



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

初版：2018 年 8 月 23 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 Azure の 利用開始

Cisco 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、ワークロードを実行します。

この章では、Azure マーケットプレイス内における 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 または Firepower Device Manager を使用できます。その他の管理オプションを使用できる場合もあります。

- [FTDv と Microsoft Azure クラウドについて \(1 ページ\)](#)
- [FTDv および Azure の前提条件および要件 \(2 ページ\)](#)
- [FTDv および Azure のガイドラインと制限事項 \(3 ページ\)](#)
- [Firepower デバイスの管理方法 \(5 ページ\)](#)
- [Azure 上の FTDv のネットワークトポロジの例 \(6 ページ\)](#)
- [導入時に作成されるリソース \(7 ページ\)](#)
- [Accelerated Networking \(AN\) \(8 ページ\)](#)
- [Azure ルーティング \(9 ページ\)](#)
- [仮想ネットワーク内の VM のルーティング設定 \(9 ページ\)](#)
- [IP アドレス \(10 ページ\)](#)

## FTDv と Microsoft Azure クラウドについて

FTDv (Firepower Threat Defense Virtual) は、Microsoft Azure マーケットプレイスに統合され、次のインスタンスタイプをサポートします。

- Standard D3 (4 つの vCPU、14 GB、4 つの vNIC)
- Standard D3\_v2 (4 つの vCPU、14 GB、4 つの vNIC)

- Standard D4\_v2 (8 つの vCPU、28 GB、8 つの vNIC) (バージョン 6.5 の新機能)
- Standard D5\_v2 (16 の vCPU、56 GB、8 つの vNIC) (バージョン 6.5 の新機能)
- Standard\_D8s\_v3—8 vCPU、32 GB、4vNIC (バージョン 7.1 の新機能)
- Standard\_D16s\_v3—16 vCPU、64 GB、8vNIC (バージョン 7.1 の新機能)
- Standard\_F8s\_v2—8 vCPU、16 GB、4vNIC (バージョン 7.1 の新機能)
- Standard\_F16s\_v2—16 vCPU、32 GB、8vNIC (バージョン 7.1 の新機能)

## FTDv および Azure の前提条件および要件

### 前提条件

- Microsoft Azure アカウント。 <https://azure.microsoft.com/en-us/> で 1 つ作成できます。  
Azure でアカウントを作成した後は、ログインしてマーケットプレイスから Cisco Firepower Threat Defense を検索し、「Cisco Firepower NGFW Virtual (NGFWv)」を選択します。
- Cisco スマートアカウント。 [Cisco Software Central](#) で作成できます。  
FTDv のライセンス。Firepower システムで使用できる機能ライセンスの概要 (ヘルプリンクを含む) については、『[Cisco Firepower System Feature Licenses](#)』を参照してください。
- FTDv と Firepower System の互換性については、『[Cisco Firepower Threat Defense Virtual Compatibility](#)』を参照してください。

### 通信パス

- 管理インターフェイス — FTDv を Firepower Management Center に接続するために使用されます。



(注) 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。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。

- 診断インターフェイス — 診断およびレポートに使用されます。通過トラフィックには使用できません。
- 内部インターフェイス (必須) — Firepower Threat Defense Virtual を内部ホストに接続するために使用されます。

- 外部インターフェイス（必須） — Firepower Threat Defense Virtual を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。

## FTDv および Azure のガイドラインと制限事項

### サポートされる機能

- ルーテッドファイアウォール モードのみ
- Azure Accelerated Networking (AN)
- 管理モード：次の 2 つのいずれかを選択できます。
  - Firepower Management Center を使用して FTDv を管理することができます。「[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理（67 ページ）](#)」を参照してください。
  - 統合 Firepower Device Manager を使用して FTDv を管理することができます。「[Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理（85 ページ）](#)」を参照してください（バージョン 6.5 以上）。



---

(注) PAYG ライセンスは、FDM (Firepower Device Manager) モードで展開されている FTDv デバイスではサポートされていません。

---

- パブリック IP アドレス：Management 0/0 および GigabitEthernet 0/0 にパブリック IP アドレスが割り当てられます。

必要に応じて、その他のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、[パブリック IP アドレス \[英語\]](#) を参照してください。

- インターフェイス：
  - FTDv デフォルトでは 4 つの vNIC を使用して展開されます。
  - より大規模なインスタンスのサポートにより、最大 8 つの vNIC を使用して FTDv を展開できます。
  - FTDv の展開に vNIC を追加するには、Microsoft の「[仮想マシンのネットワーク インターフェイスの追加と削除](#)」に示されるガイドラインに従います。
  - FTDv インターフェイスは、マネージャを使用して設定します。インターフェイスのサポートと設定の詳細については、管理プラットフォーム (Firepower Management Center または Firepower Device Manager) の構成ガイドを参照してください。

## FTDv スマートライセンスのパフォーマンス階層

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

表 1: FTDv 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	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）。
- PAYG（Pay As You Go）ライセンス。顧客がシスコ スマート ライセンシングを購入せずに FTDv を実行できる従量制課金モデル。登録された PAYG FTDv デバイスでは、ライセンス供与されたすべての機能（マルウェア、脅威、URL フィルタリング、VPN など）が有効になっています。ライセンス供与された機能は、FMC から編集または変更することはできません（バージョン 6.5 以上）。



（注） PAYG ライセンスは、FDM（Firepower Device Manager）モードで展開されている FTDv デバイスではサポートされていません。

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「Licensing the Firepower System」の章を参照してください。

## サポートされない機能

- ライセンス：
  - PLR（パーマネントライセンス予約）
  - PAYG（Pay As You Go）（バージョン 6.4 以前）
- ネットワーキング（これらの制限事項の多くは Microsoft Azure の制約）：
  - ジャンボフレーム
  - IPv6

- 802.1Q VLAN
- トランスペアレントモードおよびその他のレイヤ2機能。ブロードキャストなし、マルチキャストなし。
- Azure の観点からデバイスが所有していないIPアドレスのプロキシARP（一部のNAT機能に影響）
- 無差別モード（サブネットトラフィックのキャプチャなし）
- インラインセットモード、パッシブモード



(注) Azure ポリシーにより FTDv のトランスペアレントファイアウォールモードやインラインモードでの動作は阻止されます。これは、Azure ポリシーがインターフェイスの無差別モードでの動作を許可していないためです。

- ERSPAN（GRE を使用。これは Azure では転送されません）
- 管理：
  - コンソールアクセス。管理は Firepower Management Center を使用してネットワーク上で実行されます（SSH はセットアップおよびメンテナンスの一部の作業に使用可能）
  - Azure ポータルの「パスワードのリセット」機能
  - コンソールベースのパスワード回復。ユーザーはコンソールにリアルタイムアクセスができないため、パスワードの回復もできません。パスワード回復イメージの起動ができません。唯一の対応手段は、新規の Firepower Threat Defense Virtual VM を導入することです。
- 高可用性（アクティブ/スタンバイ）
- クラスタリング
- VM のインポート/エクスポート
- FDM（Firepower Device Manager）ユーザーインターフェイス（バージョン6.4 以前）

## 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](#)』 [英語]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。

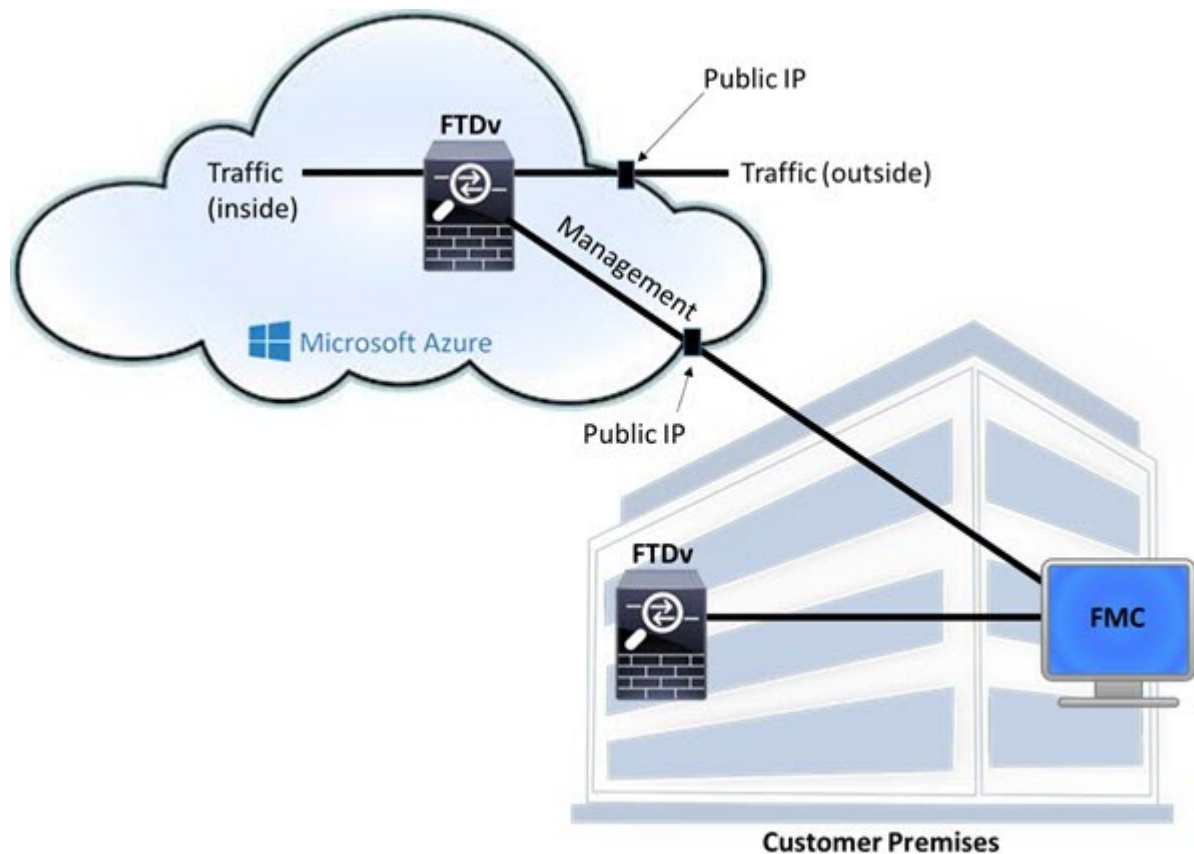


**注意** 現在、シスコには FDM Firepower 設定を FMC に移行するオプションはありません。その逆も同様です。Firepower デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

## Azure 上の FTDv のネットワークトポロジの例

次の図は、Azure 内でルーテッドファイアウォールモードに設定された Firepower Threat Defense Virtual の代表的なトポロジを示しています。最初に定義されるインターフェイスが常に管理インターフェイスであり、Management 0/0 および GigabitEthernet 0/0 のみにパブリック IP アドレスが割り当てられます。





## 導入時に作成されるリソース

Azure に Firepower Threat Defense Virtual を導入すると、次のリソースが作成されます。

- Firepower Threat Defense 仮想マシン (VM)
- リソースグループ
  - Firepower Threat Defense Virtual は常に新しいリソースグループに導入されます。ただし、Firepower Threat Defense Virtual を別のリソースグループ内の既存仮想ネットワークにアタッチすることはできません。
- 4 枚の NIC (名前は、*vm name-Nic0*、*vm name-Nic1*、*vm name-Nic2*、*vm name-Nic3*)

これらの NIC は、Firepower Threat Defense Virtual インターフェイスの Management、Diagnostic 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1 にそれぞれマッピングされます。
- セキュリティグループ (名前は、*vm name-mgmt-SecurityGroup*)

このセキュリティグループは VM の Nic0 にアタッチされます。Nic0 は Firepower Threat Defense Virtual 管理インターフェイスにマッピングされています。

このセキュリティグループには、Firepower Management Center インターフェイス (TCP ポート 8305) 用の SSH (TCP ポート 22) および管理トラフィックを許可するルールが含まれます。導入後に、これらの値を変更できます。

- パブリック IP アドレス (導入時に選択した値に従って命名)。

任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、「[パブリック IP アドレス](#)」を参照してください。

- [新規ネットワーク (New Network)] オプションを選択すると、4 つのサブネットを備えた仮想ネットワークが作成されます。
- サブネットごとのルーティングテーブル (既存の場合は最新のもの)

テーブルには、*subnet name-FTDv-RouteTable* という名前が付けられます。

各ルーティングテーブルには、Firepower Threat Defense Virtual IP アドレスを持つ他の 3 つのサブネットへのルートがネクストホップとして含まれています。トラフィックを他のサブネットまたはインターネットに到達させる必要がある場合は、デフォルトルートを追加することもできます。

- 選択したストレージアカウントの起動時診断ファイル

起動時診断ファイルは、ブロブ (サイズの大きいバイナリオブジェクト) 内に配置されます。

- 選択したストレージアカウントのブロブおよびコンテナ VHD にある 2 つのファイル (名前は、*vm name-disk.vhd* および *vm name-<uuid>.status*)
- ストレージアカウント (既存のストレージアカウントが選択されていない場合)



(注) VM を削除すると、保持を希望する任意のリソースを除き、これらの各リソースを個別に削除する必要があります。

## Accelerated Networking (AN)

Azure の Accelerated Networking (AN) 機能により、VM に対するシングルルート I/O 仮想化 (SR-IOV) が可能になります。これにより、VMNIC がハイパーバイザをバイパスしてその下の PCIe カードに直接アクセスできるようになり、ネットワークが高速化します。AN は VM のスループットパフォーマンスを大幅に向上させ、コアの追加 (つまり VM の拡大) にも対応します。

AN はデフォルトではディセーブルになっています。Azure は、事前プロビジョニングされた仮想マシンでの AN の有効化をサポートしています。Azure で VM を停止し、ネットワークカードのプロパティを更新して *enableAcceleratedNetworking* パラメータを *true* に設定するだけです。

Microsoft ドキュメントの「[既存の VM で高速ネットワークを有効にする](#)」を参照してください。その後、VM を再起動します。

## Azure ルーティング

Azure 仮想ネットワークサブネットでのルーティングは、サブネットの有効ルーティングテーブルによって決定されます。有効ルーティングテーブルは、組み込みのシステムルートとユーザー定義ルート（UDR）テーブルが組み合わされたものです。



(注) 有効ルーティングテーブルは VM NIC のプロパティの下に表示されます。

ユーザー定義のルーティングテーブルは表示および編集できます。システムルートとユーザー定義ルートを組み合わせて有効ルーティングテーブルを構成する際に、最も固有なルート（同位のものを含め）がユーザー定義ルーティングテーブルに含められます。システムルーティングテーブルには、Azure の仮想ネットワーク インターネット ゲートウェイを指すデフォルトルート（0.0.0.0/0）が含まれます。また、システム ルーティング テーブルには、Azure の仮想ネットワーク インフラストラクチャ ゲートウェイを指すネクストホップとともに、他の定義済みのサブネットへの固有ルートが含まれます。

Firepower Threat Defense Virtual 経由でトラフィックをルーティングするには、各データサブネットに関連付けられたユーザー定義ルーティングテーブルのルートを追加または更新する必要があります。対象トラフィックは、そのサブネット上の Firepower Threat Defense Virtual IP アドレスをネクストホップとして使用してルーティングする必要があります。また、必要に応じて、0.0.0.0/0 のデフォルトルートを Firepower Threat Defense Virtual IP のネクストホップとともに追加できます。

システム ルーティング テーブル内は既存の固有ルートであるために、Firepower Threat Defense Virtual をネクストホップとして指定する固有ルートをユーザー定義ルーティングテーブルに追加する必要があります。追加しない場合、ユーザー定義テーブル内のデフォルトルートではなく、システム ルーティング テーブル内のより固有なルートが選択され、トラフィックが Firepower Threat Defense Virtual をバイパスしてしまいます。

## 仮想ネットワーク内の VM のルーティング設定

Azure 仮想ネットワーク内のルーティングは、クライアントの特定のゲートウェイ設定ではなく、有効なルーティングテーブルに依存します。仮想ネットワーク内で稼働するクライアントは、DHCPによって、それぞれのサブネット上の 1 アドレスとなるルートを指定されることがあります。これはプレースホルダで、仮想ネットワークのインフラストラクチャ仮想ゲートウェイにパケットを送信するためにだけ使用されます。パケットは、VM から送信されると、有効なルーティングテーブル（ユーザー定義のテーブルによって変更された）に従ってルーティングされます。有効なルーティングテーブルは、クライアントでゲートウェイが 1 とし

て、または Firepower Threat Defense Virtual アドレスとして設定されているかどうかに関係なく、ネクストホップを決定します。

Azure VM ARP テーブルには、すべての既知のホストに対して同じ MAC アドレス (1234.5678.9abc) が表示されます。これによって、Azure VM からのすべてのパケットが、有効なルーティングテーブルを使用してパケットのパスを決定する Azure ゲートウェイに到達するように保証されます。

## IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- Firepower Threat Defense Virtual 上の最初の NIC (Management にマッピングされる) には、アタッチ先のサブネット内のプライベート IP アドレスが付与されます。

パブリック IP アドレスは、プライベート IP アドレスに関連付けられる場合があり、Azure インターネットゲートウェイは NAT 変換を処理します。

Firepower Threat Defense Virtual の導入後に、パブリック IP アドレスをデータインターフェイス (GigabitEthernet0/0 など) に関連付けることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、[パブリック IP アドレス \[英語\]](#) を参照してください。

- ダイナミックパブリック IP アドレスは、Azure の停止/開始サイクル中に変化する可能性があります。ただし、Azure の再起動中および Firepower Threat Defense Virtual のリロード中は保持されています。
- スタティックパブリック IP アドレスは、Azure 内でそれらを変更するまで変わりません。
- Firepower Threat Defense Virtual インターフェイスは、DHCP を使用してそれらの IP アドレスを設定することができます。Azure インフラストラクチャは、Azure で設定された IP アドレスが確実に Firepower Threat Defense Virtual インターフェイスに割り当てられるように動作します。



## 第 2 章

# Firepower Threat Defense Virtual の展開

この章では、Azure 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。

- [Azure の展開について \(11 ページ\)](#)
- [エンドツーエンドの手順 \(12 ページ\)](#)
- [ソリューションテンプレートを使用した Azure マーケットプレイスからの展開 \(14 ページ\)](#)
- [VHD およびリソーステンプレートを使用した Azure からの展開 \(17 ページ\)](#)

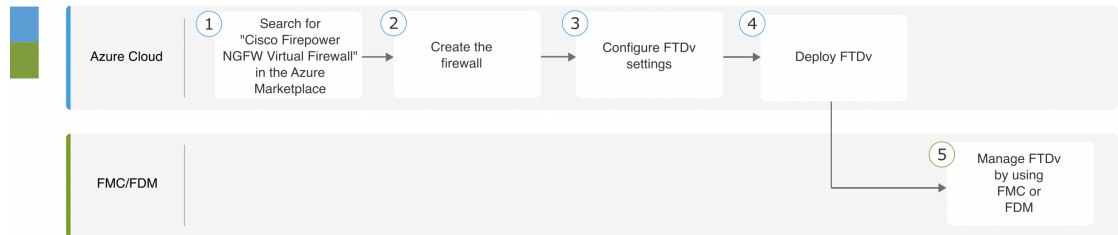
## Azure の展開について

テンプレートを使用して、Azure に FTDv を展開できます。2 種類のテンプレートが用意されています。

- **Azure マーケットプレイスのソリューションテンプレート**：Azure マーケットプレイスで使用可能なソリューションテンプレートを使用すると、Azure ポータルを使用して FTDv を展開できます。既存のリソースグループおよびストレージアカウントを使用して（あるいは、それらを新規に作成して）、仮想アプライアンスを展開できます。ソリューションテンプレートを使用するには、「[ソリューションテンプレートを使用した Azure マーケットプレイスからの展開 \(14 ページ\)](#)」を参照してください。
- **VHD からの管理対象イメージを使用したカスタムテンプレート**（<https://software.cisco.com/download/home> から入手可能）：マーケットプレイススペースの展開の他に、圧縮仮想ディスク（VHD）が用意されています。これを Azure にアップロードして、Azure に FTDv を展開するプロセスを簡素化できます。管理対象イメージと 2 つの JSON ファイル（テンプレートファイルおよびパラメータファイル）を使用して、単一の協調操作で FTDv のすべてのリソースを導入およびプロビジョニングできます。カスタムテンプレートを使用するには、「[VHD およびリソーステンプレートを使用した Azure からの展開 \(17 ページ\)](#)」を参照してください。

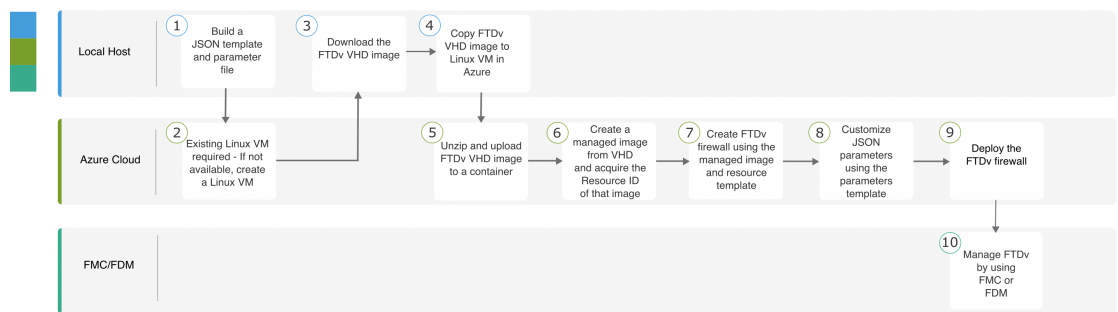
## エンドツーエンドの手順

次のフローチャートは、ソリューションテンプレートを使用して Microsoft Azure に FTDv を展開するワークフローを示しています。



	ワークスペース	手順
①	Azure Cloud	ソリューションテンプレートを使用した <a href="#">Azure マーケットプレイスからの展開</a> : Azure マーケットプレイスで「Cisco Firepower NGFW Virtual Firewall」を検索します。
②	Azure Cloud	ソリューションテンプレートを使用した <a href="#">Azure マーケットプレイスからの展開</a> : ファイアウォールを作成します。
③	Azure Cloud	ソリューションテンプレートを使用した <a href="#">Azure マーケットプレイスからの展開</a> : FTDv 設定を構成します。
④	Azure Cloud	ソリューションテンプレートを使用した <a href="#">Azure マーケットプレイスからの展開</a> : FTDv を展開します。
⑤	FMC/FDM	FTDv の管理 : <ul style="list-style-type: none"> <li>• <a href="#">Firepower Management Center</a> を使用した <a href="#">Firepower Threat Defense Virtual</a> の管理</li> <li>• <a href="#">Firepower Device Manager</a> を使用した <a href="#">Firepower Threat Defense Virtual</a> の管理</li> </ul>

次のフローチャートは、VHD とリソーステンプレートを使用して Microsoft Azure に FTDv を展開するワークフローを示しています。





	ワークスペース	手順
①	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開 : JSON テンプレートとパラメータファイルを作成します。
②	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : 既存の Linux VM が必要です。利用できない場合は、Linux VM を作成します。 <ul style="list-style-type: none"> <li>• Azure CLI による Linux 仮想マシンの作成</li> <li>• Azure ポータルによる Linux 仮想マシンの作成</li> </ul>
③	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開 : Cisco ダウンロードソフトウェア ページから FTDv VHD イメージをダウンロードします。
④	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開 : Azure の Linux VM に FTDv VHD イメージをコピーします
⑤	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : FTDv VHD イメージを解凍し、コンテナにアップロードします。
⑥	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : VHD から管理対象イメージを作成し、イメージのリソース ID を取得します。
⑦	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : 管理対象イメージとリソーステンプレートを使用して FTDv ファイアウォールを作成します。
⑧	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : パラメータテンプレートを使用して JSON パラメータをカスタマイズします。
⑨	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開 : FTDv ファイアウォールを展開します。
⑩	FMC/FDM	FTDv の管理 : <ul style="list-style-type: none"> <li>• Firepower Management Center を使用した Firepower Threat Defense Virtual の管理</li> <li>• Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理</li> </ul>

# ソリューションテンプレートを使用した Azure マーケットプレイスからの展開

次の手順は、Azure マーケットプレイスで利用できる FTDv のソリューションテンプレートを展開する方法を示しています。これは、Microsoft Azure 環境で FTDv をセットアップする手順の概略です。Azure のセットアップの詳細な手順については、「[Azure を試してみる](#)」を参照してください。

Azure に FTDv を導入すると、リソース、パブリック IP アドレス、ルートテーブルなどのさまざまな設定が自動的に生成されます。導入後に、これらの設定をさらに管理できます。たとえば、アイドルタイムアウト値を、デフォルトの短いタイムアウトから変更することができます。



(注) [GitHub](#) リポジトリで利用できるカスタマイズ可能な ARM テンプレートについては、「[VHD およびリソーステンプレートを使用した Azure からの展開 \(17 ページ\)](#)」を参照してください。

## 手順

**ステップ 1** [Azure Resource Manager \(ARM\)](#) ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮要素を表示します。

**ステップ 2** [Azure マーケットプレイス (Azure Marketplace)] > [仮想マシン (Virtual Machines)] を順に選択します。

**ステップ 3** マーケットプレイスで「Cisco Firepower NGFW Virtual (FTDv)」を検索して選択し、[作成 (Create)] をクリックします。

**ステップ 4** 基本的な設定を行います。

- a) 仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

**重要** 既存の名前を使用している場合、導入は失敗します。

- b) **Byol** または **PAYG** のいずれかのライセンス方式を選択します。

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) を選択します。

シスコ スマート ライセンシングを購入せずに従量制課金モデルを使用するには、**PAYG** (Pay As You Go) ライセンスを選択します。



**重要** **PAYG** は、Firepower Management Center を使用して FTDv を管理する場合にのみ使用できます。

- c) FTDv 管理者のユーザー名を入力します。

(注) 「admin」という名前は Azure で予約されており、使用できません。

- d) 認証タイプとして、パスワードまたは SSH キーのいずれかを選択します。

パスワードを選択した場合は、パスワードを入力して確定します。

SSH キーを選択した場合は、リモート ピアの RSA 公開キーを指定します。

- e) FTDv の設定時にログインする際に **Admin** ユーザーアカウントで使用するパスワードを作成します。

- f) サブスクリプションを選択します。

- g) 新しいリソースグループを作成します。

FTDv は新しいリソースグループに導入する必要があります。既存のリソースグループに展開するオプションは、既存のリソースグループが空の場合にのみ機能します。

ただし、後の手順でネットワークオプションを設定する際に、FTDv を別のリソースグループ内に存在している仮想ネットワークへ接続できます。

- h) 地理的なロケーションを選択します。このロケーションは、導入で使用する全リソース (FTDv、ネットワーク、ストレージアカウントなど) で統一する必要があります。

- i) [OK] をクリックします。

#### ステップ 5 FTDv の設定項目を設定します。

- a) 仮想マシンのサイズを選択します。

- b) ストレージアカウントを選択します。

(注) 既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名には、小文字と数字のみを使用できます。

- c) パブリック IP アドレスを選択します。

選択したサブスクリプションとロケーションで使用可能なパブリック IP アドレスを選択するか、[新規作成 (Create new)] をクリックします。

新しいパブリック IP アドレスを作成する場合は、Microsoft が所有する IP アドレスのブロックの中から 1 つ取得するため、特定のアドレスを選択することはできません。インターフェイスに割り当てることができるパブリック IP アドレスの最大数は、Azure サブスクリプションに基づいています。

**重要** Azure は、デフォルトでダイナミックパブリック IP アドレスを作成します。VM を停止させて再起動すると、パブリック IP が変わることがあります。固定 IP アドレスを使用する場合は、スタティックアドレスを作成する必要があります。導入後にパブリック IP アドレスを変更して、ダイナミックアドレスからスタティックアドレスに変更することもできます。

- d) DNS ラベルを追加します。

(注) 完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、  
<dnslabel>.<location>.cloudapp.azure.com の形式になります。

e) 仮想ネットワークを選択します。

既存の Azure Virtual Network (VNet) を選択するか、新しいものを作成して、VNet の IP アドレス空間を入力できます。デフォルトでは、Classless Inter-Domain Routing (CIDR) の IP アドレスは 10.0.0.0/16 です。

f) FTDv ネットワーク インターフェイスで 4 つのサブネットを構成します。

- **FTDv 管理**インターフェイス (第 1 サブネット (Azure の Nic0) に接続)
- **FTDv 診断**インターフェイス (第 2 サブネット (Azure の Nic1) に接続)
- **FTDv 外部**インターフェイス (第 3 サブネット (Azure の Nic2) に接続)
- **FTDv 内部**インターフェイス (第 4 サブネット (Azure の Nic3) に接続)

g) [OK] をクリックします。

**ステップ 6** 構成サマリを確認し、[OK] をクリックします。

**ステップ 7** 利用条件を確認し、[購入 (Purchase)] をクリックします。

導入時間は Azure によって異なります。FTDv VM が実行されていることが Azure から報告されるまで待機します。

---

## 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 \(67 ページ\)](#)」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 \(85 ページ\)](#)」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。

# VHD およびリソーステンプレートを使用した Azure からの展開

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム FTDv イメージを作成できます。VHD イメージを使用して展開するには、Azure ストレージアカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスクイメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azure テンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。

## 始める前に

- FTDv テンプレートの展開には、JSON テンプレートおよび対応する JSON パラメータファイルが必要です。VHD および ARM テンプレートを使用した Azure への FTDv の導入例は、[Github](#)を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
  - この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM (Ubuntu 16.04 など) を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。
- VM を作成する必要がある場合は、次のいずれかの方法を使用します。
- [Azure CLI による Linux 仮想マシンの作成](#)
  - [Azure ポータルによる Linux 仮想マシンの作成](#)
- Azure サブスクリプションには、FTDv を展開する場所で使用可能なストレージアカウントが必要です。

## 手順

- 
- ステップ 1** [シスコ ダウンロード ソフトウェア](#) ページから FTDv 圧縮 VHD イメージをダウンロードします。
- a) [製品 (Products)] > [セキュリティ (Security)] > [ファイアウォール (Firewalls)] > [次世代ファイアウォール (NGFW) (Next-Generation Firewalls (NGFW))] > [Firepower NGFW Virtual] に移動します。
  - b) [Firepower Threat Defense ソフトウェア (Firepower Threat Defense Software)] をクリックします。
- 手順に従ってイメージをダウンロードしてください。
- たとえば、Cisco\_Firepower\_Threat\_Defense\_Virtual-6.2.3-81.vhd.bz2 です。
- ステップ 2** Azure の Linux VM に圧縮 VHD イメージをコピーします。

Azure との間でファイルをやり取りするために使用できるオプションが数多くあります。この例では、SCP（セキュアコピー）を示します。

```
# scp /username@remotehost.com/dir/Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2 <linux-ip>
```

**ステップ 3** Azure の Linux VM にログインし、圧縮 VHD イメージをコピーしたディレクトリに移動します。

**ステップ 4** FTDv VHD イメージを解凍します。

ファイルを解凍または圧縮解除するために使用できるオプションが数多くあります。この例では Bzip2 ユーティリティを示しますが、Windows ベースのユーティリティも正常に機能します。

```
# bunzip2 Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2
```

**ステップ 5** Azure ストレージアカウントのコンテナに VHD をアップロードします。既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウント名には、小文字と数字のみを使用できます。

ストレージアカウントに VHD をアップロードするために使用できるオプションが数多くあります。AzCopy、Azure Storage Copy Blob API、Azure Storage Explorer、Azure CLI、Azure ポータルなどです。FTDv VHD ほどの容量があるファイルには、Azure ポータルを使用しないことを推奨します。

次の例は、Azure CLI を使用した構文を示しています。

```
azure storage blob upload \
  --file <unzipped vhd> \
  --account-name <azure storage account> \
  --account-key yX7txxxxxxxxldnQ== \
  --container <container> \
  --blob <desired vhd name in azure> \
  --blobtype page
```

**ステップ 6** VHD から管理対象イメージを作成します。

- a) Azure ポータルで、[イメージ (Images)] を選択します。
- b) [追加 (Add)] をクリックして、新しいイメージを作成します。
- c) 次の情報を入力します。
  - [名前 (Name)] : 管理対象イメージのユーザー定義の名前を入力します。
  - [サブスクリプション (Subscription)] : ドロップダウンリストからサブスクリプションを選択します。
  - [リソースグループ (Resource group)] : 既存のリソースグループを選択するか、新しいリソースグループを作成します。
  - [OS ディスク (OS disk)] : OS タイプとして Linux を選択します。
  - [ストレージブロッブ (Storage blob)] : ストレージアカウントを参照して、アップロードした VHD を選択します。
  - [アカウントタイプ (Account type)] : ドロップダウンリストから [標準 (HDD) (Standard (HDD))] を選択します。

- [ホストキャッシング (Host caching)] : ドロップダウンリストから [読み取り/書き込み (Read/write)] を選択します。
- [データディスク (Data disks)] : デフォルトのままにしておきます。データディスクを追加しないでください。

d) [作成 (Create)] をクリックします。

「イメージが正常に作成されました (Successfully created image)」というメッセージが [通知 (Notifications)] タブの下に表示されるまで待ちます。

(注) 管理対象イメージが作成されたら、アップロードした VHD とアップロードストレージアカウントを削除できます。

**ステップ 7** 新規に作成した管理対象イメージのリソース ID を取得します。

Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。リソース ID は、この管理対象イメージから新しい FTDv ファイアウォールを展開するときに必要になります。

- a) Azure ポータルで、[イメージ (Images)] を選択します。
- b) 前のステップで作成した管理対象イメージを選択します。
- c) [概要 (Overview)] をクリックして、イメージのプロパティを表示します。
- d) クリップボードにリソース ID をコピーします。

リソース ID は、次の形式を取ります。

```
/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>
```

**ステップ 8** 管理対象イメージおよびリソーステンプレートを使用して、FTDv ファイアウォールを構築します。

- a) [新規 (New)] を選択し、オプションから選択できるようになるまで [テンプレート展開 (Template Deployment)] を検索します。
- b) [作成 (Create)] を選択します。
- c) [エディタで独自のテンプレートを構築する (Build your own template in the editor)] を選択します。

カスタマイズできる空白のテンプレートが作成されます。VHD および ARM テンプレートを使用した Azure への FTDv の導入例は、[Github](#) を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。

- d) カスタマイズした JSON テンプレートコードをウィンドウに貼り付け、[保存 (Save)] をクリックします。
- e) ドロップダウンリストから [サブスクリプション (Subscription)] を選択します。
- f) 既存の [リソースグループ (Resource group)] を選択するか、新しいリソースグループを作成します。
- g) ドロップダウンリストから [ロケーション (Location)] を選択します。

- h) 前ステップからの管理対象イメージの[リソースID (Resource ID)]を[VM管理対象イメージID (Vm Managed Image Id)]フィールドに貼り付けます。

- ステップ 9** [カスタム展開 (Custom deployment)] ページの最上部にある [パラメータの編集 (Edit parameters)] をクリックします。カスタマイズできるパラメータテンプレートが作成されます。
- a) [ファイルのロード (Load file)] をクリックし、カスタマイズした FTDv パラメータファイルを参照します。VHD および ARM テンプレートを使用した Azure への FTDv の導入例は、[Github](#) を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
- b) カスタマイズした JSON パラメータコードをウィンドウに貼り付け、[保存 (Save)] をクリックします。
- ステップ 10** カスタム展開の詳細を確認します。[基本 (Basics)] と [設定 (Settings)] の情報 ([リソース ID (Resource ID)] など) が、想定した展開設定に一致することを確認します。
- ステップ 11** 利用規約を確認し、[上記の利用規約に同意します (I agree to the terms and conditions stated above)] チェックボックスをオンにします。
- ステップ 12** [購入 (Purchase)] をクリックし、管理対象イメージおよびカスタムテンプレートを使用して FTDv ファイアウォールを展開します。

テンプレートファイルとパラメータファイルに競合がなければ、展開が正常に完了しているはずです。

管理対象イメージは、同じサブスクリプションおよび地域内の複数の展開に使用できます。

---

### 次のタスク

- Azure で FTDv の IP 設定を更新します。



## 第 3 章

# Firepower Threat Defense Virtual Auto Scale for Azure の展開

- [Azure での FTDv の Auto Scale ソリューション](#) (21 ページ)
- [導入パッケージのダウンロード](#) (24 ページ)
- [Auto Scale ソリューションのコンポーネント](#) (24 ページ)
- [Auto Scale ソリューションの前提条件](#) (26 ページ)
- [Auto Scale の展開](#) (43 ページ)
- [Auto Scale ロジック](#) (60 ページ)
- [Auto Scale のロギングとデバッグ](#) (61 ページ)
- [Auto Scale のガイドラインと制約事項](#) (62 ページ)
- [Auto Scale のトラブルシューティング](#) (63 ページ)
- [付録：ソースコードからの Azure 関数の構築](#) (64 ページ)

## Azure での FTDv の Auto Scale ソリューション

### Auto Scale ソリューションについて

FTDv Auto Scale for Azure は、Azure が提供するサーバーレス インフラストラクチャ (Logic App、Azure 関数、ロードバランサ、セキュリティグループ、仮想マシンスケールセットなど) を使用する完全なサーバーレス実装です。

FTDv Auto Scale for Azure の実装の主な機能には次のものがあります。

- Azure Resource Manager (ARM) テンプレートベースの展開。
- CPU およびメモリ (RAM) に基づくスケーリングメトリックのサポート：



(注) 詳細については、「[Auto Scale ロジック \(60 ページ\)](#)」を参照してください。

- FTDv 展開とマルチ可用性ゾーンをサポート。
- 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をサポート。
- Auto Scale 機能の有効化と無効化をサポート。
- FMC でのみ動作。Firepower Device Manager はサポートされていません。
- PAYG または BYOL ライセンスモードでの FTDv 展開のサポート。PAYG は、FTDv ソフトウェアバージョン 6.5 以降にのみ適用されます。「[サポートされるソフトウェアプラットフォーム \(22 ページ\)](#)」を参照してください。
- シスコでは、導入を容易にするために、Auto Scale for Azure 導入パッケージを提供しています。

### 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、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、Azure 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) Azure Auto Scale ソリューションを導入するために、Azure 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。

## Auto Scale の導入例

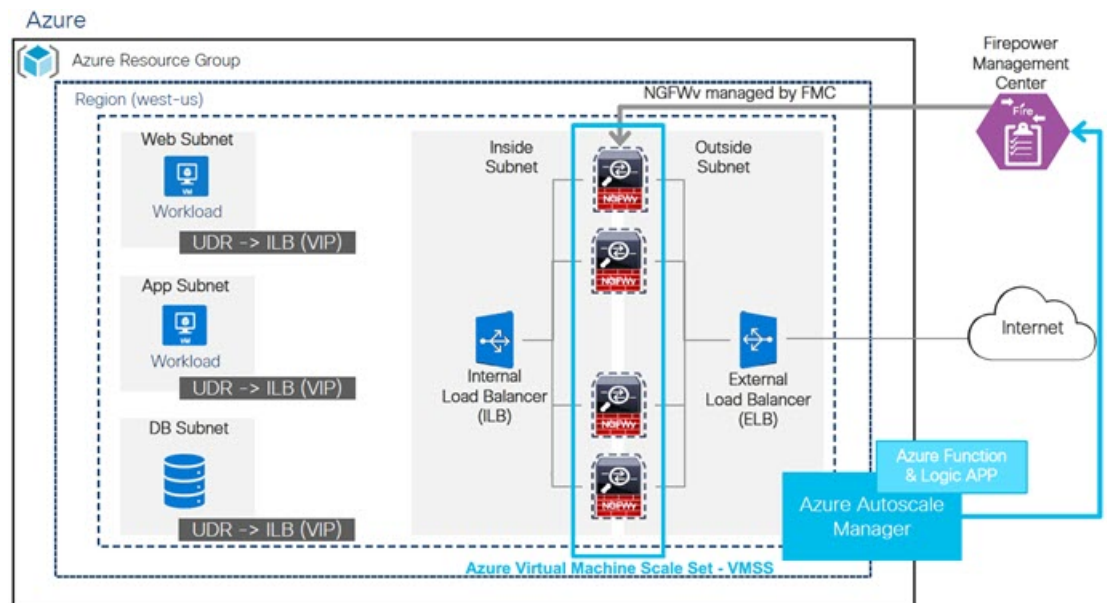
FTDv Auto Scale for Azure は、FTDv スケールセットを Azure の内部ロードバランサ (ILB) と Azure の外部ロードバランサ (ELB) の間に配置する自動水平スケーリングソリューションです。

- ELB は、インターネットからのトラフィックをスケールセット内の FTDv インスタンスに分散させます。その後、ファイアウォールがアプリケーションにトラフィックを転送します。



- ILB は、アプリケーションからのアウトバウンドインターネット トラフィックをスケールセット内の FTDv インスタンスに分散させます。その後、ファイアウォールがインターネットにトラフィックを転送します。
- ネットワークパケットが、単一の接続で両方（内部および外部）のロードバランサを通過することはありません。
- スケールセット内の FTDv インスタンスの数は、負荷条件に基づいて自動的にスケーリングおよび設定されます。

図 1: FTDv Auto Scale の導入例の図



## スコープ

このドキュメントでは、FTDv Auto Scale for Azure ソリューションのサーバーレスコンポーネントを展開する詳細な手順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。
- ここに記載されている手順と実行順序に従っていることを確認します。

## 導入パッケージのダウンロード

FTDv Auto Scale for Azure ソリューションは、Azure が提供するサーバーレス インフラストラクチャ（Logic App、Azure 関数、ロードバランサ、仮想マシンスケールセットなど）を使用する Azure Resource Manager（ARM）テンプレートベースの展開です。

FTDv Auto Scale for Azure 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/azure>



**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 を定期的に確認してください。

ASM\_Function.zip パッケージの作成方法については、「[付録：ソースコードからの Azure 関数の構築（64 ページ）](#)」を参照してください。

## Auto Scale ソリューションのコンポーネント

FTDv Auto Scale for Azure 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。

### Azure 関数（Function App）

Function App とは一連の Azure 関数です。基本的な機能は次のとおりです。

- Azure メトリックを定期的に通信またはプローブします。
- FTDv の負荷をモニターし、スケールイン/スケールアウト操作をトリガーします。
- 新しい FTDv を FMC に登録します。
- FMC を介して新しい FTDv を設定します。
- スケールインした FTDv を FMC から登録解除（削除）します。

関数は、圧縮された Zip パッケージの形式で提供されます（「[Azure Function App パッケージの構築（27 ページ）](#)」を参照）。関数は、特定のタスクを実行するために可能な限り独立しており、拡張機能や新しいリリースのサポートのために必要に応じてアップグレードできます。

### Orchestrator (Logic App)

Auto Scale Logic App は、ワークフロー、つまり一連のステップの集合です。Azure 関数は独立したエンティティであり、相互に通信できません。この Orchestrator は、関数の実行を順序付けし、関数間で情報を交換します。

- Logic App は、Auto Scale Azure 関数間で情報をオーケストレーションおよび受け渡すために使用されます。
- 各ステップは、Auto Scale Azure 関数または組み込みの標準ロジックを表します。
- Logic App は JSON ファイルとして提供されます。
- Logic App は、GUI または JSON ファイルを使用してカスタマイズできます。

### 仮想マシンスケールセット (VMSS)

VMSS は、FTDv デバイスなどの同種の仮想マシンの集合です。

- VMSS では、新しい同一の VM をセットに追加できます。
- VMSS に追加された新しい VM は、ロードバランサ、セキュリティグループ、およびネットワーク インターフェイスに自動的に接続されます。
- VMSS には組み込みの Auto Scale 機能があり、FTDv for Azure では無効になっています。
- VMSS で FTDv インスタンスを手動で追加したり、削除したりしないでください。

### Azure Resource Manager (ARM) テンプレート

ARM テンプレートは、FTDv Auto Scale for Azure 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。

ARM テンプレートは、以下を含む Auto Scale Manager コンポーネントの入力を提供します。

- Azure Function App
- Azure Logic App
- 仮想マシンスケールセット (VMSS)
- 内部および外部ロードバランサ。
- 展開に必要なセキュリティグループおよびその他のコンポーネント。



#### 重要

ユーザー入力の検証に関しては、ARM テンプレートには限界があるため、展開時に入力を検証する必要があります。

# Auto Scale ソリューションの前提条件

## Azure のリソース

### リソース グループ

このソリューションのすべてのコンポーネントを展開するには、既存または新しく作成されたリソースグループが必要です。



(注) 後で使用するために、リソースグループ名、リソースグループが作成されたリージョン、および Azure サブスクリプション ID を記録します。

### ネットワーキング

仮想ネットワークが使用可能または作成済みであることを確認します。Auto Scale 展開では、ネットワークリソースの作成、変更、管理は行われません。

FTDv には 4 つのネットワーク インターフェイスが必要なため、仮想ネットワークには次の 4 つのサブネットが必要です。

1. 管理トラフィック
2. 診断トラフィック
3. 内部トラフィック
4. 外部トラフィック

サブネットが接続されているネットワーク セキュリティ グループで、次のポートを開く必要があります。

- SSH (TCP/22)

ロードバランサと FTDv 間の正常性プローブに必要です。

サーバーレス機能と FTDv 間の通信に必要です。

- TCP/8305

FTDv と FMC 間の通信に必要です。

- HTTPS (TCP/443)

サーバーレスコンポーネントと FMC 間の通信に必要です。

- アプリケーション固有のプロトコルまたはポート

ユーザーアプリケーションに必要です (TCP/80 など)。



- (注) 仮想ネットワーク名、仮想ネットワーク CIDR、4 つすべてのサブネットの名前、および外部と内部のサブネットのゲートウェイ IP アドレスを記録します。

## Azure Function App パッケージの構築

FTDv Azure Auto Scale ソリューションでは、*ASM\_Function.zip* アーカイブファイルを作成する必要があります。このファイルから、圧縮された ZIP パッケージの形式で一連の個別の Azure 関数が提供されます。

ASM\_Function.zip パッケージの作成方法については、「[付録：ソースコードからの Azure 関数の構築（64 ページ）](#)」を参照してください。

関数は、特定のタスクを実行するために可能な限り独立しており、拡張機能や新しいリリースのサポートのために必要に応じてアップグレードできます。

## Firepower Management Center の準備

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。

デバイスグループを含め、FTDv の設定と管理に必要なすべてのオブジェクトを作成します。そうすることで、複数のデバイスにポリシーを簡単に展開して、更新をインストールできます。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。

後続の項では、FMC を準備するための基本的な手順の概要を説明します。詳細については、完全な『[Firepower Management Center Configuration Guide](#)』を参照してください。FMC を準備する際は、次の情報を必ず記録してください。

- FMC パブリック IP アドレス。
- FMC ユーザー名およびパスワード。
- セキュリティポリシー名。
- 内部および外部のセキュリティゾーン オブジェクト名。
- デバイスグループ名。

## 新しい FMC ユーザーの作成

Auto Scale Manager だけが使用する管理者権限を持つ FMC で新しいユーザーを作成します。



- 重要** 他の FMC セッションとの競合を防ぐために、FTDv Auto Scale ソリューション専用の FMC ユーザーアカウントを持つことが重要です。

## 手順

**ステップ 1** 管理者権限を持つ FMC で新しいユーザーを作成します。[システム (System)] > [ユーザー (Users)] の順にクリックし、[ユーザーの作成 (Create User)] をクリックします。

ユーザー名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン (-)、およびアンダースコア (\_) が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン (-) は使用不可、すべて数字は不可、ピリオド (.)、アットマーク (@)、またはスラッシュ (/) は使用不可

**ステップ 2** 使用環境に必要なユーザーオプションを入力します。詳細については、『[FMC configuration guide](#)』を参照してください。

## アクセス制御の設定

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。アクセスコントロールポリシー内では、アクセスコントロールルールによって複数の管理対象デバイスでネットワークトラフィックを処理する詳細な方法が提供されます。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。FMC 設定ガイド[英語]の「Best Practices for Access Control」を参照してください。

## 手順

**ステップ 1** [ポリシー (Policies)] > [アクセス制御 (Access Control)] を選択します。

**ステップ 2** [新しいポリシー (New Policy)] をクリックします。

**ステップ 3** [名前 (Name)] に一意の名前を入力し、オプションで [説明 (Description)] を入力します。

**ステップ 4** 導入のセキュリティ設定とルールを設定する場合は、『[FMC configuration guide](#)』を参照してください。

## ライセンスの設定

すべてのライセンスは FMC によって FTD に提供されます。オプションで、次の機能ライセンスを購入できます。

- **脅威** : セキュリティ インテリジェンスと Cisco Firepower の次世代 IPS
- **マルウェア** : 強化されたネットワーク向けの高度なマルウェア防御 (AMP)
- **URL** : URL フィルタリング
- **RA VPN** : AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。



- (注) 脅威、マルウェア、または URL ライセンスを購入する場合は、1、3、または 5 年間アップデートにアクセスするための適合するサブスクリプション ライセンスも必要です。

### 始める前に

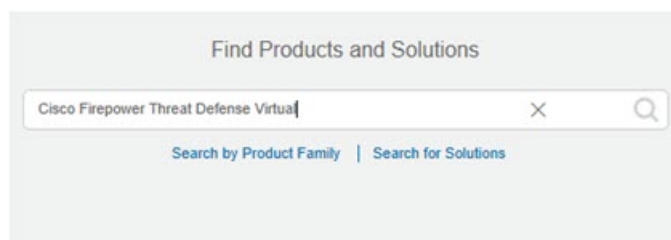
- Cisco Smart Software Manager にマスター アカウントを持ちます。  
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化 (3DES/AES) ライセンスを使用する必要があります。

### 手順

- ステップ 1** お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェア ライセンシングアカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [製品とソリューションの検索 (Find Products and Solutions)] 検索フィールドを使用します。次のライセンス PID を検索します。

図 2: ライセンス検索



- (注) PID が見つからない場合は、注文に手動で PID を追加できます。

- ステップ 2** まだ追加していない場合は、Smart Licensing サーバーに FMC を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細については、『[FMC Configuration Guide](#)』を参照してください。

## セキュリティ ゾーン オブジェクトの作成

展開用の内部および外部セキュリティ ゾーン オブジェクトを作成します。

## 手順

- ステップ1 [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- ステップ2 オブジェクトタイプのリストから、[インターフェイス (Interface)] を選択します。
- ステップ3 [追加 (Add)] > [セキュリティゾーン (Security Zone)] をクリックします。
- ステップ4 [名前 (Name)] (inside、outside など) を入力します。
- ステップ5 [インターフェイスタイプ (Interface Type)] として [ルーテッド (Routed)] を選択します。
- ステップ6 [保存 (Save)] をクリックします。

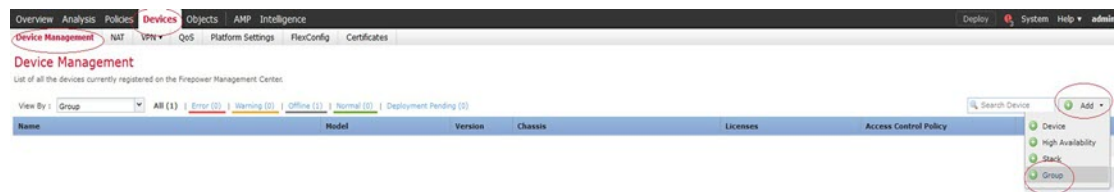
## デバイスグループの作成

デバイスグループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

## 手順

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

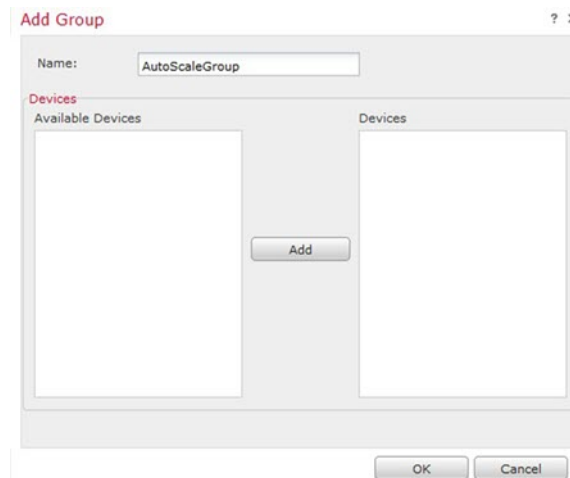
図 3: Device Management



- ステップ2 [追加 (Add)] ドロップダウンメニューから、[グループの追加 (Add Group)] を選択します。
- ステップ3 名前を入力します。例: AutoScaleGroup。

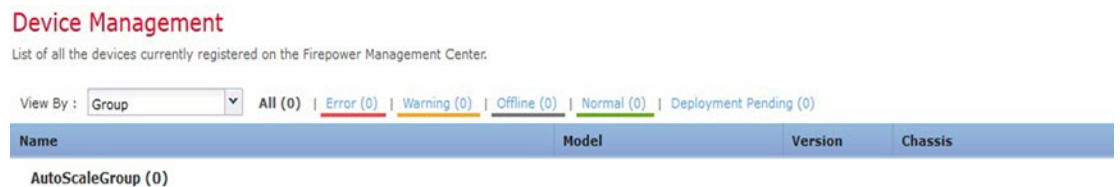


図 4: デバイスグループの追加



**ステップ 4** [OK] をクリックして、デバイス グループを追加します。

図 5: 追加されたデバイスグループ



## セキュアシェルのアクセスの設定

FTD デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、複数のデバイス間で各機能の値を共有できます。FTDv Auto Scale for Azure には、内部ゾーンと外部ゾーン、および Auto Scale グループ用に作成されたデバイスグループで SSH を許可するための FTD プラットフォーム設定ポリシーが必要です。これは、FTDv のデータインターフェイスがロードバランサからの正常性プローブに応答するために必要です。

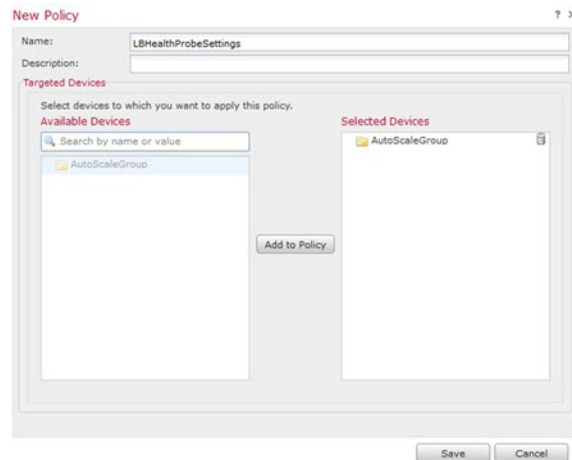
### 始める前に

- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールに必要なグループがすでに存在することを確認します。[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択して、オブジェクトを設定します。例として、次の手順の azure-utility-ip (168.63.129.16) オブジェクトを参照してください。

## 手順

**ステップ 1** [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] を選択し、FTD ポリシー (例: LBHealthProbeSettings) を作成または編集します。

図 6: FTD プラットフォーム設定ポリシー



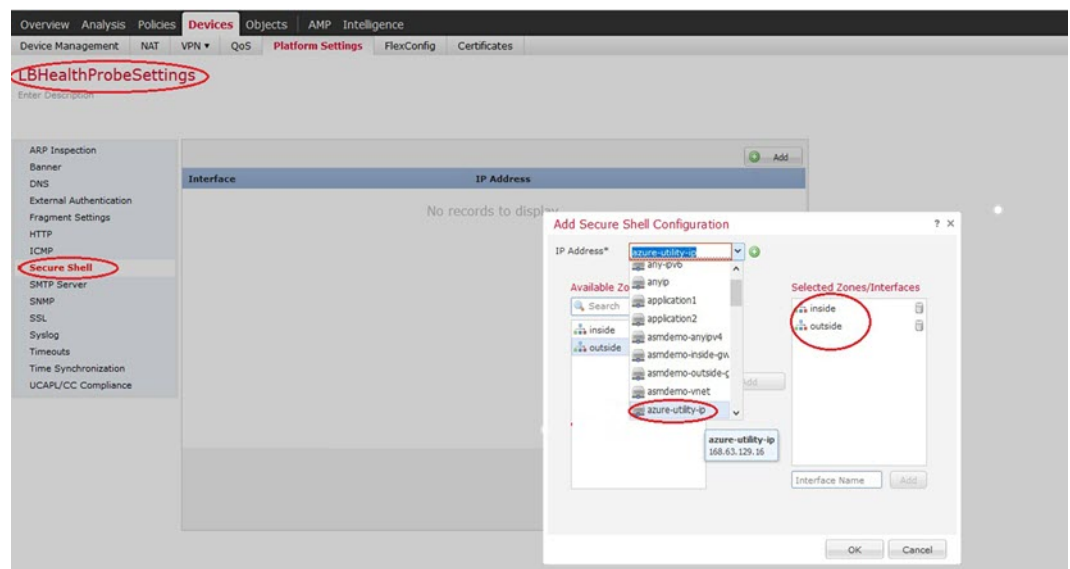
**ステップ 2** [セキュア シェル (Secure Shell)] を選択します。

**ステップ 3** SSH 接続を許可するインターフェイスと IP アドレスを指定します。

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] をクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。

- [IP アドレス (IP Address)] : SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクト (例: azure-utility-ip (168.63.129.16))。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- [セキュリティゾーン (Security Zones)] : SSH 接続を許可するインターフェイスを含むゾーンを追加します。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。セキュリティゾーンは、FMC の [オブジェクト (Objects)] ページで作成できます。セキュリティゾーンの詳細については、FMC Configuration Guide を参照してください。
- [OK] をクリックします。

図 7: FTDv Auto Scale の SSH アクセス



ステップ 4 [Save (保存)] をクリックします。

これで、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

## NAT の設定

NAT ポリシーを作成し、外部インターフェイスからアプリケーションにトラフィックを転送するために必要な NAT ルールを作成し、このポリシーを Auto Scale 用に作成したデバイスグループにアタッチします。

### 手順

- ステップ 1 [デバイス (Devices)] > [NAT] の順に選択します。
- ステップ 2 [新しいポリシー (New Policy)] ドロップダウン リストで、[Threat Defense NAT] を選択します。
- ステップ 3 [名前 (Name)] に一意の名前を入力します。
- ステップ 4 必要に応じて、[説明 (Description)] を入力します。
- ステップ 5 NAT ルールを設定します。NAT ルールの作成および NAT ポリシーの適用方法のガイドラインについては、『[FMC configuration guide](#)』の「Configure NAT for Threat Defense」の手順を参照してください。次の図に、基本的なアプローチを示します。

図 8: NAT ポリシーの例

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
1	+	Dynamic	outside	inside	any-ipv4	Interface	Original HTTP	Interface	Application1	Original HTTP	One-False
2	+	Dynamic	outside	inside	any-ipv4	Interface	Original HTTP1	Interface	Application2	Original HTTP1	One-False
3	+	Dynamic	inside	outside	any-ipv4	Interface		Interface			One-False

(注) 変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。

ステップ 6 [保存 (Save)] をクリックします。

## 入力パラメータ

次の表に、テンプレートパラメータおよび例を示します。各パラメータの値を決めたら、Azure サブスクリプションに ARM テンプレートを展開するときに、各パラメータを使用して FTDv デバイスを作成できます。「[Auto Scale ARM テンプレートの展開 \(43 ページ\)](#)」を参照してください。

表 2: テンプレートパラメータ

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
resourceNamePrefix	文字列* (3 ~ 10 文字)	すべてのリソースは、このプレフィックスを含む名前で作成されます。 注：小文字のみを使用してください。 例：ftdv	新規作成
virtualNetworkRg	文字列	仮想ネットワークのリソースグループの名前。 例：cisco-virtualnet-rg	既存
virtualNetworkName	文字列	仮想ネットワーク名（作成済み） 例：cisco-virtualnet	既存

パラメータ名	使用できる値/ タイプ	説明	リソースの作成タイプ
virtualNetworkCidr	CIDR 形式 x.x.x.x/y	仮想ネットワークのCIDR（作成済み）	既存
mgmtSubnet	文字列	管理サブネット名（作成済み）  例：cisco-mgmt-subnet	既存
diagSubnet	文字列	診断サブネット名（作成済み）  例：cisco-diag-subnet	既存
insideSubnet	文字列	内部サブネット名（作成済み）  例：cisco-inside-subnet	既存
internalLbIp	文字列	内部サブネットの内部ロードバランサの IP アドレス（作成済み）。  例：1.2.3.4	既存
insideNetworkGatewayIp	文字列	内部サブネットのゲートウェイ IP アドレス（作成済み）	既存
outsideSubnet	文字列	外部サブネット名（作成済み）  例：cisco-outside-subnet	既存
outsideNetworkGatewayIp	文字列	外部サブネットゲートウェイ IP（作成済み）	既存
deviceGroupName	文字列	FMC のデバイスグループ（作成済み）	既存
insideZoneName	文字列	FMC の内部ゾーン名（作成済み）	既存
outsideZoneName	文字列	FMC の外部ゾーン名（作成済み）	既存
softwareVersion	文字列	FTDv バージョン（展開時にドロップダウンから選択）	既存

パラメータ名	使用できる値/ タイプ	説明	リソースの作成 タイプ
vmSize	文字列	FTDv インスタンスのサイズ (展開時にドロップダウンから選択)	該当なし
ftdLicensingSku	文字列	FTDv ライセンスモード (PAYG/BYOL)  注: PAYG はバージョン 6.5+ でサポートされています。	該当なし
licenseCapability	カンマ区切り 文字列	BASE、MALWARE、 URLFilter、THREAT	該当なし
ftdVmManagementUserName	文字列 *	FTDv VM 管理の管理者ユーザー名。  これは「admin」にはできません。VM 管理者ユーザー名のガイドラインについては、「Azure」を参照してください。	新規作成
ftdVmManagementUserPassword	文字列 *	FTDv VM 管理の管理者ユーザーのパスワード。  パスワードの長さは 12 ～ 72 文字で、小文字、大文字、数字、特殊文字を使用する必要があります。また、文字の繰り返しは 2 回までにする必要があります。  (注) テンプレートには、このパラメータのコンプライアンスチェック機能はありません。	新規作成
fmcIpAddress	文字列 x.x.x.x	FMC のパブリック IP アドレス (作成済み)	既存
fmcUserName	文字列	管理権限を持つ FMC ユーザー名 (作成済み)	既存
fmcPassword	文字列	前述の FMC ユーザー名の FMC パスワード (作成済み)	既存

パラメータ名	使用できる値/ タイプ	説明	リソースの作成タイプ
policyName	文字列	FMC で作成されたセキュリティポリシー（作成済み）	既存
scalingPolicy	POLICY-1/POLICY-2	<p><b>POLICY-1</b>：設定された期間に、いずれかの FTDv の平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。</p> <p><b>POLICY-2</b>：設定された期間に、Auto Scale グループ内のすべての FTDv デバイスの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。</p> <p>どちらの場合も、スケールインロジックは同じままです。設定された期間に、すべての FTDv デバイスの平均負荷がスケールインしきい値を下回るとスケールインがトリガーされます。</p>	該当なし
scalingMetricsList	文字列	<p>スケーリングの決定に使用されるメトリック。</p> <p>許可：CPU CPU、メモリ デフォルト：CPU</p>	該当なし
cpuScaleInThreshold	文字列	<p>CPU メトリックのスケールインしきい値（パーセント単位）。</p> <p>デフォルト：10</p> <p>FTDv メトリック（CPU 使用率）がこの値を下回ると、スケールインがトリガーされます。</p> <p>「<a href="#">Auto Scale ロジック（60 ページ）</a>」を参照してください。</p>	該当なし

パラメータ名	使用できる値/ タイプ	説明	リソースの作成タイプ
cpuScaleOutThreshold	文字列	<p>CPU メトリックのスケールアウトしきい値（パーセント単位）。</p> <p>デフォルト：80</p> <p>FTDvメトリック（CPU 使用率）がこの値を上回ると、スケールアウトがトリガーされます。</p> <p>「cpuScaleOutThreshold」は、常に「cpuScaleInThreshold」より大きくする必要があります。</p> <p>「<a href="#">Auto Scale ロジック（60 ページ）</a>」を参照してください。</p>	該当なし
memoryScaleInThreshold	文字列	<p>メモリメトリックのスケールインしきい値（パーセント単位）。</p> <p>デフォルト：0</p> <p>FTDvメトリック（CPU 使用率）がこの値を下回ると、スケールインがトリガーされます。</p> <p>「<a href="#">Auto Scale ロジック（60 ページ）</a>」を参照してください。</p>	該当なし



パラメータ名	使用できる値/ タイプ	説明	リソースの作成タイプ
memoryScaleOutThreshold	文字列	<p>メモリメトリックのスケールアウトしきい値（パーセント単位）。</p> <p>デフォルト：0</p> <p>FTDvメトリック（CPU 使用率）がこの値を上回ると、スケールアウトがトリガーされます。</p> <p>「memoryScaleOutThreshold」は、常に「memoryScaleInThreshold」より大きくする必要があります。</p> <p>「<a href="#">Auto Scale ロジック（60 ページ）</a>」を参照してください。</p>	該当なし
minFtdCount	整数	<p>任意の時点でスケールセットで使用可能な最小 FTDv インスタンス数。</p> <p>例：2。</p>	該当なし
maxFtdCount	整数	<p>スケールセットで許可される最大 FTDv インスタンス数。</p> <p>例：10</p> <p>（注） この数は FMC の容量によって制限されます。</p> <p>Auto Scale ロジックではこの変数の範囲はチェックされないため、慎重に入力してください。</p>	該当なし

パラメータ名	使用できる値/ タイプ	説明	リソースの作成 タイプ
metricsAverageDuration	整数	<p>ドロップダウンから選択します。</p> <p>この数値は、メトリックが平均化される時間（分単位）を表します。</p> <p>この変数の値が5（5分）の場合、Auto Scale Manager がスケジュールされると、メトリックの過去 5 分間の平均がチェックされ、その結果に基づいてスケーリングの判断が行われます。</p> <p>（注） Azure の制限により、有効な数値は 1、5、15、および 30 だけです。</p>	該当なし

パラメータ名	使用できる値/ タイプ	説明	リソースの作 成タイプ
initDeploymentMode	BULK/STEP		

パラメータ名	使用できる値/ タイプ	説明	リソースの作成 タイプ
		<p>主に最初の展開、またはスケールセットに FTDv インスタンスが含まれていない場合に適用されます。</p> <p><b>BULK : Auto Scale Manager</b> は、「minFtdCount」個の FTDv インスタンスを同時に展開しようとしています。</p> <p>(注) 起動は並行して行われますが、FMC への登録は FMC の制限により順次実行されます。</p> <p><b>STEP : Auto Scale Manager</b> は、スケジュールされた間隔ごとに「minFtdCount」個の FTDv デバイスを 1 つずつ展開します。</p> <p>(注) STEP オプションでは、「minFtdCount」個のインスタンスが FMC で起動および設定されて、動作可能になるまで時間がかかりますが、デバッグに役立ちます。</p> <p><b>BULK オプション</b>では、（並行実行のため）「minFtdCount」個すべての FTDv を起動するのに 1 つの FTDv 起動と同じ時間がかかりますが、FMC の登録は順次実行されます。</p> <p>「minFtdCount」個の FTDv を展開するための合計時間 = (1 つの FTDv の起動時</p>	

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
		間 + 1 つの FTDv 登録および設定時間 * minFtdCount) 。	
* Azure には、新しいリソースの命名規則に関する制限があります。制限を確認するか、またはすべて小文字を使用してくださいスペースやその他の特殊文字は使用しないでください。			

## Auto Scale の展開

### 導入パッケージのダウンロード

FTDv Auto Scale for Azure ソリューションは、Azure が提供するサーバーレス インフラストラクチャ（Logic App、Azure 関数、ロードバランサ、仮想マシンスケールセットなど）を使用する Azure Resource Manager（ARM）テンプレートベースの展開です。

FTDv Auto Scale for Azure 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/azure>



**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 を定期的に確認してください。

ASM\_Function.zip パッケージの作成方法については、「付録：ソースコードからの Azure 関数の構築（64 ページ）」を参照してください。

### Auto Scale ARM テンプレートの展開

ARM テンプレートは、FTDv Auto Scale for Azure に必要なリソースを展開するために使用されます。特定のリソースグループ内では、ARM テンプレートを展開することで次の内容が作成されます。

- 仮想マシンスケールセット（VMSS）
- 外部ロードバランサ
- 内部ロードバランサ
- Azure Function App

- Logic App
- セキュリティグループ（データインターフェイスおよび管理インターフェイス用）

### 始める前に

- GitHub リポジトリ (<https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure>) から、ARM テンプレート `azure_ftdv_autoscale.json` をダウンロードします。

### 手順

**ステップ 1** 複数の Azure ゾーンに FTDv インスタンスを展開する必要がある場合は、展開リージョンで使用可能なゾーンに基づいて、ARM テンプレートを編集します。

例：

```
"zones": [
  "1",
  "2",
  "3"
],
```

この例は、3 つのゾーンを持つ「Central US」リージョンを示しています。

**ステップ 2** 外部ロードバランサで必要なトラフィックルールを編集します。この「json」配列を拡張することで、任意の数のルールを追加できます。

例：

```
{
  "type": "Microsoft.Network/loadBalancers",
  "name": "[variables('elbName')]",
  "location": "[resourceGroup().location]",
  "apiVersion": "2018-06-01",
  "sku": {
    "name": "Standard"
  },
  "dependsOn": [
    "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"
  ],
  "properties": {
    "frontendIPConfigurations": [
      {
        "name": "LoadBalancerFrontEnd",
        "properties": {
          "publicIPAddress": {
            "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
          }
        }
      }
    ],
    "backendAddressPools": [
      {
```

```

        "name": "backendPool"
      }
    ],
    "loadBalancingRules": [
      {
        "properties": {
          "frontendIPConfiguration": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/frontendIpConfigurations/LoadBalancerFrontend')]"
          },
          "backendAddressPool": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/backendAddressPools/BackendPool')]"
          },
          "probe": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers',
variables('elbName')), '/probes/lbprobe')]"
          },
          "protocol": "TCP",
          "frontendPort": "80",
          "backendPort": "80",
          "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
        },
        "Name": "lbrule"
      }
    ]
  },

```

(注) このファイルを編集しない場合は、導入後に Azure ポータルから編集することもできます。

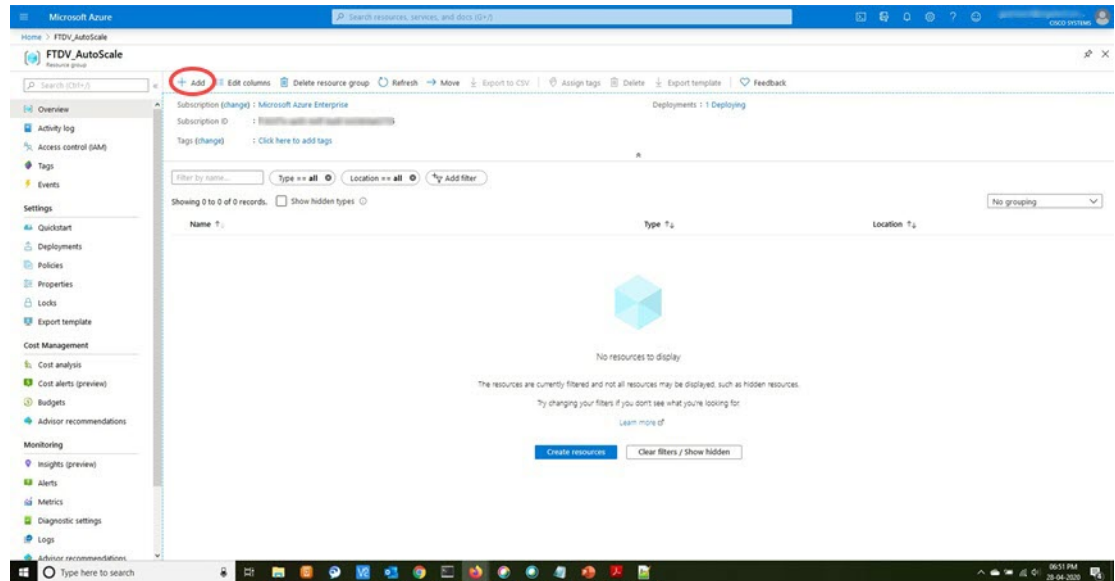
**ステップ 3** Microsoft アカウントのユーザー名とパスワードを使用して、Microsoft Azure ポータルにログインします。

**ステップ 4** [リソースグループ (Resource Groups)] ブレードにアクセスするには、サービスのメニューから [リソースグループ (Resource groups)] をクリックします。サブスクリプション内のすべてのリソースグループがブレードに一覧表示されます。

新しいリソースグループを作成するか、既存の空のリソースグループを選択します。たとえば、*FTDv\_AutoScale*。

## Auto Scale ARM テンプレートの展開

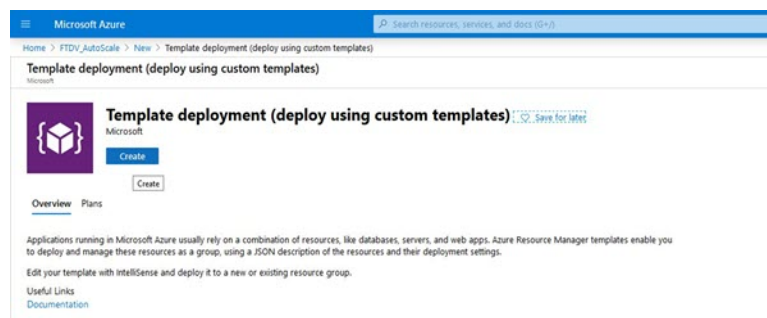
図 9: Azure ポータル



**ステップ 5** [リソースの作成 (+) (Create a resource (+))] をクリックして、テンプレート展開用の新しいリソースを作成します。[リソースグループの作成 (Create Resource Group)] ブレードが表示されます。

**ステップ 6** [マーケットプレイスの検索 (Search the Marketplace)] で、「テンプレートの展開 (カスタムテンプレートを使用した展開) (Template deployment (deploy using custom templates))」と入力し、Enter を押します。

図 10: カスタムテンプレートの展開

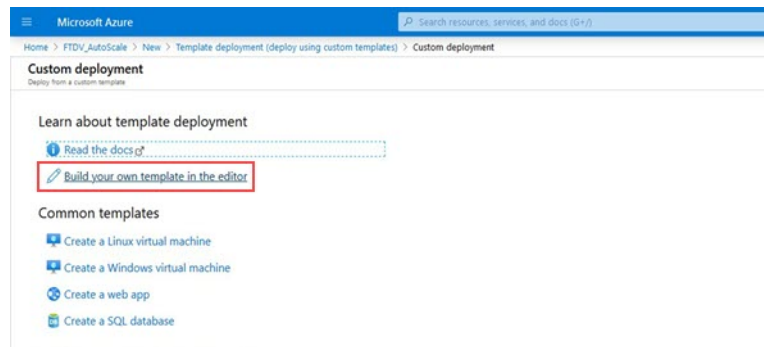


**ステップ 7** [作成 (Create)] をクリックします。

**ステップ 8** テンプレートを作成するためのオプションは複数あります。[エディタで独自のテンプレートを作成する (Build your own template in editor)] を選択します。

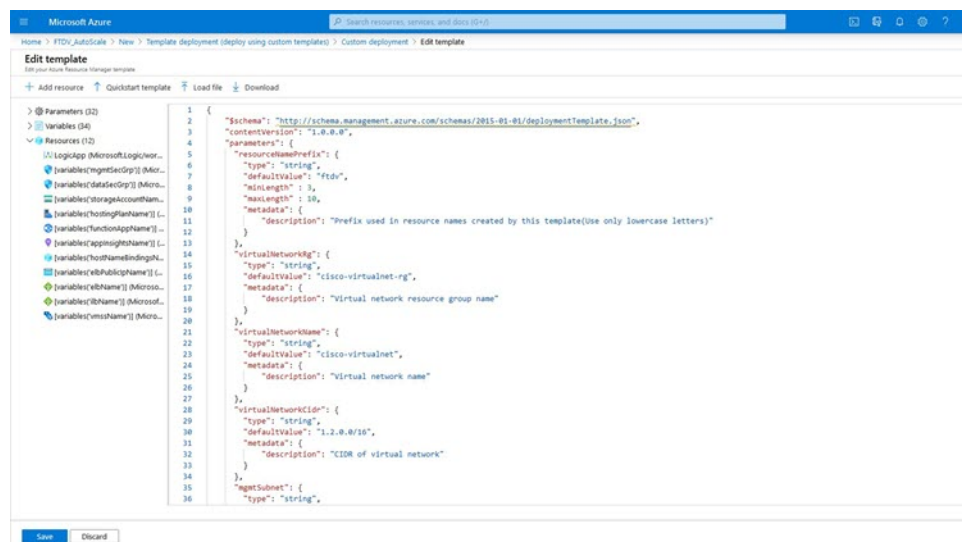


図 11:独自のテンプレートの作成



**ステップ 9** [テンプレートの編集 (Edit template)] ウィンドウで、すべてのデフォルトコンテンツを削除し、更新した `azure_ftdv_autoscale.json` からコンテンツをコピーして、[保存 (Save)] をクリックします。

**図 12: Edit Template**



**ステップ 10** 次のセクションで、すべてのパラメータを入力します。各パラメータの詳細については、「[入力パラメータ \(34 ページ\)](#)」を参照してください。次に、[購入 (Purchase)] をクリックします。

図 13: ARM テンプレートパラメータ

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. The page is titled 'Custom deployment' and has a breadcrumb trail: 'Home > FTDV\_AutoScale > New > Template deployment (deploy using custom template) > Custom deployment'. The page is divided into two main sections: 'BASICS' and 'SETTINGS'. The 'BASICS' section includes fields for 'Subscription' (Microsoft Azure Enterprise), 'Resource group' (FTDV\_AutoScale), and 'Location' (East US). The 'SETTINGS' section includes fields for 'Resource Name Prefix' (ftdv), 'Virtual Network ID' (ftdv-vnet), 'Virtual Network Name' (ftdv-vnet-virtualnetwork), 'Virtual Network CIDR' (10.1.0.0/16), 'Management Subnet' (ManagementSub), 'Diagnostic Subnet' (DiagSub), 'Internal Subnet' (InternalSub), 'Internal Network Gateway IP' (10.1.1.1), 'Internal IP' (10.1.1.100), and 'Outside Subnet' (OutsideSub). There are also links for 'Edit template', 'Edit parameters', and 'Learn more'.

(注) [パラメータの編集 (Edit Parameters)] をクリックして、JSON ファイルを編集するか、または事前入力されたコンテンツをアップロードできます。

ARM テンプレートの入力検証機能は限られているため、入力を検証するのはユーザーの責任です。

**ステップ 11** テンプレートの展開が成功すると、FTDV Auto Scale for Azure ソリューションに必要なすべてのリソースが作成されます。次の図のリソースを参照してください。[タイプ (Type)] 列には、Logic App、VMSS、ロードバランサ、パブリック IP アドレスなどの各リソースが示されます。

図 14: FTDV Auto Scale テンプレートの展開

The screenshot shows the 'FTDV\_AutoScale' resource group in the Microsoft Azure portal. The page displays a list of resources created by the template deployment. The resources are listed in a table with columns for Name, Type, and Location. The resources include:

Name	Type	Location
ftdv-appinsight	Application Insights	East US
ftdv-datadogsecgrp	Network security group	East US
ftdv-lb	Load balancer	East US
ftdv-lb-public-ip	Public IP address	East US
ftdv-function-app	App Service plan	East US
ftdv-function-app	App Service	East US
ftdv-lb	Load balancer	East US
ftdv-logic-app	Logic app	East US
ftdv-mgmtsecgrp	Network security group	East US
ftdv-vmss	Virtual machine scale set	East US
ftdv-storageaccount	Storage account	East US

## Azure Function App の展開

ARMテンプレートを展開すると、AzureによってスケルトンFunction Appが作成されます。このアプリは、Auto Scale Manager ロジックに必要な関数を使用して手動で更新および設定する必要があります。

始める前に

- ASM\_Function.zip パッケージをビルドします。「付録：ソースコードからの Azure 関数の構築（64 ページ）」を参照してください。

手順

**ステップ 1** ARM テンプレートを展開したときに作成した Function App に移動し、関数が存在しないことを確認します。ブラウザで次の URL にアクセスします。

`https://<Function App Name>.scm.azurewebsites.net/DebugConsole`

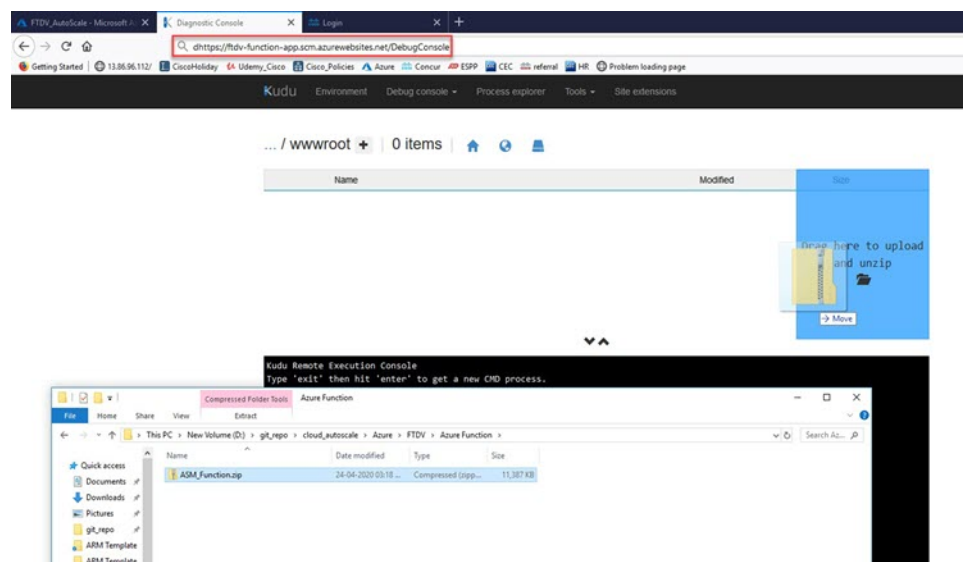
「[Auto Scale ARM テンプレートの展開（43 ページ）](#)」の例の場合、次のようになります。

`https://ftdv-function-app.scm.azurewebsites.net/DebugConsole`

**ステップ 2** ファイルエクスプローラで、site/wwwroot に移動します。

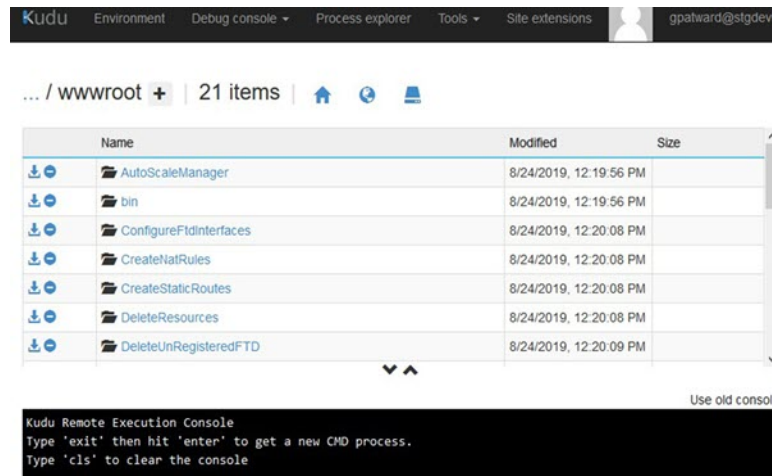
**ステップ 3** ASM\_Function.zip をファイルエクスプローラの右隅にドラッグアンドドロップします。

図 15: FTDv Auto Scale 関数のアップロード



**ステップ 4** アップロードが成功すると、すべてのサーバーレス関数が表示されます。

図 16: FTDv サーバーレス関数

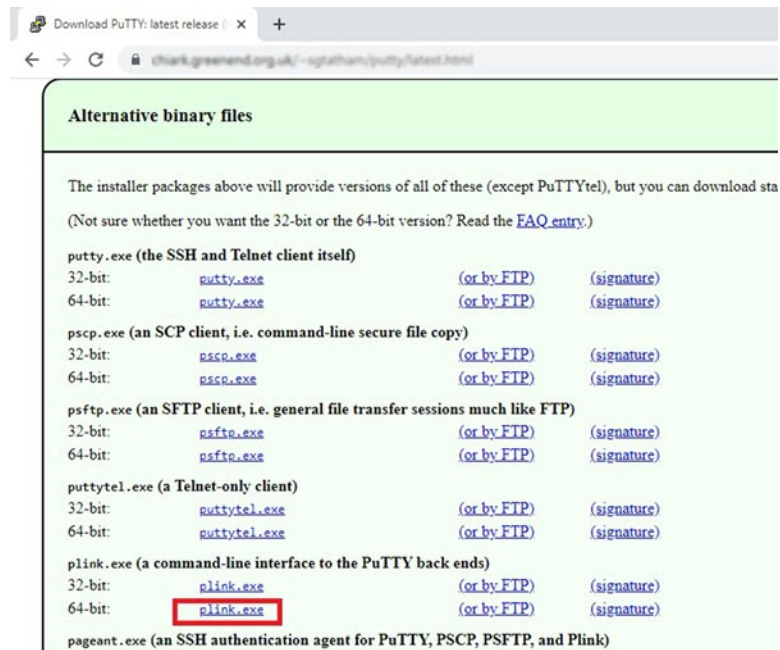


### ステップ 5 PuTTY SSH クライアントをダウンロードします。

Azure 関数は、SSH 接続を介して FTDv にアクセスする必要があります。ただし、サーバーレスコードで使用されるオープンソースライブラリは、FTDv で使用される SSH キー交換アルゴリズムをサポートしていません。したがって、事前に構築された SSH クライアントをダウンロードする必要があります。

[www.putty.org](http://www.putty.org) から PuTTY コマンドラインインターフェイスを PuTTY バックエンド (plink.exe) にダウンロードします。

図 17: PuTTY のダウンロード



### ステップ 6 SSH クライアントの実行ファイル **plink.exe** の名前を **ftdssh.exe** に変更します。

- ステップ 7** `ftdssh.exe` をファイルエクスプローラの右隅（前のステップで **ASM\_Function.zip** をアップロードした場所）にドラッグアンドドロップします。
- ステップ 8** SSH クライアントが Function App とともに存在することを確認します。必要に応じてページを更新します。

## 設定の微調整

Auto Scale Manager を微調整したり、デバッグで使用したりするために使用できる設定がいくつかあります。これらのオプションは、ARM テンプレートには表示されませんが、Function App で編集できます。

始める前に



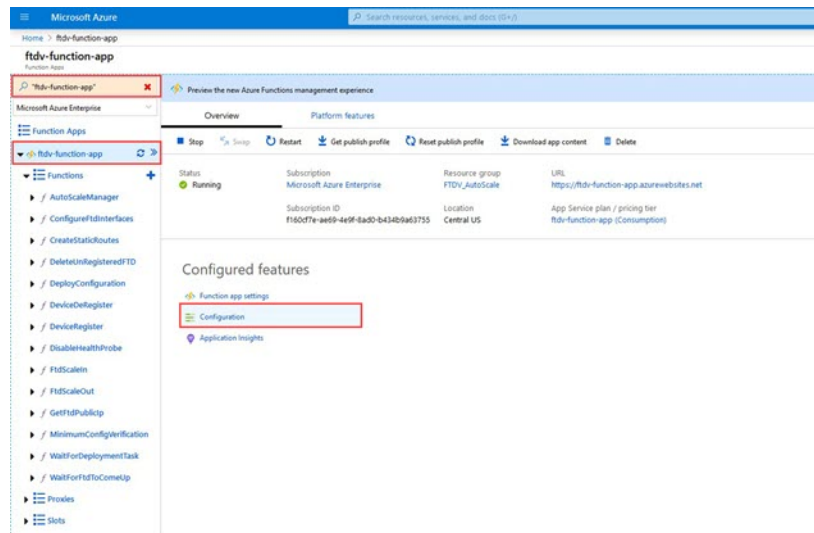
（注） 設定はいつでも編集できます。設定を編集する場合は、次の手順に従います。

- Function App を無効にします。
- 既存のスケジュール済みタスクが終了するまで待ちます。
- 設定を編集して保存します。
- Function App を有効にします。

手順

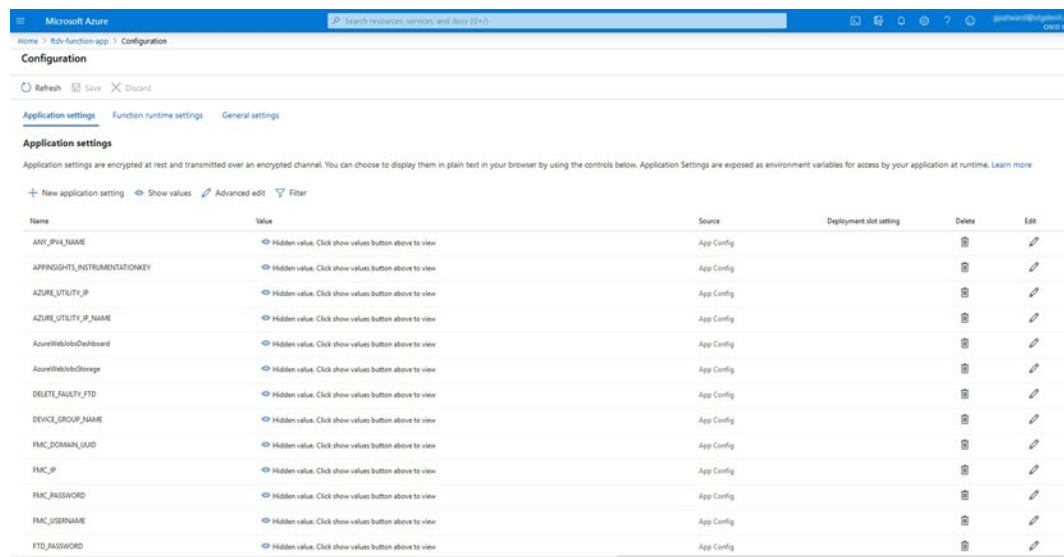
- ステップ 1** Azure ポータルで、FTDv Function App を検索して選択します。

図 18 : FTDv Function App



**ステップ 2** ここでは、ARMテンプレートを介して渡された設定も編集できます。変数名は、ARMテンプレートとは異なる場合がありますが、変数の目的は名前から簡単に識別できます。

図 19 : アプリケーションの設定



ほとんどのオプションは、名前を見ればわかります。次に例を示します。

- [構成名 (Configuration Name)] : 「DELETE\_FAULTY\_FTD」 ([デフォルト値] (Default value)) : YES

スケールアウト中に、新しいFTDvインスタンスが起動し、FMCに登録されます。登録が失敗した場合、このオプションに基づいて、Auto Scale ManagerがそのFTDvインスタンスを保持するか、削除するかを決定します。 ([はい (Yes)] : 障害のあるFTDvを削除し

ます。[いいえ (No)] : FMC に登録できない場合でも、FTDv インスタンスを保持します)。

- **Function App** 設定では、Azure サブスクリプションにアクセスできるユーザーは、すべての変数 (「password」などのセキュアな文字列を含んでいる変数を含む) をクリアテキスト形式で表示できます。

この点に関するセキュリティ上の懸念がある場合 (たとえば、Azure サブスクリプションが組織内の低い権限を持つユーザー間で共有されている場合)、ユーザーは Azure の Key Vault サービスを使用してパスワードを保護できます。この設定をすると、関数の設定でクリアテキストの「password」を入力する代わりに、ユーザーは、パスワードが保存されている Key Vault によって生成された、セキュアな識別子を入力する必要があります。

(注) Azure のドキュメントを検索して、アプリケーションデータを保護するためのベストプラクティスを見つけてください。

---

## 仮想マシンスケールセットでの IAM ロールの設定

Azure Identity and Access Management (IAM) は、Azure Security and Access Control の一部として使用され、ユーザーの ID を管理および制御します。Azure リソースのマネージド ID は、Azure Active Directory で自動的にマネージド ID が Azure サービスに提供されます。

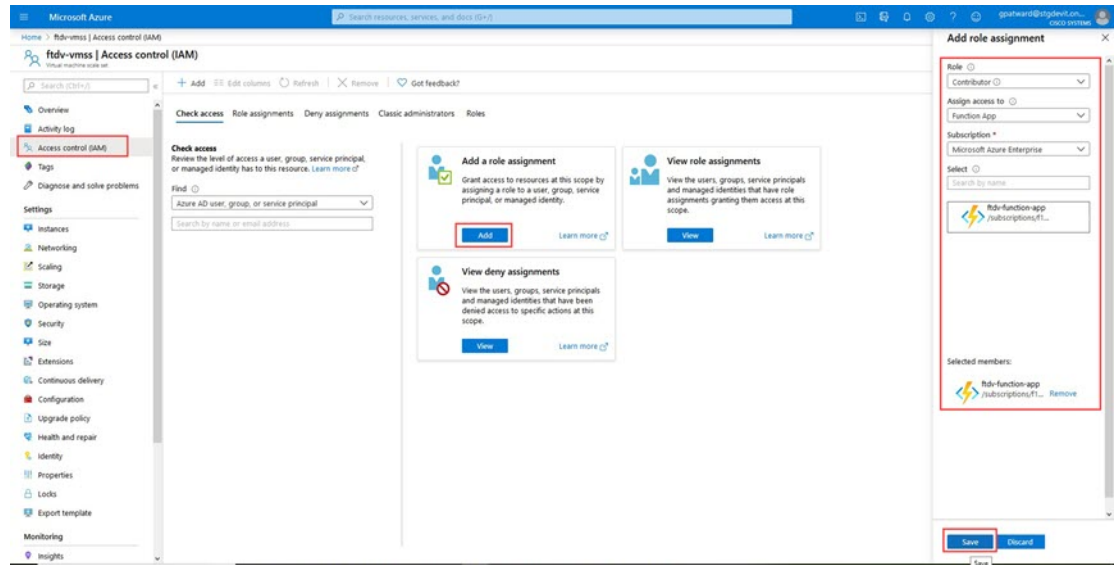
これにより、明示的な認証ログイン情報がなくても、Function App が仮想マシンスケールセット (VMSS) を制御できます。

### 手順

---

- ステップ 1** Azure ポータルで、VMSS に移動します。
- ステップ 2** [アクセス制御 (IAM) (Access control (IAM))] をクリックします。
- ステップ 3** [追加 (Add)] をクリックしてロールの割り当てを追加します。
- ステップ 4** [ロール割り当ての追加 (Add role assignment)] ドロップダウンから、[共同作成者 (Contributor)] を選択します。
- ステップ 5** [アクセスの割り当て先 (Assign access to)] ドロップダウンから、[Function App] を選択します。
- ステップ 6** FTDv Function App を選択します。

図 20: AIM ロールの割り当て



ステップ 7 [保存 (Save)] をクリックします。

(注) まだ FTDv インスタンスが起動していないことも確認する必要があります。

## Azure セキュリティグループの更新

ARM テンプレートは、管理インターフェイス用とデータインターフェイス用の 2 つのセキュリティグループを作成します。管理セキュリティグループは、FTDv 管理アクティビティに必要なトラフィックのみを許可します。ただし、データインターフェイスのセキュリティグループはすべてのトラフィックを許可します。

### 手順

展開のトポロジとアプリケーションのニーズに基づいてセキュリティグループのルールを微調整します。

(注) データインターフェイスのセキュリティグループは、少なくともロードバランサからの SSH トラフィックを許可する必要があります。



## Azure Logic App の更新

Logic App は、Auto Scale 機能の Orchestrator として機能します。ARM テンプレートによってスケルトン Logic App が作成されます。このアプリケーションを手動で更新して、Auto Scale Orchestrator として機能するために必要な情報を提供する必要があります。

### 手順

**ステップ 1** リポジトリから、LogicApp.txt ファイルをローカルシステムに取得し、次のように編集します。

**重要** 手順をすべて読んで理解してから続行してください。

手動の手順は、ARM テンプレートでは自動化されないため、Logic App のみ後で個別にアップグレードできます。

- a) 必須: すべての「SUBSCRIPTION\_ID」を検索し、サブスクリプション ID 情報に置き換えます。
- b) 必須: すべての「RG\_NAME」を検索し、リソースグループ名に置き換えます。
- c) 必須: すべての「FUNCTIONAPPNAME」を検索し、Function App 名に置き換えます。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"AutoScaleManager": {
  "inputs": {
    "function": {
      "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"
    }
  },
  "body": "@body('AutoScaleManager')",
  "function": {
    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"
  },
  "runAfter": {
    "Delay_For_connection_Draining": [
      "AutoScaleManager"
    ]
  }
},
"Deploy_Changes_to_FTD": {
  "inputs": {
    "body": "@body('AutoScaleManager')",
    "function": {
      "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"
    }
  },
  "runAfter": {
    "Delay_For_connection_Draining": [
      "AutoScaleManager"
    ]
  }
},
"DeviceDeRegister": {
  "inputs": {
    "body": "@body('AutoScaleManager')",
    "function": {
      "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"
    }
  },
  "runAfter": {
    "Delay_For_connection_Draining": [
      "AutoScaleManager"
    ]
  }
}
```

- d) (任意) トリガー間隔を編集するか、デフォルト値 (5) のままにします。これは、Auto Scale 機能が定期的にトリガーされる時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"triggers": {
  "Recurrence": {
    "conditions": [],
    "inputs": {},
    "recurrence": {
      "frequency": "Minute",
      "interval": 5
    },
  },
}
```

- e) (任意) ドレインする時間を編集するか、デフォルト値 (5) のままにします。これは、スケールイン操作中にデバイスを削除する前に、FTDv から既存の接続をドレインする時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"actions": {
  "Branch_based_on_Scale-In_or_Scale-Out_condition": {
    "actions": {
      "Delay_For_connection_Draining": {
        "inputs": {
          "interval": {
            "count": 5,
            "unit": "Minute"
          }
        }
      }
    }
  }
}
```

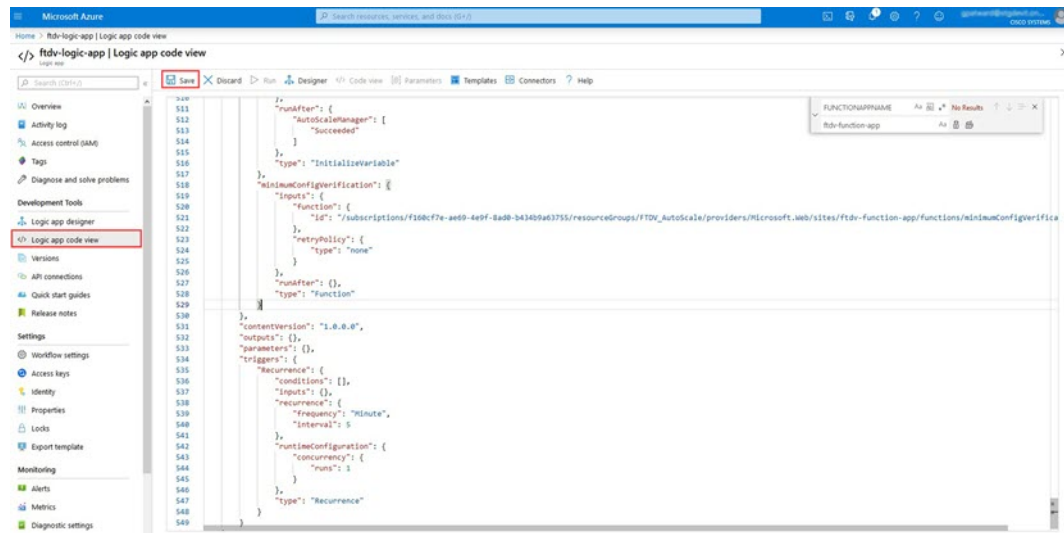
- f) (任意) クールダウン時間を編集するか、デフォルト値 (10) のままにします。これは、スケールアウト完了後に NO ACTION を実行する時間です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"actions": {
  "Branch_based_on_Scale-Out_or_Invalid_condition": {
    "actions": {
      "Cooldown_time": {
        "inputs": {
          "interval": {
            "count": 10,
            "unit": "Second"
          }
        }
      }
    }
  }
}
```

- (注) これらの手順は、Azure ポータルからも実行できます。詳細については、Azure のドキュメントを参照してください。

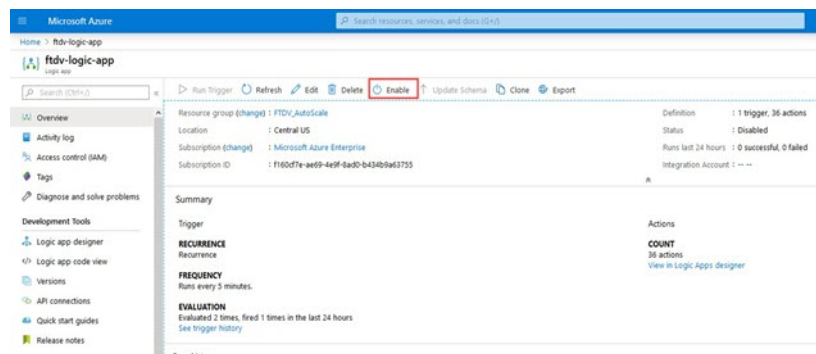
**ステップ 2** [Logic Appコードビュー (Logic App code view)] に移動し、デフォルトの内容を削除して、編集した LogicApp.txt ファイルの内容を貼り付け、[保存 (Save)] をクリックします。

図 21: Logic App コードビュー



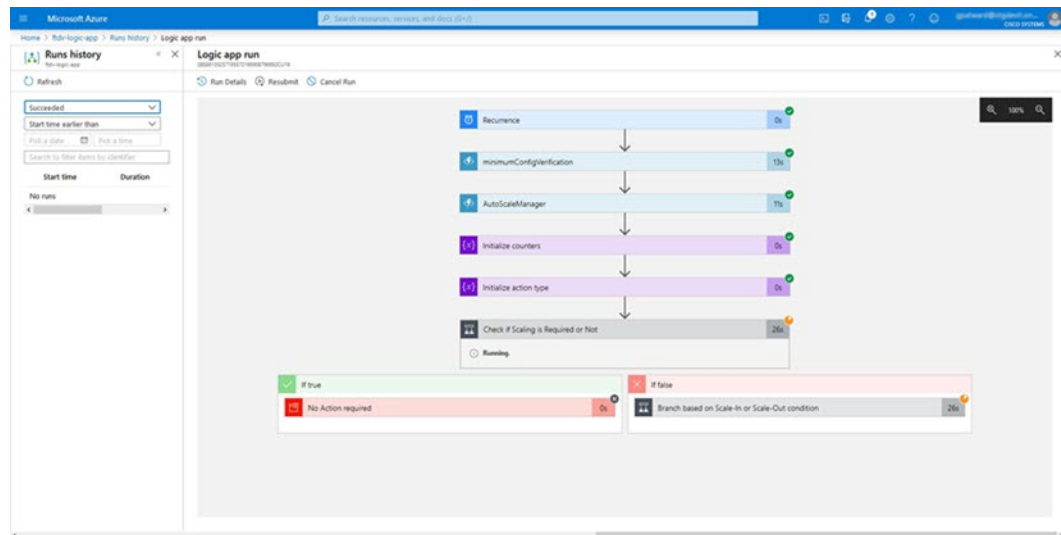
**ステップ 3** Logic App を保存すると、[無効 (Disabled)] 状態になります。Auto Scale Manager を起動する場合は、[有効化 (Enable)] をクリックします。

図 22: Logic App の有効化



**ステップ 4** 有効にすると、タスクの実行が開始されます。[実行中 (Running)] ステータスをクリックしてアクティビティを表示します。

図 23: Logic App の実行ステータス



- ステップ 5 Logic App が起動すると、導入関連のすべての手順が完了します。
- ステップ 6 FTDv インスタンスが作成されていることを VMSS で確認します。

図 24: FTDv 実行中のインスタンス

Name	Status	Health state
ftdv-vmss_0	Creating (Running)	
ftdv-vmss_1	Creating (Running)	
ftdv-vmss_2	Creating (Running)	

この例では、ARM テンプレートの展開で「minFtdCount」が「3」に設定され、「initDeploymentMode」が「BULK」に設定されているため、3 つの FTDv インスタンスが起動されます。

## FTDv のアップグレード

FTDv アップグレードは、仮想マシンスケールセット（VMSS）のイメージアップグレードの形式でのみサポートされます。したがって、FTDv は Azure REST API インターフェイスを介してアップグレードします。



- (注) 任意の REST クライアントを使用して FTDv をアップグレードできます。次に簡単な例を示します。

### 始める前に

- 市場で入手可能な新しい FTDv イメージバージョンを取得します（例：650.32.0）。
- 元のスケールセットの展開に使用する SKU を取得します（例：ftdv-azure-byol）。
- リソースグループと仮想マシンスケールセット名を取得します。

### 手順

**ステップ 1** ブラウザで次の URL にアクセスします。

<https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0>

**ステップ 2** パラメータセクションに詳細を入力します。

図 25: FTDv のアップグレード

The screenshot shows the Microsoft Azure REST API Explorer interface. The Request URL is `https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachineScaleSets/{vmScaleSetName}`. The Parameters section includes `subscriptionId` (Microsoft Azure Enterprise), `resourceGroupName` (FtdAutoScaleRG), `vmScaleSetName` (demo-ftdv-vms), and `api-version` (2018-06-01). The Headers section includes `Content-Type` (application/json). The Body section contains a JSON payload for updating the scale set.

**ステップ 3** 新しい FTDv イメージバージョン、SKU、トリガー RUN を含む JSON 入力を [本文 (Body)] セクションに入力します。

```
{
  "properties": {
    "virtualMachineProfile": {
      "storageProfile": {
        "imageReference": {
          "publisher": "cisco",
          "offer": "cisco-ftdv",
          "sku": "ftdv-azure-byol",
          "version": "650.32.0"
        }
      }
    }
  }
}
```

```

    },
    },
  },
}

```

**ステップ 4** VMSS が変更を受け入れると、Azure から成功の応答が返ってきます。

新しいイメージは、スケールアウト操作の一環として起動される新しい FTDv インスタンスで使用されます。

- 既存の FTDv インスタンスは、スケールセットに存在している間、古いソフトウェアイメージを使用し続けます。
- 前述の動作を上書きし、既存の FTDv インスタンスを手動でアップグレードできます。これを行うには、VMSS の [アップグレード (Upgrade)] ボタンをクリックします。選択した FTDv インスタンスが再起動されて、アップグレードされます。アップグレードされた FTDv インスタンスは手動で再登録および再設定する必要があります。この方法は推奨されません。

## Auto Scale ロジック

### スケーリングメトリック

ARM テンプレートは、FTDv 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。ARM テンプレートの展開中に、スケーリングメトリックに次のオプションがあります。

- CPU
- CPU、メモリ（バージョン 6.7 以降）。



(注) CPU メトリックは Azure から、メモリメトリックは FMC から収集されます。

### スケールアウトロジック

- **POLICY-1**：設定された期間に、いずれか FTDv の平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。「CPU、MEMORY」スケーリングメトリックを使用する場合、スケールアウトしきい値は、スケールセット内の任意の FTDv の平均 CPU またはメモリ使用率です。
- **POLICY-2**：設定された期間に、すべての FTDv デバイスの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。「CPU、MEMORY」スケーリン

グメトリックを使用する場合、スケールアウトしきい値は、スケールセット内の**すべての** FTDv デバイスの平均 CPU またはメモリ使用率です。

## スケールインロジック

- 設定された期間に、**すべての** FTDv デバイスの CPU 使用率が設定されたスケールインしきい値を下回った場合。「CPU、MEMORY」スケーリングメトリックを使用する場合、スケールセット内のすべての FTDv デバイスの CPU およびメモリ使用率が、設定された期間に設定されたスケールインしきい値を下回ると、CPU の負荷が最小の FTDv が終了用  
に選択されます

## 注意

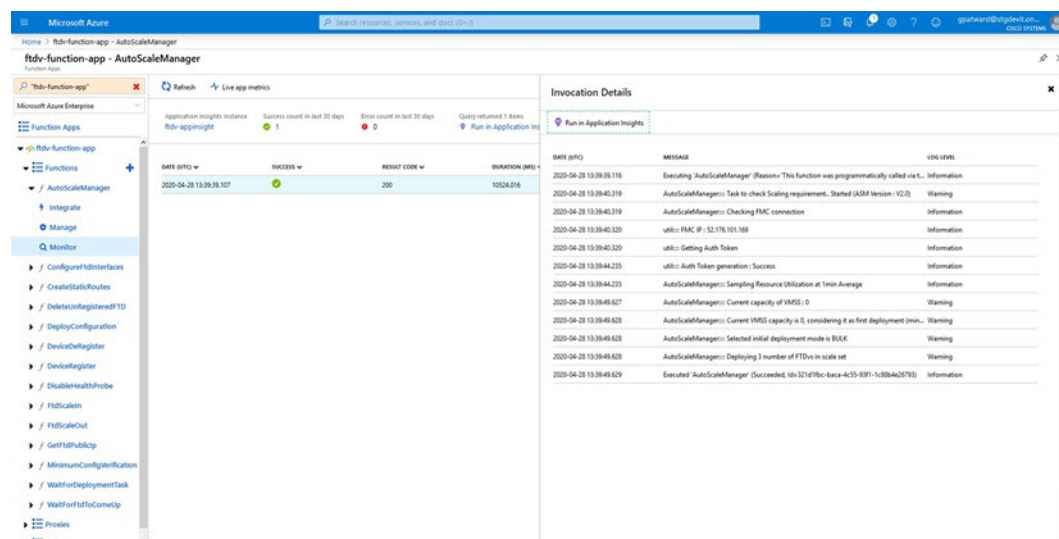
- スケールイン/スケールアウトは1つずつ行われます（つまり、一度に1つの FTDv だけがスケールインまたはスケールアウトされます）。
- FMC から受信したメモリ消費量のメトリックは、経時的に計算された平均値ではなく、瞬間的なスナップショット/サンプル値です。したがって、スケーリングを決定する際にメモリメトリックだけを考慮することはできません。展開時にメモリのみのメトリックを使用するオプションはありません。

# Auto Scale のロギングとデバッグ

サーバーレスコードの各コンポーネントには、独自のロギングメカニズムがあります。また、ログはアプリケーションインサイトにパブリッシュされます。

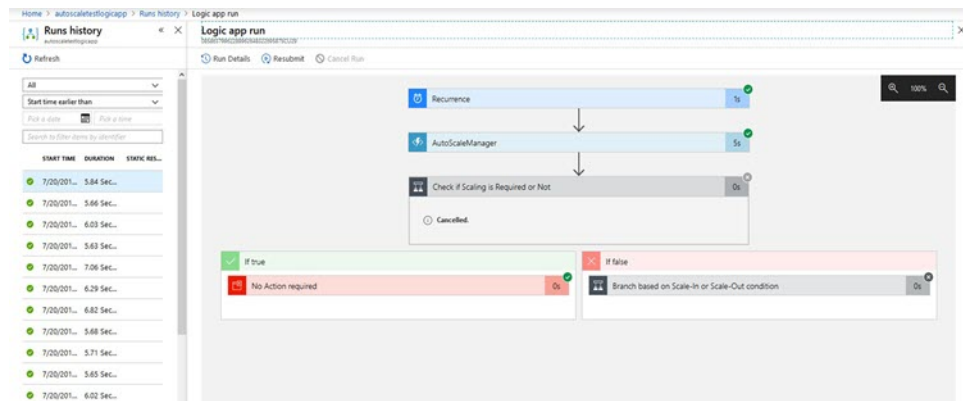
- 個々の Azure 関数のログを表示できます。

図 26: Azure 関数ログ



- Logic App とその個々のコンポーネントの実行ごとに同様のログを表示できます。

図 27: Logic App の実行ログ



- 必要な場合は、Logic App で実行中のタスクをいつでも停止または終了できます。ただし、現在実行中の FTDv デバイスが起動または終了すると、一貫性のない状態になります。
- 各実行または個々のタスクにかかった時間は、Logic App で確認できます。
- Function App は、新しい zip をアップロードすることでいつでもアップグレードできます。Logic App を停止し、すべてのタスクの完了を待ってから、Function App をアップグレードします。

## Auto Scale のガイドラインと制約事項

FTDv Auto Scale for Azure を導入する場合は、次のガイドラインと制限事項に注意してください。

- (バージョン 6.6 以前) スケーリングの決定は、CPU 使用率に基づきます。
- (バージョン 6.7 以降) スケーリングの決定には、CPU のみの使用率、または CPU とメモリの使用率を使用できます。
- FMC 管理が必要です。FDM はサポートされていません。
- FMC にはパブリック IP アドレスが必要です。
- FTDv 管理インターフェイスは、パブリック IP アドレスを持つように設定されます。
- IPv4 だけがサポートされます。
- FTDv Auto Scale for Azure は、デバイスグループに適用され、スケールアウトされた FTDv インスタンスに伝播されるアクセスポリシー、NAT ポリシー、プラットフォーム設定などの設定のみをサポートします。FMC を使用してデバイスグループの設定のみ変更できます。デバイス固有の設定はサポートされていません。



- ARM テンプレートの入力検証機能は限られているため、入力を正しく検証するのはユーザーの責任です。
- Azure 管理者は、Function App 環境内の機密データ（管理者ログイン情報やパスワードなど）をプレーンテキスト形式で確認できます。Azure Key Vault サービスを使用して、センシティブデータを保護できます。

## Auto Scale のトラブルシューティング

次に、FTDv Auto Scale for Azure の一般的なエラーシナリオとデバッグのヒントを示します。

- FMC への接続に失敗する：FMC の IP またはログイン情報を確認してください。FMC が障害または到達不能状態であるか確認します。
- FTDv に SSH 接続できない：複雑なパスワードがテンプレートを介して FTDv に渡されているか確認します。セキュリティグループで SSH 接続が許可されているか確認します。
- ロードバランサのヘルスチェックエラー：FTDv がデータインターフェイスの SSH に応答しているか確認します。セキュリティグループの設定を確認します。
- トラフィックの問題：ロードバランサーール、FTDv で設定された NAT ルールおよびステックルートを確認します。テンプレートとセキュリティグループルールで提供される Azure 仮想ネットワーク/サブネット/ゲートウェイの詳細を確認します。
- FTDv を FMC に登録できない：新しい FTDv デバイスに対応するために FMC の容量を確認します。ライセンスを確認します。FTDv バージョンの互換性を確認します。
- Logic App が VMSS にアクセスできない：VMSS の IAM ロール設定が正しいか確認します。
- Logic App の実行時間が長すぎる：スケールアウトされた FTDv デバイスで SSH アクセスを確認します。FMC でデバイス登録の問題を確認します。Azure VMSS で FTDv デバイスの状態を確認します。
- サブスクリプション ID 関連の Azure 関数のスローエラー：アカウントでデフォルトのサブスクリプションが選択されていることを確認します。
- スケールイン操作の失敗：Azure でのインスタンスの削除には長時間かかることがあります。このような状況では、スケールイン操作がタイムアウトし、エラーが報告されますが、最終的にはインスタンスが削除されます。
- 設定を変更する前に、Logic App を無効にし、実行中のすべてのタスクが完了するまで待ちます。

## 付録：ソースコードからの Azure 関数の構築

### システム要件

- Microsoft Windows デスクトップ/ラップトップ。
- Visual Studio (Visual Studio 2019 バージョン 16.1.3 でテスト済み)



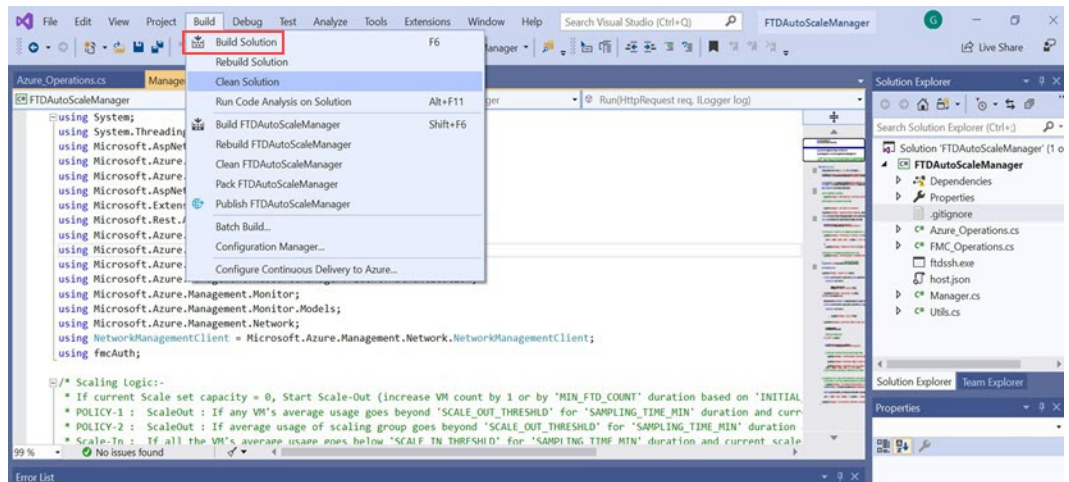
(注) Azure 関数は C# を使用して記述されます。

- 「Azure 開発」ワークロードを Visual Studio にインストールする必要があります。

### Visual Studio を使用したビルド

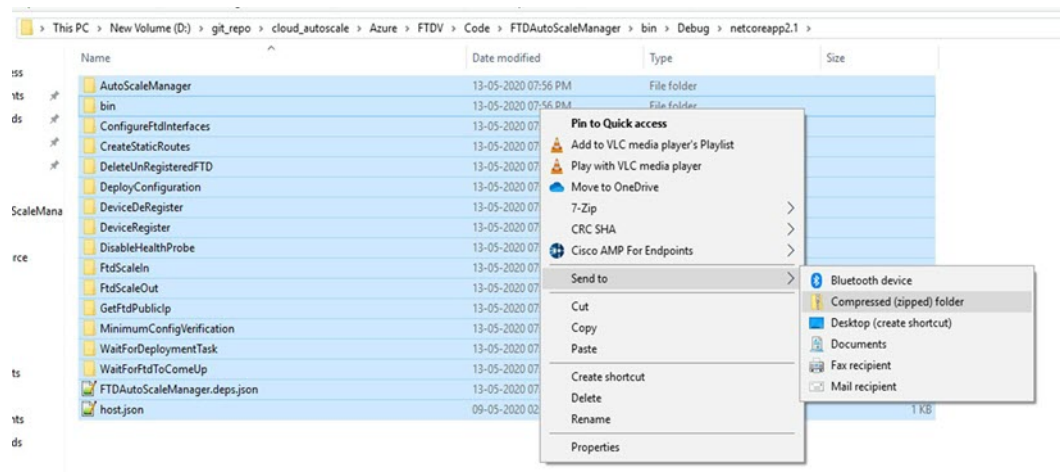
1. 「code」フォルダをローカルマシンにダウンロードします。
2. 「FTDAutoScaleManager」フォルダに移動します。
3. Visual Studio でプロジェクトファイル「FTDAutoScaleManager」を開きます。
4. クリーンアップしてビルドするには、Visual Studio の標準手順を使用します。

図 28 : Visual Studio ビルド



5. ビルドが正常にコンパイルされたら、\bin\Release\netcoreapp2.1 フォルダに移動します。
6. すべての内容を選択し、[送信先 (Send to)] > [圧縮 (ZIP) フォルダ (Compressed (zipped) folder)] の順にクリックして、ZIP ファイルを ASM\_Function.zip として保存します。

図 29 : ASM\_Function.zip のビルド







## 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](#) (67 ページ)
- [Firepower Management Center へのログイン](#) (68 ページ)
- [Firepower Management Center へのデバイスの登録](#) (68 ページ)
- [基本的なセキュリティポリシーの設定](#) (71 ページ)
- [Firepower Threat Defense CLI へのアクセス](#) (83 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 'Add Device' dialog box is shown with the following fields and values:

- 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。使用が必要で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 \(81 ページ\)](#)」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 \(83 ページ\)](#)」) 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](#) (71 ページ)
  - ステップ 2 [DHCP サーバーの設定](#) (75 ページ)
  - ステップ 3 [デフォルトルートの追加](#) (76 ページ)
  - ステップ 4 [NAT の設定](#) (78 ページ)
  - ステップ 5 [アクセス制御の設定](#) (81 ページ)
  - ステップ 6 [設定の展開](#) (82 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。

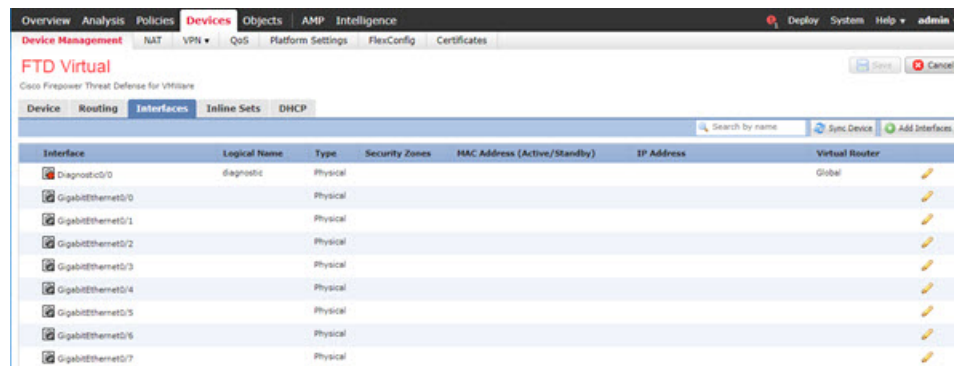
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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

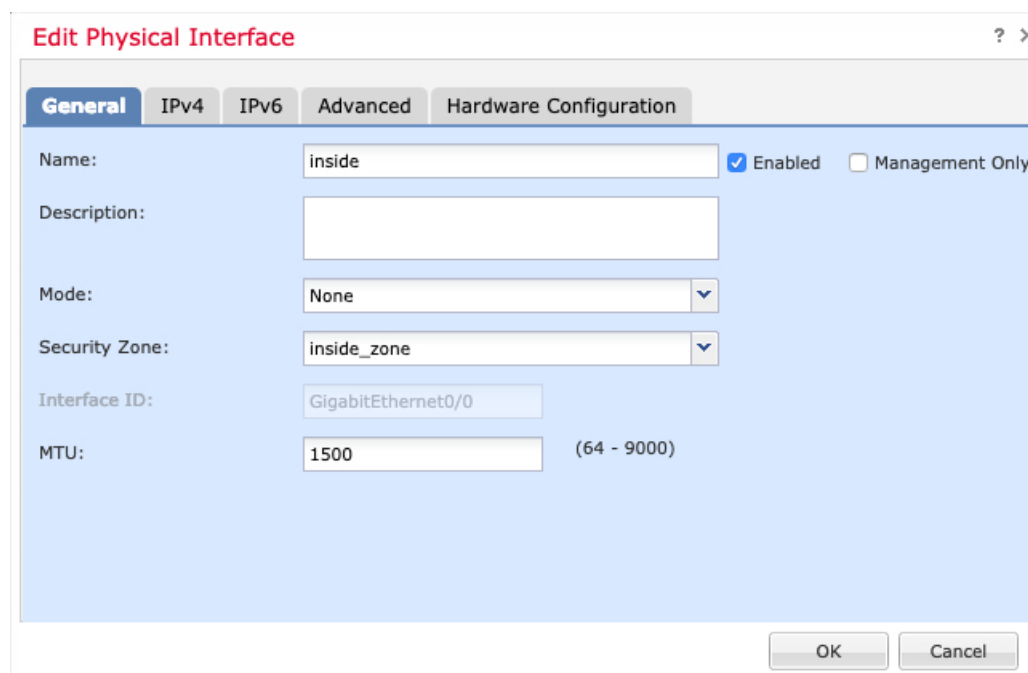
ステップ1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、デバイスをクリックします。

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。



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 **inside** 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。

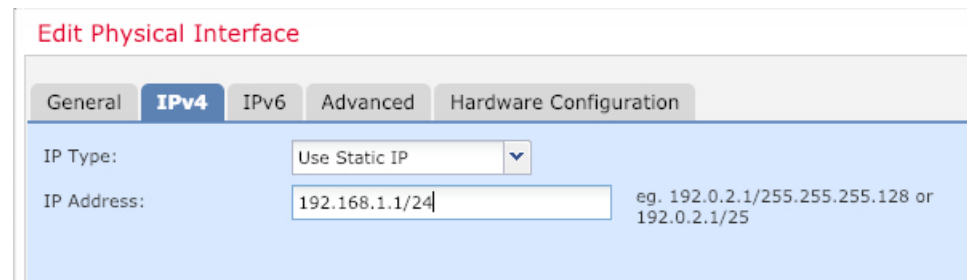
たとえば、**inside\_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てする必要があります。インターフェイスは、1つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできませんが、外部から内部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



- [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)

OK Cancel

- a) 48 文字までの [名前 (Name)] を入力します。  
たとえば、インターフェイスに「outside」という名前を付けます。
- b) [有効 (Enabled)] チェックボックスをオンにします。
- c) [モード (Mode)] は [なし (None)] に設定したままにします。
- d) [セキュリティゾーン (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。

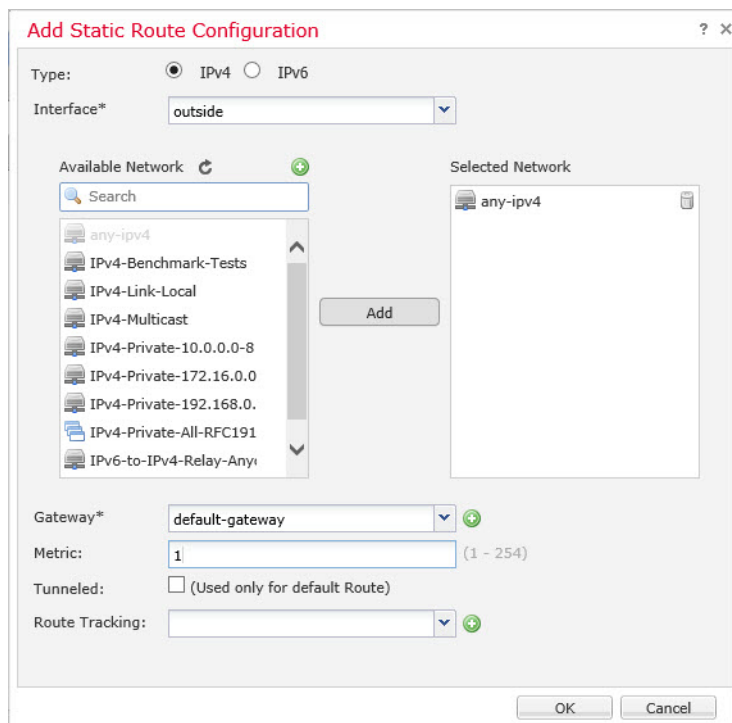
## デフォルトルートの追加

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。

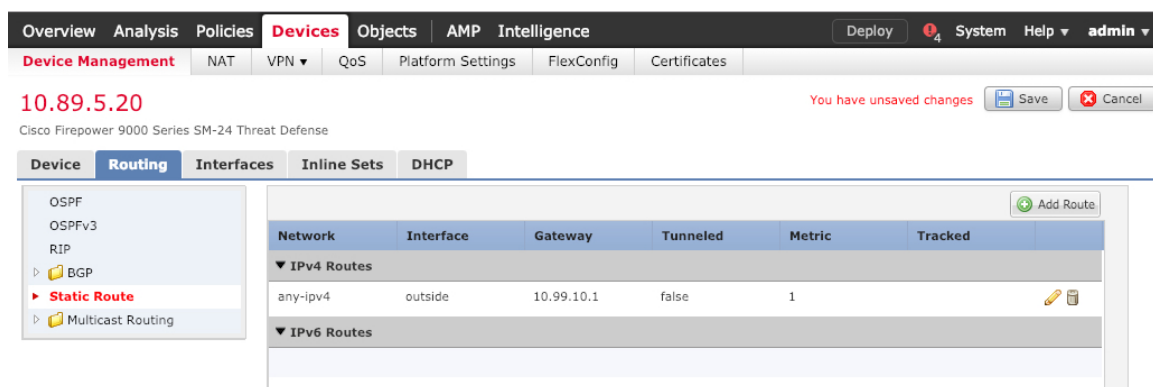
ステップ 2 [ルーティング (Routing)] > [スタティックルート (Static route)] を選択し、[ルートを追加 (Add route)] をクリックして、次のように設定します。



- [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。



ステップ 4 [保存 (Save)] をクリックします。

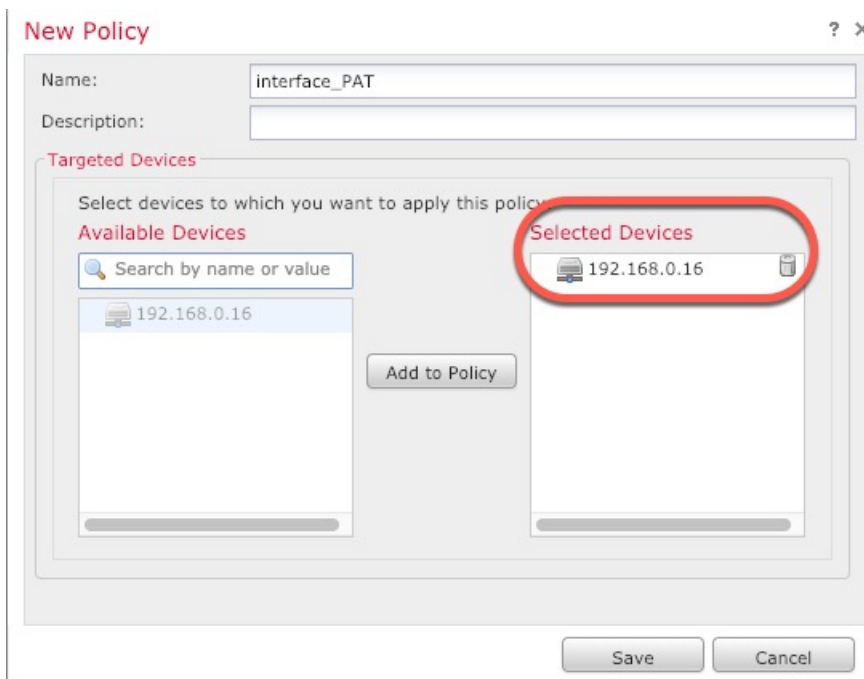
## NAT の設定

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。



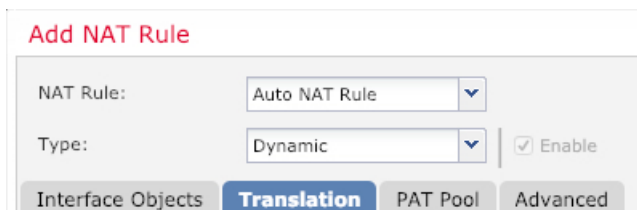


ポリシーが FMC に追加されます。引き続き、ポリシーにルールを追加する必要があります。

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

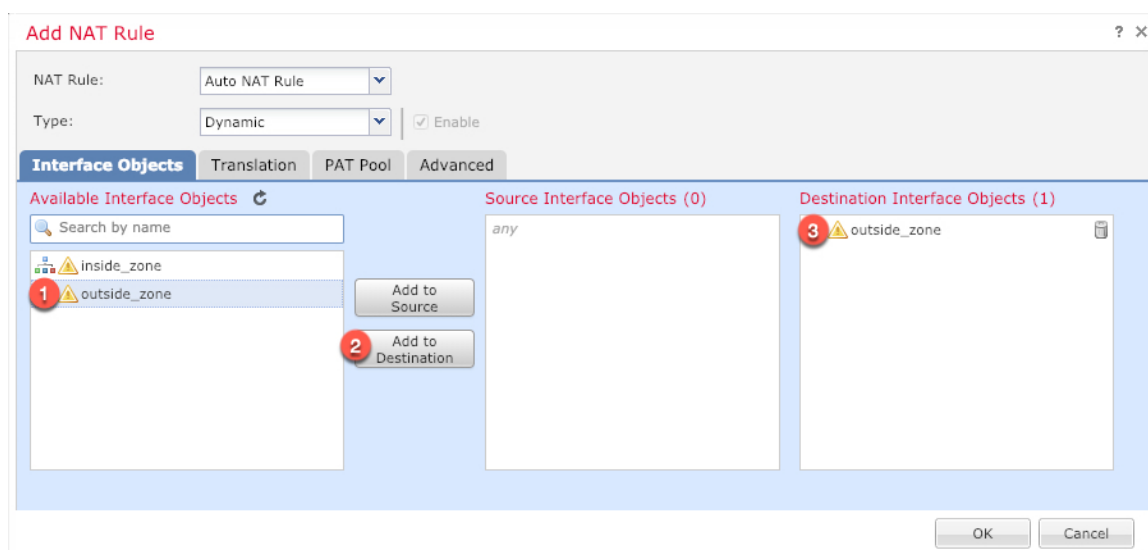
[NATルールの追加 (Add NAT Rule)] ダイアログボックスが表示されます。

**ステップ 4** 基本ルールのオプションを設定します。

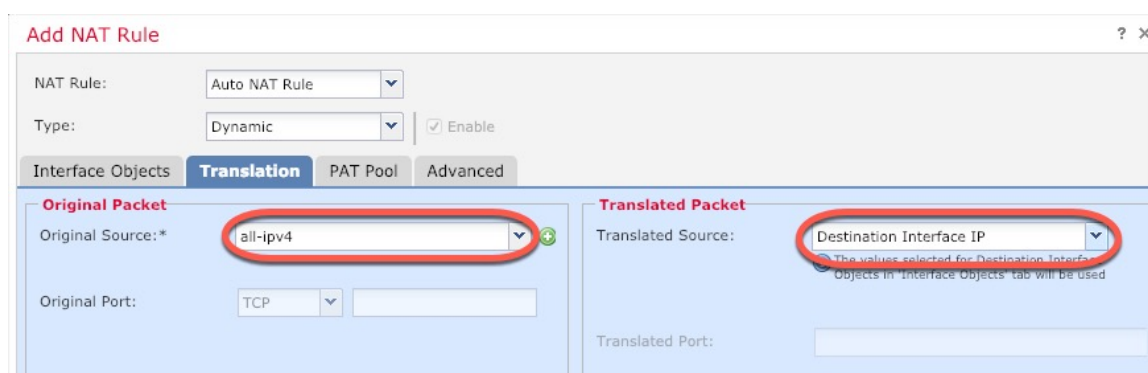


- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

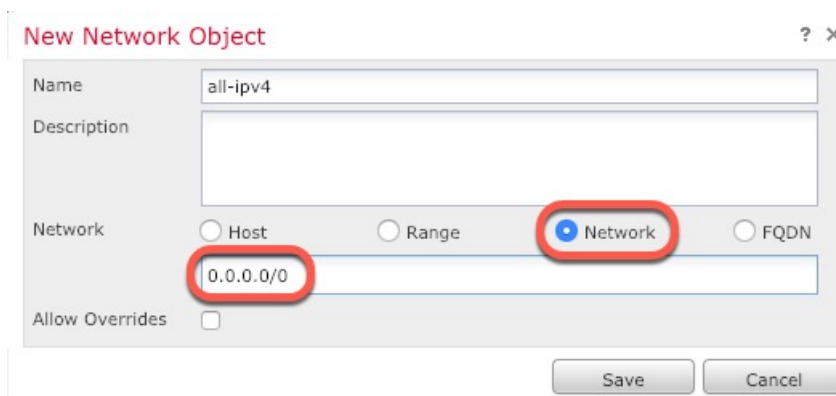
**ステップ 5** [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。



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。

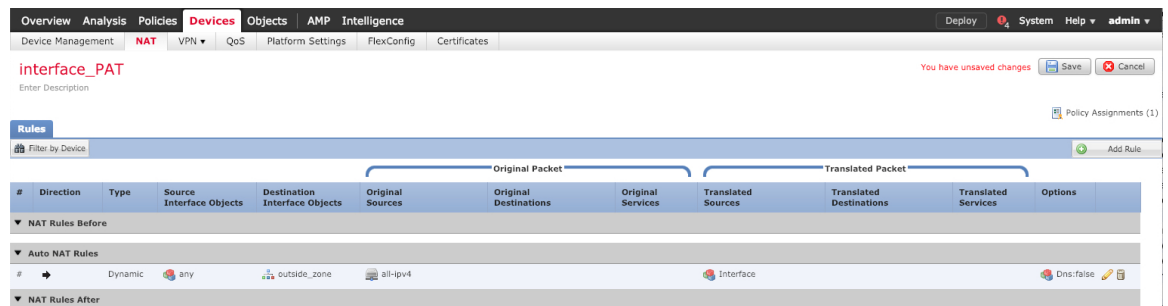


(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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

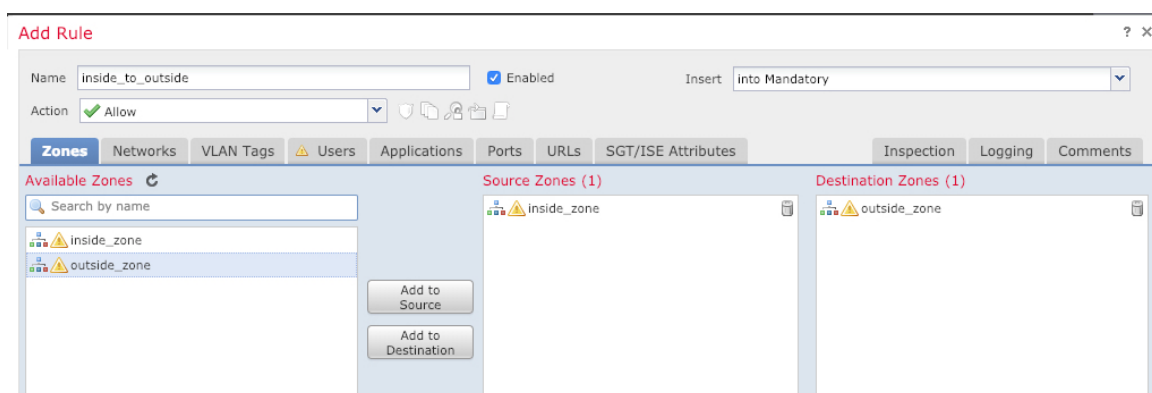
FTDv を FMC に登録したときに、基本の [すべてのトラフィックをブロック (Block all traffic)] アクセス コントロール ポリシーを作成した場合は、デバイスを通るトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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。

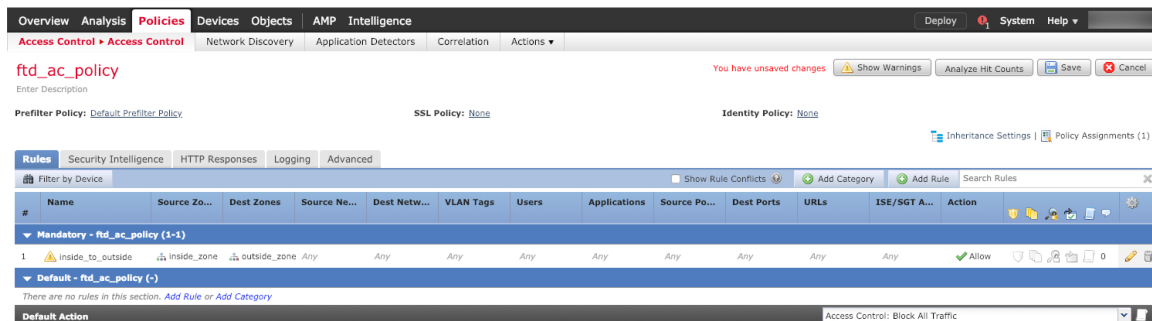


- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside\_to\_outside**)。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

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。



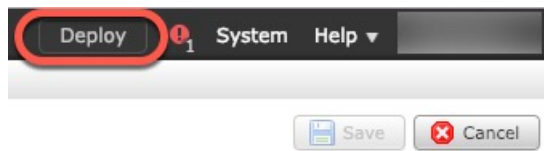
**ステップ 4** [保存 (Save)] をクリックします。

## 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

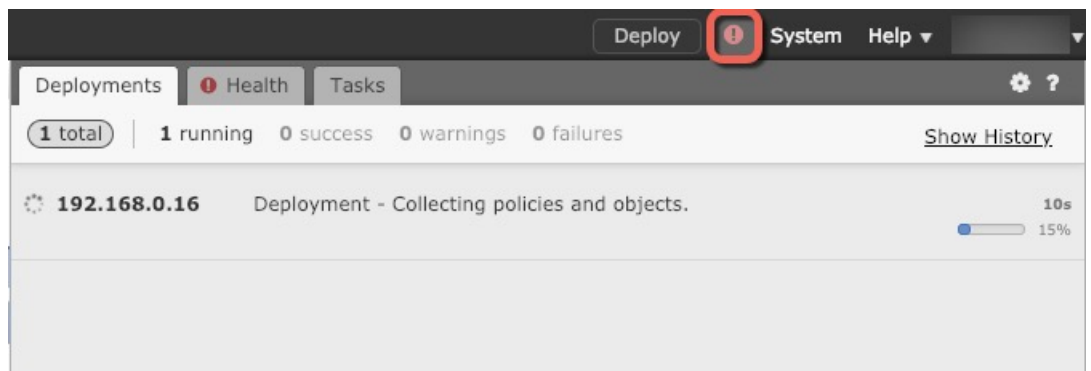
**ステップ 1** 右上の [展開 (Deploy)] をクリックします。



**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](#) (85 ページ)
- [初期設定](#) (86 ページ)
- [Firepower Device Manager でデバイスを設定する方法](#) (89 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](#) (67 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的なサブネットまたは 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）に初めてログインする際には、デバイスのセットアップウィザードを使用してシステムの初期設定を完了します。

### 手順

- ステップ 1** ブラウザを開き、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://192.168.45.45> で開きます。
- ステップ 2** ユーザー名 **admin**、およびパスワード **Admin123** を使用してログインします。
- 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、デフォルトに戻したい場合は、[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 \(89 ページ\)](#)」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

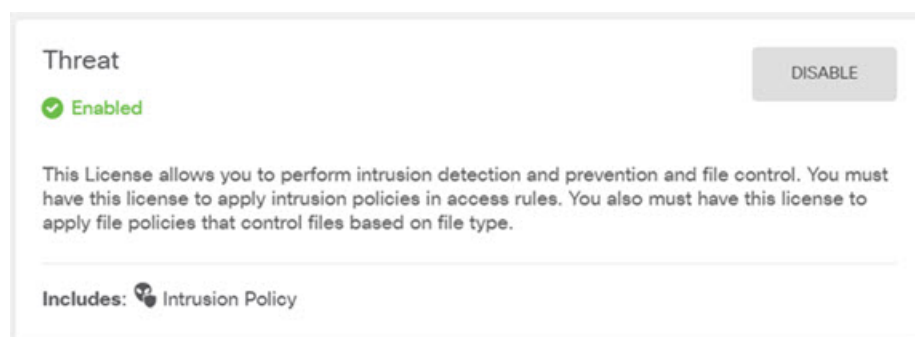
**ステップ 1** [デバイス (Device)] を選択してから、[スマートライセンス (Smart License)] グループの [設定の表示 (View Configuration)] をクリックします。

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 RAVPN 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 30: 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 31: 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:  /

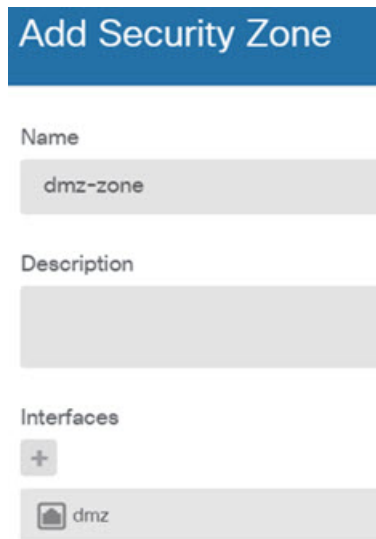
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

**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には常にゾーン 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 32: セキュリティ ゾーンオブジェクト

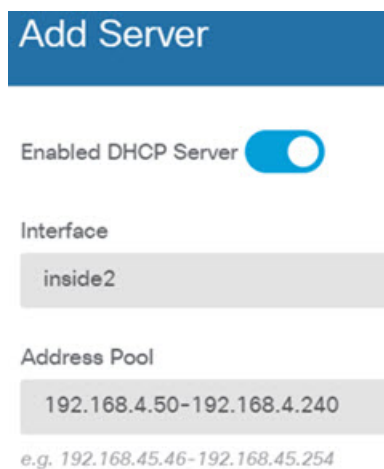


**ステップ 4** 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [DHCPサーバー (DHCP Server)] を選択してから、[DHCPサーバー (DHCP Servers)] タブを選択します。

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 33: 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構成します。

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 34: デフォルトルート

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and values:

- Protocol:** IPv4 (selected with a blue radio button), IPv6 (unselected with a grey radio button).
- Gateway:** isp-gateway
- Interface:** outside
- Metric:** 1
- Networks:** any-ipv4 (selected from a dropdown menu)

**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 ポリシーを構成します。

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に、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 ゾーンとの間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 35: アクセス コントロール ポリシー

Order	Title	Action
2	Inside_DMZ	Allow

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
inside_zone	ANY	ANY	dmz-zone	ANY	ANY

**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。





