# cisco.



## 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/



# 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  $(1 \, \stackrel{\sim}{\sim} \stackrel{\sim}{\mathrel{\sim}})$
- 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)  $(8 \sim \checkmark)$
- 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  $(4 \circ \mathcal{O} \text{ vCPU}, 14 \text{ GB}, 4 \circ \mathcal{O} \text{ vNIC})$
- Standard D3\_v2  $(4 \supset \mathcal{O} \text{ vCPU}, 14 \text{ GB}, 4 \supset \mathcal{O} \text{ vNIC})$

- 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。

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。

C/

- 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。
- Â
- 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す。
- •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)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な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 アドレスを設定で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。



# 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ベースの展開の他に、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。

Azure Cloud	1 Search for "Cisco Firepower NGFW Virtual Firewall" in the Azure Marketplace	2 Create the firewall	3 Configure FTDv settings	4 Deploy FTDv	
FMC/FDM					5 Manage FTDv by using FMC or FDM

	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 Azure マーケットプレイ スからの展開: 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 Azure マーケットプレイ スからの展開: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 Azure マーケットプレイ スからの展開: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 Azure マーケットプレイ スからの展開:FTDv を展開します。
5	FMC/FDM	<ul> <li>FTDv の管理:</li> <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>

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。
		• 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
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 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	<ul> <li>FTDv の管理:</li> <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使用できる 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 を使ってみる」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 リポジトリで使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想要素を表示します。

- **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、導入で使用される全リソース (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 10.0.0/16 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Nicl)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1 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50GB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 yX7txxxxxx1dnQ== \
    --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1** 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。



# 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  $(21 \, \stackrel{\sim}{\sim} \stackrel{\scriptstyle \checkmark}{
  ightarrow})$
- 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:



- •FTDv展開とマルチ可用性ゾーンのサポート。
- •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。
- 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

FTDvAuto 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。

- 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。

#### G

- **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。

スコープ

# 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。

#### C/

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

C)

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) ライセンスを使用できる必要があります。

#### 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

Cisco Firepower	Threat Defense Virtual	×	0
,		~	~
	Search by Product Family Search	for Solutions	

(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。

Group

#### 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。

🗵 3 : Device Management

Overview Analysis Policies Devices O	Objects AMP Intelligence				Depl	loy 🧕 System	n Help <b>+ adm</b>
Device Management NAT VPN Q	S Platform Settings FlexConfig Certificates						
Device Management List of all the devices currently registered on the Fire	epower Management Certer.						
View By I Group All (1)	Error (c)   warning (c)   Office (c)   Normal (c)   Depic	syment rending (o)			-	Search Device	0 A00 .
Name	Model	Version	Chassis	Licenses	Access Control Policy	0 0	Device
						0 :	igh Availability

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

Name:	AutoScale	Group		
evices				
Available De	evices		Devices	
		Add		

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

#### **Device Management**

List of all the devices currently registered on the Firepower Management Center.

View By : Group  All (0)   Error (0)   Warning (0)   Offline (0)	Normal (0)   Deployment Pendir	ng (0)	
Name	Model	Version	Chassis
AutoScaleGroup (0)			

## セキュアシェルアクセスの設定

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、ルールで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

ne:	LBHealthProbeSet	ttings		
geted Device:				
Select device Available De	s to which you want to a prices	apply this policy.	Selected Devices	
Search b	y name or value		AutoScaleGroup	ũ
		Add to Policy		

- 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

ARP Inspection			0	
Banner	Interface	IP Address		
External Autorhitotation HTTP HTTP EXP Secure Shell SMP SSL Syslog Time Synchronization UCAPL/CC Compliance		No records to displ	Address* Valiable Zo Search appkaton sotide armdemo-insi	/Interfaces

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

Devic	e Management	NAT VPN	QoS Platform S	Settings FlexConfig	Certificates					Deproy	R Stress Heb	admin
ut	oscaleNAT									Show War	mings 🗍 🗇 🗠	Cance
											Policy /	Assignments
a rite	by Device				-						0	Add Rule
						Original Packet			Translated Packet		2	
•	Direction	Туре	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT	Rules Before											
	•	Dynamic	rth outside	👍 inside	iii) any-ipv4	🚳 Interface	Criginal HTTP	🚳 Interface	application1	Criginal HTTP	🚳 Dnatfalse	18
	•	Dynamic	👍 outside	da inside	any-ipv4	🝓 Interface	Original HTTP1	🚳 Interface	application2	Criginal HTTP1	S Dristfalse	08
Auto	NAT Rules											
		for some in	1. baries	1 marite	ill and a			a laterda es			Constalas	20

(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。	新規作成
		注:小文字のみを使用してく ださい。	
		例:ftdv	
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
I

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 <b>できませ</b> 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 *	<ul> <li>FTDv VM 管理の管理者ユー ザーのパスワード。</li> <li>パスワードの長さは 12 ~ 72 文字で、小文字、大文字、数</li> <li>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。</li> <li>(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。</li> </ul>	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

I

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	POLCY-IPOLICY2	POLICY-1: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。 POLICY-2: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。 どちらの場合も、スケールイ	該当なし
		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。	
scalingMetricsList	文字列	スケーリングの決定に使用さ れるメトリック。 許可:CPU CPU、メモリ デフォルト:CPU	該当なし
cpuScaleInThreshold	文字列	<ul> <li>CPUメトリックのスケールインしきい値(パーセント単位)。</li> <li>デフォルト:10</li> <li>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。</li> <li>「Auto Scale ロジック(60ページ)」を参照してください。</li> </ul>	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	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)。	該当なし
		デフォルト:80	
		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。	
		「cpuScaleOutThreshold」は、 常に「cpuScaleInThreshold」よ り <b>大きく</b> する必要がありま す。	
		「Auto Scale ロジック (60 ページ)」を参照してくださ い。	
memoryScaleInThreshold	文字列	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)。	該当なし
		デフォルト:0	
		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。	
		「Auto Scale ロジック (60 ページ)」を参照してくださ い。	

I

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	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)。	該当なし
		デフォルト:0	
		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。	
		[memoryScaleOutThreshold]	
		は、常に 「memoryScaleInThreshold」よ り <b>大きく</b> する必要がありま す。	
		「Auto Scale ロジック (60 ページ)」を参照してくださ い。	
minFtdCount	整数	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。	該当なし
		例:2。	
maxFtdCount	整数	<ul> <li>スケールセットで許可される</li> <li>最大 FTDv インスタンス数。</li> <li>例:10</li> <li>(注) この数は FMC の容</li> </ul>	該当なし
		量によって制限され ます。	
		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。	

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	ドロップダウンから選択しま す。 この数値は、メトリックが平	該当なし
		均化される時間(分単位)を表します。	
		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。	
		<ul> <li>(注) Azure の制限により、有効な数値は</li> <li>1、5、15、および30だけです。</li> </ul>	

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
		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。	
		BULK: Auto Scale Manager は、「minFtdCount」 個の FTDvインスタンスを同時に展 開しようとします。	
		<ul> <li>(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。</li> </ul>	
		STEP: Auto Scale Manager 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。	
		<ul> <li>(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。</li> </ul>	
		BULK オプションで 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。	
		「minFtdCount」個の FTDv を展開するた めの合計時間 = (1 つの FTDv の起動時	

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 はすべて小文字を使用してくた	フ命名規則に関⁻ ごさい <b>スペース</b> ↑	する制限があります。制限を確認 やその他の特殊文字は使用しない	認するか、また 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'))]"
                  }
                }
            }
          1,
          "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。

#### 図 9: Azure ポータル

Microsoft Azure	P Search resources, services, and docs (G+/)			? 😳	
Home > FTDV_AutoScale					
FTDV_AutoScale					\$ ×
P Search (Ctrl+/)	] e + Add = Edit columns	CSV   🕅 Assign tags 📋 Delete 🛓 Export template   🎔 Feedback			
N Overview	Subscription (change) : Microsoft Azure Enterprise	Deployments : 1 Deploying			
Activity log	Subscription ID :				
Access control (AM)	Tags (change) : Click here to add tags				
Tags		*			
F Events	Filter by name				
Settings	Showing 0 to 0 of 0 records.			No grouping	V
4 Quickstart	Name Tu	Type †4	Location †4		
a Deployments					
De Policies					
1 Properties					
🔒 Locks					
Export template					
Cost Management					
1 Cost analysis		No resources to display			
Cost alerts (preview)	The resource	is are currently filtered and not all resources may be displayed, such as hidden resources.			
3 Budgets		Ty changing your filters if you don't see what you're looking for			
Advisor recommendations		Learn more of			
Monitoring		Contraction of the Class Research and Address			
Insights (preview)		Create resources Clear filters / Show hidden			
Alerts					
sa Metrics					
Diagnostic settings					
P Logs					

- **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

Microsoft Azure	P Search resources, services, and docs (G+/)
Iome > FTDV_AutoScale > New > Template deployment (d	leploy using custom templates)
Template deployment (deploy using custon	n templates)
Emplate deploymer	tt (deploy using custom templates)
Overview Plans	
Applications running in Microsoft Azure usually rely on a con to deploy and manage these resources as a group, using a .	bination of resources, like databases, servers, and web apps. Ature Resource Manager templates enable you ISON description of the resources and their deployment settings.
Edit your template with intelliSense and deploy it to a new or	existing resource group.
Useful Links Documentation	

- **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。

L

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。

🗵 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 カパラメータ (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

Microsoft Arure	P. Starch recourse, services, and does stimp	
ne > FTDV_AutoScale > New 3	Template deployment (deploy using custom templates) > Custom deployment	
ustom deployment		
TEMPLATE		
Customized template	Edit template Edit saramet. Learn more	
	and support the product of the state	
IASICS		
lubscription *	Microsoft Azure Enterprise	
Resource group *	Inthy,AutoScale	
	Create new	
ocation *	(US) Central US	
attings.		
lesource Name Prefix 🛈	hdv	
Artual Network Rg 🔿	PidiutoScaleRS	
Artual Network Name	Ind-utoScaleVirtualNetwork	
Virtual Network Cidr 🔘	10100/16	
Mpmt Subnet 〇	ManagementSub	
Nag Subnet O	Desive	
nside Subnet ()	middlab	
nside Network Gateway In	10.121	
nternal th IR	L METERNA	
Annual Internet (C)	C4030530	

(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。

	P. Search resources, services, and docs (G+/)	
Home > FTDV_AutoScale		
FTDV_AutoScale		
,0 Search (Otd+/)	, + Add III Edit columns 🕫 Delete resource group 🕐 Refresh → Move 🛓 Export to CSV   🕅 Assign tags 🛞 D	elete 🛓 Export template 🕴 🗢 Feedback
Overview  Activity log  Activity log  Access control (AAA)  Tags	Suborofonio Dango I: Morofo Javo Energila Suborofonio D : Moothe-aeld-aeld-baldbald355 Tags Chango I : Click here to add tags	Deployments : 2 Succeeded
F Events Settings	Ifter ty name.     (type ** all •)     (tocalion ** all •)     (*p Add filter)       Showing to 11 of 11 records.     Showindden types ·)	
4 Quidstart	Name 1.	Type 14
Deployments	• thdrappinsight	Application Insights
Policies	Ridv-dataint/SecGrp	Network security group
E Properties	C 💠 Rdvelb	Load balancer
A Locks	🗌 🗮 fidireit-publicip	Public IP address
Export template	🔲 📙 Rdv-function-app	App Service plan
Cost Management	🗌 🚸 Rdv-function-app	App Service
to Cost analysis	🗋 💠 hdv-lib	Load balancer
Cost alerts (preview)	M tovilogic-app	Logic app
(i) Budoets	🗌 😵 ftdv-mgmtint/SecGrp	Network security group
Advisor recommendations	🛄 🗞 ftdv-vmss	Virtual machine scale set
Monitoring	E ftdrgr/jeinspizow	Storage account
Insights (preview)     Alerts     Metrics     Diagnostic settings		
Logs     Advisor recommendations	< Previous Page 1 v of 1 Next >	

図 14: FTDv Auto Scale テンプレートの展開

### 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

	0			
9 C W	dhttps://ftdv-ft	Inction-app.scm.azurewebsites.net/DebugConsole		
ing started   @ 13.36.36.11	2/ CiscoHoliday 🚺 Ode	my_clico 🔛 cisco_Policies 🔨 Azure 🔤 Concur 🔊 ESPP	CEC all refersi A RK CP Problem loading page	
		Kudu Environment Debug console - Proc		
		/ wwwroot + 0 items   🏫	•	
		Name	Modifie	d Sizo
				1
			**	→ Move
		Kudu Remote Execution Console Type 'exit' then hit 'enter' to get a new CM	V A	→ Maye
File Home Sh	Compressed Fi	Kudu Remote Execution Console Type 'exit' then hit 'enter' to get a new CR oten two	V process.	×
	are View Etrai This PC > New Volume (D) 1	Kudu Remote Execution Console Type - sail: 'then hit 'enter' to get a new CH Generation A Aure Function t giuppo - doud, untersafe - Abare > FTDV - Abare function	♥A D process.	- C ×
<ul> <li>□ □ □ □ ▼ □</li> <li>□ □ □ □ ▼ □</li> <li>□ □ □ □ □ □ □ □ □ □</li> <li>□ □ □ □ □ □ □ □</li> <li>□ □ □ □ □ □ □</li> <li>□ □ □ □ □ □</li> <li>□ □ □ □ □</li> <li>□ □ □ □ □</li> <li>□ □ □ □</li> <li>□ □&lt;</li></ul>	are View Datas This PC > New Volume (D) 1 Name	Kudu Remote Execution Console Type "exit" them hit "enter" to get a new CM a s gtreps - cloud,wtoscak > Acue > FTD/ > Acue Function Determodind Type 1	D process.	- □ × × 0 × 0 × 0 × 0
I     D     w       Tee     Hone     So       ←     →     ↑     So       # Quick access     B     Docoments     d	are View Compressed Fi Data This PC > New Volume (0) Name AMJ Function.ap	Kudu Renote Execution Console           Type "exit" then hit "enter" to get a new CM           a           gitreps + doud_addoute > Acure > FTDV > Acure Function           Determodified         Type           24-06-2020 05.116         Compressed (pmp)	D process.	→ More → More → 0 Sauch AL
Image: training train	Are View Compressed Fr This PC > New Volume (D) 1 Name AMA Function ap	tudo Breaste Execution Console Type "exit" then hit "emien" to get a new CH internation git repo + doud, adocule > Azur > FTOV > Azur function Date modified Type 1 24-04-2020 02/4 Compressed (ppp	▼▲ 0 process. 3 5 11,321 KB	× • • • • • • • • • • • • • • • • • • •
I     O     ■       File     Home     Dh       €     →     ↑       ■     Documents     #       ■     Doemtosts     #       ■     Potentists     #	are View Compressed Fr Detain This PC > New Volume (D) 1 Name F ADM Function ap	Kudu Remote Execution Console Type "exit" then hit "enter" to get a new CM a splingo (dout, whosek > Apre > FTOV > Apre Function Determodified Type 1 24:04:000 05:15 Compressed (syp	D process.	→ Move → Move → 0 → 0 5 seech Al
I         D         v         I           file         None         So           d         -         ↑         -           Documents         #         Documents         #	are Very Compressed In This PC + News (Norme (D) + Name Assault - Assault function.clp	Kudu Remote Execution Contole Type Fail: then hit "enter" to get a new CP contention at sgl.rep > dout,wdsscale > Azwe > FTDV > Azwe Function Date modified           Date modified         Type         1 26-04-2020 05/18 Compressed (sep)	C process Sise 11,02782	→ More → More v 0 Sauth A <sub>L</sub>

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。

义	16 :	FTDv	サー	バー	レス関数	
---	------	------	----	----	------	--

	Name	Modified	Size	
Ŧo	The AutoScaleManager	8/24/2019, 12:19:56 PM		
t o	🖀 bin	8/24/2019, 12:19:56 PM		
F0	ConfigureFtdInterfaces	8/24/2019, 12:20:08 PM		
10	CreateNatRules	8/24/2019, 12:20:08 PM		
+0	CreateStaticRoutes	8/24/2019, 12:20:08 PM		
t o	E DeleteResources	8/24/2019, 12:20:08 PM		
t o	E DeleteUnRegisteredFTD	8/24/2019, 12:20:09 PM		

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 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



- . . .

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

#### ☑ 18 : FTDv Function App

Microsoft Azure	P. Search resources, services, and docs (G+/).
Home > ftdv-function-app ftdv-function-app function App	
🔎 "fidv-function-app" 🛛 🗙	n Preview the new Azure Functions management experience
Microsoft Azure Enterprise 🛛 🗠	Overview Putform features
E Function Apps	The Star David Warman David and Warman and The
🕶 🚸 ftdv-function-app 🛛 🕽 🎽	stop 3 2010 O Metalt Z Vet poent prove Q Meter public Z volverosa up content E celete
Encloss     f Autosclettanager     f Autosclettanager     f Configure/Initiates     f OresteStatioBoutes     f OtestestatioBoutes     f OtestestatioBoutes     f Otestestationes     f Otestestationes     f Otabletestationes     f Otabletestationes     f Otabletestationes     f Otabletestationes     f Otabletestationes	Statu:     Subscription     Resource group     URL       ● Running     Microsoft Azure Enterprise     FIDV, AutoScale     Http://differ-function-seps.autreweb/stas.net       Subscription ID HidodTr+ax85-449F-tabbleALB66493755     Location Central US     Ago Sarrise plan / pricing ter Risk-function-seps (Consumption)       Configured features
f GetFtdPublictp     f MinimumConfigVerification     f WaitForDeploymentTask     f WaitForFtdToComeUp     The Deployment	
Slots	

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

	P Search resources, services, and dots (G+J)		S & O (		grates (Datates) OSCO
Home > ftdv-function-app > Configuration					
Configuration					
O Refresh 🖾 Save 🗙 Discard					
Application settings Function runtime setting	ngs General settings				
Application settings					
Application settings are encrypted at rest and tri	ansmitted over an encrypted channel. You can choose to display them in plain test in your browser by usin	ng the controls below. Application Settings are exposed as env	ronment variables for access by your app	lication at runtime	. Learn more
- Nan pacification cattion	A Advanced with 🖂 Eller				
T we approach setting Show values	Anyando ent 1 miler				
Name	Value	Source	Deployment slot setting	Delete	Eak .
ANY JPV4 NAME	Hidden value. Click show values button above to view	App Config		8	0
APPINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click show values button above to view	App Config			0
AZURE_UTIUTY_IP	Hidden value. Click show values button above to view	App Config		8	0
AZURE_UTILITY_IP_NAME	Hidden value. Click show values button above to view	App Config		8	0
AzureWeblobsDeshboard	Hidden value. Click show values button above to view	App Config		8	0
AzureWebJobsStorage	Hidden value. Click show values button above to view	App Config		8	0
DELETE_FAULTY_FTD	Hidden value. Click show values botton above to view	App Config		8	0
DEVICE_GROUP_NAME	Hidden value. Click show values button above to view	App Config		8	0
FMC_DOMAIN_UUD	Hidden value. Click show values button above to view	App Config		8	0
PMC_P	Hidden value. Click show values button above to view	App Config		8	0
FMC_RASSWORD	Hidden value. Click show values button above to view	App Config		8	0
FMC, USERNAME	Hidden value. Click show values button above to view	App Config		8	0

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

Microsoft Azure	P Search resources	services, and does (G+)	© ? 😳 gpatward@stgdevit.on
Home > ftdv-vmss   Access control (IA	M		Add role assignment
Rg ftdv-vmss   Access con	trol (IAM)		Table ()
P Search (Ctri+/)	e + Add EE Edit columns ○ Refresh   × Remove   ♥	Got feedback?	Contributor O V
			Assign access to 📀
Overview	Check access Role assignments Deny assignments Classic a	dministrators Roles	Function App 🗸 🗸
Activity log	2.0.0.0000		Subscription *
Access control (AM)	Check access Review the level of access a user, group, service principal,	Add a role assignment     View role assignments	Microsoft Azure Enterprise 🗸
Tags	or managed identity has to this resource. Learn more of		Select ③
Diagnose and solve problems	Find ()	assigning a role to a user, group, service and managed identities that have role	Search by name
Settings	Azure AD user, group, or service principal 🗸 🗸	principal, or managed identity: assignments granting them access at this scope.	ftdv-function-app
Instances	Search by name or email address		/subscriptions/1_
2 Networking		Add Learn more C* View Learn more C*	
K Scaling		View days are immente	
Storage		View the years among respire noise	
👽 Operating system		and managed identities that have been	
C Security		scope.	
Size		Your Learn more of	
E Extensions			Selected members:
Continuous delivery			/ fide-function-app
Configuration			/subscriptions/f1 Remove
Dupgrade policy			
🗣 Health and repair			
💲 identity			
III Properties			
A Locks			
Export template			
Monitoring			Sun Divisio
Insights			Lawe Cours

#### 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 NAVE/providers/Microsoft.Web/sites/FUNCTIONAPPNAVE/functions/AutoScaleVenager"
            }
                            "Deploy_Changes_to FTD": {
                                 "inputs": {
                                      "body": "@body('AutoScaleManager')",
                                      "function": {
                                           "id":
"/subscriptions/SUBSCRIPTION ID/resourceGroups/RG NAVE/providers/Microsoft.Neb/sites/FUNCTIONAPENAVE/functions/DeployConfiguration"
                                      }
                            "DeviceDeRegister": {
                                 "inputs": {
                                      "body": "@body('AutoScaleManager')",
                                      "function": {
                                           "id":
"/subscriptions/SUBSCRIPTION ID/resourceGroups/RG NAME/providers/Microsoft.Web/sites/FUNCTIONAPPRAME/functions/DeviceDeRegister"
                                      }
                                 },
                                 "runAfter": {
                                      "Delay For connection Draining": [
```

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。

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。

- (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 Logic App.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

Microsoft Azure		.P Search resources, services, and docs (G+I)			
iome > ftdv-logic-app					
tdy-logic-app					
P Search (Ctrl+,)		▷ Run Trigger 🕐 Refresh 🧷 Edit 🗑 Delete 🕐 Enable ↑ Update Schema 🚯 Clone 🚭 Export			
A Overview	^	Resource group (change) 1 FTDV, AutoScale	Definition	: 1 trigger, 36 actions	
Activity log		Location : Central US	Status	: Disabled	
Access control (1) b		Subscription (change) I Microsoft Azure Enterprise	Runs last 24 hours	: 0 successful, 0 failed	
R ACCESS CONTROL (MANY		Subscription ID : f160d7e-ae69-4e9f-6ad0-b434b9a63755	Integration Account 1		
P Triagnose and solve problem Development Tools		Summary Trigger	Actions		
Logic app designer		RECURRENCE	COUNT		
/> Logic app code view		Recurrence	36 actions		
Versions		FREQUENCY Runs every 5 minutes.	the state of the state		
API connections		EVALUATION			
Quick start guides		Evaluated 2 times, fired 1 times in the last 24 hours			
miles and a second		see trigger notory			

**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

Microsoft Azure	P. Search resources, services, a	mő docs (0+))			
Home > ftdv-logic-app > Runs history > Logic ap	p run				
[♣] Runs history < × http://app.app	Logic app run				×
O Refresh	😒 Run Details 🛞 Resubmit 🚫 Cancel Run				
Succeeded V Start time earlier than V		8 Recurrence	a°		Q 10% Q
Pick a date         Pick a time           Search to fater korns by identifier           Start time         Duration		iminimumConfigVentication	05		
No runs		JutoScaleManager	n		
		(x) Initialize counters	• • • •		
		(x) Initialize action type	a°		
		Check # Scaling is Required or Not	26		
		(),			
	er fine		If false		
	No Action required	6	Branch based on Scale-In or Scale-Out con	dtion 26	Ĩ

- 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

Microsoft Azure		P	earch resources, services, and docs (G	+/)
Home > ftdv-vmss   Instances				
ftdv-vmss   Instances				
A Search (Ctrl+/)	≪ ▷ start	🤇 Restart 🔲 Deallocate 🕒 Reim	age 🗊 Delete 个 Upgrade 💟	Refresh   Protection Policy
S Overview	A Searc	h virtual machine instances		
Activity log	Nar	ne	Status	Health state
Access control (IAM)	t ft dv	-vmss_0	Creating (Running)	
Tags	ndv	rvmss_1	Creating (Running)	
Diagnose and solve problems	t ft dv	-vmss_2	Creating (Running)	
Settings				
Instances				
Networking				
Scaling				
Storage				

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。



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

MICrosoft Azure					Contract Laters 1-000-107-1089 📞 Dearch 📿 PONTAN			
				Overview Solutions Products - Documentation Pricing Training	nketplace v Partners v Support v Blog More v Free account >			
					Request URL			
1-06-0	24				PATCH https://management.azure.com/subscriptions/1160dTe-ae69-4e94-8ad0-b434td9a63755;hesourceGroups,PtdAutoScaleRt			
ale s	et.							
				© Copy				
//ma	nagement	azure.com/s	ubscript	lons/{subscriptionId}/resourceGroups/{resourceGroupName}/provider	Parameters			
					subscription24" Microsoft Azure Enterprise 💙			
me	ters				resourceGrouptane* PtdAutoScaleRG			
	In	Required	Туре	Description	vesca) esettame* demo-fidu-vmss			
d	path	True	string	Subscription credentials which uniquely identify Microsoft Azure subscription. The subscription ID forms part of the URI for every service call.	api-version* 2018-06-01			
	path	True	string	The name of the resource group.	nate value +			
	path	True	string	The name of the VM scale set to create or update.				
	query	True	string	Client Api Version.	Headers			
					context-type" application/json			
					name value +			
BO	dy							
		Туре		Description	Body			
		VirtualMad	ineScaleSe	tidentity The identity of the virtual machine scale set, if configured.	k			
e mezi	la oro/en-U	Norfes/central/		The purchase plan when deploying a virtual machine scale set from Vf	"properties": {     "victualBackLeeRradLie": {     "victualBackLeeRradLie": {     } }			

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。



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

Home > ftdv-function-app - AutoScaleN	Aanager							
ftdv-function-app - AutoSca	leManager							\$
P "ftdv-function-app"	🔾 Refresh 🔸 Live app m	vetrics			Invocation Details			*
Acrosoft Azure Enterprise 🛛 🗸					,			
Function Apps	Application insights instance ftdv-appinsight	Success count in fait 30 days	Error count in last 30 days	Query returned 1 items     P Run in Application Ins	Run in Application Insights			
🔹 🥎 ftdv-function-app								
+ ⊞ Functions +	DATE (MTC) V	success v	RESULT CODE V	DURATION (MS) -	BARE (URC)	MISSAGE	LOG UNVEL	
· / AutoScaleManager	2020-04-28 13:39:39:107	0	200	10524.016	2020-04-28 13:39:39:116	Executing 'AutoScaleManager' (Reasons' This function was programmatically called via t.	Information	
9 Integrate					2020-04-28 13-39-40-319	AutoScaleManageriii Task to check Scaling requirement. Started (ASM Version : V22)	Warning	
O Manage					2020-04-28 19:39:40:319	AutoScaleManaget::: Checking MAC connection	Information	
Q Monitor					2020.04.28.15-26-40.120	utile - Gattion Auth Token	Information	
Configural Industratives					2020-04-28 13:39:44 235	util:::: Auth Token generation : Success	Information	
· / ConstatiuticReater					2020-04-28 13:39:44.235	AutoScaleManager::: Sampling Resource Utilization at 1min Average	Information	
Colored States (TT)					2020-04-28 13:39:49.627	AutoScaleManaget::: Current capacity of VMSS::0	Warning	
· / Desta Cardinaution					2020-04-28 13:39:49:628	AutoScaleManager Current VMSS capacity is 0, considering it as first deployment (min	Warning	
• f organyconnya ann					2020-04-28 13:39:49:628	AutoScaleManager::: Selected initial deployment mode is BULK	Warning	
• / DeviceDenegister					2020-04-28 13:39:49:628	AutoScaleManager Deploying 3 number of FTDvs in scale set	Warning	
<ul> <li>J DeviceRegister</li> </ul>					2020-04-28 13:39:49.629	Executed 'AutoScaleManager' (Succeeded, Ids 321d19bc-baca-4c55-93/1-1c88b4e26793)	Information	
DisableHealthProbe								
FtdScalein								
FtdScaleOut								
f GetFtdPublicip								
f MinimumConfigVerification								
f Wait/orDeploymentTask								
f WaitForFtdToComeUp								
Proxies								

• 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

Home > autoscaletestlogicapp > Runs history >	Logic app run				
Runs history « ×	Logic app run				×
🖏 Refresh	③ Run Details () Resubmit () Cancel Run				
		(2) Recumence			Q 1075 Q
Pick a date			L		
Search to filter dama by identifier		4utoScaleManager		55	
START TIME DURATION STATIC RES.		-	$\downarrow$		
• 7/20/201 5.66 Sec		Check if Scaling is Required or Not		Os	
Ø 7/20/201 6.03 Sec		() Cancelled.			
Ø 7/20/201 5.63 Sec	1 March		M faire		
© 7/20/201_ 7.06 Sec_	R DOR		in tage		0
0 7/20/201 6.29 Sec	No Action required	0	Branch based on Scale-In or S	cale-Out condition	Os
O 7/20/201 6.82 Sec					
● 7/20/201 5.68 Sec					
O 7/20/201 5.71 Sec					
O 7/20/201 5.65 Sec					
Ø 7/20/201 6.02 Sec					

- ・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:ロードバランサルール、FTDvで設定されたNATルールおよびスタ ティ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

- 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

Image: Weight of the second	Build         Debug         Test         Analyze         Tools         Extensions         Window         Help         Search Visual Studio (Ctrl+Q)         P         FTDAutod           Build Solution         F6         anager ▼         戸         ●         ●         ●         ●         ■         ●         ■         ●         ■         ●         ●         ■         ●         ■	icaleManager 🕜 – 🗗 🗙 LÂ Live Share 🖌
Azure_Operations.cs Manag	e Clean Solution	▼ Solution Explorer V ×
EDTDAutoScaleManager Using System; using System.Threadi using Microsoft.Azur using Microsoft.Azur using Microsoft.Asph using Microsoft.Rest using Microsoft.Rest using Microsoft.Azur using Microsoft.Azur using Microsoft.Azur	Run Code Analysis on Solution     Alt +F11     per <ul> <li>Run ChittpRequest reg. (Logger log)</li> </ul> Will Bild FTDAutoScaleManager         Shift +F6           Rebuild FTDAutoScaleManager         Pack FTDAutoScaleManager           Pack FTDAutoScaleManager         Pack FTDAutoScaleManager           Batch Build         Configuration Manager           Configure Continuous Delivery to Azure         Enter State	Search Solution Explorer (Club)     Search Solution FIDAUSCaleManager (1 e     Club FIDAU
using Microsoft.Azur using Microsoft.Azur using Microsoft.Azur using Microsoft.Azur using faking Kicrosoft.Azur using faclung Logici- * If current Scale * POLICY-1 : Scale * POLICY-2 : Scale * Scale-In : If Al 99% • ON issues found	Anagement.Monitor; .Management.Monitor; .Management.Monitor; .Management.Metwork; entClient = Microsoft.Azure.Management.Network.NetworkManagementClient; et capacity = 0, Start Scale-Out (increase VM count by 1 or by 'MIN_FID_COUNT' duration based on 'INITIAL Dut : If any VM's average usage goes beyond 'SCALE_OUT_IMRESHLO' for 'SAMPLING_TIME_MIN' duration and current but : If average usage of scaling group goes beyond 'SCALE_OUT_IMRESHLO' for 'SAMPLING_TIME_MIN' duration the VM's average usage more helow 'SCALE IN THRESHLD' for 'SAMPLING_TIME_MIN' duration and current scale *	

- 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

Name	Date modified	Туре		Size
AutoScaleManager	13-05-2020 07:56 PM	File folder		
🦲 bin	13-05-2020 07 <mark>;56.PM</mark>	File folder		
ConfigureFtdInterfaces	13-05-2020 07 Pin t	o Quick access		
CreateStaticRoutes	13-05-2020 07 🛓 Add	to VLC media player's Playlist		
DeleteUnRegisteredFTD	13-05-2020 07 🛓 Play	with VLC media player		
DeployConfiguration	13-05-2020 07 🌰 Mov	e to OneDrive		
a 🕒 DeviceDeRegister	13-05-2020 07 7-Zip	)	>	
DeviceRegister	13-05-2020 07 CRC	SHA	>	
DisableHealthProbe	13-05-2020 07 🔀 Cisco	AMP For Endpoints	>	
	13-05-2020 07			
FtdScaleOut	13-05-2020 07	to	>	Bluetooth device
GetFtdPublicIp	13-05-2020 07 Cut			Compressed (zipped) folde
MinimumConfigVerification	13-05-2020 07 Copy	/		Desktop (create shortcut)
	13-05-2020 07 Paste	•		Documents
WaitForFtdToComeUp	13-05-2020 07	te chost cut		Fax recipient
🔛 FTDAutoScaleManager.deps.json	13-05-2020 07 Delet			Mail recipient
🔛 host.json	09-05-2020 02	le .		1 KB



# 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  $\sim \mathcal{O} \square \mathcal{J} / \mathcal{V}$  (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。

Host:*	ftd-1.cisco.com	-
Display Name:	ftd-1.cisco.com	
Registration Key:*		
Group:	None	*
Access Control Policy:*	Initial Policy	~
Smart Dicensing		
Maiware Threat URL Filtering		
Maiware Threat URL Filtering Advanced		
Maiware Threat URL Filtering Advanced Unique NAT ID: <sup>†</sup>	✓ cisco123nat	

- [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じ登録 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(81ページ)」を参照してください。

Name:	ftd_ac_policy			
Description:				
Select Base Policy:	None		~	
Default Action:	Block all traffic O Intrusio	n Prevention 🔿 Ne	twork Discovery	

- [スマートライセンス (Smart Licensing)]:展開する機能に必要なスマートライセンスとして、[マルウェア (Malware)] (AMP マルウェアインスペクションを使用する予定の場合)、[脅威 (Threat)](侵入防御を使用する予定の場合)、および[URL](カテゴリベースの URL フィルタリングを実装する予定の場合)を割り当てます。
- •[一意の NAT ID (Unique NAT ID)]: FTDv ブートストラップ設定で指定した NAT ID を 指定します。
- 「パケットの転送(Transfer Packets)]: デバイスから FMC へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、 デバイスが検査用としてイベントメタデータ情報とパケットデータを FMCに送信します。 このオプションを無効にした場合は、イベント情報だけが FMCに送信され、パケットデー タは送信されません。
- ステップ3 [登録(Register)]をクリックし、正常に登録されたことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが 表示されます。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。

Overview Analysis Policies	Devices Objects	AMP Inte	elligence			<b>e</b> , o	eploy System H	icip + admin +
Device Management NAT	VPN VQoS Platfor	m Settings	FlexConfig C	ertificates				
FTD Virtual							8	Cancel
isco Firepower Threat Defense for VMIS	iare (							
Device Routing Interface	Inline Sets DHG	OP .						
					Q, S	earch by name	Sync Device	Add Interfaces •
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address		Virtual Router	
Disgnostic0/0	diagnostic	Physical					Global	1
GipabitEthernet0/0		Physical						1
GipsbitEthernet0/1		Physical						1
Gipsbitthemet0/2		Physical						1
GipabitEthemetb/3		Physical						1
GipabitEthernet0/4		Physical						1
GigabitEthernetD/S		Physical						1
GigabitEthernetD/6		Physical						1
GipabitEthemet0/7		Physical						1

**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 Int	terface								? X
	General IPv4	IPv6	Advanced	Hardware	Configuration	Ľ				
	Name:		inside				Enabled	🗌 Ма	nagement	Only
	Description:									
	Mode:		None			*				
	Security Zone:		inside_zone			*				
	Interface ID:		GigabitEthern	et0/0						
	MTU:		1500		(64 - 9000)					
							OF	¢	Cancel	
a	) 48 文字までの	)[名前	(Name) ]	を入力しる	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すが、 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。

Edit Phys	sical Int	erface			
General	IPv4	IPv6	Advanced	Hardware Configu	uration
IP Type: IP Address	:	l	Jse Static IP	<b>v</b>	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 Inter	face				? ×
General IPv4	IPv6 Advar	ced Hardware	e Configuration		
Name:	outside			Enabled	Management Only
Description:					
Mode:	None			*	
Security Zone:	outside	zone		*	
Interface ID:	Gigabit	thernet0/0			
MTU:	1500		(64 - 9000)		
				0	K 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 Phys	Edit Physical Interface								
General	IPv4	IPv6	Advanced	Hardware	e Configuration				
IP Type:		ι	Jse DHCP	¥					
Obtain def DHCP:	ault route	using 🧧	2						
DHCP rout	e metric:	1	L		(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					
			ОК	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。

Type:	◉ IPv4 ○ IPv6		
Interface*	outside	~	
Available Net	work C 🔘	Selected Network	
🔍 Search		any-ipv4	1
any-ipv4			
💂 IPv4-Ben	chmark-Tests		
📄 IPv4-Link	c-Local		
📄 IPv4-Mult	ticast	dd	
📰 IPv4-Priv	ate-10.0.0.0-8		
IPv4-Priv	ate-172.16.0.0		
IPv4-Priv	ate-192.168.0.		
IPv4-Priv	ate-All-RFC191		
IPV6-t0-1	PV4-Relay-Any		
Gateway*	default-gateway	▼ ②	
Metric:	1	(1 - 254)	
Tunneled:	Used only for default Rou	te)	
Route Tracking:		v ()	

- •[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 Obj	jects AMP Int	elligence		Deplo	y 🔒 System	Help <del>v</del> ad
Device Management NAT	VPN VOS	Platform Settings	FlexConfig	Certificates			
10.89.5.20 Cisco Firepower 9000 Series SM-24 Thi	reat Defense				You have un	saved changes	Save 🛛 🔀
Device Routing Interfac	es Inline Sets	DHCP					
OSPF							O Add Route
OSPFv3	Network	Interface	Gateway	Tunneled	Metric	Tracked	
▷ 📁 BGP	▼ IPv4 Routes						
► Static Route	any-ipv4	outside	10.99.10.1	false	1		P 🗎
Multicast Routing	▼ 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。

Description: Targeted Devices Select devices to which you want to apply this po Available Devices Search by name or value	Selected Devices	
Targeted Devices Select devices to which you want to apply this po Available Devices Search by name or value	Selected Devices	
Select devices to which you want to apply this po Available Devices Search by name or value	Selected Devices	
Search by name or value	Selected Devices	
	192.168.0.16	
192,168,0.16	-	
Add to Policy		
		I

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。

Add NAT Rule			
NAT Rule:	Auto NAT Rule	¥	
Type:	Dynamic	~	I Enable
Interface Objects	Translation	PAT Pool	Advanced

- [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。

					?
NAT Rule: Type:	Auto NAT Rule	▼ ▼	nable		
Interface Objects	Translation	PAT Pool Adv	vanced		
Available Interface (	)bjects 🖒		Source Interface Objects (0)	Destination Interface Objects (1)	
Search by name  inside_zone  inside_zone		Add to Source	any	3 🛆 outside_zone	

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。

Add NAT Rule						?	×
NAT Rule:	Auto NAT Rule	~					
Type:	Dynamic	~	🕑 Enable				
Interface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:*	all-ipv4			3	Translated Source:	Destination Interface IP	
Original Port:	ТСР	*					
					Translated Port:		

•[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。

Name	all-ipv4			
Description				
Network	O Host	O Range	Network	○ FQDN
Allow Override	s			

(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1 [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。

Overview An	alysis Po	licies Devices C	bjects AMP Int	elligence	16				Deploy 04 S	ystem Help	≠ admin <del>v</del>
interface		VPN V QOS	Platform Settings	FlexConfig C	ertificates			You	have unsaved change	s 📄 Save	Cancel
Enter Description											
Rules										Policy	Assignments (
Hilter by Device										0	Add Rule
					Original Pack	et		Translated Packet		1	
# Direction	Туре	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
▼ NAT Rules Befo	re										
▼ Auto NAT Rules											
# +	Dynamic	🥵 any	outside_zone	📄 all-ipv4			🥵 Interface			🍓 Dns:false	e 🥜 🗟
▼ NAT Rules Afte	r										

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、デバイスを通過す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。

Add Rule												? ×
Name inside	e_to_outside				🗹 Enal	oled	Insert	into Manda	tory			~
Action 🖌 A	llow			▼ ∪ D ,@ t	6							
Zones	Networks	VLAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attributes	5		Inspection	Logging	Comments
Available Zor	nes 🖒				Source	Zones (1	L)		Destina	tion Zones (1)		
Search by	name				👬 🛦 i	nside_zon	e	6	<u></u>	utside_zone		6
📩 📐 inside_	zone											
📩 📐 outside	e_zone											
				Add to Source								
				Add to Destination								

- •[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。

Over	view Analysis P	olicies Dev	ices Objects	AMP Int	elligence							Dep	oloy 🏮	System Help 🔻	
Acce	s Control + Access	Control Ne	twork Discovery	Application	n Detectors	Correlation	Actions <b>v</b>								
ftd_ Enter I	ftd_ac_policy  You have unsaved changes  Analyze Hit Counts  Hit Counts  Cancel														
Prefilt	Prefilter Policy: <u>Default Prefilter Policy</u> SSL Policy: <u>None</u> Identity Policy: <u>None</u>														
	Tag Inheritance Settings   🕎 Policy Assignments (1)														
Rule	s Security Intellige	nce HTTP Re	sponses Logo	ing Advance	ed										
台F	Iter by Device								Show Rul	e Conflicts 😡	Add Categor	y 🕓 Add Ru	le Search F	tules	×
#	Name	Source Zo	Dest Zones	Source Ne	Dest Netw	VLAN Tags	Users	Applications	Source Po	Dest Ports	URLs	ISE/SGT A	Action	U 🗅 🧏 🕁 🔳 🛡	*
- M	andatory - ftd_ac_pol	cy (1-1)													
1	🔌 inside_to_outside	🚓 inside_zone	🚓 outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	002000	a 🖉
🐨 D	afault - ftd_ac_policy	(-)													
There	are no rules in this sect	ion. <mark>Add Rule</mark> or A	Add Category												
Defa	alt Action										Access Cor	trol: Block All Tr	affic		× _ i

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。

Dep	ploy Policies Version:2019-03-05 03:17 PM					? ×
	Device	Inspect Interruption	Туре	Group	Current Version	(j)
	<b>■</b> 192.168.0.16	No	FTD		2019-02-28 07:11 AM	

**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。



# 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) 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 Manage 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

Threat	DISABLE
C Enabled	
This License allows you to perform intrusion detection and p	revention and file control. You must
have this license to apply intrusion policies in access rules. A apply file policies that control files based on file type.	ou also must have this license to

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(2) 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。

and states and states and the				
Edit Physi	cal Interfa	ace	Э	
in the second				
Interface Name				Statue
internace realitie				Otatuo
dmz				
Description				
IPv4 Address	IPv6 Address		Advanced Options	
Туре				
Static 🗸				
IP Address and	Subnet Mask			
100 160 6 1		,	24	
192.108.0.1		1	24	
e.g. 192.168.5.15/	17 or 192.168.5.1	15/25	5.255.128.0	

図 31:インターフェイスの編集

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

Add Security Zone
Name
dmz-zone
Description
Interfaces +
dmz

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

Add Server
Enabled DHCP Server
Interface
inside2
Address Pool
192.168.4.50-192.168.4.240
e.g. 192.168.45.46-192.168.45.254

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

Add Static Route							
Protocol							
O IPv4	O IPv6						
Gateway							
isp-gatewa	y						
Interface							
outside							
Metric							
1							
Networks							
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の間のトラフィック 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

Add Ad	ccess	Rul	e								
Order	Title				Action						
2 ~	Inside	_DM2	Z		🔁 Allo	w 🖍					
Source/De	stination	Ap	plications UR	Ls User	rs Intrusion Policy	/ Fi	le policy Log	gging			
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。

© 2018–2021 Cisco Systems, Inc. All rights reserved.