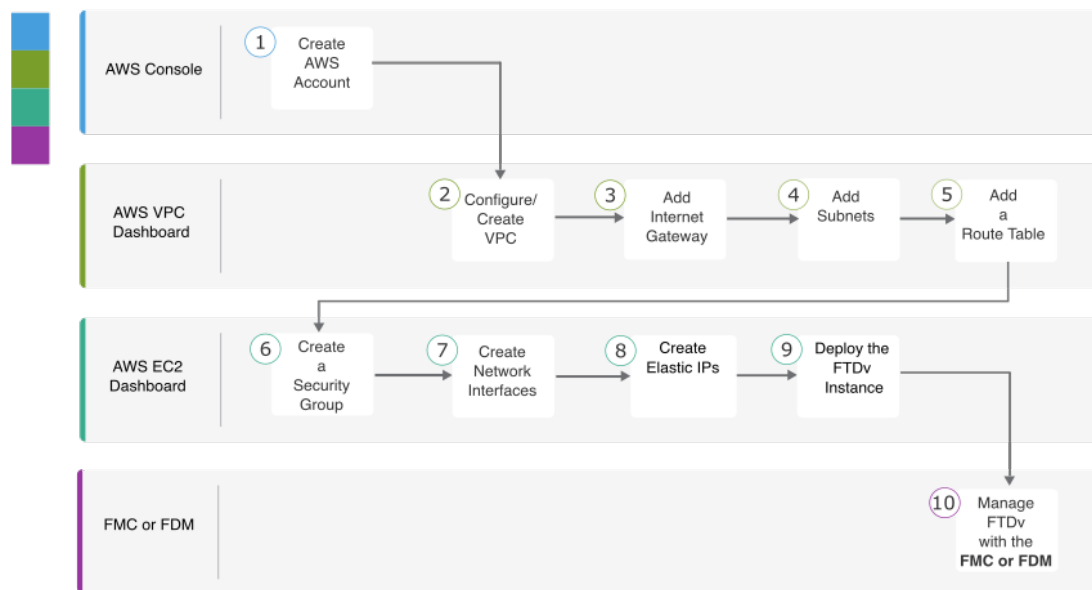
インスタンス タイプ	vCPU	メモリ (RAM)	vNIC
C5.xlarge	4	8 GB	4
C 5.2 xlarge	8	16 GB	4
C5.4xlarge	16	32 GB	8
C4.xlarge	4	7.5 GB	4
C3.xlarge	4	7.5 GB	4
c5a.xlarge	4	8	4
c5a.2xlarge	8	16	4
c5a.4xlarge	16	32	8
c5ad.xlarge	4	8	4
c5ad.2xlarge	8	16	4
c5ad.4xlarge	16	32	8
c5d.xlarge	4	8	4
c5d.2xlarge	8	16	4
c5d.4xlarge	16	32	8
i3en.xlarge	4	32	4
i3en.2xlarge	8	64	4
i3en.3xlarge	12	96	4
inf1.xlarge	4	8	4
inf1.2xlarge	8	16	4
m5.xlarge	4	16	4
m5.2xlarge	8	32	4
m5.4xlarge	16	64	8
m5a.xlarge	4	16	4
m5a.2xlarge	8	32	4
m5a.4xlarge	16	64	8
m5ad.xlarge	4	16	4
m5ad.2xlarge	8	32	4

インスタンス タイプ	vCPU	メモリ (RAM)	vNIC
m5ad.4xlarge	16	64	8
m5d.xlarge	4	16	4
m5d.2xlarge	8	32	4
m5d.4xlarge	16	64	8
m5dn.xlarge	4	16	4
m5dn.2xlarge	8	32	4
m5dn.4xlarge	16	64	8
m5n.xlarge	4	16	4
m5n.2xlarge	8	32	4
m5n.4xlarge	16	64	8
m5zn.xlarge	4	16	4
m5zn.2xlarge	8	32	4
m5zn.3xlarge	12	48	8
r5.xlarge	4	32	4
r5.2xlarge	8	64	4
r5.4xlarge	16	128	8
r5a.xlarge	4	32	4
r5a.2xlarge	8	64	4
r5a.4xlarge	16	128	8
r5ad.xlarge	4	32	4
r5ad.2xlarge	8	64	4
r5ad.4xlarge	16	128	8
r5b.xlarge	4	32	4
r5b.2xlarge	8	64	4
r5b.4xlarge	16	128	8
r5d.xlarge	4	32	4
r5d.2xlarge	8	64	4
r5d.4xlarge	16	128	8

インスタンス タイプ	vCPU	メモリ (RAM)	vNIC
r5dn.xlarge	4	32	4
r5dn.2xlarge	8	64	4
r5dn.4xlarge	16	128	8
r5n.xlarge	4	32	4
r5n.2xlarge	8	64	4
r5n.4xlarge	16	128	8
z1d.xlarge	4	32	4
z1d.2xlarge	8	64	4
z1d.3xlarge	12	96	8

エンドツーエンドの手順

次のフローチャートは、Amazon Web Services (AWS) に FTDv を展開するためのワークフローを示しています。



	ワークスペース	手順
①	AWS コンソール	www.amazon.com : AWS コンソールでユーザーアカウントを作成します。

	ワークスペース	手順
②	AWS VPC ダッシュボード	VPC の設定/作成 : AWS アカウント専用の VPC を作成および設定します。
③	AWS VPC ダッシュボード	インターネットゲートウェイの追加 : VPC をインターネットに接続するために、インターネットゲートウェイを追加します。
④	AWS VPC ダッシュボード	サブネットの追加 : VPC にサブネットを追加します。
⑤	AWS VPC ダッシュボード	ルートテーブルの追加 : VPC 用に設定したゲートウェイにルートテーブルを接続します。
⑥	AWS EC2 ダッシュボード	セキュリティグループの作成 : 許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティグループを作成します。
⑦	AWS EC2 ダッシュボード	ネットワークインターフェースの作成 : 静的 IP アドレスを使用して、FTDv のネットワーク インターフェースを作成します。
⑧	AWS EC2 ダッシュボード	Elastic IP の作成 : Elastic IP は、Firepower Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。
⑨	AWS EC2 ダッシュボード	FTDv インスタンスの展開 : AWS ポータルから Firepower Threat Defense Virtual を展開します。
⑩	FMC または FDM	FTDv の管理 : <ul style="list-style-type: none"> • Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 • Firepower Device Manager Center を使用した Firepower Threat Defense Virtual の管理

Firepower デバイスの管理方法

Firepower Threat Defense デバイスの管理には次の 2 つのオプションを選択できます。

Firepower Device Manager

Firepower Device Manager (FDM) オンボード統合マネージャ。

FDM は、一部の Firepower Threat Defense デバイスに組み込まれている Web ベースの設定インターフェイスです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。



(注) FDM をサポートしている Firepower Threat Defense デバイスのリストについては、『[Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#)』を参照してください。

Firepower Management Center

Cisco Firepower Management Center (FMC)。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの FDM の代わりに FMC を使用してデバイスを設定します。



重要 FDM と FMC の両方を使用して Firepower デバイスを管理することはできません。いったん FDM の統合管理を有効にすると、ローカル管理を無効にして、FMC を使用するように管理を再設定しない限り、FMC を使用して Firepower デバイスを管理することはできなくなります。一方、Firepower を FMC に登録すると、FDM のオンボード管理サービスは無効になります。



注意 現在、シスコには FDM Firepower 設定を FMC に移行するオプションはありません。その逆も同様です。Firepower デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

AWS ソリューションの概要

AWS は、Amazon.com によって提供されるリモート コンピューティング サービスの集合で、Web サービスとも呼ばれており、クラウド コンピューティング プラットフォームを構成します。これらのサービスは、世界の 11 の地理的地域で運用されます。通常、Firepower Management Center Virtual および Firepower Threat Defense Virtual を展開する際には、以下の AWS サービスに精通している必要があります。

- Amazon Elastic Compute Cloud (EC2) : 仮想コンピュータをレンタルして、お客様独自のアプリケーションおよびサービス (ファイアウォールなど) を Amazon のデータセンターで起動および管理できるようにする Web サービス。

- Amazon Virtual Private Cloud (VPC) : Amazon パブリック クラウド内の隔離されたプライベート ネットワークを設定できるようにする Web サービス。EC2 インスタンスは VPC 内で実行されます。
- Amazon Simple Storage Service (S3) : データ ストレージ インフラストラクチャを提供する Web サービス。

AWS でアカウントを作成し、VPC および EC2 コンポーネントを (AWS ウィザードまたは手動設定のいずれかを使用して) 設定し、Amazon Machine Image (AMI) インスタンスを選択します。AMI は、インスタンスを起動するために必要なソフトウェア構成を含むテンプレートです。



(注) AMI イメージは AWS 環境の外部ではダウンロードできません。

Firepower Threat Defense Virtual の前提条件

- Amazon アカウント。 <http://aws.amazon.com/> で 1 つ作成できます。
- FTDv コンソールにアクセスするには、SSH クライアント (Windows 場合の PuTTY、Macintosh の場合はターミナルなど) が必要です。
- Cisco スマートアカウント。Cisco Software Central で 1 つ作成できます。
<https://software.cisco.com/>
- 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。
- Firepower Threat Defense Virtual 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。

6.7 以降では、必要に応じて、管理インターフェイスの代わりにデータインターフェイスを FMC の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスからの FMC アクセスは、ハイアベイラビリティ展開ではサポートされません。FMC アクセスに対するデータインターフェイスの設定に関する詳細については、『[FTD command reference](#)』の `configure network management-data-interface` コマンドを参照してください。

- 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 または Elastic IP。

FTDv および AWS のガイドラインと制限事項

サポートされる機能

- 仮想プライベート クラウド (VPC) への導入
- 拡張ネットワーク (SR-IOV) (使用可能な場合)
- Amazon マーケットプレイスからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザー導入
- ルーテッドモード (デフォルト)
- ERSPAN を使用するパッシブモード

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 2: 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/34 GB	16 Gbps	10,000

- シスコ スマート ライセンス アカウントを使用する BYOL (Bring Your Own License) 。

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。

Firepower Threat Defense Virtual の制限事項

- 推奨されるインスタンスは c4.xlarge です。c3.xlarge インスタンスでは AWS リージョンでの可用性が制限されます。
- 起動時には、2つの管理インターフェイスが構成されている必要があります。
- 起動するには、2つのトラフィック インターフェイスと2つの管理インターフェイス（合計4つのインターフェイス）が必要です。



(注) Firepower Threat Defense Virtual は、4つのインターフェイスがないと起動しません。

- AWS でトラフィック インターフェイスを設定する場合、[送信元/宛先の変更の確認 (Change Source/Dest. Check)] オプションを無効にする必要があります。
- IP アドレス設定は (CLI から設定したものでも Firepower Management Center から設定したものでも) AWS コンソールで作成されたものと一致する必要があります。展開時に設定を書き留めてください。
- Firepower Threat Defense Virtual を登録した後、インターフェイスを編集し、Firepower Management Center で有効にする必要があります。IP アドレスは、AWS で設定されたインターフェイスと一致している必要があることに注意してください。
- IPv6 は現時点でサポートされていません。
- トランスペアレント モード、インライン モード、パッシブ モードは現時点でサポートされていません。
- インターフェイスを変更する場合、以下のようにして、AWS コンソールから変更を行う必要があります。
 - Firepower Management Center から登録を解除します。
 - AWS AMI ユーザー インターフェイス経由でインスタンスを停止します。
 - AWS AMI ユーザー インターフェイス経由で、変更するインターフェイスを切り離します。
 - 新しいインターフェイスを接続します (2つのトラフィック インターフェイスと2つの管理インターフェイスを起動する必要があることを念頭に置いてください)。
 - AWS AMI ユーザー インターフェイス経由でインスタンスを開始します。
 - Firepower Management Center に再登録します。

- Firepower Management Center から、デバイス インターフェイスを編集し、AWS コンソールから行った変更と一致するように、IP アドレスおよび他のパラメータを変更します。
- ブート後にインターフェイスを追加することはできません。
- 複製/スナップショットは現時点でサポートされていません。

AWS 環境の設定

Firepower Threat Defense Virtual を AWS に展開するには、展開に固有の要件および設定を使用して Amazon VPC を設定する必要があります。ほとんどの環境では、セットアップ ウィザードに従ってセットアップを実行できます。AWS では、概要から詳細機能に至るまで、サービスに関する有用な情報を扱ったオンラインドキュメントを提供しています。詳細については、<https://aws.amazon.com/documentation/gettingstarted/> を参照してください。

AWS のセットアップを適切に制御するために、続くセクションでは、Firepower Threat Defense Virtual インスタンスの起動前の VPC および EC2 構成について説明します。

- [VPC の作成 \(10 ページ\)](#)
- [インターネット ゲートウェイの追加 \(11 ページ\)](#)
- [サブネットの追加 \(12 ページ\)](#)
- [ルート テーブルの追加 \(13 ページ\)](#)
- [セキュリティ グループの作成 \(13 ページ\)](#)
- [ネットワーク インターフェイスの作成 \(14 ページ\)](#)
- [Elastic IP の作成 \(15 ページ\)](#)

はじめる前に

- AWS アカウントを作成します。
- AMI が Firepower Threat Defense Virtual のインスタンスに使用できることを確認します。

VPC の作成

仮想プライベート クラウド (VPC) は、AWS アカウント専用の仮想ネットワークです。これは、AWS クラウド内の他の仮想ネットワークから論理的に分離されています。Firepower Management Center Virtual インスタンスや Firepower Threat Defense Virtual インスタンスなどの AWS リソースを VPC で起動できます。VPC を設定できます。さらに、その IP アドレス範囲を選択し、サブネットを作成し、ルートテーブル、ネットワーク ゲートウェイ、およびセキュリティ設定を作成できます。

手順

ステップ 1 <http://aws.amazon.com/> にログインし、地域を選択します。

AWS は互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

ステップ 2 [サービス (Services)] > [VPC] の順にクリックします。

ステップ 3 [VPCダッシュボード (VPC Dashboard)] > [使用するVPC (Your VPCs)] の順にクリックします。

ステップ 4 [VPCの作成 (Create VPC)] をクリックします。

ステップ 5 [VPCの作成 (Create VPC)] ダイアログボックスで、次のものを入力します。

- VPC を識別するユーザー定義の [名前タグ (Name tag)]。
- IP アドレスの [CIDRブロック (CIDR block)]。CIDR (クラスレス ドメイン間ルーティング) の表記法は、IP アドレスとそれに関連付けられているルーティングプレフィックスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。
- [デフォルト (Default)] の [テナント (Tenancy)] 設定。この VPC で起動されたインスタンスが、起動時に指定されたテナント属性を使用するようにします。

ステップ 6 [はい、作成します (Yes, Create)] をクリックして、VPC を作成します。

次のタスク

次のセクションで説明されているように、VPC にインターネットゲートウェイを追加します。

インターネットゲートウェイの追加

VPC をインターネットに接続するために、インターネットゲートウェイを追加できます。VPC の外部の IP アドレスのトラフィックをインターネットゲートウェイにルーティングできます。

はじめる前に

- Firepower Threat Defense Virtual インスタンスの VPC を作成します。

手順

ステップ 1 [サービス (Services)] > [VPC] の順にクリックします。

ステップ 2 [VPCダッシュボード (VPC Dashboard)] > [インターネットゲートウェイ (Internet Gateway)] の順にクリックしてから、[インターネットゲートウェイの作成 (Create Internet Gateway)] をクリックします。

ステップ 3 ユーザー定義の [名前タグ (Name tag)] を入力してゲートウェイを特定し、[はい、作成します (Yes, Create)] をクリックしてゲートウェイを作成します。

ステップ 4 前のステップで作成したゲートウェイを選択します。

ステップ 5 [VPCに接続 (Attach to VPC)] をクリックして、以前に作成した VPC を選択します。

ステップ 6 [はい、接続します (Yes, Attach)] をクリックして、ゲートウェイを VPC に追加します。

デフォルトでは、ゲートウェイが作成されて VPC に接続されるまで、VPC で起動されたインスタンスはインターネットと通信できません。

次のタスク

次のセクションで説明されているように、VPC にサブネットを追加します。

サブネットの追加

Firepower Threat Defense Virtual インスタンスが接続できる VPC の IP アドレス範囲をセグメント化することができます。セキュリティおよび運用のニーズに応じて、インスタンスをグループ化するためのサブネットを作成できます。Firepower Threat Defense Virtual の場合、管理用のサブネットとトラフィック用のサブネットを作成する必要があります。

はじめる前に

- Firepower Threat Defense Virtual インスタンスの VPC を作成します。

手順

ステップ 1 [サービス (Services)] > [VPC] の順にクリックします。

ステップ 2 [VPCダッシュボード (VPC Dashboard)] > [サブネット (Subnets)] の順にクリックして、[サブネットの作成 (Create Subnet)] をクリックします。

ステップ 3 [サブネットの作成 (Create Subnet)] ダイアログボックスで、次のものを入力します。

- サブネットを識別するユーザー定義の [名前タグ (Name tag)]。
- このサブネットに使用する [VPC]。
- このサブネットが存在する [可用性ゾーン (Availability Zone)]。[設定なし (No Preference)] を選択して、Amazon が選択するゾーンを選びます。
- IP アドレスの [CIDRブロック (CIDR block)]。サブネットの IP アドレスの範囲は、VPC の IP アドレス範囲のサブセットである必要があります。ブロック サイズは、/16 ネットワーク マスクから /28 ネットワーク マスクの範囲で指定する必要があります。サブネットのサイズは VPC のサイズと同じにすることができます。

ステップ 4 [はい、作成します (Yes, Create)] をクリックして、サブネットを作成します。

ステップ 5 必要な数のサブネットについて、手順を繰り返します。管理トラフィックには別のサブネットを作成し、データ トラフィックに必要な数のサブネットを作成します。

次のタスク

次のセクションで説明されているように、VPC にルート テーブルを追加します。

ルート テーブルの追加

VPC 用に設定したゲートウェイにルート テーブルを接続できます。また、複数のサブネットを1つのルート テーブルに関連付けることができます。しかし、1つのサブネットは一度に1つのルート テーブルにしか関連付けることができません。

手順

- ステップ 1 [サービス (Services)] > [VPC] の順にクリックします。
- ステップ 2 [VPCダッシュボード (VPC Dashboard)] > [ルートテーブル (Route Tables)] の順にクリックしてから、[ルートテーブルの作成 (Create Route Table)] をクリックします。
- ステップ 3 ルート テーブルを識別するユーザー定義の [名前タグ (Name tag)] を入力します。
- ステップ 4 このルート テーブルを使用する [VPC] をドロップダウン リストから選択します。
- ステップ 5 [はい、作成します (Yes, Create)] をクリックして、ルート テーブルを作成します。
- ステップ 6 作成したルート テーブルを選択します。
- ステップ 7 [ルート (Routes)] タブをクリックして、詳細ペインにルート情報を表示します。
- ステップ 8 [編集 (Edit)] をクリックして、[別のルートを追加 (Add another route)] をクリックします。
 - a) [宛先 (Destination)] 列に、0.0.0.0/0 を入力します。
 - b) [ターゲット (Target)] 列で、ゲートウェイを選択します。
- ステップ 9 [保存 (Save)] をクリックします。

次のタスク

次のセクションで説明するように、セキュリティ グループを作成します。

セキュリティ グループの作成

許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティ グループを作成できます。各インスタンスに割り当てることができる、さまざまな異なるルールを使用して、複数のセキュリティ グループを作成できます。

手順

- ステップ 1 [サービス (Services)] > [EC2] の順にクリックします。
- ステップ 2 [EC2ダッシュボード (EC2 Dashboard)] > [セキュリティグループ (Security Groups)] の順にクリックします。

- ステップ 3** [セキュリティグループの作成 (Create Security Group)] をクリックします。
- ステップ 4** [セキュリティグループの作成 (Create Security Group)] ダイアログボックスで、次の内容を入力します。
- セキュリティグループを識別するユーザー定義の [セキュリティグループ名 (Security group name)]。
 - このセキュリティグループの [説明 (Description)]。
 - このセキュリティグループに関連付けられた VPC。
- ステップ 5** [セキュリティグループルール (Security group rules)] を設定します。
- [インバウンド (Inbound)] タブをクリックして、[ルールの追加 (Add Rule)] をクリックします。

(注) Firepower Management Center Virtual を AWS の外部から管理するには、HTTPS および SSH アクセスが必要です。それに基づいて、送信元 IP アドレスを指定する必要があります。また、Firepower Management Center Virtual と Firepower Threat Defense Virtual の両方を AWS VPC 内で設定している場合、プライベート IP 管理サブネットアクセスを許可する必要があります。
 - [アウトバウンド (Outbound)] タブをクリックしてから、[ルールの追加 (Add Rule)] をクリックして、アウトバウンドトラフィックのルールを追加するか、デフォルトの [すべてのトラフィック (All traffic)] ([タイプ (Type)] の場合) および [任意の宛先 (Anywhere)] ([宛先 (Destination)] の場合) のままにします。
- ステップ 6** セキュリティグループを作成するには、[作成 (Create)] をクリックします。

次のタスク

次のセクションで説明されているように、ネットワーク インターフェイスを作成します。

ネットワーク インターフェイスの作成

静的 IP アドレスを使用して、Firepower Threat Defense Virtual のネットワーク インターフェイスを作成できます。具体的な展開の必要に応じてネットワーク インターフェイス (内部および外部) を作成します。

手順

- ステップ 1** [サービス (Services)] > [EC2] の順にクリックします。
- ステップ 2** [EC2ダッシュボード (EC2 Dashboard)] > [ネットワークインターフェイス (Network Interfaces)] の順にクリックします。
- ステップ 3** [ネットワークインターフェイスの作成 (Create Network Interface)] をクリックします。
- ステップ 4** [ネットワークインターフェイスの作成 (Create Network Interface)] ダイアログボックスで、次のものを入力します。

- a) ネットワークインターフェイスに関するオプションのユーザー定義の[説明 (Description)]。
- b) ドロップダウンリストから[サブネット (Subnet)]を選択します。Firepower Threat Defense Virtual インスタンスを作成する VPC のサブネットが選択されていることを確認します。
- c) [プライベートIP (Private IP)]アドレスを入力します。自動割り当てではなく、スタティック IP アドレスを使用することが推奨されています。
- d) [セキュリティグループ (Security groups)]を1つ以上選択します。セキュリティグループの必要なポートがすべて開いていることを確認します。

ステップ 5 [はい、作成します (Yes, Create)] をクリックして、ネットワーク インターフェイスを作成します。

ステップ 6 作成したネットワーク インターフェイスを選択します。

ステップ 7 右クリックして、[送信元/宛先の変更の確認 (Change Source/Dest. Check)]を選択します。

ステップ 8 [編集 (Edit)] をクリックして、[別のルートを追加 (Add another route)] をクリックします。

ステップ 9 [無効 (Disable)] を選択します。作成したすべてのネットワーク インターフェイスについて、この操作を繰り返します。

次のタスク

次のセクションで説明するように、Elastic IP アドレスを作成します。

Elastic IP の作成

インスタンスが作成されると、パブリック IP アドレスはそのインスタンスに関連付けられません。インスタンスを停止してから開始すると、そのパブリック IP アドレスは自動的に変更されます。この問題を解決するには、Elastic IP アドレッシングを使用して、永続的なパブリック IP アドレスをそのインスタンスに割り当てます。Elastic IP は、Firepower Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。



(注) 少なくとも、Firepower Threat Defense Virtual 管理インターフェイス用と診断インターフェイス用の Elastic IP アドレスを作成してください。

手順

ステップ 1 [サービス (Services)] > [EC2] の順にクリックします。

ステップ 2 [EC2ダッシュボード (EC2 Dashboard)] > [Elastic IP (Elastic IPs)] の順にクリックします。

ステップ 3 [新規アドレスの割り当て (Allocate New Address)] をクリックします。

ステップ 4 必要な数の Elastic IP およびパブリック IP について、この手順を繰り返します。

ステップ 5 [はい、割り当てます (Yes, Allocate)] をクリックして、Elastic IP を作成します。

ステップ 6 展開に必要な数の Elastic IP について、この手順を繰り返します。

次のタスク

次のセクションの説明に従い、Firepower Threat Defense Virtual を展開します。



第 2 章

Firepower Threat Defense Virtual の展開

この章では、AWS ポータルから Firepower Threat Defense Virtual を展開する方法について説明します。

- [Firepower Threat Defense Virtual インスタンスの展開 \(17 ページ\)](#)

Firepower Threat Defense Virtual インスタンスの展開

始める前に

次のことを推奨します。

- [AWS 環境の設定 \(10 ページ\)](#) の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Firepower Threat Defense Virtual のインスタンスに使用できることを確認します。

手順

- ステップ 1** <https://aws.amazon.com/marketplace> (Amazon マーケットプレイス) に移動してサインインします。
- ステップ 2** Amazon マーケットプレイスにログイン後、Firepower Threat Defense Virtual (Cisco Firepower NGFW Virtual (NGFWv) : BYOL) 用に提供されているリンクをクリックします。
(注) すでに AWS を使用していた場合、リンクを有効にするには、いったんサインアウトしてから、サインインし直す必要があります。
- ステップ 3** [続行 (Continue)] をクリックしてから、[手動起動 (Manual Launch)] タブをクリックします。
- ステップ 4** [条件に同意する (Accept Terms)] をクリックします。
- ステップ 5** [EC2コンソールを使用して起動する (Launch with EC2 Console)] をクリックします。
- ステップ 6** Firepower Threat Defense Virtual でサポートされている [インスタンスタイプ (Instance Type)] を選択します (c4.xlarge を推奨) 。

ステップ 7 画面下部にある [次：インスタンスの詳細の設定 (Next: Configure Instance Details)] ボタンをクリックします。

- 前に作成した VPC に一致するように [ネットワーク (Network)] を変更します。
- 前に作成した管理サブネットに一致するように [サブネット (Subnet)] を変更します。IP アドレスを指定するか、または自動生成を使用できます。
- [ネットワーク インターフェイス (Network Interfaces)] の下にある [デバイスの追加 (Add Device)] ボタンをクリックして、eth1 ネットワーク インターフェイスを追加します。
- eth0 に使用される、事前に作成した管理サブネットに一致するように、[サブネット (Subnet)] を変更します。

(注) Firepower Threat Defense Virtual には、2 つの管理インターフェイスが必要です。

- [高度な詳細 (Advanced Details)] の下で、デフォルトのログイン情報を追加します。デバイス名とパスワードの要件に合わせて、以下の例を変更してください。

注意： [高度な詳細 (Advanced Details)] フィールドにデータを入力する際には、プレーンテキストのみを使用してください。テキスト エディタからこの情報をコピーする場合、プレーンテキストとしてのみコピーしてください。[高度な詳細 (Advanced Details)] フィールドに Unicode データ (空白を含む) をコピーする場合、インスタンスが破損する可能性があります。破損した場合は、インスタンスを終了して、作成し直す必要があります。

Firepower Management Center を使用して FTDv を管理するためのログイン設定の例：

```
#Sensor
{
    "AdminPassword": "<your_password>",
    "Hostname": "<your_hostname>",
    "ManageLocally": "No",
    "FmcIp": "<IP address of FMC>",
    "FmcRegKey": "<registration_passkey>",
    "FmcNatId": "<NAT_ID_if_required>"
}
```

Firepower Device Manager を使用して FTDv を管理するためのログイン設定の例：

```
#Sensor
{
    "AdminPassword": "<your_password>",
    "Hostname": "<your_hostname>",
    "ManageLocally": "Yes"
}
```

ステップ 8 [次：ストレージの追加 (Next: Add Storage)] をクリックします。
デフォルトを受け入れることも、ボリュームを変更することもできます。

ステップ 9 [次：タグ インスタンス (Next: Tag Instance)] をクリックします。

タグは大文字と小文字を区別するキーと値のペアで構成されます。たとえば、[キー (Key)] = 名前、[値 (Value)] = ファイアウォールでタグを定義できます。

- ステップ 10** [次: セキュリティグループの設定 (Next: Configure Security Group)] を選択します。
- ステップ 11** [既存のセキュリティグループを選択する (Select an existing Security Group)] をクリックして、以前に設定されたセキュリティグループを選択するか、または新しいセキュリティグループを作成できます。セキュリティグループの作成の詳細については、AWS の資料を参照してください。
- ステップ 12** [確認して起動する (Review and Launch)] をクリックします。
- ステップ 13** [起動 (Launch)] をクリックします。
- ステップ 14** 既存のキー ペアを選択するか、新しいキー ペアを作成します。
- (注) 既存のキーペアを選択することも、新しいキーペアを作成することもできます。キーペアは、AWS 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場合があるため、必ず既知の場所に保存してください。
- ステップ 15** [インスタンスの起動 (Launch Instances)] をクリックします。
- ステップ 16** [起動の表示 (View Launch)] をクリックし、プロンプトに従います。
- ステップ 17** [EC2ダッシュボード (EC2 Dashboard)] > [ネットワーク インターフェイス (Network Interfaces)] の順にクリックします。
- ステップ 18** [AWS 環境の設定 \(10 ページ\)](#) で以前に作成したインターフェイス トラフィックを特定し、[接続 (Attach)] をクリックします。このインターフェイスが Firepower Threat Defense Virtual インスタンスの eth2 インターフェイスになります。
- ステップ 19** [AWS 環境の設定 \(10 ページ\)](#) で以前に作成したインターフェイス トラフィックを特定し、[接続 (Attach)] をクリックします。このインターフェイスが Firepower Threat Defense Virtual インスタンスの eth3 インターフェイスになります。
- (注) 4 つのインターフェイスを設定する必要があります。設定しないと、Firepower Threat Defense Virtual の起動プロセスが完了しません。
- ステップ 20** [EC2ダッシュボード (EC2 Dashboard)] > [インスタンス (Instances)] の順にクリックします。
- ステップ 21** インスタンスを右クリックし、[インスタンスの設定 (Instance Settings)] > [システムログの取得 (Get System Log)] の順に選択して、ステータスを表示します。
- (注) 接続の問題に関する警告が表示される可能性があります。これが予想されるのは、EULA が完了するまで eth0 インターフェイスがアクティブにならないためです。
- ステップ 22** 20 分後、Firepower Threat Defense Virtual を Firepower Management Center に登録できるようになります。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする (Enable Local Manager)]で [いいえ (No)]を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 \(47 ページ\)](#)」を参照してください。
- [ローカルマネージャを有効にする (Enable Local Manager)]で [はい (Yes)]を選択した場合は、統合されている Firepower Device Manager を使用して FTDv を管理します。「[Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理 \(65 ページ\)](#)」を参照してください。

管理オプションの選択方法の概要については、「[Firepower デバイスの管理方法 \(5 ページ\)](#)」を参照してください。



第 3 章

AWS 用の Firepower Threat Defense Virtual Auto Scale の展開

このドキュメントでは、FTDv Auto Scale Manager のサーバーレスコンポーネントを AWS に導入する方法について説明します。



重要

導入を開始する前に、ドキュメント全体をお読みください。導入を開始する前に、前提条件を満たしていることを確認します。

- [AWS での FTDv の Auto Scale ソリューション \(21 ページ\)](#)
- [Auto Scale ソリューションの前提条件 \(25 ページ\)](#)
- [Auto Scale の展開 \(30 ページ\)](#)
- [Auto Scale メンテナンスタスク \(40 ページ\)](#)
- [Auto Scale のトラブルシューティングとデバッグ \(44 ページ\)](#)

AWS での FTDv の Auto Scale ソリューション

次のセクションでは、Auto Scale ソリューションのコンポーネントが AWS の FTDv でどのように機能するか説明します。

Auto Scale ソリューションについて

シスコでは、Lambda、Auto Scaling グループ、Elastic Load Balancing (ELB)、Amazon S3 バケット、SNS、CloudWatch などの複数の AWS サービスを使用して、FTDv ファイアウォールの Auto Scaling グループを導入するための CloudFormation テンプレートとスクリプトを提供しています。

AWS の FTDv Auto Scale は、AWS 環境の FTDv インスタンスに水平 Auto Scaling 機能を追加する、完全なサーバーレス実装です（つまり、この機能の自動化に関与するヘルパー VM はありません）。

FTDv Auto Scale ソリューションは、以下の内容を提供する CloudFormation テンプレートベースの導入です。

- FMC による FTDv インスタンスの登録と登録解除の完全な自動化。
- スケールアウトされた FTDv インスタンスへの NAT ポリシー、アクセスポリシー、およびルートの自動適用。
- ロードバランサとマルチ可用性ゾーンのサポート。
- Auto Scale 機能の有効化と無効化のサポート。
- FMC でのみ動作。Firepower Device Manager はサポートされていません。

Auto Scale の機能拡張 (バージョン 6.7)

- カスタム指標パブリッシャ：新しい Lambda 関数は、Auto Scale グループ内のすべての FTDv インスタンスのメモリ消費量について FMC を 2 分ごとにポーリングし、その値を CloudWatch メトリックにパブリッシュします。詳細については、[入力パラメータ \(30 ページ\)](#) を参照してください。
- メモリ消費に基づく新しいスケールリングポリシーを使用できます。
- FMC への SSH およびセキュアトンネル用の FTDv プライベート IP 接続。
- FMC の設定検証。
- ELB でより多くのリスニングポートを開くためのサポート。
- シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。

サポートされるソフトウェア プラットフォーム

FTDv Auto Scale ソリューションは、FMC によって管理される FTDv に適用可能で、ソフトウェアバージョンに依存しません。『[Cisco Firepower Compatibility Guide](#)』を参照してください。このガイドには、オペレーティングシステムとホスティング環境の要件を含む、Cisco Firepower ソフトウェアとハードウェアの互換性が記載されています。

- [Firepower Management Centers: Virtual](#) 表には、AWS 上の FMCv における Firepower の互換性および仮想ホスティング環境の要件が一覧表示されています。
- [Firepower Threat Defense Virtual Compatibility](#) 表には、AWS 上の FTDv における Firepower の互換性および仮想ホスティング環境の要件が一覧表示されています。



(注) AWS Auto Scale ソリューションを導入するために、AWS 上の FTDv でサポートされる Firepower の最小バージョンはバージョン 6.4 です。メモリベースのスケールリングを使用するには、FMC がバージョン 6.6 以降を実行している必要があります。

Auto Scale の導入例

この FTDv AWS Auto Scale ソリューションの導入例は、[図 1 : FTDv Auto Scale の導入例の図 \(23 ページ\)](#) に示されています。AWS ロードバランサはインバウンドで開始された接続のみを許可するため、外部で生成されたトラフィックのみが Cisco FTDv ファイアウォール経由で内部を通過できます。



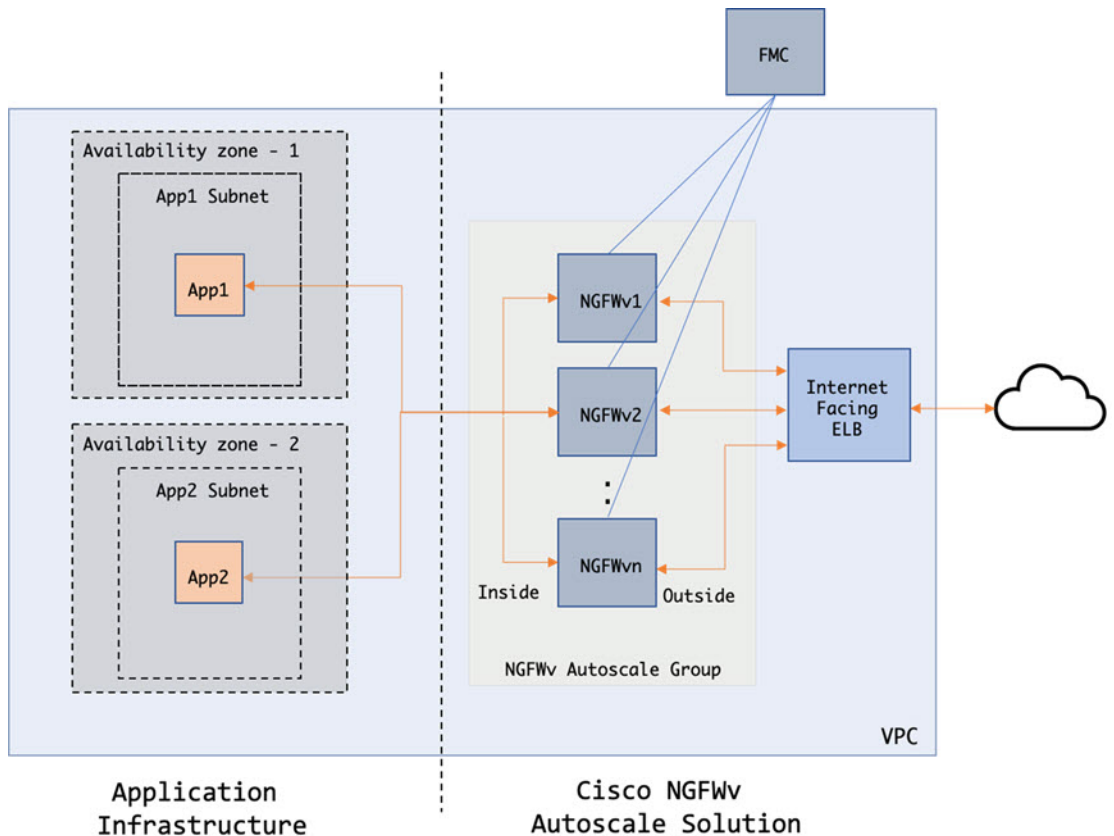
- (注) 前提条件の[SSL サーバー証明書 \(28 ページ\)](#) で説明されているように、セキュアなポートには SSL/TLS 証明書が必要です。

インターネットに面したロードバランサは、ネットワークロードバランサまたはアプリケーションロードバランサです。いずれの場合も、AWS のすべての要件と条件が適用されます。導入例の図に示されているように、点線の右側部分は FTDv テンプレートを介して展開されます。左側は完全にユーザー定義の部分です。



- (注) アプリケーションが開始したアウトバウンドトラフィックは FTDv を通過しません。

図 1 : FTDv Auto Scale の導入例の図



トラフィックのポートベースの分岐が可能です。この分岐は、NAT ルールによって実現できます。FMC でのオブジェクト、デバイスグループ、NAT ルール、アクセスポリシーの設定 (37 ページ) を参照してください。たとえば、インターネットに面した LB DNS、ポート : 80 のトラフィックは、アプリケーション 1 にルーティングでき、ポート : 88 のトラフィックはアプリケーション 2 にルーティングできます。

Auto Scale ソリューションの仕組み

FTDv インスタンスをスケールインおよびスケールアウトするには、Auto Scale Manager と呼ばれる外部エンティティがメトリックをモニターし、Auto Scale グループに FTDv インスタンスの追加または削除を指示し、FTDv デバイスを管理 FMC に登録および登録解除して、FTDv インスタンスを設定します。

Auto Scale Manager は、AWS サーバーレスアーキテクチャを使用して実装され、AWS リソース、FTDv、および FMC と通信します。シスコでは、Auto Scale Manager コンポーネントの導入を自動化する CloudFormation テンプレートを提供しています。このテンプレートにより、包括的なソリューションが機能するために必要なその他のリソースも展開されます。



(注) サーバーレス Auto Scale スクリプトは CloudWatch イベントによってのみ呼び出されるため、インスタンスの起動時にのみ実行されます。

Auto Scale ソリューションのコンポーネント

Auto Scale ソリューションは、次のコンポーネントで構成されています。

CloudFormation テンプレート

CloudFormation テンプレートは、AWS の Auto Scale ソリューションに必要なリソースを展開するために使用されます。テンプレートの構成は次のとおりです。

- Auto Scale グループ、ロードバランサ、セキュリティグループ、およびその他のコンポーネント。
- 展開をカスタマイズするためのユーザー入力を取り込むテンプレート。



注 テンプレートのユーザー入力の検証には限界があるため、展開時に入力を検証するのはユーザーの責任です。

Lambda 関数

Auto Scale ソリューションは、Python で開発された一連の Lambda 関数で、ライフサイクルフック、SNS、CloudWatch イベントやアラームイベントからトリガーされます。基本的な機能は次のとおりです。

- インスタンスに対して Diag、Gig0/0、および Gig0/1 インターフェイスを追加/削除します。
- ロードバランサのターゲットグループに Gig0/1 インターフェイスを登録します。
- 新しい FTDv を FMC に登録します。
- FMC を介して新しい FTDv を設定し展開します。
- スケールインした FTDv を FMC から登録解除（削除）します。
- FMC からメモリメトリックをパブリッシュします。

Lambda 関数は、Python パッケージの形式でお客様に提供されます。

ライフサイクルフック

- ライフサイクルフックは、インスタンスに関するライフサイクルの変更通知を取得するために使用されます。
- インスタンス起動の場合、ライフサイクルフックを使用して、FTDv インスタンスにインターフェイスを追加し、ターゲットグループに外部インターフェイス IP を登録できる Lambda 関数をトリガーします。
- インスタンス終了の場合、ライフサイクルフックを使用して Lambda 関数をトリガーし、ターゲットグループから FTDv インスタンスを登録解除します。

Simple Notification Service (SNS)

- AWS の Simple Notification Service (SNS) を使用してイベントが生成されます。
- AWS にはサーバーレス Lambda 関数に適した Orchestrator がないという制限があるため、ソリューションは、イベントに基づいて Lambda 関数をオーケストレーションするための一種の関数チェーンとして SNS を使用します。

Auto Scale ソリューションの前提条件

展開ファイルのダウンロード

FTDv Auto Scale for AWS ソリューションの起動に必要なファイルをダウンロードします。Firepower バージョン用の展開スクリプトとテンプレートは、次の GitHub リポジトリから入手できます。

- <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/aws>



注目 Auto Scale 用のシスコ提供の導入スクリプトおよびテンプレートは、オープンソースの例として提供されており、通常の Cisco TAC サポートの範囲内ではカバーされないことに注意してください。更新と ReadMe の手順については、GitHub を定期的を確認してください。

インフラストラクチャ設定

複製/ダウンロードされた GitHub リポジトリでは、**infrastructure.yaml** ファイルはテンプレートフォルダにあります。この CFT は、バケットポリシーを使用して VPC、サブネット、ルート、ACL、セキュリティグループ、VPC エンドポイント、および S3 バケットを展開するために使用できます。この CFT は、要件に合わせて変更できます。

次のセクションでは、これらのリソースと Auto Scale での使用について詳しく説明します。これらのリソースを手動で展開し、Auto Scale で使用することもできます。



(注) **infrastructure.yaml** テンプレートは、VPC、サブネット、ACL、セキュリティグループ、S3 バケット、および VPC エンドポイントのみを展開します。SSL 証明書、Lambda レイヤ、または KMS キーリソースは作成されません。

VPC

アプリケーション要件に応じて VPC を作成する必要があります。VPC には、インターネットへのルートがある少なくとも 1 つのサブネットを持つインターネットゲートウェイがあることが想定されます。セキュリティグループ、サブネットなどの要件については、該当するセクションを参照してください。

サブネット

サブネットは、アプリケーションの要件に応じて作成できます。導入例に示されているように、FTDv VM の動作には 3 つのサブネットが必要です。



(注) 複数の可用性ゾーンのサポートが必要な場合、サブネットは AWS クラウド内のゾーンプロパティであるため、各ゾーンにサブネットが必要です。

外部サブネット

外部サブネットには、インターネットゲートウェイへの「0.0.0.0/0」のデフォルトルートが必要です。このサブネットには、FTDv の外部インターフェイスが含まれ、インターネットに面した NLB も含まれます。

内部サブネット

これは、NAT/インターネットゲートウェイの有無にかかわらず、アプリケーションサブネットに似ています。FTDv 正常性プローブでは、ポート 80 経由で AWS メタデータサーバー (169.254.169.254) に到達できる必要があることに注意してください。



- (注) この AutoScale ソリューションでは、ロードバランサの正常性プローブが `inside/Gig0/0` インターフェイスを介して AWS メタデータサーバーにリダイレクトされます。ただし、ロードバランサから FTDv に送信される正常性プローブ接続を提供する独自のアプリケーションでこれを変更できます。この場合、AWS メタデータサーバー オブジェクトをそれぞれのアプリケーションの IP アドレスに置き換えて、正常性プローブ応答を提供する必要があります。

管理サブネット

このサブネットには、FTDv 管理インターフェイスが含まれます。このサブネットで FMC を使用している場合、FTDv への Elastic IP アドレス (EIP) の割り当ては任意です。診断インターフェイスもこのサブネット上にあります。

Lambda サブネット

AWS Lambda 関数では、デフォルトゲートウェイとして NAT ゲートウェイを持つ 2 つのサブネットが必要です。これにより、Lambda 関数が VPC に対してプライベートになります。Lambda サブネットは、他のサブネットと同じ幅である必要はありません。Lambda サブネットのベストプラクティスについては、AWS のドキュメントを参照してください。

アプリケーションサブネット

Auto Scale ソリューションからこのサブネットに課せられる制限はありませんが、アプリケーションに VPC 外部のアウトバウンド接続が必要な場合は、サブネット上にそれぞれのルートが設定されている必要があります。これは、アウトバウンドで開始されたトラフィックがロードバランサを通過しないためです。[AWS Elastic Load Balancing ユーザーガイド \[英語\]](#) を参照してください。

セキュリティ グループ

提供された Auto Scale グループテンプレートでは、すべての接続が許可されます。Auto Scale ソリューションを機能させるために必要なのは、次の接続だけです。

表 3: 必須のポート

ポート	使用方法	サブネット
8305	FMC から FTDv へのセキュアなトンネル接続	管理サブネット

ポート	使用方法	サブネット
正常性プローブポート (デフォルト: 8080)	インターネットに面したロードバランサの正常性プローブ	外部サブネット、内部サブネット
アプリケーションポート	アプリケーションデータトラフィック	外部サブネット、内部サブネット

FMC インスタンスのセキュリティグループまたは ACL

Lambda 関数と FMC 間の HTTPS 接続を許可します。Lambda 関数は、NAT ゲートウェイをデフォルトルートとして持つ Lambda サブネットに保持されるため、FMC は NAT ゲートウェイ IP アドレスからのインバウンド HTTPS 接続を持つことができます。

Amazon S3 バケット

Amazon Simple Storage Service (Amazon S3) は、業界をリードする拡張性、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクトストレージサービスです。ファイアウォールテンプレートとアプリケーションテンプレートの両方に必要なすべてのファイルを S3 バケットに配置できます。

テンプレートが展開されると、S3 バケット内の Zip ファイルを参照して Lambda 関数が作成されます。したがって、S3 バケットはユーザーアカウントにアクセス可能である必要があります。

SSL サーバー証明書

インターネットに面したロードバランサが TLS/SSL をサポートしている必要がある場合、証明書 ARN が必要です。詳細については、次のリンクを参照してください。

- [サーバー証明書の使用](#)
- [テスト用の秘密キーと自己署名証明書の作成](#)
- [自己署名 SSL 証明書を使用した AWS ELB の作成 \(サードパーティリンク\)](#)

ARN の例: `arn:aws:iam::[AWS Account]:server-certificate/[Certificate Name]`

Lambda レイヤ

`autoscale_layer.zip` は、Python 3.6 がインストールされた Ubuntu 18.04 などの Linux 環境で作成できます。

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.6 ./layer/
```

```
source ./layer/bin/activate
pip3 install pycrypto==2.6.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/.libs_cffi_backend/
cp -r ./layer/lib/python3.6/site-packages/* ./python/
cp -r ./layer/lib/python3.6/site-packages/.libs_cffi_backend/* ./python/.libs_cffi_backend/
zip -r autoscale_layer.zip ./python
```

作成された **autoscale_layer.zip** ファイルは、*lambda-python-files* フォルダにコピーする必要があります。

KMS マスターキー

これは、FMC および FTDv パスワードが暗号化形式の場合に必要です。それ以外の場合、このコンポーネントは必要ありません。パスワードは、ここで提供される KMS のみを使用して暗号化する必要があります。KMS ARN が CFT で入力される場合、パスワードを暗号化する必要があります。それ以外の場合、パスワードはプレーンテキストである必要があります。

マスターキーと暗号化の詳細については、パスワードの暗号化と KMS に関する AWS のドキュメントの [キーの作成 \[英語\]](#) と [AWS CLI コマンドリファレンス \[英語\]](#) を参照してください。

例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtectIoN'
{
  "KeyId": "KMS-ARN",
  "CiphertextBlob":
  "AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFFpSXUU7HQrnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
  G9w0BBwagWzBZAqEAMFQGCsqGSIb3DQEHAATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
  +wxpWktXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

CiphertextBlob キーの値をパスワードとして使用する必要があります。

Python 3 環境

make.py ファイルは、複製されたリポジトリの最上位ディレクトリにあります。これにより、python ファイルが Zip ファイルに圧縮され、ターゲットフォルダにコピーされます。これらのタスクを実行するには、Python 3 環境が使用可能である必要があります。

Auto Scale の展開

準備

アプリケーションが展開されているか、アプリケーションの展開プランが利用可能である必要があります。

入力パラメータ

導入前に、次の入力パラメータを収集する必要があります。

表 4: Auto Scale 入力パラメータ

パラメータ	使用できる値/タイプ	説明
PodNumber	文字列 許可パターン: <code>"\d{1,3}"</code>	これはポッド番号です。Auto Scale グループ名 (FTDv-Group-Name) の末尾に追加されます。たとえば、この値が「1」の場合、グループ名は <i>FTDv-Group-Name-1</i> になります。 1 桁以上 3 桁以下の数字である必要があります。 デフォルト: 1
AutoscaleGrpNamePrefix	文字列	これは Auto Scale グループ名プレフィックスです。ポッド番号がサフィックスとして追加されます。 最大: 18 文字 例: Cisco-FTDv-1
NotifyEmailID	文字列	Auto Scale イベントはこの電子メールアドレスに送信されます。サブスクリプション電子メール要求を受け入れる必要があります。 例: admin@company.com
VpcId	文字列	デバイスを展開する必要がある VPC ID。これは、AWS の要件に従って設定する必要があります。 タイプ: AWS::EC2::VPC::Id 「 <i>infrastructure.yaml</i> 」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。

パラメータ	使用できる値/タイプ	説明
LambdaSubnets	リスト	Lambda 関数が展開されるサブネット。 タイプ : List<AWS::EC2::Subnet::Id> 「 <i>infrastructure.yaml</i> 」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
LambdaSG	リスト	Lambda 機能のセキュリティグループ。 タイプ : List<AWS::EC2::SecurityGroup::Id> 「 <i>infrastructure.yaml</i> 」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
S3BktName	文字列	ファイルの S3 バケット名。これは、AWS の要件に従ってアカウントに設定する必要があります。 「 <i>infrastructure.yaml</i> 」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
LoadBalancerType	文字列	インターネットに面したロードバランサのタイプ（「アプリケーション」または「ネットワーク」）。 例 : アプリケーション
LoadBalancerSG	文字列	ロードバランサのセキュリティグループ。ネットワークロードバランサの場合は使用されません。ただし、セキュリティグループ ID を指定する必要があります。 タイプ : List<AWS::EC2::SecurityGroup::Id> 「 <i>infrastructure.yaml</i> 」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。

パラメータ	使用できる値/タイプ	説明
LoadBalancerPort	整数	<p>ロードバランサポート。このポートは、選択したロードバランサタイプに基づいて、プロトコルとして HTTP/HTTPS または TCP/TLS を使用して LB で開きます。</p> <p>ポートが有効な TCP ポートであることを確認します。これはロードバランサリスナーの作成に使用されます。</p> <p>デフォルト : 80</p>
SSL認証	文字列	<p>セキュアポート接続の SSL 証明書の ARN。指定しない場合、ロードバランサで開かれるポートは TCP/HTTP になります。指定した場合、ロードバランサで開かれるポートは TLS/HTTPS になります。</p>
TgHealthPort	整数	<p>このポートは、正常性プローブのターゲットグループによって使用されます。FTDv のこのポートに到達する正常性プローブは、AWS メタデータサーバーにルーティングされるため、トラフィックには使用しないでください。このポートは有効な TCP ポートである必要があります。</p> <p>アプリケーション自体が正常性プローブにตอบสนองするようにする場合は、それに応じて FTDv の NAT ルールを変更できます。このような場合、アプリケーションがตอบสนองしないと、FTDv は Unhealthy インスタンスのしきい値アラームにより、非正常としてマークされ、削除されます。</p> <p>例 : 8080</p>
AssignPublicIP	ブール値	<p>「true」を選択すると、パブリック IP が割り当てられます。BYOL タイプの FTDv の場合、これは https://tools.cisco.com に接続するために必要です。</p> <p>例 : TRUE</p>

パラメータ	使用できる値/タイプ	説明
InstanceType	文字列	<p>Amazon マシンイメージ (AMI) は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。</p> <p>FTDv をサポートする AMI インスタンスタイプのみを使用する必要があります。『Firepower Release Notes』を参照してください。</p> <p>例 : c4.2xlarge</p>
LicenseType	文字列	<p>FTDv ライセンスタイプ (BYOL または PAYG) 。関連する AMI ID が同じライセンスタイプであることを確認します。</p> <p>例 : BYOL</p>
AmiId	文字列	<p>FTDv AMI ID (有効な Cisco FTDv AMI ID) 。</p> <p>タイプ : AWS::EC2::Image::Id</p> <p>リージョンとイメージの目的のバージョンに応じて、正しい AMIID を選択してください。Auto Scale 機能は、Firepower バージョン 6.4+、BYOL/PAYG イメージをサポートします。いずれの場合も、AWS マーケットプレイスでライセンスに同意する必要があります。</p> <p>BYOL の場合、設定 JSON ファイルの「licenseCaps」キーを「BASE」、「MALWARE」、「THREAT」、「URLFilter」などの機能で更新してください。</p>
NoOfAZs	整数	<p>FTDv を展開する必要がある可用性ゾーンの数 (1 ~ 3) 。ALB 導入の場合、AWS で必要な最小値は 2 です。</p> <p>例 : 2。</p>

パラメータ	使用できる値/タイプ	説明
ListOfAzs	カンマ区切り文字列	<p>ゾーンの順序のカンマ区切りリスト。</p> <p>(注) ゾーンのリスト順は重要です。サブネットリストは同じ順序で指定する必要があります。</p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p> <p>例 : us-east-1a、us-east-1b、us-east-1c</p>
MgmtInterfaceSG	文字列	<p>FTDv 管理インターフェイスのセキュリティグループ。</p> <p>タイプ : List<AWS::EC2::SecurityGroup::Id></p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p>
InsideInterfaceSG	文字列	<p>FTDv 内部インターフェイスのセキュリティグループ。</p> <p>タイプ : AWS::EC2::SecurityGroup::Id</p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p>
OutsideInterfaceSG	文字列	<p>FTDv 外部インターフェイスのセキュリティグループ。</p> <p>タイプ : AWS::EC2::SecurityGroup::Id</p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p> <p>例 : sg-0c190a824b22d52bb</p>

パラメータ	使用できる値/タイプ	説明
MgmtSubnetId	カンマ区切りリスト	<p>管理サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。</p> <p>タイプ : List<AWS::EC2::SecurityGroup::Id></p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p>
InsideSubnetId	カンマ区切りリスト	<p>内部/Gig0/0 サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。</p> <p>タイプ : List<AWS::EC2::SecurityGroup::Id></p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p>
OutsideSubnetId	カンマ区切りリスト	<p>外部/Gig0/1 サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。</p> <p>タイプ : List<AWS::EC2::SecurityGroup::Id></p> <p>「<i>infrastructure.yaml</i>」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。</p>
KmsArn	文字列	<p>既存の KMS の ARN (保存時に暗号化するための AWS KMS キー)。指定した場合は、FMC および FTDv のパスワードを暗号化する必要があります。パスワードの暗号化は、指定された ARN のみを使用して実行する必要があります。</p> <p>暗号化パスワードの生成例 : " aws kms encrypt --key-id <KMS ARN> --plaintext <password> " 次のような生成されたパスワードを使用してください。</p> <p>例 : arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e</p>

パラメータ	使用できる値/タイプ	説明
ngfwPassword	文字列	<p>すべてのFTDvインスタンスには、起動テンプレート（自動スケールグループ）の[ユーザーデータ（Userdata）]フィールドに入力されたデフォルトのパスワードが設定されています。</p> <p>この入力により、FTDvにアクセスできるようになると、パスワードが新しく提供されたパスワードに変更されます。</p> <p>KMS ARN が使用されていない場合は、プレーンテキストのパスワードを使用してください。KMS ARNが使用されている場合は、暗号化されたパスワードを使用する必要があります。</p> <p>例：Cisco123789! または AQIAGcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU</p>
fmcServer	数値文字列	<p>Lambda 関数と FTDv 管理インターフェイスの両方に到達可能な管理 FMC の IP アドレス。</p> <p>例：10.10.17.21</p>
fmcOperationsUsername	文字列	<p>管理 FMC で作成された Network-Admin 以上の特権ユーザー。ユーザーおよびロールの作成については、『Firepower Management Center Configuration Guide』を参照してください。</p> <p>例：apiuser-1</p>
fmcOperationsPassword	文字列	<p>KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。</p> <p>例：Cisco123@ または AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQrnCAajB</p>
fmcDeviceGrpName	文字列	<p>FMC のデバイスグループ名。</p> <p>例：AWS-Cisco-NGFW-VMs-1</p>
fmcPublishMetrics	ブール値	<p>「TRUE」に設定すると、指定されたデバイスグループ内の登録済み FTDv センサーのメモリ消費量を取得するために、2分に1回実行される Lambda 関数が作成されます。</p> <p>使用可能な値：TRUE、FALSE</p> <p>例：TRUE</p>

パラメータ	使用できる値/タイプ	説明
fmcMetricsUsername	文字列	AWS CloudWatch にメトリックを公開するための一意の FMC ユーザー名。ユーザーおよびロールの作成については、『 Firepower Management Center Configuration Guide 』を参照してください。 「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。 例：publisher-1
fmcMetricsPassword	文字列	AWS CloudWatch にメトリックを公開するための FMC パスワード。KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。 「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。 例：Cisco123789!
CpuThresholds	カンマ区切り整数	CPU しきい値の下限と CPU しきい値の上限。最小値は 0 で、最大値は 99 です。 デフォルト：10, 70 しきい値の下限はしきい値の上限よりも小さくする必要があります。 例：30,70
MemoryThresholds	カンマ区切り整数	MEM しきい値の下限と MEM しきい値の上限。最小値は 0 で、最大値は 99 です。 デフォルト：40, 70 しきい値の下限はしきい値の上限よりも小さくする必要があります。「fmcPublishMetrics」パラメータが「FALSE」の場合、影響はありません。 例：40,50

FMC でのオブジェクト、デバイスグループ、NAT ルール、アクセスポリシーの設定

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) を使用して FTDv を管理できます。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。詳細については、[Firepower Management Center を使用した Firepower Threat Defense Virtual について \(47 ページ\)](#) を参照してください。

FTDv の設定に使用されるオブジェクトはすべて、ユーザーが作成する必要があります。



重要 デバイスグループを作成し、ルールを適用する必要があります。デバイスグループに適用されたすべての設定が FTDv インスタンスにプッシュされます。

オブジェクト

次のオブジェクトを作成します。

表 5: FTDv 管理用の FMC 設定オブジェクト

オブジェクトタイプ	名前	値
ホスト	aws-metadata-server	169.254.169.254
ポート	health-check-port	必要に応じて、8080 またはその他のポート
ゾーン	内部またはその他の名前	—
ゾーン	外部またはその他の名前	—

NAT ポリシー

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。NAT ポリシーの詳細については、[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 \(47 ページ\)](#) の NAT の設定 (58 ページ) を参照してください。

NAT ポリシーには 1 つの必須ルールが必要です。

- 送信元ゾーン (Source Zone) : 外部ゾーン
- 宛先ゾーン (Dest Zone) : 内部ゾーン
- 元の送信元 (Original-sources) : any-ipv4
- 元の送信元ポート (Original source port) : 元/デフォルト
- 元の宛先 (Original Destinations) : インターフェイス (Interface)
- 元の宛先ポート (Original-destination-port) : 8080 またはユーザーが設定する正常性ポート
- 変換済み送信元 (Translated-sources) : any-ipv4
- 変換済み送信元ポート (Translated source port) : 元/デフォルト
- 変換済み宛先 (Translated-destination) : aws-metadata-server
- 変換済み宛先ポート (Translated-destination-port) : 80/HTTP

同様に、この設定が FTDv デバイスにプッシュされるように、データトラフィック NAT ルールを追加できます。



重要 作成された NAT ポリシーはデバイスグループに適用する必要があります。Lambda 関数からの FMC 検証でこれを検証します。

アクセス ポリシー

内部から外部へのトラフィックを許可するアクセス制御を設定します。必要なすべてのポリシーを含むアクセスポリシーを作成できます。このポートのトラフィックが到達できるように、正常性ポートオブジェクトを許可する必要があります。アクセスポリシーの詳細については、[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 \(47 ページ\)](#) の [アクセス制御の設定 \(61 ページ\)](#) を参照してください。

設定 JSON ファイルの更新

Configuration.json ファイルは、[GitHub](#) リポジトリから取得したアーカイブ Zip の一部である *lambda_python_files* フォルダにあります。JSON キーは変更しないでください。FTDv VM のスタティックルートは、JSON ファイルで設定する必要があります。

スタティックルートの設定例については、次を参照してください。

```
{
  "interface": "inside",
  "network": "any-ipv4",
  "gateway": "",
  "metric": "1"
}
```

JSON ファイルのすべての値は、デフォルトの FTDv パスワードを除き、要件に応じて変更できます。

Amazon Simple Storage Service (S3) へのファイルのアップロード

target ディレクトリ内のすべてのファイルを Amazon S3 バケットにアップロードする必要があります。必要に応じて、CLI を使用して、*target* ディレクトリ内のすべてのファイルを Amazon S3 バケットにアップロードできます。

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

スタックの展開

展開のすべての前提条件が完了すると、AWS CloudFormation スタックを作成できます。

target ディレクトリ内の *deploy_ngfw_autoscale.yaml* ファイルを使用します。

[入力パラメータ \(30 ページ\)](#) で収集されたパラメータを入力します。

展開の検証

テンプレートの展開が成功したら、Lambda 関数と CloudWatch イベントが作成されていることを検証する必要があります。デフォルトでは、Auto Scale グループのインスタンスの最小数と最大数はゼロです。AWS EC2 コンソールで必要な数のインスタンスを使用して、Auto Scale グループを編集する必要があります。これにより、新しい FTDv インスタンスがトリガーされます。

1 つのインスタンスのみを起動してワークフローを確認し、そのインスタンスが期待どおりに動作しているかどうかを検証することを推奨します。その後、FTDv の実際の要件を展開でき、動作を確認することもできます。AWS スケーリングポリシーによる削除を回避するために、最小数の FTDv インスタンスをスケールイン保護としてマークできます。

Auto Scale メンテナンスタスク

スケーリングプロセス

このトピックでは、Auto Scale グループの 1 つ以上のスケーリングプロセスを一時停止してから再開する方法について説明します。

スケールアクションの開始と停止

スケールアクションを開始および停止するには、次の手順を実行します。

- AWS 動的スケーリングの場合：スケールアウトアクションを有効化または無効化する方法については、次のリンクを参照してください。

[スケーリングプロセスの一時停止と再開](#)

ヘルスマニター

60 分ごとに、CloudWatch Cron ジョブは、Health Doctor モジュールの Auto Scale Manager Lambda をトリガーします。

- 有効な FTDv VM に属する異常な IP がある場合、FTDv の展開時間が 1 時間を超えると、そのインスタンスは削除されます。
- それらの IP が有効な FTDv VM の IP ではない場合、IP だけがターゲットグループから削除されます。

ヘルスマニターは、デバイスグループ、アクセスポリシー、および NAT ルールの FMC 構成も検証します。IP/インスタンスが正常でない場合、または FMC 検証が失敗した場合、ヘルスマニターはユーザーに電子メールを送信します。

ヘルスマニターの無効化

ヘルスマニターを無効にするには、`constant.py` で `constant` を「True」に設定します。

ヘルスマニターの有効化

ヘルスマニターを有効にするには、`constant.py` で固定値を「False」に設定します。

ライフサイクルフックの無効化

まれに、ライフサイクルフックを無効にする必要があります。無効にすると、インスタンスに追加のインターフェイスが追加されません。また、FTDv インスタンスの展開に連続して失敗することがあります。

Auto Scale Manager の無効化

Auto Scale Manager を無効化するには、それぞれの CloudWatch イベント「`notify-instance-launch`」と「`notify-instance-terminate`」を無効化する必要があります。これらのイベントを無効にしても、新しいイベントの Lambda はトリガーされません。ただし、すでに実行されている Lambda アクションは続行されます。Auto Scale Manager が突然停止することはありません。スタックの削除またはリソースの削除による突然の停止を試みると、不定状態になる可能性があります。

ロードバランサのターゲット

AWS ロードバランサでは、複数のネットワーク インターフェイスを持つインスタンスに対してインスタンスタイプのターゲットが許可されないため、Gigabit0/1 インターフェイス IP はターゲットグループのターゲットとして設定されます。ただし、現在のところ、AWS Auto Scale のヘルスチェックは、IP ではなく、インスタンスタイプのターゲットに対してのみ機能します。また、これらの IP はターゲットグループから自動的に追加されたり、削除されたりしません。したがって、Auto Scale ソリューションは、これら両方のタスクをプログラムで処理します。ただし、メンテナンスやトラブルシューティングの場合は、手動で実行する必要があります。

ターゲットグループへのターゲットの登録

FTDv インスタンスをロードバランサに登録するには、Gigabit0/1 インスタンス IP（外部サブネット）をターゲットとしてターゲットグループに追加する必要があります。「[IP アドレスによるターゲットの登録または登録解除](#)」を参照してください。

ターゲットグループからのターゲットの登録解除

ロードバランサに対する FTDv インスタンスの登録を解除するには、Gigabit0/1 インスタンス IP（外部サブネット）をターゲットグループのターゲットとして削除する必要があります。「[IP アドレスによるターゲットの登録または登録解除](#)」を参照してください。

インスタンスのスタンバイ

AWS では、Auto Scale グループでのインスタンスの再起動は許可されませんが、ユーザーはインスタンスをスタンバイ状態にして再起動アクションを実行できます。これは、ロードバランサのターゲットがインスタンスタイプの場合に最も機能しますが、FTDv VM は、複数のネットワークインターフェイスがあるため、インスタンスタイプのターゲットとして設定できません。

インスタンスをスタンバイ状態にする

インスタンスがスタンバイ状態になると、正常性プローブが失敗するまで、ターゲットグループ内のそのインスタンスの IP は同じ状態のままになります。このため、インスタンスをスタンバイ状態にする前に、ターゲットグループからそれぞれの IP を登録解除することをお勧めします。詳細については、[ターゲットグループからのターゲットの登録解除 \(41 ページ\)](#) を参照してください。

IP が削除されたら、「[Auto Scaling グループからのインスタンスの一時的な削除](#)」を参照してください。

スタンバイ状態からのインスタンスの削除

同様に、インスタンスをスタンバイ状態から実行状態に移行できます。スタンバイ状態から削除すると、インスタンスの IP がターゲットグループのターゲットに登録されます。「[ターゲットグループへのターゲットの登録 \(41 ページ\)](#)」を参照してください。

トラブルシューティングやメンテナンスのためにインスタンスをスタンバイ状態にする方法の詳細については、[AWS News Blog](#) を参照してください。

Auto Scale グループからのインスタンスの削除または分離

Auto Scale グループからインスタンスを削除するには、まずインスタンスをスタンバイ状態に移行する必要があります。「[インスタンスをスタンバイ状態にする](#)」を参照してください。スタンバイ状態になったインスタンスは、削除または分離できます。「[Auto Scaling グループから EC2 インスタンスをデタッチする](#)」を参照してください。

FMC 側に変更はありません。必要な変更は手動で実行する必要があります。

インスタンスで終了

インスタンスを終了するには、スタンバイ状態にする必要があります。[インスタンスのスタンバイ \(42 ページ\)](#) を参照してください。インスタンスがスタンバイ状態になったら、終了できます。

インスタンスのスケールイン保護

Auto Scale グループから特定のインスタンスが誤って削除されないようにするために、そのインスタンスをスケールイン保護として作成できます。インスタンスがスケールイン保護されている場合、スケールインイベントが原因で終了することはありません。

インスタンスをスケールイン保護状態にするには、次のリンクを参照してください。

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>



重要 正常（EC2 インスタンスだけでなく、ターゲット IP が正常）なインスタンスの最小数をスケールイン保護として設定することをお勧めします。

ログイン情報と登録 ID の変更

設定の変更は、すでに実行中のインスタンスには自動的に反映されません。変更は新しいデバイスにのみ反映されます。このような変更は、既存のデバイスに手動でプッシュする必要があります。

FMC ユーザー名とパスワードの変更

FMC の IP、ユーザー名、またはパスワードを変更する場合は、Auto Scale Manager Lambda 関数とカスタム指標パブリッシャ Lambda 関数の環境変数でそれぞれの変更を実行する必要があります。「[AWS Lambda 環境変数の使用](#)」を参照してください。

Lambda の次回実行時に、変更された環境変数が参照されます。



(注) 環境変数は Lambda 関数に直接渡されます。パスワードの複雑さはチェックされません。

FTDv Admin パスワードを変更します。

FTDv パスワードを変更すると、インスタンスを実行するために各デバイスでパスワードを手動で変更する必要があります。新しい FTDv デバイスをオンボードする場合、FTDv パスワードは Lambda 環境変数から取得されます。「[AWS Lambda 環境変数の使用](#)」を参照してください。

登録 ID と NAT ID の変更

新しい FTDv デバイスを異なる登録 ID と NAT ID でオンボードする場合、FMC 登録のために、Configuration.json ファイルでこの情報を変更する必要があります。Configuration.json ファイルは、[Lambda] リソースページにあります。

アクセスポリシーと NAT ポリシーの変更

アクセスポリシーまたは NAT ポリシーへの変更は、デバイスグループの割り当てにより、今後のインスタンスに自動的に適用されます。ただし、既存の FTDv インスタンスを更新するには、設定変更を手動でプッシュして、FMC から展開する必要があります。

AWS リソースに対する変更

AWS の導入後、Auto Scale グループ、起動設定、CloudWatch イベント、スケーリングポリシーなど、多くの項目を変更できます。CloudFormation スタックにリソースをインポートするか、既存のリソースから新しいスタックを作成できます。

AWS リソースで実行される変更を管理する方法の詳細については、「[既存リソースの CloudFormation 管理への取り込み](#)」を参照してください。

CloudWatch ログの収集および分析

CloudWatch ログをエクスポートするには、「[AWS CLI を使用した Amazon S3 へのログデータのエクスポート](#)」を参照してください。

Auto Scale のトラブルシューティングとデバッグ

AWS CloudFormation コンソール

AWS CloudFormation コンソールで CloudFormation スタックへの入力パラメータを確認できます。これにより、Web ブラウザからスタックを直接作成、監視、更新、削除できます。

目的のスタックに移動し、[パラメータ (parameter)] タブを確認します。[Lambda 関数環境変数 (Lambda Functions environment variables)] タブで Lambda 関数への入力を確認することもできます。configuration.json ファイルは、Auto Scale Manager Lambda 関数自体でも表示できます。

AWS CloudFormation コンソールの詳細については、『AWS CloudFormation ユーザーガイド (AWS CloudFormation User Guide)』を参照してください。

Amazon CloudWatch ログ

個々の Lambda 関数のログを表示できます。AWS Lambda はお客様の代わりに Lambda 関数を自動的に監視し、Amazon CloudWatch を通じてメトリックを報告します。関数の障害のトラブルシューティングに役立つように、Lambda は関数によって処理されたすべての要求をログに記録し、Amazon CloudWatch ログを通じてコードによって生成されたログも自動的に保存します。

Lambda コンソール、CloudWatch コンソール、AWS CLI、または CloudWatch API を使用して、Lambda のログを表示できます。ロググループと CloudWatch コンソールを介したロググループへのアクセスの詳細については、『Amazon CloudWatch ユーザーガイド (Amazon CloudWatch

User Guide)』でモニターリングシステム、アプリケーション、およびカスタムログファイルについて参照してください。

ロードバランサのヘルスチェックの失敗

ロードバランサのヘルスチェックには、プロトコル、ping ポート、ping パス、応答タイムアウト、ヘルスチェック間隔などの情報が含まれます。ヘルスチェック間隔内に 200 応答コードを返す場合、インスタンスは正常と見なされます。

一部またはすべてのインスタンスの現在の状態が `OutOfService` であり、説明フィールドに「インスタンスがヘルスチェックの異常しきい値の数以上連続して失敗しました (Instance has failed at least the Unhealthy Threshold number of health checks consecutively)」というメッセージが表示された場合、インスタンスはロードバランサのヘルスチェックに失敗しています。

FMC 構成の正常性プローブ NAT ルールを確認する必要があります。詳細については、『[Troubleshoot a Classic Load Balancer: Health checks](#)』を参照してください。

トラフィックの問題

FTDv インスタンスのトラフィックの問題をトラブルシューティングするには、ロードバランサールール、NAT ルール、および FTDv インスタンスで設定されているスタティックルートを確認する必要があります。

セキュリティグループのルールなど、展開テンプレートで提供される AWS 仮想ネットワーク/サブネット/ゲートウェイの詳細も確認する必要があります。たとえば、「EC2 インスタンスのトラブルシューティング (Troubleshooting EC2 instances)」<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-troubleshoot.html>など、AWS のドキュメントを参照することもできます。

FMC への接続に失敗

管理接続が中断された場合は、FMC 構成とログイン情報を確認する必要があります。『*Firepower Management Center Configuration Guide*』の「Requirements and Prerequisites for Device Management」を参照してください。

デバイスが FMC への登録に失敗 FMC

デバイスが FMC に登録できない場合は、FMC 構成に障害があるか到達不能であるか、または FMC に新しいデバイスを収容するキャパシティがあるかどうかを判断する必要があります。

『*Firepower Management Center Configuration Guide*』の「Add a Device to the FMC」を参照してください。

FTDv に SSH 接続不可能 FTDv

FTDv に SSH 接続できない場合は、テンプレートを介して複雑なパスワードが FTDv に渡されたかどうかを確認します。



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 \(47 ページ\)](#)
- [Firepower Management Center へのログイン \(48 ページ\)](#)
- [Firepower Management Center へのデバイスの登録 \(48 ページ\)](#)
- [基本的なセキュリティポリシーの設定 \(51 ページ\)](#)
- [Firepower Threat Defense CLI へのアクセス \(63 ページ\)](#)

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 \(61 ページ\)](#)」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 \(63 ページ\)](#)」) 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 \(51 ページ\)](#)
 - ステップ 2 [DHCP サーバーの設定 \(55 ページ\)](#)
 - ステップ 3 [デフォルトルートの追加 \(56 ページ\)](#)
 - ステップ 4 [NAT の設定 \(58 ページ\)](#)
 - ステップ 5 [アクセス制御の設定 \(61 ページ\)](#)
 - ステップ 6 [設定の展開 \(62 ページ\)](#)
-

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。

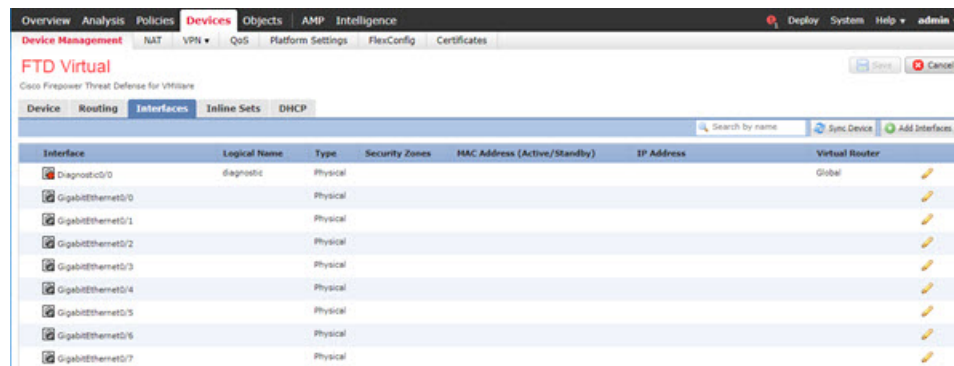
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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。

Edit Physical Interface

General | IPv4 | IPv6 | Advanced | Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

- 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。

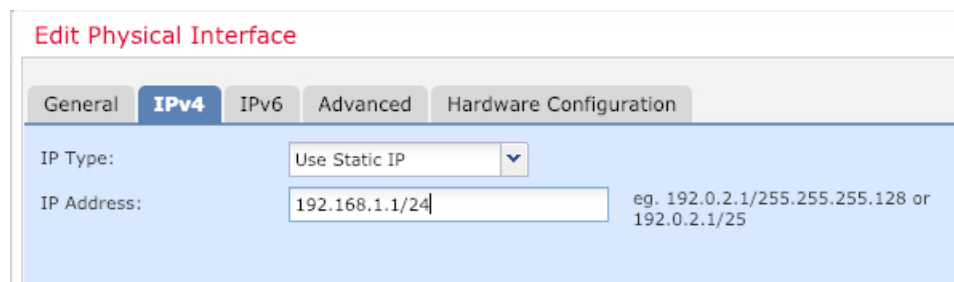
たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできませんが、外部から内部に向けては設定できません。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 is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the IP address field, there is a note: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- [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。

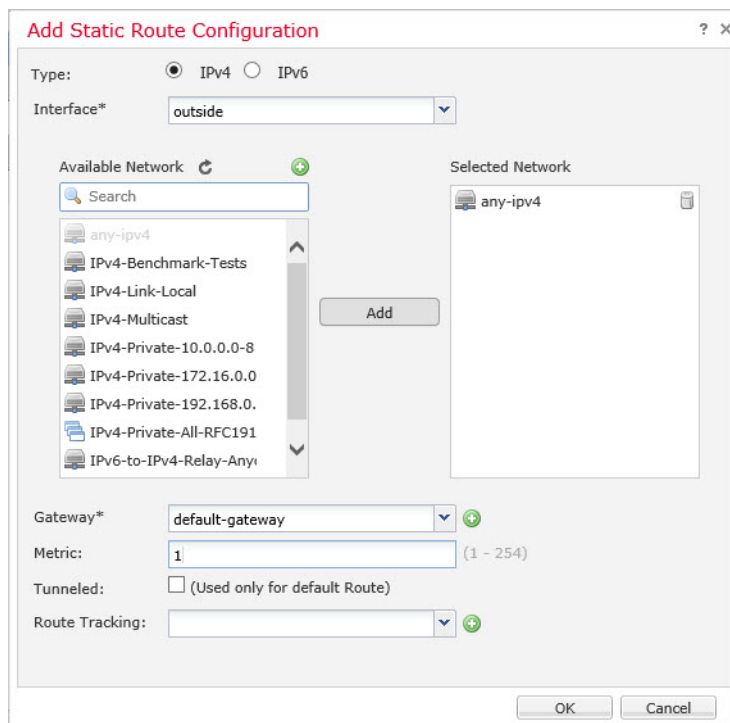
デフォルトルートの追加

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。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

10.89.5.20 You have unsaved changes Save Cancel

Cisco Firepower 9000 Series SM-24 Threat Defense

Device Routing Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	<input checked="" type="checkbox"/>
▼ IPv6 Routes					

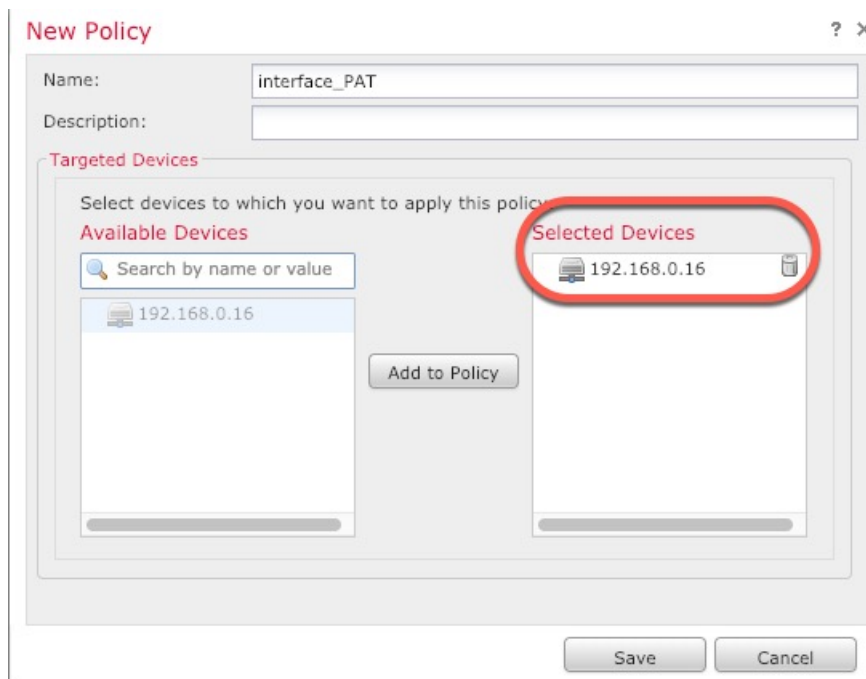
ステップ4 [保存 (Save)]をクリックします。

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。

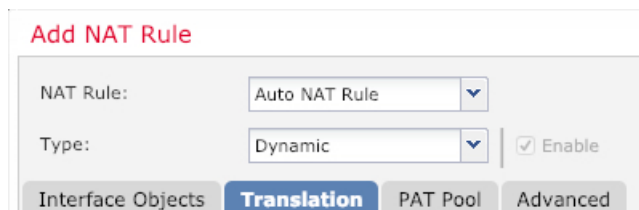


ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ 3 [ルールの追加 (Add Rule)] をクリックします。

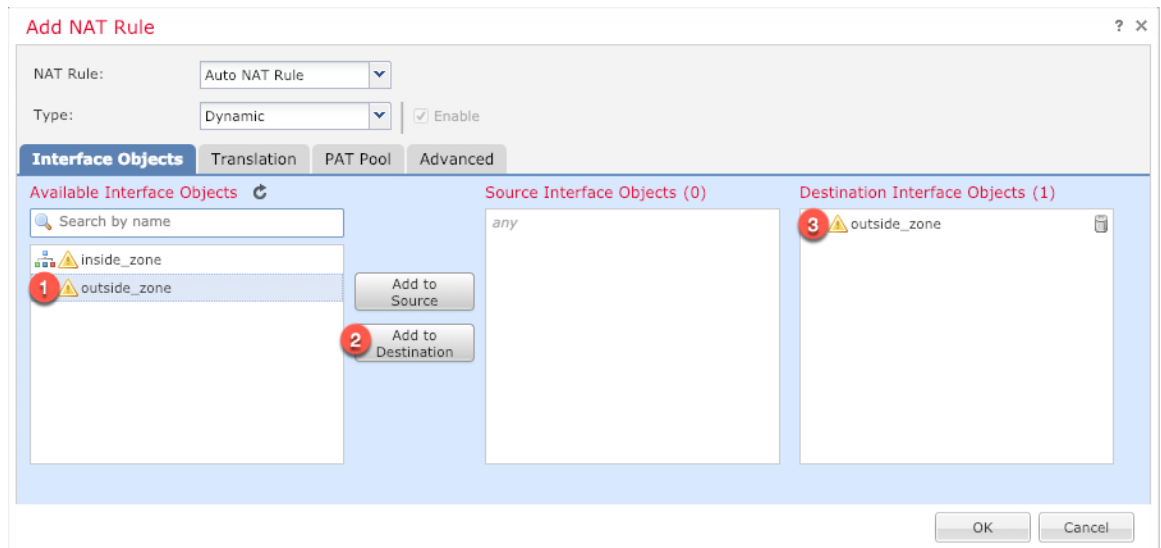
[NATルールの追加 (Add NAT Rule)] ダイアログボックスが表示されます。

ステップ 4 基本ルールのオプションを設定します。

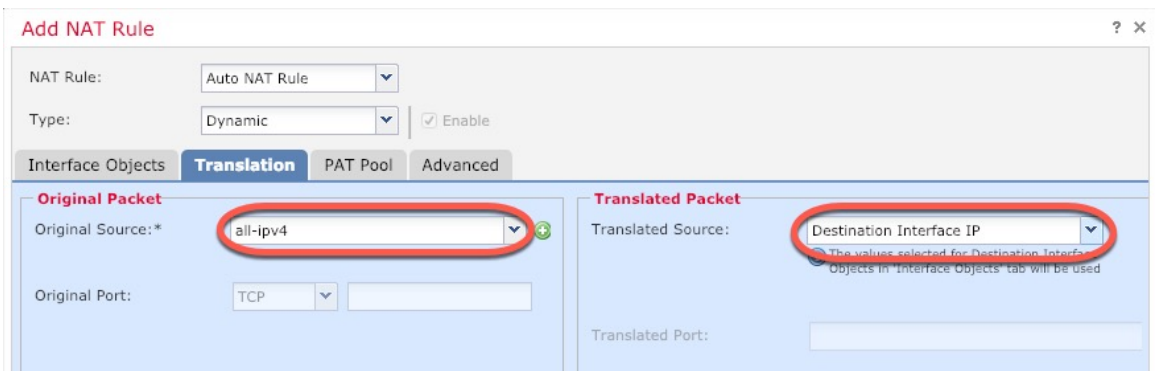


- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

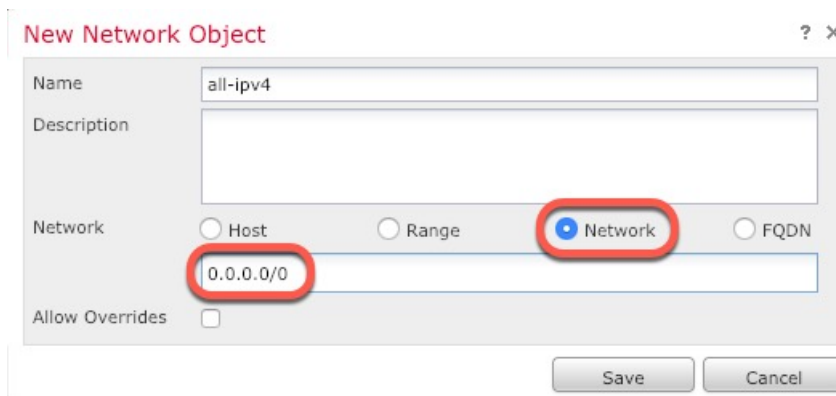
ステップ 5 [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。



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。

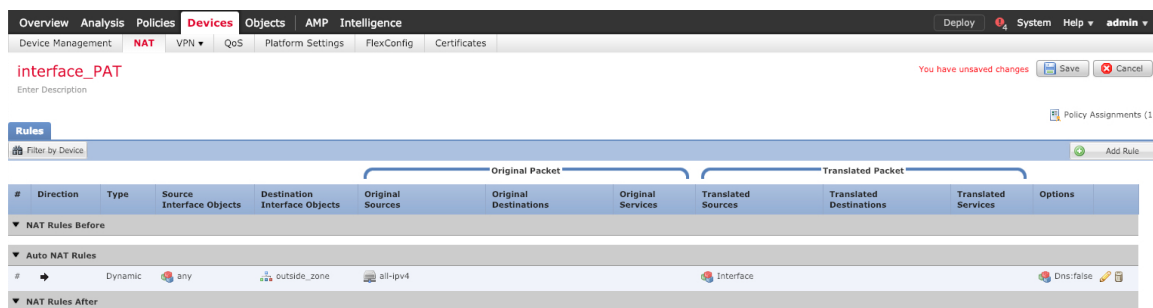


- (注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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

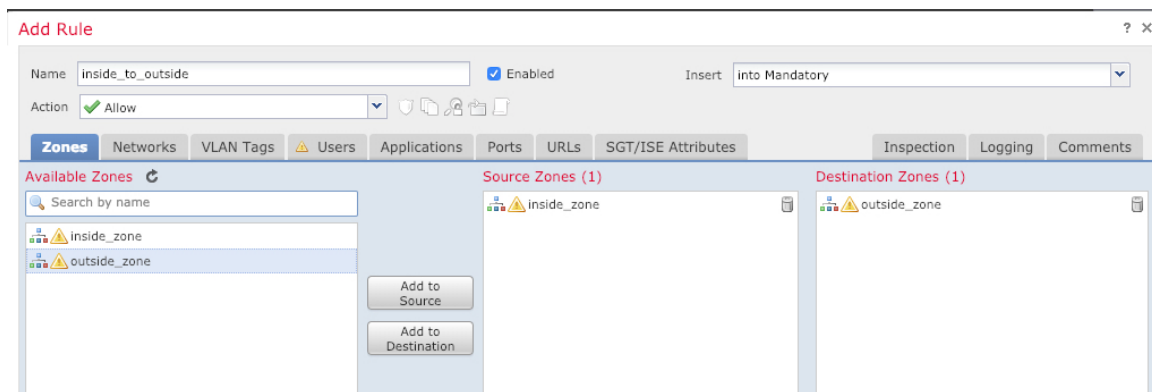
FTDv を FMC に登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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。

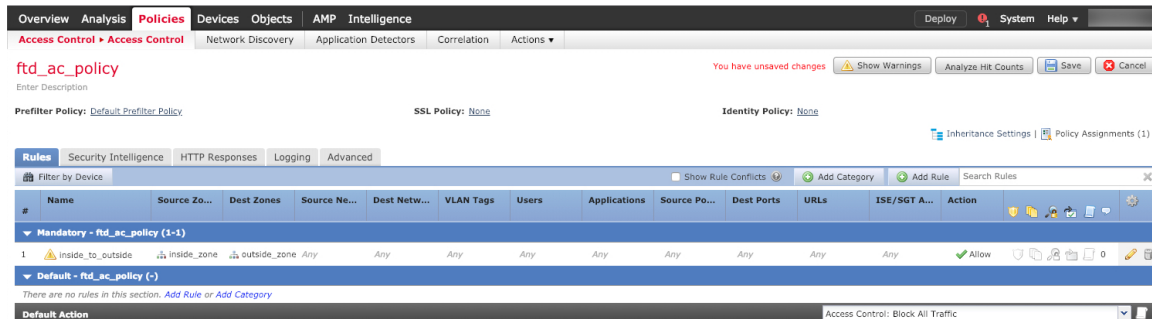


- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside_to_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

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。



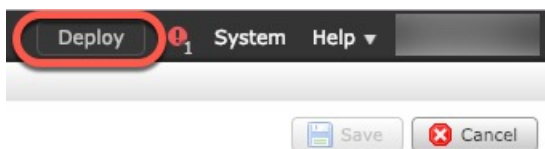
ステップ 4 [保存 (Save)] をクリックします。

設定の展開

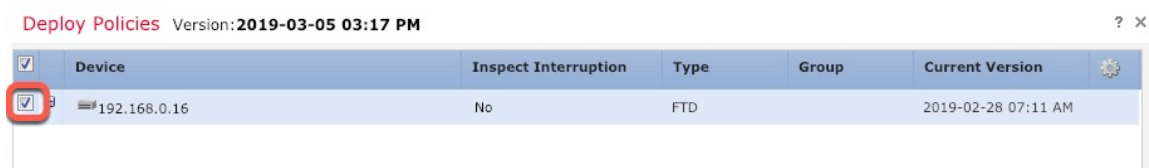
設定の変更を FTDv に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

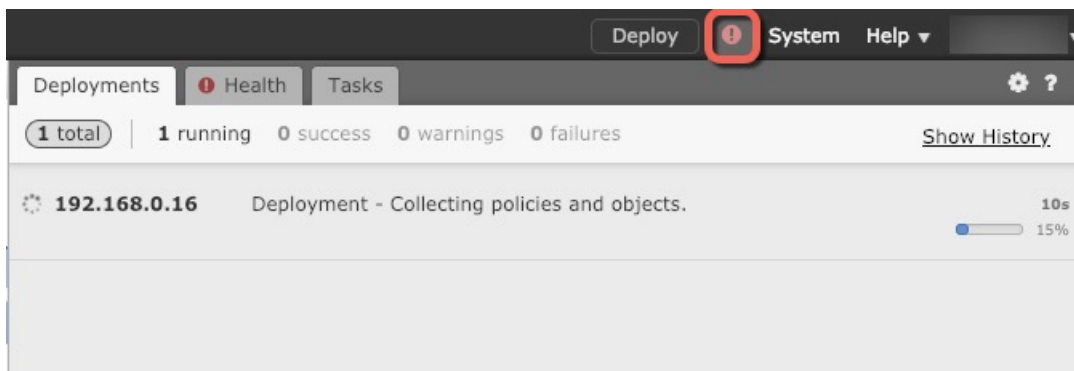
ステップ 1 右上の [展開 (Deploy)] をクリックします。



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。



第 5 章

Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理

この章では、FDM 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。高可用性ペアを展開する場合は、FDM のコンフィギュレーションガイドを参照してください。

- [Firepower Device Manager を使用した Firepower Threat Defense Virtual について \(65 ページ\)](#)
- [初期設定 \(66 ページ\)](#)
- [Firepower Device Manager でデバイスを設定する方法 \(69 ページ\)](#)

Firepower Device Manager 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 の管理には Firepower Device Manager (FDM) を使用できます。これは、一部の Firepower Threat Defense モデルに組み込まれている Web ベースのデバイスセットアップ ウィザードです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Firepower Device Manager の代わりに Firepower Management Center を使用してデバイスを設定します。詳細については、[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 \(47 ページ\)](#) を参照してください。

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。

デフォルト設定

FTDv のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマートライセンスを使用する場合やシステムデータベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、**Management 0-0** と **GigabitEthernet 0-1** (内部) の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに **Management 0-0** を接続することもできます。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

FTDv は、初回起動時に少なくとも 4 つのインターフェイスで電源がオンになる必要があります。

- 仮想マシン上の 1 番目のインターフェイス (**Management 0-0**) は、管理インターフェイスです。
- 仮想マシンでの 2 番目のインターフェイスは診断インターフェイス (**Diagnostic0-0**) です。
- 仮想マシン上の 3 番目のインターフェイス (**GigabitEthernet 0-0**) は、外部インターフェイスです。
- 仮想マシン上の 4 番目のインターフェイス (**GigabitEthernet 0-1**) は、内部インターフェイスです。

データトラフィック用に最大 6 つのインターフェイスを追加し、合計で 8 つのデータインターフェイスを使用できます。追加のデータインターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データインターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。「VMware インターフェイスの設定」を参照してください。

初期設定

FTDv の機能をネットワークで正しく動作させるには、初期設定を完了する必要があります。これには、セキュリティアプライアンスをネットワークに挿入して、インターネットまたは他の上流に位置するルータに接続するために必要なアドレスの設定が含まれます。2 つの方法のいずれかでシステムの初期設定を行うことができます。

- FDM Web インターフェイスの使用（推奨）。FDM は Web ブラウザで実行します。このインターフェイスを使用して、システムを設定、管理、モニターできます。
- コマンドライン インターフェイス（CLI）セットアップウィザードを使用します（オプション）。FDM の代わりに CLI のセットアップウィザードを初期設定に使用できます。またトラブルシューティングに CLI を使用できます。システムの設定、管理、監視には引き続き FDM 使用します。「Firepower Threat Defense CLI ウィザードの起動（オプション）」を参照してください。

次のトピックでは、これらのインターフェイスを使用してシステムの初期設定を行う方法について説明します。

Firepower Device Manager の起動

Firepower Device Manager（FDM）を使用して、システムの構成、管理、モニターを行います。ブラウザで設定可能な機能を、コマンドラインインターフェイス（CLI）で設定することはできません。セキュリティ ポリシーを実装するには、Web インターフェイスを使用する必要があります。

Firefox、Chrome、Safari、Edge ブラウザの最新バージョンを使用します。



(注) 初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（[高度な詳細（Advanced Details）]>[ユーザーデータ（User Data）]）していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは 5 分間ロックされます。再度ログインを試みる前に待機する必要があります。

手順

- ステップ 1** ブラウザを使用して FDM にログインします。CLI での初期設定を完了していない場合は、Firepower Device Manager を **https:ip-address** で開きます。このアドレスは次のいずれかになります。
 - 管理アドレス。（ほとんどのプラットフォームの）デフォルトでは、管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。
 - FTDv が Microsoft Azure や Amazon Web Services などのパブリッククラウド環境に展開されている場合、パブリック IP アドレスはパブリックアドレスのプールから FTDv インスタンスに自動的に割り当てられます。クラウドダッシュボードからパブリック IP アドレスを見つけます。
- ステップ 2** ユーザー名 **admin** とデフォルトのパスワードでログインします。

バージョン 7.0 以降では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義 ([高度な詳細 (Advanced Details)] > [ユーザーデータ (User Data)]) していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

以前のリリースでは、デフォルトの管理者パスワードは **Admin123** でした。

ステップ 3 これがシステムへの初めてのログインであり、CLI セットアップウィザードを使用していない場合、エンドユーザーライセンス契約を読んで承認し、管理パスワードを変更するように求められます。続行するには、これらの手順を完了する必要があります。

ステップ 4 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)] をクリックします。

(注) [次へ (Next)] をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

a) [外部インターフェイス (Outside Interface)]: これは、ゲートウェイモードまたはルータに接続するためのデータポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

[IPv4 の設定 (Configure IPv4)]: 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv4 アドレスを設定しないという選択肢もあります。

[IPv6 の設定 (Configure IPv6)]: 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b) [管理インターフェイス (Management Interface)]

[DNS サーバ (DNS Servers)]: システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻りたい場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名 (Firewall Hostname)]: システムの管理アドレスのホスト名です。

(注) デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスを設定する場合は、アウトバウンドとインバウンドのトラフィックに対してシステムから 2 つのデフォルトアクセスルールが提供されます。初期セットアップ後に、これらのアクセスルールに戻って編集できます。

ステップ 5 システム時刻を設定し、[次へ (Next)] をクリックします。

a) [タイムゾーン (Time Zone)]: システムのタイムゾーンを選択します。

- b) [NTPタイムサーバ (NTP Time Server)]: デフォルトの NTP サーバを使用するか、使用している NTPサーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ6 システムのスマートライセンスを設定します。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager (SSM) のアカウントにログインし、新しいトークンを作成して、編集ボックスにそのトークンをコピーします。

評価ライセンスを使用するには、[登録せずに90日間の評価期間を開始する (Start 90 day evaluation period without registration)]を選択します。後でデバイスを登録し、スマートライセンスを取得するには、メニューからデバイスの名前をクリックして [デバイスダッシュボード (Device Dashboard)]に進み、[スマートライセンス (Smart Licenses)]グループのリンクをクリックします。

ステップ7 [完了 (Finish)]をクリックします。

次のタスク

- Firepower Device Manager を使用してデバイスを設定します。「[Firepower Device Manager でデバイスを設定する方法 \(69 ページ\)](#)」を参照してください。

Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバー。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

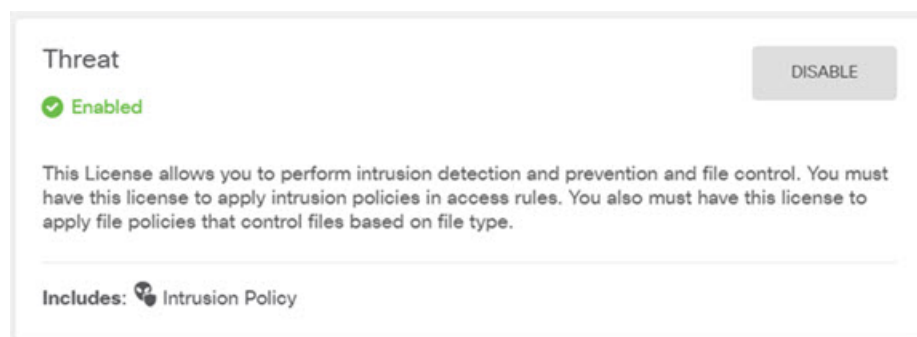
ステップ 1 [デバイス (Device)] を選択してから、[スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。

使用するオプションのライセンス ([脅威 (Threat)]、[マルウェア (Malware)]、[URL]) でそれぞれ [有効化 (Enable)] をクリックします。セットアップ中にデバイスを登録した場合は、必要な RA VPN ライセンスも有効にできます。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。[登録の要求 (Request Register)] をクリックして、手順に従います。評価ライセンスの有効期限が切れる前に登録してください。

たとえば、有効な脅威ライセンスは次のようになります。

図 2: 有効な脅威ライセンス



ステップ 2 他のインターフェイスを設定した場合は、[デバイス (Device)] を選択してから、[インターフェイス (Interfaces)] グループの [設定の表示 (View Configuration)] をクリックして、各インターフェイスを設定します。

他のインターフェイスのブリッジグループを作成するか、別々のネットワークを設定するか、または両方の組み合わせを設定できます。各インターフェイスの [編集 (Edit)] アイコン (🔗) をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」(DMZ) として使用するためのインターフェイスを構成します。完了したら [保存 (Save)] をクリックします。

図 3: インターフェイスの編集

Edit Physical Interface

Interface Name: Status:

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type: ▾

IP Address and Subnet Mask: /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

ステップ 3 新しいインターフェイスを構成する場合は、[オブジェクト (Objects)] を選択し、目次から [セキュリティゾーン (Security Zones)] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーンオブジェクトを編集する必要があります。

次の例では、DMZ インターフェイスのために新しい DMZ ゾーンを作成する方法を示します。

図 4: セキュリティゾーンオブジェクト

ステップ 4 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [DHCPサーバー (DHCP Server)] を選択してから、[DHCPサーバー (DHCP Servers)] タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバーがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバーをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

[構成 (Configuration)] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例では、アドレスプールの 192.168.4.50 ~ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。

図 5: DHCPサーバー

ステップ 5 [デバイス (Device)] を選択してから、[ルーティング (Routing)] グループで [設定の表示 (View Configuration)] (または [最初のスタティックルートを作成 (Create First Static Route)]) をクリックし、デフォルトルートを作成します。

デフォルトルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (::0/0) です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルトルートをすでに持っていることがあります。

(注) このページで定義したルートは、データインターフェイス用のみです。管理インターフェイスには影響しません。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルトルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。[ゲートウェイ (Gateway)] の下部の [新しいネットワークを作成する (Create New Network)] ドロップダウンリストをクリックしてこのオブジェクトを作成することができます。

図 6: デフォルトルート

The screenshot shows the 'Add Static Route' configuration page. The 'Protocol' section has 'IPv4' selected with a radio button. The 'Gateway' field contains 'isp-gateway'. The 'Interface' field contains 'outside'. The 'Metric' field contains '1'. The 'Networks' section has a '+' button and a dropdown menu showing 'any-ipv4'.

ステップ 6 [ポリシー (Policies)] を選択してネットワークのセキュリティポリシーを作成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーン間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合、全インターフェイスに対する

インターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

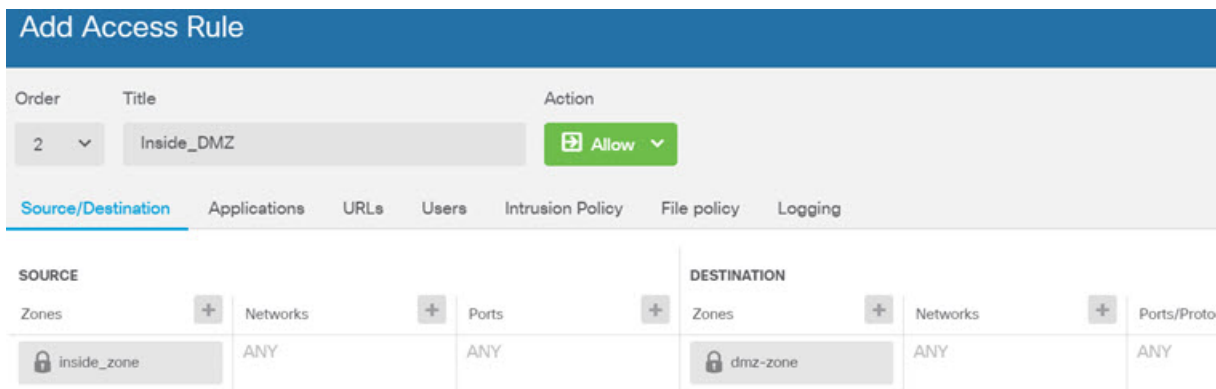
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセスルールを微調整できます。次のポリシーを設定できます。

- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)] : 個々のユーザーにネットワークアクティビティを関連付ける、またはユーザーまたはユーザーグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティインテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT] (ネットワークアドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザーグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル (マルウェア) ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [侵入 (Intrusion)] : 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 7: アクセス コントロール ポリシー




ステップ 7 [デバイス (Device)] を選択してから、[更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 8 メニューの [導入 (Deploy)] ボタンをクリックし、[今すぐ導入する (Deploy Now)] ボタン



() をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

次のタスク

Firepower Device Manager による Firepower Threat Defense Virtual の管理の詳細については、[『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』](#) または Firepower Device Manager のオンラインヘルプを参照してください。

このドキュメントは、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。

