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

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

- Standard D3（4 つの vCPU、14 GB、4 つの vNIC）
- Standard D3_v2（4 つの vCPU、14 GB、4 つの vNIC）

- Standard D4_v2（8 つの vCPU、28 GB、8 つの vNIC）（**バージョン 6.5 の新機能**）
- Standard D5_v2（16 の vCPU、56 GB、8 つの vNIC）（**バージョン 6.5 の新機能**）
- Standard_D8s_v3—8 vCPU、32 GB、4vNIC（**バージョン 7.1 の新機能**）
- Standard_D16s_v3—16 vCPU、64 GB、8vNIC（**バージョン 7.1 の新機能**）
- Standard_F8s_v2—8 vCPU、16 GB、4vNIC（**バージョン 7.1 の新機能**）
- Standard_F16s_v2—16 vCPU、32 GB、8vNIC（**バージョン 7.1 の新機能**）

FTDv および Azure の前提条件および要件

前提条件

- Microsoft Azure アカウント。https://azure.microsoft.com/en-us/ で 1 つ作成できます。

  Azure でアカウントを作成した後は、ログインしてマーケットプレイスから Cisco Firepower Threat Defense を検索し、「Cisco Firepower NGFW Virtual (NGFWv)」を選択します。

- Cisco スマートアカウント。Cisco Software Central で作成できます。

  FTDv のライセンス。Firepower システムで使用できる機能ライセンスの概要（ヘルプリンクを含む）については、『Cisco Firepower System Feature Licenses』を参照してください。

- FTDv と Firepower System の互換性については、『Cisco Firepower Threat Defense Virtual Compatibility』を参照してください。

通信パス

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

  （注） 6.7 以降では、必要に応じて、管理インターフェイスの代わりにデータインターフェイスを FMC の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。FMC アクセスに対するデータインターフェイスの設定に関する詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。

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

- 外部インターフェイス（必須）—Firepower Threat Defense Virtual をパブリックネットワークに接続するために使用されます。

FTDv および Azure のガイドラインと制限事項

サポートされる機能

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

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

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

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

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

FTDv スマートライセンスのパフォーマンス階層

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

表 *1: FTDv* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/34 GB	16 Gbps	10,000

- シスコ スマート ライセンス アカウントを使用する BYOL（Bring Your Own License）。
- PAYG（Pay As You Go）ライセンス。顧客がシスコ スマート ライセンシングを購入せずに FTDv を実行できる従量制課金モデル。登録された PAYG FTDv デバイスでは、ライセンス供与されたすべての機能（マルウェア、脅威、URL フィルタリング、VPN など）が有効になっています。ライセンス供与された機能は、FMC から編集または変更することはできません（バージョン 6.5 以上）。

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

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

サポートされない機能

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

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

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

- ERSPAN（GRE を使用。これは Azure では転送されません）

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

Firepower デバイスの管理方法

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

Firepower Device Manager

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

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

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

Firepower Management Center

Cisco Firepower Management Center（FMC）。

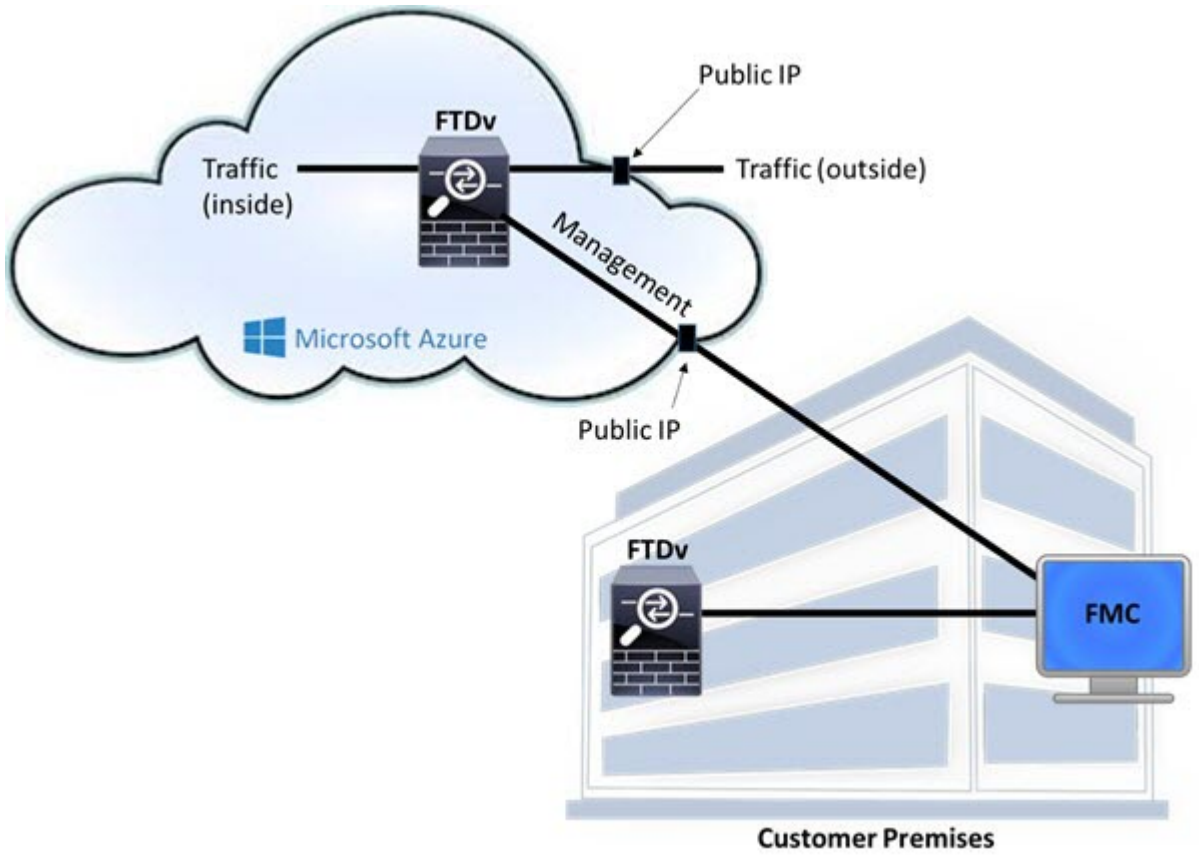
多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの FDM の代わりに FMC を使用してデバイスを設定します。

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

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

Azure 上の FTDv のネットワークトポロジの例

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



導入時に作成されるリソース

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

- Firepower Threat Defense 仮想マシン（VM）
- リソースグループ
  - Firepower Threat Defense Virtual は常に新しいリソースグループに導入されます。ただし、Firepower Threat Defense Virtual を別のリソースグループ内の既存仮想ネットワークにアタッチすることはできます。
- 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、VM NIC がハイパーバイザをバイパスしてその下の PCIe カードに直接アクセスできるようになり、ネットワークが高速化します。AN は VM のスループットパフォーマンスを大幅に向上させ、コアの追加（つまり VM の拡大）にも対応します。

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

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

Azure ルーティング

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

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

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

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

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

仮想ネットワーク内の VM のルーティング設定

Azure 仮想ネットワーク内のルーティングは、クライアントの特定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。