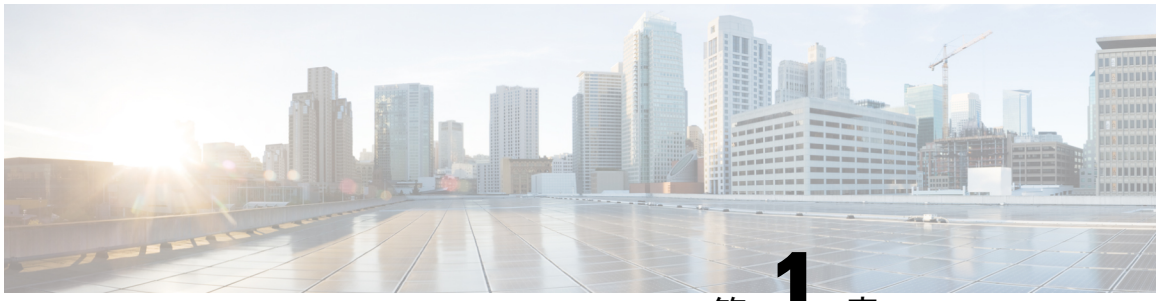
# Cisco Secure Firewall Threat Defense Virtual スタートアップガイド（バージョン 7.4）

**初版**：2023 年 12 月 13 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

# Cisco Secure Firewall Threat Defense Virtual の概要

Cisco Secure Firewall Threat Defense Virtual（Threat Defense Virtual）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ます。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

今日の組織は、ネットワークセキュリティの必要を満たす上で、物理的ソリューションと仮想コントロールポイントの組み合わせに依存しています。ビジネスには、ブランチオフィス、企業データセンター、および各拠点間のすべてのポイントで一貫したポリシーを維持しつつ、さまざまな物理ファイアウォールと仮想ファイアウォールを幅広い環境に展開する柔軟な対応が必要です。データセンターの統合から、オフィスの移転、合併と買収、アプリケーションの需要がピークに達する時期に至るまで、シスコの仮想ファイアウォールポートフォリオは、統一されたポリシーの利便性とあらゆる分野に展開できる柔軟性により、セキュリティ管理の簡素化を支援します。

Cisco Secure Firewall Threat Defense Virtual では、Snort IPS が導入されたシスコの実績のあるネットワークファイアウォール 、URL フィルタリング、およびマルウェア防御が融合されています。物理、プライベート、およびパブリッククラウド環境で一貫したセキュリティポリシーを使用して、脅威からの保護を簡素化します。ネットワークを詳細に可視化し、脅威の発生源とアクティビティをすばやく検出します。検出後、運用に影響が及ぶ前に攻撃を阻止します。

Secure Firewall Threat Defense Virtual は、人気のある仮想化ソリューションです。自動化されたリスクのランク付けと影響フラグを使用して脅威に優先順位を付け、即時の対応が必要なイベントにリソースを集中させます。ライセンスポータビリティにより、すべてのアプライアンスで一貫したポリシーと一元的な管理を維持しつつ、オンプレミスのプライベートクラウドからパブリッククラウドへと柔軟に移行できます。シスコ スマート ソフトウェア ライセンシングにより、仮想ファイアウォールのインスタンスを簡単に展開、管理、追跡できます。

• Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

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

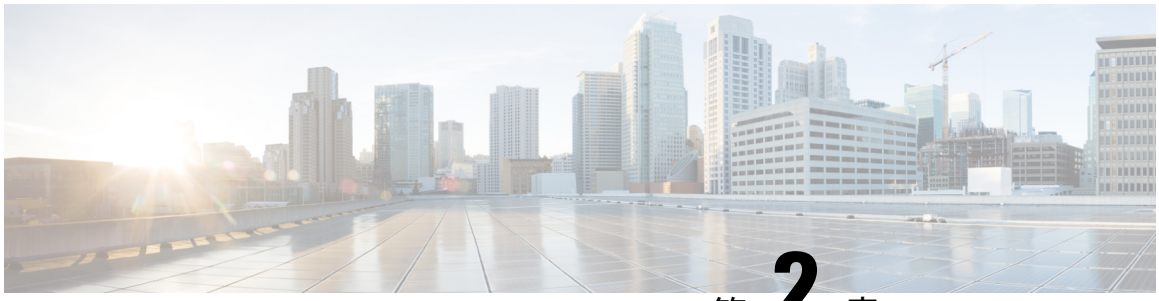
**注意** 現在、シスコには Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。



第 2 章

# VMware への Threat Defense Virtual の展開

この章では、 Threat Defense Virtual を VMware vSphere 環境（vSphere vCenter またはスタンドアロンの ESXi ホストのどちらか）に展開する手順について説明します。


- 概要 （3 ページ）
- Threat Defense Virtual の VMware 機能のサポート （4 ページ）
- システム要件 （5 ページ）
- 注意事項と制約事項 （10 ページ）
- インターフェイスの計画 （16 ページ）
- VMware の展開について （22 ページ）
- エンドツーエンドの手順 （22 ページ）
- vSphere vCenter への Threat Defense Virtual の展開 （24 ページ）
- クラスタ展開用の Day 0 構成ファイルの準備 （29 ページ）
- vSphere ESXi ホストへの Threat Defense Virtual の展開 （31 ページ）
- CLI を使用した Threat Defense Virtual のセットアップ （34 ページ）
- ESXi 構成でのパフォーマンスの向上 （36 ページ）
- NUMA のガイドライン （36 ページ）
- SR-IOV インターフェイスのプロビジョニング （37 ページ）


## 概要

シスコでは、VMware vSphere vCenter および ESXi ホスティング環境向けに 64 ビットの Threat Defense Virtual デバイスをパッケージ化しています。Threat Defense Virtual は、Cisco.com から入手可能なオープン仮想化フォーマット（OVF）パッケージで配布されます。OVF は、仮想マシン（VM）向けのソフトウェア アプリケーションをパッケージ化して配布するためのオープンソースの標準規格です。OVF パッケージでは 1 つのディレクトリに複数のファイルが含まれています。

Threat Defense Virtual は、VMware ESXi を実行できる任意の x86 デバイスに展開できます。Threat Defense Virtual を展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

# Threat Defense Virtual の VMware 機能のサポート

次の表に、Threat Defense Virtual の VMware 機能のサポートを示します。

**表 *1 : Threat Defense Virtual* の *VMware* 機能のサポート**

| 機能 | 説明 | サポート（あり/なし） | コメント |
|---|---|---|---|
| コールド クローン | クローニング中に VM の電源がオフになります。 | なし | – |
| VMotion | VM のライブ マイグレーションに使用されます。 | あり | 共有ストレージを使用します。「注意事項と制約事項」を参照してください。 |
| ホット追加 | 追加時に VM が動作しています。 | なし | – |
| ホット クローン | クローニング中に VM が動作しています。 | なし | – |
| ホット リムーブ | 取り外し中に VM が動作しています。 | なし | – |
| スナップショット | VM が数秒間フリーズします。 | なし | Management Center と管理対象デバイス間で同期されていない状況のリスク。 |
| 一時停止と再開 | VM が一時停止され、その後再開します。 | あり | – |
| vCloud Director | VMの自動配置が可能になります。 | なし | – |
| VMware FT | VM の HA に使用されます。 | なし | Threat Defense Virtual VM の障害に対してフェールオーバー機能を使用します。 |
| VM ハートビートの VMware HA | VM 障害に使用されます。 | なし | Threat Defense Virtual VM の障害に対してフェールオーバー機能を使用します。 |

| 機能 | 説明 | サポート（あり/なし） | コメント |
|---|---|---|---|
| VMware vSphere スタンドアロン Windows クライアント | VM を導入するために使用されます。 | あり | – |
| VMware vSphere Web Client | VM を導入するために使用されます。 | あり | – |

# システム要件

Threat Defense Virtual のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

VMware vCenter Server と ESXi のインスタンスを実行するシステムは、特定のハードウェアおよびオペレーティングシステム要件を満たす必要があります。サポートされるプラットフォームのリストについては、オンラインの『VMware Compatibility Guide』を参照してください。

表 *2 : Threat Defense Virtual* アプライアンスのリソース要件

| 設定 | 値 |
|---|---|
| パフォーマンス階層 | Threat Defense Virtual 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。<br>• FTDv5 4vCPU/8GB（100 Mbps）<br>• FTDv10 4vCPU/8GB（1 Gbps）<br>• FTDv20 4vCPU/8GB（3 Gbps）<br>• FTDv30 8vCPU/16GB（5 Gbps）<br>• FTDv50 12vCPU/24GB（10 Gbps）<br>• FTDv100 16vCPU/32GB（16 Gbps）<br>Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Licensing」の章を参照してください。<br>（注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。 |
| ストレージ | ディスク形式の選択に基づきます。<br>• シンプロビジョニングのディスクサイズは 48.24 GB です。 |

| 設定 | 値 |
| --- | --- |
| vNIC | Threat Defense Virtual は次の仮想ネットワークアダプタをサポートしています。<br>• **VMXNET3**：VMware 上の Threat Defense Virtual では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。vmxnet3 ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つのイーサネット アダプタは、管理インターフェイスとして設定する必要があります。1 つはデバイス管理/登録用で、もう 1 つは診断用です。<br>• **IXGBE**：ixgbe ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つの PCI デバイスは、管理インターフェイスとして設定する必要があります。1 つはデバイス管理/登録用、もう 1 つは診断用です。ixgbe ドライバは、Threat Defense Virtual のフェールオーバー（HA）の展開をサポートしていません。<br>• **E1000**：e1000 インターフェイスを使用する場合、e1000 ドライバ用の Threat Defense Virtual 管理インターフェイス（br1）は、2 つの MAC アドレス（1 つは管理用で、もう 1 つは診断用）とのブリッジインターフェイスです。<br>• **IXGBE-VF**：ixgbe-vf（10 ギガビット/秒）ドライバは、SR-IOV をサポートするカーネルでのみアクティブ化できる仮想関数デバイスをサポートしています。SR-IOV には適切なプラットフォームおよび OS のサポートが必要です。詳細については、「SR-IOV のサポート」の項を参照してください。 |

### 仮想化テクノロジーのサポート

- 仮想化テクノロジー（VT）は、動作中の仮想マシンのパフォーマンスを向上させる新しいプロセッサの機能拡張セットです。システムには、ハードウェア仮想化用のインテル VT または AMD-V の拡張機能をサポートする CPU が必要です。Intel と AMD はどちらも、CPU を識別して機能を確認するために役立つオンラインプロセッサ識別ユーティリティを提供しています。
- VT をサポートする CPU を搭載する多くのサーバーでは、VT がデフォルトで無効になっている可能性があります。その場合は、VT を手動で有効にする必要があります。システムで VT のサポートを有効にする手順については、製造元のマニュアルを参照してください。

（注） CPU が VT をサポートしているにもかかわらず BIOS にこのオプションが表示されない場合は、ベンダーに連絡して、VT のサポートを有効にすることができるバージョンの BIOS を要求してください。

### ハイパースレッディングの無効化

Threat Defense Virtual を実行するシステムでは、ハイパースレッディングを無効にすることを推奨します。「ハイパースレッディングは非推奨 （12 ページ）」を参照してください。次のプロセッサはハイパースレッディングをサポートし、コアごとに 2 つのスレッドがあります。

- Intel Xeon 5500 プロセッサのマイクロアーキテクチャに基づくプロセッサ。
- Intel Pentium 4（HT対応）
- Intel Pentium EE 840（HT対応）

ハイパースレッディングを無効にするには、初めにシステムの BIOS 設定でこれを無効にしてから、vSphere クライアントでオフにします（vSphere ではデフォルトでハイパースレッディングが有効になっています）。CPU がハイパースレッディングをサポートしているかどうかを確認するには、システムのマニュアルを参照してください。

### SR-IOV のサポート

SR-IOV 仮想機能には特定のシステムリソースが必要です。SR-IOV 対応 PCIe アダプタに加えて、SR-IOV をサポートするサーバーが必要です。以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。次の NIC がサポートされています。
  - Intel Ethernet Server Adapter X520 - DA2
  - Intel Ethernet Server Adapter X540
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。
- x86_64 マルチコア CPU：Intel Sandy Bridge 以降（推奨）。

（注） シスコでは、Threat Defense Virtual を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア

- CPU ソケットあたり 8 個以上の物理コア。

（注） Threat Defense Virtual は、複数の Non-uniform Memory Access（NUMA）ノードおよび物理コア用の複数の CPU ソケットをサポートしません。

- 割り当てられたすべての物理コアを 1 つのソケットに割り当てるようにしてください。

（注） CPU ピンニングは、フルスループットを実現するために推奨されています。

メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。オンラインの『VMware Compatibility Guide』で、SR-IOV のサポートを含む推奨システムを検索できます。

### SSSE3 のサポート

- Threat Defense Virtual には、Intel によって作成された単一命令複数データ（SIMD）命令セットである Supplemental Streaming SIMD Extensions 3（SSSE3 または SSE3S）のサポートが必要です。
- システムは SSSE3 をサポートする CPU（インテル Core 2 Duo、インテル Core i7/i5/i3、インテル Atom、AMD Bulldozer、AMD Bobcat およびそれ以降のプロセッサなど）を搭載している必要があります。
- SSSE3 命令セットと SSSE3 をサポートする CPU の詳細については、このリファレンスページを参照してください。

### CPU のサポートの確認

Linux コマンドラインを使用して、CPU ハードウェアに関する情報を取得できます。たとえば、**/proc/cpuinfo** ファイルには個々の CPU コアに関する詳細情報が含まれています。**less** または **cat** により、その内容を出力できます。

フラグ セクションで次の値を確認できます。

- vmx：インテル VT 拡張機能
- svm：AMD-V拡張機能
- ssse3：SSSE3 拡張機能

**grep** を使用すると、次のコマンドを実行して、ファイルにこれらの値が存在するかどうかを確認できます。

```
egrep "vmx|svm|ssse3" /proc/cpuinfo
```

システムが VT または SSSE3 をサポートしている場合は、フラグのリストに vmx、svm、または ssse3 が表示されます。次の例は、2 つの CPU を搭載しているシステムからの出力を示しています。

```
flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm

flags    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

# 注意事項と制約事項

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

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

表 *3 : Threat Defense Virtual* 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/32 GB | 16 Gbps | 10,000 |

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Licensing」の章を参照してください。

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「ESXi 構成でのパフォーマンスの向上 （36 ページ）」、「NUMA のガイドライン （36 ページ）」、および「SR-IOV インターフェイスのプロビジョニング （37 ページ）」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。RSS はバージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### クラスタリング

バージョン 7.2 以降、クラスタリングは VMware で展開された Threat Defense Virtual インスタンスでサポートされます。詳細については、『プライベートクラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。

### 管理モード

- Secure Firewall Threat Defense（旧称 Firepower Threat Defense） デバイスの管理には次の 2 つのオプションがあります。
  - Device Manager オンボード統合マネージャ。

（注） VMware 上の Threat Defense Virtual は、シスコ ソフトウェア バージョン 6.2.2 以降で Device Manager をサポートしています。バージョン 6.2.2 よりも前のソフトウェアを実行している VMware 上の Threat Defense Virtual は、Management Center を使用してのみ管理できます。「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

  - Management Center。

- Device Manager を使用するには、新しいイメージ（バージョン 6.2.2 以降）をインストールする必要があります。既存の Threat Defense Virtual マシンを古いバージョン（バージョン 6.2.2 よりも前）からアップグレードして Device Manager に切り替えることはできません。
- Device Manager （ローカルマネージャ）はデフォルトで有効になっています。

（注） [ローカルマネージャを有効にする（Enable Local Manager）] の [はい（Yes）] を選択すると、ファイアウォールモードが「ルーテッド」に変更されます。Device Manager を使用する場合は、これが唯一のサポートモードです。

### OVF ファイルのガイドライン

Threat Defense Virtual アプライアンスをインストールする場合、以下のインストールオプションがあります。

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

ここで、X.X.X-xxx は、使用するファイルのバージョンとビルド番号を表します。

- VI OVF テンプレートを使用して展開する場合、インストールプロセスで、Threat Defense Virtual アプライアンスの初期設定全体を実行できます。次を指定することができます。
  - 管理者アカウントの新しいパスワード。
  - アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。
  - Device Manager を使用するローカル管理（デフォルト）、または Management Center を使用するリモート管理のいずれかの管理。
  - ファイアウォールモード：[ローカルマネージャを有効にする（Enable Local Manager）] で [はい（Yes）] を選択すると、ファイアウォールモードがルーテッドに変更されます。Device Manager を使用する場合は、これが唯一のサポートモードです。

（注） VMware vCenter を使用してこの仮想アプライアンスを管理する必要があります。

- ESXi OVF テンプレートを使用して導入する場合、インストール後にシステムの必須設定を行う必要があります。この Threat Defense Virtual は ESXi でスタンドアロンのアプライアンスとして管理します。詳細については、「vSphere ESXi ホストへの Threat Defense Virtual の展開 （31 ページ）」を参照してください。

### vSphere 7.0.2 で仮想マシン（VM）の設定を保存できない

vSphere 7.0.2 を使用している場合、VM の設定を保存できない場合があります。

（注） この問題は、VMware ナレッジベースの記事 https://kb.vmware.com/s/article/83898 の手順に従って解決できます。

### vMotion のサポート

vMotion を使用する場合、共有ストレージのみを使用することをお勧めします。の導入時に、ホストクラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。ただし、vMotion を使用して Secure Firewall Management Center Virtual（旧称 Firepower Management Center Virtual） を別のホストに移行する場合、ローカルストレージを使用するとエラーが発生します。

### ハイパースレッディングは非推奨

ハイパースレッディング テクノロジーにより、単一の物理プロセッサコアを 2 つの論理プロセッサのように動作させることができます。Threat Defense Virtual を実行するシステムでは、

ハイパースレッディングを無効にすることを推奨します。Snort プロセスにより、CPU コアの処理リソースがすでに最大化されています。各 CPU に 2 つの CPU 使用スレッドをプッシュしても、パフォーマンスの向上は見込まれません。実際には、ハイパースレッディングプロセスに必要となるオーバーヘッドのためにパフォーマンスが低下することがあります。

### INIT Respawning エラーメッセージの症状

ESXi 6 および ESXi 6.5 で実行されている Threat Defense Virtual コンソールに次のエラーメッセージが表示される場合があります。

```
"INIT: Id "ftdv" respawning too fast: disabled for 5 minutes"
```

**回避策**：デバイスの電源がオフになっているときに、vSphere で仮想マシンの設定を編集してシリアルポートを追加します。

1. 仮想マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。
2. [仮想ハードウェア（Virtual Hardware）] タブで、[新規デバイス（New devide）] ドロップダウンメニューから [シリアルポート（Serial port）] を選択し、[追加（Add）] をクリックします。

   シリアルポートがバーチャルデバイスリストの一番下に表示されます。
3. [仮想ハードウェア（Virtual Hardware）] タブで、[シリアルポート（Serial Port）] を展開し、接続タイプとして [物理シリアルポートを使用（Use physical serial port）] を選択します。
4. [パワーオン時に接続（Connect at power on）] チェックボックスをオフにします。

   [OK] をクリックして設定を保存します。

### ファイアウォール保護からの仮想マシンの除外

vCenter Server が VMware NSX Manager と統合されている vSphere 環境では、分散ファイアウォール（DFW）が、NSX 用に準備されたすべての ESXi ホストクラスタで、VIB パッケージとしてカーネルで実行されます。ホストの準備により、ESXi ホストクラスタで DFW が自動的にアクティブ化されます。

Threat Defense Virtual は無差別モードを使用して動作します。無差別モードを必要とする仮想マシンのパフォーマンスは、これらの仮想マシンが分散ファイアウォールで保護されている場合、悪影響を受ける可能性があります。VMware では、無差別モードを必要とする仮想マシンは分散ファイアウォール保護から除外することを推奨しています。

1. [除外リスト（Exclusion List）] の設定に移動します。
   - NSX 6.4.1 以降で、**[ネットワークとセキュリティ（Networking & Security）] > [セキュリティ（Security）] > [ ファイアウォール（Firewall）] > [除外リスト（Exclusion List）]** に移動します。
   - NSX 6.4.0 で、**[ネットワークとセキュリティ（Networking & Security）] > [セキュリティ（Security）] > [ ファイアウォール（Firewall）] > [除外リスト（Exclusion List）]** に移動します。

2. [追加（Add）] をクリックします。
3. 除外する VM を [選択されたオブジェクト（Selected Objects）] に移動します。
4. [OK] をクリックします。

仮想マシンに複数の vNIC がある場合、それらはすべて保護から除外されます。除外リストに追加されている仮想マシンに vNIC を追加すると、新しく追加された vNIC にファイアウォールが自動的に展開されます。新しい vNIC をファイアウォール保護から除外するには、仮想マシンを除外リストから削除してから、除外リストに再度追加する必要があります。別の回避策として、仮想マシンの電源を再投入（電源をオフにしてからオン）する方法がありますが、最初のオプションの方が中断が少なくて済みます。

### vSphere 標準スイッチのセキュリティポリシー設定の変更

vSphere 標準スイッチの場合、レイヤ 2 セキュリティポリシーの 3 つの要素は、無差別モード、MAC アドレスの変更、および不正送信です。Threat Defense Virtual は無差別モードで動作し、Threat Defense Virtual の高可用性が正しく機能するかは、アクティブとスタンバイ間の MAC アドレスの切り替えにかかっています。

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。以下の必須の設定を参照してください。

表 *4 : vSphere* 標準スイッチのセキュリティ ポリシー オプション

| オプション | 必須の設定 | アクション |
|---|---|---|
| 無差別モード（Promiscuous Mode） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを編集し、[無差別モード（Promiscuous mode）] オプションを [承認（Accept）] に設定する必要があります。<br>ファイアウォール、ポートスキャナ、侵入検知システムなどは無差別モードで実行する必要があります。 |
| MAC アドレスの変更（MAC Address Changes） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[MAC アドレスの変更（MAC address changes）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。 |

| オプション | 必須の設定 | アクション |
|---|---|---|
| 不正送信（Forged Transmits） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[不正転送（Forged transmits）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。 |

（注） NSX-T を使用する VMware は認定されていないため、vSphere 標準スイッチのセキュリティポリシー設定の NSX-T 構成に関する推奨事項はありません。

**Snort**

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

# vSphere 標準スイッチのセキュリティポリシー設定の変更

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。

**ステップ 1** vSphere Web Client で、ホストに移動します。

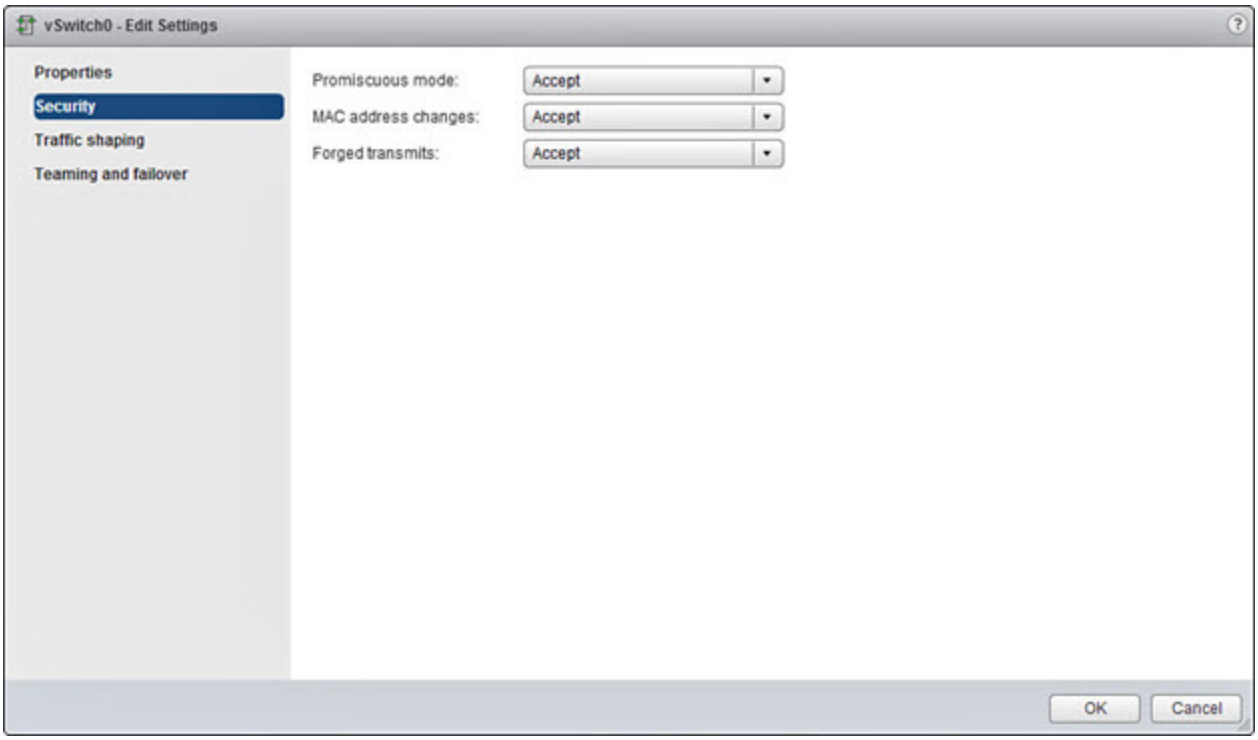
**ステップ 2** [管理（Manage）] タブで、[ネットワーク（Networking）] をクリックし、[仮想スイッチ（Virtual switches）] を選択します。

**ステップ 3** リストから標準スイッチを選択し、[設定の編集（Edit settings）] をクリックします。

**ステップ 4** [セキュリティ（Security）] を選択し、現在の設定を表示します。

**ステップ 5** 標準スイッチに接続された仮想マシンのゲストオペレーティングシステムで無差別モードの有効化、MAC アドレスの変更、および不正送信の [承認（Accept）] を選択します。

図 *1 : vSwitch* の編集設定




**ステップ 6** [OK] をクリックします。

### 次のタスク

- これらの設定が、Threat Defense Virtual デバイスの管理インターフェイスおよびフェールオーバー（HA）インターフェイスに設定されているすべてのネットワーク上で同じであることを確認します。

# インターフェイスの計画

展開の前に、Threat Defense Virtual の vNIC とインターフェイスのマッピングを計画することで、リブートと設定の問題を回避できます。Threat Defense Virtual は 10 個のインターフェイスで展開され、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。

Threat Defense Virtual は、vmxnet3（デフォルト）、ixgbe、および e1000 の仮想ネットワークアダプタをサポートしています。また、適切に設定されたシステムでは、Threat Defense Virtual は SR-IOV 用の ixgbe-vf ドライバもサポートしています。詳細については、「システム要件（5 ページ）」を参照してください。

重要 Threat Defense Virtual VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

# インターフェイスに関するガイドラインと制限事項

ここでは、VMware 上の Threat Defense Virtual で使用されるサポート対象の仮想ネットワークアダプタに関するガイドラインと制約事項について説明します。展開を計画する際は、これらのガイドラインに留意しておくことが重要です。

## 一般的なガイドライン

- 前述のように、Threat Defense Virtual は 10 個のインターフェイスで展開され、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。**少なくとも 4 つのインターフェイス**にネットワークを割り当てる必要があります。
- Threat Defense Virtual インターフェイスに HOLDING ポートグループを使用しないことをお勧めします。vSphere からの HOLDING ポートグループは、インターフェイス接続の一貫性が失われる原因になります。保留ポートは、VLAN ID に割り当てられる汎用ポートグループです。これにより、セカンダリ Threat Defense Virtual デバイスとの HA 形成中に問題が発生する可能性があります。
- 10 個の Threat Defense Virtual インターフェイスをすべて使用する必要はありません。使用しないインターフェイスの場合は、Threat Defense Virtual の設定内でそのインターフェイスを無効のままにしておいて構いません。
- 展開後に仮想マシンに仮想インターフェイスを追加することはできないので注意してください。一部のインターフェイスを削除してから、さらにインターフェイスが必要になった場合は、仮想マシンを削除してからやり直す必要があります。
- 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 Management Center に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center にアクセスするための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、『Cisco Secure Firewall Threat Defense コマンドリファレンス』の **configure network management-data-interface** コマンドを参照してください。
- Threat Defense Virtual の内部インターフェイスまたはフェールオーバーの高可用性リンクに使用される ESX ポートグループ用に 2 つの仮想 NIC をもつフェールオーバーの順序は、1 つはアクティブアップリンク、もう 1 つはスタンバイアップリンクとなるよう構成されていなければなりません。この設定は、2 つの VM が相互に ping を実行したり、Threat Defense Virtual の高可用性リンクを稼働させたりするために必要です。

### デフォルトの VMXNET3 インターフェイス

**重要** Threat Defense Virtual VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

- vmxnet3 ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つのイーサネットアダプタは、管理インターフェイスとして設定する必要があります。1 つはデバイス管理/登録用で、もう 1 つは診断用です。
- vmxnet3 では、4 つを超える vmxnet3 ネットワークインターフェイスを使用する場合、VMware vCenter によって管理されるホストを使用することを推奨します。スタンドアロンの ESXi に展開する場合、連続する PCI バス アドレスを持つ仮想マシンに対してさらに多くのネットワークインターフェイスは追加されません。ホストを VMware vCenter で管理する場合は、設定 CD-ROM の XML から正しい順序を取得できます。ホストでスタンドアロンの ESXi を実行している場合、ネットワークインターフェイスの順序を判断する唯一の方法は、 Threat Defense Virtual に表示される MAC アドレスと、VMware 構成ツールから表示される MAC アドレスとを手動で比較することです。

次の表に、vmxnet3 および ixgbe インターフェイスの Threat Defense Virtual 用のネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を示します。

**表 *5*: 送信元から宛先ネットワークへのマッピング：*vmxnet3* と *ixgbe***

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Management0/0 | 管理 |
| Network adapter 2 | Diagnostic 0-0 | Diagnostic0/0 | 診断 |
| ネットワークアダプタ 3 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部データ |
| ネットワークアダプタ 4 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部データ |
| ネットワークアダプタ 5 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet 0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ネットワークアダプタ 7 | GigabitEthernet 0-4 | GigabitEthernet 0/4 | データトラフィック（オプション） |

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| ネットワークアダプタ 8 | GigabitEthernet 0-5 | GigabitEthernet 0/5 | データトラフィック（オプション） |
| ネットワークアダプタ 9 | GigabitEthernet 0-6 | GigabitEthernet 0/6 | データトラフィック（オプション） |
| ネットワークアダプタ 10 | GigabitEthernet 0-7 | GigabitEthernet 0/7 | データトラフィック（オプション） |

### IXGBE インターフェイス

- ixgbe ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つの PCI デバイスは、管理インターフェイスとして設定する必要があります。1 つはデバイス管理/登録用で、もう 1 つは診断用です。
- ixgbe の場合は、ESXi プラットフォームで ixgbe PCI デバイスをサポートするために ixgbe NIC が必要です。また、ESXi プラットフォームには、ixgbe PCI デバイスをサポートするために必要な固有の BIOS 要件と設定要件があります。詳細については、Intel の技術概要を参照してください。
- サポートされる唯一の ixgbe トラフィックインターフェイスのタイプは、ルーテッドと ERSPAN パッシブです。これは、MAC アドレスフィルタリングに関する VMware の制限によるものです。
- ixgbe ドライバは、Threat Defense Virtual のフェールオーバー（HA）の展開をサポートしていません。

### e1000 インターフェイス

**重要** Threat Defense Virtual VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

- e1000 ドライバ用の管理インターフェイス（br1）は、2 つの MAC アドレス（1 つは管理用で、もう 1 つは診断用）とのブリッジインターフェイスです。
- e1000 インターフェイスを使用していて、Threat Defense Virtual を 6.4 にアップグレードする場合は、ネットワークスループットを向上させるために、e1000 インターフェイスを vmxnet3 または ixgbe インターフェイスのいずれかに置き換えてください。

次の表に、デフォルトの e1000 インターフェイスにおける Threat Defense Virtual 用のネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を示します。

表 *6*: 送信元から宛先ネットワークへのマッピング：*e1000* インターフェイス

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Diagnostic0/0 | 管理と診断 |
| Network adapter 2 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部データ |
| ネットワークアダプタ 3 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部データ |
| ネットワークアダプタ 4 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（必須） |
| ネットワークアダプタ 5 | GigabitEthernet0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet0-4 | GigabitEthernet 0/4 | データトラフィック（オプション） |
| ネットワークアダプタ 7 | GigabitEthernet0-5 | GigabitEthernet 0/5 | データトラフィック（オプション） |
| ネットワークアダプタ 8 | GigabitEthernet0-6 | GigabitEthernet 0/6 | データトラフィック（オプション） |
| ネットワークアダプタ 9 | GigabitEthernet0-7 | GigabitEthernet 0/7 | データトラフィック（オプション） |
| ネットワークアダプタ 10 | GigabitEthernet0-8 | GigabitEthernet 0/8 | データトラフィック（オプション） |

# VMXNET3 インターフェイスの設定

**重要** 6.4 のリリース以降、VMware 上の Threat Defense Virtual と Management Center Virtual では、仮想デバイスを作成する際のデフォルトインターフェイスが vmxnet3 になりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

e1000 インターフェイスを vmxnet3 に変更するには、「すべての」インターフェイスを削除し、vmxnet3 ドライバを使用してそれらを再インストールする必要があります。

展開内でインターフェイスを混在させることはできますが（Management Center で e1000 インターフェイス、およびその管理対象仮想デバイスで vmxnet3 インターフェイスなど）、同じ仮

想アプライアンス上でインターフェイスを混在させることはできません。仮想アプライアンス上のすべてのセンサーインターフェイスと管理インターフェイスは同じタイプである必要があります。

**ステップ 1** Threat Defense Virtual または Management Center Virtual マシンの電源をオフにします。

インターフェイスを変更するには、アプライアンスの電源をオフにする必要があります。

**ステップ 2** インベントリ内の Threat Defense Virtual または Management Center Virtual マシンを右クリックして、[設定の編集（Edit Settings）] をクリックします。

**ステップ 3** 該当するネットワークアダプタを選択し、[削除（Remove）] を選択します。

**ステップ 4** [追加（Add）] をクリックして、[ハードウェアの追加ウィザード（Add Hardware Wizard）] を開きます。

**ステップ 5** [イーサネットアダプタ（Ethernet Adapter）] を選択し、[次へ（Next）] をクリックします。

**ステップ 6** vmxnet3 アダプタを選択し、ネットワークラベルを選択します。

**ステップ 7** Threat Defense Virtual のすべてのインターフェイスについて手順を繰り返します。

### 次のタスク

- VMware コンソールから Threat Defense Virtual または Management Center Virtual の電源をオンにします。

# インターフェイスの追加

Threat Defense Virtual デバイスを展開する場合、合計 10 のインターフェイス（管理 X 1、診断 X 1、データ X 8 のインターフェイス）を設けることができます。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。

**注意** 仮想マシンにさらに仮想インターフェイスを追加して、Threat Defense Virtual にそれらを自動的に認識させることはできません。仮想マシンにインターフェイスを追加する場合は、完全に Threat Defense Virtual 設定を消去する必要があります。設定でそのまま残しておける唯一の部分は、管理アドレスとゲートウェイ設定です。

Threat Defense Virtual デバイス向けに追加の物理インターフェイスが必要な場合は、基本的にもう一度やり直す必要があります。新しい仮想マシンを展開するか、『Cisco Secure Firewall Device Manager Configuration Guide』の「インターフェイスの変更のスキャンとインターフェイスの移行」の手順を使用できます。

# VMware の展開について

Threat Defense Virtual は、スタンドアロンの ESXi サーバーに展開できます。vCenter vSphere を使用している場合は、vSphere Client または vSphere Web Client を使用して展開できます。Threat Defense Virtual を正常に展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

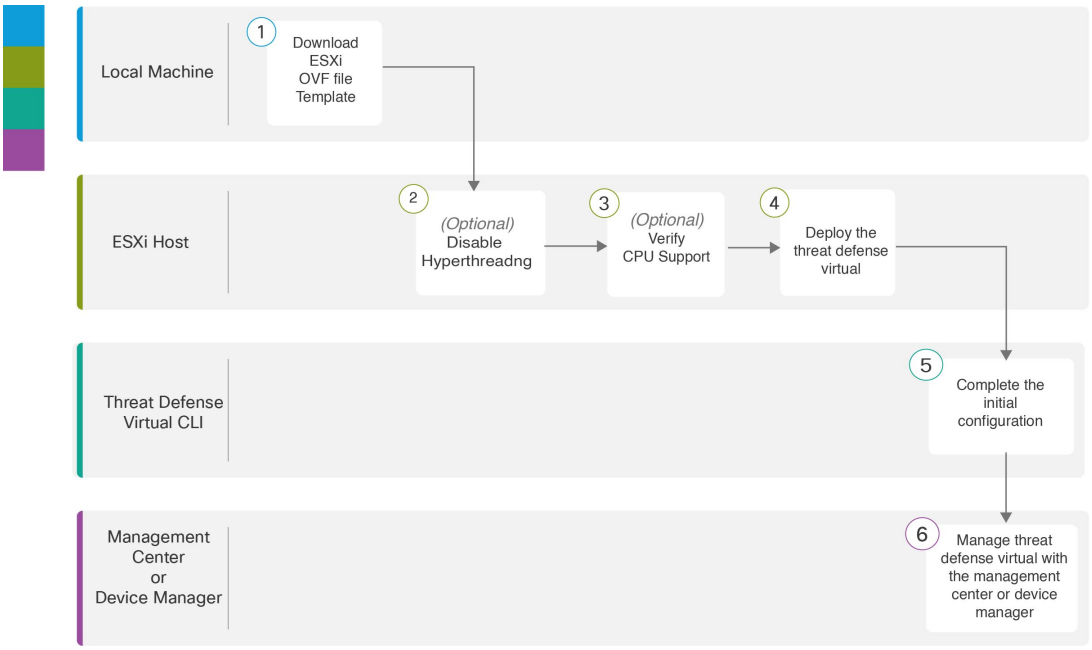
Threat Defense Virtual VMware 用の FTDv はオープン仮想化フォーマット（OVF）を使用して配布されます。OVF は、仮想マシンをパッケージ化して展開する標準的な方法です。VMware では、vSphere 仮想マシンをプロビジョニングするための方法がいくつか用意されています。お使いの環境に最適な方法は、インフラストラクチャの規模やタイプ、達成目標などの要因によって異なります。

VMware vSphere Web Client と vSphere Client は、vCenter Server、ESXi ホスト、および仮想マシンへのインターフェイスです。VSphere Web Client と vSphere Client を使用して、vCenter Server にリモート接続できます。VSphere Client では、任意の Windows システムから ESXi に直接接続することもできます。VSphere Web Client と vSphere Client は、vSphere 環境のすべての側面を管理するための主要なインターフェイスです。これらはコンソールによる仮想マシンへのアクセスも提供します。

vSphere Web Client では、すべての管理機能を使用できます。vSphere Client では、これらの機能の一部を使用できます。

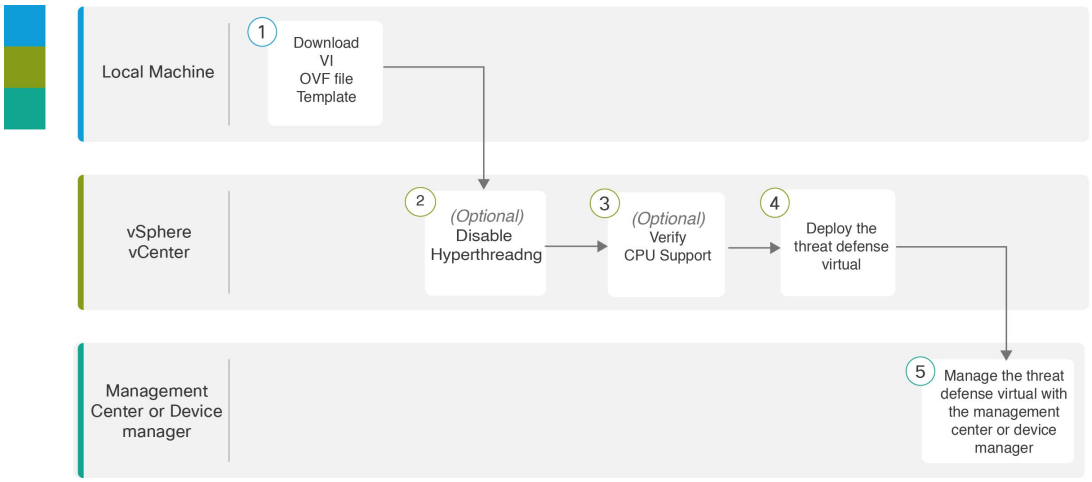
# エンドツーエンドの手順

次のフローチャートは、ESXi ホストに Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Local Machine | ESXi OVF テンプレートのダウンロード：Cisco.com から入手可能なオープン仮想フォーマット（OVF）パッケージをダウンロードします。 |
| 2 | ESXi ホスト（ESXi Host） | （任意）システム要件：Threat Defense Virtual を実行するシステムのハイパースレッディングを無効にします。 |
| 3 | ESXi ホスト（ESXi Host） | システム要件：Linux コマンドラインを使用して、CPU ハードウェアに関する情報を取得できます。 |
| 4 | ESXi ホスト（ESXi Host） | vSphere ESXi ホストへの Threat Defense Virtual の展開：Threat Defense Virtual アプライアンスを単一の ESXi ホストに展開します。 |
| 5 | Threat Defense Virtual CLI | CLI を使用した Threat Defense Virtual のセットアップ：ESXi OVF テンプレートを使用して展開した場合は、CLI を使用して Threat Defense Virtual を設定する必要があります。 |
| 6 | Management Centerまたは Device Manager | Threat Defense Virtual を管理します。<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 （455 ページ） |

次のフローチャートは、vSphere vCenter に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Local Machine | VI OVF テンプレートのダウンロード：Cisco.com から入手可能なオープン仮想フォーマット（OVF）パッケージをダウンロードします。 |
| 2 | vSphere vCenter | （任意）システム要件：Threat Defense Virtual を実行するシステムのハイパースレッディングを無効にします。 |
| 3 | vSphere vCenter | システム要件：Linux コマンドラインを使用して、CPU ハードウェアに関する情報を取得できます。 |
| 4 | vSphere vCenter | vSphere ESXi ホストへの Threat Defense Virtual の展開：Threat Defense Virtual アプライアンスを単一の ESXi ホストに展開します。 |
| 5 | Management CenterまたはDevice Manager | Threat Defense Virtual を管理します。<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 （455 ページ） |

# vSphere vCenter への Threat Defense Virtual の展開

この手順を使用して、Threat Defense Virtual アプライアンスを VMware vSphere vCenter に展開します。vSphere Web Client（または vSphere Client）を使用して、 Threat Defense Virtual マシンを展開し、設定できます。

### 始める前に

- Threat Defense Virtual を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。

**ステップ 1** vSphere Web Client（または vSphere Client）にログインします。

**ステップ 2** vSphere Web Client（または vSphere Client）を使用し、**[ファイル（File）]** > **[OVFテンプレートの展開（Deploy OVF Template）]** をクリックして、以前にダウンロードした OVF テンプレートファイルを展開します。

[OVFテンプレートの導入（Deploy OVF Template）] ウィザードが表示されます。

**ステップ 3** ファイルシステムで OVF テンプレートソースの場所を参照し、[次へ（Next）] をクリックします。

次の Threat Defense Virtual VI OVF テンプレートを選択します。

*Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*

ここで、*X.X.X-xxx* は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

**ステップ 4** [OVFテンプレートの詳細（OVF Template Details）] ページを確認し、OVF テンプレートの情報（製品名、バージョン、ベンダー、ダウンロードサイズ、ディスク上のサイズ、説明）を確認して、[次へ（Next）] をクリックします。

**ステップ 5** [エンドユーザーライセンス契約書（End User License Agreement）] ページが表示されます。OVF テンプレート（VI テンプレートのみ）でパッケージ化されたライセンス契約書を確認し、[承認（Accept）] をクリックしてライセンスの条件に同意し、[次へ（Next）] をクリックします。

**ステップ 6** [名前と場所（Name and Location）] ページで、この展開の名前を入力し、Threat Defense Virtual を展開するインベントリ内の場所（ホストまたはクラスタ）を選択して、[次へ（Next）] をクリックします。名前はインベントリフォルダ内で一意である必要があり、最大 80 文字を使用できます。

VSphere Web Client では、インベントリビューに管理対象オブジェクトの組織階層が表示されます。インベントリは、vCenter Server またはホストが管理対象オブジェクトを整理する目的で使用する階層構造です。この階層には、vCenter Server にあるすべての監視対象オブジェクトが含まれています。

**ステップ 7** Threat Defense Virtual を実行するリソース プールに移動して選択し、[次へ（Next）] をクリックします。

（注） このページは、クラスタにリソースプールが含まれている場合にのみ表示されます。

**ステップ 8** [導入設定（Deployment Configuration）] を選択します。[設定（Configuration）] ドロップダウンリストから、サポートされている 3 つの vCPU/メモリ値のいずれかを選択し、[次へ（Next）] をクリックします。

**重要** Threat Defense Virtual は、調整可能な vCPU およびメモリリソースを使用して展開されます。

**ステップ 9** 仮想マシンファイルを保存する [保存（Storage）] 場所を選択し、[次へ（Next）] をクリックします。

このページで、宛先クラスタまたはホストですでに設定されているデータストアから選択します。仮想マシン コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。

**ステップ 10** 仮想マシンの仮想ディスクを保存するための「ディスク形式」を選択し、[次へ（Next）] をクリックします。

[シックプロビジョン（Thick Provisioned）] を選択すると、すべてのストレージは、ただちに割り当てられます。[シンプロビジョン（Thin Provisioned）] を選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

**ステップ 11** [ネットワークマッピング（Network Mapping）] ページで、OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ（Next）] をクリックします。

Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Management Center または Device Manager から設定できます。

**重要** Threat Defense Virtual VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集（Edit Settings）] ダイアログボックスからネットワークを変更できます。展開後、Threat Defense Virtual インスタンスを右クリックして [設定の編集（Edit Settings）] を選択します。ただし、この画面には Threat Defense Virtual の ID は表示されません（ネットワークアダプタ ID のみ）。

以下に示す、Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を参照してください（これらは vmxnet3 デフォルトのインターフェイスです）。

**表 *7:* 送信元から宛先ネットワークへのマッピング：*vmxnet3***

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Management0/0 | 管理 |
| Network adapter 2 | Diagnostic 0-0 | Diagnostic0/0 | 診断 |
| ネットワークアダプタ 3 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部データ |
| ネットワークアダプタ 4 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部データ |
| ネットワークアダプタ 5 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet 0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ネットワークアダプタ 7 | GigabitEthernet 0-4 | GigabitEthernet 0/4 | データトラフィック（オプション） |

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| ネットワークアダプタ 8 | GigabitEthernet 0-5 | GigabitEthernet 0/5 | データトラフィック（オプション） |
| ネットワークアダプタ 9 | GigabitEthernet 0-6 | GigabitEthernet 0/6 | データトラフィック（オプション） |
| ネットワークアダプタ 10 | GigabitEthernet 0-7 | GigabitEthernet 0/7 | データトラフィック（オプション） |

Threat Defense Virtual を展開する際には、合計 10 個のインターフェイスを指定できます。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。すべての Threat Defense Virtual インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、Threat Defense Virtual 設定内でそのインターフェイスを無効のままにしておいて構いません。

**ステップ 12** [プロパティ（Properties）] ページで、OVF テンプレート（VI テンプレートのみ）でパッケージ化された、ユーザー設定可能なプロパティを設定します。

a) **パスワード**

Threat Defense Virtual 管理アクセス用のパスワードを設定します。

b) **ネットワーク**

完全修飾ドメイン名（FQDN）、DNS、検索ドメイン、ネットワークプロトコル（IPv4 または IPv6）などのネットワーク情報を設定します。

c) **管理**

管理モードを設定します。[ローカルマネージャを有効にする（Enable Local Manager）] のドロップダウン矢印をクリックし、Web ベースの Device Manager 統合設定ツールを使用する場合は [はい（Yes）] を選択します。Management Center を使用してこのデバイスを管理するには、[いいえ（No）] を選択します。管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

d) **ファイアウォールモード**

初期ファイアウォールモードを設定します。[ファイアウォールモード（Firewall Mode）] のドロップダウン矢印をクリックし、サポートされている 2 つのモードである [ルーテッド（Routed）] または [トランスペアレント（Transparent）] のどちらかを選択します。

[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、[ルーテッド（Routed）] ファイアウォール モードのみを選択できます。ローカルの Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。

e) **導入タイプ**

導入タイプを [スタンドアロン（Standalone）] または [クラスタ（Cluster）] に設定します。[クラスタ（Cluster）] を選択して、クラスタ制御リンクに必要なジャンボフレームの予約を有効にします。スタンドアロンまたは高可用性の展開には、[スタンドアロン（Standalone）] を選択します。スタンド

アロンデバイスとして展開した場合でもクラスタで使用できますが、展開後にクラスタリング用のジャンボフレームを有効にすると、再起動が必要になることに注意してください。

f) **登録**

[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、管理を行う Firepower Management Center にこのデバイスを登録するのに必要なクレデンシャルを指定する必要があります。次の情報を入力します。

- [管理を行うDefense Center（Managing Defense Center）]：Management Center のホスト名または IP アドレスを入力します。
- [登録キー（Registration Key）]：登録キーは、ユーザーが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。デバイスを Management Center に追加するときに、この登録キーを思い出す必要があります。
- [NAT ID]：Threat Defense Virtual と Management Center がネットワークアドレス変換（NAT）デバイスによって分離されていて、Management Center が NAT デバイスの背後にある場合は、一意の NAT ID を入力します。これは、ユーザーが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。

g) [次へ（Next）] をクリックします。

**ステップ 13** [準備完了（Ready To Complete）] セクションで、表示された情報を確認します。これらの設定を使用して展開を開始するには、[終了（Finish）] をクリックします。変更を加えるには、[戻る（Back）] をクリックして前の各画面に戻ります。

オプションで、[展開後に電源をオン（Power on after deployment）] オプションにチェックマークを付けて、Threat Defense Virtual の電源をオンにし、[終了（Finish）] をクリックします。

ウィザードが完了すると、vSphere Web Client によって仮想マシンが処理されます。[グローバル情報（Global Information）] 領域の [最近使用したタスク（Recent Tasks）] ペインで [OVF展開の初期設定（Initialize OVF deployment）] ステータスを確認できます。

この手順が終了すると、[OVFテンプレートの展開（Deploy OVF Template）] 完了ステータスが表示されます。

Threat Defense Virtual インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。新しい VM の起動には、最大 30 分かかることがあります。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

### 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# クラスタ展開用の Day 0 構成ファイルの準備

Threat Defense Virtual を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキスト ファイルです。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。

**重要** day0.iso ファイルは、最初のブート時に使用できる必要があります。

導入時に Day 0 の構成ファイルを使用すると、導入プロセスで Threat Defense Virtual アプライアンスの初期設定をすべて実行できます。次を指定することができます。

- エンド ユーザー ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 管理モード。Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）を参照してください。

  Management Center フィールド（[FmcIp]、[FmcRegKey]、[FmcNatId]）に情報を入力します。使用していない管理モードでは、フィールドを空のままにします。
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。
- Threat Defense Virtual をクラスタとして展開するかスタンドアロンで展開するかを指定できる展開タイプ。

**（注）** この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

## 手順の概要

1. Threat Defense Virtual を展開する Linux ホストにログインします。

2. Threat Defense Virtual 用に「day0-config」というテキストファイルを作成します。このテキストファイルには、クラスタ展開の設定、ネットワーク設定、および Management Center の管理に関する情報を追加する必要があります。
3. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。
4. ターゲットの ESXi ホストにログインします。
5. クラスタモードで Threat Defense Virtual を展開する仮想マシンインスタンスを開きます。
6. 仮想マシンの電源をオンにする前に、作成した day0 の ISO イメージファイルを参照して、[ハードウェア構成（Hardware Configuration）] の設定の下にある [CD/DVD ドライブ1（CD/DVD drive 1）] フィールドにアタッチします。
7. 仮想マシンの電源をオンにして、クラスタモードで Threat Defense Virtual を展開します。

## 手順の詳細

**ステップ 1** Threat Defense Virtual を展開する Linux ホストにログインします。

**ステップ 2** Threat Defense Virtual 用に「day0-config」というテキストファイルを作成します。このテキストファイルには、クラスタ展開の設定、ネットワーク設定、および Management Center の管理に関する情報を追加する必要があります。

**例**：

```
#Firepower Threat Defense
{

     "DeploymentType": "Cluster"

}
```

Management Center フィールド（[FmcIp]、[FmcRegKey]、[FmcNatId]）に情報を入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

**ステップ 3** テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

**例**：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

**ステップ 4** ターゲットの ESXi ホストにログインします。

**ステップ 5** クラスタモードで Threat Defense Virtual を展開する仮想マシンインスタンスを開きます。

**ステップ 6** 仮想マシンの電源をオンにする前に、作成した day0 の ISO イメージファイルを参照して、[ハードウェア構成（Hardware Configuration）] の設定の下にある [CD/DVD ドライブ1（CD/DVD drive 1）] フィールドにアタッチします。

**ステップ 7** 仮想マシンの電源をオンにして、クラスタモードで Threat Defense Virtual を展開します。

# vSphere ESXi ホストへの Threat Defense Virtual の展開

以下の手順を使用して、Threat Defense Virtual アプライアンスを単一の ESXi ホストに展開します。VMware Host Client（または vSphere Client）を使用して、単一の ESXi ホストを管理でき、Threat Defense Virtual マシンの展開や設定といった仮想化の基本的な操作などの管理タスクを実行できます。

（注） VMware Host Client は vSphere Web Client とユーザーインターフェイスが似ていますが、まったく異なるものであることに注意してください。vSphere Web Client は、vCenter Server に接続して複数の ESXi ホストを管理する場合に使用します。一方、VMware Host Client は単一の ESXi ホストを管理する場合に使用します。

vCenter 環境に Threat Defense Virtual アプライアンスを展開する方法については、「vSphere vCenter への Threat Defense Virtual の展開 （24 ページ）」参照してください。

### 始める前に

- Threat Defense Virtual を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。

**ステップ 1** Cisco.com から VMware ESXi 用の Threat Defense Virtual インストールパッケージをダウンロードして、ローカル管理コンピュータに保存します。

https://www.cisco.com/go/ftd-software

Cisco.com へのログインとシスコサービス契約が必要です。

**ステップ 2** tar ファイルを作業ディレクトリに解凍します。ディレクトリからファイルを削除しないでください。次のファイルが含まれています。

- Cisco_Firepower_Threat_Defense_Virtual-VI-*X.X.X-xx*.ovf：vCenter 展開用
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.ovf：ESXi 展開用
- Cisco_Firepower_Threat_Defense_Virtual-*X.X.X-xx*.vmdk：VMware 仮想ディスク ファイル
- Cisco_Firepower_Threat_Defense_Virtual-VI-*X.X.X-xx*.mf：vCenter 展開用マニフェストファイル
- Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.mf：ESXi 展開用マニフェストファイル

ここで、*X.X.X-xx* は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

**ステップ 3** ブラウザで、*http://host-name/ui* または *http://host-IP-address/ui* の形式で、対象の ESXi ホスト名または IP アドレスを入力します。

ログイン画面が表示されます。

**ステップ 4** 管理者のユーザー名とパスワードを入力します。

**ステップ 5** [ログイン（Login）] をクリックして続行します。

これで、ターゲットの ESXi ホストにログインしました。

**ステップ 6** VMware Host Client のインベントリで、[ホスト（Host）] を右クリックし、[VMの作成/登録（Create/Register VM）] を選択します。

[新規仮想マシンウィザード（New Virtual Machine Wizard）] が開きます。

**ステップ 7** [作成タイプの選択（Select creation type）] ページで、[OVFまたはOVAファイルから仮想マシンを導入（Deploy a virtual machine from an OVF or OVA file）] を選択し、[次へ（Next）] をクリックします。

**ステップ 8** ウィザードの [OVFおよびVMDKファイルの選択（Select OVF and VMDK files）] ページで次の操作を行います。

a) Threat Defense Virtual マシンの名前を入力します。

仮想マシン名には 80 文字まで含めることができます。マシン名は各 ESXi インスタンスの中で一意にする必要があります。

b) 青いペインをクリックし、 Threat Defense Virtual tar ファイルを解凍したディレクトリを参照して、ESXi OVF テンプレートと付随する VMDK ファイルを選択します。

Cisco_Firepower_Threat_Defense_Virtual-ESXi-*X.X.X-xx*.ovf

Cisco_Firepower_Threat_Defense_Virtual-*X.X.X-xx*.vmdk

ここで、*X.X.X-xx* は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

**注目** 必ず ESXi OVF を選択してください。

**ステップ 9** [次へ（Next）] をクリックします。

使用しているローカルシステムストレージが開きます。

**ステップ 10** ウィザードの [ストレージの選択（Select storage）] ページで、アクセス可能なデータストアのリストからデータストアを選択します。

仮想マシンの設定ファイルとすべての仮想ディスクが、このデータストアに保存されます。データストアはそれぞれ、サイズ、速度、可用性などのプロパティが異なる場合があります。

**ステップ 11** [次へ（Next）] をクリックします。

**ステップ 12** Threat Defense Virtual の ESXi OVF と一緒にパッケージ化されている [展開オプション（Deployment options）] を設定します。

a) [ネットワークマッピング（Network Mapping）] : OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ（Next）] をクリックします。

Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Management Center または Device Manager から設定できます。

**重要** Threat Defense Virtual VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを**強く推奨します**。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集（Edit Settings）] ダイアログボックスからネットワークを変更できます。展開後、Threat Defense Virtual インスタンスを右クリックして [設定の編集（Edit Settings）] を選択します。ただし、この画面には Threat Defense Virtual の ID は表示されません（ネットワークアダプタ ID のみ）。

以下に示す、Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を参照してください（これらは vmxnet3 デフォルトのインターフェイスです）。

**表 *8 :* 送信元から宛先ネットワークへのマッピング：*vmxnet3***

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Management0/0 | 管理 |
| Network adapter 2 | Diagnostic 0-0 | Diagnostic0/0 | 診断 |
| ネットワークアダプタ 3 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部データ |
| ネットワークアダプタ 4 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部データ |
| ネットワークアダプタ 5 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet 0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ネットワークアダプタ 7 | GigabitEthernet 0-4 | GigabitEthernet 0/4 | データトラフィック（オプション） |
| ネットワークアダプタ 8 | GigabitEthernet 0-5 | GigabitEthernet 0/5 | データトラフィック（オプション） |
| ネットワークアダプタ 9 | GigabitEthernet 0-6 | GigabitEthernet 0/6 | データトラフィック（オプション） |
| ネットワークアダプタ 10 | GigabitEthernet 0-7 | GigabitEthernet 0/7 | データトラフィック（オプション） |

Threat Defense Virtual を展開する際には、合計 10 個のインターフェイスを指定できます。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。すべての Threat Defense Virtual インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、Threat Defense Virtual 設定内でそのインターフェイスを無効のままにしておいて構いません。

b) [ディスクプロビジョニング（Disk provisioning）]：仮想マシンの仮想ディスクを保存するためのディスク形式を選択します。

[シック（Thick）] プロビジョニングを選択すると、すべてのストレージがただちに割り当てられます。[シン（Thin）] プロビジョニングを選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

**ステップ 13** 新規仮想マシンウィザードの [準備完了（Ready To Complete）] ページで、仮想マシンの設定を確認します。

a) （任意）ウィザードの設定を確認または変更するには、[戻る（back）] をクリックして戻ります。
b) （任意）作成タスクを破棄してウィザードを閉じるには、[キャンセル（Cancel）] をクリックします。
c) [終了（Finish）] をクリックして作成タスクを完了し、ウィザードを終了します。

ウィザードが完了すると、ESXi ホストによって VM が処理されます。展開のステータスは [最近使用したタスク（Recent Tasks）] で確認できます。展開が成功すると、[結果（Results）] 列に [正常に完了（Completed successfully）] が表示されます。

新しい Threat Defense Virtual 仮想マシンインスタンスが、ESXi ホストの仮想マシンインベントリの下に表示されます。新しい仮想マシンの起動には、最大 30 分かかることがあります。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

### 次のタスク

- CLI を使用して仮想デバイスのセットアップを完了します。これは、ESXi OVF テンプレートを使用して Threat Defense Virtual を展開する場合の次の手順になります。「CLI を使用した Threat Defense Virtual のセットアップ （34 ページ）」を参照してください。

# CLI を使用した Threat Defense Virtual のセットアップ

ESXi OVF テンプレートを使用して展開した場合は、CLI を使用して Threat Defense Virtual をセットアップする必要があります。Threat Defense Virtual アプライアンスには Web インターフェイスがありません。また、展開時に VI OVF テンプレートを使用し、セットアップウィザードを使用しなかった場合も、CLI を使用してシステムに必要な設定を行うことができます。

（注） VI OVF テンプレートを使用して展開し、かつセットアップウィザードを使用した場合は、仮想デバイスが設定済みであり、それ以上のデバイス設定は必要ありません。以降の手順は、選択する管理モードによって異なります。

新しく設定されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアッププロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定およびファイアウォールモードを設定します。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が (y/n) のように括弧で囲まれて示されます。デフォルト値は、[y] のように大カッコ内に列挙されます。選択を確定するには、Enter キーを押します。

**ステップ 1** VMware コンソールを開きます。

**ステップ 2** [firepowerログイン（firepower login）] プロンプトで、ユーザー名 **admin** とパスワード **Admin123** のデフォルトのクレデンシャルでログインします。

**ステップ 3** Threat Defense Virtual システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理で Device Manager を使用）

**ステップ 4** セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

設定が実装されたときに、VMware コンソールにメッセージが表示される場合があります。

**ステップ 5** プロンプトに従ってシステム設定を行います。

**ステップ 6** コンソールが firepower # プロンプトに戻るときに、設定が正常に行われたことを確認します。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

### 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# ESXi 構成でのパフォーマンスの向上

ESXi ホストの CPU 構成時の設定を調整することによって、ESXi 環境内の Threat Defense Virtual のパフォーマンスを向上させることができます。[Scheduling Affinity] オプションによって、仮想マシンの CPU をホストの物理コア（およびハイパースレッディングが有効になっている場合のハイパースレッド）にどのように分散させるかを制御できます。この機能を使用すれば、各仮想マシンを、指定したアフィニティセット内のプロセッサに割り当てることができます。

詳細については、以下の VMware ドキュメントを参照してください。

- 「*Administering CPU Resources*」の章（『vSphere Resource Management』）。
- 『Performance Best Practices for VMware vSphere』
- vSphere Client のオンライン ヘルプ。

# NUMA のガイドライン

Non-uniform Memory Access（NUMA）は、マルチプロセッサシステムのプロセッサに対するメインメモリモジュールの配置について記述する共有メモリアーキテクチャです。プロセッサが自身のノード（リモートメモリ）内に存在しないメモリにアクセスする場合は、ローカルメモリにアクセスする場合よりも低速の速度で、NUMA 接続を介してデータを転送する必要があります。

X86 サーバーアーキテクチャは、複数のソケットおよびソケット内の複数のコアで構成されています。各 CPU ソケットとそのメモリおよび I/O が、NUMA ノードと呼ばれます。メモリからパケットを効率的に読み取るには、ゲストアプリケーションおよび関連付けられている周辺機器（NIC など）が同じノード内に存在する必要があります。

最適な Threat Defense Virtual パフォーマンスを実現するには：

- Threat Defense Virtual VM は、1 つの NUMA ノード上で実行する必要があります。1 つの Threat Defense Virtual が 2 つのソケットで実行されるように展開されている場合、パフォーマンスは大幅に低下します。
- 8 コア Threat Defense Virtual では、ホスト CPU の各ソケットが、それぞれ 8 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- 16 コア Threat Defense Virtual では、ホスト CPU 上の各ソケットが、それぞれ 16 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- NIC は、Threat Defense Virtual VM と同じ NUMA ノード上にある必要があります。

NUMA システムと ESXi の使用に関する詳細については、VMware ドキュメント『*vSphere Resource Management*』で、お使いの VMware ESXi バージョンを参照してください。このドキュメントおよびその他の関連ドキュメントの最新エディションを確認するには、http://www.vmware.com/support/pubs を参照してください。

# SR-IOV インターフェイスのプロビジョニング

Single Root I/O Virtualization（SR-IOV）により、さまざまなゲスト オペレーティング システムを実行している複数の VM が、ホストサーバー内の単一の PCIe ネットワークアダプタを共有できるようになります。SR-IOV では、VM がネットワーク アダプタとの間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。最近の x86 サーバー プロセッサには、SR-IOV に必要なダイレクト メモリの転送やその他の操作を容易にする Intel VT-d テクノロジーなど、チップセットの拡張機能が搭載されています。

SR-IOV 仕様では、次の 2 つのデバイス タイプが定義されています。

- 物理機能（PF）：基本的にスタティック NIC です。PF は、SR-IOV 機能を含む完全な PCIe デバイスです。PF は、通常の PCIe デバイスとして検出、管理、設定されます。単一 PF は、一連の仮想関数（VF）の管理および設定を提供できます。
- Virtual Function（VF）：ダイナミック vNIC に似ています。VF は、データ移動に必要な最低限のリソースを提供する、完全または軽量の仮想 PCIe デバイスです。VF は直接的には管理されず、PF を介して配信および管理されます。1 つ以上の VF を 1 つの VM に割り当てることができます。

VF は、仮想化されたオペレーティング システム フレームワーク内の Threat Defense Virtual 仮想マシンに最大 10 Gbps の接続を提供できます。このセクションでは、VMware 環境で VF を設定する方法について説明します。

# SR-IOV インターフェイスのベストプラクティス

## SR-IOV インターフェイスに関するガイドライン

VMware vSphere 5.1 以降のリリースは、特定の設定の環境でしかSR-IOV をサポートしません。vSphere の一部の機能は、SR-IOV が有効になっていると機能しません。

Threat Defense Virtual と SR-IOV に関するシステム要件に加えて、VMware と SR-IOV に関する要件、サポートされている NIC、機能の可用性、およびアップグレード要件の詳細については、VMware マニュアル内の「Supported Configurations for Using SR-IOV」で確認する必要があります。

このセクションでは、VMware システム上の SR-IOV インターフェイスのプロビジョニングに関するさまざまなセットアップ手順と設定手順を示します。このセクション内の情報は、VMware ESXi 6.0 と vSphere Web Client、Cisco UCS C シリーズ サーバー、および Intel Ethernet Server Adapter X520 - DA2 を使用した特定のラボ環境内のデバイスから作成されたものです。

## SR-IOV インターフェイスに関する制限事項

Threat Defense Virtual を起動すると、ESXi で表示される順序とは逆の順序で、SR-IOV インターフェイスが表示される場合があります。これにより、インターフェイス設定エラーが発生し、特定の Threat Defense Virtual マシンへのネットワーク接続が切断する場合があります。

**注意** Threat Defense Virtual で SR-IOV ネットワーク インターフェイスの設定を開始する前に、インターフェイスのマッピングを確認することが重要です。これにより、ネットワーク インターフェイスの設定が、VM ホストの正しい物理 MAC アドレスインターフェイスに適用されます。

Threat Defense Virtual が起動したら、MAC アドレスとインターフェイスのマッピングを確認できます。**show interface** コマンドを使用して、インターフェイスの MAC アドレスなど、インターフェイスの詳細情報を確認します。インターフェイス割り当てが正しいことを確認するには、**show kernel ifconfig** コマンドの結果と MAC アドレスを比較します。

## ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ Threat Defense Virtual 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

# ESXi ホスト BIOS の確認

### 始める前に

VMware に SR-IOV インターフェイスを備えた Threat Defense Virtual を導入するには、仮想化をサポートして有効にする必要があります。VMware では、SR-IOV サポートに関するオンラインの『Compatibility Guide』だけでなく、仮想化が有効か無効かを検出するダウンロード可能な『CPU Identification Utility』も含めて、仮想化サポートの各種確認手段を提供しています。

また、ESXi ホストにログインすることによって、BIOS 内で仮想化が有効になっているかどうかを判断することもできます。

**ステップ 1** 次のいずれかの方法を使用して、ESXi シェルにログインします。

- ホストへの直接アクセスがある場合は、Alt+F2 を押して、マシンの物理コンソールのログインページを開きます。
- ホストにリモートで接続している場合は、SSH または別のリモート コンソール接続を使用して、ホスト上のセッションを開始します。

**ステップ 2** ホストによって認識されるユーザ名とパスワードを入力します。

**ステップ 3** Run the following commands:

```
esxcfg-info|grep "\----\HV Support"
```

- HV Support コマンドの出力は、使用可能なハイパーバイザサポートのタイプを示します。可能性のある値の説明を以下に示します。
- 0：VT/AMD-V は、サポートがこのハードウェアでは使用できないことを示します。
- 1：VT/AMD-V は、VT または AMD-V を使用できますが、このハードウェアではサポートされないことを示します。
- 2：VT/AMD-V は、VT または AMD-V を使用できますが、現在、BIOS 内で有効になっていないことを示します。
- 3：VT/AMD-V は、VT または AMD-V が BIOS 内で有効になっており、使用できることを示します。

```
~ # esxcfg-info|grep "\----\HV Support"
         |----HV Support.........................3
```

値の 3 は、仮想化がサポートされており、有効になっていることを示します。

### 次のタスク

ホスト物理アダプタ上で SR-IOV を有効にします。

# ホスト物理アダプタ上での SR-IOV の有効化

仮想マシンを仮想機能に接続する前に、vSphere Web Client を使用して、SR-IOV を有効にし、ホスト上の仮想機能の数を設定します。

### 始める前に

- SR-IOV 互換ネットワーク インターフェイス カード（NIC）がインストールされていることを確認します。「システム要件 （5 ページ）」を参照してください。

**ステップ 1** vSphere Web Client で、SR-IOV を有効にする ESXi ホストに移動します。

**ステップ 2** [Manage] タブで、[Networking] をクリックし、[Physical adapters] を選択します。

SR-IOV プロパティを調査することにより、物理アダプタが SR-IOV をサポートしているかどうかを確認できます。

**ステップ 3** 物理アダプタを選択し、[Edit adapter settings] をクリックします。

**ステップ 4** SR-IOV の下で、[Status] ドロップダウン メニューから [Enabled] を選択します。

**ステップ 5** [Number of virtual functions] テキストボックスに、アダプタに設定する仮想機能の数を入力します。

（注） インターフェイスあたり 2 つ以上の VF を使用**しない**ことをお勧めします。物理インターフェイスを複数の仮想機能で共有すると、パフォーマンスが低下する可能性があります。

**ステップ 6** [OK] をクリックします。

**ステップ 7** ESXi ホストを再起動します。

物理アダプタ エントリで表現された NIC ポートで仮想機能がアクティブになります。これらは、ホストの [Settings] タブの [PCI Devices] リストに表示されます。

### 次のタスク

- SR-IOV 機能と設定を管理するための標準 vSwitch を作成します。

# vSphere スイッチの作成

SR-IOV インターフェイスを管理するための vSphere スイッチを作成します。

**ステップ 1** vSphere Web Client で、ESXi ホストに移動します。

**ステップ 2** [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。

**ステップ 3** プラス（+）記号付きの緑色の地球アイコンである [Add host networking] アイコンをクリックします。

**ステップ 4** [標準スイッチ用仮想マシンポートグループ（Virtual Machine Port Group for a Standard Switch）] 接続タイプを選択して、[次へ（Next）] をクリックします。

**ステップ 5** [New standard switch] を選択して、[Next] をクリックします。

**ステップ 6** 物理ネットワーク アダプタを新しい標準スイッチに追加します。

a) 割り当てられたアダプタの下で、緑色のプラス（+）記号をクリックしてアダプタを追加します。

b) リストから SR-IOV に対応するネットワーク インターフェイスを選択します。たとえば、Intel(R) 82599 10 Gigabit Dual Port Network Connection を選択します。

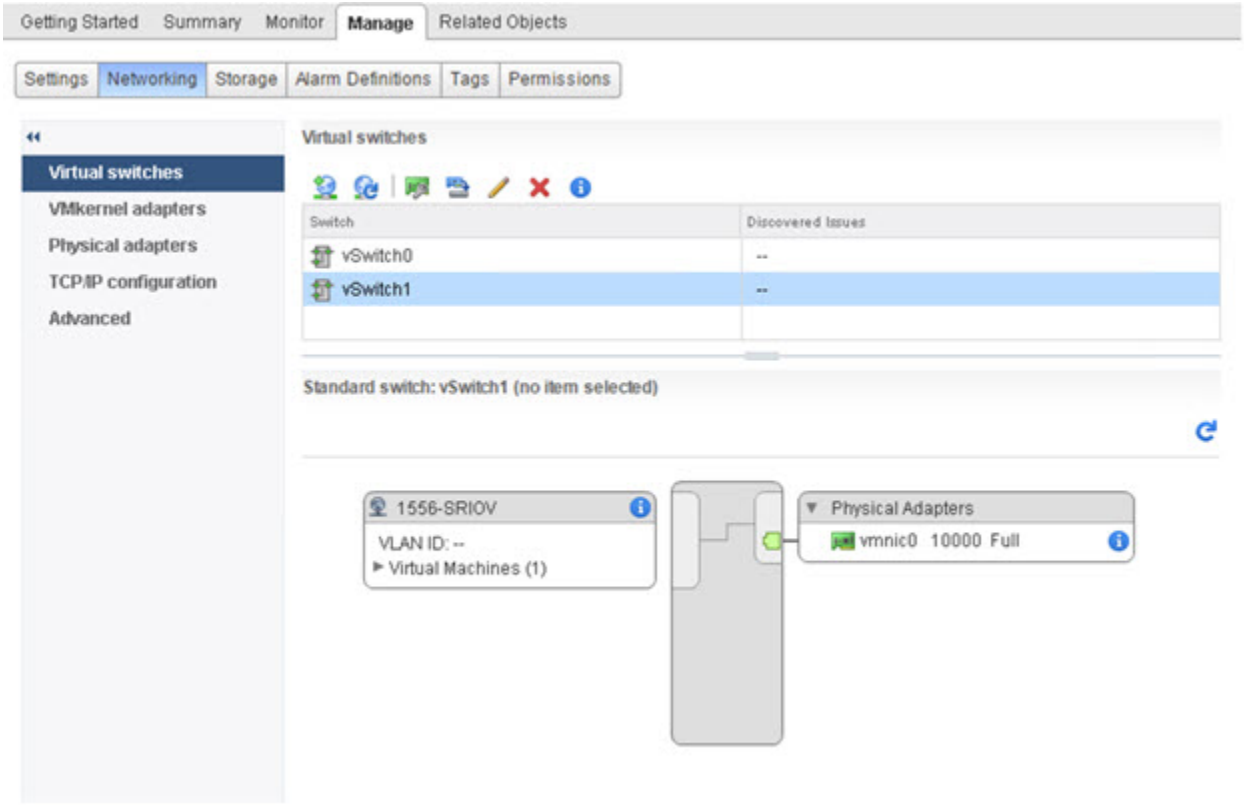
c) [Failover order group] ドロップダウン メニューで、[Active adapters] から選択します。

d) [OK] をクリックします。

**ステップ 7** SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。

**ステップ 8** [Ready to complete] ページで選択を確認してから、[Finish] をクリックします。

図 *2 : SR-IOV* インターフェイスがアタッチされた新しい *vSwitch*




### 次のタスク

- 仮想マシンの互換性レベルを確認します。

# 仮想マシンの互換性レベルのアップグレード

互換性レベルは、ホストマシンで使用可能な物理ハードウェアに対応する仮想マシンで使用可能な仮想ハードウェアを決定します。Threat Defense Virtual VM は、ハードウェアレベルを 10 以上にする必要があります。これにより、SR-IOV のパススルー機能が Threat Defense Virtual に公開されます。この手順では、Threat Defense Virtual を短時間で最新のサポートされている仮想ハードウェアバージョンにアップグレードします。

仮想マシンのハードウェアバージョンと互換性については、vSphere 仮想マシン管理マニュアルを参照してください。

**ステップ 1** vSphere Web Client から vCenter Server にログインします。

**ステップ 2** 変更する Threat Defense Virtual マシンを見つけます。

a) データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択して、[Related Objects] タブをクリックします。

b) [仮想マシン（Virtual Machines）] をクリックして、リストから Threat Defense Virtual マシンを選択します。

**ステップ 3** 選択した仮想マシンの電源をオフにします。

**ステップ 4** Threat Defense Virtual を右クリックして、**[アクション（Actions）] > [すべてのvCenterアクション（All vCenter Actions）] > [互換性（Compatibility）] > [VMアップグレードの互換性（Upgrade VM Compatibility）]** を選択します。

**ステップ 5** [はい（Yes）] をクリックして、アップグレードを確認します。

**ステップ 6** 仮想マシンの互換性で [ESXi 5.5以降（ESXi 5.5 and later）] オプションを選択します。

**ステップ 7** （オプション）[通常のゲストOSのシャットダウン後にのみアップグレード（Only upgrade after normal guest OS shutdown）] を選択します。

選択された仮想マシンが、選択された [互換性（Compatibility）] 設定の対応するハードウェアバージョンにアップグレードされ、仮想マシンの [概要（Summary）] タブで新しいハードウェアバージョンが更新されます。

### 次のタスク

- SR-IOV パススルー ネットワーク アダプタを介して Threat Defense Virtual と仮想機能を関連付けます。

# Threat Defense Virtual への SR-IOV NIC の割り当て

Threat Defense Virtual マシンと物理 NIC がデータを交換可能なことを保証するには、Threat Defense Virtual を SR-IOV パススルー ネットワーク アダプタとして 1 つ以上の仮想機能に関連付ける必要があります。次の手順では、vSphere Web Client を使用して、SR-IOV NIC を Threat Defense Virtual マシンに割り当てる方法について説明します。

**ステップ 1** vSphere Web Client から vCenter Server にログインします。

**ステップ 2** 変更する Threat Defense Virtual マシンを特定します。

a) データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択して、[Related Objects] タブをクリックします。

b) [仮想マシン（Virtual Machines）] をクリックして、リストから Threat Defense Virtual マシンを選択します。

**ステップ 3** 仮想マシンの [Manage] タブで、**[Settings] > [VM Hardware]** を選択します。

**ステップ 4** [Edit] をクリックして、[Virtual Hardware] タブを選択します。

**ステップ 5** [New device] ドロップダウン メニューで、[Network] を選択して、[Add] をクリックします。

[New Network] インターフェイスが表示されます。

**ステップ 6** [New Network] セクションを展開して、使用可能な SRIOV オプションを選択します。

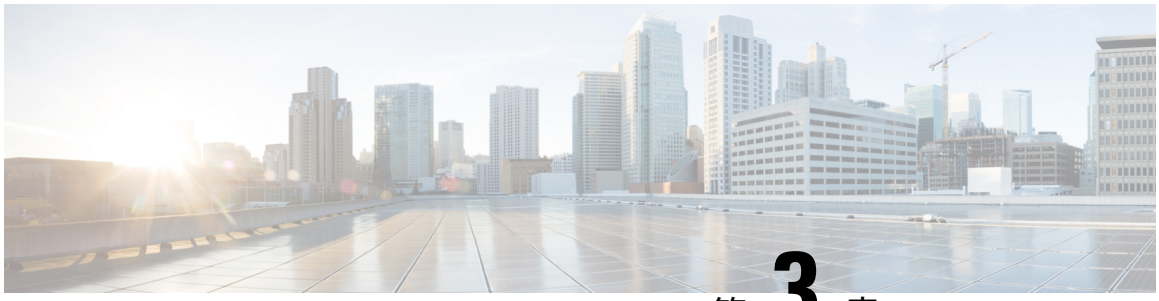
**ステップ 7** [Adapter Type] ドロップダウン メニューで、[SR-IOV passthrough] を選択します。

**ステップ 8** [Physical function] ドロップダウン メニューで、パススルー仮想マシン アダプタに対応する物理アダプタを選択します。

**ステップ 9** 仮想マシンの電源をオンにします。

仮想マシンの電源をオンにすると、ESXi ホストが物理アダプタから空いている仮想機能を選択して、それを SR-IOV パススルー アダプタにマップします。ホストが仮想マシン アダプタと基礎となる仮想機能のすべてのプロパティを確認します。

（注） 無差別モードの制限により、SR-IOV ドライバを使用する一部の Intel ネットワーク アダプタ（Intel X710 や 82599 など）では、SR-IOV インターフェイスを Threat Defense Virtual のパッシブ インターフェイスとして使用することはできません。このような場合は、この機能をサポートするネットワーク アダプタを使用してください。Intel ネットワーク アダプタの詳細については、『Intel Ethernet Products』[英語] を参照してください。



第 3 章

# Threat Defense Virtual の KVM への展開

この章では、Threat Defense Virtual を KVM 環境に展開する手順について説明します。


- 概要 （45 ページ）
- システム要件 （46 ページ）
- 注意事項と制約事項 （48 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （53 ページ）
- 前提条件 （54 ページ）
- エンドツーエンドの手順 （55 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備 （57 ページ）
- Threat Defense Virtual の起動 （59 ページ）
- トラブルシューティング （65 ページ）


## 概要

KVM は、仮想化拡張機能（Intel VT など）を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネル モジュール（kvm.ko）と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。

KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual 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 *9 : Threat Defense Virtual* 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/32 GB | 16 Gbps | 10,000 |

Threat Defense Virtual 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* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。

# システム要件

Threat Defense Virtual のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入するインスタンス数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

表 *10 : Threat Defense Virtual* アプライアンスのリソース要件

| 設定 | 値 |
|---|---|
| パフォーマンス階層 | **バージョン 7.0 以降**<br>Threat Defense Virtual 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。<br>• FTDv5 4vCPU/8GB（100 Mbps）<br>• FTDv10 4vCPU/8GB（1 Gbps）<br>• FTDv20 4vCPU/8GB（3 Gbps）<br>• FTDv30 8vCPU/16GB（5 Gbps）<br>• FTDv50 12vCPU/24GB（10 Gbps）<br>• FTDv100 16vCPU/32GB（16 Gbps）<br>Threat Defense Virtual 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* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。<br>（注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。 |
| コアおよびメモリの数 | **バージョン 6.4 からバージョン 6.7**<br>Threat Defense Virtual は、調整可能な vCPU およびメモリリソースを使用して展開されます。サポートされている vCPU/メモリのペアの値は、次の 3 つです。<br>• 4 vCPU/8 GB（デフォルト）<br>• 8 vCPU/16 GB<br>• 12 vCPU/24 GB<br>（注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。上記の 3 つの組み合わせだけがサポートされます。 |

| 設定 | 値 |
|---|---|
| | **バージョン 6.3 以前**<br>Threat Defense Virtual は、固定の vCPU およびメモリリソースを使用して展開されます。サポートされている vCPU/メモリのペアの値は次の 1 つだけです。<br>• 4 vCPU/8 GB<br>（注） vCPU とメモリの調整はサポートされていません。 |
| ハードディスク プロビジョニング サイズ | • 50 GB<br>• 調整可能な設定です。virtio ブロック デバイスをサポート |
| vNIC | KVM の Threat Defense Virtual は次の仮想ネットワークアダプタをサポートしています。<br>• **VIRTIO**：Virtio は、KVM の IO 仮想化のメインプラットフォームであり、IO 仮想化のハイパーバイザに共通のフレームワークを提供します。ホストの実装はユーザー空間（QEMU）にあるため、ホストにドライバは必要ありません。<br>• **IXGBE-VF**：ixgbe-vf（10 ギガビット/秒）ドライバは、SR-IOV をサポートするカーネルでのみアクティブ化できる仮想関数デバイスをサポートしています。SR-IOV には適切なプラットフォームおよび OS のサポートが必要です。詳細については、「SR-IOV のサポート」を参照してください。 |

# 注意事項と制約事項

• ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要

（注） Threat Defense Virtual のデフォルト設定では、管理インターフェイス、診断インターフェイス、および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。

• Virtio ドライバをサポート

• SR-IOV の ixgbe-vf ドライバをサポート

• 合計 10 個のインターフェイスをサポート

- Threat Defense Virtual のデフォルト設定は、管理インターフェイス（管理と診断）および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用することを前提としています（外部インターフェイス経由）。
- Threat Defense Virtual は、少なくとも 4 つのインターフェイスを備え、firstboot で電源がオンになる必要があります。4 つのインターフェイスがなければ展開は実行されません。
- Threat Defense Virtual では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワークインターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。
  - 管理インターフェイス（1）（必須）

（注） 管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center へのアクセスに関するデータインターフェイス設定の詳細については、『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（2）（必須）
  - 外部インターフェイス（3）（必須）
  - 内部インターフェイス（4）（必須）
  - データインターフェイス（5 ～ 10）（オプション）

Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークに関する以下の用語索引を参照してください。

**表 *11* : 送信元から宛先ネットワークへのマッピング**

| ネットワーク アダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| vnic0* | Management0-0 | Management0/0 | 管理 |
| vnic1* | Diagnostic 0-0 | Diagnostic0/0 | 診断 |
| vnic2 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部 |
| vnic3* | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部 |

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| * 重要同じサブネットに接続します。 | | | |

- 仮想マシンの複製はサポートされません。
- コンソールアクセスでは、Telnet を介したターミナルサーバーをサポートします。
- KVM で IPv6 をサポートする設定の vNIC を作成するには、IPv6 設定パラメータで構成される XML ファイルをインターフェイスごとに作成する必要があります。**virsh net-create** <<*interface configuration XML file name*>> コマンドを使用してこれらの XML ファイルを実行することにより、IPv6 ネットワークプロトコルを使用する vNIC をインストールできます。

  インターフェイスごとに、次の XML ファイルを作成できます。

  - 管理インターフェイス：*mgmt-vnic.xml*
  - 診断インターフェイス：*diag-vnic.xml*
  - 内部インターフェイス：*inside-vnic.xml*
  - 外部インターフェイス：*outside-vnic.xml*

  **例**：

  IPv6 設定の管理インターフェイス用の XML ファイルを作成する方法。

```
<network>
             <name>mgmt-vnic</name>
             <bridge name='mgmt-vnic' stp='on' delay='0' />
             <ip family='ipv6' address='2001:db8::a111:b220:0:abcd' prefix='96'/>
        </network>
```

  同様に、他のインターフェイス用の XML ファイルも作成する必要があります。

  次のコマンドを実行して、KVM にインストールされている仮想ネットワークアダプタを確認できます。

```
virsh net-list
         brctl show
```

### CPU モード

KVM は、さまざまな種類の CPU をエミュレートできます。VM の場合、通常はホストシステムの CPU に厳密に一致するプロセッサタイプを選択する必要があります。これにより、ホストの CPU 機能（CPU フラグとも呼ばれます）が VM で使用できるようになります。CPU タイプを**ホスト**に設定する必要があります。その場合、VMはホストシステムとまったく同じCPUフラグを持ちます。

### クラスタリング

クラスタリングはKVMで展開されたThreat Defense Virtualインスタンスでサポートされます。詳細については、『プライベートクラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「KVM での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### SR-IOV のサポート

SR-IOV 仮想機能には特定のシステムリソースが必要です。SR-IOV 対応 PCIe アダプタに加えて、SR-IOV をサポートするサーバーが必要です。以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。次の NIC がサポートされています。
  - Intel Ethernet Server Adapter X710
  - Intel Ethernet Server Adapter X520 - DA2
  - Intel Ethernet Network Adapter E810-CQDA2
    - ファームウェア (NVM イメージ) とネットワークドライバーは、NVM ユーティリティツールを使用して Intel® Network Adapter E810 で更新されます。不揮発性メモリ (NVM) イメージとネットワークドライバーは、Intel® Network Adapter E810 上で組み合わせて更新する互換性のあるコンポーネントのセットです。NVM とソフトウェアの互換性マトリックスについては、「Intel® Ethernet Controller E810 データシート」を参照して、Intel® Network Adapter E810 の正しいファームウェアドライバーを更新してください。
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。
- x86_64 マルチコア CPU：Intel Sandy Bridge 以降（推奨）。

（注） シスコでは、Threat Defense Virtual を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア
  - CPU ソケットあたり 8 個以上の物理コア。
  - 単一のソケット上で 8 コアにする必要があります。

（注） CPU ピンニングは、フルスループットを実現するために推奨されています。

- メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。KVM の場合は、SR-IOV サポートの CPU の互換性を確認できます。KVM 上の Threat Defense Virtual では、x86 ハードウェアしかサポートされないことに注意してください。

### ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ Threat Defense Virtual 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、お

よび読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。

- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# 前提条件

- Cisco.com から Threat Defense Virtual qcow2 ファイルをダウンロードし、Linux ホストに格納します。

  https://software.cisco.com/download/navigator.html

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

- このマニュアルの導入例では、ユーザーが Ubuntu 18.04 LTS を使用していることを前提としています。Ubuntu 18.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin
  - bridge-utils
  - Virt-Manager
  - virtinst
  - virsh tools
  - genisoimage
- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での Threat Defense Virtual のスループットを最大化できます。一般的なホスト調整の概念については、『Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture』を参照してください。
- 以下の機能は Ubuntu 18.04 LTS の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 18.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPUを 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。

  - pinning：qemu および vhost プロセスを特定のCPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。

- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM と システムの互換性については、「Cisco Firepower Threat Defense Virtual Compatibility」を参照してください。
- 次の方法で、仮想マシンが KVM を実行しているかどうかを確認します。
  - **lsmod** を実行して、Linux カーネルのモジュールの一覧を表示します。KVM が実行されている場合は、次の出力が表示されます。

    **root@kvm-host:~$ lsmod | grep kvm**

    **kvm_intel 123675 0**

    **kvm 257361 1 kvm_intel**

- **ls -l /dev/kvm** が対象の VM に存在しない場合は、おそらく **QEMU** を実行しており、KVM ハードウェアアシスト機能を利用していません。

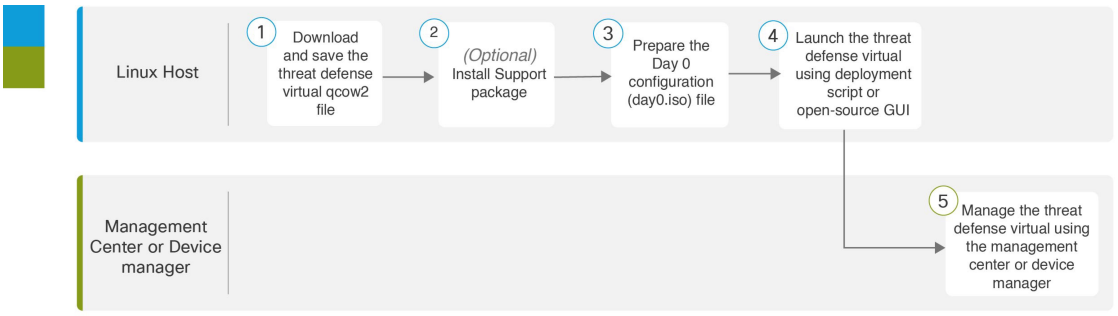
  **root@kvm-host:~$ ls -l /dev/kvm**

  **crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm**
- 次のコマンドを実行して、ホストマシンが KVM をサポートしているかどうかも確認します。

  **root@kvm-host:~$ sudo kvm-ok**
- KVM アクセラレーションを使用することもできます。

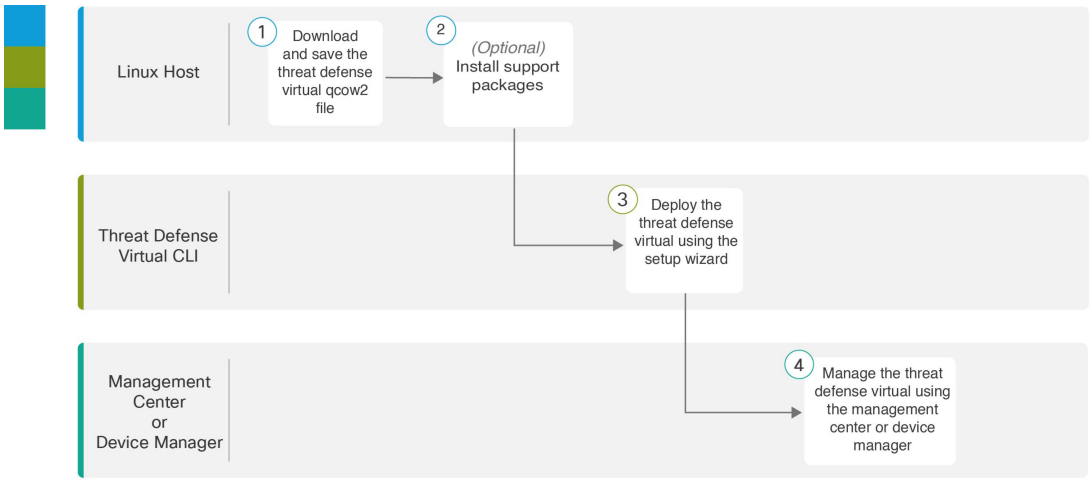
# エンドツーエンドの手順

次のフローチャートは、Day 0 の構成ファイルを使用して KVM インスタンスに Threat Defense Virtual を展開する際のワークフローを示しています。



| | ワークスペース | 手順 |
|---|---|---|
| 1 | Linux ホスト | 前提条件 （54 ページ） ：Linux ホストに Threat Defense Virtual qcow2 ファイルをダウンロードして保存します。 |
| 2 | Linux ホスト | 前提条件 （54ページ） ：サポートパッケージをインストールします。 |
| 3 | Linux ホスト | 第 0 日のコンフィギュレーション ファイルの準備 |
| 4 | Linux ホスト | Threat Defense Virtual の起動 ：<br>• 導入スクリプトを使用した起動<br>• グラフィカル ユーザー インターフェイス （GUI） の起動 |
| 5 | Management Center | Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 |

次のフローチャートは、Day 0 の構成ファイルを使用せずに KVM インスタンスに Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Linux ホスト | 前提条件 （54 ページ） ：Linux ホストに Threat Defense Virtual qcow2 ファイルをダウンロードして保存します。 |
| 2 | Linux ホスト | 前提条件 （54ページ） ：サポートパッケージをインストールします。 |
| 3 | Threat Defense Virtual CLI | 第 0 日のコンフィギュレーション ファイルを使用しない起動 ：セットアップウィザードを使用して Threat Defense Virtual を展開します。 |

| | ワークスペース | 手順 |
|---|---|---|
| 4 | Management Center | Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 |

# 第 0 日のコンフィギュレーション ファイルの準備

Threat Defense Virtual を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキスト ファイルです。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。

**重要** day0.iso ファイルは、最初のブート時に使用できる必要があります。

導入時に Day 0 の構成ファイルを使用すると、導入プロセスで Threat Defense Virtual アプライアンスの初期設定をすべて実行できます。次を指定することができます。

- エンド ユーザー ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 管理モード。Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）を参照してください。

  [ローカルに管理（ManageLocally）] を [はい（Yes）] に設定するか、または Management Center フィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に情報を入力することができます。使用していない管理モードでは、フィールドを空のままにします。
- 最初のファイアウォール モード。最初のファイアウォール モード（**ルーテッド**または**トランスペアレント**）を設定します。

  ローカルの Device Manager を使用して展開を管理する予定の場合は、ファイアウォール モードには**ルーテッド**のみを設定できます。Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。
- Threat Defense Virtual をクラスタモードで展開するかスタンドアロンモードで展開するかを指定できる展開タイプ。

導入時に Day 0 の構成ファイルを使用しない場合は、起動後にシステムの必須設定を指定する必要があります。詳細については、「第 0 日のコンフィギュレーション ファイルを使用しない起動 （64 ページ）」を参照してください。

（注） この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

### 手順の概要

1. 「day0-config」というテキスト ファイルに Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Management Center の管理に関する情報を追加します。
2. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。
3. 手順を繰り返して、導入する Device Manager ごとに一意のデフォルト設定ファイルを作成します。

### 手順の詳細

**ステップ 1** 「day0-config」というテキスト ファイルに Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Management Center の管理に関する情報を追加します。

**例**：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "r2M$9^Uk69##",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "enabled",
    "IPv6Addr": "2001:db8::a111:b221:1:abca/96",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"No"
}
```

ローカルの Device Manager を使用するには、Day 0 の構成ファイル内で [ローカルに管理（ManageLocally）] に対して [はい（Yes）] と入力します。または、Management Center のフィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

**ステップ 2** テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

**例**：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

または

例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

**ステップ 3** 手順を繰り返して、導入する Device Manager ごとに一意のデフォルト設定ファイルを作成します。

### 次のタスク

- virt-install を使用している場合は、virt-install コマンドに次の行を追加します。

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- virt-manager を使用している場合、virt-manager の GUI を使用して仮想 CD-ROM を作成できます。「グラフィカル ユーザー インターフェイス（GUI）の起動 （61 ページ）」を参照してください。

# Threat Defense Virtual の起動

## 導入スクリプトを使用した起動

virt-install ベースの導入スクリプトを使用して Threat Defense Virtual を起動できます。

環境に最適なゲスト キャッシング モードを選択してパフォーマンスを最適化できることに注意してください。使用中のキャッシュ モードは、データ損失が発生するかどうかに影響を与え、キャッシュ モードはディスクのパフォーマンスにも影響します。

各 KVM ゲスト ディスク インターフェイスで、指定されたいずれかのキャッシュモード（*writethrough*、*writeback*、*none*、*directsync*、または *unsafe*）を指定できます。*writethrough* モードは読み取りキャッシュを提供します。*writeback* は読み取り/書き込みキャッシュを提供します。*directsync* はホストページキャッシュをバイパスします。*unsafe* はすべてのコンテンツをキャッシュし、ゲストからのフラッシュ要求を無視する可能性があります。

- *cache=writethrough* は、ホストで突然の停電が発生した場合の KVM ゲスト マシン上のファイル破損を低減できます。*writethrough* モードの使用をお勧めします。
- ただし、*cache=writethrough* は、*cache=none* よりディスク I/O 書き込みが多いため、ディスク パフォーマンスに影響する可能性もあります。
- *--disk* オプションの cache パラメータを削除する場合、デフォルトは *writethrough* になります。
- キャッシュ オプションを指定しないと、VM を作成するために必要な時間も大幅に短縮される場合もあります。これは、古いRAID コントローラにはディスク キャッシング能力が低いものがあることが原因です。そのため、ディスク キャッシングを無効にして（*ache=none*）、*writethrough* をデフォルトに設定すると、データの整合性を確保できます。

- Threat Defense Virtual のバージョン 6.4 以降は、調整可能な vCPU およびメモリリソースを使用して展開されます。6.4 より前のバージョンの Threat Defense Virtual は、固定構成の 4 vCPU/8 GB デバイスとして展開されていました。各 Threat Defense Virtual プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *12 : virt-install* でサポートされる *vCPU* およびメモリ パラメータ

| **--vcpus** | **--ram** | **Threat Defense Virtual** プラットフォームのサイズ |
|---|---|---|
| 4 | 8192 | 4vCPU/8GB（デフォルト） |
| 8 | 16384 | 8vCPU/16GB |
| 12 | 24576 | 12vCPU/24GB |

**ステップ 1** 「virt_install_ftdv.sh」という virt-install スクリプトを作成します。

Threat Defense Virtual VM の名前は、この KVM ホスト上の他の仮想マシン（VM）全体において一意であることが必要です。Threat Defense Virtual は最大 10 個のネットワーク インターフェイスをサポートできます。この例では、4 つのインターフェイスを使用しています。仮想 NIC は VirtIO にする必要があります。

（注） Threat Defense Virtual のデフォルト設定は、管理インターフェイス、診断インターフェイス、および内部インターフェイスを**同じサブネット**上に配置することを前提としてます。システムでは、少なくとも 4 つのインターフェイスが正常に起動する必要があります。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- (1) 管理インターフェイス（必須）
- (2) 診断インターフェイス（必須）
- (3) 外部インターフェイス（必須）
- (4) 内部インターフェイス（必須）
- (5)（任意）データインターフェイス：最大6

**例**：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
```

```
--virt-type=kvm \
--import \
--watchdog i6300esb,action=reset \
--disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
--disk path=<day0_filename>.iso,format=iso,device=cdrom \
--console pty,target_type=serial \
--serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
--force
```

**ステップ 2** virt_install スクリプトを実行します。

**例：**

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

ウィンドウが開き、VMのコンソールが表示されます。VMが起動中であることを確認できます。VMが起動するまでに数分かかります。VM が起動したら、コンソール画面から CLI コマンドを実行できます。

### 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。

- [ローカルに管理（Manage Locally）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# グラフィカル ユーザー インターフェイス（GUI）の起動

GUI を使用して KVM 仮想マシンを管理するためのオープンソースオプションがいくつかあります。以下の手順では、virt-manager（Virtual Machine Manager とも呼ばれる）を使用して Threat Defense Virtual を起動します。virt-manager は、ゲスト仮想マシンを作成および管理するためのグラフィカルツールです。

（注） KVM は、さまざまな種類の CPU をエミュレートできます。VM の場合、通常はホストシステムの CPU に厳密に一致するプロセッサタイプを選択する必要があります。これにより、ホストの CPU 機能（CPU フラグとも呼ばれます）が VM で使用できるようになります。CPU タイプを**ホスト**に設定する必要があります。その場合、VMはホストシステムとまったく同じCPUフラグを持ちます。

**ステップ 1** virt-manager を起動します（**[アプリケーション（Applications）]** > **[システムツール（System Tools）]** > **[仮想マシンマネージャ（Virtual Machine Manager）]**）。

ハイパーバイザの選択、およびルート パスワードの入力を求められる可能性があります。

**ステップ 2** 左上隅のボタンをクリックし、[VMの新規作成（New VM）] ウィザードを開きます。

**ステップ 3** 仮想マシンの詳細を入力します。

a) オペレーティング システムの場合、[既存のディスクイメージをインポート（Import existing disk image）] を選択します。

この方法でディスク イメージ（事前にインストールされた、ブート可能なオペレーティング システムを含んでいるもの）をインポートできます。

b) [次へ（Forward）] をクリックして続行します。

**ステップ 4** ディスク イメージをロードします。

a) [参照...（Browse...）] をクリックしてイメージ ファイルを選択します。
b) [OSタイプ（OS type）] には [汎用（Generic）] を選択します。
c) [次へ（Forward）] をクリックして続行します。

**ステップ 5** メモリおよび CPU オプションを設定します。

**重要** Threat Defense Virtual は、展開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。

各 Threat Defense Virtual プラットフォームの --vcpus および --ram パラメータでサポートされているパフォーマンス階層と値については、次の表を参照してください。

表 *13 :* 仮想マシンマネージャでサポートされる *vCPU* およびメモリパラメータ

| CPU | メモリ | Threat Defense Virtual プラットフォームのサイズ |
|---|---|---|
| 4 | 8192 | 4vCPU/8GB（デフォルト） |
| 8 | 16384 | 8vCPU/16GB |
| 12 | 24576 | 12vCPU/24GB |

a) Threat Defense Virtual プラットフォームサイズに対応する**メモリ（RAM）**パラメータを設定します。
b) Threat Defense Virtual プラットフォームサイズに対応する **CPU** パラメータを設定します。
c) [次へ（Forward）] をクリックして続行します。

**ステップ 6** [インストール前に設定をカスタマイズする（Customize configuration before install）] チェックボックスをオンにして、[名前（Name）] を指定してから [完了（Finish）] をクリックします。

この操作を行うと、別のウィザードが開き、仮想マシンのハードウェア設定を追加、削除、設定することができます。

**ステップ 7** CPU 構成を次のように変更します。

左側のパネルから [プロセッサ（Processor）] を選択し、**[設定（Configuration）] > [ ホストCPU構成のコピー（Copy host CPU configuration）]** を選択します。

これによって、物理ホストの CPU モデルと設定が VM に適用されます。

**ステップ 8** 仮想ディスクを設定します。

a) 左側のパネルから [ディスク1（Disk 1）] を選択します。
b) [詳細オプション（Advanced Options）] をクリックします。
c) [ディスクバス（Disk bus）] を [Virtio] に設定します。
d) [ストレージ形式（Storage format）] を [qcow2] に設定します。

**ステップ 9** シリアル コンソールを設定します。

a) 左側のパネルから [コンソール（Console）] を選択します。
b) [削除（Remove）] を選択してデフォルト コンソールを削除します。
c) [ハードウェアを追加（Add Hardware）] をクリックしてシリアル デバイスを追加します。
d) [デバイスタイプ（Device Type）] で、[TCP net console (tcp)] を選択します。
e) [モード（Mode）] で、[サーバーモード（バインド）（Server mode (bind)）] を選択します。
f) [ホスト（Host）] には「**0.0.0.0**」と入力し、IP アドレスと一意の**ポート**番号を入力します。
g) [Telnetを使用（Use Telnet）] ボックスをオンにします。
h) デバイス パラメータを設定します。

**ステップ 10** KVMゲストがハングまたはクラッシュしたときに何らかのアクションが自動でトリガーされるようウォッチドッグ デバイスを設定します。

a) [ハードウェアを追加（Add Hardware）] をクリックしてウォッチドック デバイスを追加します。
b) [モデル（Model）] で、[デフォルト（default）] を選択します。
c) [アクション（Action）] で、[ゲストを強制的にリセット（Forcefully reset the guest）] を選択します。

**ステップ 11** 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。

[ハードウェアの追加（Add Hardware）] をクリックしてインターフェイスを追加し、**macvtap** を選択するか、共有デバイス名を指定します（ブリッジ名を使用）。

（注） KVM 上の Threat Defense Virtual では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

vnic0：管理インターフェイス（必須）

vnic1：診断インターフェイス（必須）

vnic2：外部インターフェイス（必須）

vnic3：内部インターフェイス（必須）

vnic4-9：データ インターフェイス（オプション）

**重要** vnic0、vnic1、および vnic3 は、必ず同じサブネットにマップするようにしてください。

**ステップ 12** 第 0 日のコンフィギュレーション ファイルを使用して展開する場合、ISO の仮想 CD-ROM を作成します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) [ストレージ（Storage）] を選択します。
c) [管理対象またはその他既存のストレージを選択（Select managed or other existing storage）] をクリックし、ISO ファイルの場所を参照します。
d) [デバイスタイプ（Device type）] で、[IDE CDROM] を選択します。

**ステップ 13** 仮想マシンのハードウェアを設定した後、[適用（Apply）] をクリックします。

**ステップ 14** virt-manager の [インストールの開始（Begin installation）] をクリックして、指定したハードウェア設定で仮想マシンを作成します。

### 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。

- [ローカルに管理（ManageLocally）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# 第 0 日のコンフィギュレーション ファイルを使用しない起動

Threat Defense Virtual アプライアンスには Web インターフェイスがないため、Day 0 の構成ファイルを使用せずに導入した場合には、CLI を使用して仮想デバイスを設定する必要があります。

新しく展開されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアッププロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定およびファイアウォールモードを設定します。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が (*y*/*n*) のように括弧で囲まれて示されます。デフォルト値は、[*y*] のように大カッコ内に列挙されます。選択を確定するには、Enter キーを押します。

（注） 初期セットアップの完了後に仮想デバイスに関するこれらの設定を変更するには、CLI を使用する必要があります。

**ステップ 1** Threat Defense Virtual でコンソールを開きます。

**ステップ 2** [firepower ログイン（firepower login）] プロンプトで、ユーザー名 *admin* とパスワード *Admin123* のデフォルトのクレデンシャルでログインします。

**ステップ 3** Threat Defense Virtual システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理が必要）

**ステップ 4** セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

**ステップ 5** プロンプトに従ってシステム設定を行います。

**ステップ 6** コンソールが # プロンプトに戻るときに、設定が正常に行われたことを確認します。

**ステップ 7** CLI を閉じます。

### 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、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# トラブルシューティング

ここでは、仮想マシンへの KVM 導入に関連する基本的なトラブルシューティング手順について説明します。

### 仮想マシンが KVM を実行しているかどうかを確認

次の方法で、仮想マシンが KVM を実行しているかどうかを確認します。

- **lsmod** コマンドを実行して、Linux カーネルのモジュールの一覧を表示します。KVM が実行されている場合は、次の出力が表示されます。

  **root@kvm-host:~$ lsmod | grep kvm**

  **kvm_intel 123675 0**

  **kvm 257361 1 kvm_intel**

- **ls -l /dev/kvm** コマンドが対象の VM に存在しない場合は、おそらく **QEMU** を実行しており、KVM ハードウェアアシスト機能を利用していません。

  **root@kvm-host:~$ ls -l /dev/kvm**

  **crw------- 1 root root 10, 232 Mar 23 13:53 /dev/kvm**

- 次のコマンドを実行して、ホストマシンが KVM をサポートしているかどうかも確認します。

  **root@kvm-host:~$ sudo kvm-ok**

- KVM アクセラレーションを使用することもできます。

### Threat Defense Virtual の導入中にブートループが発生する

仮想マシンでブートループが発生した場合は、次のことを確認する必要があります。

- 導入先の VM が 8 GB 以上のメモリを備えているかを確認します。
- 導入先の VM が 4 つ以上のインターフェイスを備えているかを確認します。
- 導入先の VM が 4 つ以上の vCPU を備えているかを確認します。
- QEMU プロセスがサーバークラスの CPU（SandyBridge、IvyBridge、Haswell など）を使用しているかを確認します。**ps -edaf | grep qemu** コマンドを使用してプロセスのパラメータを調べます。

### Management Center Virtual の導入中にブートループが発生する

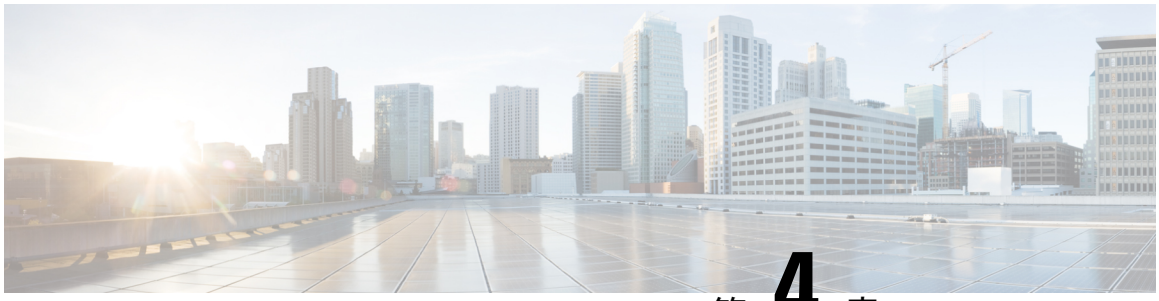
仮想マシンでブートループが発生した場合は、次のことを確認する必要があります。

- 導入先の VM が 28 GB 以上のメモリを備えているかを確認します。
- 導入先の VM が 4 つ以上のインターフェイスを備えているかを確認します。
- 導入先の VM が 4 つ以上の vCPU を備えているかを確認します。
- QEMU プロセスがサーバークラスの CPU（SandyBridge、IvyBridge、Haswell など）を使用しているかを確認します。**ps -edaf | grep qemu** コマンドを使用してプロセスのパラメータを調べます。

### 導入後のトラブルシューティング

Threat Defense Virtual で **system generate-troubleshoot <space> ALL** コマンドを実行して問題を確認し、デバッグ用のログをキャプチャします。

または、**system generate-troubleshoot <space>** の後に疑問符（**?**）または**タブ**ボタンを使用すると、使用可能なオプションやコマンドが表示されます。



第 4 章

# AWS での Threat Defense Virtual の展開

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


- 概要 （69 ページ）
- エンドツーエンドの手順 （71 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （72 ページ）
- AWS ソリューションの概要 （73 ページ）
- 前提条件 （74 ページ）
- 注意事項と制約事項 （75 ページ）
- AWS 環境の設定 （78 ページ）
- Threat Defense Virtual の導入 （84 ページ）
- イメージスナップショットを使用した Threat Defense Virtual （87 ページ）
- Amazon GuardDuty サービスと Threat Defense Virtual の統合 （90 ページ）
- 概要 （90 ページ）
- Amazon GuardDuty と Secure Firewall Threat Defense の統合 （96 ページ）
- 既存のソリューション展開構成の更新 （110 ページ）


## 概要

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

表 *14 :* システム要件

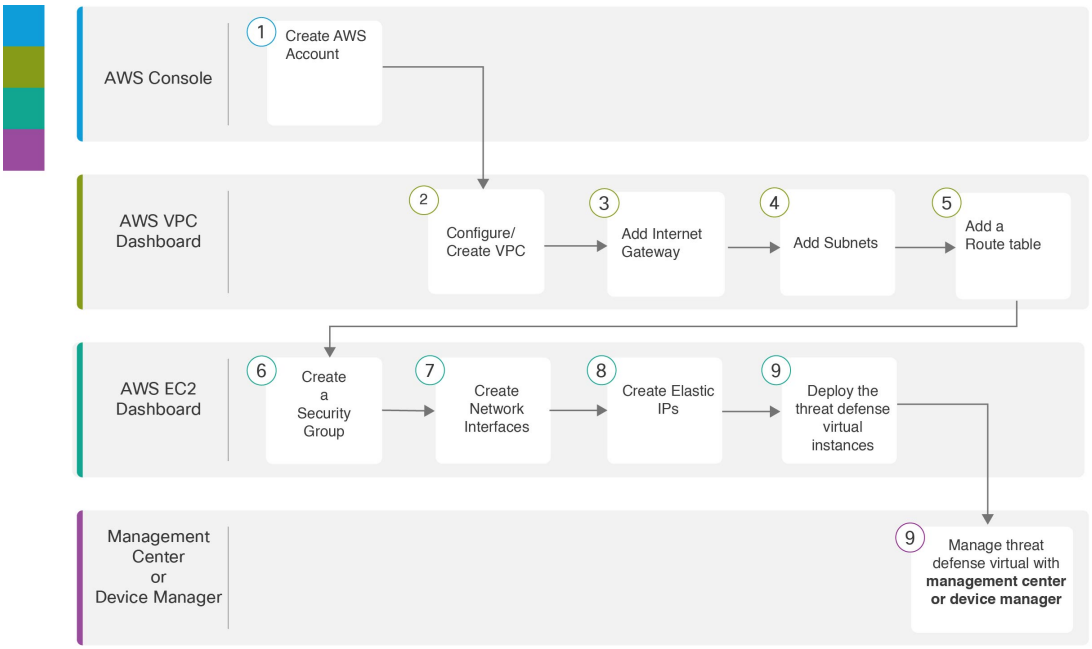
| インスタンス タイプ | Threat Defense Virtual | vCPU | メモリ（GB） | インターフェイスの最大数 |
|---|---|---|---|---|
| c5a.xlarge | 7.1.0 以上 | 4 | 8 | 4 |
| c5a.2xlarge | | 8 | 16 | 4 |
| c5a.4xlarge | | 16 | 32 | 8 |
| c5ad.xlarge | | 4 | 8 | 4 |
| c5ad.2xlarge | | 8 | 16 | 4 |
| c5ad.4xlarge | | 16 | 32 | 8 |
| c5d.xlarge | | 4 | 8 | 4 |
| c5d.2xlarge | | 8 | 16 | 4 |
| c5d.4xlarge | | 16 | 32 | 8 |
| c5n.xlarge | | 4 | 10.5 | 4 |
| c5n.2xlarge | | 8 | 21 | 4 |
| c5n.4xlarge | | 16 | 54 | 8 |
| m5n.xlarge | | 4 | 16 | 4 |
| m5n.2xlarge | | 8 | 32 | 4 |
| m5n.4xlarge | | 16 | 64 | 8 |
| m5zn.xlarge | | 4 | 16 | 4 |
| m5zn.2xlarge | | 8 | 32 | 4 |
| c5.xlarge | 6.6.0 以上 | 4 | 8 | 4 |
| c5.2xlarge | | 8 | 16 | 4 |
| c5.4xlarge | | 16 | 32 | 8 |
| c4.xlarge | 6.4.0 以降 | 4 | 7.5 | 4 |
| c3.xlarge | | 4 | 7.5 | 4 |

（注） Threat Defense Virtual では、インスタンスサイズのサイズ変更によるインスタンスタイプの変更はサポートされていません。新規展開でのみ、異なるインスタンスサイズで Threat Defense Virtual を展開できます。

AWS マーケットプレイスにリストされている NGFWv でサポートされている EC2 インスタンスタイプについては、https://aws.amazon.com/marketplace/pp/prodview-p2336sqyya34e#pdp-overview 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、Amazon Web Services（AWS）に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | AWS コンソール | www.amazon.com：AWS コンソールでユーザーアカウントを作成します。 |
| 2 | AWS VPC ダッシュボード | VPC の作成：AWS アカウント専用の VPC を作成および設定します。 |
| 3 | AWS VPC ダッシュボード | インターネット ゲートウェイの追加：VPC をインターネットに接続するために、インターネットゲートウェイを追加します。 |
| 4 | AWS VPC ダッシュボード | サブネットの追加：VPC にサブネットを追加します。 |

| | ワークスペース | 手順 |
|---|---|---|
| 5 | AWS VPC ダッシュボード | ルートテーブルの追加：VPC 用に設定したゲートウェイにルートテーブルを接続します。 |
| 6 | AWS EC2 ダッシュボード | セキュリティ グループの作成：許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティグループを作成します。 |
| 7 | AWS EC2 ダッシュボード | ネットワーク インターフェイスの作成：静的 IP アドレスを使用して、Threat Defense Virtual のネットワーク インターフェイスを作成します。 |
| 8 | AWS EC2 ダッシュボード | Elastic IP の作成：Elastic IP は、Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。 |
| 9 | AWS EC2 ダッシュボード | Threat Defense Virtual の導入：AWS ポータルから Threat Defense Virtual を展開します。 |
| 10 | Management Centerまたは Device Manager | Threat Defense Virtual を次のように管理します。<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

重要 Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# AWS ソリューションの概要

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

- Amazon Elastic Compute Cloud（EC2）：仮想コンピュータをレンタルして、お客様独自のアプリケーションおよびサービス（ファイアウォールなど）を Amazon のデータセンターで起動および管理できるようにする Web サービス。
- Amazon Virtual Private Cloud（VPC）：Amazon パブリック クラウド内の隔離されたプライベート ネットワークを設定できるようにする Web サービス。EC2 インスタンスは VPC 内で実行されます。

- Amazon Simple Storage Service（S3）：データ ストレージ インフラストラクチャを提供する Web サービス。

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

（注） AMI イメージは AWS 環境の外部ではダウンロードできません。

# 前提条件

- AWS アカウントhttp://aws.amazon.com/ で 1 つ作成できます。
- Threat Defense Virtual コンソールにアクセスするには、SSH クライアント（例：Windows の場合は PuTTY、MacOS の場合はターミナル）が必要です。
- Cisco スマートアカウント。Cisco Software Central で 1 つ作成できます。https://software.cisco.com/
- Threat Defense Virtual へのライセンス付与。

  Cisco Secure Firewall Management Center

  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「Licensing the System」を参照してください。

  Secure Firewall デバイスマネージャ

  - Secure Firewall デバイスマネージャ からセキュリティサービスのすべてのパフォーマンス階層型ライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、「Threat Defense Virtual のライセンス」を参照してください。

- Threat Defense Virtual インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。

    管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。

データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center へのアクセスに関するデータインターフェイス設定の詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。

- トラフィック インターフェイス（2）：Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。

- 通信パス：
  - Threat Defense Virtual にアクセスするためのパブリック IP/Elastic IP。

### サポートされるソフトウェア プラットフォーム

Threat Defense Virtual Auto Scale ソリューションは、Management Center によって管理される Threat Defense Virtual に適用可能です。ソフトウェアバージョンには依存しません。『Cisco Firepower Compatibility Guide』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、シスコの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 の表には、AWS 上の Management Center Virtual における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 の表には、AWS 上の Threat Defense Virtual における互換性および仮想ホスティング環境の要件が一覧表示されています。

（注） AWS Auto Scale ソリューションを導入するためには、AWS 上で Threat Defense Virtual バージョン 6.4 以上を使用する必要があります。メモリベースのスケーリングを使用するには、Management Center バージョン 6.6 以降を実行している必要があります。

# 注意事項と制約事項

### サポートされる機能

- 仮想プライベート クラウド（VPC）への導入
- 拡張ネットワーク（SR-IOV）
- Amazon マーケットプレイスからの導入
- L3 ネットワークの導入
- ルーテッドモード（デフォルト）
- ERSPAN を使用するパッシブモード

- クラスタリング (バージョン 7.2 以降) 詳細については、『パブリッククラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。
- Amazon CloudWatch によって記録されたヘルスモニタリングのメトリクス
- ジャンボ フレーム
- スナップショット (バージョン 7.2 以降)
- IPv6

### サポートされない機能

- 複製
- トランスペアレントモード、インラインモード、パッシブモード
- Transport Layer Security（TLS）サーバーアイデンティティ検出は、AWS での Geneve シングルアームセットアップではサポートされていません。

### ライセンシング

- 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）がサポートされています。
- 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 Threat Defense Virtual を実行できる従量制課金モデル。登録された PAYG Threat Defense Virtual 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。これらのライセンス機能には、登録済みの Management Center で自動的に「アクティブ」のフラグが付けられます。ライセンス供与された機能は、Management Center 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、Device Manager モードで展開されている Threat Defense Virtual デバイスではサポートされていません。

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Firepower Management Center Administration Guide』の「Licenses」の章を参照してください。

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual のバージョン 7.0.0 リリース以降では、Threat Defense Virtual 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 *15 : Threat Defense Virtual* 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 | 4 コア/8 GB | 100 Mbps | 50 |
| FTDv10 | 4 コア/8 GB | 1 Gbps | 250 |
| FTDv20 | 4 コア/8 GB | 3Gbps | 250 |
| FTDv30 | 8 コア/16 GB | 5 Gbps | 250 |
| FTDv50 | 12 コア/24 GB | 10 Gbps | 750 |
| FTDv100 | 16 コア/34 GB | 16 Gbps | 10,000 |

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「AWS での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### Threat Defense Virtual の制限事項

- 推奨されるインスタンスは c5.xlarge です。c3.xlarge インスタンスでは AWS リージョンでの可用性が制限されます。
- 起動時には、2 つの管理インターフェイスが構成されている必要があります。
- 起動するには、2 つのトラフィック インターフェイスと 2 つの管理インターフェイス（合計 4 つのインターフェイス）が必要です。

（注） Threat Defense Virtual はこの 4 つのインターフェイスがなければ起動しません。

- AWS でトラフィック インターフェイスを設定する場合、[送信元/宛先の変更の確認（Change Source/Dest. Check）] オプションを無効にする必要があります。
- IP アドレス（IPv4 および IPv6）設定は（CLI から設定したものでも Management Center から設定したものでも）AWS コンソールで作成されたものと一致する必要があります。展開時に設定を書き留めてください。

- Threat Defense Virtual を登録した後、インターフェイスを編集し、Management Center で有効にする必要があります。IP アドレスは、AWS で設定されたインターフェイスと一致している必要があることに注意してください。
- トランスペアレント モード、インライン モード、パッシブ モードは現時点でサポートされていません。
- インターフェイスを変更するには、AWS コンソールから変更を行う必要があります。AWS コンソールで、Management Center からインターフェイスの登録を解除し、AWS AMI ユーザーインターフェイスを使用しているインスタンスを停止します。次に、変更するインターフェイスを切り離し、新しいインターフェイスを接続します（起動するには、2 つのトラフィック インターフェイスと 2 つの管理インターフェイスが必要であることに注意してください）。ここで、インスタンスを起動し、Management Center に再登録します。

  Management Center から、デバイス インターフェイスを編集し、AWS コンソールから行った変更と一致するように、IP アドレス（IPv4 および IPv6）と他のパラメータを変更します。

（注） IPv6 は、デュアルスタック（IPv4 + IPv6）モードでのみ使用できます。

- ブート後にインターフェイスを追加することはできません。
- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

# AWS 環境の設定

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

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

- VPC の作成 （79 ページ）

• インターネット ゲートウェイの追加 （80 ページ）
• サブネットの追加 （81 ページ）
• ルート テーブルの追加 （81 ページ）
• セキュリティ グループの作成 （82 ページ）
• ネットワーク インターフェイスの作成 （83 ページ）
• Elastic IP の作成 （83 ページ）

### はじめる前に

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

# VPC の作成

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

VPC とサブネットで IPv6 CIDR ブロックを有効にする方法については、AWS のドキュメント『Enable IPv6 in a VPC with a public and private subnet』を参照してください。

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

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

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

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

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

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

a) VPC を識別するユーザー定義の [名前タグ（Name tag）]。

b) IP アドレスの **IPv4 CIDR ブロック**。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。

c) IP アドレスの **IPv6 CIDR ブロック**。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。[::/0] が例として挙げられます。

d) 仮想プライベートクラウドで IPv6 を有効にするには、**Amazon 提供の IPv6 CIDR ブロック**として **IPv6 CIDR ブロック**を選択します。
e) [デフォルト（Default）] の [テナント（Tenancy）] 設定。この VPC で起動されたインスタンスが、起動時に指定されたテナント属性を使用するようにします。

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

### 次のタスク

（注） IPv6 だけを使用して、仮想ネットワーク、サブネット、インターフェースなどを構築することはできません。デフォルトでは IPv4 が使用され、IPv6 も一緒に有効にできます。

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

# インターネット ゲートウェイの追加

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

### はじめる前に

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

**ステップ 1** [サービス（Services）] > [VPC] の順にクリックします。
**ステップ 2** [VPC ダッシュボード（VPC Dashboard）] > [インターネットゲートウェイ（Internet Gateway）] の順にクリックしてから、[インターネットゲートウェイの作成（Create Internet Gateway）] をクリックします。
**ステップ 3** ユーザー定義の [名前タグ（Name tag）] を入力してゲートウェイを特定し、[はい、作成します（Yes, Create）] をクリックしてゲートウェイを作成します。
**ステップ 4** 前のステップで作成したゲートウェイを選択します。
**ステップ 5** [VPCに接続（Attach to VPC）] をクリックして、以前に作成した VPC を選択します。
**ステップ 6** [はい、接続します（Yes, Attach）] をクリックして、ゲートウェイを VPC に追加します。

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

### 次のタスク

次のセクションで説明されているように、VPC にサブネットを追加します。

# サブネットの追加

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

### はじめる前に

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

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

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

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

a) サブネットを識別するユーザー定義の [名前タグ（Name tag）]。

b) このサブネットに使用する [VPC]。

c) このサブネットが存在する [可用性ゾーン（Availability Zone）]。 [設定なし（No Preference）] を選択して、Amazon が選択するゾーンを選びます。

d) IP アドレスの [CIDRブロック（CIDR block）]（IPv4 および IPv6）。サブネットの IP アドレスの範囲は、VPC の IP アドレス範囲のサブセットである必要があります。ブロック サイズは、/16 ネットワーク マスクから /28 ネットワーク マスクの範囲で指定する必要があります。サブネットのサイズは VPC のサイズと同じにすることができます。

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

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

### 次のタスク

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

# ルート テーブルの追加

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

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

**ステップ 2** [VPCダッシュボード（VPC Dashboard）] > [ルートテーブル（Route Tables）] の順にクリックしてから、[ルートテーブルの作成（Create Route Table）] をクリックします。

**ステップ 3** ルート テーブルを識別するユーザー定義の [名前タグ（Name tag）] を入力します。

**ステップ 4** このルート テーブルを使用する [VPC] をドロップダウン リストから選択します。

**ステップ 5** [はい、作成します（Yes, Create）] をクリックして、ルート テーブルを作成します。

**ステップ 6** 作成したルート テーブルを選択します。

**ステップ 7** [ルート（Routes）] タブをクリックして、詳細ペインにルート情報を表示します。

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

a) [宛先（Destination）] 列に、「0.0.0.0/0」、または、IPv6 トラフィックについてはすべて [::/0] を入力します。

b) [ターゲット（Target）] 列で、ゲートウェイを選択します。

**ステップ 9** [保存（Save）] をクリックします。

### 次のタスク

次のセクションで説明するように、セキュリティ グループを作成します。

# セキュリティ グループの作成

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

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

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

**ステップ 3** [セキュリティグループの作成（Create Security Group）] をクリックします。

**ステップ 4** [セキュリティグループの作成（Create Security Group）] ダイアログボックスで、次の内容を入力します。

a) セキュリティ グループを識別するユーザー定義の [セキュリティグループ名（Security group name）]。

b) このセキュリティ グループの [説明（Description）]。

c) このセキュリティ グループに関連付けられた VPC。

**ステップ 5** [セキュリティグループルール（Security group rules）] を設定します。

a) [インバウンド（Inbound）] タブをクリックして、[ルールの追加（Add Rule）] をクリックします。

（注） Management Center Virtual を AWS の外部から管理するには、HTTPS および SSH アクセスが必要です。それに基づいて、送信元 IP アドレスを指定する必要があります。また、Management Center Virtual と Threat Defense Virtual の両方を AWS VPC 内で設定している場合、プライベート IP 管理サブネットアクセスを許可する必要があります。

b) [アウトバウンド（Outbound）] タブをクリックしてから、[ルールの追加（Add Rule）] をクリックして、アウトバウンドトラフィックのルールを追加するか、デフォルトの [すべてのトラフィック（All traffic）]（[タイプ（Type）] の場合）および [任意の宛先（Anywhere）]（[宛先（Destination）] の場合）のままにします。

**ステップ 6** セキュリティ グループを作成するには、[作成（Create）] をクリックします。

### 次のタスク

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

# ネットワーク インターフェイスの作成

Threat Defense Virtual のネットワーク インターフェイスは、静的 IP アドレス（IPv4 および IPv6）または DHCP を使用して作成できます。具体的な展開の必要に応じてネットワーク インターフェイス（内部および外部）を作成します。

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

**ステップ 2** [EC2ダッシュボード（EC2 Dashboard）] > [ネットワークインターフェイス（Network Interfaces）] の順にクリックします。

**ステップ 3** [ネットワークインターフェイスの作成（Create Network Interface）] をクリックします。

**ステップ 4** [ネットワークインターフェイスの作成（Create Network Interface）] ダイアログボックスで、次のものを入力します。

a) ネットワーク インターフェイスに関するオプションのユーザー定義の [説明（Description）]。

b) ドロップダウン リストから [サブネット（Subnet）] を選択します。Threat Defense Virtual インスタンスを作成する VPC のサブネットが選択されていることを確認します。

c) [プライベートIP（Private IP）] アドレスを入力します。静的 IP アドレス（IPv4 および IPv6）または自動生成（DHCP）を使用できます。

d) [セキュリティグループ（Security groups）] を 1 つ以上選択します。セキュリティ グループの必要なポートがすべて開いていることを確認します。

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

**ステップ 6** 作成したネットワーク インターフェイスを選択します。

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

**ステップ 8** [送信元または送信先の確認（Source/destination check）] の下にある [有効化（Enable）] チェックボックスをオフにして、[保存（Save）] をクリックします。

### 次のタスク

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

# Elastic IP の作成

インスタンスが作成されると、パブリック IP アドレスはそのインスタンスに関連付けられます。インスタンスを停止してから開始すると、そのパブリック IP アドレス（IPv4 および IPv6）

は自動的に変更されます。この問題を解決するには、Elastic IP アドレッシングを使用して、永続的なパブリック IP アドレスをそのインスタンスに割り当てます。Elastic IP は、Threat Defense Virtual および他のインスタンスへのリモート アクセスに使用されるパブリック IP 用に予約されます。

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

**ステップ 1** [サービス（Services）] > [EC2] の順にクリックします。
**ステップ 2** [EC2ダッシュボード（EC2 Dashboard）] > [Elastic IP（Elastic IPs）] の順にクリックします。
**ステップ 3** [新規アドレスの割り当て（Allocate New Address）] をクリックします。
**ステップ 4** 必要な数の Elastic IP およびパブリック IP について、この手順を繰り返します。
**ステップ 5** [はい、割り当てます（Yes, Allocate）] をクリックして、Elastic IP を作成します。
**ステップ 6** 展開に必要な数の Elastic IP について、この手順を繰り返します。

### 次のタスク

次のセクションで説明されているように、Threat Defense Virtual を展開します。

# Threat Defense Virtual の導入

### 始める前に

次のことを推奨します。

- AWS 環境の設定 （78 ページ）の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Threat Defense Virtual インスタンスで使用できることを確認します。

**ステップ 1** https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。
**ステップ 2** Amazon マーケットプレイスにログイン後、Threat Defense Virtual（Cisco Firepower NGFW Virtual（NGFWv）： BYOL）用に提供されているリンクをクリックします。

（注） すでに AWS を使用していた場合、リンクを有効にするには、いったんサインアウトしてから、サインインし直す必要があります。

**ステップ 3** [続行（Continue）] をクリックしてから、[手動起動（Manual Launch）] タブをクリックします。
**ステップ 4** [条件に同意する（Accept Terms）] をクリックします。

**ステップ 5** [EC2コンソールを使用して起動する（Launch with EC2 Console）] をクリックします。

**ステップ 6** Threat Defense Virtual でサポートされる [インスタンスタイプ（Instance Type）] を選択します。推奨タイプは c4.xlarge です。

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

- 前に作成した VPC に一致するように [ネットワーク（Network）] を変更します。
- 前に作成した管理サブネットに一致するように [サブネット（Subnet）] を変更します。IP アドレスを指定するか、または自動生成を使用できます。
- [パブリック IP（Public IP）]（IPv4 および IPv6）の [自動生成（Auto-generate）] を有効にすることができます。
- IPv6 だけを使用して、仮想ネットワーク、サブネット、インターフェースなどを構築することはできません。デフォルトでは IPv4 が使用され、IPv6 も一緒に有効にできます。IPv6 移行の詳細については、「AWS IPv6 の概要」と「AWS VPC」を参照してください。
- [ネットワーク インターフェイス（Network Interfaces）] の下にある [デバイスの追加（Add Device）] ボタンをクリックして、eth1 ネットワーク インターフェイスを追加します。
- eth0 に使用される、事前に作成した管理サブネットに一致するように、[サブネット（Subnet）] を変更します。

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

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

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

Management Center を使用して Threat Defense Virtual を管理するためのサンプルログイン設定：

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "IPv6Mode": "dhcp",
            "ManageLocally": "No",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>"
}
```

Device Manager を使用して Threat Defense Virtual を管理するためのサンプルログイン設定：

```
#Sensor
```

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

**ステップ 8** [次：ストレージの追加（Next: Add Storage）] をクリックします。

デフォルト値で続行できます。

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

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

**ステップ 10** [次：セキュリティ グループの設定（Next: Configure Security Group）] を選択します。

**ステップ 11** [既存のセキュリティグループを選択する（Select an existing Security Group）] をクリックして、以前に設定されたセキュリティ グループを選択するか、または新しいセキュリティ グループを作成できます。セキュリティ グループの作成の詳細については、AWS の資料を参照してください。

**ステップ 12** [確認して起動する（Review and Launch）] をクリックします。

**ステップ 13** [起動（Launch）] をクリックします。

**ステップ 14** 既存のキー ペアを選択するか、新しいキー ペアを作成します。

（注） 既存のキー ペアを選択することも、新しいキー ペアを作成することもできます。キー ペアは、AWS が保存する公開キーと、ユーザーが保存する秘密キー ファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キー ペアはインスタンスへの接続に必要となる場合があるため、必ず既知の場所に保存してください。

**ステップ 15** [インスタンスの起動（Launch Instances）] をクリックします。

**ステップ 16** [起動の表示（View Launch）] をクリックし、プロンプトに従います。

**ステップ 17** [EC2ダッシュボード（EC2 Dashboard）] > [ネットワーク インターフェイス（Network Interfaces）] の順にクリックします。

**ステップ 18** AWS 環境の設定 （78 ページ）で以前に作成したインターフェイス トラフィックを特定し、[接続（Attach）] をクリックします。これは、Threat Defense Virtual インスタンス上の **eth2** インターフェイスになります。

**ステップ 19** AWS 環境の設定 （78 ページ）で以前に作成したインターフェイス トラフィックを特定し、[接続（Attach）] をクリックします。これは、Threat Defense Virtual インスタンス上の **eth3** インターフェイスになります。

（注） 4 つのインターフェイスを設定する必要があります。設定しないと、Threat Defense Virtual の起動プロセスが完了しません。

**ステップ 20** [EC2ダッシュボード（EC2 Dashboard）] > [インスタンス（Instances）] の順にクリックします。

**ステップ 21** インスタンスを右クリックし、[インスタンスの設定（Instance Settings）] > [システムログの取得（Get System Log）] の順に選択して、ステータスを表示します。

（注） 接続の問題に関する警告が表示される可能性があります。これが予想されるのは、EULA が完了するまで eth0 インターフェイスがアクティブにならないためです。

**ステップ 22** 20 分後、Threat Defense Virtual を Management Center に登録します。

### 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、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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 Device Manager を使用して Threat Defense Virtual を管理します。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理（455 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

# イメージスナップショットを使用した Threat Defense Virtual

AWS ポータルで Amazon Machine Image（AMI）スナップショットを使用して Threat Defense Virtual を作成および展開できます。イメージスナップショットは、状態データのない、複製された Threat Defense Virtual イメージインスタンスです。

## Threat Defense Virtualスナップショットの概要

Threat Defense Virtual インスタンスのスナップショットイメージを作成するプロセスは、Threat Defense Virtual および FSIC に対して実行される最初のブート手順をスキップすることにより、初期システムの初期化時間を最小限に抑えるのに役立ちます。スナップショットイメージは、事前に入力されたデータベースと Threat Defense Virtual 初期ブートプロセスで構成されます。これにより、イメージは Management Center またはその他の管理センターのシステム ID に関連する一意の ID（UUID、シリアル番号）を再生成できます。このプロセスは、自動スケール展開に不可欠な Threat Defense Virtual の起動時間を短縮するのに役立ちます。

# Threat Defense Virtual スナップショット AMI の作成

Threat Defense Virtual のイメージスナップショットの作成は、既存の Threat Defense Virtual イメージを複製して、Azure ポータルで Threat Defense Virtual のプレーンインスタンスを作成するプロセスです。

### 始める前に

- Threat Defense Virtual バージョン 7.2 以降を展開している必要があります。Threat Defense Virtual の展開については、「AWS での Threat Defense Virtual の展開 （69 ページ）」を参照してください。
- イメージスナップショットの準備をしている Threat Defense Virtual インスタンスを Management Center Virtual や Device Manager などのマネージャに登録しないでください。

**ステップ 1** Threat Defense Virtual インスタンスを展開した AWS コンソールに移動します。

（注） イメージスナップショットとして複製する予定の Threat Defense Virtual インスタンスが Management Center に登録されていないこと、または他のローカルマネージャに設定されたり設定が適用されたりしていないことを確認します。

**ステップ 2** 次のスクリプトを使用して、エキスパートシェルからプレスナップショット プロセスを実行します。

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

スクリプトで `prepare_snapshot` コマンドを使用すると、スクリプトの実行の確認を求める中間メッセージが表示されます。スクリプトを実行するには、[Y] を押します。

または、`root@firepower:/ngfw/var/common# prepare_snapshot -f` のように、このコマンドに `-f` を追加して、ユーザーの確認メッセージをスキップしてスクリプトを直接実行することもできます。

このスクリプトは、Threat Defense Virtual インスタンスに関連付けられたすべての回線設定、展開されたポリシー、設定されたマネージャ、UUID を削除します。処理が完了すると、Threat Defense Virtual インスタンスはシャットダウンされます。Threat Defense Virtual インスタンスは、AWS ポータルの [インスタンス（Instances）] ページに一覧表示されます。

**ステップ 3** http://aws.amazon.com/ にログインし、地域を選択します。

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

### 次のタスク

スナップショット AMI を使用して Threat Defense Virtual インスタンスを展開します。参照 スナップショット AMI を使用した Threat Defense Virtual インスタンスの展開 （89 ページ）

（注） Threat Defense Virtual コンソールから CLI コマンド **show version** および **show snapshot detail** を実行すると、作成した Threat Defense Virtual のイメージスナップショットのバージョンと詳細を確認できます。

# スナップショット AMI を使用した Threat Defense Virtual インスタンスの展開

### 始める前に

次のことを推奨します。

- AWS 環境の設定 （78 ページ）の説明に従って、AWS VPC および EC2 のエレメントを設定します。
- AMI が Threat Defense Virtual インスタンスで使用できることを確認します。

**ステップ 1** https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

**ステップ 2** **[EC2ダッシュボード（EC2 Dashboard）] > [インスタンス（Instances）]**の順にクリックします。イメージのスナップショットを作成するために展開した Threat Defense Virtual インスタンスが [インスタンス（Instances）] ページに表示されます。

（注） イメージのスナップショットを作成するには、操作ステータス（[インスタンス状態（Instance Status）]）が [停止（Stopped）] の Threat Defense Virtual インスタンスを常に選択する必要があります。

**ステップ 3** [インスタンス（Instances）] ページで、対応する [インスタンス状態（Instance Status）] が [停止（Stopped）] と示されている Threat Defense Virtual インスタンスを特定して選択します。

**ステップ 4** [アクション（Actions）] ドロップダウンメニューから、[イメージとテンプレート（Image and templates）] をポイントし、[イメージの作成（Create Image）] をクリックします。

**ステップ 5** [イメージの作成（Create Image）] ページで、イメージのスナップショットの名前と説明を入力します。

**ステップ 6** [再起動なし（No reboot）] セクションの下にある [有効化（Enable）] チェックボックスをオンにします。

**ステップ 7** [Create Image] をクリックします。Threat Defense Virtual のイメージスナップショット AMI が作成されます。

**ステップ 8** **[イメージ（Images）] > [AMI（AMIs）]**の順にクリックします。このページでは、新しく作成したイメージのスナップショット AMI を表示できます。

**ステップ 9** イメージスナップショット AMI を選択します。

**ステップ 10** [起動（Launch）] をクリックして、イメージスナップショット AMI を使用して新しい Threat Defense Virtual インスタンスを展開します。

**ステップ 11** Threat Defense Virtual インスタンスの展開を続行します。Threat Defense Virtual の導入 （84 ページ）またはAWS での Threat Defense Virtual Auto Scale ソリューションについて （114 ページ）を参照してください。

# Amazon GuardDuty サービスと Threat Defense Virtual の統合

Amazon GuardDuty は AWS 環境において、VPC ログ、CloudTrail 管理イベントログ、CloudTrail S3 データイベントログ、DNS ログといったさまざまなソースからのデータを処理して、不正の可能性がある悪意のあるアクティビティを特定する監視サービスです。

## 概要

シスコでは、管理センターとデバイスマネージャを介して Amazon GuardDuty サービスと Secure Firewall Threat Defense Virtual を統合するソリューションを提供しています。

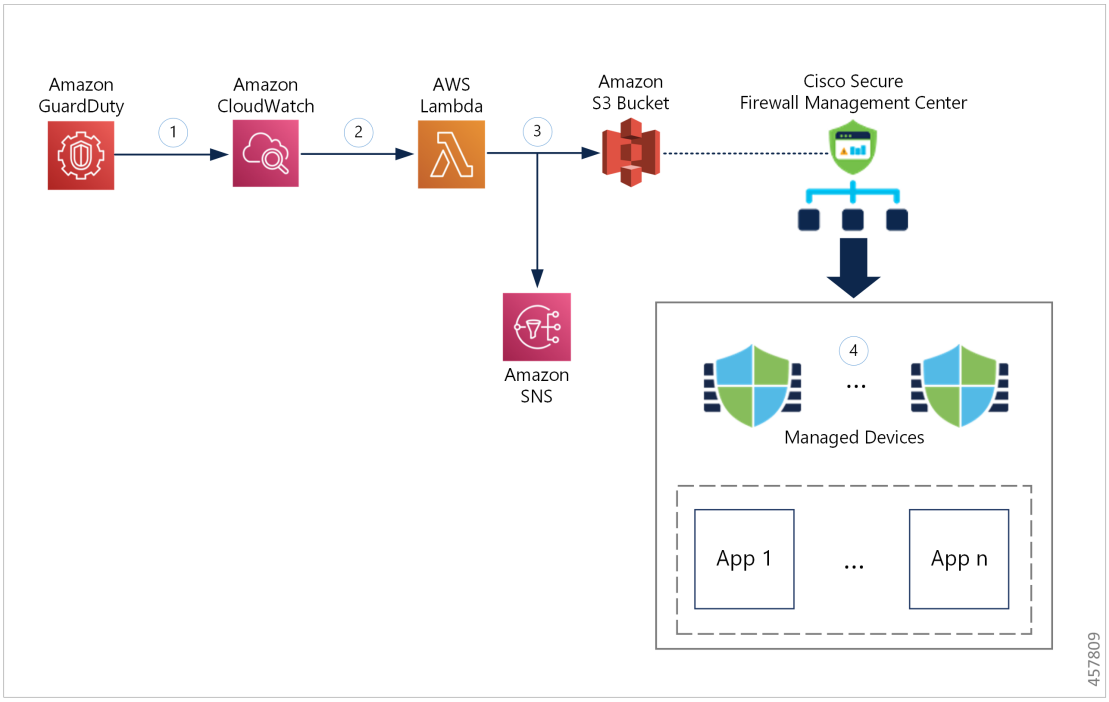
このソリューションでは、Amazon GuardDuty から受け取った脅威分析データや検出結果（脅威、攻撃などを生成する悪意のある IP）を使用して、その情報（悪意のある IP）をマネージャ（Secure Firewall Management Center Virtual および Secure Firewall デバイスマネージャ）経由で Secure Firewall Threat Defense Virtual にフィードし、これらのソース（悪意のある IP）が発生源となる将来の脅威から基盤となるネットワークやアプリケーションを保護します。

## エンドツーエンドの手順

次の統合ソリューションとワークフローの図は、Amazon GuardDuty の Secure Firewall Threat Defense Virtual との統合を理解するのに役立ちます。

### セキュリティ インテリジェンス ネットワーク フィードを使用した Secure Firewall Management Center Virtual との統合

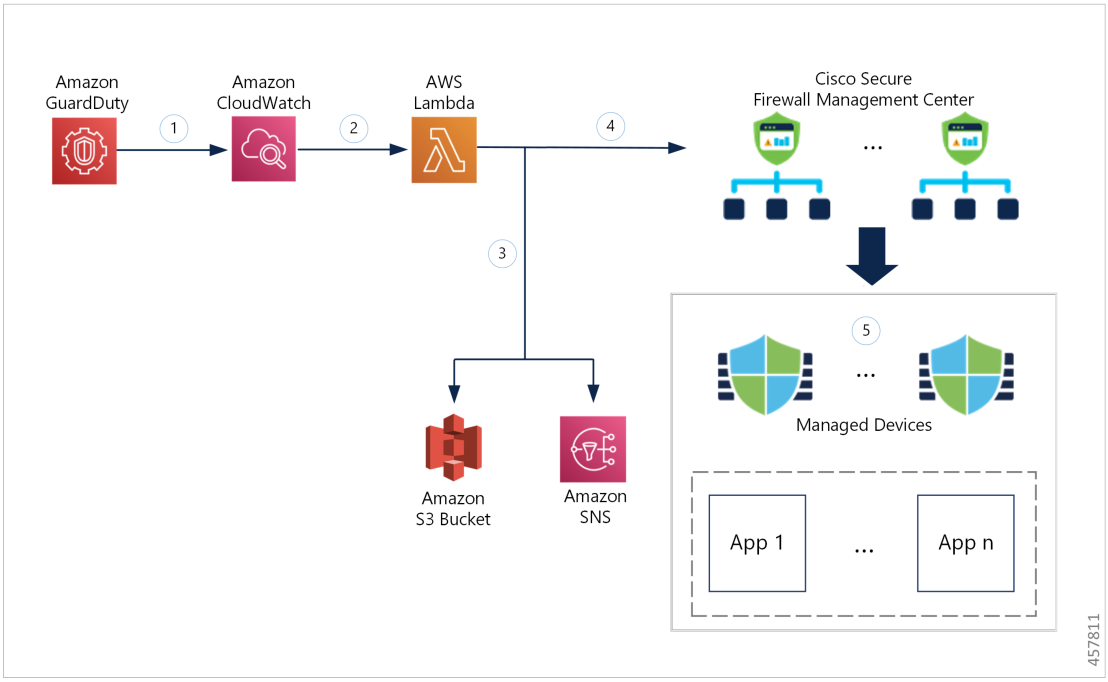
次のワークフロー図は、セキュリティ インテリジェンス ネットワーク フィード URL を使用した Secure Firewall Management Center Virtual と Amazon GuardDuty の統合ソリューションを示しています。




| | |
|---|---|
| 1 | GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。 |
| 2 | CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。 |
| 3 | Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。 |
| 4 | Secure Firewall Management Center のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。<br>このアクセスポリシーでは、セキュリティインテリジェンス ネットワーク フィードが、Lambda 関数によって提供された悪意のある IP アドレスレポートファイルの S3 オブジェクト URL と共に使用されます。 |

## ネットワーク オブジェクト グループを使用した Secure Firewall Management Center Virtual との統合

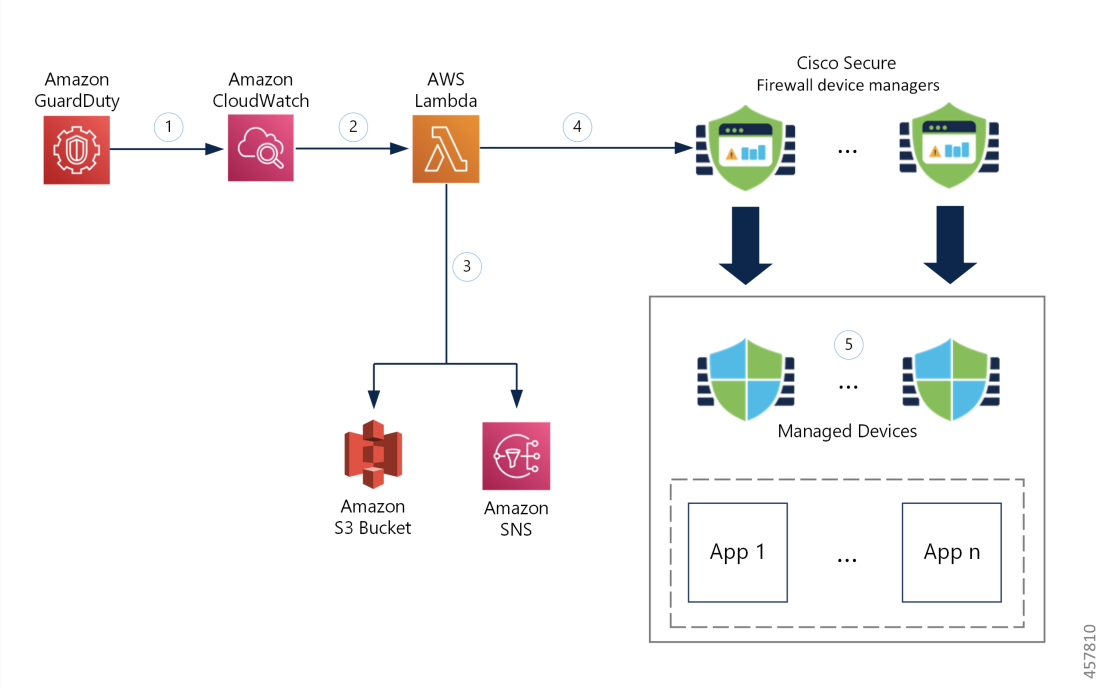
次のワークフロー図は、ネットワーク オブジェクト グループを使用した Secure Firewall Management Center Virtual と Amazon GuardDuty の統合ソリューションを示しています。




| | |
|---|---|
| 1 | GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。 |
| 2 | CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。 |
| 3 | Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。 |
| 4 | Lambda 関数は、悪意のあるホスト IP アドレスを追加して Secure Firewall Management Center Virtual のネットワーク オブジェクト グループを設定または更新します。 |
| 5 | Secure Firewall Management Center のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。<br>このアクセス コントロール ポリシーは、Lambda 関数によって検出された悪意のある IP アドレスが追加されたネットワーク オブジェクト グループを使用します。 |

## ネットワーク オブジェクト グループを使用した Secure Firewall Device Manager との統合

次のワークフロー図は、ネットワーク オブジェクト グループを使用した Secure Firewall Device Manager と Amazon GuardDuty の統合ソリューションを示しています。




| | |
|---|---|
| 1 | GuardDuty サービスは、悪意のあるアクティビティを検出すると、脅威の検出結果を CloudWatch に送信します。 |
| 2 | CloudWatch イベントにより、AWS Lambda 関数がアクティブ化されます。 |
| 3 | Lambda 関数は、S3 バケットのレポートファイル内に記載された悪意のあるホストを更新し、SNS 経由で通知を送信します。 |
| 4 | Lambda 関数は、悪意のあるホスト IP アドレスを追加して Secure Firewall Device Manager のネットワーク オブジェクト グループを設定または更新します。 |
| 5 | Secure Firewall Device Manager のアクセス コントロール ポリシーは、設定されたアクションに基づいてトラフィックを処理するように管理対象デバイスに指示します。たとえば、GuardDuty によって報告された悪意のあるホストからのトラフィックをブロックします。<br>このアクセス コントロール ポリシーは、Lambda 関数によって検出された悪意のある IP アドレスが追加されたネットワーク オブジェクト グループを使用します。 |

# この統合の主要コンポーネント

| コンポーネント | 説明 |
|---|---|
| **Amazon GuardDuty** | 特定のリージョン（EC2、S3、IAM など）のさまざまな AWS リソースについて、脅威検出結果の生成を行う Amazon サービス。 |

| | |
|---|---|
| **Amazon Simple Storage Service（S3）** | ソリューションに関連するさまざまなアーティファクトを保存するために使用される Amazon サービスは以下のとおりです。<br>• Lambda 関数の zip ファイル<br>• Lambda レイヤの zip ファイル<br>• Cisco Secure Firewall Management Center Secure Firewall と Device Manager 構成の入力ファイル（.ini）<br>• Lambda 関数によって報告された悪意のある IP アドレスのリストが保存された出力レポートファイル（.txt） |
| **Amazon CloudWatch** | Amazon サービスは次の目的で使用されます。<br>• GuardDuty サービスで報告された検出結果についてモニタリングし、Lambda 関数をトリガーして検出結果を処理します。<br>• CloudWatch ロググループで Lambda 関数に関連するアクティビティをロギングします。 |
| **Amazon Simple Notification Service（SNS）** | 電子メール通知をプッシュするために使用される Amazon サービスです。この電子メール通知には、次の内容が含まれます。<br>• Lambda 関数によって正常に処理された GuardDuty 検出結果の詳細。<br>• Lambda 関数によって Cisco Secure Firewall Manager で実行された更新の詳細。<br>• Lambda 関数によって発生した重大なエラー。 |
| **AWS Lambda 関数** | AWS サーバーレス コンピューティング サービスはイベントに応じてコードを実行し、基盤となるコンピューティングリソースを自動的に管理します。CloudWatch イベントルールが GuardDuty の検出結果に基づいて Lambda 関数をトリガーします。Lambda 関数はこの連携で以下を実行します。<br>• GuardDuty の検出結果を処理して、重大度、接続方向、悪意のある IP アドレスの存在など、必要なすべての基準が満たされていることを確認します。<br>•（設定に応じて）悪意のある IP アドレスを追加して、Cisco Secure Firewall Manager のネットワーク オブジェクト グループを更新します。<br>• S3 バケットのレポートファイルで悪意のある IP アドレスを更新します。<br>• Cisco Secure Firewall の管理者に対して、さまざまなマネージャの更新やエラーについて通知します。 |

| | |
|---|---|
| **CloudFormation テンプレート** | AWS での連携に必要なさまざまなリソースを展開するために使用されます。<br><br>CloudFormation テンプレートには、次のリソースが含まれています。<br><br>• **AWS::SNS::Topic**：電子メール通知をプッシュするための SNS トピック。<br><br>• **AWS::Lambda::Function, AWS::Lambda::LayerVersion**：Lambda 関数とレイヤファイル。<br><br>• **AWS::Events::Rule**：GuardDuty の検出結果イベントに基づいて Lambda 関数をトリガーする CloudWatch イベントルール。<br><br>• **AWS::Lambda::Permission**：Lambda 関数をトリガーする CloudWatch イベントルールのアクセス許可。<br><br>• **AWS::IAM::Role、AWS::IAM::Policy**：各種 AWS リソースの Lambda 関数へのさまざまなアクセス許可を付与する IAM ロールとポリシーリソース。<br><br>このテンプレートは、展開をカスタマイズするためのユーザー入力を取り込みます。 |

# サポートされるソフトウェア プラットフォーム

- GuardDuty 統合ソリューションは、Secure Firewall Management Center Virtual または Secure Firewall Device Manager によって管理される Secure Firewall Threat Defense Virtual に適用できます。
- Lambda 関数は、管理センターのネットワーク オブジェクト グループと、任意の仮想プラットフォームに展開されたデバイスマネージャを更新できます。Lambda 関数がパブリック IP アドレスを介してこれらのマネージャに接続できることを確認してください。

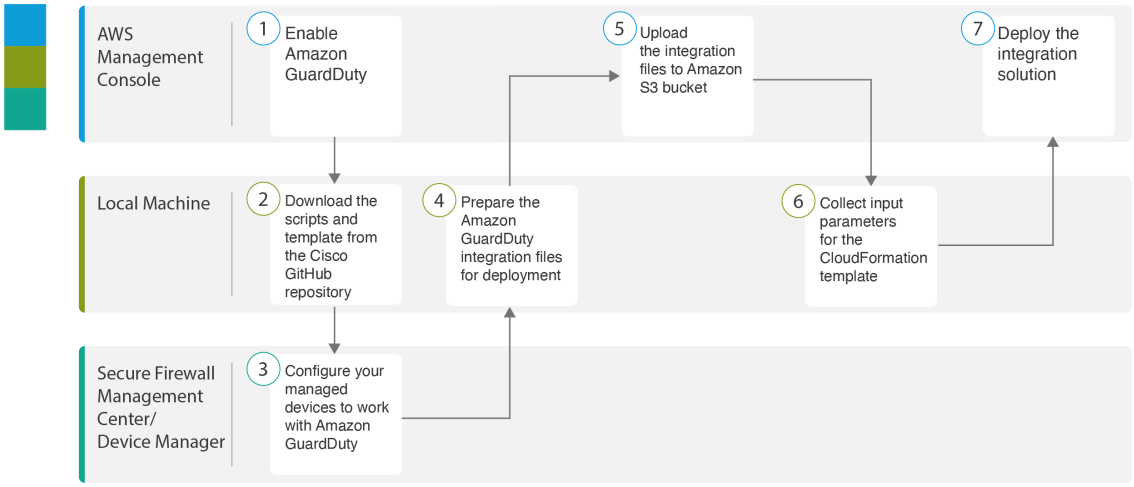
# 注意事項と制約事項

- Lambda 関数は、悪意のある IP アドレスを追加した Cisco Secure Firewall マネージャのネットワーク オブジェクト グループの更新のみを実行します。したがって、これらの更新または変更を管理対象デバイスに展開する必要があります。
- この統合で使用される AWS のサービスはリージョン固有です。したがって、異なるリージョンの GuardDuty 検出結果を使用する場合は、リージョン固有のインスタンスを展開する必要があります。
- Lambda 関数は、REST API を介して Cisco Secure Firewall マネージャを更新します。したがって、他の方法やマネージャ（Cisco Defense Orchestrator など）を使用することはできません。

- パスワードベースのログインのみを使用できます。他の認証方式はサポートされていません。
- 入力ファイルで暗号化されたパスワードを使用している場合は、次の点に注意してください。
  - 対称 KMS キーを使用した暗号化のみがサポートされます。
  - すべてのパスワードは、Lambda 関数にアクセス可能な単一の KMS キーを使用して暗号化する必要があります。

# Amazon GuardDuty と Secure Firewall Threat Defense の統合

次のタスクを実行して、Amazon GuardDuty と Secure Firewall Threat Defense を統合します。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | AWS 管理コンソール | AWS での Amazon GuardDuty サービスの有効化 （97 ページ） |
| 2 | Local Machine | Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード （97 ページ） |
| 3 | Secure Firewall Management CenterまたはSecure Firewall Device Manager | Amazon GuardDuty と連携するための管理対象デバイスの設定 （98 ページ） |
| 4 | Local Machine | 展開に向けた Amazon GuardDuty リソースファイルの準備 （101 ページ） |
| 5 | AWS 管理コンソール | Amazon Simple Storage Service へのファイルのアップロード （105 ページ） |

| | ワークスペース | 手順 |
|---|---|---|
| 6 | Local Machine | CloudFormation テンプレートの入力パラメータの収集 （105 ページ） |
| 7 | AWS 管理コンソール | スタックの展開 （108 ページ） |

# AWS での Amazon GuardDuty サービスの有効化

ここでは、AWS で Amazon GuardDuty サービスを有効にする方法について説明します。

### 始める前に

すべての AWS リソースが同じリージョンにあることを確認します。

**ステップ 1** https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

**ステップ 2** [サービス（Services）] > [GuardDuty] を選択します。

**ステップ 3** [GuardDuty] ページで [利用を開始する（Get Started）] をクリックします。

**ステップ 4** [GuardDutyの有効化（Enable GuardDuty）] をクリックして、Amazon GuardDuty サービスを有効にします。

GuardDuty の有効化の詳細については、AWS ドキュメントの『Getting started with GuardDuty』[英語] を参照してください。

### 次のタスク

Cisco GitHub リポジトリから Amazon GuardDuty ソリューションファイル（テンプレートとスクリプト）をダウンロードします。Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード （97 ページ） を参照してください。

# Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションリポジトリのダウンロード

Amazon GuardDuty ソリューションに必要なファイルをダウンロードします。Secure Firewall Threat Defense Virtual の該当するバージョン用の導入スクリプトとテンプレートは、次の Cisco GitHub リポジトリから入手できます。

https://github.com/CiscoDevNet/cisco-ftdv

以下は、Cisco GitHub リポジトリリソースのリストです。

| ファイル | 説明 |
|---|---|
| READ.MD | ReadMe ファイル |

| ファイル | 説明 |
|---|---|
| configuration/ | Secure Firewall Threat Defense Virtual マネージャの構成ファイルテンプレート。 |
| images/ | Secure Firewall Threat Defense Virtual および Amazon GuardDuty 統合ソリューションの図が格納されています。 |
| lambda/ | Lambda 関数の Python ファイル。 |
| templates/ | 導入用の CloudFormation テンプレート |

# Amazon GuardDuty と連携するための管理対象デバイスの設定

Lambda 関数は Amazon GuardDuty の検出結果を処理し、CloudWatch イベントをトリガーした悪意のある IP アドレスを特定します。Secure Firewall Threat Defense Virtual は 次のいずれかの方法で Secure Firewall Management Center Virtual および Secure Firewall Device Manager を介してこの脅威データを受信します。

- **ネットワーク オブジェクト グループの更新**：Lambda 関数は、悪意のある IP アドレスを追加してマネージャのネットワーク オブジェクト グループを更新します。次に、このネットワーク オブジェクト グループを使用してトラフィックを処理するアクセス コントロール ポリシーを設定できます。この方法は Secure Firewall Management Center Virtual と Secure Firewall Device Manager が対象です。
- **セキュリティ インテリジェンス ネットワーク フィード**：Lambda 関数は、悪意のある IP アドレスを追加して Amazon S3 バケット内のレポートファイルを作成または更新します。レポートファイルの URL を使用してセキュリティ インテリジェンス フィードを設定し、このフィードを使用してトラフィックを処理するアクセス コントロール ポリシーを設定できます。この方法は Secure Firewall Management Center Virtual のみが対象です。

## レポートファイルの URL を使用したセキュリティ インテリジェンス ネットワーク フィードの設定

ここでは、Secure Firewall Management Center Virtual でセキュリティ インテリジェンス ネットワーク フィードを設定する方法について説明します。

### 始める前に

- Secure Firewall Management Center Virtual で脅威ライセンスが有効になっていることを確認します。「脅威ライセンス」を参照してください。
- Amazon S3 バケットで使用可能なレポートファイルの URL を作成して書き留めておきます。
- Secure Firewall Management Center Virtual から Amazon S3 バケット内のレポートファイルにアクセスできることを確認します。

**ステップ 1** Secure Firewall Management Center Virtual にログインします。

**ステップ 2** Amazon S3 バケットのレポートファイル URL を使用して、セキュリティ インテリジェンス ネットワーク フィードを作成します。セキュリティ インテリジェンス ネットワーク フィードを手動で作成する方法については、「カスタム セキュリティ インテリジェンス フィード」を参照してください。

**ステップ 3** トラフィックを処理するセキュリティ インテリジェンス ネットワーク フィード URL を使用して、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「手動 URL フィルタリング オプション」および「アクセス コントロール ルールの作成と編集」を参照してください。

（注） 展開の前または後に、セキュリティ インテリジェンス ネットワーク フィードを作成し、アクセス コントロール ポリシーの URL を更新できます。Amazon S3 バケットに出力レポートファイルを作成している場合は、展開前にセキュリティ インテリジェンス ネットワーク フィードを作成できます。展開後にセキュリティ インテリジェンス ネットワーク フィードを作成している場合は、Amazon GuardDuty から最初の検出結果の電子メール通知を受信するまで待ち、その電子メール通知で指定された URL を使用してセキュリティ インテリジェンス ネットワーク フィードを設定します。

**ステップ 4** Secure Firewall Management Center Virtual に設定の変更を展開します。「設定変更の展開」を参照してください。

### 次のタスク

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （101 ページ） を参照してください。

## ネットワーク オブジェクト グループの作成

Secure Firewall Management Center Virtual および Secure Firewall デバイスマネージャ で Lambda 関数のネットワーク オブジェクト グループを設定または作成して、Amazon GuardDuty によって検出された悪意のある IP アドレスを更新する必要があります。

Lambda 関数でネットワーク オブジェクト グループを設定しない場合、デフォルト名 **aws-gd-suspicious-hosts** のネットワーク オブジェクト グループが Lambda 関数によって作成され、悪意のある IP アドレスが更新されます。

### Secure Firewall Management Center Virtual でのネットワーク オブジェクト グループの作成

ここでは、Secure Firewall Management Center Virtual でネットワーク オブジェクト グループを作成する方法について説明します。

**ステップ 1** Secure Firewall Management Center Virtual にログインします。

**ステップ 2** ダミーの IP アドレスを使用してネットワーク オブジェクト グループを作成します。「ネットワークオブジェクト」を参照してください。

**ステップ 3** ネットワーク オブジェクト グループを使用してトラフィックを処理するためのアクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「アクセス コントロール ポリシーの管理」および「アクセス コントロール ルールの作成および編集」を参照してください。

ヒント　Lambda 関数が悪意のある IP アドレスを追加してネットワーク オブジェクト グループを更新していることを確認した後に、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新することもできます。

**ステップ 4** 設定変更を管理対象デバイスに展開します。「設定変更の展開」を参照してください。

---

**次のタスク**

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （101 ページ） を参照してください。

### Secure Firewall Device Manager のネットワーク オブジェクト グループの作成

ここでは、Secure Firewall デバイスマネージャ でネットワーク オブジェクト グループを作成する方法について説明します。

---

**ステップ 1** Secure Firewall Device Manager にログインします。

**ステップ 2** ダミーの IP アドレスを使用してネットワーク オブジェクト グループを作成します。「ネットワークオブジェクトとグループの設定」を参照してください。

**ステップ 3** ネットワーク オブジェクト グループを使用してトラフィックを処理するためのアクセス コントロール ポリシーやアクセス制御ルールを作成または更新します。「アクセス コントロール ポリシーの設定」および「アクセス制御ルールの設定」を参照してください。

ヒント　Lambda 関数が悪意のある IP アドレスを追加してネットワーク オブジェクト グループを更新していることを確認した後に、アクセス コントロール ポリシーやアクセス制御ルールを作成または更新することもできます。

**ステップ 4** 設定変更を管理対象デバイスに展開します。「変更の展開」を参照してください。

---

**次のタスク**

展開に向けて Amazon GuardDuty ソースファイルを準備します。展開に向けた Amazon GuardDuty リソースファイルの準備 （101 ページ） を参照してください。

## Secure Firewall Management Center Virtual で Lambda 関数を利用するためのユーザーアカウントの作成

Lambda 関数には、管理センターとデバイスマネージャでネットワーク オブジェクト グループを更新するための管理者権限を持つユーザーアカウントが必要です。したがって、管理センターとデバイスマネージャで管理者権限を持つ排他的なユーザーアカウントを作成する必要が

あります。ユーザーアカウントの作成は、ネットワーク オブジェクト グループの更新メソッドを使用する場合にのみ必要です。

ユーザーアカウントの作成の詳細については、以下を参照してください。

- FDM および FTD ユーザ アクセスの管理
- FMC のユーザーアカウント

## （任意）パスワードの暗号化

必要に応じて、入力構成ファイルに暗号化されたパスワードを指定できます。プレーンテキスト形式でパスワードを指定することもできます。

Lambda関数にアクセスできる単一のKMSキーを使用して、すべてのパスワードを暗号化します。**aws kms encrypt --key-id** <*KMS-ARN*> **--plaintext** <*password*> コマンドを使用して暗号化されたパスワードを生成します。このコマンドを実行するには、AWS CLI をインストールして設定する必要があります。

（注） パスワードが対称 KMS キーを使用して暗号化されていることを確認します。

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

例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext <password>
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

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

# 展開に向けた Amazon GuardDuty リソースファイルの準備

Amazon GuardDuty ソリューションの展開リソースファイルは、Cisco GitHub リポジトリで入手できます。

AWS に Amazon GuardDuty ソリューションを展開する前に、次のファイルを準備する必要があります。

- Secure Firewall Threat Defense Virtual マネージャの構成入力ファイル
- Lambda 関数の zip ファイル

- Lambda レイヤの zip ファイル

## 構成入力ファイルの準備

構成テンプレートでは、Amazon GuardDuty ソリューションと連携する管理センターまたはデバイスマネージャの詳細を定義する必要があります。ネットワーク オブジェクト グループの更新メソッドで管理センターやデバイスマネージャと Amazon GuardDuty の統合を計画している場合にのみ、構成ファイルを更新することを推奨します。

### 始める前に

- 構成ファイルにユーザーアカウントの詳細を指定する前に、デバイスマネージャのユーザーアカウントを認証および検証します。
- 構成ファイルで複数の管理センターやデバイスマネージャを設定している場合は、各管理センターやデバイスマネージャのパラメータが構成ファイルに1つだけ入力され、重複するエントリがないことを確認します。
- 管理センターとデバイスマネージャの IP アドレスと名前を書き留めておく必要があります。
- 管理センターとデバイスマネージャでこれらのネットワーク オブジェクト グループにアクセスして更新するには、Lambda 関数の管理者権限を持つユーザーアカウントを作成しておく必要があります。

**ステップ 1** Amazon GuardDuty リソースファイルをダウンロードしたローカルマシンにログインします。

**ステップ 2** **ngfwv-template > configuration** フォルダを参照します。

**ステップ 3** テキストエディタツールで `ngfwv-manager-config-input.ini` ファイルを開きます。

このファイルには、Amazon GuardDuty ソリューションの統合と展開を計画している管理センターまたはデバイスマネージャの詳細を入力する必要があります。

**ステップ 4** 各パラメータに対応する管理センターまたはデバイスマネージャに関する以下の詳細を入力します。

| パラメータ | 説明 |
|---|---|
| [ngfwv-1] | セクション名：管理センターまたはデバイスマネージャの一意の識別子。 |
| public-ip | 管理センターまたはデバイスマネージャの IP アドレス。 |
| device-type | 管理センターまたはデバイスマネージャを介して Amazon GuardDuty ソリューションを展開する管理対象デバイスのタイプ。使用できる値は FMC または FDM です。 |

| パラメータ | 説明 |
|---|---|
| ユーザー名 | 管理センターまたはデバイスマネージャにログインするためのユーザー名。 |
| パスワード | 管理センターまたはデバイスマネージャにログインするためのパスワード。パスワードには、プレーンテキスト形式または KMS を使用して暗号化された文字列を使用できます。 |
| object-group-name | Lambda 関数が悪意のあるホスト IP を追加して更新するネットワーク オブジェクト グループの名前。複数のネットワーク オブジェクト グループ名を入力する場合は、カンマ区切り値になっていることを確認してください。 |

**ステップ 5** `ngfwv-manager-config-input.ini` ファイルを保存して閉じます。

### 次のタスク

Lambda 関数のアーカイブファイルを作成します。Lambda 関数のアーカイブファイルの準備（103 ページ） を参照してください。

## Lambda 関数のアーカイブファイルの準備

ここでは、Linux 環境で Lambda 関数ファイルをアーカイブする方法について説明します。

（注） アーカイブプロセスは、ファイルのアーカイブを実行するローカルマシンのオペレーティングシステムによって異なる場合があります。

**ステップ 1** Amazon GuardDuty リソースをダウンロードしたローカルマシンで CLI コンソールを開きます。

**ステップ 2** `/lambda` フォルダに移動し、ファイルをアーカイブします。

以下は、Linux ホストからのサンプルトランスクリプトです。

```
$ cd lambda
$ zip ngfwv-gd-lambda.zip *.py
adding: aws.py (deflated 71%) adding: fdm.py (deflated 79%)
adding: fmcv.py (deflated 79%)
adding: main.py (deflated 73%)
adding: utils.py (deflated 65%)
$
```

zip ファイル `ngfwv-gd-lambda.zip` が作成されます。

**ステップ 3** 終了して CLI コンソールを閉じます。

### 次のタスク

zip ファイル `ngfwv-gd-lambda.zip` を使用して、Lambda レイヤの zip ファイルを作成します。Lambda レイヤファイルの準備 （104 ページ）を参照してください

## Lambda レイヤファイルの準備

ここでは、Linux 環境で Lambda レイヤファイルをアーカイブする方法について説明します。

（注） アーカイブプロセスは、ファイルのアーカイブを実行するローカルマシンのオペレーティングシステムによって異なる場合があります。

**ステップ 1** Amazon GuardDuty リソースをダウンロードしたローカルマシンで CLI コンソールを開きます。

**ステップ 2** CLI コンソールで次のアクションを実行します。

以下は、Python 3.9 がインストールされている Ubuntu 22.04 などの Linux ホストでのサンプルトランスクリプトです。

```
$ mkdir -p layer
$ virtualenv -p /usr/bin/python3.9 ./layer/
$ source ./layer/bin/activate
$ pip3.9 install cffi==1.15.0
$ pip3.9 install cryptography==37.0.2
$ pip3.9 install paramiko==2.7.1
$ pip3.9 install requests==2.23.0
$ mkdir -p ./python/.libs_cffi_backend/
$ cp -r ./layer/lib/python3.9/site-packages/* ./python/
$ zip -r ngfwv-gd-lambda-layer.zip ./python
```

zip ファイル `ngfwv-gd-lambda-layer.zip` が作成されます。

Lambda レイヤを作成するには、Python 3.9 とその依存関係をインストールする必要があることに注意してください。

以下は、Ubuntu 22.04 などの Linux ホストに Python 3.9 をインストールするためのサンプルトランスクリプトです。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

**ステップ 3** 終了して CLI コンソールを閉じます。

### 次のタスク

Amazon S3 バケットでは、Secure Firewall Threat Defense Virtual の構成ファイル、Lambda 関数の zip ファイル、および Lambda レイヤの zip ファイルをアップロードする必要があります。Amazon Simple Storage Service へのファイルのアップロード （105 ページ）を参照してください

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

すべての Amazon GuardDuty ソリューション アーティファクトを準備したら、AWS ポータルの Amazon Simple Storage Service（S3）バケットフォルダにファイルをアップロードする必要があります。

**ステップ 1** https://aws.amazon.com/marketplace（Amazon マーケットプレイス）に移動してサインインします。

**ステップ 2** Amazon S3 コンソールを開きます。

**ステップ 3** Amazon GuardDuty アーティファクトをアップロードするための Amazon S3 バケットを作成します。Amazon S3 の作成 [英語] を参照してください。

**ステップ 4** 次の Amazon GuardDuty アーティファクトを Amazon S3 バケットにアップロードします。

- Secure Firewall Threat Defense Virtual構成ファイル：`ngfwv-config-input.ini`

  （注） 管理センターでセキュリティ インテリジェンスのネットワーク フィード メソッドを使用して Amazon GuardDuty ソリューションを展開する場合、このファイルをアップロードする必要はありません。

- Lambda レイヤ zip ファイル：`ngfwv-gd-lambda-layer.zip`
- Lambda 関数 zip ファイル：`ngfwv-gd-lambda.zip`

### 次のタスク

Amazon GuardDuty リソースの展開に使用する CloudFormation テンプレートを準備します。CloudFormation テンプレートの入力パラメータの収集 （105 ページ） を参照してください。

# CloudFormation テンプレートの入力パラメータの収集

シスコでは、AWS の Amazon GuardDuty ソリューションに必要なリソースを展開する際に使用する CloudFormation テンプレートを提供しています。展開する前に、次のテンプレートパラメータの値を収集します。

**Template Parameters**

| パラメータ | 説明 | 例 |
|---|---|---|
| 展開名* | このパラメータに入力する名前は、Cloud Formation テンプレートによって作成されるすべてのリソースのプレフィックスとして使用されます。 | **cisco-ngfwv-gd** |
| GD 検出結果の最小の重大度レベル* | Amazon GuardDuty の検出結果で処理の対象となる最小重大度レベルは、**1.0** から **8.9** の範囲にする必要があります。報告された検出結果の重大度が最小範囲よりも低い場合は無視されます。<br>重大度の分類は次のとおりです。<br>• 低：1.0 ～ 3.9<br>中：4.0 ～ 6.9<br>高：7.0 ～ 8.9 | **4.0%** |
| 管理者の電子メール ID* | 管理センターまたはデバイスマネージャ の Lambda 関数によって実行された更新に関する通知を受信する Secure Firewall Threat Defense Virtual マネージャ の管理者の電子メールアドレス。 | **abc@xyz.com** |
| S3 バケット名* | Amazon GuardDuty アーティファクトファイル （Lambda 関数の zip ファイル、Lambda レイヤの zip ファイル、および Secure Firewall Threat Defense Virtual 設定マネージャファイル）が格納された Amazon S3 バケットの名前。 | 例：**ngfwv-gd-bucket** |
| S3 バケットフォルダ/パスプレフィックス | 構成ファイルが保存されている Amazon S3 バケットのパスまたはフォルダ名。フォルダがない場合は、このフィールドを空白のままにします。 | 例：「」または「**cisco/ngfwv-gd/**」 |
| Lambda レイヤの zip ファイル名* | Lambda レイヤの zip ファイル名。 | 例：`ngfwv-gd-lambda-layer.zip` |

| パラメータ | 説明 | 例 |
|---|---|---|
| Lambda 関数の zip ファイル名* | Lambda 関数の zip ファイル名。 | 例：`ngfwv-gd-lambda.zip` |
| Cisco Secure Firewall Management Center Secure Firewall と Device Manager マネージャの構成ファイル名 | Cisco Firewall Threat Defense Virtual のマネージャ設定の詳細が保存された ***.ini** ファイル（パブリック IP、ユーザー名、パスワード、デバイスタイプ、ネットワーク オブジェクト グループ名など）。<br>（注） このファイルは、Amazon GuardDuty との統合でネットワーク オブジェクト グループの更新メソッドを使用している場合にのみ必要です。<br>セキュリティ インテリジェンス フィード メソッドを使用している場合は、この入力をスキップできます。 | 例：`ngfwv-config-input.ini` |
| パスワードの暗号化に使用される KMS キーの ARN | 既存の KMS（パスワードの暗号化に使用される AWS KMS キー）の ARN。Secure Firewall Threat Defense Virtual の構成入力ファイルでプレーンテキスト パスワードが指定されている場合は、このパラメータを空のままにしておくことができます。指定する場合、Secure Firewall Threat Defense Virtual の構成入力ファイルに記載されているすべてのパスワードを暗号化する必要があります。パスワードの暗号化には、指定された ARN のみを使用する必要があります。暗号化パスワードの生成：aws kms encrypt --key-id <KMS ARN> --plaintext <password> | 例：**arn:aws:kms:<region>:<awsaccountid>:key/<keyid>** |
| デバッグログの有効化/無効化* | CloudWatch で Lambda 関数のデバッグログを有効または無効にします。 | 例：**enable** または **disable** |

*：必須フィールド

**次のタスク**

CloudFormation テンプレートを使用してスタックを展開します。スタックの展開 （108 ページ）を参照してください

# スタックの展開

Amazon GuardDuty ソリューションを導入するためのすべての前提条件プロセスを完了した後に、AWS CloudFormation スタックを作成します。対象ディレクトリのテンプレートファイル（`templates/cisco-ngfwv-gd-integration.yaml`）を使用し、「CloudFormation テンプレートの入力パラメータの収集」で収集したパラメータを指定します。

**ステップ 1** AWS コンソールにログインします。

**ステップ 2** [サービス（Services）] > [CloudFormation] > [スタック（Stacks）] > [スタックの作成（Create stack）]（新しいリソースを使用）> [テンプレートの準備（Prepare template）]（テンプレートはフォルダ内にあります）> [テンプレートの指定（Specify template）] > [テンプレートソース（Template source）]（ターゲットディレクトリ `templates/cisco-ngfwv-gd-integration.yaml` からテンプレートファイルをアップロード）> [スタックの作成（Create Stack）] の順に操作を行います。

AWS でスタックを展開する方法の詳細については、AWS ドキュメント [英語] を参照してください。

**次のタスク**

展開を検証します。展開の検証 （109 ページ） を参照してください。

また、Amazon GuardDuty によって報告された脅威検出の更新に関する電子メール通知を受信するように登録します。電子メール通知の登録 （108 ページ） を参照してください。

# 電子メール通知の登録

CloudFormation テンプレートでは、GuardDutyの検出結果の更新に関する通知を受信するように、電子メール ID が設定されています。これは Lambda 関数によって実行されます。AWS に CloudFormation テンプレートを展開すると、Amazon Simple Notification Service（SNS）サービスを介してこの電子メール ID に電子メール通知が送信され、通知の更新を登録するように要求されます。

**ステップ 1** 電子メール通知を開きます。

**ステップ 2** 電子メール通知で利用可能な**サブスクリプション**リンクをクリックします。

### 次のタスク

展開を検証します。展開の検証 （109 ページ） を参照してください。

# 展開の検証

この項で説明されているように、AWS には Amazon GuardDuty ソリューションを検証するオプションがあります。CloudFormation の展開が完了したら、以下に示す展開の検証手順を実行できます。

### 始める前に

展開を検証するためのコマンドを実行するには、AWS コマンド ライン インターフェイス（CLI）がインストールおよび設定されていることを確認します。AWS CLI のドキュメントについては、AWS のコマンド ライン インターフェイス [英語] を参照してください。

**ステップ 1** AWS 管理コンソールにログインします。

**ステップ 2** [サービス（Services）] > [GuardDuty] > [設定（Settings）] > [GuardDutyの概要（About GuardDuty）] > [ディテクタID（Detector ID）] に移動して、ディテクタ ID を書き留めます。

このディテクタ ID は、Amazon GuardDuty のサンプル検出結果を生成するために必要です。

**ステップ 3** AWS CLI コンソールを開き、次のコマンドを実行して Amazon GuardDuty のサンプル検出結果を生成します。

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

```
aws guardduty create-sample-findings --detector-id <detector-id> --finding-types
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
```

**ステップ 4** Amazon GuardDuty コンソールの結果リストでサンプルの検出結果を確認します。

サンプル検出結果には、プレフィックス **[sample]** が含まれています。接続方向、リモート IP アドレスなどの属性を参照して、サンプル検出結果の詳細を確認できます。

**ステップ 5** Lambda 関数が実行されるのを待ちます。

Lambda 関数がトリガーされたら、以下を確認します。

- 受信した Amazon GuardDuty の検出結果と、Lambda 関数によって実行された Secure Firewall Threat Defense Virtual マネージャ の更新に関する詳細が記載された電子メール通知。
- レポートファイルが Amazon S3 バケットに生成されているかどうかを確認します。レポートファイルには、サンプルの Amazon GuardDuty の検出結果によって報告された悪意のある IP アドレスが含まれています。レポートファイル名は、`<deployment-name>-report.txt` の形式になっています。
- ネットワーク オブジェクト グループの更新メソッドの場合：設定されたマネージャ（Secure Firewall Management Center Virtual または Secure Firewall デバイスマネージャ）で、サンプルの検出結果から更新された悪意のある IP アドレスを追加してネットワーク オブジェクト グループが更新されていることを確認します。

- セキュリティ インテリジェンス フィード メソッドの場合：レポートファイルの URL が管理センターの設定で既に更新されているかどうかを確認します。レポートファイル URL の最終更新タイムスタンプは、管理センターの次のパスで表示できます。
  - [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence ）] > [ネットワークリストとフィード（Network Lists and Feeds）] > 設定したフィードを選択
  - または、フィードを手動で更新してから、[最終更新（Last Updated）] のタイムスタンプを確認することもできます。次のパスでフィードを選択して更新できます。

    [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence ）] > [ネットワークリストとフィード（Network Lists and Feeds）] > [フィードの更新（Update Feeds）]

**ステップ 6** [AWSコンソール（AWS Console）] > [サービス（Services）] > [CloudWatch] > [ログ（Logs）] > [ロググループ（Log groups）] に移動し、ロググループを選択して、CloudWatch コンソールで Lambda ログを確認します。CloudWatch のロググループ名は、 `<deployment-name>-lambda` の形式になっています。

**ステップ 7** 展開を検証した後、次のようにサンプル検出結果によって生成されたデータをクリーンアップすることを推奨します。

a) AWS コンソールから [サービス（Services）] > [GuardDuty] > [結果（Findings）] > [結果を選択（Select the finding）] > [アクション（Actions）] > [アーカイブ（Archive）] に移動して、サンプルの検出結果データを表示します。

b) ネットワーク オブジェクト グループに追加された悪意のある IP アドレスを削除して、キャッシュされたデータを Secure Firewall Management Center Virtual から消去します。

c) Amazon S3 バケットのレポートファイルをクリーンアップします。サンプルの検出結果で報告された悪意のある IP アドレスを削除することで、ファイルを更新できます。

# 既存のソリューション展開構成の更新

展開後に S3 バケットや S3 バケットフォルダとパスプレフィックス値を更新しないことを推奨します。ただし、展開したソリューションの構成を更新する必要がある場合は、AWS コンソールの [CloudFormation] ページで [スタックの更新（Update Stack）] オプションを使用します。

以下のパラメータを更新できます。

| パラメータ | 説明 |
|---|---|
| Secure Firewall Threat Defense Virtual マネージャの構成ファイル名 | Amazon S3 バケットの構成ファイルを追加または更新します。以前のファイルと同じ名前でファイルを更新できます。構成ファイル名が変更された場合は、AWS コンソールの [ス |

| パラメータ | 説明 |
|---|---|
| | タックの更新（Update stack）]オプションを使用して、このパラメータを更新できます。 |
| GD 検出結果の最小の重大度レベル* | AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。 |
| 管理者の電子メール ID* | AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、電子メール ID のパラメータ値を更新します。SNS サービスコンソールを介して電子メールのサブスクリプションを追加または更新することもできます。 |
| S3 バケット名* | Amazon S3 バケット内の zip ファイルを新しい名前で更新してから、AWS コンソールの [スタックの更新（Update Stack）] オプションを使用してパラメータを更新します。 |
| Lambda レイヤの zip ファイル名* | Amazon S3 バケット内の Lambda レイヤ zip ファイル名を新しい名前で更新してから、AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、このパラメータ値を更新します。 |
| Lambda 関数の zip ファイル名* | Amazon S3 バケット内の Lambda 関数 zip ファイルを新しい名前で更新してから、AWS コンソールの [スタックの更新（Update stack）] オプションを使用して、このパラメータ値を更新します。 |
| パスワードの暗号化に使用される KMS キーの ARN | AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。 |
| デバッグログの有効化/無効化* | AWS コンソールの [スタックの更新（Update stack）]オプションを使用して、パラメータ値を更新します。 |

**ステップ 1** AWS 管理コンソールに進みます。

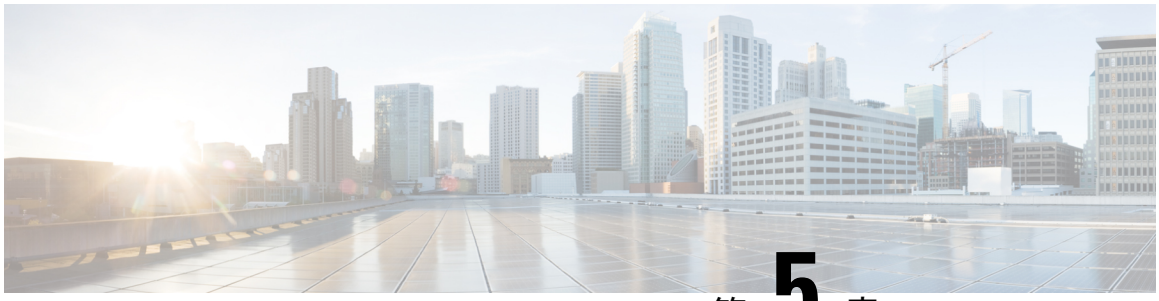
**ステップ 2** 必要に応じて、新しいバケットとフォルダを作成します。

**ステップ 3** 以下に示すアーティファクトが古いバケットから新しいバケットにコピーされていることを確認します。

- Secure Firewall Threat Defense Virtual構成ファイル：`ngfwv-config-input.ini`

- Lambda レイヤ zip ファイル：`ngfwv-gd-lambda-layer.zip`
- Lambda 関数 zip ファイル：`ngfwv-gd-lambda.zip`
- Output レポートファイル：`<deployment-name>-report.txt`

**ステップ 4** パラメータ値を更新するには、**Services > CloudFormation > Stacks > > Update (Update Stack) > Prepare template > Use current template > Next >** <*update parameters*>**> Update Stack** に移動します。



第 5 章

# AWS への Threat Defense Virtual Auto Scale ソリューションの導入

このドキュメントでは、Threat Defense Virtual Auto Scale ソリューションを AWS に展開する方法について説明します。


- AWS での Threat Defense Virtual Auto Scale ソリューションについて （114 ページ）
- NLB を使用した Auto Scale ソリューション （115 ページ）
- NLB を使用して Auto Scale ソリューションを展開するためのエンドツーエンドのプロセス （116 ページ）
- GWLB を使用した Auto Scale ソリューション （118 ページ）
- GWLB を使用して Auto Scale ソリューションを展開するためのエンドツーエンドのプロセス （119 ページ）
- Threat Defense Virtual および AWS のガイドラインと制限事項 （120 ページ）
- GWLB または NLB を使用した Auto Scale ソリューションの設定に必要なコンポーネント （122 ページ）
- GitHub の CloudFormation テンプレート （125 ページ）
- GitHub からローカルホストへの必要なファイルと CFT のダウンロード （142 ページ）
- NLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの NLB インフラストラクチャ テンプレートのカスタマイズと展開 （142 ページ）
- GWLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの GWLB インフラストラクチャ テンプレートのカスタマイズと展開 （143 ページ）
- Management Center でのネットワーク インフラストラクチャの設定 （144 ページ）
- Configuration.json ファイルの更新 （150 ページ）
- AWS CLI を使用したインフラストラクチャ コンポーネントの設定 （151 ページ）
- target フォルダの作成 （153 ページ）
- Amazon S3 バケットへのファイルのアップロード （153 ページ）
- NLB を使用した Auto Scale ソリューション：NLB を使用した Auto Scale ソリューションの展開 （153 ページ）
- GWLB を使用した Auto Scale ソリューション：GWLB を使用した Auto Scale ソリューションの展開 （154 ページ）
- VPC のルーティングの設定 （155 ページ）

• Auto Scale グループの編集 （156 ページ）
• 展開の検証 （156 ページ）
• メンテナンス タスク （157 ページ）
• トラブルシューティング （161 ページ）
• 導入例：AWS で GWLB を使用して North-South トラフィックを検査する Threat Defense Virtual の Auto Scale ソリューション （163 ページ）

# AWS での Threat Defense Virtual Auto Scale ソリューションについて

AWS などのパブリッククラウド環境に展開された Threat Defense Virtual インスタンスでは、ネットワークトラフィックでスパイクとディップが発生することがあるアプリケーションがサポートされます。トラフィックのスパイクにより、展開された Threat Defense Virtual インスタンスの数がネットワークトラフィックの検査には十分ではないシナリオが発生する可能性があります。トラフィックがディップすると、Threat Defense Virtual インスタンスがアイドル状態になり、不要な運用コストが発生する可能性があります。

Auto Scale ソリューションは、トラフィックがスパイクした場合に Threat Defense Virtual インスタンスの数を自動的にスケールアップし、トラフィックが小休止しているときにインスタンスの数をスケールダウンするのに役立つため、ネットワークリソースを効率的に処理して、運用コストを削減できます。

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

バージョン 6.4 以降、ネットワークロードバランサ（NLB）ベースの Auto Scale ソリューションは、Management Center によって管理される Threat Defense Virtual でサポートされます。バージョン 7.2 以降では、ゲートウェイロードバランサ（GWLB）ベースの Auto Scale ソリューションもサポートされています。

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

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

- Management Center による Threat Defense Virtual 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 Threat Defense Virtual インスタンスへの NAT ポリシー、アクセスコントロール 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。

- Management Center でのみ動作し、Device Manager はサポート対象外。

### Auto Scale の機能拡張（バージョン 6.7）

- カスタム指標パブリッシャ：新しい Lambda 関数は、Auto Scale グループ内のすべての Threat Defense Virtual インスタンスのメモリ消費量について Management Center を 2 分ごとにポーリングし、その値を CloudWatch メトリックに公開します。
- メモリ消費に基づく新しいスケーリングポリシーを使用できます。
- Management Center への SSH およびセキュアトンネル用の Threat Defense Virtual プライベート IP 接続。
- Management Center 設定の検証。
- ELB でより多くのリスニングポートを開くためのサポート。
- シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。

# NLB を使用した Auto Scale ソリューション

AWS ロードバランサはインバウンドで開始された接続のみを許可するため、外部で生成されたトラフィックのみが Cisco Threat Defense Virtual ファイアウォール経由で内部を通過できます。

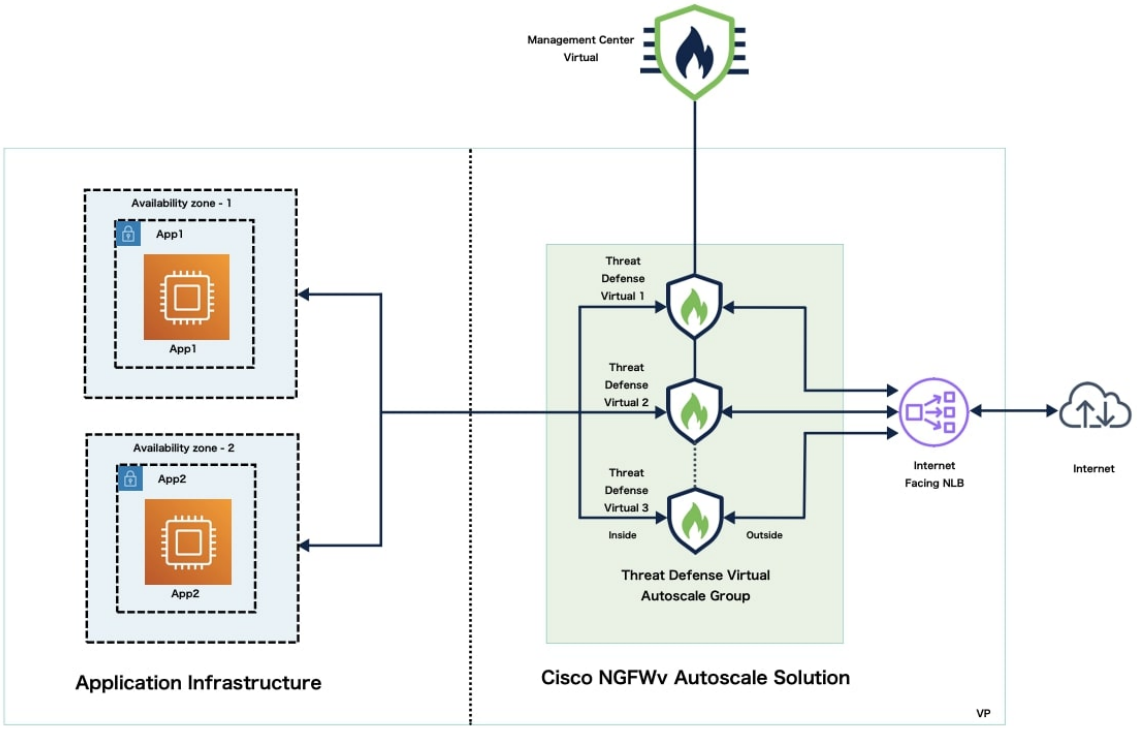
インターネットに面したロードバランサは、ネットワークロードバランサまたはアプリケーション ロード バランサです。いずれの場合も、AWS のすべての要件と条件が適用されます。以下のトポロジの例で示されているように、点線の右側部分は Threat Defense Virtual テンプレートを介して展開されます。左側はユーザー定義の部分です。

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

トラフィックのポートベースの分岐が可能です。この分岐は、NAT ルールによって実現できます。Management Center での「ホストオブジェクトの作成」、「デバイスグループの追加」、「NLB を使用した Auto Scale ソリューション：ネットワークアドレス変換（NAT）ポリシーの設定と展開」、基本的なアクセス コントロール ポリシーの作成（149 ページ）、「基本的なアクセス コントロール ポリシーの作成」を参照してください。たとえば、インターネットに面した LB DNS、ポート：80 のトラフィックは、アプリケーション 1 にルーティングでき、ポート：88 のトラフィックはアプリケーション 2 にルーティングできます。

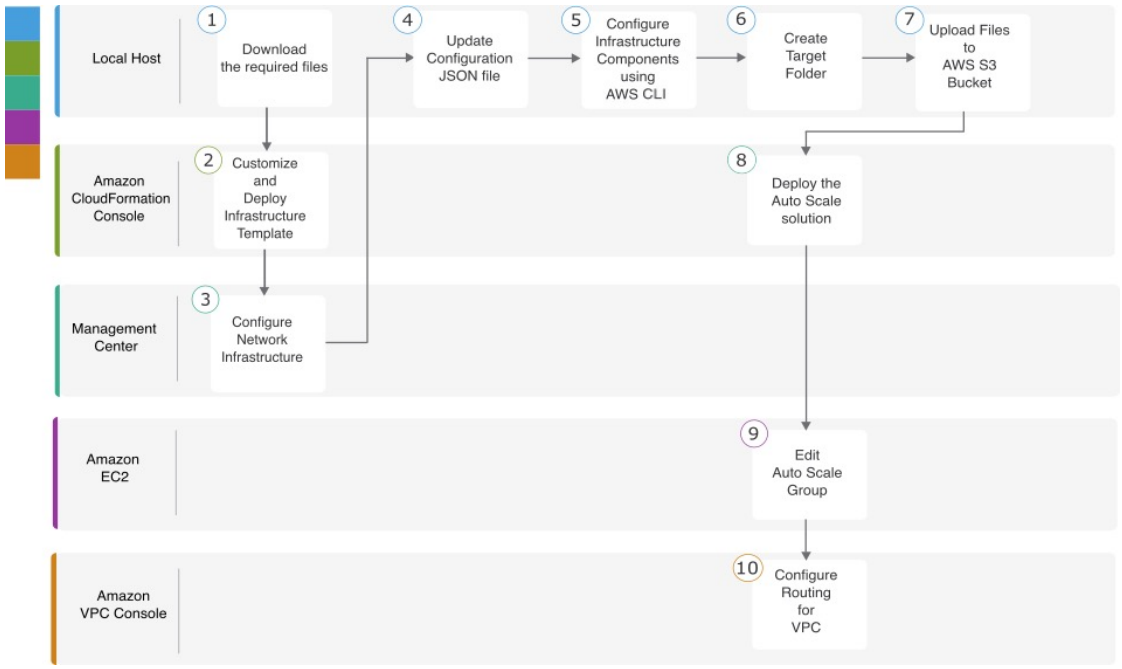
トポロジの例

図 *3 : NLB* を使用した *Threat Defense Virtual Auto Scale* ソリューション




# NLB を使用して Auto Scale ソリューションを展開するためのエンドツーエンドのプロセス

次のフローチャートは、Amazon Web Services（AWS）に NLB を使用して Threat Defense Virtual Auto Scale ソリューション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 | GitHub からローカルホストへの必要なファイルと CFT のダウンロード |
| 2 | Amazon CloudFormation コンソール | NLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの NLB インフラストラクチャテンプレートのカスタマイズと展開（142 ページ） |
| 3 | Management Center | Management Center でのネットワーク インフラストラクチャの設定（144 ページ） |
| 4 | ローカルホスト | Configuration.json ファイルの更新（150 ページ） |
| 5 | ローカルホスト | AWS CLI を使用したインフラストラクチャ コンポーネントの設定（151 ページ） |
| 6 | ローカルホスト | target フォルダの作成（153 ページ） |
| 7 | ローカルホスト | Amazon S3 バケットへのファイルのアップロード（153 ページ） |
| 8 | Amazon CloudFormation コンソール | NLB を使用した Auto Scale ソリューション：NLB を使用した Auto Scale ソリューションの展開（153 ページ） |
| 9 | Amazon EC2 コンソール | Auto Scale グループの編集（156 ページ） |

| | ワークスペース | 手順 |
|---|---|---|
| 10 | Amazon VPC コンソール | VPC のルーティングの設定 （155 ページ） |

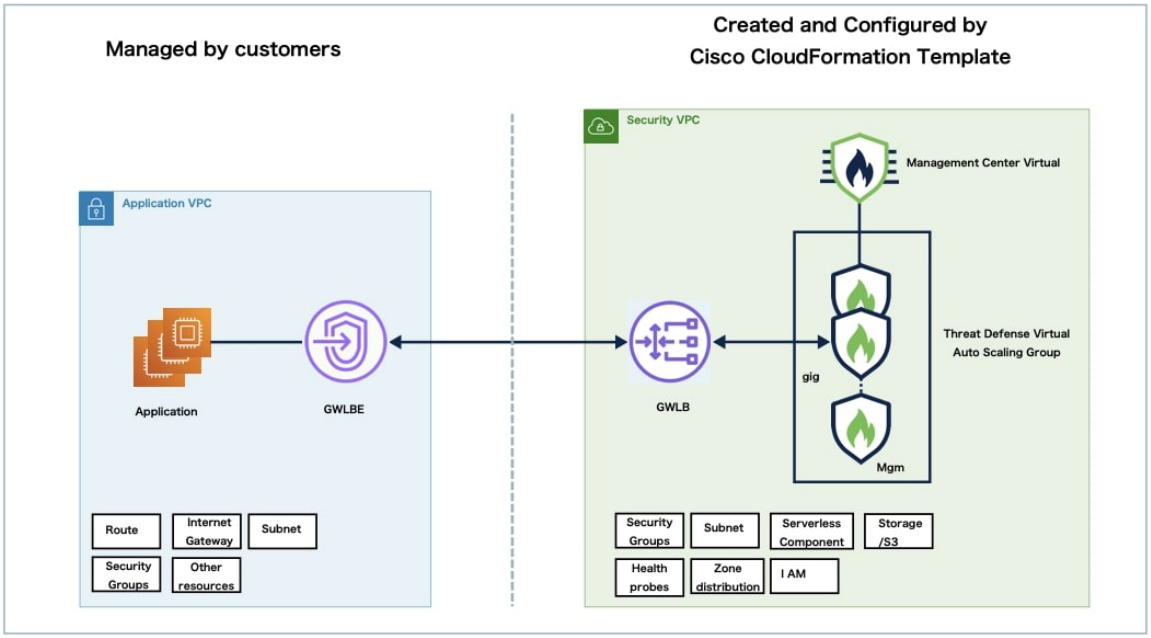
# GWLB を使用した Auto Scale ソリューション

AWS ゲートウェイロードバランサ（GWLB）を使用すると、インバウンド接続とアウトバウンド接続の両方を許可できるため、内部と外部で生成されたトラフィックが Cisco Threat Defense Virtual ファイアウォール経由で内部を通過できます。

トラフィックは GWLBe から GWLB に送信され、その後、検査のために Threat Defense Virtual に送信されます。いずれの場合も、AWS のすべての要件と条件が適用されます。導入例の図に示されているように、点線の右側部分は Threat Defense Virtual テンプレートを介して展開された Threat Defense Virtual GWLB Auto Scale ソリューションです。左側は完全にユーザー定義の部分です。

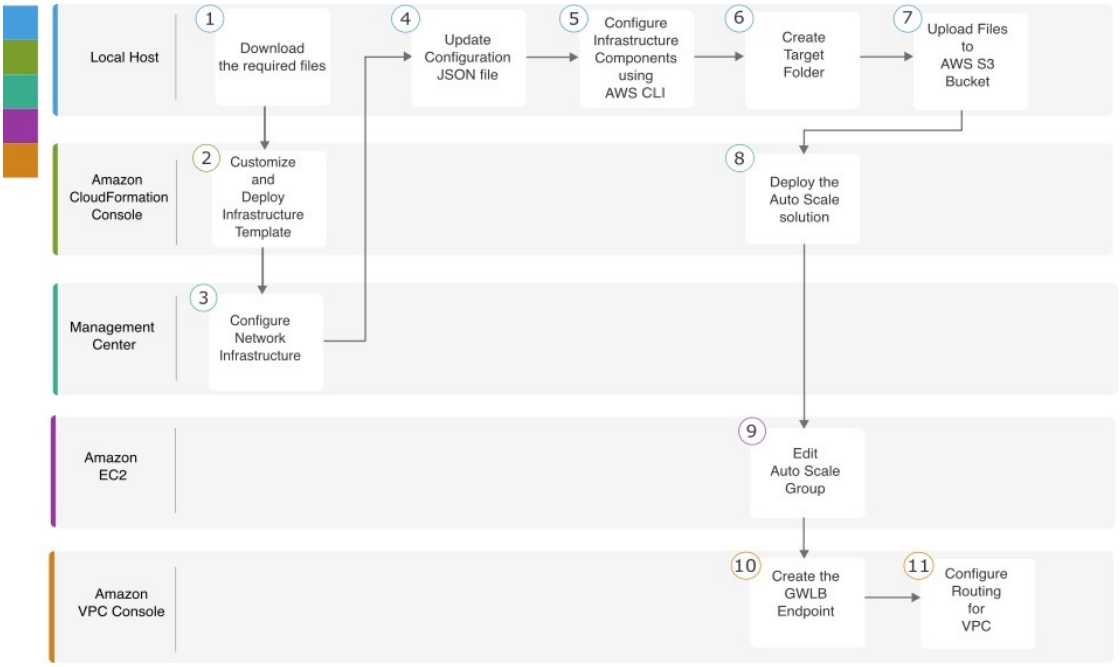
## トポロジの例

図 *4 : GWLB* を使用した *Threat Defense Virtual Auto Scale* ソリューション



# GWLB を使用して Auto Scale ソリューションを展開するためのエンドツーエンドのプロセス

次のフローチャートは、Amazon Web Services（AWS）に GWLB を使用して Threat Defense Virtual Auto Scale ソリューション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 | GitHub からローカルホストへの必要なファイルと CFT のダウンロード |
| 2 | Amazon CloudFormation コンソール | GWLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの GWLB インフラストラクチャ テンプレートのカスタマイズと展開 （143 ページ） |
| 3 | Management Center | Management Center でのネットワーク インフラストラクチャの設定 （144 ページ） |
| 4 | ローカルホスト | Configuration.json ファイルの更新 （150 ページ） |
| 5 | ローカルホスト | AWS CLI を使用したインフラストラクチャ コンポーネントの設定 （151 ページ） |
| 6 | ローカルホスト | target フォルダの作成 （153 ページ） |

| | ワークスペース | 手順 |
|---|---|---|
| 7 | ローカルホスト | Amazon S3 バケットへのファイルのアップロード （153 ページ） |
| 8 | Amazon CloudFormation コンソール | GWLB を使用した Auto Scale ソリューション：GWLB を使用した Auto Scale ソリューションの展開 （154 ページ） |
| 9 | Amazon EC2 コンソール | Auto Scale グループの編集 （156 ページ） |
| 10 | Amazon VPC コンソール | GWLB ソリューションを使用した Auto Scale：GWLB エンドポイントの作成 （154 ページ） |
| 11 | Amazon VPC コンソール | VPC のルーティングの設定 （155 ページ） |

# Threat Defense Virtual および AWS のガイドラインと制限事項

### ライセンシング

- 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）がサポートされています。
- 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 Threat Defense Virtual を実行できる従量制課金モデル。登録された PAYG Threat Defense Virtual 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、Management Center 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、Device Manager モードで展開されている Threat Defense Virtual デバイスではサポートされていません。

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Firepower Management Center Administration Guide』の「Licenses」の章を参照してください。

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual のバージョン 7.0.0 リリース以降では、Threat Defense Virtual 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 *16 : Threat Defense Virtual* 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 | 4 コア/8 GB | 100 Mbps | 50 |
| FTDv10 | 4 コア/8 GB | 1 Gbps | 250 |
| FTDv20 | 4 コア/8 GB | 3Gbps | 250 |
| FTDv30 | 8 コア/16 GB | 5 Gbps | 250 |
| FTDv50 | 12 コア/24 GB | 10 Gbps | 750 |
| FTDv100 | 16 コア/34 GB | 16 Gbps | 10,000 |

## ベスト プラクティス

- Management Center Virtual で必要なコンポーネントを設定していることを確認します。詳細については、「Management Center でのネットワーク インフラストラクチャの設定」を参照してください。
- CloudFormation テンプレートのパラメータに必要な値を入力していることを確認します。詳細については、「GitHub の CloudFormation テンプレート」を参照してください。

## 前提条件

- AWS アカウントhttp://aws.amazon.com/ で 1 つ作成できます。
- Threat Defense Virtual のコンソールにアクセスするには、SSH クライアント（例：Windows の場合は PuTTY、macOS の場合はターミナル）が必要です。
- Cisco スマートアカウント。Cisco Software Central で作成できますhttps://software.cisco.com/
- 構成ファイルとテンプレートをダウンロードするための GitHub アカウント。
- Threat Defense Virtual インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - 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 Management Center の管理用に設定できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから Management Center へのアクセスは、高可用性の展開ではサポートされません。Management Center アクセス用のデータインターフェイスの設定の詳細については、FTD コマンドリファレンスの configure network management-data-interface コマンドを参照してください。

- トラフィック インターフェイス（2）：Threat Defense Virtual を内部ホストおよびパブリックネットワークに接続するために使用されます。

- 通信パス：Threat Defense Virtual にアクセスするためのパブリック IP/Elastic IP。

# GWLB または NLB を使用した Auto Scale ソリューションの設定に必要なコンポーネント

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

### CloudFormation テンプレート

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

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

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

### Lambda 関数

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

- インスタンスに対して Diag、Gig0/0、および Gig 0/1 インターフェイスを追加/削除します。
- ロードバランサのターゲットグループに Gig0/1 インターフェイスを登録します。
- Management Center で Threat Defense Virtual を新規登録します。
- Management Center を介して新規の Threat Defense Virtual を展開します。
- スケールインした Threat Defense Virtual を Management Center から登録解除（削除）します。
- Management Center からメモリメトリックをパブリッシュします。

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

### ライフサイクルフック

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

### Simple Notification Service（SNS）

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

### VPC

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

### セキュリティ グループ

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

| ポート | 使用方法 | サブネット |
|---|---|---|
| 8305 | Management Center から Threat Defense Virtual へのセキュアなトンネル接続 | 管理サブネット |
| 正常性プローブポート（デフォルト：8080） | インターネットに面したロードバランサの正常性プローブ | 外部サブネット、内部サブネット |
| アプリケーションポート | アプリケーション データ トラフィック | 外部サブネット、内部サブネット |

### Management Center インスタンスのセキュリティグループまたは ACL

これらは、Lambda 関数と Management Center 間の HTTPS 接続を許可するために必要です。Lambda 関数は、NAT ゲートウェイをデフォルトルートとして持つ Lambda サブネットに保持されるため、Management Center には NAT ゲートウェイ IP アドレスからのインバウンド HTTPS 接続を設定できます。

### サブネット

サブネットは、アプリケーションの要件に応じて作成できます。Threat Defense Virtual が動作するには 3 つのサブネットが必要です。

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

### 外部サブネット

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

### 内部サブネット

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

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

### 管理サブネット

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

### Lambda サブネット

AWS Lambda 関数では、デフォルトゲートウェイとして NAT ゲートウェイを持つ 2 つのサブネットが必要です。これにより、Lambda 関数が VPC に対してプライベートになります。Lambda サブネットは、他のサブネットと同じ幅である必要はありません。

### アプリケーションサブネット

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

### サーバーレスコンポーネント

#### S3 バケット

Amazon Simple Storage Service（Amazon S3）は、業界をリードする拡張性、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクト ストレージ サービスです。必要なすべてのファイルを S3 バケットに配置できます。

テンプレートが展開されると、S3 バケット内の zip ファイルを参照して Lambda 関数が作成されるため、S3 バケットはユーザーアカウントにアクセスできる必要があります。

# GitHub の CloudFormation テンプレート

サポートされている Auto Scale ソリューション用に 2 つのテンプレートセットが用意されています。1 つのセットは NLB を使用した Auto Scale ソリューションの設定用で、もう 1 つのセットは GWLB を使用した Auto Scale ソリューションの設定用です。

# NLB を使用した Auto Scale ソリューション

GitHub では、次のテンプレートを使用できます。

- infrastructure.yaml
- deploy_ngfw_autoscale.yaml

表 *17*: テンプレートパラメータのリスト

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| PodNumber | 許可される文字列パターン：'^\d{1,3}$' | これはポッド番号です。この番号は、Auto Scale グループ名（threat defense virtual-Group-Name）の末尾に追加されます。たとえば、値が「1」の場合、グループ名は threat defense virtual-Group-Name-1 になります。<br>1 桁以上 3 桁以下の数字である必要があります。デフォルト：1。 |
| AutoscaleGrpNamePrefix | 文字列 | これは Auto Scale グループ名プレフィックスです。ポッド番号がサフィックスとして追加されます。<br>最大：18 文字<br>例：Cisco-threat defense virtual-1。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| NotifyEmailID | 文字列 | Auto Scale イベントはこの電子メールアドレスに送信されます。サブスクリプション電子メール要求を受け入れる必要があります。<br>例：admin@company.com。 |
| VpcId | 文字列 | デバイスを展開する必要がある VPC ID。これは、AWS の要件に従って設定する必要があります。<br>タイプ：AWS::EC2::VPC::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LambdaSubnets | リスト | Lambda 関数が展開されるサブネット。<br>タイプ：List<AWS::EC2::Subnet::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LambdaSG | リスト | Lambda 機能のセキュリティグループ。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| S3BktName | 文字列 | ファイルの S3 バケット名。これは、AWS の要件に従ってアカウントに設定する必要があります。<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LoadBalancerType | 文字列 | インターネットに面したロードバランサのタイプ（「アプリケーション」または「ネットワーク」）。<br>例：アプリケーション |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| LoadBalancerSG | 文字列 | ロードバランサのセキュリティグループ。ネットワークロードバランサの場合は使用されません。ただし、セキュリティグループ ID を指定する必要があります。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LoadBalancerPort | 整数 | ロードバランサポート。このポートは、選択したロードバランサタイプに基づいて、プロトコルとして HTTP/HTTPS または TCP/TLS を使用して LB で開きます。<br>ポートが有効な TCP ポートであることを確認します。これはロードバランサリスナーの作成に使用されます。<br>デフォルト：80 |
| SSL認証 | 文字列 | セキュアポート接続の SSL 証明書の ARN。指定しない場合、ロードバランサで開かれるポートは TCP/HTTP になります。指定した場合、ロードバランサで開かれるポートは TLS/HTTPS になります。 |
| TgHealthPort | 整数 | このポートは、正常性プローブのターゲットグループによって使用されます。Threat Defense Virtual のこのポートに到達する正常性プローブは、AWS メタデータサーバーにルーティングされるため、トラフィックには使用しないでください。このポートは有効な TCP ポートである必要があります。<br>アプリケーション自体が正常性プローブに応答するようにする場合は、応答するように Threat Defense Virtual の NAT ルールを変更できます。そのような場合、アプリケーションが応答しないと、Unhealthy インスタンスのしきい値アラームにより、Threat Defense Virtual は非正常とマークされて削除されます。<br>例：8080 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| AssignPublicIP | ブール値 | 「true」を選択すると、パブリック IP が割り当てられます。BYOL タイプの Threat Defense Virtual の場合、パブリック IP は https://tools.cisco.com に接続するために必要です。<br>例：TRUE |
| InstanceType | 文字列 | Amazon マシンイメージ（AMI）は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。<br>Threat Defense Virtual をサポートする AMI インスタンスタイプのみを使用する必要があります。<br>例：c4.2xlarge |
| LicenseType | 文字列 | Threat Defense Virtual ライセンスタイプ（BYOL または PAYG）。関連する AMI ID が同じライセンスタイプであることを確認します。<br>例：BYOL |
| AmiId | 文字列 | Threat Defense Virtual AMI ID（有効な Cisco Threat Defense Virtual AMI ID）。<br>タイプ：AWS::EC2::Image::Id<br>リージョンとイメージの目的のバージョンに応じて、正しい AMI ID を選択してください。Auto Scale 機能は、バージョン 6.4+、BYOL/PAYG イメージをサポートします。いずれの場合も、AWS マーケットプレイスでライセンスに同意する必要があります。<br>BYOL の場合、設定 JSON ファイルの「licenseCaps」キーを「BASE」、「MALWARE」、「THREAT」、「URLFilter」などの機能で更新してください。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| NoOfAZs | 整数 | Threat Defense Virtual を展開する必要がある可用性ゾーンの数（1 ー 3）。ALB 導入の場合、AWS で必要な最小値は 2 です。<br>例：2。 |
| ListOfAzs | カンマ区切り文字列 | ゾーンの順序のカンマ区切りリスト。<br>（注） ゾーンのリスト順は重要です。サブネットリストは同じ順序で指定する必要があります。<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。<br>例：us-east-1a、us-east-1b、us-east-1c |
| MgmtInterfaceSG | 文字列 | Threat Defense Virtual 管理インターフェイスのセキュリティグループ。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| InsideInterfaceSG | 文字列 | Threat Defense Virtual 内部インターフェイスのセキュリティグループ。<br>タイプ：AWS::EC2::SecurityGroup::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| OutsideInterfaceSG | 文字列 | Threat Defense Virtual 外部インターフェイスのセキュリティグループ。<br>タイプ：AWS::EC2::SecurityGroup::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。<br>例：sg-0c190a824b22d52bb |

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

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| ngfwPassword | 文字列 | すべての Threat Defense Virtual インスタンスには、起動テンプレート（Auto Scale グループ）の [ユーザーデータ（Userdata）] フィールドに入力されたデフォルトのパスワードが設定されています。<br>この入力により、Threat Defense Virtual にアクセスできるようになると、パスワードが新しく提供されたパスワードに変更されます。<br>KMS ARN が使用されていない場合は、プレーンテキストのパスワードを使用してください。KMS ARN が使用されている場合は、暗号化されたパスワードを使用する必要があります。<br>例：Cisco123789! または AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU |
| fmcServer | 数値文字列 | Lambda 関数と Threat Defense Virtual 管理インターフェイスの両方に到達可能な Management Center 管理用の IP アドレス。<br>例：10.10.17.21 |
| fmcOperationsUsername | 文字列 | Management Center を管理する際に作成された Network-Admin 以上の特権ユーザー。ユーザーおよびロールの作成の詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語] を参照してください。<br>例：apiuser-1 |
| fmcOperationsPassword | 文字列 | KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。<br>例：Cisco123@ または AQICAHgcQAtz/hvaxMtJvY/x/mKI3dFPpSXUHQRnCAajB |
| fmcDeviceGrpName | 文字列 | Management Center のデバイスグループ名。<br>例：AWS-Cisco-NGFW-VMs-1 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| fmcPerformanceLicenseTier | 文字列 | Threat Defense Virtual デバイスを Management Center Virtual に登録する際に使用されたパフォーマンス階層ライセンス。<br>使用できる値：FTDv/FTDv5/FTDv10/FTDv20/FTDv30/FTDv50/FTDv100 |
| fmcPublishMetrics | ブール値 | 「TRUE」に設定すると、指定されたデバイスグループ内の登録済み Threat Defense Virtual センサーのメモリ消費量を取得するために、2 分に 1 回実行される Lambda 関数が作成されます。<br>使用可能な値：TRUE、FALSE<br>例：TRUE |
| fmcMetricsUsername | 文字列 | AWS CloudWatch にメトリックを公開するための一意の Management Center ユーザー名。ユーザーおよびロールの作成の詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語] を参照してください。<br>「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。<br>例：publisher-1 |
| fmcMetricsPassword | 文字列 | AWS CloudWatch にメトリックを公開するための Management Center パスワード。KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。<br>「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。<br>例：Cisco123789! |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| CpuThresholds | カンマ区切り整数 | CPU しきい値の下限と CPU しきい値の上限。最小値は 0 で、最大値は 99 です。<br>デフォルト：10, 70<br>しきい値の下限はしきい値の上限よりも小さくする必要があります。<br>例：30,70 |
| MemoryThresholds | カンマ区切り整数 | MEM しきい値の下限と MEM しきい値の上限。最小値は 0 で、最大値は 99 です。<br>デフォルト：40, 70<br>しきい値の下限はしきい値の上限よりも小さくする必要があります。「fmcPublishMetrics」パラメータが「FALSE」の場合、影響はありません。<br>例：40,50 |

# GWLB を使用した Auto Scale ソリューション

**GitHub で利用可能なテンプレート**

- infrastructure_gwlb.yaml
- deploy_ngfw_autoscale_with_gwlb.yaml

**表 *18*：テンプレートパラメータのリスト**

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| PodNumber | 文字列<br>許可パターン：'^\d{1,3}$' | これはポッド番号です。Auto Scale グループ名（Threat Defense Virtual-Group-Name）の末尾に追加されます。たとえば、この値が「1」の場合、グループ名は *Threat Defense Virtual-Group-Name-1.* になります。<br>1 桁以上 3 桁以下の数字である必要があります。<br>デフォルト：1 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| AutoscaleGrpNamePrefix | 文字列 | これはAuto Scaleグループ名プレフィックスです。ポッド番号がサフィックスとして追加されます。<br>最大：18 文字<br>例：Cisco-Threat Defense Virtual-1 |
| NotifyEmailID | 文字列 | Auto Scale イベントはこの電子メールアドレスに送信されます。サブスクリプション電子メール要求を受け入れる必要があります。<br>例：admin@company.com |
| VpcId | 文字列 | デバイスを展開する必要がある VPC ID。これは、AWS の要件に従って設定する必要があります。<br>タイプ：AWS::EC2::VPC::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LambdaSubnets | リスト | Lambda 関数が展開されるサブネット。<br>タイプ：List<AWS::EC2::Subnet::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LambdaSG | リスト | Lambda 機能のセキュリティグループ。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| S3BktName | 文字列 | ファイルの S3 バケット名。これは、AWS の要件に従ってアカウントに設定する必要があります。<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| LoadBalancerType | 文字列 | インターネットに面したロードバランサのタイプ（「アプリケーション」または「ネットワーク」）。<br>例：アプリケーション |
| LoadBalancerSG | 文字列 | ロードバランサのセキュリティグループ。ネットワークロードバランサの場合は使用されません。ただし、セキュリティグループ ID を指定する必要があります。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| LoadBalancerPort | 整数 | ロードバランサポート。このポートは、選択したロードバランサタイプに基づいて、プロトコルとして HTTP/HTTPS または TCP/TLS を使用して LB で開きます。<br>ポートが有効な TCP ポートであることを確認します。これはロードバランサリスナーの作成に使用されます。<br>デフォルト：80 |
| SSL認証 | 文字列 | セキュアポート接続の SSL 証明書の ARN。指定しない場合、ロードバランサで開かれるポートは TCP/HTTP になります。指定した場合、ロードバランサで開かれるポートは TLS/HTTPS になります。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| TgHealthPort | 整数 | このポートは、正常性プローブのターゲットグループによって使用されます。Threat Defense Virtual のこのポートに到達する正常性プローブは、AWS メタデータサーバーにルーティングされるため、トラフィックには使用しないでください。このポートは有効な TCP ポートである必要があります。<br>アプリケーション自体が正常性プローブに応答するようにする場合は、それに応じて Threat Defense Virtual の NAT ルールを変更できます。このような場合、アプリケーションが応答しないと、Threat Defense Virtual は Unhealthy インスタンスのしきい値アラームにより、非正常としてマークされ、削除されます。<br>例：8080 |
| AssignPublicIP | ブール値 | 「true」を選択すると、パブリック IP が割り当てられます。BYOL タイプの Threat Defense Virtual の場合、これは https://tools.cisco.com に接続するために必要です。<br>例：TRUE |
| InstanceType | 文字列 | Amazon マシンイメージ（AMI）は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。<br>Threat Defense Virtual をサポートする AMI インスタンスタイプのみを使用する必要があります。<br>例：c4.2xlarge |
| LicenseType | 文字列 | Threat Defense Virtual ライセンスタイプ（BYOL または PAYG）。関連する AMI ID が同じライセンスタイプであることを確認します。<br>例：BYOL |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| AmiId | 文字列 | Threat Defense Virtual AMI ID（有効な Cisco Threat Defense Virtual AMI ID）。<br>タイプ：AWS::EC2::Image::Id<br>リージョンとイメージの目的のバージョンに応じて、正しい AMI ID を選択してください。Auto Scale 機能は、バージョン 6.4+、BYOL/PAYG イメージをサポートします。いずれの場合も、AWS マーケットプレイスでライセンスに同意する必要があります。<br>BYOL の場合、設定 JSON ファイルの「licenseCaps」キーを「BASE」、「MALWARE」、「THREAT」、「URLFilter」などの機能で更新してください。 |
| NoOfAZs | 整数 | Threat Defense Virtual を展開する必要がある可用性ゾーンの数（1 ー 3）。ALB 導入の場合、AWS で必要な最小値は 2 です。<br>例：2。 |
| ListOfAzs | カンマ区切り文字列 | ゾーンの順序のカンマ区切りリスト。<br>（注） ゾーンのリスト順は重要です。サブネットリストは同じ順序で指定する必要があります。<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。<br>例：us-east-1a、us-east-1b、us-east-1c |
| MgmtInterfaceSG | 文字列 | Threat Defense Virtual 管理インターフェイスのセキュリティグループ。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| InsideInterfaceSG | 文字列 | Threat Defense Virtual 内部インターフェイスのセキュリティグループ。<br>タイプ：AWS::EC2::SecurityGroup::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| OutsideInterfaceSG | 文字列 | Threat Defense Virtual 外部インターフェイスのセキュリティグループ。<br>タイプ：AWS::EC2::SecurityGroup::Id<br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。<br>例：sg-0c190a824b22d52bb |
| MgmtSubnetId | カンマ区切りリスト | 管理サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| InsideSubnetId | カンマ区切りリスト | 内部/Gig0/0 サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| OutsideSubnetId | カンマ区切りリスト | 外部/Gig0/1 サブネット ID のカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。<br>タイプ：List<AWS::EC2::SecurityGroup::Id><br>「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 |
| KmsArn | 文字列 | 既存の KMS の ARN（保存時に暗号化するための AWS KMS キー）。 指定した場合、Management Center と Threat Defense Virtual のパスワードを暗号化する必要があります。 パスワードの暗号化は、指定された ARN のみを使用して実行する必要があります。<br>暗号化パスワードの生成例： " aws kms encrypt --key-id <KMS ARN> --plaintext <password> " 次のような生成されたパスワードを使用してください。<br>例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e |
| ngfwPassword | 文字列 | すべての Threat Defense Virtual インスタンスには、起動テンプレート（自動スケールグループ）の [ユーザーデータ（Userdata）] フィールドに入力されたデフォルトのパスワードが設定されています。<br>この入力により、Threat Defense Virtual にアクセスできるようになると、パスワードが新しく提供されたパスワードに変更されます。<br>KMS ARN が使用されていない場合は、プレーンテキストのパスワードを使用してください。KMS ARN が使用されている場合は、暗号化されたパスワードを使用する必要があります。<br>例：Cisco123789! または AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU |
| fmcServer | 数値文字列 | Lambda 関数と Threat Defense Virtual 管理インターフェイスの両方に到達可能な Management Center 管理用の IP アドレス。<br>例：10.10.17.21 |

| パラメータ | 使用できる値/タイプ | 説明 |
|---|---|---|
| fmcOperationsUsername | 文字列 | Management Center を管理する際に作成された Network-Admin 以上の特権ユーザー。ユーザとロールの作成の詳細については、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』を参照してください。<br>例：apiuser-1 |
| fmcOperationsPassword | 文字列 | KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。<br>例：Cisco123@ または AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB |
| fmcDeviceGrpName | 文字列 | Management Center のデバイスグループ名。<br>例：AWS-Cisco-NGFW-VMs-1 |
| fmcPerformanceLicenseTier | 文字列 | Threat Defense Virtual デバイスを Management Center Virtual に登録する際に使用されたパフォーマンス階層ライセンス。<br>使用できる値：FTDv/FTDv20/FTDv30/FTDv50/FTDv100<br>（注） FTDv5 および FTDv10 パフォーマンス階層ライセンスは、AWS ゲートウェイロードバランサではサポートされていません。 |
| fmcPublishMetrics | ブール値 | 「TRUE」に設定すると、指定されたデバイスグループ内の登録済み Threat Defense Virtual センサーのメモリ消費量を取得するために、2 分に 1 回実行される Lambda 関数が作成されます。<br>使用可能な値：TRUE、FALSE<br>例：TRUE |

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

# GitHub からローカルホストへの必要なファイルと CFT のダウンロード

GitHub から **lambda-python-files** フォルダをダウンロードします。このフォルダには、次のファイルが含まれています。

- Lambda レイヤの作成に使用される Python（.py）ファイル。
- 必要に応じて、スタティックルートを追加し、ネットワークパラメータをカスタマイズするために使用される configuration.json ファイル。

GitHub から次の CloudFormation テンプレートをダウンロードします。

- NLB を使用した Auto Scale ソリューションのテンプレート：
  - **Infrastructure.yaml**：AWS 環境のコンポーネントをカスタマイズするために使用されます。
  - **deploy_ngfw_autoscale.yaml**：NLB ソリューションを使用した AWS Auto Scale の展開に使用されます。
- GWLB を使用した Auto Scale ソリューションのテンプレート：
  - **Infrastructure_gwlb.yaml**：AWS 環境のコンポーネントをカスタマイズするために使用されます。
  - **deploy_ngfw_autoscale_with_gwlb.yaml**：GWLB ソリューションを使用して AWS Auto Scale を展開するために使用されます。

（注） 可能な場合は、テンプレートパラメータの値を収集します。収集すると、AWS 管理コンソールでテンプレートを展開するときに、値をすばやく簡単に入力できます。

# NLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの NLB インフラストラクチャテンプレートのカスタマイズと展開

NLB を使用して Auto Scale ソリューションを展開する場合は、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]**の順に選択し、**[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 2** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose file）] をクリックして、ファイルをダウンロードしたフォルダから **infrastructure.yaml** を選択します。

**ステップ 3** [次へ（Next）] をクリックします。

**ステップ 4** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 5** ***Infrastructure.yaml*** テンプレートの入力パラメータの値を指定します。

**ステップ 6** [次へ（Next）] をクリックします。

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして **infrastructure.yaml** テンプレートを展開し、スタックを作成します。

**ステップ 10** 展開が完了したら [出力（Outputs）] に移動し、**S3 バケット名**を書き留めます。

# GWLB を使用した Auto Scale ソリューション：Amazon CloudFormation コンソールでの GWLB インフラストラクチャ テンプレートのカスタマイズと展開

GWLB を使用して Auto Scale ソリューションを展開する場合は、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]**の順に選択し、**[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 2** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose file）] をクリックして、ファイルをダウンロードしたフォルダから **infrastructure_gwlb.yaml** を選択します。

**ステップ 3** [次へ（Next）] をクリックします。

**ステップ 4** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 5** ***Infrastructure_gwlb.yaml*** テンプレートの入力パラメータの値を指定します。

**ステップ 6** [次へ（Next）] をクリックします。

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして **infrastructure_gwlb.yaml** テンプレートを展開し、スタックを作成します。

**ステップ 10** 展開が完了したら [出力（Outputs）] に移動し、**S3 バケット名**を書き留めます。

# Management Center でのネットワーク インフラストラクチャの設定

登録済みの Threat Defense Virtual の Management Center でデバイスグループ、オブジェクト、ヘルスチェックポート、NAT ポリシー、およびアクセスポリシーを作成および設定します。

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 Management Center を使用して Threat Defense Virtual を管理できます。Threat Defense Virtual は、Threat Defense Virtual 仮想マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

詳細については、「Cisco Secure Firewall Management Center を備えた Cisco Secure Firewall Threat Defense Virtual について」を参照してください。

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

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

## デバイスグループの追加

Management Center を使用すると、デバイスをグループ化して、複数のデバイスへのポリシーの展開や更新のインストールを簡単に実行できます。グループに属するデバイスのリストは、展開または縮小表示できます。

**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。

**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** 既存のグループを編集するには、編集するグループの [編集（Edit）]（編集アイコン）をクリックします。

**ステップ 4** 名前を入力します。

**ステップ 5** [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift を押しながらクリックします。

**ステップ 6** [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

**ステップ 7** [OK] をクリックして、デバイス グループを追加します。

# ホストオブジェクトの作成

**ステップ 1** Management Center にログインします。

**ステップ 2** **[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 3** オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

**ステップ 4** [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

**ステップ 5** 名前を入力します。

**ステップ 6** 説明を入力します。

**ステップ 7** [ネットワーク（Network）] フィールドで [ホスト（Host）] オプションを選択し、次の値を入力します。

a) オブジェクトタイプの名前：**aws-metadata-server**。

b) ホストプロトコルのタイプに応じて、IPv4 の IP アドレス **169.254.169.254** を入力します。

**ステップ 8** [保存（Save）] をクリックします。

# ポートオブジェクトの作成

**ステップ 1** Management Center にログインします。

**ステップ 2** **[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 3** オブジェクト タイプのリストから [ポート（Port）] を選択します。

**ステップ 4** [ポートの追加（Add Port）] ドロップダウンメニューで、[オブジェクトの追加（Add Object）] を選択します。

**ステップ 5** 名前を入力します。

**ステップ 6** [プロトコル（Protocol）] を選択します。[ホスト（Host）] オブジェクトタイプに入力したプロトコルを選択する必要があります。選択したプロトコルに応じて、[ポート（Port）] で制限するか、または ICMP の [タイプ（Type）] および [コード（Code）] を選択します。

**ステップ 7** **8080** と入力します。ここで入力するポート番号は、要件に応じてカスタマイズできます。

（注） [すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウンリストを使用して、ポートでオブジェクトを制限する必要があります。

**ステップ 8** [保存（Save）] をクリックします。

# セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成

**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）]**の順にクリックするか、**[追加（Add）]**>**[インターフェイスグループ（Interface Group）]**の順にクリックします。

**ステップ 4** [名前（Name）] : *inside-sz/outside-sz* と入力します。

**ステップ 5** [インターフェイスタイプ（Interface Type）] : [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。

# ヘルスチェックプローブのポートの有効化

ヘルスチェックプローブのポート 22（SSH）またはポート 443（HTTP）を有効にできます。

## ヘルスチェックプローブのポート 22（SSH）の有効化

ヘルスチェックプローブにポート 22（SSH）を使用している場合は、次の手順を実行して、ヘルスチェックプローブのポートを有効にします。

**ステップ 1** **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[SSHアクセス（SSH Access）]**の順に選択します。

**ステップ 2** **[+ Add]** をクリックします。

**ステップ 3** ドロップダウンリストから関連する [IPアドレス（IP Address）] を選択します。

**ステップ 4** [使用可能なゾーン/インターフェイス（Available Zones/Interfaces）] ウィンドウで、GWLB または外部サブネットに接続されている外部インターフェイスを選択します。

**ステップ 5** [追加（Add）] をクリックして、選択したインターフェイスを [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] ウィンドウに追加します。

**ステップ 6** [OK] をクリックします。

**ステップ 7** [保存（Save）] をクリックします。

## ヘルスチェックプローブのポート 443（HTTP）の有効化

ヘルスチェックプローブにポート 443（HTTP）を使用している場合は、次の手順を実行して、ヘルスチェックプローブのポートを有効にします。

**ステップ 1** **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[HTTPアクセス（HTTP Access）]** の順に選択します。

**ステップ 2** [HTTPサーバーの有効化（Enable HTTP Server）] チェックボックスをオンにします。

**ステップ 3** [ポート（Port）] フィールドに、**443** と入力します。

**ステップ 4** **[+ Add]** をクリックします。

**ステップ 5** ドロップダウンリストから関連する [IPアドレス（IP Address）] を選択します。

**ステップ 6** [使用可能なゾーン/インターフェイス（Available Zones/Interfaces）] ウィンドウで、GWLB または外部サブネットに接続されている外部インターフェイスを選択します。

**ステップ 7** [追加（Add）] をクリックして、選択したインターフェイスを [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] ウィンドウに追加します。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [保存（Save）] をクリックします。

# NLB を使用した Auto Scale ソリューション：ネットワークアドレス変換（NAT）ポリシーの設定と展開

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。NAT ポリシーの詳細については、「Cisco Secure Firewall Management Center を使用した Cisco Secure Firewall Threat Defense Virtual の管理」の「NAT の設定」を参照してください。

NAT ポリシーには 1 つの必須ルールが必要です。以下に、NAT ルールの例を示します。

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

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

**重要** 作成された NAT ポリシーは、デバイスグループに適用する必要があります。この点は、Lambda 関数を使用した Management Center の検証によって検証されます。

**ステップ 1** Cisco Secure Firewall Management Center にログインします。

**ステップ 2** [デバイス（Devices）] メニューで [NAT] をクリックします。

**ステップ 3** 新しいポリシーを作成するには、**[新しいポリシー（New Policy）] > [Threat Defense NAT]**をクリックします。

**ステップ 4** NAT ポリシーの名前と説明を入力します。

**ステップ 5** [保存（Save）] をクリックします。

新しいポリシーが追加されて、[NAT] ページに表示されます。

**ステップ 6** [ルールの追加（Add Rule）] をクリックします。

**ステップ 7** [NATルール（NAT Rule）] ドロップダウンリストから [手動NATルール（Manual NAT Rule）] を選択します。

**ステップ 8** [挿入（Insert）] ドロップダウンリストから、[カテゴリ内（In Category）] および [前のNATルール（NAT Rule Before）] を選択します。

**ステップ 9** [タイプ（Type）] ドロップダウンメニューから [静的（Static）] を選択します。

**ステップ 10** 説明を入力します。

**ステップ 11** [インターフェイス オブジェクト（Interface Objects）] メニューで、送信元と宛先のオブジェクトを追加します。

**ステップ 12** [変換（Translations）] メニューで、各パラメータに次の値を追加します。

| パラメータ | 値 |
|---|---|
| 元の送信元 | any-ipv4 |
| [元の宛先（Original Destination）] | アドレス（Address） |
| [元の送信元ポート（Original Source Port）] | HTTP |
| [元の宛先ポート（Original Destination Port）] | 8080 |
| 変換済み送信元 | any-ipv4 |
| [変換済み送信元ポート（Translated Source Port）] | 元/デフォルト |
| [変換済みの宛先（Translated Destination）] | aws-metadata-server |
| [変換済みの宛先ポート（Translated Destination Port）] | 80/HTTP |

**ステップ 13** [保存（Save）] をクリックし、ルールを保存して追加します。

**ステップ 14** Threat Defense Virtual に展開するために作成した新しいルールを選択します。

**ステップ 15** **[展開（Deploy）]**>**[展開（Deployment）]**の順にクリックし、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

# 基本的なアクセス コントロール ポリシーの作成

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

新しいアクセス コントロール ポリシーを作成すると、そのポリシーにデフォルトのアクションと設定が含まれます。ポリシーを作成すると、要件に合わせてポリシーを調整できるよう、すぐに編集セッションに移行します。

**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** 一意の名前と説明を入力します。

**ステップ 4** 最初の [デフォルトアクション（Default Action）] : [すべてのトラフィックをブロック（Block all traffic）] を指定します。

**ステップ 5** [保存（Save）] をクリックします。

**ステップ 6** 作成した新しいポリシーの [編集（Edit）] アイコンをクリックします。

**ステップ 7** [ルールの追加（Add Rule）] をクリックします。

**ステップ 8** 次のパラメータを設定します。

- 名前：inside-to-outside
- 挿入：into Mandatory
- アクション：許可
- 送信元ゾーンと宛先ゾーンを追加します。

**ステップ 9** [適用（Apply）] をクリックします。

# Configuration.json ファイルの更新

**configuration.json** ファイルは、GitHub からダウンロードした **lambda_python_files** フォルダにあります。Management Center で設定したパラメータを使用して、**configuration.json** ファイルのパラメータを更新します。JSON キーは変更しないでください。

configuration.json ファイル内のスクリプトは次のとおりです。

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],   //Management center virtual licenses
  "fmcIpforDeviceReg": "DONTRESOLVE",   //Management center virtual IP address
  "RegistrationId": "cisco",  //Registration ID used while configuring the manager in
the Threat defense virtual
  "NatId": "cisco",  //NAT ID used while configuring the manager in the Threat defense
virtual
  "fmcAccessPolicyName": "aws-asg-policy",  //Access policy name configured in the
Management center virtual
  "fmcNatPolicyName": "AWS-Cisco-NGFW-VMs",  //NAT Policy name configured in the Management
 center virtual (Not required for GWLB-based deployment)
  "fmcInsideNicName": "inside", //Threat defense virtual inside interface name
  "fmcOutsideNicName": "outside", //Threat defense virtual outside interface name
  "fmcInsideNic": "GigabitEthernet0/0", //Threat defense virtual inside interface NIC
Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance
types)
  "fmcOutsideNic": "GigabitEthernet0/1", //Threat defense virtual outside interface NIC
 Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance
types
  "fmcOutsideZone": "Outside-sz", //Outside Interface security zone name that is set in
 the Management center virtual
  "fmcInsideZone": "Inside-sz", //Inside Interface security zone name that is set in the
 Management center virtual
  "MetadataServerObjectName": "aws-metadata-server", //Host object name created for the
 IP 169.254.169.254 in the Management center virtual  (Not required for GWLB-based
deployment)
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Inside-sz"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Outside-sz"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],  //Interface-related configuration
  "trafficRoutes": [
    {
      "interface": "inside",
      "network": "any-ipv4",
```

```
      "gateway": "",
      "metric": "1"
    }
  ] //This traffic route is used for the Threat defense virtual instance's health check
}
```

このファイルの **trafficRoutes** パラメータを変更することで、Threat Defense Virtual のスタティックルートを設定できます。スタティックルートの設定例を次に示します。

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

# AWS CLI を使用したインフラストラクチャ コンポーネントの設定

テンプレートでは、Threat Defense Virtual および Management Center の Lambda レイヤと暗号化されたパスワードは作成されません。次の手順を使用して、各コンポーネントを設定します。AWS CLI の詳細については、「AWS コマンドラインインターフェイス」を参照してください。

## コンピューティングリソースを管理するための Lambda レイヤ zip ファイルの作成

Linux ホストに Python フォルダを作成し、Lambda レイヤを作成します。

**ステップ 1** Linux ホストに Python フォルダ（Ubuntu 22.04 など）を作成します。

**ステップ 2** Linux ホストに Python 3.9 をインストールします。以下に、Python 3.9 をインストールするためのサンプルスクリプトを示します。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

**ステップ 3** Linux 環境で Lambda レイヤ zip ファイル（autoscale_layer.zip）を作成します。このファイルは、Lambda 関数に不可欠な Python ライブラリを提供します。

次のスクリプトを実行して、autoscale_layer.zip ファイルを作成します。

```
#!/bin/bash
mkdir -p layer
mkdir -p python
```

```
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install attrs==23.1.0
pip3 install bcrypt==3.2.2
pip3 install certifi==2022.12.7
pip3 install cffi==1.15.1
pip3 install chardet==3.0.4
pip3 install cryptography==2.9.1
pip3 install idna==2.10
pip3 install jsonschema==3.2.0
pip3 install paramiko==2.7.1
pip3 install pycparser==2.21
pip3 install pycryptodome==3.15.0
pip3 install PyNaCl==1.5.0
pip3 install pyrsistent==0.19.3
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install six==1.16.0
pip3 install urllib3==1.25.11
echo "Copy from ./layer directory to ./python\n"
cp -r./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

**ステップ 4** **autoscale_layer.zip** ファイルを作成したら、GitHub からダウンロードした **lambda-python-files** フォルダに **autoscale_layer.zip** ファイルをコピーします。

# （任意）Threat Defense Virtual および Management Center の暗号化パスワードの作成

Infrastructure_gwlb.yaml テンプレートファイルに KMS ARN 値が入力されている場合は、Threat Defense Virtual および Management Center で設定するパスワードを暗号化する必要があります。AWS KMS コンソールを使用してキー ARN を特定するには、Finding the key ID and key ARN [英語] を参照してください。ローカルホストで、次の AWS CLI コマンドを実行してパスワードを暗号化します。

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext
'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXH
JAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45
AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

「CiphertextBlob」の値は暗号化されたパスワードです。このパスワードは、**infrastructure_gwlb.yaml** ファイルの **NGFWv パスワード**（Threat Defense Virtual パスワード）または **Auto Scale 自動化の FMC パスワード**（Management Center のパスワード）パラメータの値として使用します。このパスワードは、**CloudWatch にメトリックを公開するための FMC パスワード**の値としても使用できます。

# target フォルダの作成

ローカルホストで次のコマンドを使用して、Amazon S3 バケットにアップロードする必要があるファイルを含む target フォルダを作成します。

**python3 make.py build**

ローカルホストに「target」という名前のフォルダが作成されます。target フォルダには、Auto Scale ソリューションの展開に必要な *zip* ファイルと *yaml* ファイルが含まれています。

# Amazon S3 バケットへのファイルのアップロード

ローカルホストで次のコマンドを使用して、target ディレクトリにあるすべてのファイルを Amazon S3 バケットにアップロードします。

**$ cd ./target**

**$ aws s3 cp . s3://**<*bucket-name*> **--recursive**

# NLB を使用した Auto Scale ソリューション：NLB を使用した Auto Scale ソリューションの展開

NLB を使用して Auto Scale ソリューションを展開する場合は、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]** > **[スタック（Stacks）]**の順に選択し、テンプレートによって作成されたスタックをクリックします。

**ステップ 2** **[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 3** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose File）] をクリックして、target フォルダから ***deploy_ngfw_autoscale.yaml*** を選択します。

**ステップ 4** [次へ（Next）] をクリックします。

**ステップ 5** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 6** ***deploy_ngfw_autoscale.yaml*** テンプレートの入力パラメータの値を指定します。

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして ***deploy_ngfw_autoscale.yaml*** テンプレートを展開し、スタックを作成します。

これで、NLB を使用した Threat Defense Virtual の Auto Scale ソリューションを設定するために必要な両方のテンプレートの展開が完了しました。

# GWLB を使用した Auto Scale ソリューション：GWLB を使用した Auto Scale ソリューションの展開

GWLB を使用して Auto Scale ソリューションを展開する場合は、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]** > **[スタック（Stacks）]**の順に選択し、テンプレートによって作成されたスタックをクリックします。

**ステップ 2** **[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 3** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose File）] をクリックして、target フォルダから ***deploy_ngfw_autoscale_with_gwlb.yaml*** を選択します。

**ステップ 4** [次へ（Next）] をクリックします。

**ステップ 5** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 6** ***deploy_ngfw_autoscale_with_gwlb.yaml*** テンプレートの入力パラメータの値を指定します。

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして ***deploy_ngfw_autoscale_with_gwlb.yaml*** テンプレートを展開し、スタックを作成します。

これで、GWLB を使用して Threat Defense Virtual 用の Auto Scale ソリューションを設定するために必要な両方のテンプレートの展開が完了しました。

# GWLB ソリューションを使用した Auto Scale：GWLB エンドポイントの作成

GWLB を使用して Auto Scale ソリューションを展開する場合は、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[ネットワーキングおよびコンテンツ配信（Networking & Content Delivery）]** > **[VPC]** > **[エンドポイントサービス（Endpoint Services）]**の順に選択します。

**ステップ 2** [エンドポイントサービスの作成（Create Endpoint Service）] をクリックします。

**ステップ 3** [ロードバランサタイプ（Load balancer type）] で [ゲートウェイ（Gateway）] を選択します。

**ステップ 4** [使用可能なロードバランサ（Available load Balancers）] で、Auto Scale の展開の一部として作成されたゲートウェイロードバランサを選択します。

**ステップ 5** [エンドポイントの承認が必要（Require acceptance for endpoint）] で [承認が必要（Acceptance required）] を選択します。選択すると、エンドポイントサービスの接続要求を手動で受け入れる必要があります。

**ステップ 6** [サポートされているIPアドレスタイプ（Supported IP address types）] で [IPv4]を選択します。

**ステップ 7** [作成（Create）] をクリックします。

**ステップ 8** 新たに作成したエンドポイントサービスのサービス名をコピーします。

**ステップ 9** **[サービス（Services）] > [ネットワーキングおよびコンテンツ配信（Networking & Content Delivery）] > [VPC] > [エンドポイント（Endpoints）]**の順に選択します。

**ステップ 10** [エンドポイントの作成（Create endpoint）] をクリックします。

**ステップ 11** [サービスカテゴリ（Service category）] で [その他のエンドポイントサービス（Other endpoint services）] を選択します。

**ステップ 12** [サービス名（Service name）] にサービスの名前を入力し、[サービスの確認（ Verify service）] を選択します。

**ステップ 13** [VPC] フィールドで、エンドポイントを作成する VPC を選択します。

**ステップ 14** [サブネット（Subnets）] で、エンドポイントを作成するサブネットを選択します。

**ステップ 15** [IPアドレスタイプ（IP address type）] で [IPv4] オプションを選択して、エンドポイント ネットワーク インターフェイスに IPv4 アドレスを割り当てます。

**ステップ 16** [エンドポイントの作成（Create endpoint）] をクリックします。

# VPC のルーティングの設定

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）] > [ネットワーキングおよびコンテンツ（Networking & Content）] > [仮想プライベートクラウド（Virtual Private Cloud）] > [ルートテーブル（Route tables）]**の順に選択します。

**ステップ 2** インターネットゲートウェイのルートテーブルを選択し、次の手順を実行します。

1. **[アクション（Actions）] > [ルートの編集（Edit routes）]**の順にクリックします。
2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、アプリケーションサーバーのサブネットの IPv4 CIDR ブロックを入力します。[ターゲット（Target）] で、VPC エンドポイントを選択します。
3. [変更の保存（Save Changes）] をクリックします。

**ステップ 3** アプリケーションサーバーがあるサブネットのルートテーブルを選択し、次の手順を実行します。

1. **[アクション（Actions）] > [ルートの編集（Edit routes）]**の順にクリックします。
2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、**0.0.0.0/0** と入力します。[ターゲット（Target）] で、VPC エンドポイントを選択します。

3. [変更の保存（Save Changes）] をクリックします。

**ステップ 4** ゲートウェイロードバランサのエンドポイントがあるサブネットのルートテーブルを選択し、次の手順を実行します。

1. **[アクション（Actions）] > [ルートの編集（Edit routes）]**の順にクリックします。
2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、**0.0.0.0/0** と入力します。[ターゲット（Target）] で、インターネットゲートウェイを選択します。
3. [変更の保存（Save Changes）] をクリックします。

# Auto Scale グループの編集

デフォルトでは、Auto Scale グループの Threat Defense Virtual インスタンスの最小数と最大数はそれぞれ 0 と 2 に設定されています。要件に応じて各値を変更します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）] > [コンピューティング（Compute）] > [EC2]**の順に選択し、[Auto Scalingグループ（Auto Scaling Groups）] をクリックします。

**ステップ 2** 作成したAuto Scalingグループを選択し、[編集（Edit）]をクリックして、要件に応じて[必要な容量（Desired capacity）]、[最小容量（Minimum capacity）]、[最大容量（Maximum capacity）] フィールドの値を変更します。各値は、Auto Scaling 機能のために起動する Threat Defense Virtual インスタンスの数に対応します。[必要な容量（Desired capacity）] を、最小容量値と最大容量値の範囲内の値に設定します。

**ステップ 3** **[更新（Update）]**をクリックします。

（注） Threat Defense Virtual インスタンスを 1 つだけ起動し、そのインスタンスが想定どおりに動作しているか確認することを推奨します。その後、要件に応じて追加のインスタンスを起動できます。

# 展開の検証

テンプレートの展開が成功したら、Amazon CloudWatch コンソールに移動して、ログが収集され、必要なアラームが作成されていることを確認します。

## ログ

ログファイルを確認して、Management Center の接続に関する問題をトラブルシューティングします。

**ステップ 1** **AWS 管理**コンソールで、**[サービス（Services）] > [管理とガバナンス（Management and Governance）] > [CloudWatch]**の順に選択します。

**ステップ 2** [ロググループ（Log groups）] をクリックし、表示されているいずれかのロググループをクリックしてログを表示します。

## アラーム

必要なアラームが Amazon CloudWatch コンソールで作成されていることを確認します。

**ステップ 1** **AWS 管理**コンソールで、**[サービス（Services）] > [管理とガバナンス（Management and Governance）] > [CloudWatch]**の順に選択します。

**ステップ 2** **[アラーム（Alarms）] > [すべてのアラーム（All Alarms）]**の順にクリックして、スケールアウトおよびスケールイン機能をトリガーする条件とともにアラームのリストを表示します。

# メンテナンス タスク

## スケーリングプロセス

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

### スケールアクションの開始と停止

スケールアクションを開始および停止するには、次の手順を実行します。

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

  スケーリングプロセスの一時停止と再開

## ヘルスモニター

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

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

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

#### ヘルスモニターの無効化

ヘルスモニターを無効にするには、***constant.py*** で固定値を「True」に設定します。

#### ヘルスモニターの有効化

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

## ライフサイクルフックの無効化

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

## Auto Scale Manager の無効化

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

## ロードバランサのターゲット

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

### ターゲットグループへのターゲットの登録

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

### ターゲットグループからのターゲットの登録解除

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

# インスタンスのスタンバイ

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

### インスタンスをスタンバイ状態にする

インスタンスがスタンバイ状態になると、正常性プローブが失敗するまで、ターゲットグループ内のそのインスタンスの IP は同じ状態のままになります。このため、インスタンスをスタンバイ状態にする前に、ターゲットグループからそれぞれの IP を登録解除することをお勧めします。詳細については、ロードバランサのターゲット（158 ページ）を参照してください。

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

### スタンバイ状態からのインスタンスの削除

同様に、インスタンスをスタンバイ状態から実行状態に移行できます。スタンバイ状態から削除すると、インスタンスの IP がターゲットグループのターゲットに登録されます。「ロードバランサのターゲット （158 ページ）」を参照してください。

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

### Auto Scale グループからのインスタンスの削除または分離

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

Management Center 側に変更はありません。必要な変更は手動で実行する必要があります。

# インスタンスで終了

インスタンスを終了するには、スタンバイ状態にする必要があります。インスタンスのスタンバイ （159ページ）を参照してください。インスタンスがスタンバイ状態になったら、終了できます。

# インスタンスのスケールイン保護

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

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

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

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

# 設定の変更

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

既存のインスタンスの設定を手動で更新しているときに問題が発生した場合は、それらのインスタンスをスケーリンググループから削除し、新しいインスタンスに置き換えることを推奨します。

### Management Center のユーザー名とパスワードの変更

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

Lambda の次回実行時に、変更された環境変数が参照されます。

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

### Threat Defense Virtual の管理者パスワードを変更します。

Threat Defense Virtual パスワードを変更すると、インスタンスを実行するために各デバイスでパスワードを手動で変更する必要があります。新しい Threat Defense Virtual デバイスをオンボー

ドする場合、Threat Defense Virtual パスワードは Lambda 環境変数から取得されます。「AWS Lambda 環境変数の使用」を参照してください。

### 登録 ID と NAT ID の変更

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

# アクセスポリシーと NAT ポリシーの変更

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

# AWS リソースに対する変更

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

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

# CloudWatch ログの収集および分析

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

# トラブルシューティング

### AWS CloudFormation コンソール

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

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

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

### Amazon CloudWatch ログ

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

Lambda コンソール、CloudWatch コンソール、AWS CLI、または CloudWatch API を使用して、Lambda のログを表示できます。ロググループと CloudWatch コンソールを介したロググループへのアクセスの詳細については、『*Amazon CloudWatch* ユーザーガイド（*Amazon CloudWatch User Guide*）』でモニターリングシステム、アプリケーション、およびカスタムログファイルについて参照してください。

### ロードバランサのヘルスチェックの失敗

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

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

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

### トラフィックの問題

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

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

### Management Center への接続に失敗

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

### デバイスが FMC への登録に失敗 Management Center

デバイスが Management Center に登録できない場合は、Management Center 構成に障害があるか到達不能であるか、または Management Center に新しいデバイスを収容するキャパシティがあ

るかどうかを判断する必要があります。『*Firepower Management Center Configuration Guide*』の「Add a Device to the FMC」を参照してください。

#### Threat Defense Virtual に SSH 接続できない

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

# 導入例：AWS で GWLB を使用して North-South トラフィックを検査する Threat Defense Virtual の Auto Scale ソリューション

これは、AWS 環境でゲートウェイロードバランサ（GWLB）を使用して Threat Defense Virtual インスタンスの Auto Scaling を設定し、North-South トラフィックを検査する方法を説明するユースケースドキュメントです。

## AWS で GWLB を使用して North-South トラフィックを検査する Threat Defense Virtual Auto Scale ソリューションの設定方法

Auto Scale ソリューションを使用すると、トラフィック検査用にホストされている Threat Defense Virtual インスタンスのグループの展開、スケーリング、および管理ができます。トラフィックは、パフォーマンスまたは使用容量に応じて、単一または複数の Threat Defense Virtual インスタンスに分散されます。

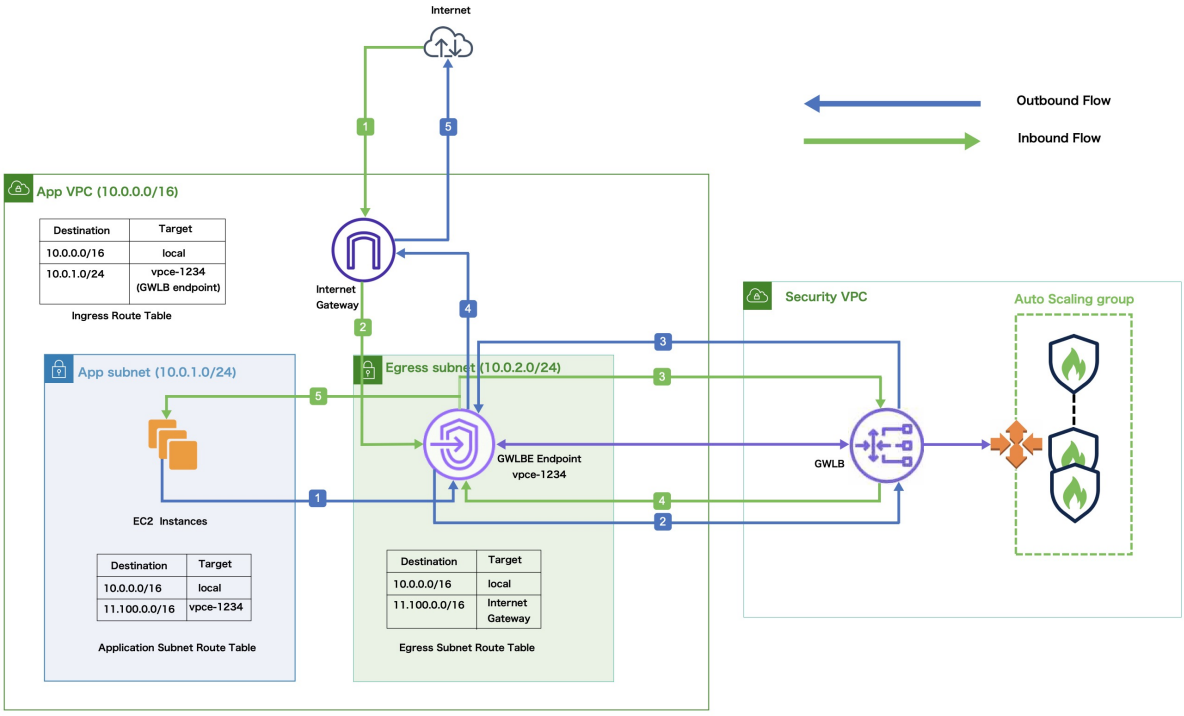
GWLB は、内部および外部で生成されたトラフィックを管理する単一のエントリおよびエグジットポイントとして機能し、トラフィック負荷に基づいて Threat Defense Virtual インスタンスの数をリアルタイムでスケールアップまたはスケールダウンします。

（注） この導入例で使用されているパラメータ値はサンプル値です。要件に応じて各値を変更します。

## トポロジの例

このトポロジの例は、インバウンドおよびアウトバウンドのネットワークトラフィックフローが GWLB を介して Threat Defense Virtual インスタンスに分散され、アプリケーション VPC にルーティングされてから、逆方向にルーティングされる方法を示しています。

図 *5 : GWLB* を使用した *Threat Defense Virtual Auto Scale* ソリューション



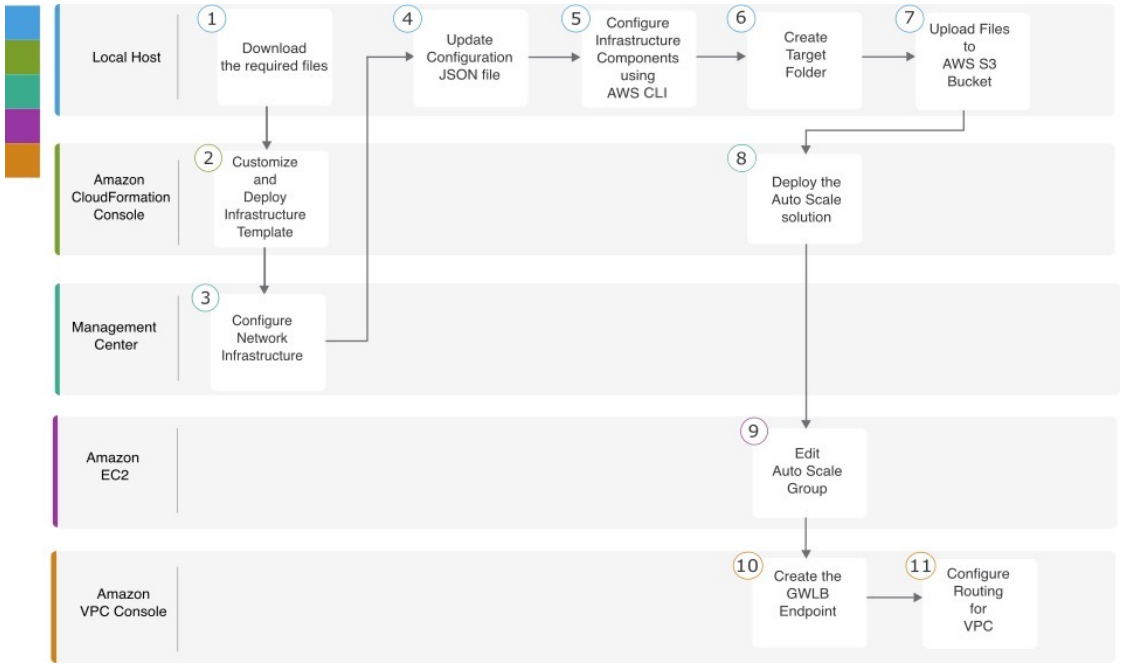

| インバウンドトラフィック検査 | |
|---|---|
| 1 | インターネットゲートウェイ（IGW）が、インターネットからトラフィックを受信します。 |
| 2 | トラフィックが、入力ルートテーブルのルートに従ってゲートウェイロードバランサのエンドポイント（GWLBe）にルーティングされます。 |
| 3 | GWLBeが、セキュリティ仮想プライベートクラウド（VPC）のエンドポイントサービスに接続されます。GWLBが受信したトラフィックをカプセル化し、検査のために Threat Defense Virtual Auto Scaling グループに転送します。 |
| 4 | Auto Scaling グループによって検査されたトラフィックが GWLB に返されてから GWLB エンドポイントに返されます。 |
| 5 | GWLBエンドポイントが、アプリケーションサブネット内のリソースにルーティングされるアプリケーション VPC にトラフィックを転送します。 |

| アウトバウンドトラフィック検査 | |
|---|---|
| 1 | アプリケーションサブネットリソースからのトラフィックが、同じVPC内のGWLBeにルーティングされます。 |

| アウトバウンドトラフィック検査 | |
|---|---|
| 2 | GWLBe が、セキュリティ VPC のエンドポイントサービスに接続されます。GWLB が受信したトラフィックをカプセル化し、検査のために Auto Scaling グループに転送します。 |
| 3 | Auto Scaling グループによって検査されたトラフィックが GWLB に返されてから GWLBe に返されます。 |
| 4 | 送信元 VPC に到着したトラフィックが、出力サブネットルートテーブルで定義されたルートに従って IGW に転送されます。 |
| 5 | IGW がトラフィックをインターネットに送信します。 |

# エンドツーエンドの手順

次のフローチャートは、Amazon Web Services（AWS）に GWLB を使用して Threat Defense Virtual Auto Scale ソリューション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 | 前提条件 |
| 2 | Amazon CloudFormation コンソール | Amazon CloudFormation コンソール：インフラストラクチャ テンプレートのカスタマイズと展開 |

| | ワークスペース | 手順 |
|---|---|---|
| 3 | Management Center | Management Center：Threat Defense Virtual の Management Center でのネットワーク インフラストラクチャの設定 |
| 4 | ローカルホスト | ローカルホスト：設定 JSON ファイルの更新 |
| 5 | ローカルホスト | ローカルホスト：ローカルホストでの AWS CLI を使用したインフラストラクチャ コンポーネントの設定 |
| 6 | ローカルホスト | ローカルホスト：target フォルダの作成 |
| 7 | ローカルホスト | ローカルホスト：Amazon S3 バケットへの AWS GWLB Auto Scale ソリューション展開ファイルのアップロード |
| 8 | Amazon CloudFormation コンソール | Amazon CloudFormation コンソール：GWLB を使用した Threat Defense Virtual の Auto Scale ソリューションの展開 |
| 9 | Amazon EC2 コンソール | Amazon EC2 コンソール：Auto Scale グループのインスタンス数の編集 |
| 10 | Amazon VPC コンソール | GWLB エンドポイントの作成 |
| 11 | Amazon VPC コンソール | カスタマー VPC のルーティングの設定 |

# 前提条件

- GitHub から **lambda-python-files** フォルダをダウンロードします。このフォルダには、次のファイルが含まれています。
  - Lambda レイヤの作成に使用される Python（.py）ファイル。
  - 必要に応じて、スタティックルートを追加し、ネットワークパラメータをカスタマイズするために使用される configuration.json ファイル。
- GitHub から次の CloudFormation テンプレートをダウンロードします。
  - **Infrastructure_gwlb.yaml**：AWS 環境のコンポーネントをカスタマイズするために使用されます。
  - **deploy_ngfw_autoscale_with_gwlb.yaml**：GWLB ソリューションを使用して AWS Auto Scale を展開するために使用されます。
- （任意）可能な場合は、テンプレートパラメータの値を収集します。収集すると、AWS 管理コンソールでテンプレートを展開するときに、値をすばやく簡単に入力できます。

# Amazon CloudFormation コンソール：インフラストラクチャ テンプレートのカスタマイズと展開

インフラストラクチャテンプレートをカスタマイズして展開するには、この項に記載されている手順を実行します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]**の順に選択し、**[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 2** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose file）] をクリックして、ファイルをダウンロードしたフォルダから **infrastructure_gwlb.yaml** を選択します。

**ステップ 3** [次へ（Next）] をクリックします。

**ステップ 4** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 5** ***Infrastructure_gwlb.yaml*** テンプレートの入力パラメータの値を指定します。

| パラメータ | 値 |
|---|---|
| **ポッドの設定** | |
| ポッド名 | *infrastructure* |
| ポッド番号 | 1 |
| S3 バケット名 | demo-us-bkt |
| VPC CIDR | 20.0.0.0/16 |
| 可用性ゾーンの数 | 2 |
| ListOfAzs（可用性ゾーンのリスト） | us-west-1a,us-west-1b |
| 管理サブネットの名前 | MgmtSubnet-1,MgmtSubnet-2 |
| MgmtSubnetCidrs | 20.1.250.0/24,20.1.251.0/24 |
| 内部サブネットの名前 | InsideSubnet-1,InsideSubnet-2 |
| InsideSubnetCidrs | 20.1.100.0/24,20.1.101.0/24 |
| 外部サブネットの名前 | OutsideSubnet-1,OutsideSubnet-2 |
| OutsideSubnetCidrs | 20.1.200.0/24,20.1.201.0/24 |
| Lambda サブネットの名前 | LambdaSubnet-1,LambdaSubnet-2 |
| Lambda サブネット CIDR | 20.1.50.0/24,20.1.51.0/24 |

**ステップ 6** [次へ（Next）] をクリックします。

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして **infrastructure_gwlb.yaml** テンプレートを展開し、スタックを作成します。

**ステップ 10** 展開が完了したら [出力（Outputs）] に移動し、**S3 バケット名**を書き留めます。

# Management Center：Threat Defense Virtual の Management Center でのネットワーク インフラストラクチャの設定

登録済み Threat Defense Virtual の Management Center で、オブジェクト、デバイスグループ、ヘルスチェックポート、およびアクセスポリシーを作成および設定します。

## ホストオブジェクトの作成

**ステップ 1** Management Center にログインします。

**ステップ 2** **[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 3** オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

**ステップ 4** [ネットワークを追加（Add Network）] ドロップダウン メニューで、[オブジェクトの追加（Add Object）] を選択します。

**ステップ 5** [名前（Name）]：*aws-metadata-server* と入力します。

**ステップ 6** 説明を入力します。

**ステップ 7** [ネットワーク（Network）] フィールドで [ホスト（Host）] オプションを選択し、IPv4 アドレス：*169.254.169.254* を入力します。

**ステップ 8** [保存（Save）] をクリックします。

## ポートオブジェクトの作成

**ステップ 1** Management Center にログインします。

**ステップ 2** **[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 3** オブジェクト タイプのリストから [ポート（Port）] を選択します。

**ステップ 4** [ポートの追加（Add Port）] ドロップダウンメニューで、[オブジェクトの追加（Add Object）] を選択します。

**ステップ 5** [名前（Name）]：*test-port-object* と入力します。

**ステップ 6** [プロトコル（Protocol）] を選択します。[ホスト（Host）] オブジェクトタイプに入力したプロトコルを選択する必要があります。選択したプロトコルに応じて、[ポート（Port）] で制限します。

**ステップ 7** *8080* と入力します。ここで入力するポート番号は、要件に応じてカスタマイズできます。

（注） [すべて（All）] のプロトコルと一致させることを選択した場合は、[その他（Other）] ドロップダウン リストを使用して、ポートでオブジェクトを制限する必要があります。

**ステップ 8** [保存（Save）] をクリックします。

## セキュリティゾーンおよびインターフェイス グループ オブジェクトの作成

**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）]** の順にクリックするか、**[追加（Add）] > [インターフェイスグループ（Interface Group）]** の順にクリックします。

**ステップ 4** [名前（Name）] : *inside-sz/outside-sz* と入力します。

**ステップ 5** [インターフェイスタイプ（Interface Type）] : [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追加

Management Center を使用すると、デバイスをグループ化して、複数のデバイスへのポリシーの展開や更新のインストールを簡単に実行できます。グループに属するデバイスのリストは、展開または縮小表示できます。

**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。

**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** 既存のグループを編集するには、編集するグループの [編集（Edit）]（編集アイコン）をクリックします。

**ステップ 4** [名前（Name）] : *aws-ngfw-autoscale-dg* と入力します。

**ステップ 5** [使用可能なデバイス（Available Devices）] から、デバイス グループに追加するデバイスを 1 つ以上選択します。複数のデバイスを選択する場合は、Ctrl または Shift を押しながらクリックします。

**ステップ 6** [追加（Add）] をクリックして、選択したデバイスをデバイス グループに追加します。

**ステップ 7** [OK] をクリックして、デバイス グループを追加します。

## ヘルスチェックプローブのポート 443（HTTP）の有効化

ヘルスチェックプローブにポート 443（HTTP）を使用している場合は、次の手順を実行して、ヘルスチェックプローブのポートを有効にします。

**ステップ 1** **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[HTTPアクセス（HTTP Access）]** の順に選択します。

**ステップ 2** [HTTPサーバーの有効化（Enable HTTP Server）] チェックボックスをオンにします。

**ステップ 3** [ポート（Port）] フィールドに、**443** と入力します。

**ステップ 4** **[+ Add]** をクリックします。

**ステップ 5** ドロップダウンリストから関連する [IPアドレス（IP Address）] を選択します。

**ステップ 6** [使用可能なゾーン/インターフェイス（Available Zones/Interfaces）] ウィンドウで、GWLB または外部サブネットに接続されている外部インターフェイスを選択します。

**ステップ 7** [追加（Add）] をクリックして、選択したインターフェイスを [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] ウィンドウに追加します。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [保存（Save）] をクリックします。

## 基本的なアクセス コントロール ポリシーの作成

新しいアクセス コントロール ポリシーを作成すると、そのポリシーにデフォルトのアクションと設定が含まれます。ポリシーを作成すると、要件に合わせてポリシーを調整できるよう、すぐに編集セッションに移行します。

**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** 一意の名前（aws-access-policy）と説明を入力します。

**ステップ 4** 最初の [デフォルトアクション（Default Action）] : [すべてのトラフィックをブロック（Block all traffic）] を指定します。

**ステップ 5** [保存（Save）] をクリックします。

**ステップ 6** 作成した新しいポリシーの [編集（Edit）] アイコンをクリックします。

**ステップ 7** [ルールの追加（Add Rule）] をクリックします。

**ステップ 8** 次のパラメータを設定します。

- 名前：inside-to-outside
- 挿入：into Mandatory
- アクション：Allow
- 送信元ゾーンと宛先ゾーンを追加します。

**ステップ 9** [適用（Apply）] をクリックします。

# ローカルホスト：設定 JSON ファイルの更新

**configuration.json** ファイルは、GitHub からダウンロードした **lambda_python_files** フォルダにあります。Management Center で設定したパラメータを使用して、**configuration.json** ファイルのパラメータを更新します。

configuration.json ファイル内のスクリプトは次のとおりです。

```
"licenseCaps": ["BASE", "MALWARE", "THREAT"],   // Management center virtual licenses
  "fmcIpforDeviceReg": "DONTRESOLVE",   // Management center virtual IP address
  "RegistrationId": "cisco",  // Registration ID used while configuring the manager in
the Threat defense virtual
  "NatId": "cisco",  // NAT ID used while configuring the manager in the Threat defense
 virtual
  "fmcAccessPolicyName": "aws-access-policy",  // Access policy name configured in the
Management center virtual
  "fmcInsideNicName": "inside", //Threat defense virtual inside interface name
  "fmcOutsideNicName": "outside", //Threat defense virtual outside interface name
  "fmcInsideNic": "GigabitEthernet0/0", // Threat defense virtual inside interface NIC
Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance
types)
  "fmcOutsideNic": "GigabitEthernet0/1", // Threat defense virtual outside interface NIC
 Name - GigabitEthernet for c4 instance types, and TenGigabitEthernet for c5 instance
types
  "fmcOutsideZone": "Outside-sz", //Outside Interface security zone name that is set in
 the Management center virtual
  "fmcInsideZone": "Inside-sz", //Inside Interface security zone name that is set in the
 Management center virtual
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Inside-sz"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "Outside-sz"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],  // Interface-related configuration
  "trafficRoutes": [
    {
      "interface": "inside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "1"
    }
  ] // This traffic route is used for the Threat defense virtual instance's health check
}
```

# ローカルホスト：ローカルホストでの AWS CLI を使用したインフラストラクチャ コンポーネントの設定

テンプレートでは、Threat Defense Virtual および Management Center の Lambda レイヤと暗号化されたパスワードは作成されません。次の手順を使用して、各コンポーネントを設定します。AWS CLI の詳細については、「AWS コマンドラインインターフェイス」を参照してください。

**ステップ 1** Lambda レイヤ zip ファイルを作成します。

Linux ホストに Python フォルダを作成し、Lambda レイヤを作成します。

a) Linux ホストに Python フォルダ（Ubuntu 22.04 など）を作成します。

b) Linux ホストに Python 3.9 をインストールします。以下に、Python 3.9 をインストールするためのサンプルスクリプトを示します。

```
$ sudo apt update
$ sudo apt install software-properties-common
$ sudo add-apt-repository ppa:deadsnakes/ppa
$ sudo apt install python3.9
$ sudo apt install python3-virtualenv
$ sudo apt install zip
$ sudo apt-get install python3.9-distutils
$ sudo apt-get install python3.9-dev
$ sudo apt-get install libffi-dev
```

c) Linux 環境で Lambda レイヤ zip ファイル（autoscale_layer.zip）を作成します。このファイルは、Lambda 関数に不可欠な Python ライブラリを提供します。

次のスクリプトを実行して、autoscale_layer.zip ファイルを作成します。

```
#!/bin/bash
mkdir -p layer
mkdir -p python
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install attrs==23.1.0
pip3 install bcrypt==3.2.2
pip3 install certifi==2022.12.7
pip3 install cffi==1.15.1
pip3 install chardet==3.0.4
pip3 install cryptography==2.9.1
pip3 install idna==2.10
pip3 install jsonschema==3.2.0
pip3 install paramiko==2.7.1
pip3 install pycparser==2.21
pip3 install pycryptodome==3.15.0
pip3 install PyNaCl==1.5.0
pip3 install pyrsistent==0.19.3
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install six==1.16.0
pip3 install urllib3==1.25.11
echo "Copy from ./layer directory to ./python\n"
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r autoscale_layer.zip ./python
```

d) **autoscale_layer.zip** ファイルを作成したら、GitHub からダウンロードした **lambda-python-files** フォルダに **autoscale_layer.zip** ファイルをコピーします。

**ステップ 2** （任意）Threat Defense Virtual および Management Center の暗号化パスワードを作成します。

Infrastructure_gwlb.yaml テンプレートファイルに KMS ARN 値が入力されている場合は、Threat Defense Virtual および Management Center で設定するパスワードを暗号化する必要があります。AWS KMS コンソールを使用してキー ARN を特定するには、Finding the key ID and key ARN [英語] を参照してください。ローカルホストで、次の AWS CLI コマンドを実行してパスワードを暗号化します。

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

`CiphertextBlob` の値は暗号化されたパスワードです。このパスワードは、`infrastructure_gwlb.yaml` ファイルの **NGFWv パスワード**（Threat Defense Virtual パスワード）または Auto Scale 自動化の FMC パスワード（Management Center パスワード）パラメータの値として使用します。このパスワードは、**CloudWatch にメトリックを公開するための FMC パスワード**の値としても使用できます。

# ローカルホスト：target フォルダの作成

次のコマンドを使用して、Amazon S3 バケットにアップロードする必要があるファイルを含む target フォルダを作成します。

**python3 make.py build**

ローカルホストに「target」という名前のフォルダが作成されます。target フォルダには、Auto Scale ソリューションの展開に必要な zip ファイルと yaml ファイルが含まれています。

# ローカルホスト：Amazon S3 バケットへの AWS GWLB Auto Scale ソリューション展開ファイルのアップロード

次のコマンドを使用して、target ディレクトリにあるすべてのファイルを Amazon S3 バケットにアップロードします。

**$ cd ./target**

**$ aws s3 cp . s3://demo-us-bkt --recursive**

# Amazon CloudFormation コンソール：GWLB を使用した Threat Defense Virtual の Auto Scale ソリューションの展開

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[管理とガバナンス（Management and Governance）]** > **[CloudFormation]** > **[スタック（Stacks）]**の順に選択し、テンプレートによって作成されたスタックをクリックします。

**ステップ 2** **[スタックの作成（Create stack）]** > **[新しいリソースを使用（標準）（With new resources (standard)）]**の順にクリックします。

**ステップ 3** [テンプレートファイルのアップロード（Upload a template file）] を選択し、[ファイルの選択（Choose File）] をクリックして、target フォルダから ***deploy_ngfw_autoscale_with_gwlb.yaml*** を選択します。

**ステップ 4** [次へ（Next）] をクリックします。

**ステップ 5** [スタックの詳細の指定（Specify stack details）] ページで、スタックの名前を入力します。

**ステップ 6** ***deploy_ngfw_autoscale_with_gwlb.yaml*** テンプレートの入力パラメータの値を指定します。

スタック名：Threat-Defense-Virtual

| パラメータ | 値 |
|---|---|
| **ポッドの設定** | |
| Auto Scale グループ名プレフィックス | NGFWv-AutoScale |
| ポッド番号 | *1* |
| Auto Scale 電子メール通知 | username@cisco.com |
| **インフラストラクチャの詳細** | |
| VPC ID | vpc-05277f76370396df4 |
| S3 バケット名 | demo-us-bkt |
| Lambda 関数のサブネット | subnet-0f6bbd4de47d50c6b,subnet-0672f4c24156ac443 |
| Lambda 関数のセキュリティグループ | sg-023dfadb1e7d4b87e |
| 可用性ゾーンの数 | *2* |
| 可用性ゾーン | us-west-1a, us-west-1b |
| NGFWv 管理インターフェイスのサブネットリスト | subnet-0e0bc4961de87b170 |
| NGFWv 内部インターフェイスのサブネットリスト | subnet-0f6acf3b548d9e95b |
| NGFWv 外部インターフェイスのサブネットリスト | subnet-0cc7ac70df7144b7e |
| **GWLB の設定** | |

| パラメータ | 値 |
|---|---|
| NGFWv インスタンスのヘルスチェック用のポートを入力 | *22* |
| **Cisco NGFWv インスタンスの設定** | |
| NGFWv インスタンスタイプ | *C4.xlarge* |
| NGFWv インスタンス ライセンス タイプ | *BYOL* |
| AWS IP プールからの NGFWv のパブリック IP の割り当て | *true* |
| NGFWv インスタンスのセキュリティグループ | sg-088ae4bc1093f5833 |
| 内部の NGFWv インスタンスのセキュリティグループ | sg-0e0ce5dedcd9cd4f3 |
| 外部の NGFWv インスタンスのセキュリティグループ | sg-07dc50ff47d0c8126 |
| NGFWv AMI-ID | ami-00faf58c7ee8d11e1 |
| KMS マスターキー ARN（条件付き） | |
| NGFWv パスワード | W1nch3sterBr0s |
| **FMC 自動化の設定** | |
| FMC ホスト IP アドレス | 3.38.137.49 |
| Auto Scale 自動化の FMC ユーザー名 | autoscaleuser |
| Auto Scale 自動化の FMC パスワード | W1nch3sterBr0s |
| FMC デバイスグループ名 | aws-ngfw-autoscale-dg |
| FMCv ライセンスのパフォーマンス階層の値 | *FTDv20* |
| **FMC デバイスグループメトリックの公開の設定** | |
| FMC からのカスタムメトリックの公開 | *TRUE* |
| CloudWatch にメトリックを公開するための FMC ユーザー名 | metricuser |
| CloudWatch にメトリックを公開するための FMC パスワード | W1nch3sterBr0s |
| **スケーリングの設定** | |
| 下限および上限 CPU しきい値 | *10,70* |

| パラメータ | 値 |
|---|---|
| 下限および上限メモリしきい値 | 40、70 |

**ステップ 7** [スタックオプションの設定（Configure Stack Options）] ウィンドウで [次へ（Next）] をクリックします。

**ステップ 8** [確認（Review）] ページで設定を確認して確定します。

**ステップ 9** [スタックの作成（Create Stack）] をクリックして ***deploy_ngfw_autoscale_with_gwlb.yaml*** テンプレートを展開し、スタックを作成します。

これで、GWLB を使用して Threat Defense Virtual 用の Auto Scale ソリューションを設定するために必要な両方のテンプレートの展開が完了しました。

# Amazon EC2 コンソール：Auto Scale グループのインスタンス数の編集

デフォルトでは、Auto Scale グループの Threat Defense Virtual インスタンスの最小数と最大数はそれぞれ 0 と 2 に設定されています。要件に応じて各値を変更します。

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[コンピューティング（Compute）]** > **[EC2]**の順に選択し、[Auto Scalingグループ（Auto Scaling Groups）] をクリックします。

**ステップ 2** 作成したAuto Scalingグループを選択し、[編集（Edit）]をクリックして、要件に応じて[必要な容量（Desired capacity）]、[最小容量（Minimum capacity）]、[最大容量（Maximum capacity）] フィールドの値を変更します。各値は、Auto Scaling 機能のために起動する Threat Defense Virtual インスタンスの数に対応します。[必要な容量（Desired capacity）] を、最小容量値と最大容量値の範囲内の値に設定します。

**ステップ 3** **[更新（Update）]**をクリックします。

（注） Threat Defense Virtual インスタンスを 1 つだけ起動し、そのインスタンスが想定どおりに動作しているか確認することを推奨します。その後、要件に応じて追加のインスタンスを起動できます。

# Amazon VPC ダッシュボードコンソール：GWLB エンドポイントの作成およびカスタマー VPC のルーティングの設定

両方の CloudFormation テンプレートを展開後、GWLB エンドポイントを作成し、カスタマー VPC のルーティングを設定する必要があります。

## GWLB エンドポイントの作成

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[ネットワーキングおよびコンテンツ配信（Networking & Content Delivery）]** > **[VPC]** > **[エンドポイントサービス（Endpoint Services）]**の順に選択します。

**ステップ 2** [エンドポイントサービスの作成（Create Endpoint Service）] をクリックします。

**ステップ 3** [ロードバランサタイプ（Load balancer type）] で [ゲートウェイ（Gateway）] を選択します。

**ステップ 4** [使用可能なロードバランサ（Available load Balancers）] で、Auto Scale の展開の一部として作成されたゲートウェイロードバランサを選択します。

**ステップ 5** [作成（Create）] をクリックします。

**ステップ 6** 新たに作成したエンドポイントサービスのサービス名をコピーします。

**ステップ 7** **[サービス（Services）]** > **[ネットワーキングおよびコンテンツ配信（Networking & Content Delivery）]** > **[VPC]** > **[エンドポイント（Endpoints）]**の順に選択します。

**ステップ 8** [エンドポイントの作成（Create endpoint）] をクリックします。

**ステップ 9** [サービスカテゴリ（Service category）] で [その他のエンドポイントサービス（Other endpoint services）] を選択します。

**ステップ 10** [サービス名（Service name）] にサービスの名前を入力し、[サービスの確認（ Verify service）] を選択します。

**ステップ 11** [VPC] フィールドで、エンドポイントを作成する VPC、[アプリケーションVPC（App VPC）] を選択します。

**ステップ 12** [サブネット（Subnets）] で、エンドポイントを作成するサブネット、[出力サブネット（Egress subnet）] を選択します。

**ステップ 13** [IPアドレスタイプ（IP address type）] で [IPv4] オプションを選択して、エンドポイント ネットワーク インターフェイスに IPv4 アドレスを割り当てます。

**ステップ 14** [エンドポイントの作成（Create endpoint）] をクリックします。

**ステップ 15** **[サービス（Services）]** > **[ネットワーキングおよびコンテンツ配信（Networking & Content Delivery）]** > **[VPC]** > **[エンドポイントサービス（Endpoint services）]**の順に選択し、[エンドポイント接続（Endpoint Connections）] タブをクリックし、事前に作成した [エンドポイントID（Endpoint ID）] を選択して、[アクション（Actions）] > [エンドポイント接続要求の受け入れ（Accept endpoint connection request）] の順にクリックします。

## カスタマー VPC のルーティングの設定

**ステップ 1** AWS 管理コンソールで、**[サービス（Services）]** > **[ネットワーキングおよびコンテンツ（Networking & Content）]** > **[仮想プライベートクラウド（Virtual Private Cloud）]** > **[ルートテーブル（Route tables）]**の順に選択します。

**ステップ 2** 入力ルートテーブルを作成し、次の手順を実行します。

1. **[アクション（Actions）]** > **[ルートの編集（Edit routes）]**の順にクリックします。

2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、アプリケーションサーバーのサブネットの IPv4 CIDR ブロック（10.0.1.0/24）を入力します。[ターゲット（Target）] で、VPC エンドポイントを選択します。
3. [変更の保存（Save Changes）] をクリックします。
4. [エッジの関連付け（Edge Associations）] タブで [エッジの関連付けの編集（Edit edge associations）] をクリックし、[インターネットゲートウェイ（Internet gateway）] を選択します。
5. [変更の保存（Save Changes）] をクリックします。

**ステップ 3** アプリケーションサーバーがあるサブネットのルートテーブルを選択し、次の手順を実行します。

1. **[アクション（Actions）] > [ルートの編集（Edit routes）]**の順にクリックします。
2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、**0.0.0.0/0** と入力します。[ターゲット（Target）] で、VPC エンドポイントを選択します。
3. [変更の保存（Save Changes）] をクリックします。

**ステップ 4** ゲートウェイロードバランサのエンドポイントがあるサブネットのルートテーブルを選択し、次の手順を実行します。

1. **[アクション（Actions）] > [ルートの編集（Edit routes）]**の順にクリックします。
2. IPv4 の場合は、[ルートの追加（Add route）] をクリックします。[宛先（Destination）] に、**0.0.0.0/0** と入力します。[ターゲット（Target）] で、インターネットゲートウェイを選択します。
3. [変更の保存（Save Changes）] をクリックします。

# Amazon CloudWatch：展開の検証

テンプレートの展開が成功したら、Amazon CloudWatch コンソールに移動して、ログが収集され、必要なアラームが作成されていることを確認します。

## ログ

ログファイルを確認して、Management Center の接続に関する問題をトラブルシューティングします。

**ステップ 1** **AWS 管理**コンソールで、**[サービス（Services）] > [管理とガバナンス（Management and Governance）] > [CloudWatch]**の順に選択します。

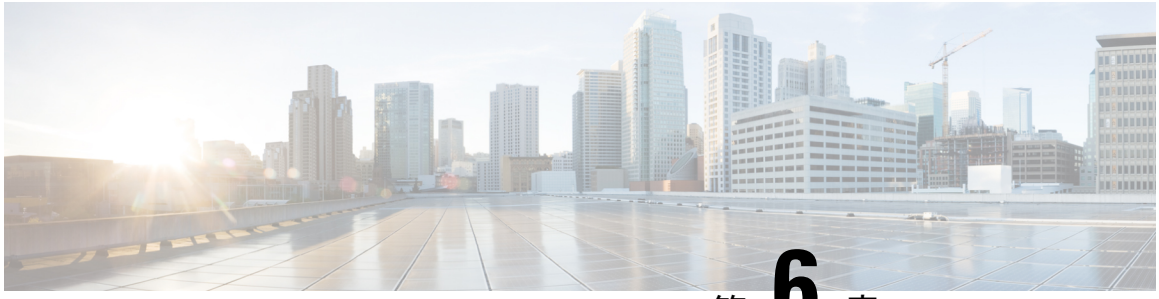
**ステップ 2** [ロググループ（Log groups）] をクリックし、表示されているいずれかのロググループをクリックしてログを表示します。

# アラーム

必要なアラームが Amazon CloudWatch コンソールで作成されていることを確認します。

**ステップ 1** **AWS 管理**コンソールで、**[サービス（Services）] > [管理とガバナンス（Management and Governance）] > [CloudWatch]**の順に選択します。

**ステップ 2** **[アラーム（Alarms）] > [すべてのアラーム（All Alarms）]**の順にクリックして、スケールアウトおよびスケールイン機能をトリガーする条件とともにアラームのリストを表示します。



第 6 章

# Azure での Threat Defense Virtual の展開

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


- 概要 （182 ページ）
- 前提条件 （182 ページ）
- 注意事項と制約事項 （183 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （187 ページ）
- Azure 上の Threat Defense Virtual のネットワークトポロジの例 （188 ページ）
- 導入時に作成されるリソース （188 ページ）
- Accelerated Networking（AN） （190 ページ）
- Azure ルーティング （191 ページ）
- 仮想ネットワーク内の VM のルーティング設定 （191 ページ）
- IP アドレス （192 ページ）
- Threat Defense Virtual の導入 （193 ページ）
- エンドツーエンドの手順 （193 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 （195 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 （199 ページ）
- Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開について （203 ページ）
- Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開のガイドラインと制限事項 （204 ページ）
- Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開におけるデータインターフェイスへの NIC マッピング （204 ページ）
- Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開 （205 ページ）
- アップグレードのシナリオ （207 ページ）
- 診断インターフェイスを使用しない Threat Defense Virtual クラスタまたは Auto Scale ソリューションの展開 （208 ページ）
- トラブルシューティング （208 ページ）
- Azure での Threat Defense Virtual の Auto Scale ソリューション （208 ページ）
- Azure Virtual WAN への Cisco Secure Firewall Threat Defense Virtual の展開 （257 ページ）

- Azure での IPv6 サポート対象 Secure Firewall Threat Defense Virtual の展開 （278 ページ）
- Azure での IPv6 をサポートする展開について （278 ページ）
- Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （280 ページ）
- VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開 （287 ページ）
- Threat Defense Virtualイメージスナップショット （292 ページ）


# 概要

Secure Firewall 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、4vNIC（**バージョン 7.1 の新機能**）

# 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。

  Threat Defense Virtual のライセンス。ヘルプリンクをはじめとしたファイアウォールシステムで使用できる機能ライセンスの概要については、『Cisco Secure Firewall Management Center 機能ライセンス』を参照してください。

- Threat Defense Virtual とシステムの互換性については、『Threat Defense Virtual Compatibility Guide 』を参照してください。

### 通信パス

- 管理インターフェイス：Threat Defense Virtual を Secure Firewall 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 Management Center 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。Management Center にアクセスするための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、『Cisco Secure Firewall Threat Defense コマンドリファレンス』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）：内部ホストに Threat Defense Virtual を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）：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。

# 注意事項と制約事項

### 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。
  - Secure Firewall Management Center を使用して Threat Defense Virtual を管理することができます。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）」を参照してください。
  - 統合 Secure Firewall デバイスマネージャ を使用して Threat Defense Virtual を管理することができます。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 （455 ページ）」を参照してください
- クラスタリング（バージョン 7.3 以降）。詳細については、『パブリッククラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。
- 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。

- IPv6

  IPv6 をサポートする Threat Defense Virtual を展開する際に考慮する必要があるガイドラインと制限事項を、以下に示します。

  - IPv6 サポートのために Azure CLI メソッドを使用してプログラムによる展開オプションを有効にする場合、Threat Defense Virtual インスタンスの事前導入は必要ありません。
  - IPV4 から IPV6 アドレッシングに手動でアップグレードしたものと同じ Vnet に、Azure Marketplace から Threat Defense Virtual を追加することはできません。

- インターフェイス:
  - Threat Defense Virtual 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 Threat Defense Virtual を展開できます。
  - Threat Defense Virtual 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。
  - Threat Defense Virtual 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（Management Center または Device Manager ）のコンフィギュレーション ガイドを参照してください。

### ライセンシング

- 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 Threat Defense Virtual を実行できる従量制課金モデル。登録された PAYG Threat Defense Virtual 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、Management Center 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、Device Manager モードで展開されている Threat Defense Virtual デバイスではサポートされていません。

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Secure Firewall Management Center Administration Guide』の「Licensing」の章を参照してください。

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual 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 *19 : Threat Defense Virtual* 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 |

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「Azure での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」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
  - 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 Threat Defense Virtual 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 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。唯一の方法は、新しい Threat Defense Virtual VM を展開することです。
- 高可用性（アクティブ/スタンバイ）
- VM のインポート/エクスポート
- Azure での Gen 2 VM の生成
- 展開後の VM のサイズ変更
- VM の OS ディスクの Azure ストレージ SKU を Premium から Standard SKU に移行または更新、およびその逆
- Device Manager ユーザーインターフェイス（バージョン 6.4 以前）

### Azure DDoS 防御機能

Microsoft Azure の Azure DDoS Protection は、Threat Defense Virtual の最前線に実装された追加機能です。仮想ネットワークでこの機能を有効にすると、ネットワークで予想されるトラフィックの 1 秒あたりのパケット数に応じて、一般的なネットワーク層攻撃からアプリケーションを保護するのに役立ちます。この機能は、ネットワーク トラフィック パターンに基づいてカスタマイズできます。

Azure DDoS Protection 機能の詳細については、『Azure DDoS Protection Standard overview』[英語] を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、お

よび読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。

- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

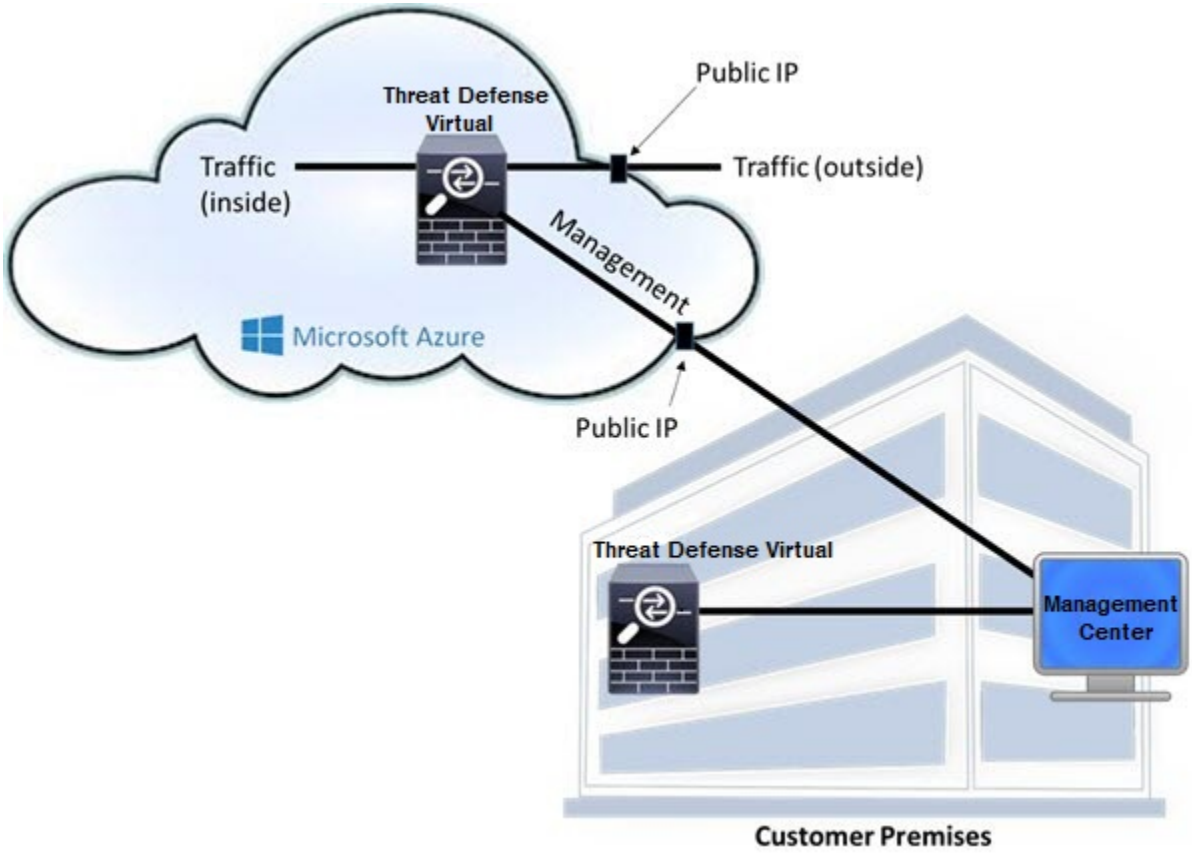
Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# Azure 上の Threat Defense Virtual 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 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 Secure Firewall Threat Defense Virtual を展開すると、次のリソースが作成されます。

- Threat Defense Virtual マシン（VM）
- リソースグループ
  - Threat Defense Virtual は常に新しいリソースグループに配置されます。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）

（注） 要件に基づいて、IPv4 のみまたはデュアルスタック（IPv4 および IPv6 が有効）で VNet を作成できます。

これらの NIC は、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）

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

  このセキュリティグループには、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、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。

### ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更

を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

# 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（IPv4：0.0.0.0/0 または IPv6：[::/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。

Azure Routing 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 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（IPv4）または [::/0]（IPv6）のデフォルトルートを 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 テーブル内の既存の限定的なルートのために、ユーザー定義のルーティングテーブルに、ネクストホップとして Threat Defense Virtual を指す限定的なルートを追加する必要があります。追加しないと、ユーザー定義の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 テーブル内のより限定的なルートが選択され、トラフィックは Threat Defense Virtual をバイパスします。

# 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 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。

- 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。

  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、『Public IP addresses』 [英語] を参照してください。

- 仮想マシンスケールセット（VMSS）の Threat Defense Virtual アプライアンスに接続されているネットワーク インターフェイスで [IP転送（IP Forwarding）] を有効にすることができます。ネットワークトラフィックの宛先がネットワーク インターフェイスで設定されている IP アドレスのいずれでもない場合、このオプションを有効にすると、そのようなネットワークトラフィックが仮想マシンで設定されている IP アドレス以外の他の IP アドレスに転送されます。ネットワーク インターフェイスで IP 転送を有効にする方法については、Azure のドキュメント「Enable or disable IP forwarding」を参照してください。

- パブリック IP アドレス（IPv4 および IPv6）はダイナミックアドレスであるため、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 の再起動時および Threat Defense Virtual のリロード時には保持されます。IPv6 パブリック IP アドレスの標準規格 [英語] を参照してください。

- 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。

- Threat Defense Virtual インターフェイスは、DHCP を使用して自身の IP アドレスを設定できます。Azure インフラストラクチャは、Azure に設定された IP アドレスが確実に Threat Defense Virtual インターフェイスに割り当てられるようにします。

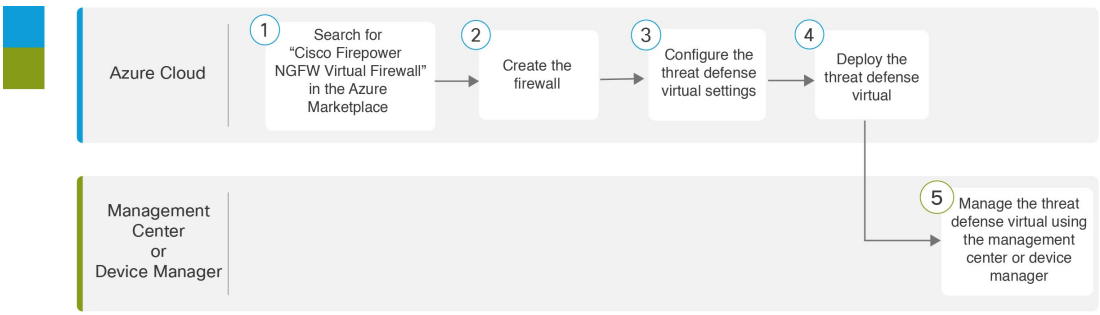
# Threat Defense Virtual の導入

テンプレートを使用して、Azure に Threat Defense Virtual 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 Threat Defense Virtual 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 （195 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 Threat Defense Virtual 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 Threat Defense Virtual 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 （199 ページ）」を参照してください。

# エンドツーエンドの手順

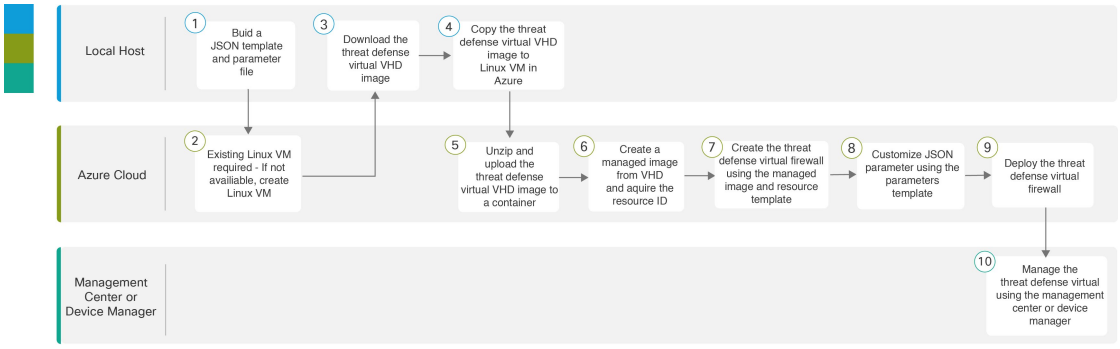
次のフローチャートは、ソリューションテンプレートを使用して Microsoft Azure に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Azure Cloud | ソリューションテンプレートを使用した 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。 |

| | ワークスペース | 手順 |
|---|---|---|
| 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：Threat Defense Virtual を設定します。 |
| 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：Threat Defense Virtual を展開します。 |
| 5 | Management Center またはDevice Manager | Threat Defense Virtual を管理します。<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

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 Threat Defense Virtual を展開する際の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。<br>• Azure CLI による Linux 仮想マシンの作成<br>• 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：シスコのソフトウェア ダウンロード ページから Threat Defense Virtual VHD イメージをダウンロードします。 |

| | ワークスペース | 手順 |
|---|---|---|
| 4 | ローカルホスト | VHD およびリソーステンプレートを使用した Azure からの展開：Azure の Linux VM に Threat Defense Virtual 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：Threat Defense Virtual 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 Threat Defense Virtual 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：Threat Defense Virtual ファイアウォールを展開します。 |
| 10 | Management Center または Device Manager | Threat Defense Virtual を管理します。<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

# 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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual を導入すると、リソース、パブリック IP アドレス（IPv4 および IPv6）、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 （199 ページ）」を参照してください。

**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 (Threat Defense Virtual)」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、Management Center を使用して Threat Defense Virtual を管理する場合にのみ使用できます。

c) Threat Defense Virtual 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) Threat Defense Virtual 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) [FTDv管理（FTDv Management）] ドロップダウンリストから、Threat Defense Virtual を登録する Management Center を選択します。

[FMC: Firepower Management Center] をデバイスの Management Center として選択している場合は、次のオプションを使用してデバイスの Management Center を設定できます。

- [はい（Yes）] をクリックして、[FMC登録情報（FMC registration information）] を入力します。

1. [FMC IP] アドレスを入力します。

2. Threat Defense Virtual インスタンスを登録するための [FMC登録キー（FMC Registration Key）] を入力します。
3. （任意）インスタンスの登録時に使用される Management Center NAT ID を入力します。

g) クラスタとして展開する仮想マシンを使用している場合は、[はい（Day-0クラスタ構成を提供します）（Yes (provide day0 cluster configuration)）] をクリックして、基本的な Day-0 構成を作成して詳細を入力します。

- [Day-0クラスタ構成（Day0 cluster configuration）] フィールドに Day-0 構成の詳細を入力します。

  Azure の Day-0 構成の作成の詳細については、『Azure への Threat Defense Virtual クラスタの展開』ガイドの「Azure 向け Day-0 構成の作成」を参照してください。

  （注） 部分的な Day-0 構成（クラスタ構成）："Cluster": {...} OR "run_config": [...] の詳細のみ設定できます。

h) サブスクリプションを選択します。

i) 新しいリソースグループを作成します。

Threat Defense Virtual 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、Threat Defense Virtual 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。

j) 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（Threat Defense Virtual、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。

k) [OK] をクリックします。

**ステップ 5** Threat Defense Virtual 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。

VM でパブリック IPv6 アドレスを割り当てる必要がある場合は、IPv6 パブリック IP アドレスの標準規格 [英語] を参照してください。

d) DNS ラベルを追加します。

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

e) 仮想ネットワークを選択します。

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

IPv6 アドレッシングに仮想マシンが必要な場合は、仮想ネットワークでそれを有効にする必要があります。例：デフォルトでは、CIDR IPv6 アドレスは [ace:cab:deca::/48] です。

（注） IPv6 だけを使用して、仮想ネットワーク、サブネット、インターフェースなどを構築することはできません。デフォルトでは IPv4 が使用され、IPv6 も一緒に有効にできます。IPv6 の詳細については、Azure IPv6 の概要 [英語] を参照してください。

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

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

（注） 上記のサブネットについて、サブネットの作成中に IPv6 の設定が必要な場合は、IPv6 オプションを選択して、インターフェイスの IPv6 サブネットを構成します。

g) [パブリックインバウンドポート（mgmt.interface）（Public inbound ports (mgmt.interface)）] の入力を指定して、ポートをパブリック用に開くかどうかを示します。デフォルトでは、[なし（None）] が選択されています。

- Azure のデフォルトのセキュリティルールを使用してネットワーク セキュリティ グループを作成し、管理インターフェイスに接続するには、[なし（None）] をクリックします。このオプションを選択すると、同じ仮想ネットワーク内の送信元からのトラフィックと Azure ロードバランサからのトラフィックが許可されます。
- インターネットでアクセスするために開くインバウンドポートを表示および選択するには、[選択したポートを許可（Allow selected ports）] をクリックします。[インバウンドポートの選択（Select

Inbound Ports）] ドロップダウンリストから、次のいずれかのポートを選択します。デフォルトでは、**SSH（22）**が選択されています。

- SSH（22）
- SFTunnel（8305）
- HTTPS（443）

h) [OK] をクリックします。

**ステップ 6** 構成サマリを確認し、[OK] をクリックします。

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

導入時間は Azure によって異なります。Threat Defense Virtual 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、Secure Firewall Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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 Secure Firewall Device Manager を使用して Threat Defense Virtual を管理します。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 （455 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 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 Threat Defense Virtual 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

- Threat Defense Virtual 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。これらのファイルは、Github リポジトリからダウンロードできます。
- 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推奨します。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短縮されます。

  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、Threat Defense Virtual 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。

**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 Threat Defense Virtual 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)）] > [Cisco Secure Firewall Threat Defense Virtual]** の順に選択します。

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-7.1.0-92.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-7.1.0-92.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** Threat Defense Virtual 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-7.1.0-92.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。Threat Defense Virtual 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 yX7txxxxxxxx1dnQ== \
       --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。

- [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。
- [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。
- [リージョン（Region）]：VM が展開されるリージョンを選択します。
- [OSタイプ（OS type）]：OS タイプとして [Linux] を選択します。
- [VMの世代（VM generation）]：[世代1（Gen 1）] を選択します。

  （注） [世代2（Gen 2）] はサポートされていません。

- [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）]：要件に応じて、ドロップダウンリストから [Standard HDD]、[Standard SSD]、または [Premium SSD] を選択します。

  このイメージの展開用に予定している VM サイズを選択する場合は、選択したアカウントタイプがその VM サイズでサポートされていることを確認します。
- [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、データディスクを追加しないでください。

d) [作成（Create）] をクリックします。

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

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

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

Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。リソース ID は、この管理対象イメージから新しい Threat Defense Virtual 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、Threat Defense Virtual 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。テンプレートファイルについては、「Github」を参照してください。

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 Threat Defense Virtual パラメータファイルを参照します。テンプレートパラメータについては、「Github」を参照してください。
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 Threat Defense Virtual 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 Threat Defense Virtual の IP 設定を更新します。

# Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開について

Cisco Secure Firewall バージョン 7.3 以前では、Threat Defense Virtual は少なくとも 4 つのインターフェイス（1 つの管理インターフェイス、1 つの診断インターフェイス、2 つのデータインターフェイス）で展開されます。

Cisco Secure Firewall バージョン 7.4.1 以降では、診断インターフェイスを削除し、少なくとも 3 つのインターフェイス（1 つの管理インターフェイスと 2 つのデータインターフェイス）を備えた Threat Defense Virtual を展開できます。この機能により、同じインスタンスタイプに追加のデータインターフェイスを使用して Threat Defense Virtual を展開できます。たとえば、Standard D4_v2 VM インスタンスでは、1 つの管理インターフェイス、1 つの診断インターフェイス、および 6 つのデータインターフェイスを備えた Threat Defense Virtual を展開する代わりに、1 つの管理インターフェイスと 7 つのデータインターフェイスを備えた Threat Defense Virtual を展開できます。

この機能は、Azure 上の Threat Defense Virtual インスタンスの新しい展開でのみサポートされます。

（注） サポートされるインターフェイスの最大数は 8 であるため、Threat Defense Virtual を展開後に最大 5 つのインターフェイスを追加して、最大 8 つのインターフェイスを持つことができます。

# Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開のガイドラインと制限事項

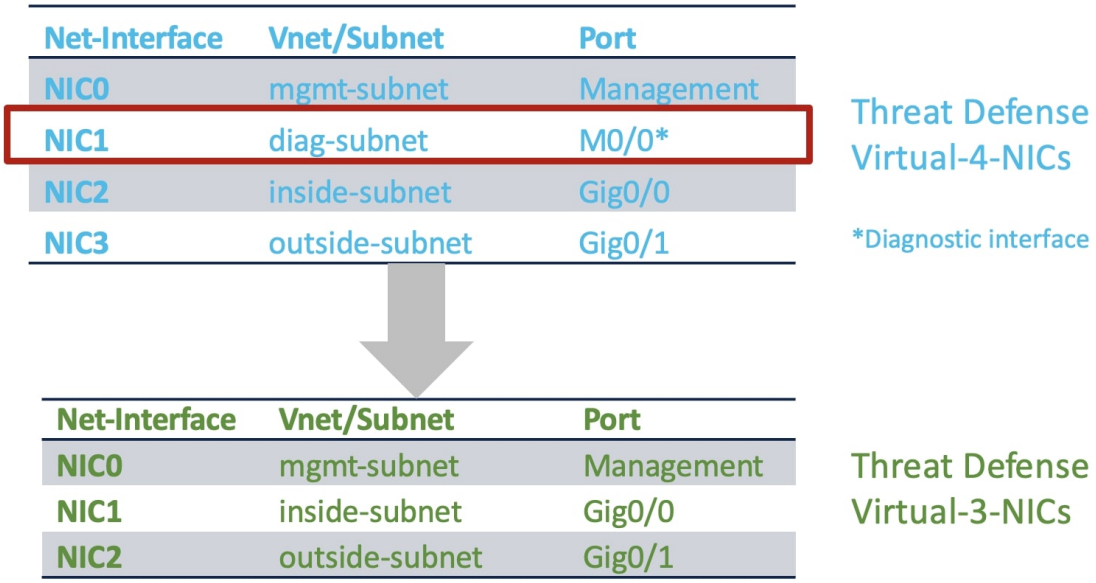
- 診断インターフェイスが削除されると、診断インターフェイスの代わりに Threat Defense Virtual 管理インターフェイスまたはデータインターフェイスを使用して syslog および SNMP がサポートされます。
- この展開では、クラスタリングと Auto Scale がサポートされています。
- 診断インターフェイスポートを持つ Threat Defense Virtual インスタンスと、診断インターフェイスポートを持たない Threat Defense Virtual インスタンスのグループ化はサポートされていません。

（注） ここでの Threat Defense Virtual インスタンスのグループ化は、Azure 上の仮想マシンスケールセット（VMSS）内のインスタンスのグループ化を指します。これは、Management Center Virtual での Threat Defense Virtual インスタンスのグループ化には関係しません。

- CMI はサポートされていません。

# Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開におけるデータインターフェイスへの NIC マッピング

以下に、診断インターフェイスを使用せずに Azure に Threat Defense Virtual を展開するためのデータインターフェイスへの NIC マッピングを示します。




# Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開

診断インターフェイスを使用せずに Threat Defense Virtual を展開するには、次の手順を実行します。

**ステップ 1** 展開オプションに応じて、次のいずれかの方法を使用してこの機能を有効にできます。

- **Solution template in the Azure Marketplace**：Azure コンソールで **`Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG`** を検索し、[作成（Create）] をクリックします。[基本（Basics）] ウィンドウで必要な情報を入力し、[ソフトウェアバージョン（Software version）] ドロップダウンリストから [7.4.x] を選択します。[診断インターフェイスの接続（Attach diagnostic interface）] の横にある [いいえ（No）] ボタンを選択します。デフォルトでは、[No] が選択されています。

  Azure マーケットプレイスのソリューションテンプレートを使用して、Azure に Threat Defense Virtual を展開する完全な手順については、「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」を参照してください。

- **Custom Template using a Managed Image from a VHD**：[仮想マシン（Virtual Machines）] > [+作成（+ Create）] > [Azure仮想マシン（Azure Virtual Machine）] > [詳細（Advanced）] ウィンドウに移動し、**Custom data** フィールドにキーと値のペア **`Diagnostic: OFF`** を含む Day-0 構成スクリプトを入力します。**Custom data** フィールドに入力できる Day-0 構成スクリプトの例を以下に示します。

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
```

```
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

（注）　キーと値のペア "Diagnostic": "ON/OFF" では、大文字と小文字が区別されます。

新規展開に使用される ARM テンプレートの **Customdata** フィールドのスクリプトも変更できます。デフォルトでは、キーと値のペアは **`Diagnostic: ON`** に設定されていて、診断インターフェイスが起動します。キーと値のペアが **`Diagnostic: OFF`** に設定されている場合、展開は診断インターフェイスを使用せずに起動します。

VHD の管理対象イメージを使用し、カスタムテンプレートを使用して Azure に Threat Defense Virtual を展開する完全な手順については、「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」を参照してください。

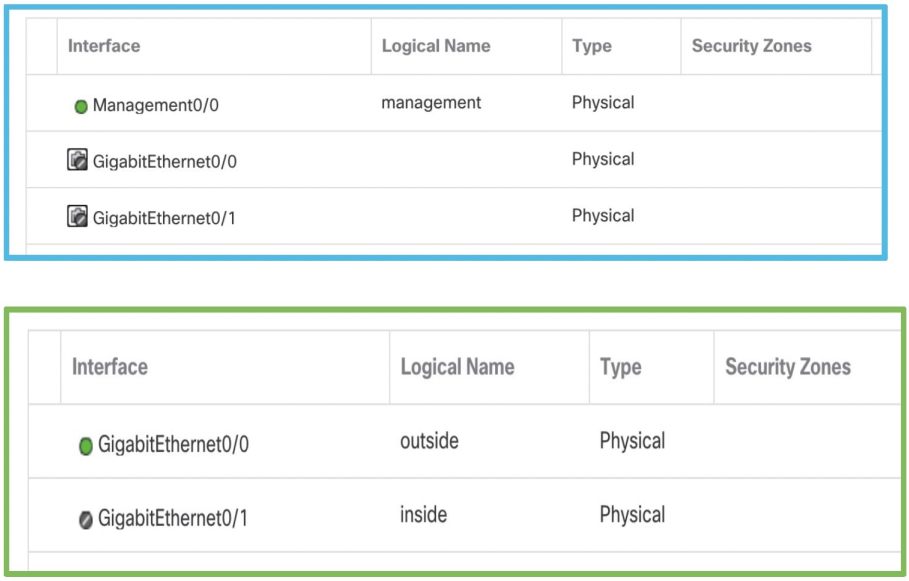
**ステップ 2**　必要な最小数の NIC（3 枚）を接続します。Azure でのインターフェイスの接続の詳細については、「仮想マシンのネットワーク インターフェイスの追加と削除」を参照してください。

**図 *6 : Azure* でのネットワーク インターフェイスの接続**


インターフェイスの詳細については、「Interface Overview」を参照してください。

**ステップ 3**　（任意）コンソールで **show interface ip brief** コマンドを使用して、インターフェイスの詳細を表示します。次に示されているように、Management Center Virtual でインターフェイスの詳細を表示することもできます。

Management Center Virtual では、インターフェイスは次のように表示されます。




# アップグレードのシナリオ

Threat Defense Virtual インスタンスは、以下のシナリオに従ってアップグレードできます。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできます。
- Cisco Secure Firewall バージョン 7.4 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできます。

次に示すアップグレードシナリオはサポートされていません。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできません。
- Cisco Secure Firewall バージョン 7.4.1 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできません。

（注） NIC の数と順序は、アップグレード後も維持されます。

# 診断インターフェイスを使用しない Threat Defense Virtual クラスタまたは Auto Scale ソリューションの展開

Threat Defense Virtual クラスタ、または診断インターフェイスを使用しない Threat Defense Virtual インスタンスで構成される Auto Scale ソリューションの新しい展開を実行するには、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されていることを確認します。

# トラブルシューティング

Threat Defense Virtual の展開時に診断インターフェイスが削除されない場合は、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されているか確認します。

# Azure での Threat Defense Virtual の Auto Scale ソリューション

## 概要

Auto Scale ソリューションにより、パフォーマンス要件に合わせてリソースを割り当て、コストを削減できます。リソースの需要が増加した場合、システムは必要に応じてリソースが割り当てられるようにします。リソースの需要が減少すると、コストを削減するためにリソースの割り当てが解除されます。

Threat Defense Virtual 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導入です。

Threat Defense Virtual Auto Scale for Azure 導入の主な特徴は次のとおりです。

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

（注） 詳細については、「Auto Scale ロジック （251 ページ）」を参照してください。

- Threat Defense Virtual 展開とマルチ可用性ゾーンのサポート。

- Management Center による Threat Defense Virtual 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 Threat Defense Virtual 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をサポート。
- Management Center でのみ動作し、Device Manager はサポート対象外。
- PAYG または BYOL ライセンスモードでの Threat Defense Virtual 展開をサポート。PAYG は、Threat Defense Virtual ソフトウェアバージョン 6.5 以降にのみ適用可能。「サポートされるソフトウェア プラットフォーム （209 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。

Azure の Threat Defense Virtual Auto Scale ソリューションは、異なるトポロジを使用して構成された 2 種類の導入例をサポートします。

- サンドイッチテクノロジーを使用した Auto Scale：Threat Defense Virtual 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）の間に配置します。
- Azure ゲートウェイロードバランサ（GWLB）を使用した Auto Scale：Azure GWLB は、セキュアファイアウォール、パブリックロードバランサ、および内部サーバーと統合されており、ファイアウォールの展開、管理、およびスケーリングを簡素化します。

### サポートされるソフトウェア プラットフォーム

Threat Defense Virtual Auto Scale ソリューションは、Management Center によって管理される Threat Defense Virtual に適用可能です。ソフトウェアバージョンには依存しません。『Cisco Firepower Compatibility Guide』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、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。

- Management Center（仮想）の表に、Management Center Virtual の互換性と仮想ホスティング環境要件を示します。
- Threat Defense Virtual の互換性の表に、Azure 上の Threat Defense Virtual の互換性と仮想ホスティング環境要件を示します。

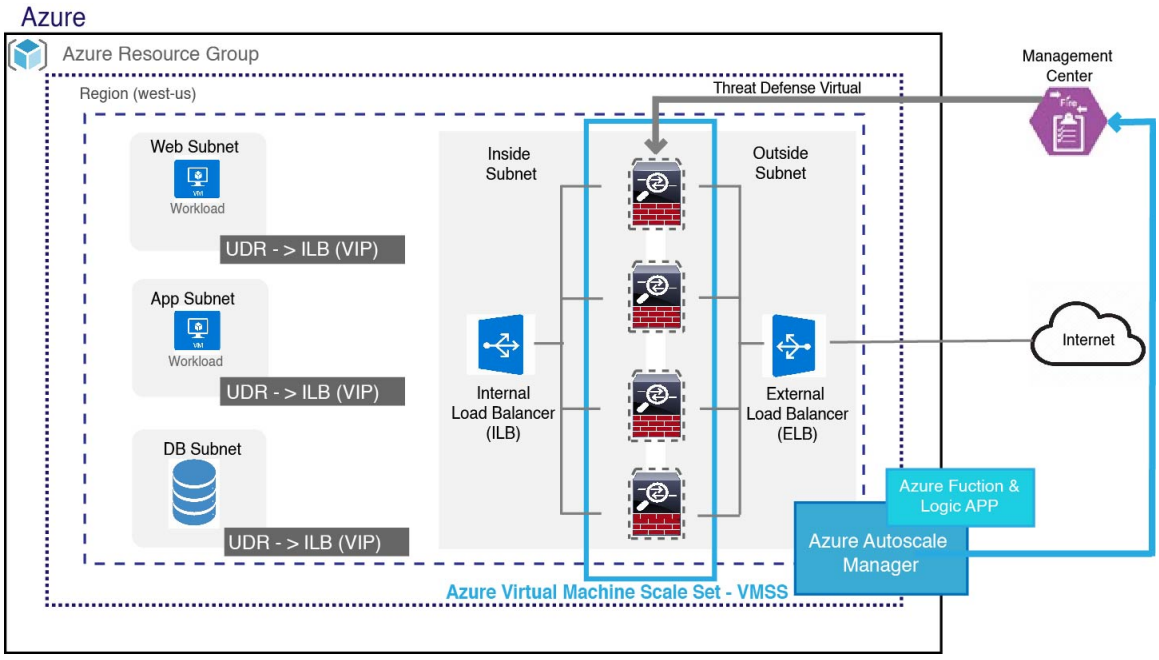
（注） Azure Auto Scale ソリューションを導入するためには、Azure 上で Threat Defense Virtual バージョン 6.4 以上を使用する必要があります。

# サンドイッチトポロジを使用した Auto Scale の導入例

Threat Defense Virtual Auto Scale for Azure は、Threat Defense Virtual 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 Threat Defense Virtual インスタンスに分散させます。その後、ファイアウォールがアプリケーションにトラフィックを転送します。
- ILB は、アプリケーションからのアウトバウンド インターネット トラフィックをスケールセット内の Threat Defense Virtual インスタンスに分散させます。その後、ファイアウォールがインターネットにトラフィックを転送します。
- ネットワークパケットが、単一の接続で両方（内部および外部）のロードバランサを通過することはありません。
- スケールセット内の Threat Defense Virtual 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 *7*: サンドイッチトポロジを使用した *Threat Defense Virtual Auto Scale* の導入例の図




# Azure Gateway Load Balancer を使用した Auto Scale の導入例

Azure Gateway Load Balancer（GWLB）は、アプリケーションサーバーなどの Azure VM との間のインターネットトラフィックが、ルーティングの変更を必要とせずに Secure Firewall によって検査されるようにします。この Azure GWLB と Secure Firewall の統合により、ファイアウォールの展開、管理、およびスケーリングが簡素化されます。また、この統合により、運用の複雑

さが軽減され、ファイアウォールでのトラフィックの単一のエントリポイントとエグジットポイントが提供されます。アプリケーションとインフラストラクチャは、送信元 IP アドレスの可視性を維持できます。一部の環境では、この可視性が非常に重要です。

Azure GWLB Auto Scale の導入例では、Threat Defense Virtual は、管理インターフェイスとデータインターフェイスの 2 つのインターフェイスのみを使用します。

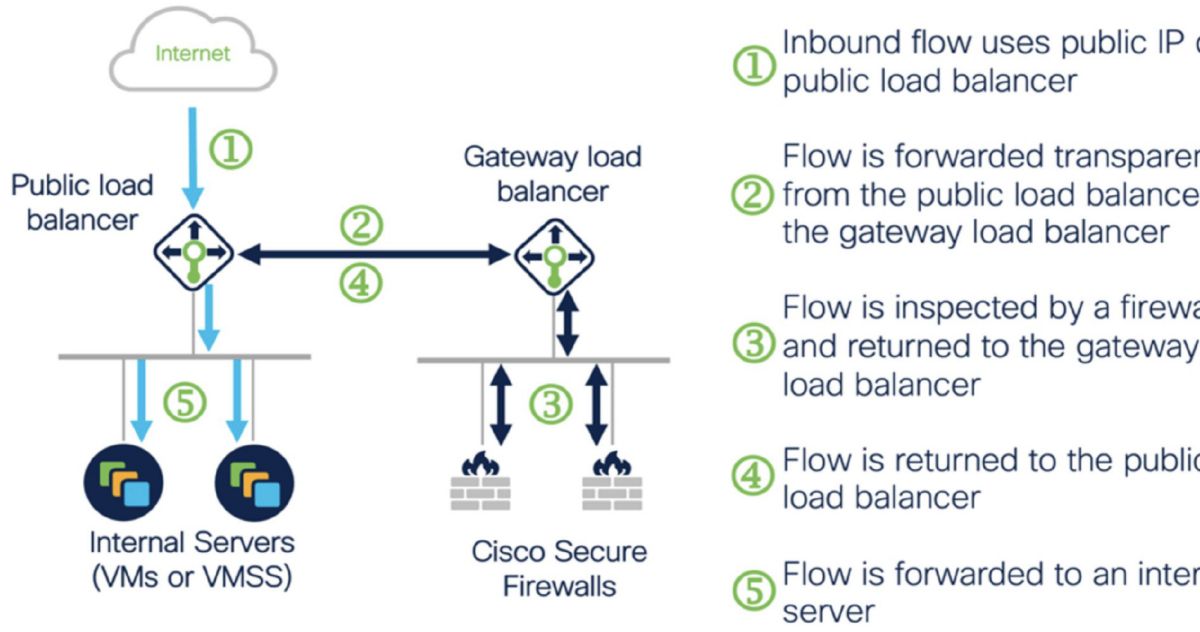
（注）
- Azure GWLB を展開する場合、ネットワークアドレス変換（NAT）は必要ありません。
- IPv4 だけがサポートされます。

### ライセンシング

PAYG と BYOL の両方がサポートされています。

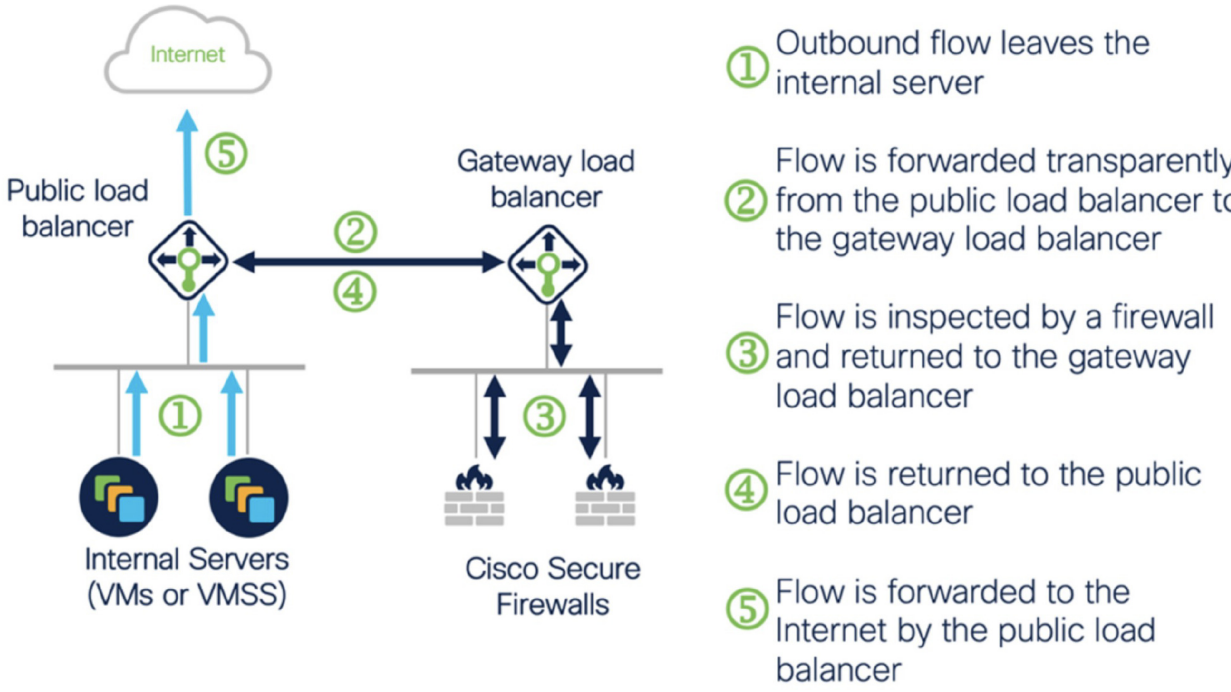
### 着信トラフィックの導入例とトポロジ

次の図は、着信トラフィックのトラフィックフローを示しています。




### 発信トラフィックの導入例とトポロジ

次の図は、発信トラフィックのトラフィックフローを示しています。

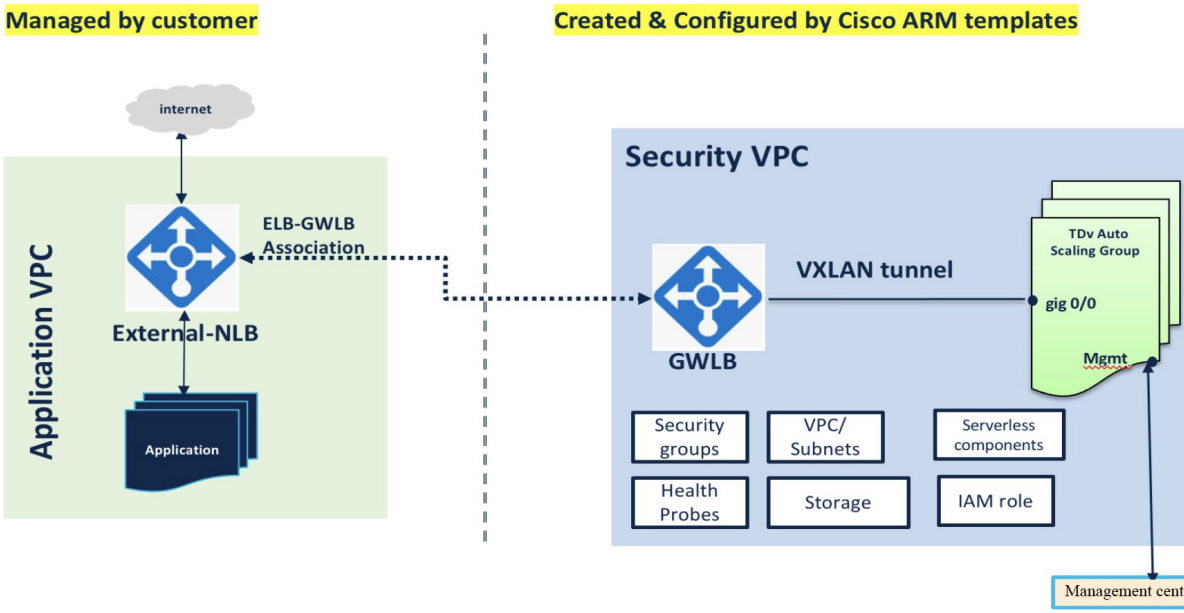



（注） Management Center を展開して設定するには、『Cisco Secure Firewall Management Center Device Configuration Guide』の手順を参照してください。展開された Management Center を使用して、Threat Defense Virtual インスタンスを管理します。

### アプリケーション VPC とセキュリティ VPC 間のトラフィックフロー

次の図では、トラフィックは既存のトポロジからファイアウォールにリダイレクトされ、外部ロードバランサによる検査が行われます。その後、トラフィックは新しく作成された GWLB にルーティングされます。ELB にルーティングされるトラフィックはすべて GWLB に転送されます。

次に、GWLB は VXLAN でカプセル化されたトラフィックを Threat Defense Virtual インスタンスに転送します。GWLB は、入力トラフィックと出力トラフィックに 2 つの別個の VXLAN トンネルを使用するため、2 つの Threat Defense Virtual アソシエーションを作成する必要があります。Threat Defense Virtual は、VXLAN でカプセル化されたトラフィックのカプセル化を解除して検査し、GWLB にルーティングします。その後、GWLB はトラフィックを ELB に転送します。




# スコープ

このドキュメントでは、Threat Defense Virtual Auto Scale for Azure ソリューションと、Azure GWLB ソリューションを使用した Auto Scale のサーバーレスコンポーネントを展開する詳細な手順について説明します。

**重要**

- 導入を開始する前に、ドキュメント全体をお読みください。
- 導入を開始する前に、前提条件を満たしていることを確認します。
- ここに記載されている手順と実行順序に従っていることを確認します。

# 導入パッケージのダウンロード

サンドイッチトポロジを使用した Threat Defense Virtual 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。

Azure GWLB ソリューションを使用した Threat Defense Virtual Auto Scale は、GWLB、ネットワーク インフラストラクチャ、Threat Defense Virtual 自動スケーリンググループ、サーバーレスコンポーネント、および他の必要なリソースを作成する ARM テンプレートベースの展開です。

両方のソリューションの展開手順はほぼ同じです。

Threat Defense Virtual 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。該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

**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、「ソースコードからの Azure 関数の構築（255 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

Threat Defense Virtual 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。
- Threat Defense Virtual 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。
- Management Center で Threat Defense Virtual を新規登録します。
- Management Center を使用して新しい Threat Defense Virtual を設定します。
- スケールインした Threat Defense Virtual を Management Center 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（217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、Threat Defense Virtual 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、Threat Defense Virtual for Azure では無効になっています。
- VMSS で Threat Defense Virtual 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、Threat Defense Virtual 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。

Threat Defense Virtual Auto Scale for Azure：ARM テンプレート **azure_ftdv_autoscale.json** は、以下を含む Auto Scale Manager コンポーネントへの入力情報を提供します。

- 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。

Threat Defense Virtual Auto Scale for Azure GWLB：ARM テンプレート **azure_ftdv_autoscale_with_GWLB.json** は、以下を含む Auto Scale Manager コンポーネントへの入力情報を提供します。

- Azure Function App
- Azure Logic App
- 仮想マシン（VM）または仮想マシンスケールセット（VMSS）
- ネットワーキング インフラストラクチャ
- ゲートウェイロードバランサ
- 展開に必要なセキュリティグループおよびその他のコンポーネント

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

# 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。サンドイッチテクノロジーを使用した 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。 ただし、Azure GWLB を使用した Auto Scale の展開では、ネットワーク インフラストラクチャが作成されることに注意してください。

Threat Defense Virtual 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 Threat Defense Virtual 間の正常性プローブに必要です。

  サーバーレス機能と Threat Defense Virtual 間の通信に必要です。

- TCP/8305

  Threat Defense Virtual と Management Center 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 Management Center 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

Threat Defense Virtual 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、「ソースコードからの Azure 関数の構築（255 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。

## Management Center の準備

Threat Defense Virtual を管理するには、フル機能のマルチデバイスマネージャである Management Center を使用します。Threat Defense Virtual は、Threat Defense Virtual マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

デバイスグループを含め、Threat Defense Virtual 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 Threat Defense Virtual インスタンスにプッシュされます。

後続の項では、Management Center 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。Management Center を準備する際は、次の情報を必ず記録してください。

- Management Center のパブリック IP アドレス。
- Management Center のユーザー名/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。

## Management Center の新規ユーザーの作成

Auto Scale Manager だけが使用する管理者権限を持つ Management Center で新規ユーザーを作成します。

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

**ステップ 1** 管理者権限を持つ Management Center 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、「Cisco Secure Firewall Management Center アドミニストレーション ガイド」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。『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』の「アクセス制御のベストプラクティス」を参照してください。

**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については、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』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、Management Center によって Threat Defense 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。

- **Cisco Secure Firewall Threat Defense の IPS**：セキュリティ インテリジェンスと Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense のマルウェア防御**：マルウェア防御
- **Cisco Secure Firewall Threat Defense の URL フィルタリング**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

（注） IPS、マルウェア防御、または URL フィルタリングライセンスをご購入の場合、1 年、3 年、または5年間アップデートを利用するには、該当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

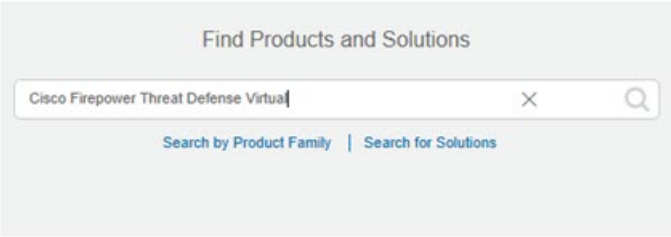
- Cisco Smart Software Manager にマスター アカウントを持ちます。

  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。

**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 *8*：ライセンス検索**




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

**ステップ 2** まだ設定していない場合は、スマート ライセンシング サーバーに Management Center 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。詳細な手順については、Cisco Secure Firewall Management Center アドミニストレーション ガイド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。

**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

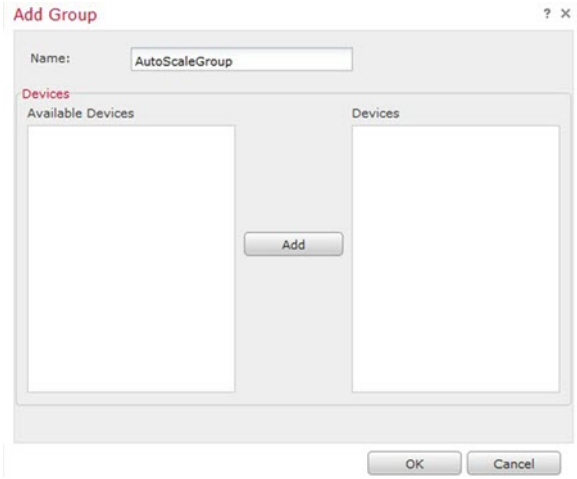
デバイス グループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

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

***図 9 : Device Management***

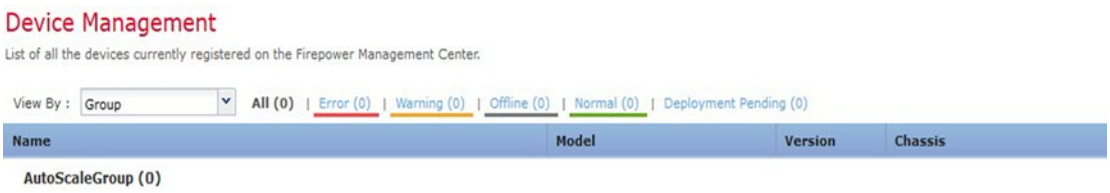

**ステップ 2** [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。
**ステップ 3** 名前を入力します。 例：AutoScaleGroup。

図 *10* : デバイスグループの追加




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

図 *11* : 追加されたデバイスグループ




## セキュアシェルアクセスの設定

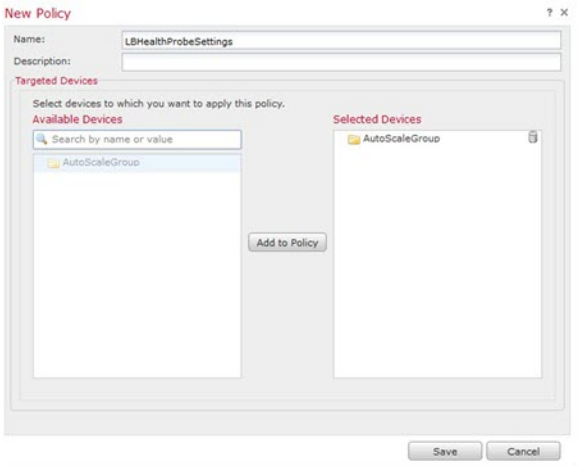
Threat Defense デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。Threat Defense Virtual Auto Scale for Azure には、内部ゾーンと外部ゾーン、および自動スケールグループ用に作成されたデバイスグループで SSH を許可するための Threat Defense プラットフォーム設定ポリシーが必要です。これは、Threat Defense Virtual のデータインターフェイスがロードバランサからの正常性プローブに応答するために必要です。

### 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。

**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、Threat Defense ポリシー（例：LBHealthProbeSettings）を作成または編集します。

図 *12 : Threat Defense* プラットフォーム設定ポリシー




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

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

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

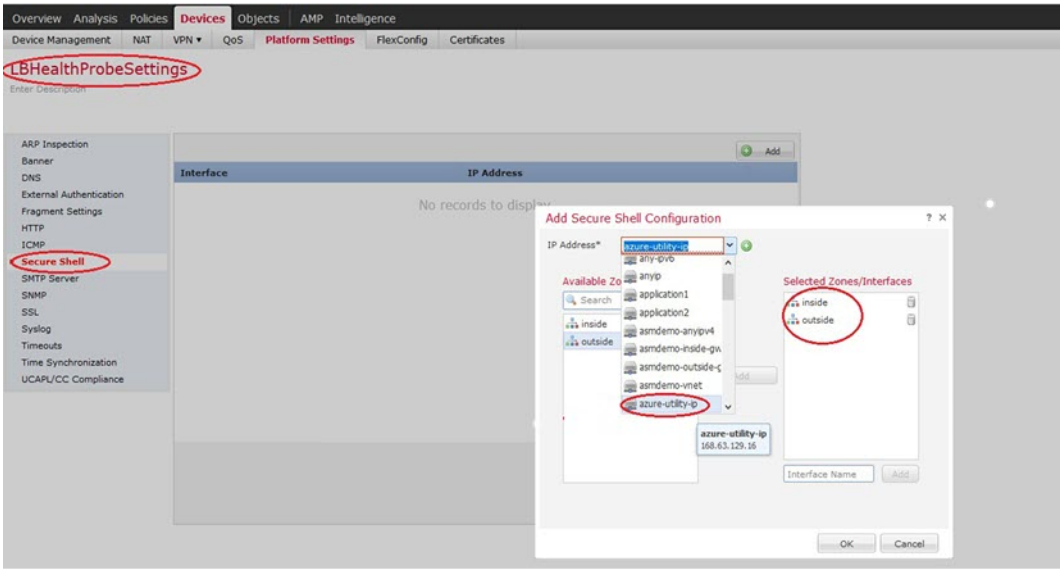
b) ルールのプロパティを設定します。

- [IPアドレス（IP Address）]：SSH接続を許可するホストまたはネットワークを特定するネットワークオブジェクト（例：azure-utility-ip（168.63.129.16））。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：SSH 接続を許可するインターフェイスを含むゾーンを追加します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。セキュリティゾーンは、Management Center 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、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』 を参照してください。

  （注） Azure Gateway Load Balancer を使用した Auto Scale の導入例では、内部インターフェイスは使用されません。

- [OK] をクリック

図 *13 : Threat Defense Virtual Auto Scale の SSH アクセス*




**ステップ 4** **[Save（保存）]** をクリックします。

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

（注） **SSH アクセス**を使用する代わりに、TCP ポート 443 を正常性プローブ用に設定することもできます。この設定を行うには、[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] > [HTTPアクセス（HTTP Access）] に移動し、 [HTTPサーバーの有効化（Enable HTTP Server）]チェックボックスをオンにして、[ポート（Port）]フィールドに[443] と入力します。この設定を内部インターフェイスと外部インターフェイスに関連付けます。ARMテンプレートの正常性プローブポートも 443 に変更する必要があります。HTTP アクセスの構成の詳細については、『Configuring HTTP』[英語] を参照してください。

## 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。

（注） サンドイッチトポロジを使用して自動スケールを構成する場合にのみ、NAT を構成する必要があります。

**ステップ 1** **[デバイス（Devices）]** > **[NAT]** の順に選択します。

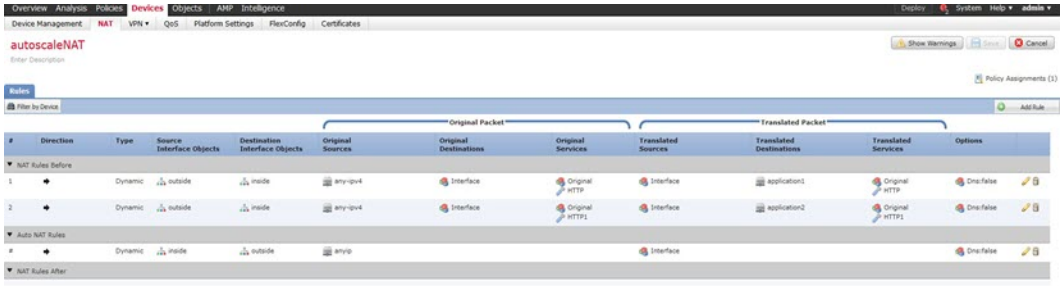
**ステップ 2** [新しいポリシー（New Policy）] ドロップダウン リストで、[Threat Defense NAT] を選択します。

**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、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』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 *14 : NAT* ポリシーの例**




（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 Threat Defense Virtual デバイスを作成できます。「Auto Scale ARM テンプレートの展開 （235 ページ）」を参照してください。Azure GWLB ソリューションを使用した Auto Scale では、テンプレートで追加の入力パラメータを設定する必要があるため、ネットワーク インフラストラクチャも作成されます。パラメータの意味は一目瞭然なので説明を省略します。

**表 *20 :* 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。<br>注：小文字のみを使用してください。<br>例：ftdv | 新規作成 |

| 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 |
|---|---|---|---|
| virtualNetworkRg | 文字列 | 仮想ネットワークのリソースグループの名前。<br>例：cisco-virtualnet-rg | 既存 |
| virtualNetworkName | 文字列 | 仮想ネットワーク名（作成済み）<br>例：cisco-virtualnet | 既存 |
| virtualNetworkCidr | CIDR 形式<br>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）<br>例：cisco-mgmt-subnet | 既存 |
| diagSubnet | 文字列 | 診断サブネット名（作成済み）<br>例：cisco-diag-subnet | 既存 |
| insideSubnet | 文字列 | 内部サブネット名（作成済み）<br>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）。<br>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）<br>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 | Management Center のデバイスグループ（作成済み） | 既存 |

| パラメータ名 | 使用できる値/タイプ | 説明 | リソースの作成タイプ |
|---|---|---|---|
| insideZoneName | 文字列 | Management Center の内部ゾーン名（作成済み） | 既存 |
| outsideZoneName | 文字列 | Management Center の外部ゾーン名（作成済み） | 既存 |
| softwareVersion | 文字列 | Threat Defense Virtual バージョン（展開時にドロップダウンから選択） | 既存 |
| vmSize | 文字列 | Threat Defense Virtual 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 | Threat Defense Virtual ライセンスモード（PAYG/BYOL）<br>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 * | Threat Defense Virtual VM 管理の管理者ユーザー名。<br>これは「admin」には**できません**。VM 管理者ユーザー名のガイドラインについては、「Azure」を参照してください。 | 新規作成 |

| 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 |
|---|---|---|---|
| ftdVmManagementUserPassword | 文字列 * | Threat Defense Virtual VM 管理の管理者ユーザーのパスワード。<br>パスワードの長さは 12 ー 72 文字で、小文字、大文字、数字、特殊文字を使用する必要があります。また、文字の繰り返しは 2 回までにする必要があります。<br>（注） テンプレートには、このパラメータのコンプライアンスチェック機能はありません。 | 新規作成 |
| fmcIpAddress | 文字列<br>x.x.x.x | Management Center 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 Management Centerユーザー名（作成済み） | 既存 |
| fmcPassword | 文字列 | 前述の Management Center ユーザー名の Management Center パスワード（作成済み） | 既存 |
| policyName | 文字列 | Management Center で作成されたセキュリティポリシー（作成済み） | 既存 |

| パラメータ名 | 使用できる値/タイプ | 説明 | リソースの作成タイプ |
|---|---|---|---|
| scalingPolicy | POLICY-1/POLICY-2 | **POLICY-1**：設定された期間に、いずれかの Threat Defense Virtual 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。<br>**POLICY-2**：設定された期間に、Auto Scale グループ内のすべての Threat Defense Virtual 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。<br>どちらの場合も、スケールインロジックは同じままです。設定された期間に、すべての Threat Defense Virtual 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。 | 該当なし |
| scalingMetricsList | 文字列 | スケーリングの決定に使用されるメトリック。<br>許可：CPU<br>CPU、メモリ<br>デフォルト：CPU | 該当なし |
| cpuScaleInThreshold | 文字列 | CPU メトリックのスケールインしきい値（パーセント単位）。<br>デフォルト：10<br>Threat Defense Virtual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。<br>「Auto Scale ロジック （251 ページ）」を参照してください。 | 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）。<br>デフォルト：80<br>Threat Defense Virtual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。<br>「cpuScaleOutThreshold」は、常に「cpuScaleInThreshold」より**大きく**する必要があります。<br>「Auto Scale ロジック （251 ページ）」を参照してください。 | 該当なし |
| 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）。<br>デフォルト：0<br>Threat Defense Virtual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。<br>「Auto Scale ロジック （251 ページ）」を参照してください。 | 該当なし |

| パラメータ名 | 使用できる値/タイプ | 説明 | リソースの作成タイプ |
|---|---|---|---|
| memoryScaleOutThreshold | 文字列 | 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）。<br>デフォルト：0<br>Threat Defense Virtual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。<br>「memoryScaleOutThreshold」は、常に「memoryScaleInThreshold」より**大きく**する必要があります。<br>「Auto Scale ロジック （251 ページ）」を参照してください。 | 該当なし |
| minFtdCount | 整数 | 任意の時点でスケールセットで使用可能な最小 Threat Defense Virtual インスタンス数。<br>例：2。 | 該当なし |
| maxFtdCount | 整数 | スケールセットで許可される最大 Threat Defense Virtual インスタンス数。<br>例：10<br>（注） この数は Management Center の容量によって制限されます。<br>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。 | 該当なし |

| パラメータ名 | 使用できる値/タイプ | 説明 | リソースの作成タイプ |
|---|---|---|---|
| metricsAverageDuration | 整数 | ドロップダウンから選択します。<br>この数値は、メトリックが平均化される時間（分単位）を表します。<br>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。<br>（注） Azure の制限により、有効な数値は 1、5、15、および 30 だけです。 | 該当なし |

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

| パラメータ名 | 使用できる値/タイプ | 説明 | リソースの作成タイプ |
|---|---|---|---|
| | | 主に最初の展開、またはスケールセットに Threat Defense Virtual インスタンスが含まれていない場合に適用されます。<br><br>BULK：Auto Scale Manager は、「minFtdCount」個の Threat Defense Virtual インスタンスを同時に展開しようとします。<br><br>（注） 起動は並行して行われますが、Management Center への登録は Management Center の制限により順次実行されます。<br><br>STEP：Auto Scale Manager は、スケジュールされた間隔ごとに「minFtdCount」個の Threat Defense Virtualデバイスを 1 つずつ展開します。<br><br>（注） STEP オプションでは、「minFtdCount」個のインスタンスが Management Center 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。<br><br>BULK オプションでは、（並行実行のため）「minFtdCount」個すべての Threat Defense Virtual を起動するのに 1 つ | |

| 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 |
|---|---|---|---|
| | | の Threat Defense Virtual 起動と同じ時間がかかりますが、Management Center の登録は順次実行されます。<br>「minFtdCount」個の Threat Defense Virtual を展開するための合計時間 =（1 つの Threat Defense Virtual の起動時間 + 1 つの Threat Defense Virtual 登録および設定時間 * minFtdCount）。 | |
| * Azure には、新しいリソースの命名規則に関する制限があります。制限を確認するか、またはすべて小文字を使用してください**スペースやその他の特殊文字は使用しないでください。** | | | |

# Auto Scale ソリューションの展開

## 導入パッケージのダウンロード

サンドイッチトポロジを使用した Threat Defense Virtual 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。

Azure GWLB ソリューションを使用した Threat Defense Virtual Auto Scale は、GWLB、ネットワーク インフラストラクチャ、Threat Defense Virtual 自動スケーリンググループ、サーバーレスコンポーネント、および他の必要なリソースを作成する ARM テンプレートベースの展開です。

両方のソリューションの展開手順はほぼ同じです。

Threat Defense Virtual 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。該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

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、「ソースコードからの Azure 関数の構築（255 ページ）」を参照してください。

## Auto Scale ARM テンプレートの展開

**サンドイッチトポロジを使用した Azure 用 Threat Defense Virtual Auto Scale**：ARM テンプレート **azure_ftdv_autoscale.json** を使用して、Azure 用 Threat Defense Virtual Auto Scale に必要なリソースを展開します。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）

**Azure GWLB を使用した Threat defense virtual Auto Scale**：ARM テンプレート **azure_ftdv_autoscale_with_GWLB.json** を使用して、Azure GWLB ソリューションによる Threat Defense Virtual Auto Scale に必要なリソースを展開します。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（VM）または仮想マシンスケールセット（VMSS）
- ゲートウェイロードバランサ
- Azure Function App
- Logic App
- ネットワーキング インフラストラクチャ
- 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

### 始める前に

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

**ステップ 1** 複数の Azure ゾーンに Threat Defense Virtual 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。サンドイッチトポロジを使用したAuto Scaleの導入例でのみ有効です。

**例**：

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

        ],
        "properties": {
          "frontendIPConfigurations": [
            {
              "name": "LoadBalancerFrontEnd",
                "properties": {
                  "publicIPAddress": {
                    "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
                  }
                }
            }
          ],
          "backendAddressPools": [
            {
              "name": "backendPool"
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/backendAddressPools/BackendPool')]"
                },
                "probe": {
```

```
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

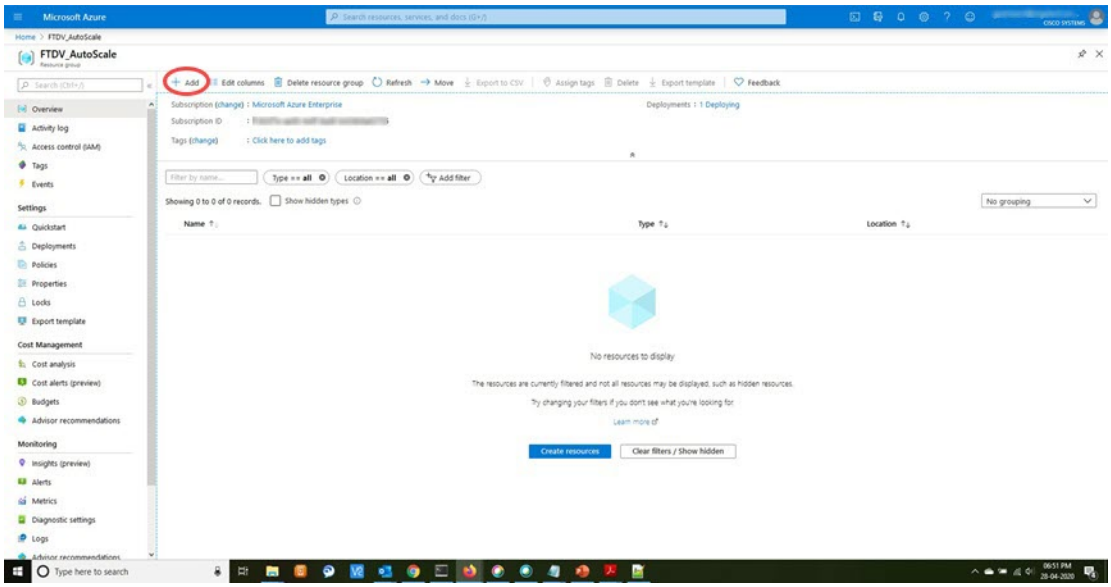
（注）　このファイルを編集しない場合は、導入後に Azure ポータルから編集することもできます。

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

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

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

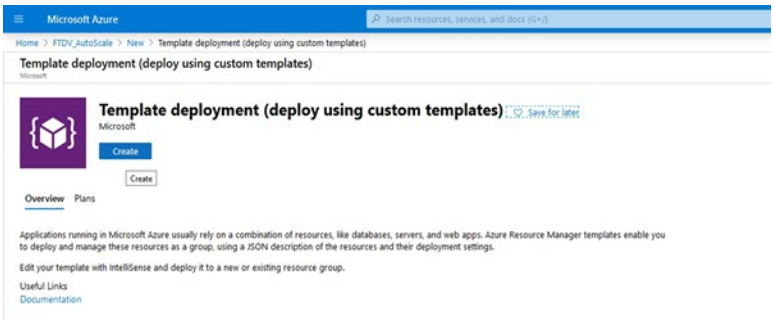
**図 *15 : Azure* ポータル**




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

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

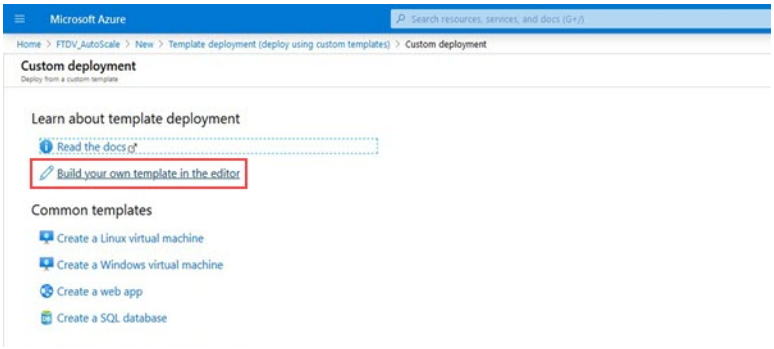
図 *16* : カスタムテンプレートの展開




**ステップ 7** [作成（Create）] をクリックします。

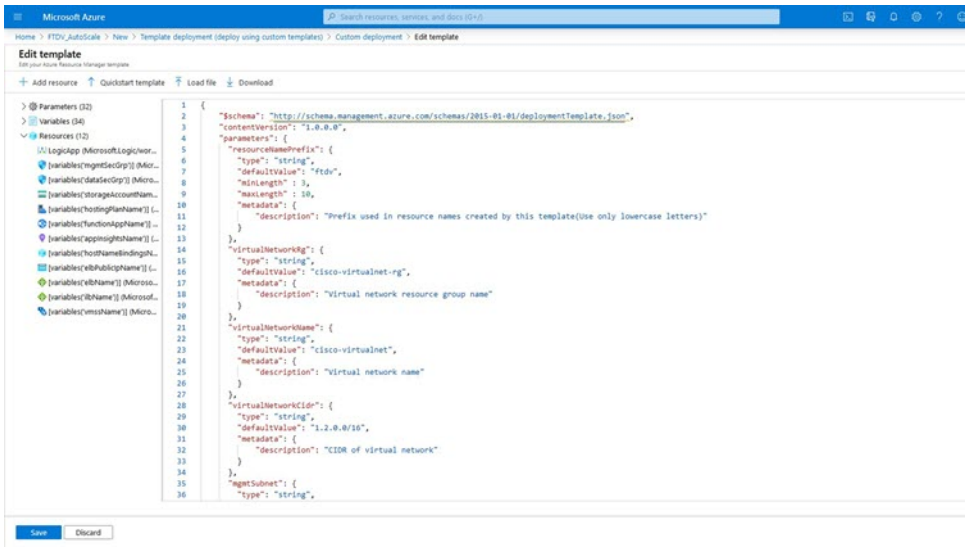
**ステップ 8** テンプレートを作成するためのオプションは複数あります。[エディタで独自のテンプレートを作成する（Build your own template in editor）] を選択します。

図 *17* : 独自のテンプレートの作成



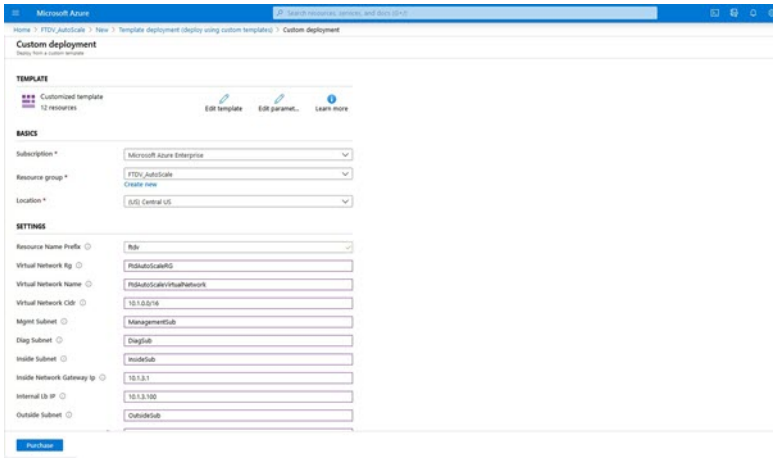

**ステップ 9** [テンプレートの編集（Edit template）] ウィンドウで、すべてのデフォルトコンテンツを削除し、更新した *azure_ftdv_autoscale.json* からコンテンツをコピーして、[保存（Save）] をクリックします。

図 *18 : Edit Template*




**ステップ 10** 次のセクションで、すべてのパラメータを入力します。各パラメータの詳細については、「入力パラメータ （224 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 *19 : ARM* テンプレートパラメータ

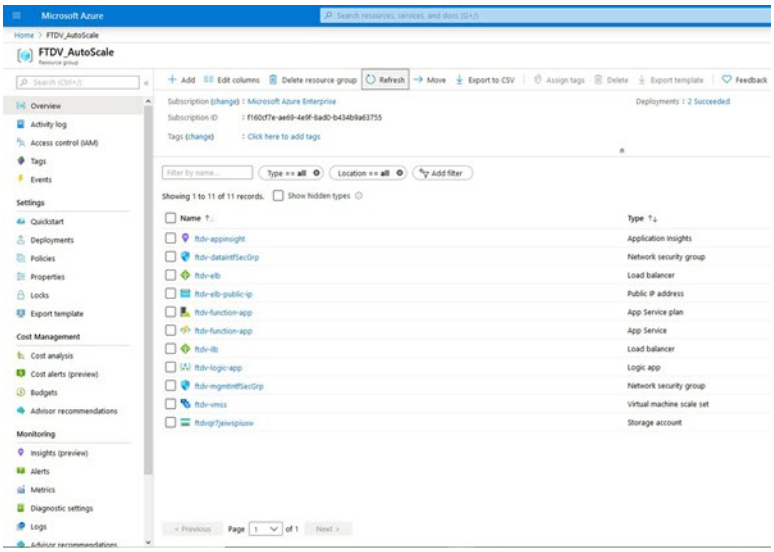



（注） [パラメータの編集（Edit Parameters）] をクリックして、JSON ファイルを編集するか、または事前入力されたコンテンツをアップロードできます。

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、Threat Defense Virtual Auto Scale for Azure ソリューションに必要なすべてのリソースが作成されます。次の図のリソースを参照してください。[タイプ（Type）] 列には、Logic App、VMSS、ロードバランサ、パブリック IP アドレスなどの各リソースが示されます。

図 *20 : Threat Defense Virtual* 自動スケール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。「ソースコードからの Azure 関数の構築（255 ページ）」を参照してください。

**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

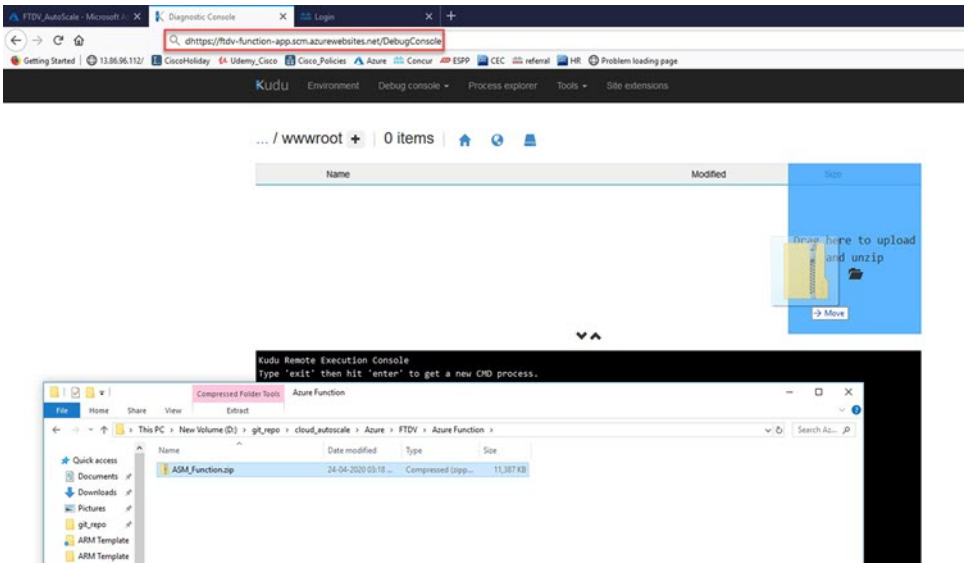
「Auto Scale ARM テンプレートの展開 （235 ページ）」の例の場合、次のようになります。

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。

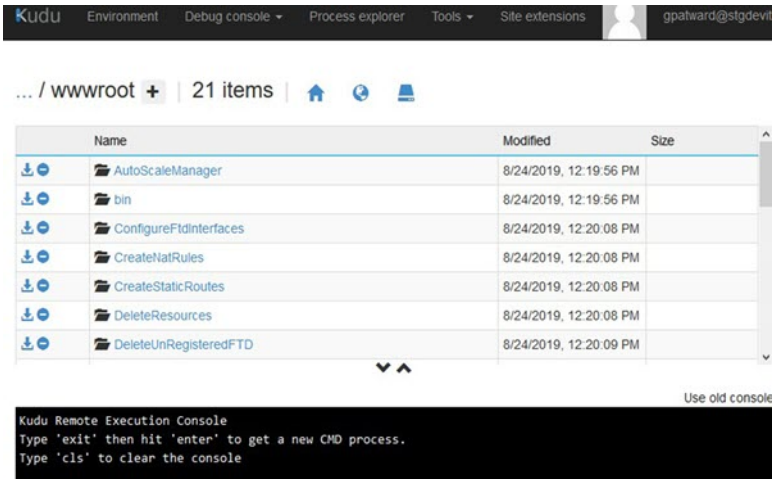
**ステップ 3** ASM_Function.zip をファイルエクスプローラの右隅にドラッグアンドドロップします。

図 *21 : Threat Defense Virtual Auto Scale* 機能のアップロード




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

図 *22 : Threat Defense Virtual* のサーバーレス機能

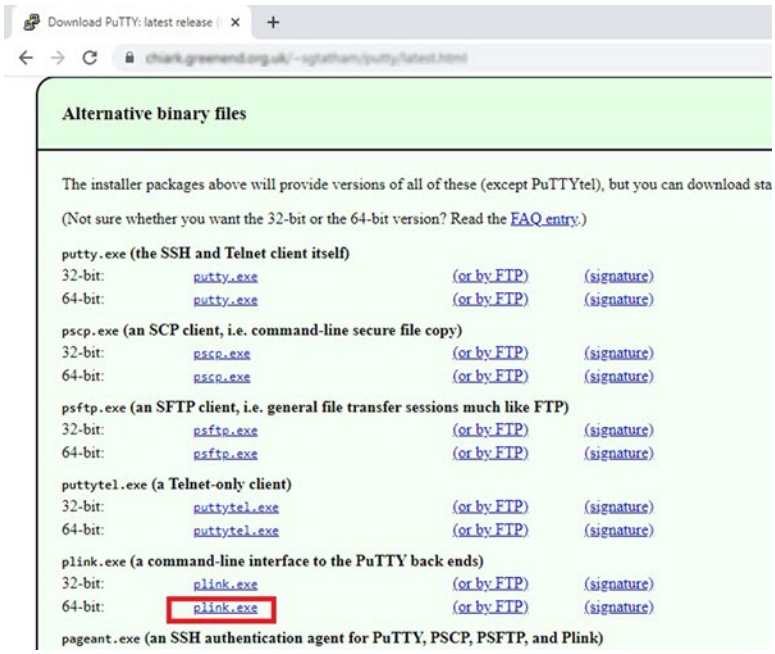



**ステップ 5** PuTTY SSH クライアントをダウンロードします。

Azure 関数は、SSH 接続を介して Threat Defense Virtual 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、Threat Defense Virtual 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 *23 : PuTTY* のダウンロード




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

**ステップ 7** **ftdssh.exe** をファイルエクスプローラの右隅（前のステップで **ASM_Function.zip** をアップロードした場所）にドラッグアンドドロップします。

**ステップ 8** SSH クライアントが Function App とともに存在することを確認します。必要に応じてページを更新します。

## 設定の微調整

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

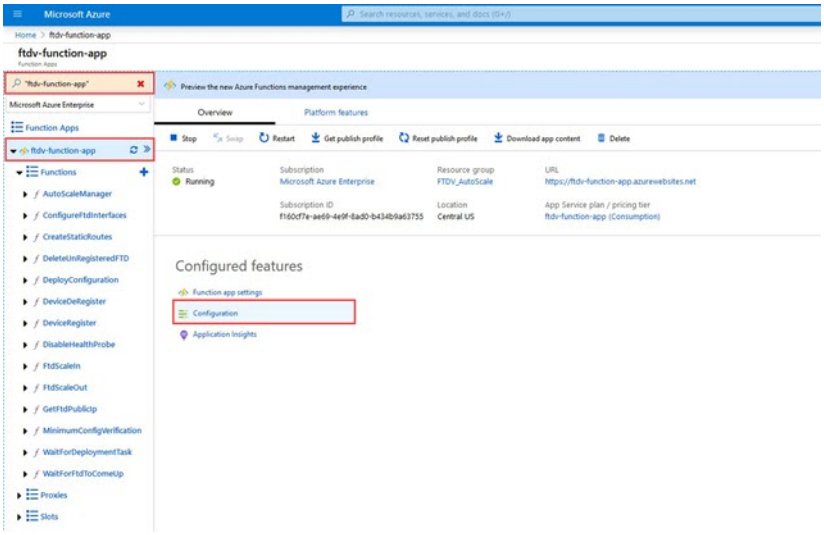
### 始める前に

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

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

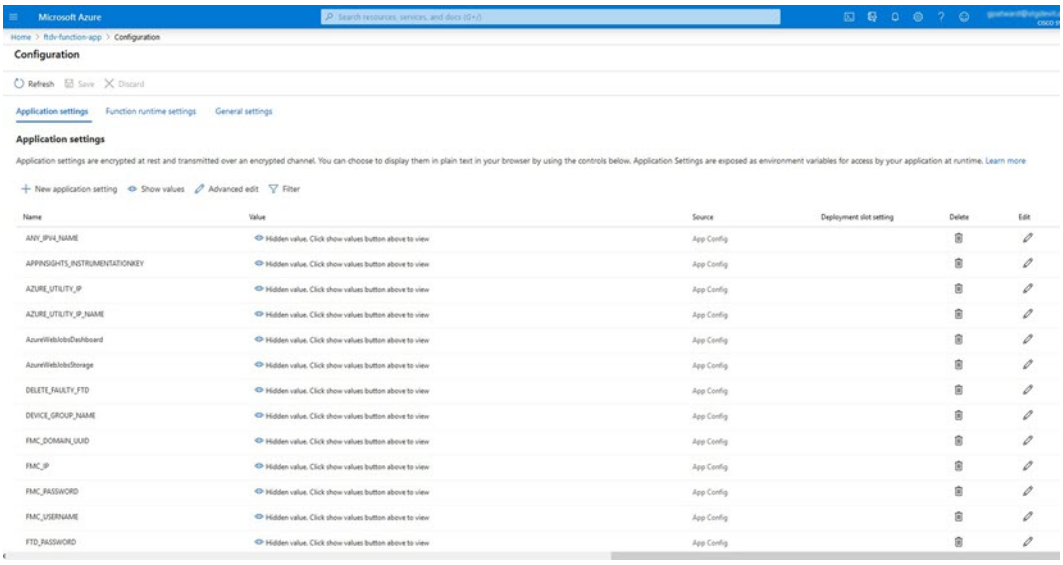
**ステップ 1** Azure ポータルで、Threat Defense Virtual Function App を検索して選択します。

図 *24 : Threat Defense Virtual* 機能アプリケーション




**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 *25 :* アプリケーションの設定




ほとんどのオプションは、名前を見ればわかります。次に例を示します。

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

スケールアウト中に、新しい Threat Defense Virtual インスタンスが起動し、Management Center 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 Threat Defense Virtual 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 Threat Defense Virtual を削除します。[いいえ（No）]：Management Center に登録できない場合でも、Threat Defense Virtual 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。

**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。

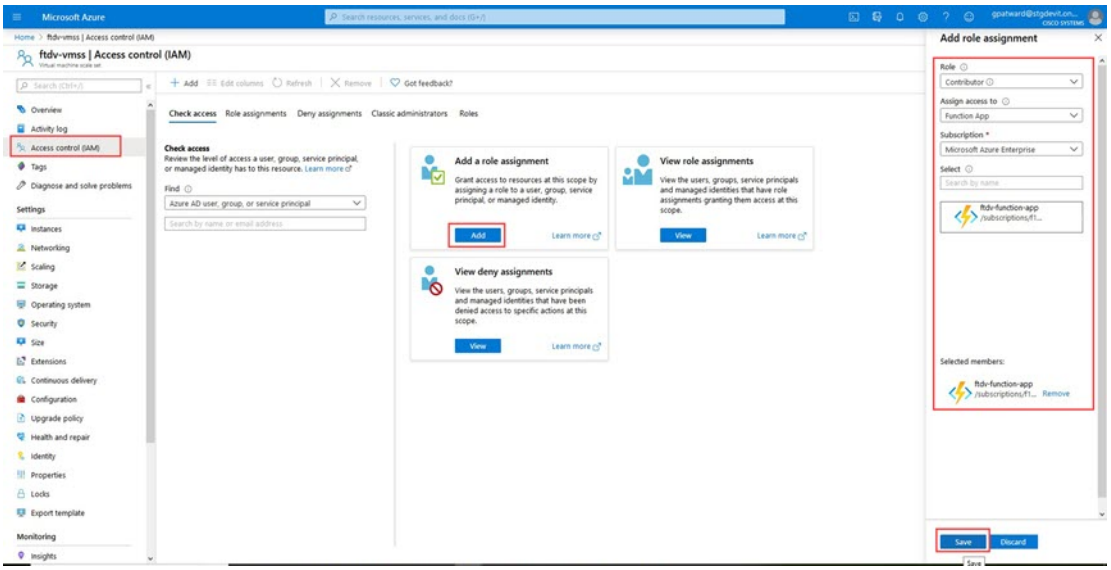
**ステップ 3** [追加（Add）] をクリックしてロールの割り当てを追加します。

**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** Threat Defense Virtual Function App を選択します。

図 *26 : AIM* ロールの割り当て




**ステップ 7** [保存（**Save**）] をクリックします。

（注） まだ Threat Defense Virtual 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、Threat Defense Virtual 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。

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。

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

**重要**　手順をすべて読んで理解してから続行してください。

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

a) 必須: すべての「SUBSCRIPTION_ID」を検索し、サブスクリプション ID 情報に置き換えます。
b) 必須: すべての「RG_NAME」を検索し、リソースグループ名に置き換えます。
c) 必須: すべての「FUNCTIONAPPNAME」を検索し、Function App 名に置き換えます。

次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

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

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

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、Threat Defense Virtual から既存の接続をドレインする時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

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

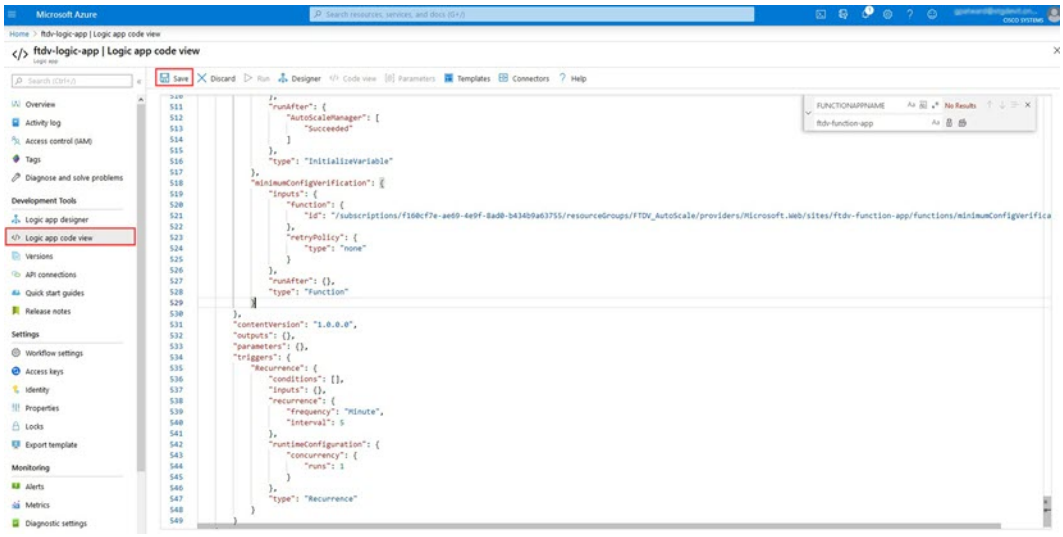
f) （任意）クールダウン時間を編集するか、デフォルト値（10）のままにします。これは、スケールアウト完了後に NO ACTION を実行する時間です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

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

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

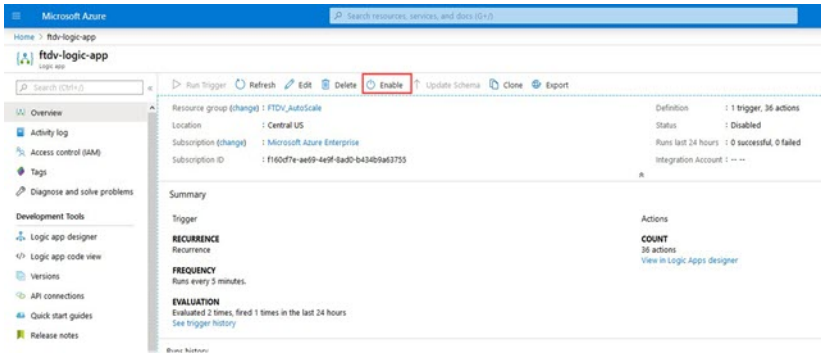
**ステップ 2** [Logic Appコードビュー（Logic App code view）] に移動し、デフォルトの内容を削除して、編集した LogicApp.txt ファイルの内容を貼り付け、[保存（Save）] をクリックします。

図 *27 : Logic App* コードビュー



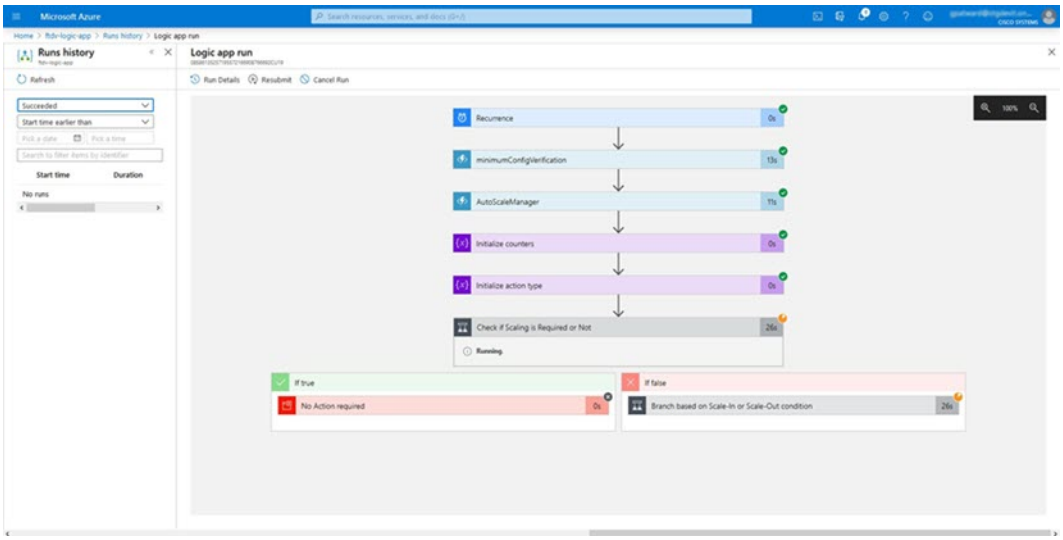

**ステップ 3** Logic App を保存すると、[無効（Disabled）] 状態になります。Auto Scale Manager を起動する場合は、[有効化（Enable）] をクリックします。

図 *28 : Logic App* の有効化




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

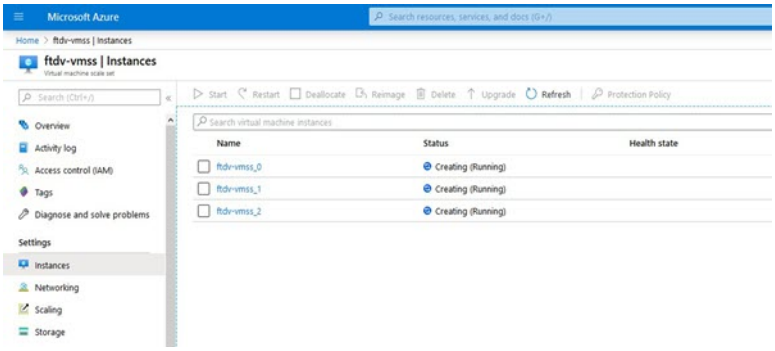
図 *29 : Logic App* の実行ステータス




**ステップ 5** Logic App が起動すると、導入関連のすべての手順が完了します。

**ステップ 6** Threat Defense Virtual 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 *30 :* 稼働中の *Threat Defense Virtual* インスタンス




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 Threat Defense Virtual インスタンスが起動されます。

## Threat Defense Virtualのアップグレード

Threat Defense Virtual 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、Threat Defense Virtual は Azure REST API インターフェイスを介してアップグレードします。

（注） 任意の REST クライアントを使用して Threat Defense Virtual をアップグレードできます。

### 始める前に

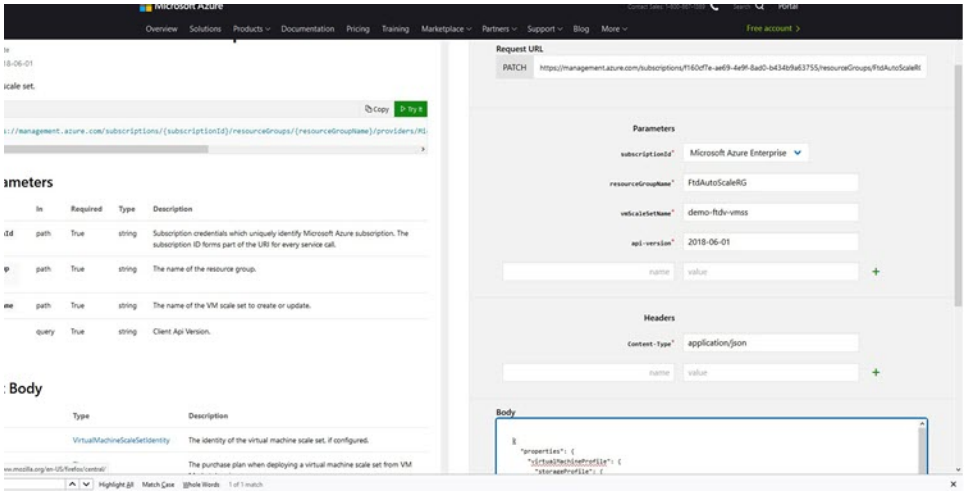
- 市場で入手可能な新しい Threat Defense Virtual イメージバージョンを取得します（例：650.32.0）。
- 元のスケールセットの展開に使用する SKU を取得します（例：ftdv-azure-byol）。
- リソースグループと仮想マシンスケールセット名を取得します。

**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（Parameters）] セクションに詳細を入力します。

**図 *31 : Threat Defense Virtual*のアップグレード**




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

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

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

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

- 既存の Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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、Threat Defense Virtual 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 Management Center 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** Threat Defense Virtual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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual が終了用に選択されます

**注意**

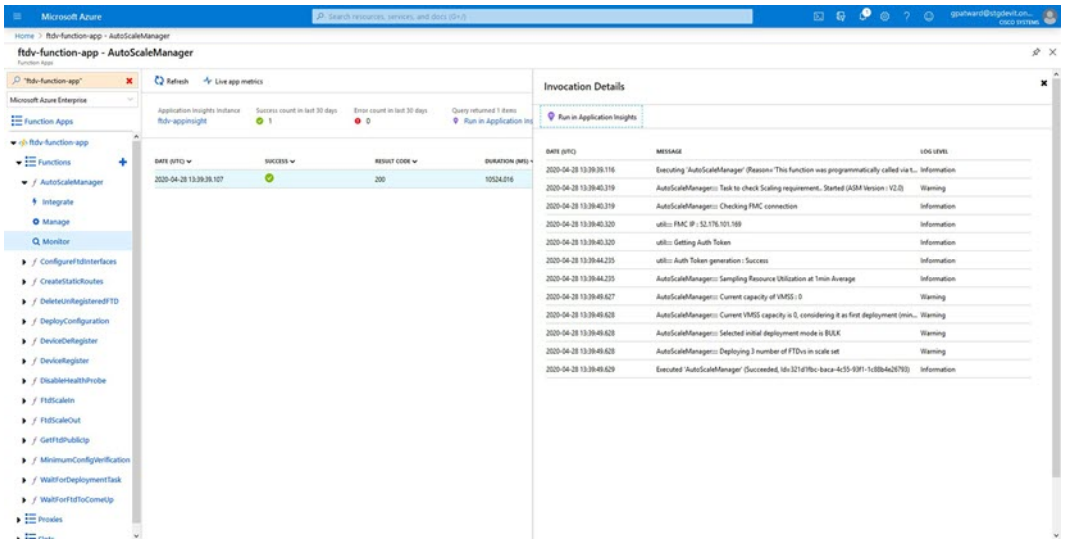
- スケールイン/スケールアウトは 1 つずつ行われます（つまり、一度に 1 つの Threat Defense Virtual だけがスケールインまたはスケールアウトされます）。
- Management Center から受信したメモリ消費量のメトリックは、経時的に計算された平均値ではなく、瞬間的なスナップショット/サンプル値です。したがって、スケーリングを決定する際にメモリメトリックだけを考慮することはできません。展開時にメモリのみのメトリックを使用するオプションはありません。

# 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。

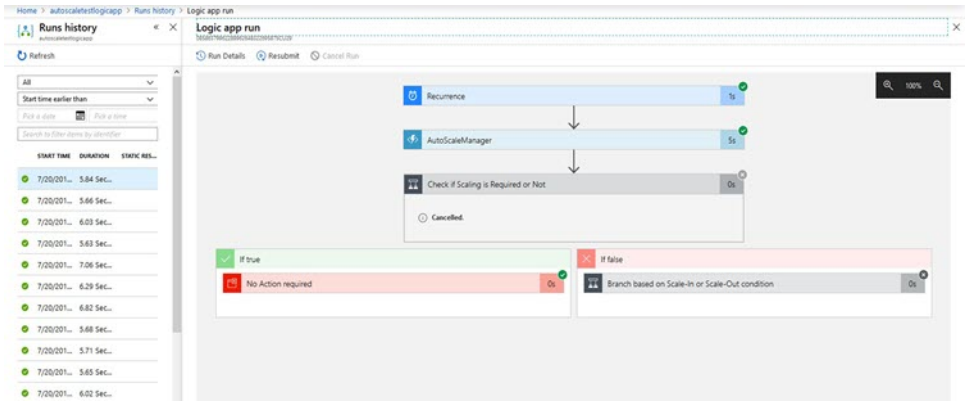
- 個々の Azure 関数のログを表示できます。

**図 *32 : Azure* 関数ログ**




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

図 *33 : Logic App* の実行ログ




- 必要な場合は、Logic App で実行中のタスクをいつでも停止または終了できます。ただし、現在実行中の Threat Defense Virtual 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

Threat Defense Virtual 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。
- Management Center の管理が必要です。Device Manager はサポートされていません。
- Management Center にはパブリック IP アドレスが必要です。
- Threat Defense Virtual 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。
- Threat Defense Virtual 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 Threat Defense Virtual 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。Management Center 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。
- 設定の変更は、すでに実行中のインスタンスには自動的に反映されません。変更は新しいデバイスにのみ反映されます。このような変更は、既存のデバイスに手動でプッシュする必要があります。
- 既存のインスタンスの設定を手動で更新しているときに問題が発生した場合は、それらのインスタンスをスケーリンググループから削除し、新しいインスタンスに置き換えることを推奨します。

# トラブルシューティング

次に、Threat Defense Virtual 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。

- Management Center への接続に失敗する：Management Center の IP またはログイン情報を確認してください。Management Center が障害状態または到達不能状態であるか確認します。
- Threat Defense Virtual 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 Threat Defense Virtual 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：Threat Defense Virtual 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、Threat Defense Virtual 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。
- Threat Defense Virtual を Management Center に登録できない：新しい Threat Defense Virtual デバイスに対応するために Management Center の容量を確認します。ライセンスを確認します。Threat Defense Virtual 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 Threat Defense Virtual デバイスで SSH アクセスを確認します。Management Center でデバイス登録の問題を確認します。Azure VMSS で Threat Defense Virtual 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。

Azure GWLB 展開を使用した Threat Defense Virtual 自動スケーリング中に問題が発生した場合のトラブルシューティングのヒントは次のとおりです。

- ELB と GWLB の関連付けを確認します。
- GWLB で正常性プローブのステータスを確認します。
- Threat Defense Virtual の物理インターフェイスおよび論理インターフェイスでトラフィックフローを確認して、VXLAN 設定を確認します。
- セキュリティグループのルールを確認します。

# ソースコードからの Azure 関数の構築

### システム要件

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

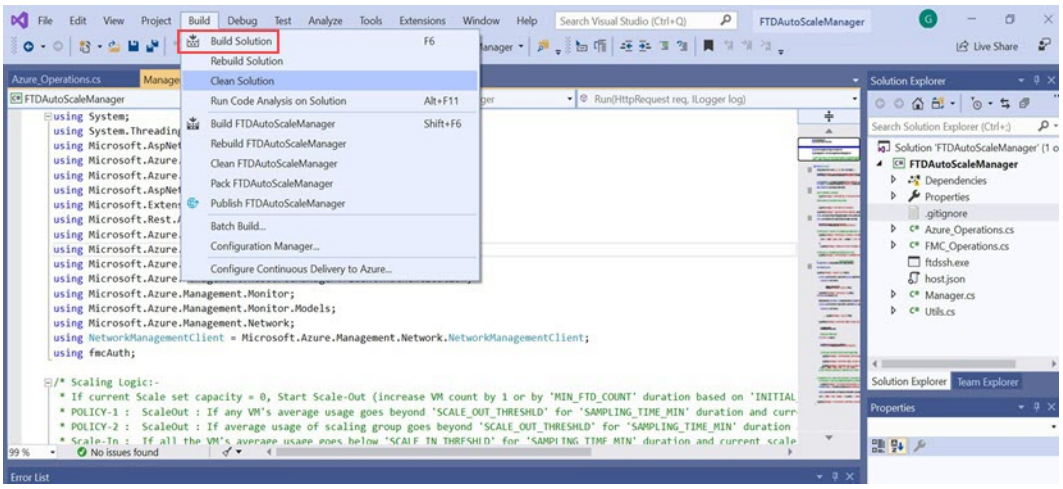
（注） Azure 関数は C# を使用して記述されます。

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

### Visual Studio を使用したビルド

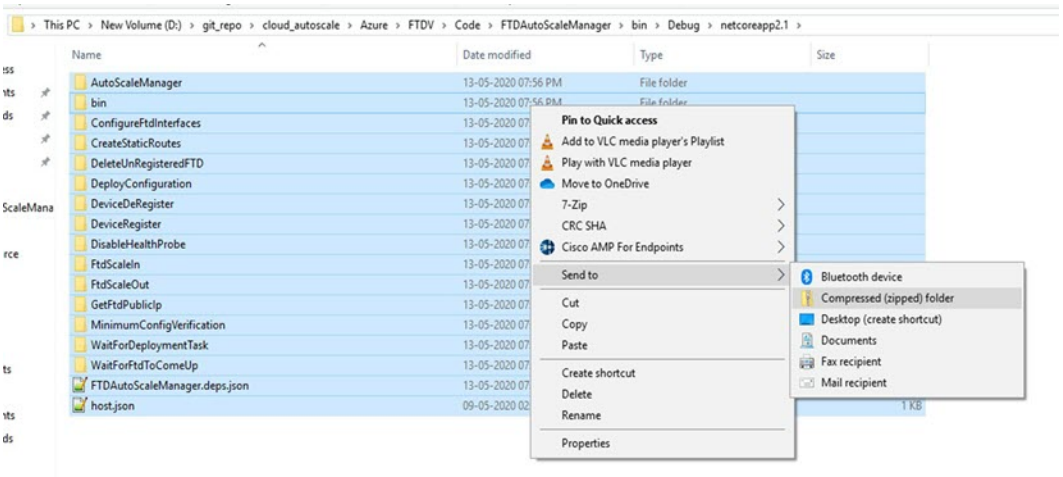
1. 「code」フォルダをローカルマシンにダウンロードします。
2. 「FTDAutoScaleManager」フォルダに移動します。
3. Visual Studio でプロジェクトファイル「FTDAutoScaleManager」を開きます。
4. クリーンアップしてビルドするには、Visual Studio の標準手順を使用します。

図 *34 : Visual Studio* ビルド




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

図 *35 : ASM_Function.zip* のビルド



# Azure Virtual WAN への Cisco Secure Firewall Threat Defense Virtual の展開

## Azure Virtual WAN での Threat Defense Virtual の概要

Microsoft Azure Virtual WAN では、「ハブアンドスポーク」アーキテクチャが採用されており、さまざまな仮想ネットワークとブランチロケーション全体のトラフィックを管理できます。Azure Virtual WAN 内では、Threat Defense Virtual と Azure Virtual ハブを統合することで、組織のオンプレミス（スポーク）ネットワーク（本社、ブランチ、リモートユーザーなど）から発信されたトラフィックがハブを通過し、Azure ネットワーク上の Vnet にアクセスする際の効率的な管理と検査が容易になります。統合し、Threat Defense Virtual 機能をファイアウォールとして使用することで、専用の接続チャネルを介したネットワークトラフィックの管理、検査、フィルタリング、およびルーティングが容易になります。

（注） Azure Virtual WAN では、インターフェイスが 3 つだけの Threat Defense Virtual 導入モデルがサポートされています。

Azure Virtual WAN ハブに Threat Defense Virtual を展開すると、次のような利点を得られます。

- ハブに接続された各スポークにファイアウォール ソリューションを実装する必要がない。
- 内部ロードバランサ（ILB）の Azure の組み込み機能を活用できる。
- 展開時の事前定義された設定によるインスタンスのスケーリング。

仮想 WAN ハブへの Threat Defense Virtual の展開については、「Azure Virtual WAN への Threat Defense Virtual の展開」を参照してください。

### Azure Virtual WAN 上の Threat Defense Virtual を介したトラフィックルーティング

#### Azure Virtual WAN でのトラフィックのルーティング方法

Azure Virtual WAN は、ルーティングテーブルを常に更新および共有しながら、異なる Azure ネットワーク間でトラフィックを送信するための最適なルートを決定するのに役立つダイナミック ルーティング プロトコルであるボーダー ゲートウェイ プロトコル（BGP）を提供します。仮想 WAN ハブは、BGP エンドポイント（高可用性用）と自律システム番号（ASN）のセットを提供します。これらは、Management Center で Threat Defense Virtual の BGP ネイバーとして設定する必要があります。

スタティックルーティング方式を使用して、Threat Defense Virtual でルートを手動で設定することもできます。

Azure でのルーティングの詳細 については、Azure ドキュメントの「BGP および VPN Gateway について」を参照してください。

### ルーティングインテント

ルーティングインテントは、検査のためにハブに展開された Threat Defense Virtual ファイアウォールにインターネット向けトラフィックとプライベートトラフィックを転送するプロセスを簡素化する、Azure Virtual WAN ハブのルーティング機能です。

詳細 については、Azure ドキュメントの Routing Intent [英語] を参照してください。

# システム要件

### スケーリング単位

最大スループットを実現するために必要なスケーリングは、Azure Virtual WAN ハブでの展開時に選択または設定する Threat Defense Virtual インスタンス（NVA）のサイズと数によって異なります。

例：**D3_V2** サイズの 2 つの Threat Defense Virtual インスタンスで 2.8 Gbps をサポートできる場合、NVA スループットは **Scale-Unit-4: 2.8 Gbps** として定義されます。

表 *21* : インスタンスタイプに基づく *Threat Defense Virtual* スループットレベル

| スケール単位 | Threat Defense Virtual インスタンス | インスタンス タイプ | スループットのサポートレベル |
|---|---|---|---|
| 4 | 2 | Standard_D3_v2 | 3.2 Gbps |
| 10 | 2 | Standard_D4_v2 | 4.8 Gbps |
| 20 | 2 | Standard_D5_v2 | 12 Gbps |
| 40 | 3 | Standard_D5_v2 | 18 Gbps |
| 60 | 4 | Standard_D5_v2 | 24 Gbps |
| 80 | 5 | Standard_D5_v2 | 30 Gbps |

# 制限事項

### インターフェイス

Azure の制限により、NVA でサポートできるネットワーク インターフェイスは最大 3 つなので、Azure Virtual WAN ハブの Threat Defense Virtual では、展開用に 3 つ のインターフェイスがサポートされます。

（注） 3 つのインターフェイスモデルをサポートする Threat Defense Virtual バージョン 7.4.1 以降は、Azure Virtual WAN の展開と互換性があります。

Threat Defense Virtual ネットワーク インターフェイスの 3 つのサブネットは次のとおりです。

- **管理インターフェイス**：パブリック IP アドレスを使用して Threat Defense Virtual を Management Center に接続する**最初のインターフェイス**です。
- **外部インターフェイス（必須）**：Threat Defense Virtual を信頼できないパブリック IP アドレスに接続する **2 番目のインターフェイス**です。
- **内部インターフェイス（必須）**：Threat Defense Virtual を仮想 WAN ハブに接続し、信頼できるプライベート IP アドレス上のホストネットワーク内に接続する **3 番目のインターフェイス**です。

### ネットワーク仮想アプライアンス（NVA）としての Threat Defense Virtual

次に、Azure Virtual WAN の NVA としての Threat Defense Virtual のネットワーク構成に関連する主な機能を示します。

- Azure Virtual WAN への Threat Defense Virtual の展開時に、Azure の内部で VNet とサブネットが作成されるため、展開完了後は、VNet とサブネットの変更や作成はできませんが、展開後にインスタンスに接続されている IP アドレスはすべて確認できます。
- インターフェイスごとにネットワーク セキュリティ グループのポートは選択できませんが、それらのポートは展開時に事前定義されます。管理インターフェイスでインターネットに接続できるのは、TCP ポート 443、8305、および 22 のみです。
- 内部インターフェイスでは、Azure Virtual WAN ハブとそのハブに接続されている内部ネットワーク内の通信のみ許可されます。

### Azure Virtual WAN ハブの Threat Defense Virtual へのアクセス制限

管理対象リソースグループに対するマネージドアプリケーションとしてハブに展開されている Threat Defense Virtual インスタンスにアクセスするための承認が必要です。管理者は、この管理対象リソースグループへの限定または制限されたアクセス権を付与できます。

Azure マネージドアプリケーションは、マネージドアプリケーションへのアクセスを定義できるジャストインタイム（JIT）アクセス機能を提供します。JIT の詳細については、Azure のドキュメントの「Azure マネージドアプリケーションの概要」および「ジャストインタイム」を参照してください。

### IP サポート

- IPv4 だけがサポートされます。

### サポートされない機能

- Day-0/カスタムデータによるブートストラップはサポートされていません。
- Threat Defense Virtual は、Azure へのメトリックのストリーミングをサポートしていません。

- オペレーティング システム ディスクの交換による仮想マシンのアップグレードはサポートされていません。
- Threat Defense Virtual への SSH キーベースのログインはサポートされていません。
- PAYG はサポートされていません。

### ライセンシング

シスコ スマート ライセンス アカウントを使用する BYOL。

# ネットワーク トポロジ

Threat Defense Virtual は、Azure Virtual WAN ハブの NVA として、インターネット、ブランチ（サイト）、または VNet などのさまざまなオンプレミスネットワーク（スポーク）からハブを通過するネットワーク トラフィック ルーティングを検査します。

ネットワークトラフィックが通過するトラフィックルートは、次のトポロジに分類されます。

- East-West：ブランチからブランチ
- East-West：VNet から VNet
- North-South：ブランチからインターネット
- North-South：VNet からインターネット

（注） Threat Defense Virtual を介した**インターネットから VNet またはブランチへの**トラフィックは、Cisco Secure Firewall バージョン 7.4.1 ではサポートされていません。

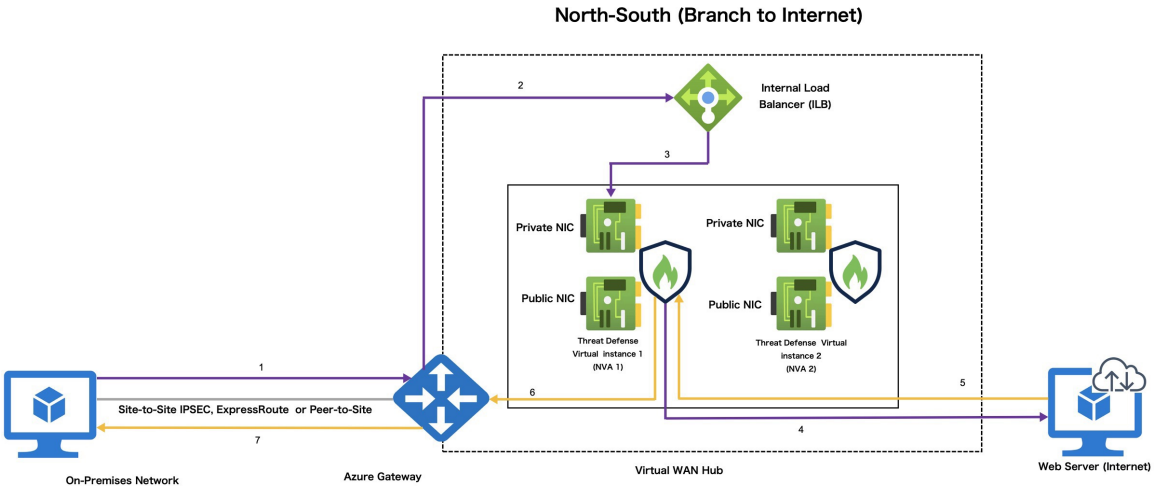
（注） Azure リージョン全体に複数のハブを展開し、仮想 WAN に接続できます。また、East-West および North-South トラフィック検査用の独自の Threat Defense Virtual を持つように各ハブを設定できます。

### 単一の仮想 WAN ハブでの Threat Defense Virtual による North-South トラフィック検査トポロジ

このトポロジは、次の間を移動するネットワークトラフィックを検査する Threat Defense Virtual を参照します。

- 仮想 WAN ハブに接続されているブランチと VNet、およびその逆。

図 *36 : Azure Virtual WAN* ハブの *Threat Defense Virtual North-South* トラフィック検査トポロジ




次の手順では、North-South トラフィック検査のトラフィックフロープロセスについて説明します。

1. オンプレミスネットワークで Azure ゲートウェイにトラフィックが送信されます。
2. ゲートウェイから ILB に転送されます。
3. ILB から Threat Defense Virtual（NVA）に送信されます。
4. NVA SNAT により PIP がインスタンス化され、インターネットに送信されます。
5. Web サーバーがインスタンス PIP Threat Defense Virtual（NVA）に応答すると、SNAT が取り消され、ゲートウェイに転送されます。
6. ゲートウェイからオンプレミスネットワークに転送されます。

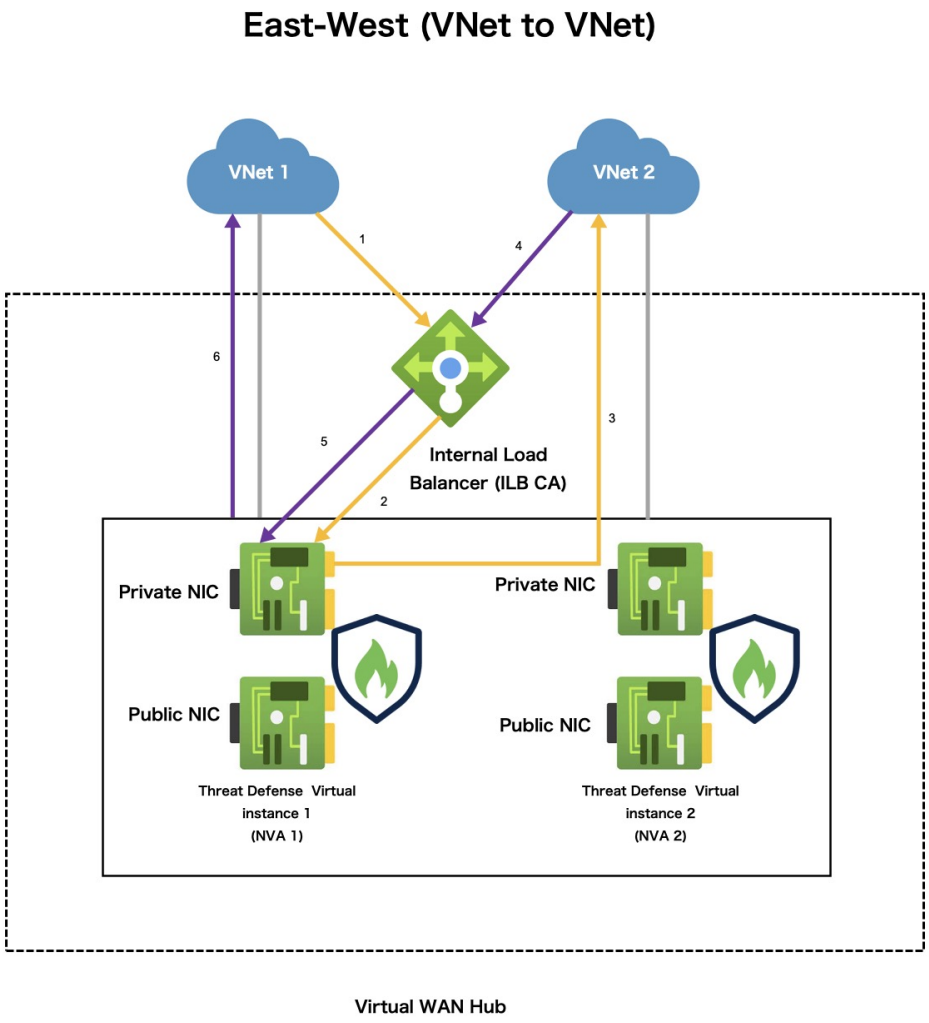
### 単一の仮想 WAN ハブでの Threat Defense Virtual による East-West トラフィック検査トポロジ

このトポロジは、次の間を移動するネットワークトラフィックを検査する Threat Defense Virtual を参照します。

- 仮想 WAN ハブに接続されているブランチと VNet、およびその逆。
- 仮想 WAN ハブに接続されたブランチまたは VNet へのインターネット。

図 *37 : Azure Virtual WAN* ハブの *Threat Defense Virtual East-West* トラフィック検査トポロジ

このトポロジは、Threat Defense Virtual を参照し、仮想 WAN ハブに接続されているサイト間（ブランチとブランチ）間と VNet 間を移動するネットワークトラフィックを検査します。




次の手順では、East-West トラフィック検査のトラフィックフロープロセスについて説明します。

1. VNet1 から ILB にトラフィックが送信されます。
2. ILB でアクティブなインスタンスが 1 つ選択されます。
3. Threat Defense Virtual（NVA）から宛先（VNet 2）に直接送信されます。
4. VNet から ILB にトラフィックが送信されます。
5. ILB から、適切な状態の Threat Defense Virtual（NVA）にトラフィックが完全に転送されます。
6. Threat Defense Virtual（NVA）から VNet 1 にトラフィックが返送されます。

# Azure Virtual WAN への Threat Defense Virtual の展開

Azure マーケットプレイスで入手可能な Azure Virtual WAN 向け Cisco Secure Firewall Threat Defense Virtual サービスを使用して、Azure Virtual WAN ハブに Threat Defense Virtual を展開できます。

## 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。
- 仮想 WAN にハブを作成します。Azure での仮想ハブの作成については、Azure のドキュメントの「ハブを作成する」を参照してください。
- 仮想 WAN ハブのアドレス空間は、/23 以下である必要があります。
- Cisco スマートアカウント。Cisco Software Central で作成できます。

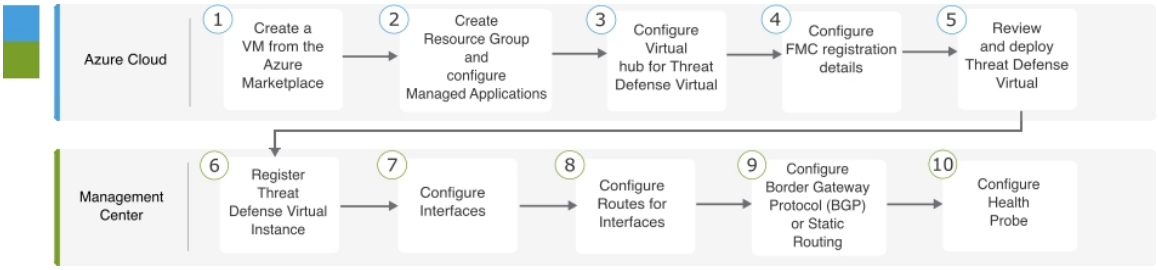
（注） Threat Defense Virtual インスタンスの展開後、そのインスタンスに接続されているすべてのパブリック IP とプライベート IP を確認できます。

### 通信パス

- 管理インターフェイス：Threat Defense Virtual を Management Center に接続するために使用されます。
- 内部インターフェイス（必須）：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）：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。

## 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 Azure Virtual WAN に Threat Defense Virtual を展開する際のワークフローを示しています。



| | ワークスペース | 手順 |
|---|---|---|
| 1 | Azure Cloud | ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：Azure マーケットプレイスで「Cisco Secure Firewall Threat Defense Virtual for Azure VWAN」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 Virtual WAN への Threat Defense Virtual の展開：リソースグループを作成し、マネージドアプリケーションを設定します。 |
| 3 | Azure Cloud | ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：仮想ハブと NVA の詳細を設定します。 |
| 4 | Azure Cloud | ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：FMC 登録の詳細を設定します。 |
| 5 | Azure Cloud | ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：Threat Defense Virtual を確認して展開します。 |
| 6 | Management Center または Device Manager | Management Center での Threat Defense Virtual インスタンスの登録：Threat Defense Virtual インスタンスを登録します。 |
| 7 | Management Center または Device Manager | インターフェイスの設定：外部インターフェイスと内部インターフェイスを設定します。 |
| 8 | Management Center または Device Manager | インターフェイスのルートの設定：ゲートウェイ IP アドレスを計算し、外部インターフェイスと内部インターフェイスのルートを設定します。 |
| 9 | Management Center または Device Manager | トラフィックルーティングの設定：ボーダーゲートウェイプロトコル（BGP）またはスタティックルーティングを設定します。 |
| 10 | Management Center または Device Manager | 正常性プローブの設定：Threat Defense Virtual インスタンスの定期的なヘルスチェックを実行するために ILB を有効にするように正常性プローブを設定します。 |

## ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開

次の手順は、Azure マーケットプレイスで利用できるソリューションテンプレートを使用して、Azure Virtual WAN に Threat Defense Virtual を展開する方法を示しています。これは、Microsoft Azure Virtual WAN 環境で Threat Defense Virtual をセットアップする手順の概略です。

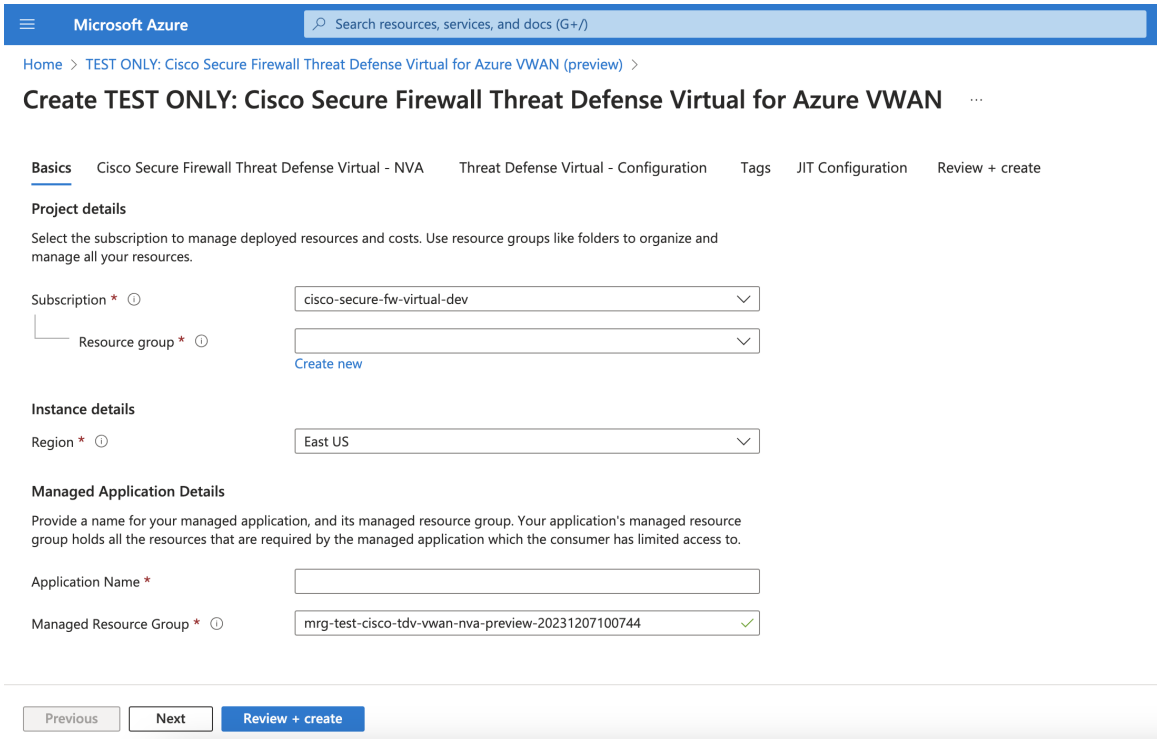
Azure のセットアップの詳細については、「Azure の使用を開始する」を参照してください。

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

Azure ポータルには、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が表示されます。

**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 Secure Firewall Threat Defense Virtual for Azure VWAN** を検索し、サービスを選択し、[作成（Create）] をクリックして [基本（Basics）] ページを表示します。




**ステップ 4** [Basics] 設定を構成します。

a) サブスクリプションを選択します。

b) 新しい [リソースグループ（Resource Group）] を作成します。

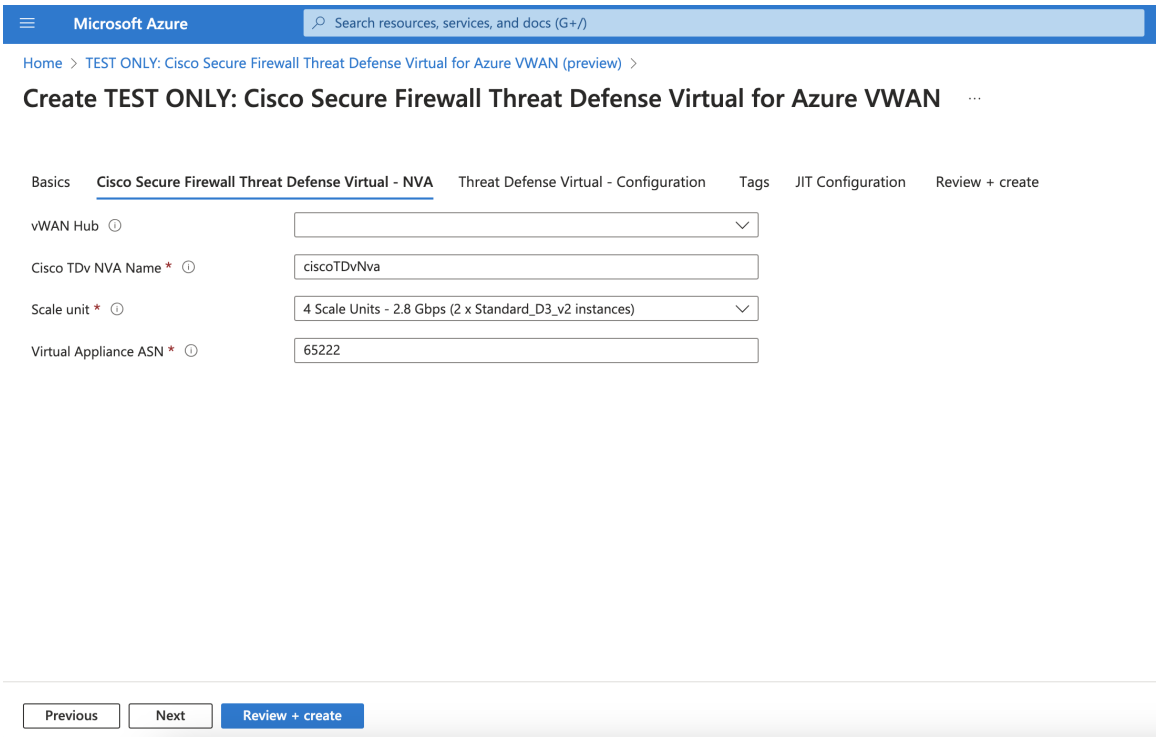
c) 仮想 WAN ハブの地理的な場所または地域を選択します。この展開で使用されるすべてのリソース（仮想 WAN ハブ、Threat Defense Virtual、ネットワーク、ストレージアカウントなど）に関して、同じ場所または地域を選択する必要があります。

**ステップ 5** [マネージドアプリケーションの詳細（Managed Application Details）] の設定を設定します。

a) Threat Defense Virtual インスタンスを NVA として展開している管理対象リソースグループのマネージドアプリケーションの名前を入力します。

b) Threat Defense Virtual インスタンスを展開する管理対象リソースグループを選択します。

**ステップ 6** [次へ（Next）] をクリックして、[Cisco Secure Firewall Threat Defense Virtual：NVA] ページを表示します。




**ステップ 7** 仮想ハブと NVA の詳細を設定します。

a) [vWANハブ（vWAN Hub）] ドロップダウンリストから仮想 WAN ハブを選択して、Threat Defense Virtual インスタンスを展開します。

b) 展開している Threat Defense Virtual インスタンスの適切な名前を入力します。

c) 展開する Threat Defense Virtual インスタンスの数を定義するスケール単位を選択します。

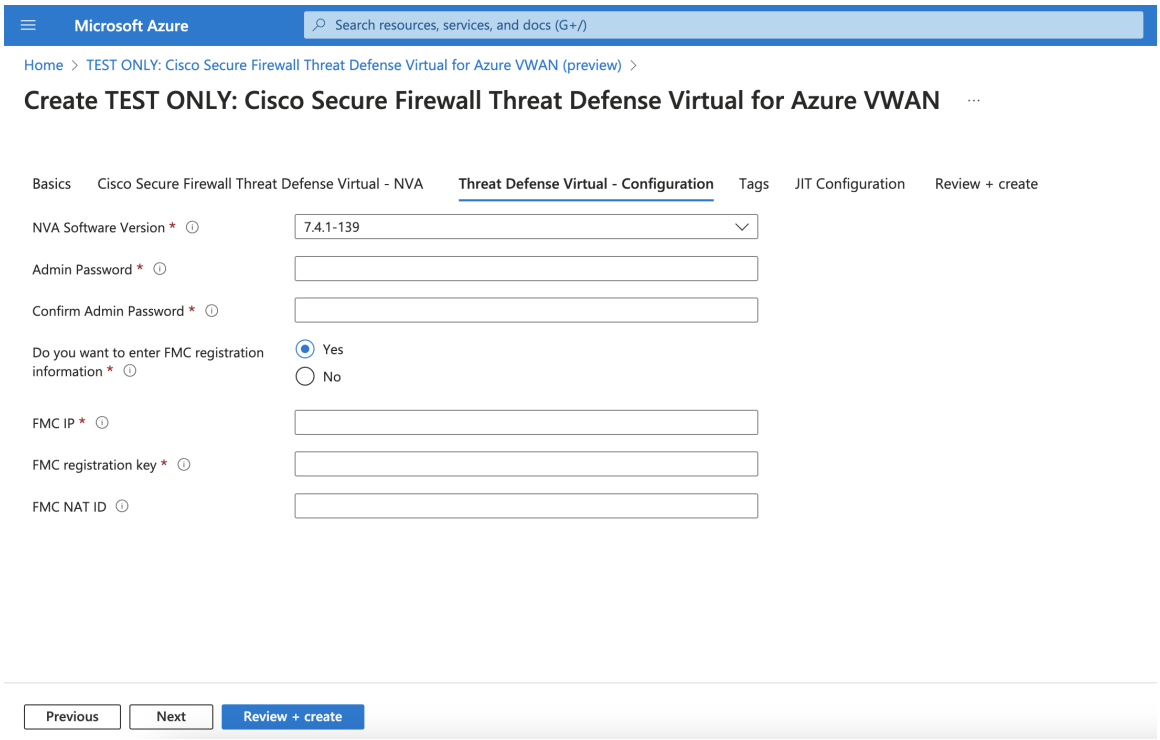
必要な NVA スループットレベルを実現するために必要なスケール単位を選択できます。たとえば、**4 つのスケール単位：2.8 Gbps（2 X Standard_D3_v2_instances）**を選択すると、「**スケール単位の数：スループットレベル（インスタンスタイプがある 2 つの Threat Defense Virtual**）が示唆されます。

（注） スケール単位では、ハブに展開している Threat Defense Virtual インスタンスの数と、関連付けられたインスタンスタイプを定義します。

d) [仮想アプライアンスASN（Virtual Appliance ASN）] を入力します。

（注） 入力する ASN 値は、64,512 ～ 65,534 の範囲内の値である必要があります。

**ステップ 8** [次へ（Next）] をクリックして、[Threat Defense Virtual：設定（Threat Defense Virtual - Configuration）] ページを表示します。




**ステップ 9** [NVAソフトウェアバージョン（NVA Software Version）] ドロップダウンリストから、適切な互換性のあるバージョンを選択します。

（注） このフィールドには、展開している対応する Threat Defense Virtual バージョンと互換性のある NVA ソフトウェアバージョンのリストが表示されます。リストから適切なバージョンを選択してください。

**ステップ 10** Threat Defense Virtual インスタンスを含む管理対象リソースグループにアクセスするために必要な管理者パスワードを作成し、確認します。

**ステップ 11** [はい（Yes）] をクリックして、[FMC登録情報（FMC registration information）] を入力します。

a) [FMC IP] アドレスを入力します。

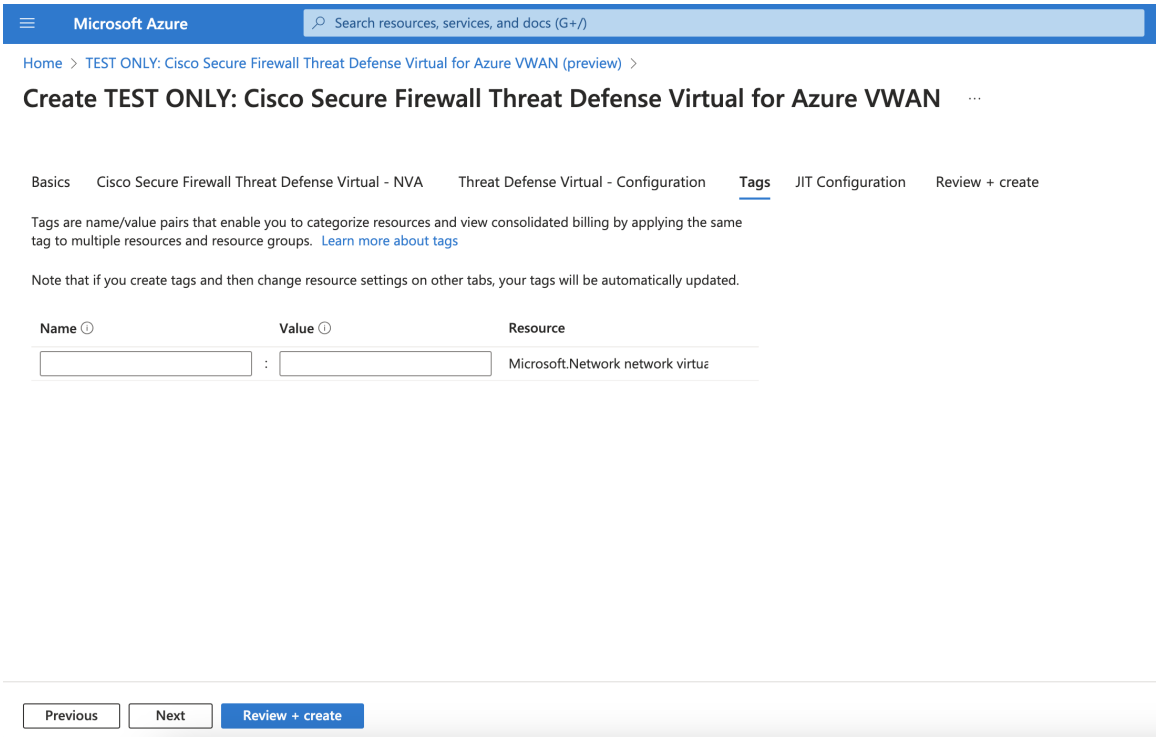
b) Threat Defense Virtual インスタンスを登録するための [FMC登録キー（FMC Registration Key）] を入力します。

（注）
- FMC 登録キーは、1 ～ 37 文字の英数字文字列である必要があります。このキーは、Threat Defense Virtual を追加するときに Management Center で入力します。

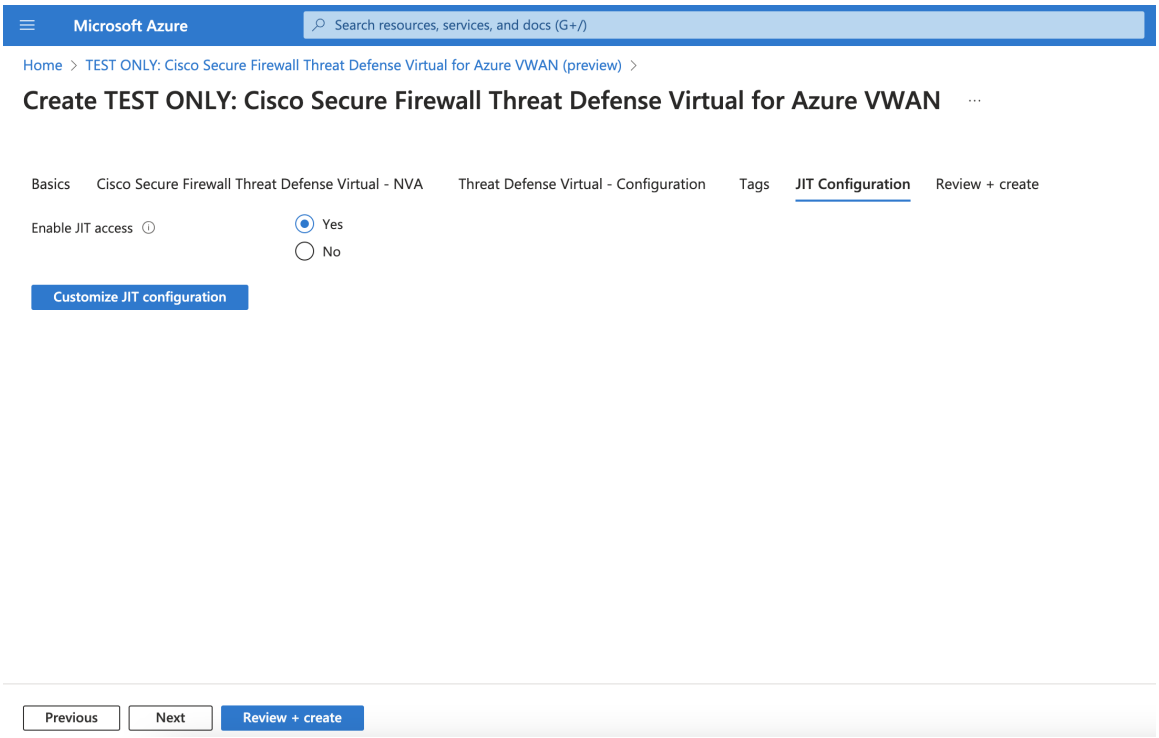
c) （任意）インスタンスの登録時に使用される Management Center NAT ID を入力します。

（注）
- NAT ID は 1 ～ 37 文字の英数字文字列である必要があり、Management Center とデバイス間の登録プロセス中に、一方で IP アドレスが指定されていない場合にのみ使用されます。NAT ID は基本的にワンタイムパスワードなので一意である必要があり、登録を待機している他のデバイスによって使用されないようにする必要があります。登録を成功させるには、Threat Defense Virtual を追加するときに、FMC で同じ NAT ID を指定してください。

**ステップ 12** [次へ（Next）] をクリックして、[タグ（Tags）] を設定します。

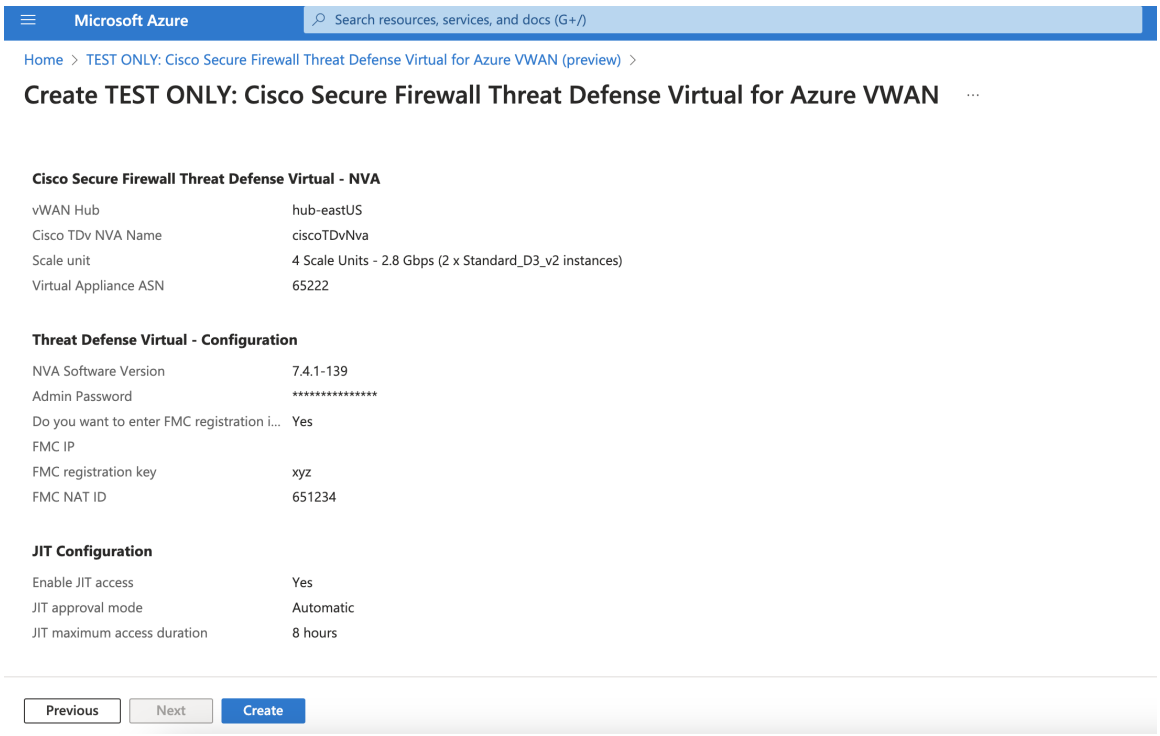



**ステップ 13** [次へ（Next）] をクリックして、[JITの設定（JIT configuration）] ページを表示します。



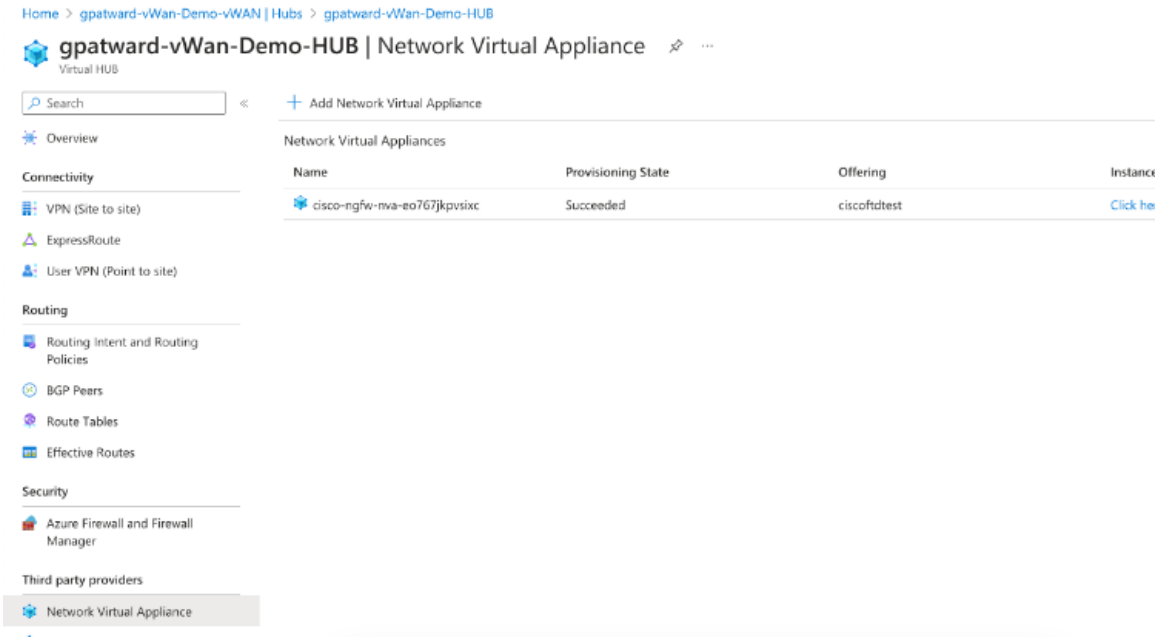
デフォルトでは、[JITアクセスの有効化（Enable JIT access）] オプションは [はい（Yes）] に設定されているため、Threat Defense Virtual インスタンスを管理およびトラブルシューティングするためのプロビジョニングアクセスの JIT が有効になります。

**ステップ 14** [次へ（Next）] をクリックして、[確認と作成（Review+Create）] ページを表示します。




**ステップ 15** 展開する前に、サブスクリプション、NVA、Threat Defense Virtual、および JIT の設定の詳細を確認し、利用規約に同意してから [作成（Create）] をクリックして、仮想 WAN ハブに Threat Defense Virtual（NVA）を展開する必要があります。

**ステップ 16** **[ホーム（Home）]> [セキュリティ（Security）]> [サードパーティプロバイダー（Third-party providers）]** の順に選択し、[ネットワーク仮想アプライアンス（Network Virtual Appliance）] をクリックして、ハブで作成された NVA を表示します。




**ステップ 17** [NVA] をクリックして、展開されたすべての Threat Defense Virtual インスタンスを表示します。

インスタンスの管理パブリック IP アドレスを使用して Threat Defense Virtual にアクセスし、SSH を使用してログインできます。

（注） ハブに展開する各 Threat Defense Virtual インスタンスのパブリック IP アドレスは、Management Center でのインスタンスの登録に使用されます。

### 次のタスク

Management Center のハブに展開した Threat Defense Virtual インスタンスを登録して設定します。

# Management Center での Threat Defense Virtual の設定

ハブに展開された各 Threat Defense Virtual インスタンスは、Management Center を介して設定します。

デバイスグループを含め、Threat Defense Virtual の設定と管理に必要なすべてのオブジェクトを作成すると、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 Threat Defense Virtual インスタンスにプッシュされます。

ここでは、Management Center で Threat Defense Virtual インスタンスを設定するための基本的な手順の概要を示します。

詳細については、Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド [英語]を参照してください。

# Management Center での Threat Defense Virtual インスタンスの登録

仮想 WAN ハブに展開されているすべての Threat Defense Virtual インスタンスを、Management Center の共通のデバイスグループに登録する必要があります。登録すると、各インスタンスにポリシーと設定をすばやく展開できます。

### 始める前に

- Azure Virtual WAN ハブに展開されている各 Threat Defense Virtual インスタンスの管理パブリック IP アドレスが必要です。このアドレスは、Management Center にデバイスをセットアップして登録するために使用されます。
- Management Center でデバイスグループを作成します。「デバイスグループの追加」を参照してください。
- アクセス コントロール ポリシーを作成します。「基本的なアクセス コントロール ポリシーの作成」を参照してください。
- ハブに Threat Defense Virtual を展開中に作成された FMC 登録キー。

**ステップ 1** Management Center にログインします。
**ステップ 2** [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
**ステップ 3** **[追加（Add）]** > **[デバイス（Device）]**の順にクリックします。
**ステップ 4** ハブに展開されている Threat Defense Virtual インスタンスのパブリック IP アドレスを入力します。
**ステップ 5** Threat Defense Virtual インスタンスの表示名を指定します。
**ステップ 6** ハブに Threat Defense Virtual を展開中に作成した Management Center の**登録キー**を入力します。
**ステップ 7** [グループ（Group）] ドロップダウンリストから、Threat Defense Virtual インスタンスを追加するデバイスグループを選択します。
**ステップ 8** [アクセスコントロールポリシー（Access Control Policy）] ドロップダウンリストから、Threat Defense Virtual インスタンスに適用するポリシーを選択します。
**ステップ 9** 必要に応じて、その他の詳細を入力します。
**ステップ 10** [登録（Register）] をクリックします。
**ステップ 11** 他の Threat Defense Virtual インスタンスを登録するには、ステップ 1 ～ 10 を繰り返します。

### 次のタスク

Threat Defense Virtual インスタンスのインターフェイスを設定します。

# インターフェイスの設定

Threat Defense Virtual インスタンスを登録したら、Management Center でそのインスタンスのインターフェイスを設定する必要があります。

Azure Virtual WAN では、次のように設定された **3 つの**インターフェイスのみサポートされます。

- パブリック IP を最初のインターフェイスとして使用する管理インターフェイス。
- パブリック IP を 2 番目のインターフェイスとして使用する外部インターフェイス。
- 3 番目のインターフェイス（プライベート IP のみを持つ）としてのプライベート IP を持つ内部インターフェイス。

**ステップ 1** Management Center にログインします。
**ステップ 2** [デバイス（Devices）] ページに移動します。
**ステップ 3** 登録した Threat Defense Virtual に対応する [編集（Edit）] アイコンをクリックします。
**ステップ 4** インターフェイスに対応する [編集（Edit）] アイコンをクリックします。例：**GigbitEthernet0/0**。
**ステップ 5** 最初のインターフェイス の名前として **`outside`** を入力します。
**ステップ 6** [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効にします。
**ステップ 7** [セキュリティゾーン（Security Zone）] ドロップダウンリストから [外側（outside）] を選択します。
**ステップ 8** [IPv4] メニューをクリックして、インターフェイスに IP のタイプを割り当てます。
**ステップ 9** [IPタイプ（IP Type）] ドロップダウンリストから、[DHCPの使用（Use DHCP）] を選択して、DHCP から IP アドレスを取得するようにインターフェイスを設定します。
**ステップ 10** [DHCPを使用してデフォルトルートを取得（Obtain default route using DHCP）] チェックボックスをオンにします。
**ステップ 11** [デフォルトルートメトリック（Default route metric）] に **`1`** と入力します。
**ステップ 12** [OK] をクリックしてコンフィギュレーションを保存します。
**ステップ 13** ステップ 1 ～ 10 を繰り返して、内部インターフェイスを設定します。

### 次のタスク

インターフェイスのルートを設定します。

# インターフェイスのルートの設定

ネットワークオブジェクトを作成し、ゲートウェイ IP アドレスを割り当てて、外部インターフェイスと内部インターフェイスのスタティックルートを設定します。

- 外部インターフェイスのルート設定では、すべてのパケットのデフォルトルートとしてゲートウェイ IP アドレスが使用されます。
- 内部インターフェイスのルート設定では、正常性プローブパケットおよびハブネットワーク範囲宛てのパケットのデフォルトルートとしてゲートウェイ IP アドレスが使用されます。

ゲートウェイ IP アドレスは、各インターフェイスの IP アドレスとサブネットマスクアドレスを使用して計算されます。

## 外部および内部インターフェイスのゲートウェイ IP アドレスの計算

ここでは、例を使用して外部インターフェイスと内部インターフェイスのゲートウェイ IP アドレスを計算するプロセスについて説明します。

**ステップ 1** Management Center にログインします。

**ステップ 2** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

**ステップ 3** ハブに展開した Threat Defense Virtual インスタンスにアクセスします。

**ステップ 4** [>_Command] フィールドに、**`show interface GigbitEthernet 0/0`** と入力して外部インターフェイスの設定を取得するか、**`show interface GigbitEthernet 0/1`** と入力して内部インターフェイスの設定の詳細を取得します。

**ステップ 5** ステップ 1 ～ 4 を繰り返して、内部インターフェイスまたは外部インターフェイスの IP アドレスとサブネットマスクアドレスを取得します。

**ステップ 6** コマンドの結果から IP アドレスとサブネットマスクアドレスをメモします。

**ステップ 7** 次の例に従って、内部および外部のゲートウェイ IP アドレスを計算します。

- 外部インターフェイスのゲートウェイ IP アドレスを計算するには、次の手順を実行します。

  **例**：GigabitEthernet0/0（外部インターフェイス）の場合

  IP アドレス：**15.0.112.136**

  [サブネット マスク（Subnet mask）]：**255.255.255.128**

  したがって、ゲートウェイ IP アドレスは（このサブネットの最初の IP アドレス）**15.0.112.129** として計算されます。

- 内部インターフェイスのゲートウェイ IP アドレスを計算するには、次の手順を実行します。

  **例**：GigabitEthernet 0/1（内部インターフェイス）の場合

  IP アドレス：**15.0.112.10**

  [サブネット マスク（Subnet mask）]：**255.255.255.128**

  したがって、ゲートウェイ IP は（このサブネットの最初の IP アドレス）**15.0.112.1** として計算されます。

### 次のタスク

内部インターフェイスと外部インターフェイスのデフォルトルートを設定します。

## 外部インターフェイスのデフォルトルートの設定

**ステップ 1** Management Center にログインします。

**ステップ 2** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

**ステップ 3** Threat Defense Virtual インスタンスをクリックします。

**ステップ 4** **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。

**ステップ 5** [ルートを追加（Add Route）] をクリックします。

**ステップ 6** [インターフェイス（Interface）] ドロップダウンリストから、[外部（Outside）] を選択します。

**ステップ 7** [使用可能なネットワーク（Available Network）] で外部インターフェイスに [any-ipv4] を選択し、[追加（Add）] をクリックします。

**ステップ 8** ゲートウェイの IP アドレスを入力します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) 計算した外部インターフェイスのゲートウェイ IP アドレスを入力します。
e) [保存（Save）] をクリックします。

## 内部インターフェイスのデフォルトルートの設定

### 始める前に

Threat Defense Virtual の CIDR IP アドレスがハブに展開されている必要があります。このアドレスは、内部インターフェイスを設定するために必要です。

**ステップ 1** Management Center にログインします。

**ステップ 2** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

**ステップ 3** Threat Defense Virtual インスタンスをクリックします。

**ステップ 4** **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。

**ステップ 5** [ルートを追加（Add Route）] をクリックします。

**ステップ 6** [インターフェイス（Interface）] ドロップダウンリストから、[内部（Inside）] を選択します。

**ステップ 7** ネットワークオブジェクトを追加して、ハブの CIDR IP アドレスを使用して内部インターフェイスを設定します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) ハブの CIDR IP アドレス（プライベートアドレス空間）を入力します。
e) [保存（Save）] をクリックします。

**ステップ 8** ネットワークオブジェクトを追加して、ロードバランサの正常性プローブの IP アドレスを使用して内部インターフェイスを設定します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) ロードバランサの正常性プローブの IP アドレスを入力します。例：**168.63.129.16**。

この IP アドレスは、標準アドレスまたは固定アドレスです。

**ステップ 9** ゲートウェイの IP アドレスを入力します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) オブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) 計算した内部インターフェイスのゲートウェイ IP アドレスを入力します。
e) [保存（Save）] をクリックします。

# トラフィックルーティングの設定

Threat Defense Virtual インスタンスとハブ間のデータ交換には、スタティックルーティングまたはボーダー ゲートウェイ プロトコル（BGP）を設定できます。これらは、仮想 WAN ハブのネットワークトラフィックに対して設定できる基本的に異なる 2 つのルーティング方法です。

BGP は、ハブと Threat Defense Virtual アプライアンス間のリアルタイムのトラフィック交換に基づいてルートを決定するダイナミック ルーティングプロトコルです。一方、スタティックルーティングでは、事前設定済みのルーティングプロトコルを使用してトラフィックが交換されます。

Azure Virtual WAN の詳細については、Microsoft Azure Virtual WAN のドキュメントを参照してください。

## スタティック ルーティングの設定

**ステップ 1** Management Center にログインします。
**ステップ 2** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。
**ステップ 3** [Threat Defense Virtual] インスタンスをクリックします。
**ステップ 4** **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。
**ステップ 5** [ルートを追加（Add Route）] をクリックします。
**ステップ 6** [インターフェイス（Interface）] ドロップダウンリストから、[外部（Outside）] を選択します。

内部インターフェイスを設定する場合は、[内部（Inside）] を選択します。

**ステップ 7** ネットワークオブジェクトの IP アドレスを追加します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) オブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) IP アドレスを入力します。
e) [保存（Save）] をクリックします。

## BGP ルーティングの有効化

**ステップ 1** Management Center にログインします。
**ステップ 2** [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
**ステップ 3** [Threat Defense Virtual] インスタンスをクリックします。
**ステップ 4** [ルーティング（Routing）] メニューをクリックします。
**ステップ 5** [全般設定（General Settings）] で [BGP] をクリックします。
**ステップ 6** [BGPの有効化（Enable BGP）] チェックボックスをオンにします。
**ステップ 7** 仮想ハブの AS 番号を入力します。
**ステップ 8** [保存（Save）] をクリックします。

### 次のタスク

BGP ネイバーを設定します。

## BGP ネイバーの設定

**ステップ 1** Management Center にログインします。
**ステップ 2** **[BGP]** > **[IPv4]** > **[ネイバー（Neighbor）]** の順に選択します。
**ステップ 3** [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。
**ステップ 4** 仮想ハブの自律システム（AS）番号を入力します。
**ステップ 5** [ネイバー（Neighbor）] で [追加（Add）] をクリックします。
**ステップ 6** メモした BGP エンドポイントの最初の IP アドレスを入力します。
**ステップ 7** [有効なアドレス（Enabled address）] チェックボックスをオンにします。
**ステップ 8** [リモートAS（Remote AS）] フィールドに AS 番号を入力します。
**ステップ 9** [詳細（Advanced）] メニューの [接続検証の無効化（Disable Connection Verification）] チェックボックスをオンにします。
**ステップ 10** [保存（Save）] をクリックします。
**ステップ 11** ステップ 1 ～ 8 を繰り返して、BGP エンドポイントの 2 番目の IP アドレスを追加します。

### 次のタスク

BGP ルート設定を確認します。

## BGP ルートの設定の確認

### 始める前に

BGP エンドポイントを設定後、Threat Defense Virtual と仮想 WAN ハブの間で BGP エンドポイントを介した接続が確立されているか確認する必要があります。

**ステップ 1** Management Center にログインします。
**ステップ 2** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**の順に選択します。
**ステップ 3** [Threat Defense Virtual] インスタンスをクリックします。
**ステップ 4** **[デバイス（Device）]** > **[全般（General）]** ウィジェットで [CLI] をクリックします。
**ステップ 5** [>_Command] フィールドに **show route** と入力し、接続ステータスを表示して確認します。

（注） コード **B** は、Threat Defense Virtual との BGP エンドポイント接続ステータスを示します。

# 正常性プローブの設定

Threat Defense Virtual のステータスが安定していることを確認するには、内部ロードバランサ（ILB）に接続する内部インターフェイス（信頼済み）を設定する必要があります。ILB は TCP ポート 443 を介して定期的なヘルスチェックプローブを実行し、Threat Defense Virtual からの応答を確認します。

**ステップ 1** Management Center にログインします。
**ステップ 2** **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[新しいポリシー（New Policy）]** > **[Threat Defense設定（Threat Defense Settings）]**の順に選択します。
**ステップ 3** Threat Defense Virtual にロードバランサに接続するための**新しいポリシー**を追加します。
**ステップ 4** 追加した新しいポリシーを編集します。
**ステップ 5** [HTTPサーバーの有効化（Enable HTTP Server）] チェックボックスをオンにし、[ポート（Port）] フィールドに **443** と入力します。
**ステップ 6** [+追加（+ Add）] をクリックして、HTTP アドレスを設定します。
**ステップ 7** 正常性プローブの IP アドレス名を選択します。
**ステップ 8** [使用可能なゾーン/インターフェイス（Available Zone/Interfaces）] から必要な IP アドレスを選択し、[追加（Add）] をクリックして [選択した ゾーン/インターフェイス（Selected Zones/Interfaces）] に追加します。
**ステップ 9** [OK] をクリック
**ステップ 10** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**の順に選択します。

**ステップ 11** [適用済みポリシー（Applied Policies）] ウィジェットの編集アイコンをクリックします。

**ステップ 12** [プラットフォーム設定（Platform Settings）] ドロップダウンリストからこのポリシーを選択します。

**ステップ 13** 必要に応じてセキュリティポリシーを更新して適用します。

HTTP アクセスの設定の詳細については、Configuring HTTP を参照してください。

## トラブルシューティング

次に、仮想 WAN での Threat Defense Virtual 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。

- トラフィックは Threat Defense Virtual にルーティングされません。
  - Management Center の正常性プローブチェックに対する Threat Defense Virtual の応答を確認します。
  - 内部インターフェイスと外部インターフェイスの派生ゲートウェイ IP アドレスが正しいか確認します。
  - スタティックルートを確認します。
- 非 RFC 1918 が Threat Defense Virtual に到達しない：ルーティングインテントでプライベートアドレスとして明示的に指定されている非 RFC 1918 の範囲を確認します。
- Threat Defense の展開エラー：Threat Defense Virtual の展開中に、**ハブプレフィックス長は 23 以下である必要がある**（**Hub Prefix Length should be less or equal to 23**）というエラーが表示された場合は、ハブのアドレス空間の CIDR が **/23** 以下であることを確認します。

# Azure での IPv6 サポート対象 Secure Firewall Threat Defense Virtual の展開

この章では、Azure ポータルから IPv6 サポート対象の Threat Defense Virtual を展開する方法について説明します。

# Azure での IPv6 をサポートする展開について

Threat Defense Virtual 製品は、7.3 以降、IPv4 と IPv6 の両方をサポートします。Azure では、仮想ネットワークを作成または使用する Marketplace サービスから Threat Defense Virtual を直接展開できますが、現在、Azure の制限により、Marketplace アプリケーション製品は、IPv4 ベースの VNet/サブネットのみを使用または作成するように制限されています。IPv6 アドレスを既存の VNet に手動で設定することはできますが、IPv6 サブネットで設定された VNet に新しい Threat Defense Virtual インスタンスを追加することはできません。Azure では、Marketplace を

介してリソースを展開する方法以外の代替アプローチを使用してサードパーティのリソースを展開するように、一定の制限を課しています。

シスコは現在、IPv6 アドレッシングをサポートするために Threat Defense Virtual を展開する 2 つの方法を提供しています。

次の 2 つの異なるカスタム IPv6 テンプレートが提供されます。

- [カスタムIPv6テンプレート（ARMテンプレート）（Custom IPv6 template (ARM template)）]：Azure 上の Marketplace イメージを内部的に参照する Azure Resource Manager（ARM）テンプレートを使用して、IPv6 設定の Threat Defense Virtual を展開するために提供されます。このテンプレートには、IPv6 サポート対象の Threat Defense Virtual を展開するように設定可能なリソースとパラメータ定義を含む JSON ファイルが含まれています。このテンプレートを使用するには、「Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （280 ページ）」を参照してください。

  プログラムによる展開は、PowerShell、Azure CLI、ARM テンプレート、または API を介してカスタムテンプレートを展開するために、Azure Marketplace 上の VM イメージへのアクセスを許可するプロセスです。VM へのアクセスを許可せずに、これらのカスタムテンプレートを VM に展開することは制限されています。このようなカスタムテンプレートを VM に展開しようとすると、次のエラーメッセージが表示されます。

  *Legal terms have not been accepted for this item on this subscription. To accept legal terms ….and configure programmatic deployment for the Marketplace item …..*

  次のいずれかの方法を使用して、Azure でのプログラムによる展開を有効にして、Marketplace イメージを参照するカスタム IPv6（ARM）テンプレートを展開できます。

  - **Azure ポータル**：カスタム IPv6 テンプレート（ARM テンプレート）を展開するために、Azure Marketplace で利用可能な Threat Defense Virtual の提供に対応するプログラムによる展開オプションを有効にします。
  - **Azure CLI**：CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

- **カスタム VHD イメージと IPv6 テンプレート（ARM テンプレート）**：Azure で VHD イメージと ARM テンプレートを使用して管理対象イメージを作成します。このプロセスは、VHD とリソーステンプレートを使用した Threat Defense Virtual の展開に似ています。このテンプレートは、展開中に管理対象イメージを参照し、IPv6 サポート対象の Threat Defense Virtual を展開するために Azure にアップロードして設定できる ARM テンプレートを使用します。VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開（287 ページ）を参照してください。

カスタム IPv6 テンプレートを使用した Marketplace イメージまたは VHD イメージを参照して、カスタム IPv6 テンプレート（ARM テンプレート）を使用して Threat Defense Virtual を展開するプロセス。

Threat Defense Virtual の展開に含まれる手順は次のとおりです。

表 *22*:

| 手順 | プロセス |
|---|---|
| 1 | IPv6 サポート対象の Threat Defense Virtual の展開を計画している Azure で、Linux VM を作成します。 |
| 2 | Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Threat Defense Virtual を展開する場合に**のみ**、Azure ポータルまたは Azure CLI でプログラムによる展開オプションを有効にします。 |
| 3 | 展開のタイプに応じて、次のカスタムテンプレートをダウンロードします。<br>• Azure Marketplace 参照イメージを使用したカスタム IPv6 テンプレート。<br>カスタム IPv6（ARM）テンプレートを使用した VHD イメージ。 |
| 4 | カスタム IPv6（ARM）テンプレートの IPv6 パラメータを更新します。<br>（注） Marketplace イメージバージョンに相当するソフトウェア イメージ バージョンのパラメータ値は、Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Threat Defense Virtual を展開する場合にのみ必要です。ソフトウェアバージョンの詳細を取得するには、コマンドを実行する必要があります。 |
| 5 | Azure ポータルまたは Azure CLI を使用して ARM テンプレートを展開します。 |

# Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開

Marketplace イメージを参照し、カスタム IPv6 テンプレート（ARM テンプレート）を使用して Threat Defense Virtual を展開するプロセス。

**ステップ 1** Azure 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** 次の方法で、Azure ポータルまたは Azure CLI を使用してプログラムによる展開を有効にします。

Azure ポータルでこのオプションを有効にするには、次の手順を実行します。

a) [Azure（サービス）（Azure Services）] で [サブスクリプション（Subscriptions）] をクリックして、サブスクリプション ブレード ページを表示します。

b) 左側のペインで、[設定（Settings）] オプションの [プラグラムによる展開（Programmatic Deployment）] をクリックします。

VM に展開されたすべてのタイプのリソースが、関連するサブスクリプション製品とともに表示されます。

c) [ステータス（Status）] 列で、カスタム IPv6 テンプレートのプログラムによる展開のために取得する Threat Defense Virtual 製品に対応する [有効化（Enable）] ボタンをクリックします。

または

Azure CLI を使用してこのオプションを有効にするには、次の手順を実行します。

a) Linux VM に移動します。
b) 次の CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

コマンドの実行時に、イメージのサブスクリプションごとに 1 回だけ規約に同意する必要があります。

**# Accept terms**

**az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>**

**# Review that terms were accepted (i.e., accepted=true)**

**az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>**

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-ftdv'
- **<sku/plan>**：'ftdv-azure-byol'

以下は、BYOL サブスクリプションプランで展開するためのプログラムによる Threat Defense Virtual の展開を有効にするコマンドスクリプトの例です。

- **az vm image terms show -p cisco -f cisco-ftdv --plan ftdv-azure-byol**

**ステップ 3** 次のコマンドを実行して、Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得します。

**az vm image list --all -p <publisher> -f <offer> -s <sku>**

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-ftdv'
- **<sku>**：'ftdv-azure-byol'

以下は、Threat Defense Virtual 用の Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得するコマンドスクリプトの例です。

**az vm image list --all -p cisco -f cisco-ftdv -s ftdv-azure-byol**

**ステップ 4** 表示される使用可能な Marketplace イメージバージョンのリストから、いずれかの Threat Defense Virtual バージョンを選択します。

Threat Defense Virtual の IPv6 サポート展開の場合は、Threat Defense Virtual バージョンを 73* 以上として選択する必要があります。

**ステップ 5** Cisco GitHub リポジトリから Marketplace カスタム IPv6 テンプレート（ARM テンプレート）をダウンロードします。

**ステップ 6** パラメータ テンプレート ファイル（JSON）で展開値を指定して、パラメータファイルを準備します。

次の表で、Threat Defense Virtual カスタム展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| vmName | csf-tdv | Azure で Threat Defense Virtual VM に名前を付けます。 |
| softwareVersion | 730.33.0 | Marketplaceイメージバージョンのソフトウェアバージョン。 |
| billingType | BYOL | ライセンス方式はBYOLまたはPAYG です。<br>BYOL ライセンスはPAYG と比較して費用対効果が高いため、BYOLサブスクライブ展開を選択することをお勧めします。 |
| adminUsername | hjohn | Threat Defense Virtual にログインするユーザー名。<br>管理者に割り当てられる予約名「admin」は使用できません。 |
| adminPassword | E28@4OiUrhx! | 管理者アカウントのパスワード。<br>パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。 |
| vmStorageAccount | hjohnvmsa | Azure ストレージアカウント。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は、3 ～ 24 文字の長 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| | | さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。 |
| availabilityZone | 0 | 展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。<br>可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。 |
| customData | {\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\":\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"} | 第 0 日構成で Threat Defense Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。<br>• 「admin」ユーザーパスワード<br>• Management Center Virtual ホスト名<br>• 管理用の Management Center Virtual ホスト名または CSF-DM。<br>「ManageLocally : yes」：これにより、CSF-DM が Threat Defense Virtual マネージャとして使用されるように設定されます。<br>Management Center Virtual を Threat Defense Virtual マネージャとして設定し、Management Center Virtual で同じ設定をするのに必要なフィールドに入力することもできます。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| virtualNetworkResourceGroup | cisco-tdv-rg | 仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。 |
| virtualNetworkName | cisco-tdv-vent | 仮想ネットワークの名前。 |
| virtualNetworkNewOrExisting | new | このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。 |
| virtualNetworkAddressPrefixes | 10.151.0.0/16 | これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| virtualNetworkv6AddressPrefixes | ace:cab:deca::/48 | これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet1Name | mgmt | 管理サブネット名。 |
| Subnet1Prefix | 10.151.1.0/24 | これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet1IPv6Prefix | ace:cab:deca:1111::/64 | これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet1StartAddress | 10.151.1.4 | 管理インターフェイスの IPv4 アドレス。 |
| subnet1v6StartAddress | ace:cab:deca:1111::6 | 管理インターフェイスの IPv6 アドレス。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| Subnet2Name | diag | データインターフェイス 1 のサブネット名。 |
| Subnet2Prefix | 10.151.2.0/24 | これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet2IPv6Prefix | ace:cab:deca:2222::/64 | これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet2StartAddress | 10.151.2.4 | データインターフェイス 1 の IPv4 アドレス。 |
| subnet2v6StartAddress | ace:cab:deca:2222::6 | データインターフェイス 1 の IPv6 アドレス。 |
| Subnet3Name | inside | データインターフェイス 2 のサブネット名。 |
| Subnet3Prefix | 10.151.3.0/24 | これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet3IPv6Prefix | ace:cab:deca:3333::/64 | これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet3StartAddress | 10.151.3.4 | データインターフェイス 2 の IPv4 アドレス。 |
| subnet3v6StartAddress | ace:cab:deca:3333::6 | データインターフェイス 2 の IPv6 アドレス。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| Subnet4Name | outside | データインターフェイス 3 のサブネット名。 |
| Subnet4Prefix | 10.151.4.0/24 | これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet4IPv6Prefix | ace:cab:deca:4444::/64 | これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet4StartAddress | 10.151.4.4 | データインターフェイス 3 の IPv4 アドレス。 |
| subnet4v6StartAddress | ace:cab:deca:4444::6 | データインターフェイス 3 の IPv6 アドレス。 |
| vmSize | Standard_D4_v2 | Threat Defense Virtual VM のサイズ。Standard_D3_v2 がデフォルトです。。 |

**ステップ 7** ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Threat Defense Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

### 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ーを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Secure Firewall Management Center を使用して Threat Defense Virtual を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center」を参照してください。

- [ローカルマネージャーを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、Secure Firewall Device Manager を使用して Threat Defense VirtualThreat Defense VirtualThreat Defense VirtualThreat Defense Virtual を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall device manager」を参照してください。

  管理オプションを選択する方法の概要については、「How to Manage Your Secure Firewall Threat Defense Virtual Device」を参照してください。

# VHD およびカスタム IPv6 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 Threat Defense Virtual イメージを作成できます。このプロセスは、VHD とリソーステンプレートを使用した Threat Defense Virtual の展開に似ています。

### 始める前に

- Github の VHD および ARM の最新テンプレートを使用した Threat Defense Virtual 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。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成
  - Azure ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、Threat Defense Virtual 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。

**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 Threat Defense Virtual 圧縮 VHD イメージ（*.bz2）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)）] > [Cisco Secure Firewall Threat Defense Virtual]** の順に選択します。

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-7.1.0-92.vhd.bz2 です。

**ステップ 2** 「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」の**ステップ 2** から**ステップ 8** の手順を実行します。

**ステップ 3** [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 Threat Defense Virtual パラメータファイルを参照します。VHD およびカスタム IPv6（ARM）テンプレートを使用した Azure への Threat Defense Virtual の展開例は、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。

次の表で、Threat Defense Virtual 展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| vmName | csf-tdv | Azure で Threat Defense Virtual VM に名前を付けます。 |
| vmImageId | /subscriptions/{subscription-id}/resourceGroups/{resource-group}/providers/Microsoft.Compute/images/{image-name} | 展開に使用されるイメージの ID。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。 |
| adminUsername | hjohn | Threat Defense Virtual にログインするユーザー名。<br>管理者に割り当てられる予約名「admin」は使用できません。 |
| adminPassword | E28@4OiUrhx! | 管理者アカウントのパスワード。<br>パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。 |
| vmStorageAccount | hjohnvmsa | Azure ストレージアカウント。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は、3 ～ 24 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| availabilityZone | 0 | 展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。<br>可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。 |
| customData | {\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"} | 第 0 日構成で Threat Defense Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。<br>• 「admin」ユーザーパスワード<br>• CSF-MCv ホスト名<br>• 管理用の CSF-MCv ホスト名または CSF-DM。<br>「ManageLocally : yes」：これにより、CSF-DM が Threat Defense Virtual マネージャとして使用されるように設定されます。<br>CSF-MCv を Threat Defense Virtual マネージャとして設定し、CSF-MCv で同じ設定をするのに必要なフィールドに入力することもできます。 |
| virtualNetworkResourceGroup | csf-tdv | 仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。 |
| virtualNetworkName | hjohn-vm-vn | 仮想ネットワークの名前。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| virtualNetworkNewOrExisting | new | このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。 |
| virtualNetworkAddressPrefixes | 10.151.0.0/16 | これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| virtualNetworkv6AddressPrefixes | ace:cab:deca::/48 | これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet1Name | mgmt-ipv6 | 管理サブネット名。 |
| Subnet1Prefix | 10.151.1.0/24 | これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet1IPv6Prefix | ace:cab:deca:1111::/64 | これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet1StartAddress | 10.151.1.4 | 管理インターフェイスの IPv4 アドレス。 |
| subnet1v6StartAddress | ace:cab:deca:1111::6 | 管理インターフェイスの IPv6 アドレス。 |
| Subnet2Name | diag | データインターフェイス 1 のサブネット名。 |
| Subnet2Prefix | 10.151.2.0/24 | これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| Subnet2IPv6Prefix | ace:cab:deca:2222::/64 | これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet2StartAddress | 10.151.2.4 | データインターフェイス 1 の IPv4 アドレス。 |
| subnet2v6StartAddress | ace:cab:deca:2222::6 | データインターフェイス 1 の IPv6 アドレス。 |
| Subnet3Name | inside | データインターフェイス 2 のサブネット名。 |
| Subnet3Prefix | 10.151.3.0/24 | これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| Subnet3IPv6Prefix | ace:cab:deca:3333::/64 | これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet3StartAddress | 10.151.3.4 | データインターフェイス 2 の IPv4 アドレス。 |
| subnet3v6StartAddress | ace:cab:deca:3333::6 | データインターフェイス 2 の IPv6 アドレス。 |
| Subnet4Name | outside | データインターフェイス 3 のサブネット名。 |
| Subnet4Prefix | 10.151.4.0/24 | これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |

| パラメータ名 | 許可される値/タイプの例 | 説明 |
|---|---|---|
| Subnet4IPv6Prefix | ace:cab:deca:4444::/64 | これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。 |
| subnet4StartAddress | 10.151.4.4 | データインターフェイス 3 の IPv4 アドレス。 |
| subnet4v6StartAddress | ace:cab:deca:4444::6 | データインターフェイス 3 の IPv6 アドレス。 |
| vmSize | Standard_D4_v2 | Threat Defense Virtual VM のサイズ。Standard_D3_v2 がデフォルトです。。 |

**ステップ 4** ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Threat Defense Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

### 次のタスク

- Azure で Threat Defense Virtual の IP 設定を更新します。

# Threat Defense Virtualイメージスナップショット

Azure ポータルでスナップショットイメージを使用して、Threat Defense Virtualを作成および展開できます。イメージスナップショットは、状態データのない、複製された Threat Defense Virtual イメージインスタンスです。

## Threat Defense Virtualスナップショットの概要

Threat Defense Virtual インスタンスのスナップショットイメージを作成するプロセスは、Threat Defense Virtual および FSIC に対して実行される最初のブート手順をスキップすることにより、初期システムの初期化時間を最小限に抑えるのに役立ちます。スナップショットイメージは、事前に入力されたデータベースと Threat Defense Virtual 初期ブートプロセスで構成されます。

これにより、イメージは Management Center またはその他の管理センターのシステム ID に関連する一意の ID（UUID、シリアル番号）を再生成できます。このプロセスは、自動スケール展開に不可欠な Threat Defense Virtual の起動時間を短縮するのに役立ちます。

# 管理対象イメージからの Threat Defense Virtual スナップショットイメージの作成

Threat Defense Virtual のイメージスナップショットの作成は、Azure ポータルで Threat Defense Virtual インスタンスの既存の管理対象イメージを複製するプロセスです。

### 始める前に

Azure ポータルで Linux VM の Azure ストレージアカウント内のコンテナにサイズ変更した VHD イメージをアップロードして、Threat Defense Virtual バージョン 7.2 以降の管理対象イメージを作成しておく必要があります。サイズ変更した VHD イメージの作成については、「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 （199 ページ）」を参照してください。

イメージスナップショットの準備をしている Threat Defense Virtual インスタンスを Management Center や Device Manager などのマネージャに登録しないでください。

**ステップ 1** Threat Defense Virtual インスタンスの管理対象イメージを作成した Azure ポータルに移動します。

（注） 複製する予定の Threat Defense Virtual インスタンスが Management Center に登録されていないこと、または他のローカルマネージャに設定されていないこと、または設定が適用されていないことを確認します。

**ステップ 2** [リソースグループ（Resource Group）] に移動し、Threat Defense Virtual インスタンスを選択します。

**ステップ 3** Threat Defense Virtual インスタンスのナビゲーションページで [シリアルコンソール（Serial Console）] をクリックします。

**ステップ 4** 次のスクリプトを使用して、エキスパートシェルからプレスナップショット プロセスを実行します。

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

スクリプトで `prepare_snapshot` コマンドを使用すると、スクリプトの実行の確認を求める中間メッセージが表示されます。スクリプトを実行するには、[Y] を押します。

または、`root@firepower:/ngfw/var/common# prepare_snapshot -f` のように、このコマンドに `-f` を追加して、ユーザーの確認メッセージをスキップしてスクリプトを直接実行することもできます。

このスクリプトは、Threat Defense Virtual インスタンスに関連付けられたすべての回線設定、展開されたポリシー、設定されたマネージャ、UUID を削除します。処理が完了すると、Threat Defense Virtual インスタンスはシャットダウンされます。

**ステップ 5** [キャプチャ（Capture）] をクリックします。

**ステップ 6** [イメージの作成（Create an image）] ページで、既存のリソースグループを選択するか、[リソースグループ（Resource Group）] ドロップダウンリストから新しいリソースグループを作成します。

**ステップ 7** [インスタンスの詳細（Instance Details）] セクションで [いいえ、管理対象イメージのみをキャプチャします（No, capture only a managed image）] をクリックして、管理対象イメージのみを作成します。

**ステップ 8** Threat Defense Virtual インスタンスの管理対象イメージを使用して作成するスナップショットイメージの名前を指定します。

**ステップ 9** [レビューと確認（Review+Create）] をクリックして、Threat Defense Virtual インスタンスの新しいスナップショットイメージを作成します。

### 次のタスク

スナップショットイメージを使用して Threat Defense Virtual インスタンスを展開します。「イメージスナップショットを使用した Threat Defense Virtual インスタンスの展開」を参照してください。

# イメージスナップショットを使用した Threat Defense Virtual インスタンスの展開

### 始める前に

次のことを推奨します。

- Threat Defense Virtual インスタンスのスナップショットイメージが使用可能であることを確認します。

**ステップ 1** Azure ポータルにログインします。

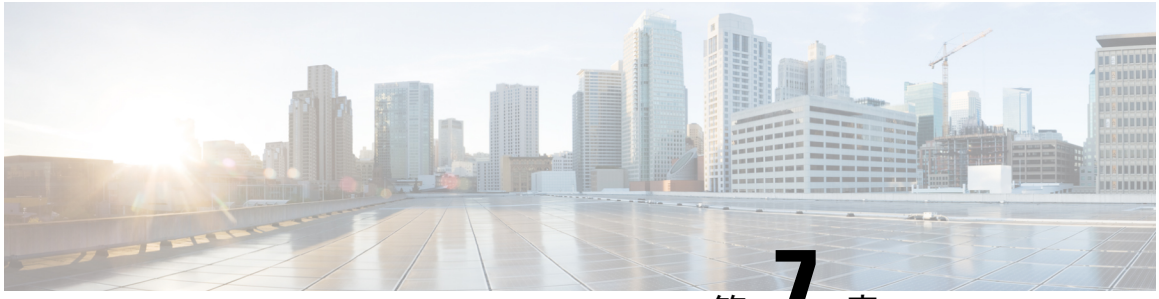
**ステップ 2** 新規に作成したスナップショットイメージのリソース ID をコピーします。

（注） Azure では、あらゆるリソース（スナップショットイメージ）がリソース ID に関連付けられています。新しい Threat Defense Virtual インスタンスを展開するには、スナップショットイメージのリソース ID が必要です。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) 管理対象イメージを使用して作成したスナップショット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** シンタックスは次の様に表されます。**/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>**

**ステップ 3** スナップショットイメージを使用して Threat Defense Virtual インスタンスの展開を続行します。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 （199 ページ） を参照してください。

（注） Threat Defense Virtual コンソールから CLI コマンド **show version** および **show snapshot detail** を実行すると、新しく展開された Threat Defense Virtual インスタンスのバージョンと詳細を確認できます。



第 7 章

# OCI への Threat Defense Virtual の導入

Threat Defense Virtual は、Oracle Cloud Infrastructure（OCI）に展開できます。OCI は、オラクルが提供するパブリック クラウド コンピューティング サービスで、高可用性のホステッド環境でアプリケーションを実行できます。

次の手順では、OCI 環境を準備し、Threat Defense Virtual インスタンスを起動する方法について説明します。OCI ポータルにログインし、OCI Marketplace で Cisco Firepower NGFW virtual firewall（NGFWv）製品を検索し、コンピューティングインスタンスを起動します。Threat Defense Virtual の起動後に、トラフィックの送信元と接続先に応じて、トラフィックをファイアウォールに転送するようにルートテーブルを設定する必要があります。


- 概要 （298 ページ）
- エンドツーエンドの手順 （300 ページ）
- 前提条件 （301 ページ）
- 注意事項と制約事項 （302 ページ）
- ネットワークトポロジの例 （304 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （305 ページ）
- OCI 環境の設定 （306 ページ）
- OCI への Threat Defense Virtual の展開 （310 ページ）
- インターフェイスの接続 （311 ページ）
- 接続された VNIC のルートルールの追加 （312 ページ）
- Auto Scale ソリューションの展開 （313 ページ）
- 前提条件 （314 ページ）
- パスワードの暗号化 （323 ページ）
- Threat Defense Virtual の構成ファイルの準備 （324 ページ）
- Auto Scale ソリューションの展開 （330 ページ）
- 展開の検証 （336 ページ）
- アップグレード （336 ページ）
- ロードバランサのバックエンドセット （337 ページ）
- OCI のAuto Scale 設定の削除 （338 ページ）
- SSH を使用した Threat Defense Virtual インスタンスへの接続 （341 ページ）
- OpenSSH を使用した Threat Defense Virtual インスタンスへの接続 （341 ページ）

• PuTTY を使用した Threat Defense Virtual インスタンスへの接続 （342 ページ）
• IPv6 のトラブルシューティング （343 ページ）

# 概要

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

# OCI のコンピューティングシェイプ

シェイプは、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソースを決定するテンプレートです。Threat Defense Virtual は、次の OCI のシェイプタイプをサポートします。

**表 *23 : Threat Defense Virtual* でサポートされるコンピューティングシェイプ**

| OCI シェイプ | サポートされている Threat Defense Virtual のバージョン | 属性 | | インターフェイス |
|---|---|---|---|---|
| | | oCPU | RAM（GB） | |
| インテル VM.DenseIO2.8 | 7.3 以降 | 8 | 120 | 最小 4、最大 8 |
| インテル VM.StandardB1.4 | 7.3 以降 | 4 | 48 | 最小 4、最大 4 |
| インテル VM.StandardB1.8 | 7.3 以降 | 4 | 96 | 最小 4、最大 8 |
| インテル VM.Standard1.4 | 7.3 以降 | 4 | 28 | 最小 4、最大 4 |
| インテル VM.Standard1.8 | 7.3 以降 | 8 | 72 | 最小 4、最大 8 |
| インテル VM.Standard2.4 | 7.1.0 以降 | 4 | 60 | 最小 4、最大 4 |
| インテル VM.Standard2.8 | 7.1.0 以降 | 8 | 120 | 最小 4、最大 8 |

| OCI シェイプ | サポートされている Threat Defense Virtual のバージョン | 属性 | | インターフェイス |
|---|---|---|---|---|
| | | oCPU | RAM（GB） | |
| インテル VM.Standard3.Flex* | 7.3 以降 | 4 | 16 | 最小 4、最大 4 |
| | 7.3 以降 | 6 | 24 | 最小 4、最大 6 |
| | 7.3 以降 | 8 | 32 | 最小 4、最大 8 |
| インテル VM.Optimized3.Flex* | 7.3 以降 | 4 | 16 | 最小 4、最大 8 |
| | 7.3 以降 | 6 | 24 | 最小 4、最大 10 |
| | 7.3 以降 | 8 | 32 | 最小 4、最大 10 |
| AMD VM.Standard.E4.Flex | 7.3 以降 | 4 | 16 | 最小 4、最大 4 |
| | 7.3 以降 | 6 | 24 | 最小 4、最大 6 |
| | 7.3 以降 | 8 | 32 | 最小 4、最大 8 |

- *SR-IOV モードは、Flex シェイプではサポートされていません。
- OCI では、1 つの oCPU は 2 つの vCPU に相当します。
- Threat Defense Virtual には、少なくとも 4 つのインターフェイスが必要です。

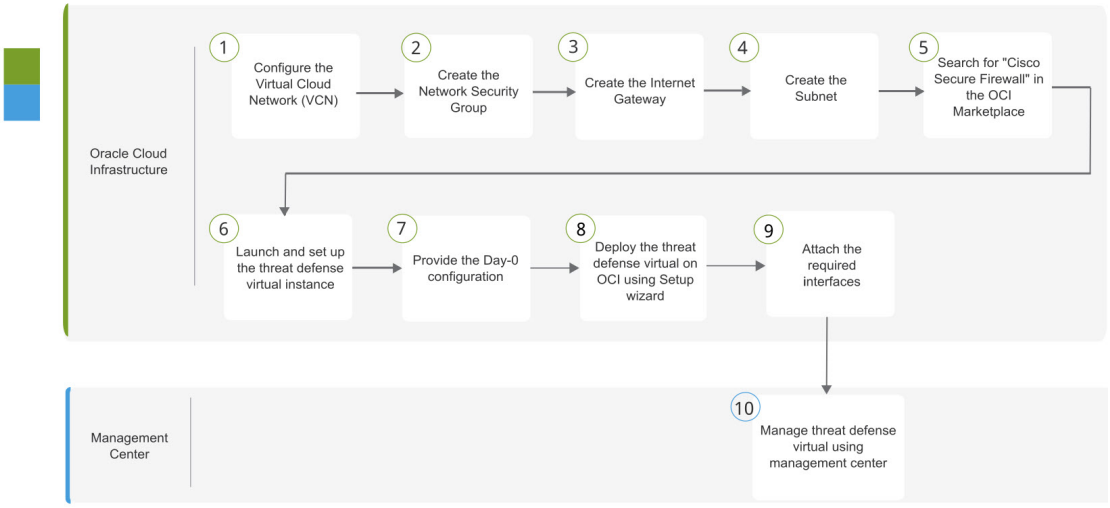
バージョン Threat Defense Virtual7.3 以降でサポートされている OCI コンピューティングシェイプの使用に関する推奨事項。

- OCI マーケットプレイス イメージ バージョン **7.3.0-69-v3** 以降は、Threat Defense Virtual 7.3 以降の OCI コンピューティングシェイプとのみ互換性があります。
- Threat Defense Virtual 7.3 以降でサポートされている OCI コンピューティングシェイプは、新しい展開でのみ使用できます。
- OCI コンピューティング シェイプ バージョン **7.3.0-69-v3** 以降は、Threat Defense Virtual 7.3 より前の OCI コンピューティング シェイプ バージョンを使用して Threat Defense Virtual で展開された VM をアップグレードすることと互換性がありません。
- インスタンスをシャットダウンした後でも、**VM.DenseIO2.8** コンピューティング シェイプ サブスクリプションの課金は継続されます。詳細については、OCIのドキュメントを参照してください。

ユーザーは、OCI でアカウントを作成し、Oracle Cloud Marketplace の Cisco Firepower NGFW 仮想ファイアウォール（NGFWv）製品を使用してコンピューティング インスタンスを起動し、OCI のシェイプを選択します。

# エンドツーエンドの手順

次のフローチャートは、Oracle Cloud Infrastructure に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Oracle Cloud Infrastructure | OCI 環境の設定：Virtual Cloud Network（VCN）を設定します（**[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [CIDRブロック（CIDR block）] > [VCNの作成（Create VCN）]**）。 |
| 2 | Oracle Cloud Infrastructure | ネットワーク セキュリティ グループの作成：ネットワーク セキュリティ グループを作成します（**[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [ネットワーク セキュリティ グループ（Network Security Groups）]> [ネットワーク セキュリティ グループの作成（Create Network Security Group）]**）。 |
| 3 | Oracle Cloud Infrastructure | インターネットゲートウェイの作成：インターネットゲートウェイを作成します**[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [インターネットゲートウェイ（Internet Gateways）] > [インターネットゲートウェイの作成（Create Internet Gateway）]**）。 |

| | ワークスペース | 手順 |
|---|---|---|
| 4 | Oracle Cloud Infrastructure | サブネットの作成：サブネットを作成します（**[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [サブネット（Subnets）] > [サブネットの作成（Create Subnet）]**）。 |
| 5 | Oracle Cloud Infrastructure | OCI への Threat Defense Virtual の展開 （310 ページ） ：OCI Marketplace で「Cisco Secure Firewall」を検索します。 |
| 6 | Oracle Cloud Infrastructure | OCI への Threat Defense Virtual の展開 （310 ページ） ：Threat Defense Virtual インスタンスを起動して設定します。 |
| 7 | Oracle Cloud Infrastructure | OCI への Threat Defense Virtual の展開 （310 ページ） ： Day-0 構成ファイルを指定します。 |
| 8 | Oracle Cloud Infrastructure | OCI への Threat Defense Virtual の展開 （310 ページ）：セットアップウィザードを使用して OCI に Threat Defense Virtual を展開します。 |
| 9 | Oracle Cloud Infrastructure | インターフェイスの接続：インターフェイスを接続します（**[コンピューティング（Compute）] > [インスタンス（Instances）] > [インスタンスの詳細（Instance Details）] > [接続されたVNIC（Attached VNICs）]**）。 |
| 10 | Management Center | Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 |

# 前提条件

- https://www.oracle.com/cloud/ で、OCI アカウントを作成します。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
- Threat Defense Virtual へのライセンス付与。
  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『*Cisco Secure Firewall Management Center Admin Guide*』の「Licensing」を参照してください。

（注） これまで Firewall Threat Defense Virtual 向けにシスコが提供していたすべてのデフォルトのソフトウェア利用資格で IPv6 の設定がサポートされます。

- インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - トラフィック インターフェイス（2）：Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。
- 通信パス：
  - Threat Defense Virtual にアクセスするためのパブリック IP。
- Threat Defense Virtual のシステム要件については、『Cisco Firepower Compatibility Guide』を参照してください。

# 注意事項と制約事項

### サポートされる機能

- OCI 仮想クラウドネットワーク（VCN）での展開
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- IPv6
- Management Center サポートのみ。
- Single Root I/O Virtualization（SR-IOV）をサポート。

### FTDv スマートライセンスのパフォーマンス階層

Threat Defense Virtual 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 *24 : Threat Defense Virtual* 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/32 GB | 16 Gbps | 10,000 |

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『*Cisco Secure Firewall Management Center Admin Guide*』の「Licensing」の章を参照してください。

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

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「OCI での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

### サポートされない機能

- Device Manager を介したローカル管理サポート。
- Threat Defense Virtual ネイティブ HA
- 自動スケール
- トランスペアレント/インライン/パッシブ モード
- DHCP を使用したデータインターフェイス設定

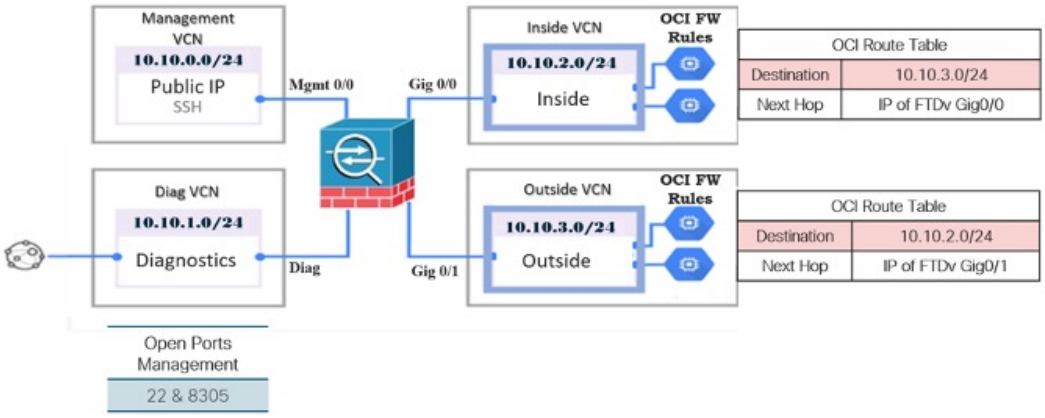
### 制限事項

- OCI に Threat Defense Virtual を展開する場合、Mellanox 5 は SR-IOV モードの vNIC としてサポートされません。
- IPv6 は、OCI 標準に準じた（VCN IPv4 および IPv6）設定のデュアルスタックでのみ機能します。
- 静的設定と DHCP 設定の両方で Firewall Threat Defense Virtual に必要な個別のルーティングルール。

# ネットワークトポロジの例

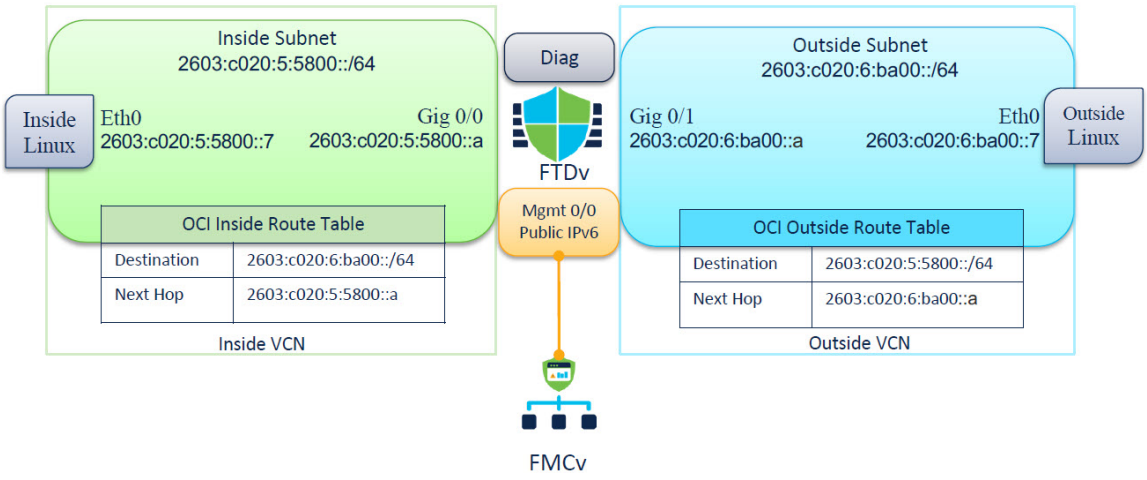
次の図は、Threat Defense Virtual 用に 4 つのサブネット（管理、診断、内部、外部）が OCI 内に設定されたルーテッド ファイアウォール モードの Threat Defense Virtual の推奨トポロジを示しています。

**図 *38 : OCI* 上の *Threat Defense Virtual* の展開例**




### Threat Defense Virtual の IPv6 展開トポロジ

- East-West Traffic Topology




# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# OCI 環境の設定

Threat Defense Virtual 展開用の仮想クラウドネットワーク（VCN）を設定します。少なくとも、Threat Defense Virtual の各インターフェイスに 1 つずつ、合計 4 つの VCN が必要です。

次の手順に進み、管理 VCN を完了できます。次に、[ネットワーキング（Networking）] に戻り、診断、内部、および外部の各インターフェイスの VCN を作成します。

**ステップ 1** OCI にログインし、地域を選択します。

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

**ステップ 2** **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]**を選択し、**[VCN の作成（Create VCN）]** をクリックします。

**ステップ 3** [名前（Name）] に、VCN のわかりやすい名前を入力します（例：*FTDv-Management*）。

**ステップ 4** VCN の **CIDR ブロック**を入力します。

a) IP アドレスの IPv4 CIDR ブロック。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。

（注） この VCN でDNS ホスト名を使用します。

b) IP アドレスの IPv6 CIDR ブロック。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。[::/0] が例として挙げられます。

c) Oracle が仮想クラウドネットワークに割り当てた IPv6/56 プレフィックスとして [IPv6 CIDRブロック（IPv6 CIDR block）] を選択します。

**ステップ 5** [IPv6 CIDRブロックの追加（Add IPv6 CIDR Block）] をクリックして、新しいIPv6ブロックを追加します。

**ステップ 6** VCN の IPv6 プレフィックス（例：/54）を追加します。

**ステップ 7** **[VCN の作成（Create VCN）]** をクリックします。

### 次のタスク

次の手順に進み、管理 VCN を完了します。管理 VCN を完了したら、診断、内部、および外部の各インターフェイスの VCN を作成します。

（注） ナビゲーションメニューからサービスを選択すると、左側のメニューにコンパートメントリストが表示されます。コンパートメントはリソースの整理に役立ち、リソースへのアクセスを制御しやすくなります。ルートコンパートメントは、テナントがプロビジョニングされるときに Oracle によって作成されます。管理者は、ルートコンパートメントにさらに多くのコンパートメントを作成し、アクセスルールを追加して、どのユーザーがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracle のドキュメント『Managing Compartments』[英語] を参照してください。

# ネットワーク セキュリティ グループの作成

ネットワーク セキュリティ グループは、一連の vNIC と、vNIC に適用される一連のセキュリティルールで構成されます。

**ステップ 1** **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [ネットワーク セキュリティ グループ（Network Security Groups）]** を選択し、**[ネットワーク セキュリティ グループの作成（Create Network Security Group）]** をクリックします。

**ステップ 2** [名前（Name）] に、ネットワーク セキュリティ グループのわかりやすい名前を入力します（例：*FTDv-Mgmt-Allow-22-8305* ）。

**ステップ 3** [Next] をクリックします。

**ステップ 4** セキュリティルールを追加します。

a) SSH アクセスに TCP ポート 22 を許可するルールを追加します。

b) HTTPS アクセスに TCP ポート 443 を許可するルールを追加します。

Threat Defense Virtual は Management Center を介して管理できます。これには、HTTPS 接続用にポート 8305 を開く必要があります。

（注） これらのセキュリティルールを管理インターフェイス/VCN に適用します。

**ステップ 5** [作成（Create）] をクリックします。

# インターネットゲートウェイの作成

管理サブネットを公的にアクセス可能にするには、インターネットゲートウェイが必要です。

**ステップ 1** **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [インターネットゲートウェイ（Internet Gateways）]**を選択し、**[インターネットゲートウェイの作成（Create Internet Gateway）]** をクリックします。

**ステップ 2** [名前（Name）] にインターネットゲートウェイのわかりやすい名前を入力します（例：*FTDv-IG*）。

**ステップ 3** **[インターネットゲートウェイの作成（Create Internet Gateway）** をクリックします。

**ステップ 4** インターネットゲートウェイへのルートを追加します。

a) **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [ルートテーブル（Route Tables）]**を選択します。

b) ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。

c) **[ルートルールの追加（Add Route Rules）]** をクリックします。

d) **[ターゲットタイプ（Target Type）]** ドロップダウンから、**[インターネットゲートウェイ（Internet Gateway）]** を選択します。

e) 宛先の IPv4 CIDR ブロックを入力します（例：0.0.0.0/0）。

f) 宛先の IPv6 CIDR ブロックを入力します（例：[::/]）。

g) **[ターゲット インターネット ゲートウェイ（Target Internet Gateway）]** ドロップダウンから、作成したゲートウェイを選択します。

h) **[ルートルールの追加（Add Route Rules）]** をクリックします。

# サブネットの作成

各 VCN には、少なくとも 1 つのサブネットがあります。管理 VCN の管理サブネットを作成します。また、診断 VCN の診断サブネット、内部 VCN の内部サブネット、および外部 VCN の外部サブネットも必要です。

**ステップ 1** **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [サブネット（Subnets）]**を選択し、**[サブネットの作成（Create Subnet）]** をクリックします。

**ステップ 2** サブネットのわかりやすい**名前**を入力します（例：*Management*）。

**ステップ 3** **[サブネットタイプ（Subnet Type）]** を選択します（推奨されるデフォルトの **[地域（Regional）]** のままにします）。

**ステップ 4** [CIDRブロック（CIDR Block）] に値を入力します（例：10.10.0.0/24）。サブネットの内部（非公開）IP アドレスは、この CIDR ブロックから取得されます。

a) IPv6 を有効にする場合は、[IPv6 CIDRブロックを有効にする（ENABLE IPv6 CIDR BLOCK）] チェックボックスをオンにします。
b) [IPv6 CIDRブロック（IPv6 CIDR Block）] で、IPV6 プレフィックス範囲を入力します。

**ステップ 5** **[ルートテーブル（Route Table）]** ドロップダウンから、以前に作成したルートテーブルのいずれかを選択します。

**ステップ 6** サブネットの **[サブネットアクセス（Subnet Access）]** を選択します。

管理サブネットの場合、これは**パブリックサブネット**である必要があります。

**ステップ 7** **[DHCP オプション（DHCP Option）]** を選択します。

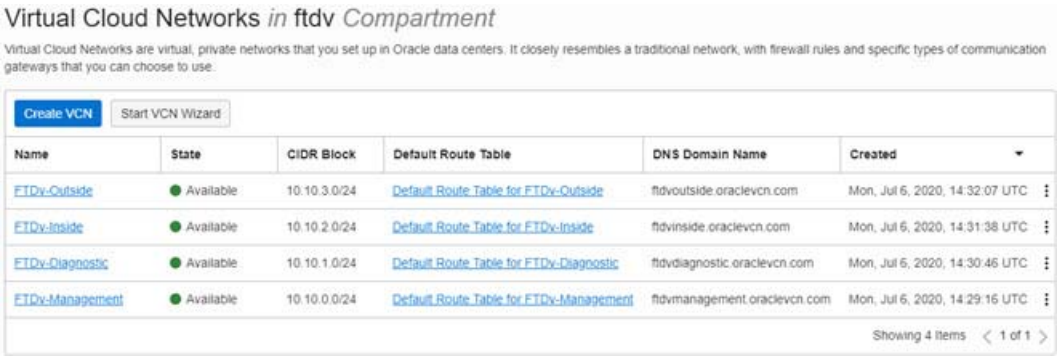
**ステップ 8** 以前作成した **[セキュリティリスト（Security List）]** を選択します。

**ステップ 9** **[サブネットの作成（Create Subnet）]** をクリックします。

### 次のタスク

VCN（管理、診断、内部、外部）を設定すると、Threat Defense Virtual を起動する準備が整います。Threat Defense Virtual VCN 構成の例については、次の図を参照してください。

**図 *39 : Threat Defense Virtual* 仮想クラウドネットワーク**




## クラウドシェルを使用した IPv6 ゲートウェイアドレス

OCI では、各サブネットに一意の IPv6 ゲートウェイアドレスがあり、IPv6 トラフィックが機能するように Threat Defense Virtual で設定する必要があります。このゲートウェイアドレスは、クラウドシェルで OCI コマンドを実行しているサブネットの詳細から取得されます。

**ステップ 1** **[OCI]** > **[CloudShellを開く（OCIクラウドターミナル）（Open CloudShell (OCI Cloud Terminal)）]**に移動します。

**ステップ 2** 次のコマンドを実行して、サブネットから IPv6 の詳細を取得します。

```
oci network subnet get -subnet_id <subnet_OCID>
```

**ステップ 3** コマンドの結果から `ipv6-virtual-router-ip` キーを見つけます。

**ステップ 4** このキーの値をコピーし、必要に応じて使用します。

# OCI への Threat Defense Virtual の展開

Oracle Cloud Marketplace の Cisco Firepower NGFW 仮想ファイアウォール（NGFWv）製品を使用して、コンピューティング インスタンスを介して OCI に Threat Defense Virtual を展開します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[マーケットプレイス（Marketplace）]** > **[アプリケーション（Applications）]**を選択します。

**ステップ 3** マーケットプレイスで「Cisco Firepower NGFW virtual firewall (NGFWv)」を検索して、製品を選択します。

**ステップ 4** 契約条件を確認し、[Oracle の利用規約とパートナーの契約条件を確認して同意します。（I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.）] チェックボックスをオンにします。

**ステップ 5** [インスタンスの起動（Launch Instance）] をクリックします。

**ステップ 6** [名前（Name）] に、インスタンスのわかりやすい名前を入力します（例：*FTDv-6-7*）。

**ステップ 7** **[シェイプの変更（Change Shape）]** をクリックし、Threat Defense Virtual に必要な CPU の数、RAM の量、およびインターフェイスの数が指定されたシェイプ（VM.Standard2.4 など）を選択します（概要（298 ページ）を参照）。

**ステップ 8** **[仮想クラウドネットワーク（Virtual Cloud Network）]** ドロップダウンから、[管理 VCN（Management VCN）] を選択します。

**ステップ 9** 自動入力されていない場合は、**[サブネット（Subnet）]** ドロップダウンから[管理サブネット（Management subnet）] を選択します。

**ステップ 10** **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** にチェックを入れ、管理 VCN に設定したセキュリティグループを選択します。

**ステップ 11** **[パブリック IP アドレスの割り当て（Assign a Public Ip Address）]** オプションボタンをクリックします。

**ステップ 12** **[SSH キーの追加（Add SSH keys）]** の下で、**[公開キーの貼り付け（Paste Public Keys）]** オプションボタンをクリックして、SSH キーを貼り付けます。

Linux ベースのインスタンスは、パスワードの代わりに SSH キーペアを使用してリモートユーザーを認証します。キーペアは、秘密キーと公開キーで構成されます。インスタンスを作成するときに、秘密キーをコンピュータに保持し、公開キーを提供します。ガイドラインについては、『Linux インスタンスでのキーペアの管理（Managing Key Pairs on Linux Instances）』https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htmを参照してください。

**ステップ 13** **[詳細オプションの表示（Show Advanced Options）]** リンクをクリックして、オプションを展開します。

**ステップ 14** [初期化スクリプト（Initialization Script）] の下で、[クラウド初期化スクリプトの貼り付け（Paste Cloud-Init Script）] オプションボタンをクリックして、Threat Defense Virtual の day0 構成を指定します。day0 構成は、Threat Defense Virtual の初回起動時に適用されます。

次に、**[クラウド初期化スクリプト（Cloud-Init Script）]** フィールドにコピーして貼り付けることができる day0 構成の例を示します。

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"IPv6Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey**：これは、デバイスを Management Center に登録するために使用される 1 回限りの登録キーです。登録キーは、ユーザー定義の最大 37 文字の英数字値です。
- **FmcNatId**：これは 1 回限り使用される一意の文字列です（ユーザーが定義）。ただし、デバイスと Management Center が NAT デバイスにより分離されている場合は、この一意の登録キーと同時に一意の NAT ID を入力する必要があります。

**ステップ 15** [作成（Create）] をクリックします。

### 次のタスク

**[作成（Create）]** ボタンをクリックした後、状態が [プロビジョニング（Provisioning）] として表示される Threat Defense Virtual インスタンスをモニターします。

**重要** ステータスをモニターすることが重要です。Threat Defense Virtual インスタンスの状態が [プロビジョニング（Provisioning）] から [実行中（Running）] に移行したら、Threat Defense Virtual の起動が完了する前に必要に応じて VNIC を接続する必要があります。

# インターフェイスの接続

Threat Defense Virtual は、1 つの VNIC が接続された状態で実行状態になります（**[コンピューティング（Compute）]** > **[インスタンス（Instances）]** > **[インスタンスの詳細（Instance Details）]** > **[接続された VNIC （Attached VNICs）]**を参照）。これはプライマリ VNIC と呼ばれ、管理 VCN にマッピングされます。Threat Defense Virtual が最初のブートを完了する前に、VNIC が Threat Defense Virtual で正しく検出されるように、以前に作成した他の VCN サブネット（診断、内部、外部）の VNIC を接続する必要があります。

**ステップ 1** 新しく起動した Threat Defense Virtual インスタンスを選択します。

**ステップ 2** **[接続された VNIC（Attached VNICs）]** > **[VNIC の作成（Create VNIC）]**の順に選択します。

**ステップ 3** [名前（Name）] に、VNIC のわかりやすい名前を入力します（例：*Inside*）。

**ステップ 4** [仮想クラウドネットワーク（Virtual Cloud Network）] ドロップダウンから VCN を選択します。

**ステップ 5** [サブネット（Subnet）] ドロップダウンからサブネットを選択します。

**ステップ 6** **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** をオンにして、選択した VCN 用に設定したセキュリティグループを選択します。

**ステップ 7** [送信元と宛先のチェックをスキップ（Skip Source Destination Check）] をオンにします。

**ステップ 8** （オプション）[プライベート IP アドレス（Private IP Address）] を指定します。これは、VNIC に対して特定の IP を選択する場合にのみ必要です。

IP を指定しない場合、OCI はサブネットに割り当てられた CIDR ブロックから IP アドレスを割り当てます。

**ステップ 9** [変更の保存 (Save Changes)] をクリックし、VNIC を作成します。

**ステップ 10** 展開で必要となる各 VNIC について、この手順を繰り返します。

# 接続された VNIC のルートルールの追加

診断、内部、および外部の各ルートテーブルにルートテーブルルールを追加します。

**ステップ 1** **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]**を選択し、VCN に関連付けられているデフォルトルートテーブル（内部または外部）をクリックします。

**ステップ 2** **[ルートルールの追加（Add Route Rules）]** をクリックします。

**ステップ 3** [ターゲットタイプ（Target Type）] ドロップダウンから、[プライベート IP（Private IP）] を選択します。

**ステップ 4** [宛先タイプ（Destination Type）] ドロップダウンから、[CIDR ブロック（CIDR Block）] を選択します。

**ステップ 5** [宛先 CIDR ブロック（Destination CIDR Block）] を入力します（例：0.0.0.0/0）。

**ステップ 6** [ターゲット選択（Target Selection）] フィールドに VNIC のプライベート IP アドレスを入力します。

VNIC に IP アドレスを明示的に割り当てていない場合は、VNIC の詳細（**[コンピューティング（Compute）]** > **[インスタンス（Instances）]** > **[インスタンスの詳細（Instance Details）]** > **[接続された VNIC（Attached VNICs）]**）で自動割り当てされた IP アドレスを確認できます。

**ステップ 7** **[ルートルールの追加（Add Route Rules）]** をクリックします。

インターネットゲートウェイを介して IPv6 インターネットアクセスを構成する場合は、次の手順を実行します。

a) **[ターゲットタイプ（Target Type）]** ドロップダウンから、**[インターネットゲートウェイ（Internet Gateway）]** を選択します。

b) [宛先CIDRのブロック（Destination CIDR Block）] で、IP アドレスを指定します。

c) [ターゲットインターネットゲートウェイ（Target Internet Gateway）] ドロップダウンから、既存のインターネット ゲートウェイ コンパートメントを選択するか、新規に作成します。

**ステップ 8** 展開で必要となる各 VNIC について、この手順を繰り返します。

（注） DHCP または IPv6 アドレスプレフィックスによるルーティングルールで構成された IPv6 アドレスが /128 の場合、Threat Defense Virtual ルートテーブルに次のルートを追加する必要があります。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

例：

- `ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b`
- `ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c`

# Auto Scale ソリューションの展開

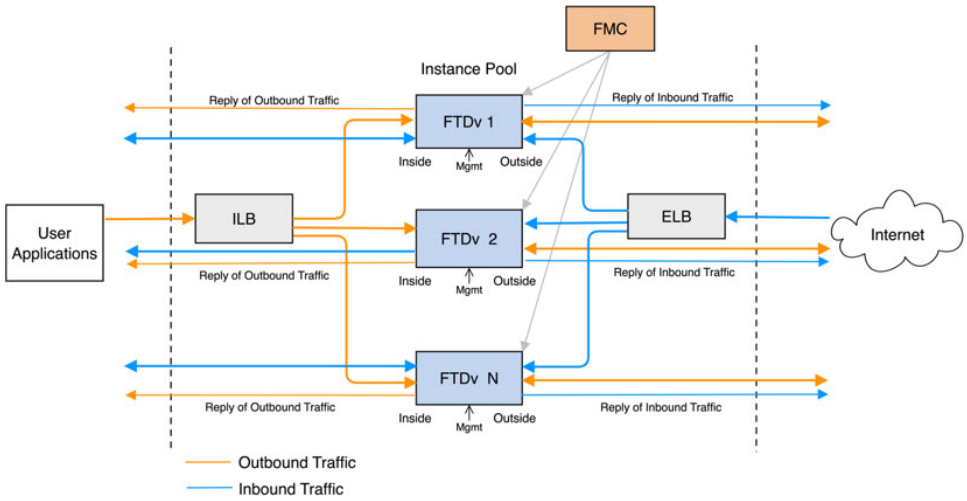
次の項では、Auto Scale ソリューションのコンポーネントが OCI の Threat Defense Virtual でどのように機能するかについて説明します。

## Auto Scale の導入例

OCI での Threat Defense Virtual Auto Scale ソリューションの導入例を次の図に示します。インターネット向けのロードバランサには、リスナーとターゲットグループの組み合わせを使用してポートが有効になっているパブリック IP アドレスがあります。

トラフィックに対してポートベースの分岐が可能であり、NAT ルールを介して実現できます。これについては次の項で説明します。

図 *40 : Secure Firewall Threat Defense Virtual Auto Scale* の導入例の図




# スコープ

このドキュメントでは、Threat Defense Virtual Auto Scale for OCI ソリューションを導入する際の詳細な手順について説明します。

**重要**

- 導入を開始する前に、ドキュメント全体をお読みください。
- 導入を開始する前に、前提条件を満たしていることを確認します。
- ここに記載されている手順と実行順序に従っていることを確認します。

# 前提条件

### 権限およびポリシー

ソリューションを導入するために必要な OCI の権限とポリシーは次のとおりです。

1. **ユーザーおよびグループ**

（注） ユーザーとグループを作成するには、OCI ユーザーまたはテナンシー管理者である必要があります。

Oracle Cloud Infrastructure のユーザーアカウントと、そのユーザーアカウントが属するグループを作成します。ユーザーアカウントを持つ関連グループが存在する場合は、作成す

る必要はありません。ユーザーとグループの作成手順については、「グループとユーザーの作成」を参照してください。

2. **グループ ポリシー**

ポリシーを作成したら、それをグループにマッピングする必要があります。ポリシーを作成するには、**[OCI]** > **[アイデンティティとセキュリティ（Identity & Security）]** > **[ポリシー（Policies）]** > **[ポリシーの作成（Create Policy）]**に移動します。次のポリシーを作成して、目的のグループに追加します。

- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> でメトリックを使用することを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> でアラームを管理することを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> で ONS トピックを管理することを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> でメトリックを検査することを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> でメトリックを読み取ることを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*> でタグの名前空間を使用することを許可します。
- グループ <*Group_Name*> がコンパートメント <*Compartment_Name*>でロググループを読み取ることを許可します。
- グループ <*Group_Name*> がインスタンスプール コンパートメント <*Compartment_Name*> を使用することを許可します。
- グループ <*Group_Name*> がテナントでクラウドシェルを使用することを許可します。
- グループ <*Group_Name*> がテナントのオブジェクトストレージ名前空間を読み取ることを許可します
- グループ <*Group_Name*> がテナント内のリポジトリを管理することを許可します。

（注） テナントレベルでポリシーを作成することもできます。ユーザーの責任と判断のもとで、すべての権限を自由に指定できます。

3. **Oracle 関数の権限**

Oracle 関数が別の Oracle Cloud Infrastructure リソースにアクセスできるようにするには、関数をダイナミックグループに含めてから、そのリソースへのダイナミック グループ アクセスを許可するポリシーを作成します。

4. **ダイナミックグループの作成**

   ダイナミックグループを作成するには、**[OCI]**>**[アイデンティティとセキュリティ（Identity & Security）]** > **ダイナミックグループ（Dynamic Group）]** > **[ダイナミックグループの作成（Create Dynamic Group）]**に移動します。

   ダイナミックグループの作成時に次のルールを指定します。

   ```
   ALL {resource.type = 'fnfunc', resource.compartment.id = '<Your_Compartment_OCID>'}
   ```

   ダイナミックグループの詳細については、次を参照してください。

   - https://docs.oracle.com/en-us/iaas/Content/Functions/Tasks/functionsaccessingociresources.htm
   - https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

5. **ダイナミックグループのポリシーの作成**

   ポリシーを追加するには、**[OCI]**> **[アイデンティティとセキュリティ（Identity & Security）]**>**[ポリシー（Policies）]**>**[ポリシーの作成（Create Policy）]**に移動します。次のポリシーをグループに追加します。

   ```
   Allow dynamic-group <Dynamic_Group_Name> to manage all-resources in compartment
   <Compartment_OCID>
   ```

### GitHub からのファイルのダウンロード

FTDv：OCI Auto Scale ソリューションは、GitHub リポジトリ形式で配布されます。リポジトリからファイルをプルまたはダウンロードできます。

### Python3 環境

*make.py* ファイルは、複製されたリポジトリ内にあります。このプログラムは、Oracle 関数とテンプレートファイルを ZIP ファイルに圧縮します。それらをターゲットフォルダーにコピーします。これらのタスクを実行するには、Python 3 環境が設定されている必要があります。

（注） この Python スクリプトは Linux 環境でのみ使用できます。

### インフラストラクチャ設定

次を設定する必要があります。

1. **VCN**

   FTDv アプリケーションの要件に応じて VCN を作成します。インターネットへのルートが割り当てられたサブネットが 1 つ以上あるインターネットゲートウェイを備えた VPC を作成します。

   VCN の作成については、「https://docs.oracle.com/en-us/iaas/Content/GSG/Tasks/creatingnetwork.htm」を参照してください。

2. **アプリケーションサブネット**

   FTDvアプリケーションの要件に応じてサブネットを作成します。このユースケースに従ってソリューションを導入するには、FTDv インスタンスの運用に 4 つのサブネットが必要です。

   サブネットの作成については、https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm# を参照してください。

3. **外部サブネット**

   サブネットには、インターネットゲートウェイへの「0.0.0.0/0」のルートが必要です。このサブネットには、Cisco FTDv の外部インターフェイスとインターネット向けロードバランサが含まれています。アウトバウンドトラフィック用に NAT ゲートウェイが追加されていることを確認します。

   詳細については、次のマニュアルを参照してください。

   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingIGs.htm
   - https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/NATgateway.htm#To_create_a_NAT_gateway

4. **内部サブネット**

   これは、NAT/インターネットゲートウェイの有無にかかわらず、アプリケーションサブネットに似ています。

（注） FTDv 正常性プローブの場合、ポート 80 を介してメタデータサーバー（169.254.169.254）に到達できます。

5. **管理サブネット**

   管理サブネットは、FTDv への SSH 接続をサポートするようにパブリックにする必要があります。

6. **機能サブネット**

   このサブネットは、Oracle 機能の展開用です。

（注） このサブネットには、NAT GW（インターネット GW ではない）への `0.0.0.0/0` ルートが必要です。

   このサブネットの NAT GW のパブリック IP は、Management Center Virtual および Threat Defense Virtual の NSG（ネットワーク セキュリティ グループ）で許可する必要があります。

7. **セキュリティ グループ：FTDv インスタンスのネットワーク セキュリティ グループ**

Oracle 関数（同じ VCN 内）が FTDv の管理アドレスに SSH 接続できるように、FTDv インスタンスのセキュリティグループを設定します。

8. **オブジェクトストレージの名前空間**

   このオブジェクトストレージの名前空間は、configuration.txt ファイルを持つ静的 Web サイトをホストするために使用されます。configuration.txt ファイルの事前認証済みリクエストを作成する必要があります。この事前認証された URL は、テンプレートの展開時に使用されます。

（注） アップロードされた次の設定に、HTTP URL を介して FTDv インスタンスからアクセスできることを確認します。

FTDv を起動すると、`$ copy /noconfirm <configuration.txt file's pre-authenticated request URL > disk0:Connfiguration.txt` コマンドが実行されます。

このコマンドにより、FTDv の起動を configuration.txt ファイルで設定できるようになります。

# Secure Firewall Management Center の前提条件

Threat Defense Virtual デバイスを管理するには、フル機能のマルチデバイスマネージャである Secure Firewall Management Center を使用します。Threat Defense Virtual は、Threat Defense Virtual 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。

複数のデバイスにポリシーを展開して、更新をインストールするには、Threat Defense Virtual の設定と管理に必要なデバイスグループをはじめとするオブジェクトを作成します。デバイスグループに適用されたすべての設定が Threat Defense Virtual インスタンスにプッシュされます。

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

- Secure Firewall Management Center のパブリック IP アドレス
- ユーザー名とパスワード（メモリベースのスケーリングが有効になっている場合は、2 つのユーザーログイン情報を指定する必要があります）
- セキュリティゾーン名
- Secure Firewall Management Center のアクセスポリシー名
- Secure Firewall Management Center の NAT ポリシー名
- Device Group Name

## Secure Firewall Management Center でのユーザーの作成

Auto Scale Manager だけが使用する管理者権限を持つ Secure Firewall Management Center で新規ユーザーを作成します。

（注） 他の FMC セッションとの競合を防ぐために、Threat Defense Virtual Auto Scale ソリューション専用の Secure Firewall Management Center ユーザーアカウントを持つ必要があります。

管理者権限を持つ Secure Firewall Management Center 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
- ハイフン（-）から始めることはできず、英字は必須。ピリオド（.）、アットマーク（@）、スラッシュ（/）は使用不可

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、『*Firepower Management Center Configuration Guide*』を参照してください。

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

**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。
**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** デバイスグループ名を入力します。
**ステップ 4** [OK] をクリックしてデバイスグループを作成します。

## ネットワークとホストオブジェクトの作成

Threat Defense Virtual の設定に使用する以下のオブジェクトを作成します。

**ステップ 1** 名前 が *oci-metadata-server* で IP が *169.254.169.254* のホストを作成します。
**ステップ 2** 名前が health-check-port で値が 8080 のポートを作成します。必要に応じて他にもポートを作成します。

**ステップ 3** 内部インターフェイスを作成し、**[インターフェイス（Interface）]**>**[セキュリティゾーン（Security Zone）]** を選択します。[ルーテッド（Routed）] をタイプとして選択します。インターフェイス名（*inside-sz* など）を指定します。

**ステップ 4** 外部インターフェイスを作成し、**[インターフェイス（Interface）]**>**[セキュリティゾーン（Security Zone）]** を選択します。[ルーテッド（Routed）] をタイプとして選択します。インターフェイス名（*outside-sz* など）を指定します。

## NAT ポリシーの作成

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 ルールを作成します。次に、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。

**ステップ 1** **[デバイス（Devices）]** > **[NAT]** の順に選択します。

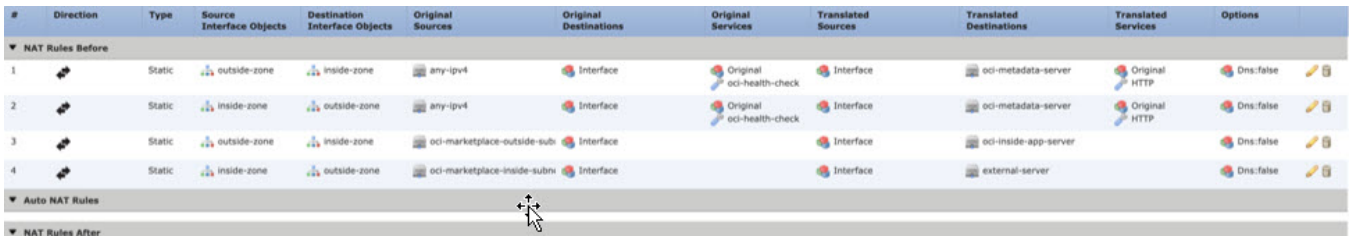
**ステップ 2** [新しいポリシー（New Policy）] ドロップダウン リストで、[Threat Defense NAT] を選択します。

**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、『Secure Firewall Management Center Device Configuration Guide』[英語] の「Configure NAT for Threat Defense」を参照してください。次の図に、ルールを設定する際の基本的なアプローチを示します。

**図 *41 : NAT* ルール**




**ステップ 6** [保存（Save）] をクリックします。

## NAT ルールの作成

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。詳細については、『Secure Firewall Management Center Device Configuration Guide』の「Configure NAT for Threat Defense」を参照してください。 [英語]

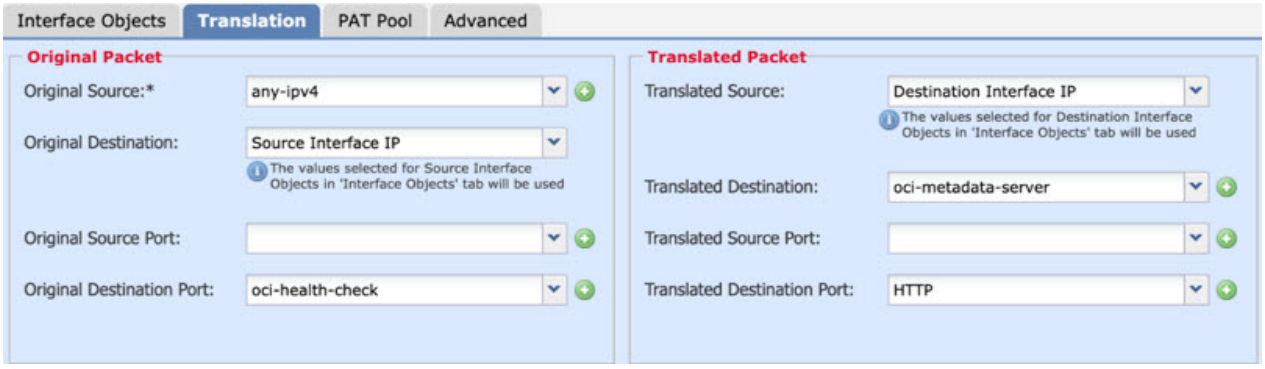
NAT ポリシーに必要な次の 2 つの必須ルールを設定します。

**ステップ 1** インバウンドヘルスチェックでは、次の NAT ルールを設定します。

- 送信元ゾーン（Source Zone）：外部ゾーン
- 宛先ゾーン（Dest Zone）：内部ゾーン
- 元の送信元（Original-sources）：any-ipv4
- 元の宛先（Original Destinations）：送信元インターフェイスの IP
- 元の送信元ポート（Original source port）：デフォルト
- 元の宛先ポート（Original-destination-port）：health-check-port
- 変換済みの送信元（Translated-sources）：宛先インターフェイスの IP
- 変換済み宛先（Translated-destination）：oci-metadata-server
- 変換済み送信元ポート（Translated source port）：デフォルト
- 変換済み宛先ポート（Translated-destination-port）：HTTP

次の図は、インバウンドヘルスチェックの NAT ルールを示しています。

**図 *42*：インバウンドヘルス *NAT* ルール**



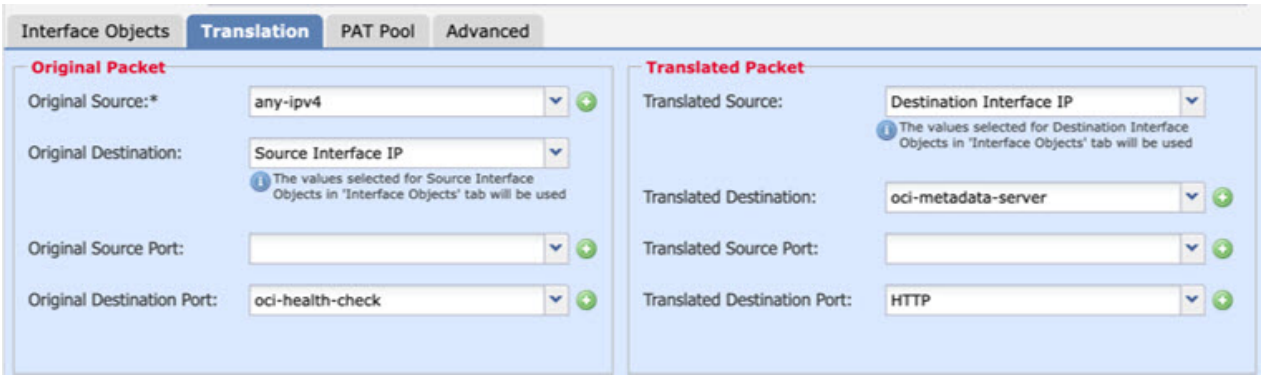

**ステップ 2** アウトバウンド ヘルス チェックでは、次の NAT ルールを設定します。

- 送信元ゾーン（Source Zone）：内部ゾーン
- 宛先ゾーン（Dest Zone）：外部ゾーン
- 元の送信元（Original-sources）：any-ipv4
- 元の宛先（Original Destinations）：送信元インターフェイスの IP
- 元の送信元ポート（Original source port）：デフォルト
- 元の宛先ポート（Original-destination-port）：health-check-port
- 変換済みの送信元（Translated-sources）：宛先インターフェイスの IP
- 変換済み宛先（Translated-destination）：oci-metadata-server
- 変換済み送信元ポート（Translated source port）：デフォルト

- 変換済み宛先ポート（Translated-destination-port）：HTTP

次の図は、アウトバウンド ヘルス チェックの NAT ルールを示しています。

**図 *43*：アウトバウンド ヘルス チェックの *NAT* ルール**




同様に、この設定が Threat Defense Virtual デバイスにプッシュされるように、任意の NAT ルールをデータ トラフィックに追加できます。

## アクセスポリシーの作成

内部から外部へのトラフィックを許可するアクセス制御を設定します。必要なすべてのポリシーを含むアクセスポリシーを作成できます。このポートのトラフィックがデバイスに到達できるように、正常性ポートオブジェクトを許可する必要があります。アクセス 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。効果的な導入を実現するには、ルールの適切な構成と順序付けが不可欠です。『Secure Firewall Management Center Device Configuration Guide』[英語] で「Best Practices for Access Control Rules」の項を参照してください。

[ポリシー割り当て（Policy Assignments）] を使用して、デバイスグループ（前提条件の一部として作成済み）をアクセスポリシーに割り当てます。

**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します。詳細については、『Secure Firewall Management Center Device Configuration Guide』[英語] の「Access Control」を参照してください。

# パスワードの暗号化

（注） この手順の詳細については、「Vault とシークレットの作成」を参照してください。

FTDv のパスワードは、自動スケーリング中に使用されるすべての FTDv インスタンスを設定するために使用されます。また、いくつかの設定目的で Rest API を呼び出すための接続を作成するために使用されます。

したがって、パスワードを時々保存して処理する必要があります。頻繁な変更と脆弱性のため、プレーンテキスト形式での「パスワードの編集や保存はできません。パスワードには、暗号化された形式のみを使用する必要があります。

暗号化された形式のパスワードを取得するには、次の手順を実行します。

**ステップ 1** Vault を作成します。

OCI Vault は、マスター暗号化キーを安全に作成および保存するサービスと、それらを使用する際に暗号化および復号する方法を提供します。したがって、Vault は、自動スケールソリューションの残りの部分と同じコンパートメントに作成する必要があります（まだ作成していない場合）。

**[OCI] > [アイデンティティとセキュリティ（Identity & Security）] > [Vault] > [新規Vaultの選択または作成（Choose or Create New Vault）]**に移動します。

**ステップ 2** マスター暗号化キーを作成します。

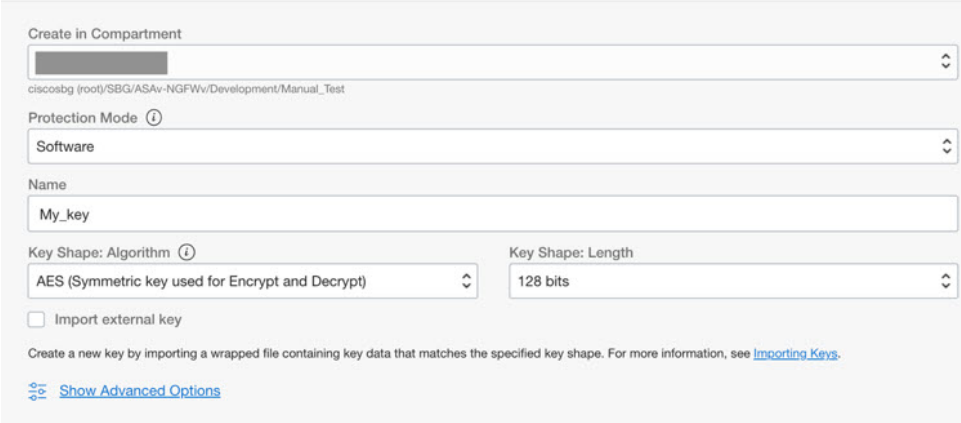
プレーンテキストのパスワードを暗号化するには、マスター暗号化キーが 1 つ必要です。

**[OCI] > [アイデンティティとセキュリティ（Identity & Security）] > [Vault] > [キーの選択または作成（Choose or Create Key）]**に移動します。

任意のビット長で、指定されたアルゴリズムのいずれかから任意のキーを選択します。

1. AES：128、192、256
2. RSA：2048、3072、4096
3. ECDSA：256、384、521

図 *44* : キーの作成




**ステップ 3** 暗号化されたパスワードを作成します。

1. **[OCI] > [ CloudShell（OCI Cloud Terminal）を開く（Open CloudShell (OCI Cloud Terminal）]**に移動します。
2. <*Password*> をお使いのパスワードに置き換えて、次のコマンドを実行します。

   ```
   echo -n '<Password>' | base64
   ```

3. 選択した Vault から、暗号化エンドポイントとマスター暗号化キーの OCID をコピーします。次のように値を置き換えてから、暗号化コマンドを実行します。
   - KEY_OCID：キーの OCID
   - Cryptographic_Endpoint_URL：Vault の暗号化エンドポイント URL
   - Password：パスワード

   **暗号化コマンド**

   ```
   oci kms crypto encrypt --key-id Key_OCID --endpoint
   Cryptographic_Endpoint_URL --plaintext <base64-value-of-password>
   ```

4. 上記のコマンドの出力から暗号文をコピーし、必要に応じて使用します。

# Threat Defense Virtual の構成ファイルの準備

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

**ステップ 1** 展開する前に、次の入力パラメータを収集します。

| パラメータ | データタイプ | 説明 |
|---|---|---|
| tenancy_ocid | 文字列 | アカウントが属するテナントの OCID。テナントの OCID を見つける方法については、こちらを参照してください。<br>テナントの OCID は `ocid1.tenancy.oc1..<unique_ID>` のようになります。 |
| region | 文字列 | リソースを作成するリージョンの一意の識別子。<br>例：us-phoenix-1、us-ashburn-1 |
| lb_size | 文字列 | 事前にプロビジョニングする外部および内部ロードバランサの合計帯域幅（入力および出力）を決定するテンプレート。<br>サポートされる値：100 Mbps、10 Mbps、10 Mbps-Micro、400 Mbps、8000 Mbps<br>例：100 Mbps |
| availability_domain | 文字列 | 例：Tpeb:PHX-AD-1、Tpeb:PHX-AD-2<br>（注） 可用性システムのドメイン名を取得するには、こちらを参照してください。 |
| min_and_max_instance_count | カンマ区切り値 | インスタンスプールに保持するインスタンスの最小数と最大数。<br>例：1,5 |
| autoscale_group_prefix | 文字列 | テンプレートを使用して作成したリソースの名前に付けるプレフィックス。たとえば、リソースプレフィックスとして「autoscale」を指定すると、すべてのリソースはautoscale_resource1、autoscale_resource2 のように名前が付けられます。 |
| mgmt_subnet_ocid | 文字列 | 使用する管理サブネットの OCID。 |
| inside_subnet_ocid | 文字列 | 使用する内部サブネットの OCID。 |
| function_subnet_ocid | 文字列 | 使用する機能サブネットの OCID。 |
| outside_subnet_ocid | 文字列 | 使用する外部サブネットの OCID。 |
| mgmt_nsg_ocid | 文字列 | 使用する管理サブネットのネットワーク セキュリティ グループの OCID。 |

| パラメータ | データタイプ | 説明 |
|---|---|---|
| inside_nsg_ocid | 文字列 | 使用する内部サブネットのネットワークセキュリティ グループの OCID。 |
| outside_nsg_ocid | 文字列 | 使用する外部サブネットのネットワークセキュリティ グループの OCID。 |
| elb_listener_port | カンマ区切り値 | 外部ロードバランサリスナーの通信ポートのリスト。<br>例： 80 |
| ilb_listener_port | カンマ区切り値 | 内部ロードバランサリスナーの通信ポートのリスト。<br>例： 80 |
| health_check_port | 文字列 | ヘルスチェックを実行するロードバランサーのバックエンドサーバーポート。<br>例：8080 |
| instance_shape | 文字列 | 作成するインスタンスのシェープ。シェイプにより、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソースが決定されます。<br>サポートされているシェープ：「VM.Standard2.4」および「VM.Standard2.8」 |
| lb_bs_policy | 文字列 | 内部および外部ロードバランサのバックエンドセットに使用するロードバランサポリシー。ロードバランサポリシーの仕組みについて詳しくは、こちらを参照してください。<br>サポートされている値：「ROUND_ROBIN」、「LEAST_CONNECTIONS」、「IP_HASH」 |
| image_name | 文字列 | インスタンスの構成に使用するマーケットプレイスのイメージ名。<br>デフォルト値：「Cisco Firepower NGFW 仮想ファイアウォール（NGFWv）（Cisco Firepower NGFW virtual firewall (NGFWv)）」<br>（注） カスタムイメージを展開する場合は、custom_image_ocid パラメータを設定する必要があります。 |

| パラメータ | データタイプ | 説明 |
|---|---|---|
| scaling_thresholds | カンマ区切り値 | スケールインとスケールアウトで使用する CPU 使用率のしきい値。スケールインとスケールアウトのしきい値をカンマで区切って入力します。<br>例：15,50<br>15 はスケールインのしきい値、50 はスケールアウトのしきい値です。 |
| compartment_id | 文字列 | リソースを作成するコンパートメントの OCID。<br>例：**ocid1.compartment.oc1..<unique_ID>** |
| compartment_name | 文字列 | コンパートメント名 |
| custom_image_ocid | 文字列 | マーケットプレイスイメージを使用しない場合に、インスタンス構成に使用するカスタムイメージの OCID。<br>（注） *custom_image_ocid* はオプションパラメータです |
| ftdv_password | 文字列 | Threat Defense Virtual を構成するために SSH 接続する際の、Threat Defense Virtual の暗号化形式のパスワード。パスワードを暗号化する方法については、コンフィギュレーションガイドを使用するか、こちらを参照してください。 |
| ftdv_license_type | 文字列 | Threat Defense Virtual ライセンスタイプ（BYOL または PAYG）。現在、BYOL がサポートされています。 |
| cryptographic_endpoint | 文字列 | 暗号化エンドポイントは、パスワードの復号に使用される URL です。Vault で検索できます。 |
| master_encryption_key_id | 文字列 | パスワードの暗号化に使用されたキーの OCID。Vault で検索できます。<br>（注） master_encryption_key_id と cryptographic_endpoint の両方が同じ Vault に属している必要があります。 |

| パラメータ | データタイプ | 説明 |
|---|---|---|
| fmc_ip | 文字列 | Secure Firewall Management Center の IP アドレス。カスタマーが Threat Defense Virtual インスタンスを管理するために使用する Management Center の IP。<br>（注） *Management Center の IP は、Threat Defense Virtual と同じサブネットにある場合にのみプライベート IP を使用できます。それ以外の場合は、パブリック IP を使用する必要があります。* |
| fmc_username | 文字列 | Management Center アカウントのユーザー名このユーザー名は、Management Center にログインして、新しい Threat Defense Virtual インスタンスの起動のたびに設定で使用されます。 |
| fmc_password | 文字列 | 暗号化された形式の Management Center のパスワード。パスワードを暗号化する手順については、こちらを参照してください。 |
| fmc_device_group_name | 文字列 | Management Center にデバイスグループがあり、この Auto Scale ソリューションのすべての Threat Defense Virtual 部分がそのグループに追加されている必要があります。これにより、同じポリシーと構成をそれらのすべてに適用できます。 |
| enable_memory_based_scaling | Bool | Secure Firewall Management Center Virtual から Threat Defense Virtual メモリ使用量を公開します。このフラグを有効にすることで、メモリ使用率にも基づいてスケーリングを実行できます。デフォルトでは、CPU 使用率が使用されます。 |
| fmc_metrics_username | 文字列 | enable_memory_based_scaling フラグを有効にしてメモリ使用率を選択した場合、実行中のすべての Threat Defense Virtual インスタンスからメモリ使用量をプルするために継続的に使用されるため、追加の Management Center ユーザー アカウントが必要です。 |
| fmc_metrics_password | 文字列 | 暗号化形式の追加の Management Center アカウントのパスワード。パスワードを暗号化する手順については、こちらを参照してください。 |

| パラメータ | データタイプ | 説明 |
|---|---|---|
| Profile Name | | OCI のユーザーのプロファイル名です。ユーザーのプロファイルセクションの下にあります。例：「oracleidentitycloudservice/ <user>@<mail>.com」 |
| Object Storage Namespace | | テナントの作成時に作成される一意の識別子です。**[OCI]**>**[管理（Administration）]**>**[テナントの詳細（Tenancy Details）]**に移動します。 |
| Authorization Token | | これは、OCI コンテナレジストリに Oracle 関数をプッシュすることを許可する Docker ログイン用のパスワードとして使用されます。**[OCI]**>**[アイデンティティ（Identity）]**>**[ユーザー（Users）]**>**[ユーザの詳細（User Details）]** > **[認証トークン（Auth Tokens）]** > **[トークンの生成（Generate Token）]**に移動します。 |

**ステップ 2** 次の内容の *Configuration.json* ファイルを作成します。

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv30",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "<autoscale-access-policy-name>",
  "fmcNatPolicyName": "<autoscale-nat-policy-name>",
  "fmcInsideNicName": "inside",
  "fmcOutsideNicName": "outside",
  "fmcInsideNic": "GigabitEthernet0/0",
  "fmcOutsideNic": "GigabitEthernet0/1",
  "fmcOutsideZone": "<outside-zone-name>",
  "fmcInsideZone": "<inside-zone-name>",
  "MetadataServerObjectName": "oci-metadata-server",
  "interfaceConfig": [
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "inside-zone"
      },
      "mode": "NONE",
      "ifname": "inside",
      "name": "GigabitEthernet0/0"
    },
    {
      "managementOnly": "false",
      "MTU": "1500",
      "securityZone": {
        "name": "outside-zone"
      },
      "mode": "NONE",
      "ifname": "outside",
      "name": "GigabitEthernet0/1"
    }
  ],
  "trafficRoutes": [
```

```
    {
      "interface": "outside",
      "network": "any-ipv4",
      "gateway": "",
      "metric": "2"
    },
    {
      "interface": "inside",
      "network": "oci-metadata-server",
      "gateway": "",
      "metric": "1"
    }
  ]
}
```

**ステップ 3** *Configuration.json* を構成設定で更新します。

**ステップ 4** 構成ファイルをオブジェクト ストレージ スペースにアップロードします。

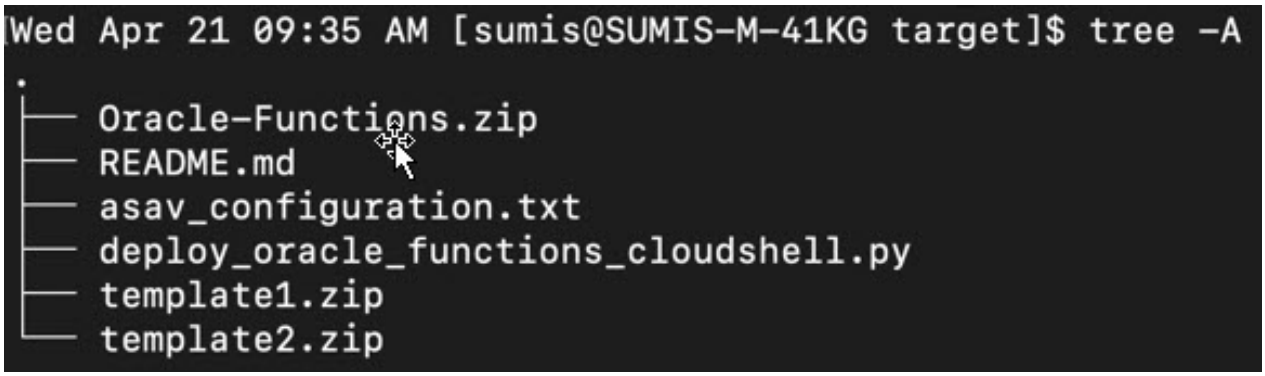
*configuration.txt* ファイルは、ユーザーが作成したオブジェクト ストレージ スペースにアップロードする必要があり、アップロードしたファイルに対する事前認証リクエストを作成する必要があります。

（注） スタックの展開で、configuration.txt の事前認証済みリクエスト URL が使用されていることを確認します。

（注） OCI で事前認証済み URL を作成するときに有効期限を定義する必要があります。ソリューションの実行中に期限切れにならないように、この期間を十分に長くしてください。

**ステップ 5** Zip ファイルを作成します。

*make.py* ファイルは、複製されたリポジトリ内にあります。`python3 make.py build` コマンドを実行して、zip ファイルを作成します。対象フォルダには以下のファイルがあります。




# Auto Scale ソリューションの展開

展開の前提条件となる手順を完了したら、OCI スタックの作成を開始します。手動展開を実行するか、クラウドシェルを使用した導入（）を実行できます。該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

# 手動展開

エンドツーエンドの Auto Scale ソリューションの展開は、次の 3 つの手順で構成されます。Terraform Template-1 スタックの展開 、Oracle 関数の展開、次いで Terraform Template-2 の展開

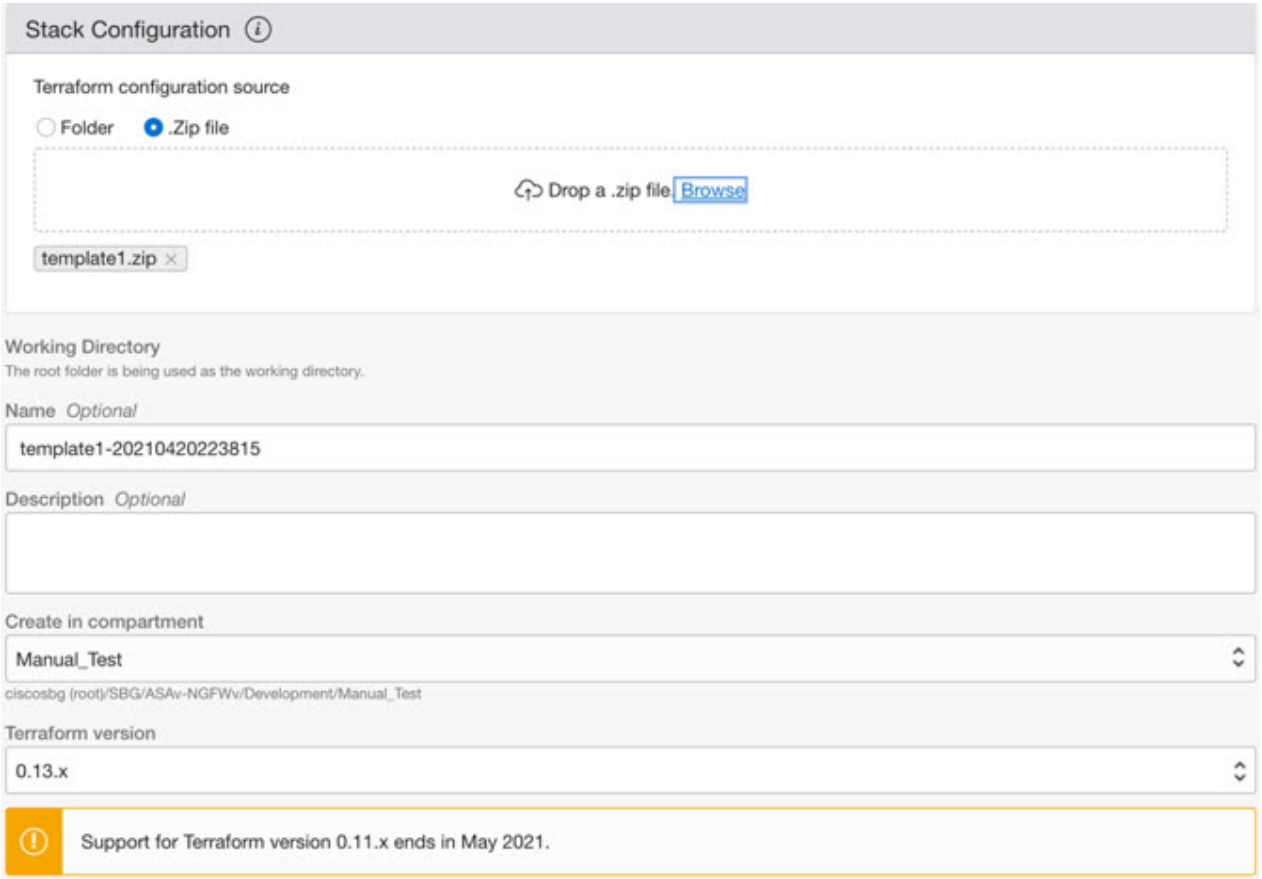
## Terraform Template-1 スタックの展開

**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[デベロッパーサービス（Developer Service）] > [リソースマネージャ（Resource Manager）] > [スタック（Stack）] > [スタックの作成（Create Stack）]**の順に選択します。

[マイ設定（My Configuration）] を選択し、次の図に示すように、対象フォルダ内にある *Terraform template1.zip* ファイルを Terraform の設定ソースとして選択します。




**ステップ 3** [トランスフォームバージョン（Transform version）] ドロップダウンリストで、0.13.x または 0.14.x を選択します。

**ステップ 4** 次の手順では、ステップ 1で収集した詳細情報をすべて入力します。

（注） 有効な入力パラメータを入力しnoてください。そうしないと、以降の手順でスタックの展開に失敗する可能性があります。

**ステップ 5** 次の手順で**[Terraformアクション（Terraform Actions）] > [適用（Apply）]**を選択します。

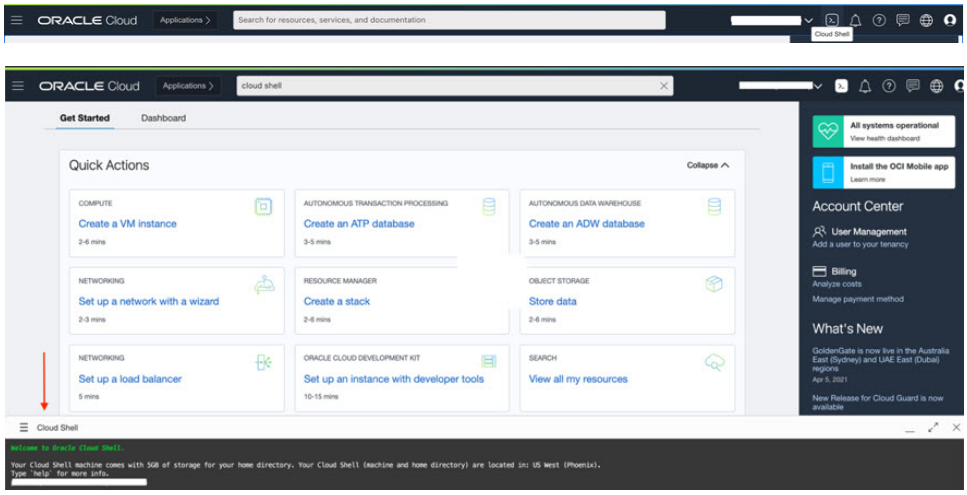
正常に展開されたら、Oracle 関数の展開に進みます。

## Oracle 関数の展開

（注） この手順は、*Terraform Template-1* の導入が成功した後にのみ実行する必要があります。

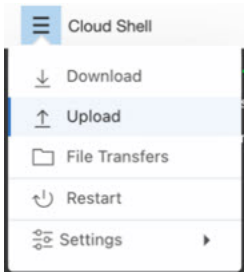
OCI では、Oracle 関数は Docker イメージとしてアップロードされ、OCI コンテナレジストリに保存されます。Oracle 関数は、導入時に OCI アプリケーション（Terraform Template-1 で作成）の 1 つにプッシュする必要があります。

**ステップ 1** OCI のクラウドシェルを開きます。

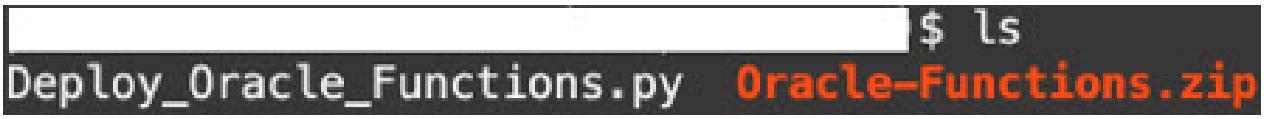



**ステップ 2** *deploy_oracle_functions_cloudshell.py* と *Oracle-Functions.zip* をアップロードします。

クラウドシェルのハンバーガーメニューから [アップロード（Upload）] を選択します。



**ステップ 3** **ls** コマンドを使用してファイルを確認します。



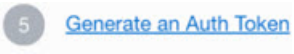

**ステップ 4** `python3 Deploy_Oracle_Functions.py -h` を実行します。以下の図に示すように、`deploy_oracle_functions_cloudshell.py` スクリプトには、いくつかの入力パラメータが必要です。詳細は help 引数を使用して確認できます。

```
$ python3 Deploy_Oracle_Functions.py -h
usage: Deploy_Oracle_Functions.py [-h] -a  -r  -p  -c  -o  -t

*** Script to deploy Oracle Function for OCI ASAv Autoscale Solution ***

Instruction to find values of required arguments:
Application Name: Name of Application created by first Terraform Template
Region Identifier: OCI -> Administration -> Region Management
Profile Name: OCI -> Profile
Compartment OCID: OCI -> Identity -> Compartment -> Compartment Details
Object Storage Namespace: OCI -> Administration -> Tenancy Details
Authorization Token: OCI -> Identity -> Users -> User Details -> Auth Tokens -> Generate Token

optional arguments:
  -h, --help  show this help message and exit
  -a          Name of Application in OCI to which functions will be deployed
  -r          Region Identifier
  -p          Profile Name of User
  -c          Compartment OCID
  -o          Object Storage Namespace
  -t          Authorization Token for Docker Login (*Please Put in Quotes)
```

スクリプトを実行するには、次の引数を渡します。

**表 *25 :* 引数と詳細**

| 引数 | 特記事項 |
|---|---|
| アプリケーション | Terraform Template-1 の導入で作成した OCI アプリケーションの名前です。この値は、Template-1 で付与された「**autoscale_group_prefix**」とサフィックス「**_application**」を組み合わせたものです。 |
| リージョン識別子（**Region Identifier**） | リージョン識別子は、さまざまな地域の OCI で固定された地域コードワードです。<br>例：フェニックスの場合は「us-phoenix-1」、メルボルンの場合は「ap-melbourne-1」。<br>すべてのリージョンとそのリージョン識別子のリストを取得するには、**[OCI]** > **[管理（Administration）]** > **[リージョン管理（Region Management）]**に移動します。 |

| 引数 | 特記事項 |
|---|---|
| プロファイル名 | OCI のシンプルなユーザープロファイル名です。<br>例：*oracleidentitycloudservice/<user> @<mail> .com*<br>名前は、ユーザーのプロファイルセクションの下にあります。 |
| コンパートメント OCID（Compartment OCID） | これは、コンパートメントの OCID（Oracle Cloud 識別子）です。ユーザーが OCI アプリケーションを格納しているコンパートメントの OCID。<br>**[OCI] > [アイデンティティ（Identity）] > [コンパートメント（Compartment）] > [コンパートメントの詳細（Compartment Details）]**に移動します。 |
| オブジェクトストレージの名前空間 | テナントの作成時に作成される一意の識別子です。<br>**[OCI] > [管理（Administration）] > [テナントの詳細（Tenancy Details）]**に移動します。 |
| 認証トークン（Authorization Token） | これは、OCI コンテナレジストリに Oracle 関数をプッシュすることを許可する Docker ログイン用のパスワードとして使用されます。導入スクリプトでトークンを引用符で囲んで指定します。<br>**[OCI] > [アイデンティティ（Identity）] > [ユーザー（Users）] > [ユーザの詳細（User Details）] > [認証トークン（Auth Tokens）] > [トークンの生成（Generate Token）]**に移動します。<br>何らかの理由でユーザーの詳細が表示されない場合は、**[開発者サービス（Developer services）] > [機能（Functions）]**をクリックします。Terraform Template-1 で作成したアプリケーションに移動します。[利用を開始する（Getting Started）] をクリックし、[クラウドシェルの設定（Cloud Shell Setup）] を選択すると、手順を進めていく中で、以下に示すように認証トークンを生成するためのリンクが表示されます。<br>  |

**ステップ 5** 有効な入力引数を渡して、`python3 Deploy_Oracle_Functions.py` コマンドを実行します。すべての機能を展開するには時間がかかります。その後、ファイルを削除してクラウドシェルを閉じることができます。

## Terraform Template-2 の展開

Template-2 は、アラーム、関数を呼び出すための ONS トピックなど、アラーム作成に関連するリソースを展開します。Template-2 の展開は、Terraform Template-1 の展開に似ています。

**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[デベロッパーサービス（Developer Service）] > [リソースマネージャ（Resource Manager）] > [スタック（Stack）] > [スタックの作成（Create Stack）]**の順に選択します。

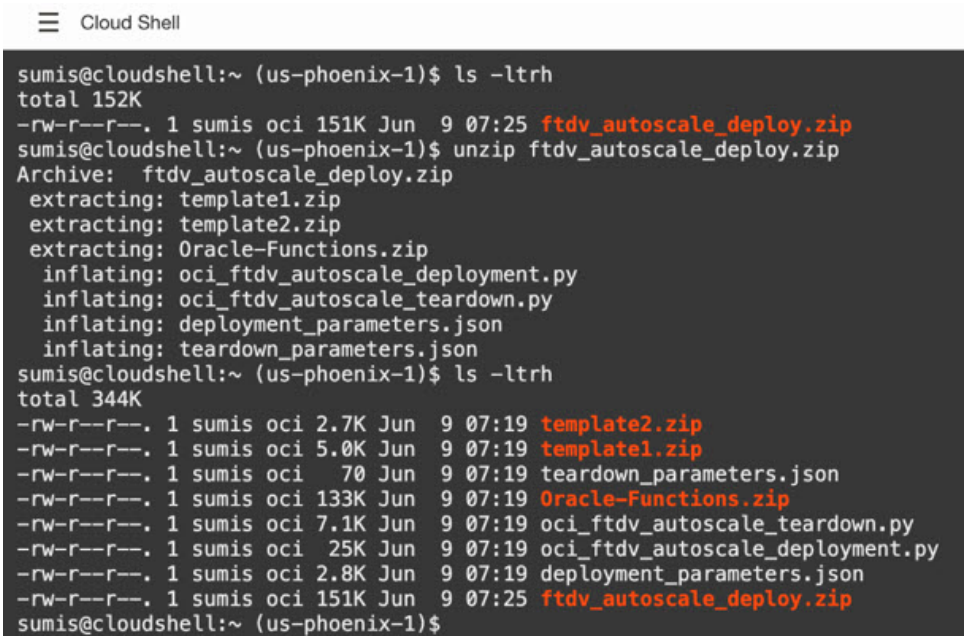
Terraform 設定のソースとして、ターゲットフォルダにある *Terraform template template2.zip* を選択します。

**ステップ 3** 次のステップで、**Terraformアクション（Terraform Actions）] > [適用（Apply）]**をクリックします。

# クラウドシェルを使用した導入

導入のオーバーヘッドを回避するために、簡単なエンドツーエンドの導入スクリプトを呼び出して、自動スケールソリューション（terraform template1、template2、および Oracle 関数）を導入できます。

**ステップ 1** 対象フォルダ内にある *ftdv_autoscale_deploy.zip* ファイルをクラウドシェルにアップロードして、ファイルを抽出します。




**ステップ 2** `python3 make.py build` コマンドを実行する前に、*deployment_parameters.json* の入力パラメータが更新されていることを確認してください。

**ステップ 3** 自動スケールソリューションの導入を開始するには、クラウドシェルで `python3 oci_ftdv_autoscale_deployment.py` コマンドを実行します。

ソリューションの展開が完了するまでに約 10 ～ 15 分かかります。

ソリューションの展開中にエラーが発生した場合、エラーログが保存されます。

# 展開の検証

すべてのリソースが展開され、Oracle関数がアラームとイベントに接続されているかどうかを検証します。デフォルトでは、インスタンスプールのインスタンスの最小数と最大数はゼロです。OCI UI でインスタンスプールを編集して、必要な最小数と最大数に設定できます。これにより、新しい Threat Defense Virtual インスタンスがトリガーされます。

1 つのインスタンスのみを起動してワークフローを確認し、そのインスタンスが期待どおりに動作しているかどうかを検証することを推奨します。この検証をポストすると、Threat Defense Virtual の実際の要件を展開できます。

（注） OCI スケーリングポリシーによる削除を回避するために、最小数の Threat Defense Virtual インスタンスを**スケールイン保護**として指定します。

# アップグレード

### Auto Scale スタックのアップグレード

このリリースではアップグレードはサポートされていません。スタックを再導入する必要があります。

### Threat Defense Virtual VM のアップグレード

このリリースでは、Threat Defense Virtual VM のアップグレードはサポートされていません。必要な Threat Defense Virtual イメージを使用してスタックを再導入する必要があります。

### インスタンスプール

1. インスタンスプール内のインスタンスの最小数と最大数を変更するには、次の手順を実行します。

   **[デベロッパーサービス（Developer Services）] > [機能（Function）] > [アプリケーション名（Terraform template-1で作成済み）（Application Name(created by Terraform Template 1)）] > [設定（Configuration）]** をクリックします。

   min_instance_count と max_instance_count をそれぞれ変更します。

2. インスタンスの削除/終了は、スケールインと同等ではありません。インスタンスプール内のいずれかのインスタンスがスケールインアクションではなく外部アクションのために削除/終了された場合、インスタンスプールは自動的に新しいインスタンスを開始して回復します。

3. Max_instance _count では、スケールアウトアクションのしきい値制限を定義しますが、UI を介してインスタンスプールのインスタンス数を変更することでしきい値を上回ることができます。UI のインスタンス数が、OCI アプリケーションで設定された max_instance_count 未満であることを確認します。それ以外の場合は、適切なしきい値に増やします。

4. アプリケーションから直接インスタンスプール内のインスタンスの数を減らしても、プログラムで設定されたクリーンアップアクションは実行されません。両方のロードバランサからバックエンドがドレインおよび削除されないため、Threat Defense Virtual に供与されているライセンスは失われます。

5. 何らかの理由で、Threat Defense Virtual インスタンスに異常があり応答せず、一定期間 SSH 経由で到達できない場合、インスタンスがインスタンスプールから強制的に削除され、ライセンスが失われる可能性があります。

**Oracle 関数**

- Oracle 関数は、実際には Docker イメージです。Docker イメージは、OCI コンテナレジストリのルートディレクトリに保存されます。Docker イメージは削除しないでください。Auto Scale ソリューションで使用される関数も削除されます。
- Terraform Template-1 によって作成された OCI アプリケーションには、Oracle 関数が正しく動作するために必要な重要な環境変数が含まれています。必須でない限り、これらの環境変数の値もフォーマットも変更しないでください。加えられた変更は、新しいインスタンスにのみ反映されます。

# ロードバランサのバックエンドセット

OCI でインスタンスプールにロードバランサを関連付ける場合、Threat Defense Virtual で管理インターフェースとして設定されたプライマリインターフェースを使用した方法のみサポートされています。したがって、内部インターフェイスは内部ロードバランサのバックエンドセットに紐づけられます。外部インターフェイスは、外部ロードバランサのバックエンドセットに紐づけられます。これらの IP はバックエンドセットに自動的に追加されたり、削除されたりしません。Auto Scale ソリューションでは、これら両方のタスクをプログラムで処理します。ただし、外部アクション、メンテナンス、トラブルシューティングの場合は、手動で実行する必要性が生じることがあります。

要件に応じて、リスナーとバックエンドセットを使用して、ロードバランサーで追加のポートを開くことができます。今後のインスタンス IP はバックエンドセットに自動的に追加されますが、既存のインスタンス IP は手動で追加する必要があります。

### ロードバランサでのリスナーの追加

ロードバランサでポートをリスナーとして追加するには、**[OCI]** > **[ネットワーキング（Networking）]** > **[ロードバランサ（Load Balancer）]** > **[リスナー（Listener）]** > **[リスナーの作成（Create Listener）]**に移動します。

**バックエンドをバックエンドセットに登録**

Threat Defense Virtual インスタンスをロードバランサに登録するには、Threat Defense Virtual インスタンスの外部インターフェイス IP を外部ロードバランサのバックエンドセットでバックエンドとして設定する必要があります。内部インターフェイス IP は、内部ロードバランサーのバックエンドセットでバックエンドとして設定する必要があります。使用しているポートがリスナーに追加されていることを確認してください。

# OCI のAuto Scale 設定の削除

Terraform を使用して導入されたスタックは、OCI の Resource Manager を使用して、同じ方法で削除できます。スタックを削除すると、そのスタックによって作成されたすべてのリソースが削除され、これらのリソースに関連付けられているすべての情報が完全に削除されます。

（注） スタックを削除する場合は、インスタンスプールのインスタンスの最小数を 0 にして、インスタンスが終了するまで待つことを推奨します。そうすることで、すべてのインスタンスの削除が容易になり、インスタンスが残りません。

手動による削除するか、クラウドシェルを使用した Auto Scale の削除 を使用できます。

## 手動による削除

エンドツーエンドの Auto Scale ソリューションの削除は、次の 3 つの手順で構成されます。Terraform Template-2 スタックの削除、Oracle 関数の削除、次いで Terraform Template-1 スタックの削除

### Terraform Template-2 スタックの削除

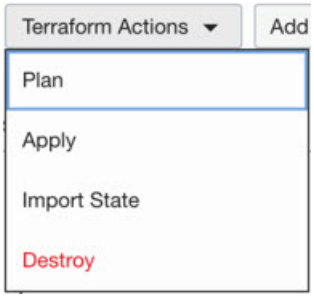
自動スケール設定を削除するには、最初に Terraform Template-2 スタックを削除する必要があります。

**ステップ 1** OCI ポータルにログインします。

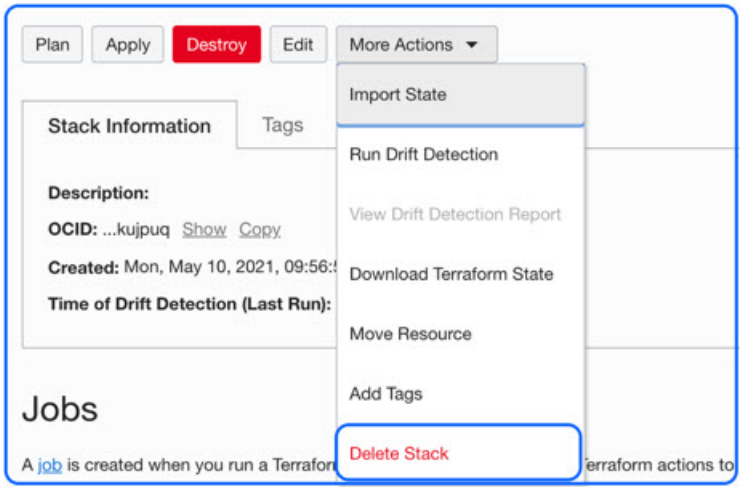
地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[デベロッパーサービス（Developer Service）]** > **[リソースマネージャ（Resource Manager）]** > **[スタック（Stack）]**の順に選択します。

**ステップ 3** Terraform Template-2 によって作成されたスタックを選択し、次の図に示すように [Terraformアクション（Terraform Actions）] ドロップダウンメニューで [破棄（Destroy）] を選択します。




破棄ジョブが作成されます。リソースが順次削除されるまで時間がかかります。破棄ジョブが完了したら、下の図に示すようにスタックを削除できます。




**ステップ 4** Oracle 関数の削除に進みます。

## Oracle 関数の削除

Oracle 関数の展開は Terraform Template スタック展開の一部としてではなく、クラウドシェルを使用して個別にアップロードします。したがって、削除も Terraform スタックの削除ではサポートされていません。Terraform Template-1 によって作成された OCI アプリケーション内のすべての Oracle 関数を削除する必要があります。

**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[開発者サービス（Developer Services）]** > **[機能（Functions）]**の順に選択します。Template-1 スタックで作成されたアプリケーション名を選択します。

**ステップ 3** このアプリケーション内で各機能にアクセスして削除します。

## Terraform Template-1 スタックの削除

（注） Template-1 スタックの削除は、すべての Oracle 関数を削除した後にのみ成功します。

Terraform Template-2 の削除と同じです。

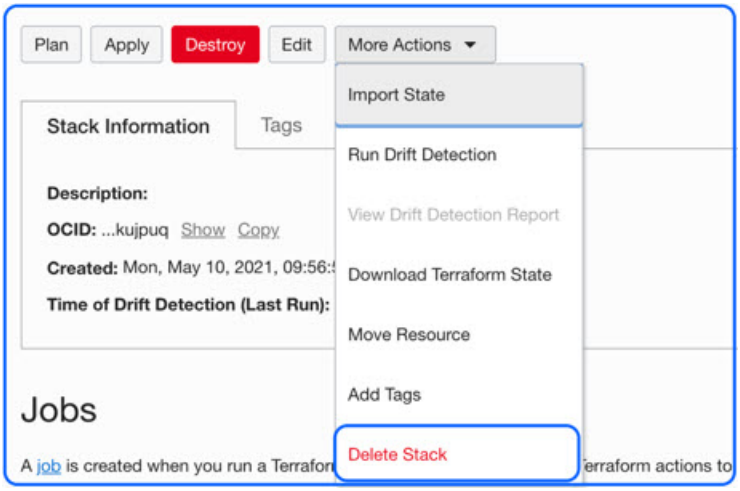
**ステップ 1** OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

**ステップ 2** **[デベロッパーサービス（Developer Service）] > [リソースマネージャ（Resource Manager）] > [スタック（Stack）]**の順に選択します。

**ステップ 3** Terraform Template-2 によって作成されたスタックを選択し、[Terraformアクション（Terraform Actions）] ドロップダウンメニューで [破棄（Destroy）] を選択します。破棄ジョブが作成されます。リソースが順次削除されるまで時間がかかります。

**ステップ 4** 破棄ジョブが完了したら、下の図に示すように、[その他の操作（More Actions）] ドロップダウンメニューからスタックを削除できます。




Terraform Template-1 スタックの削除が成功したら、すべてのリソースが削除され、残存しているリソースがないことを確認する必要があります。

# クラウドシェルを使用した Auto Scale の削除

スクリプトを使用してスタックやオラクル関数を削除するには、 コマンドシェルで `python3 oci_ftdv_autoscale_teardown.py` コマンドを実行します。スタックが手動で展開されている場合は、stack1 と stack2 のスタック ID を更新し、*teardown_parameters.json* ファイルのアプリケーション ID を更新します。

# SSH を使用した Threat Defense Virtual インスタンスへの接続

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

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

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

ここで、

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

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

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

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

<username> は、Threat Defense Virtual インスタンスのユーザー名です。

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

# OpenSSH を使用した Threat Defense Virtual インスタンスへの接続

Windows システムから Threat Defense Virtual インスタンスに接続するには、OpenSSH を使用してインスタンスにログインします。

**ステップ 1** このキーペアを初めて使用する場合は、自分だけがファイルを読み取れるようにファイルの権限を設定する必要があります。

次の手順を実行します。

a) Windows Explorer で、秘密キーファイルに移動し、ファイルを右クリックして **[プロパティ（Properties）]** をクリックします。
b) **[セキュリティ（Security）]** タブで、**[詳細設定（Advanced）]** をクリックします。
c) **[オーナー（Owner）]** が自分のユーザーアカウントであることを確認します。

d) **[継承の無効化（Disable Inheritance）]** をクリックし、**[継承された権限をこのオブジェクトの明示的な権限に変換する（Convert inherited permissions into explicit permissions on this object）]** を選択します。
e) 自分のユーザーアカウントではない各権限エントリを選択し、**[削除（Remove）]** をクリックします。
f) 自分のユーザーアカウントのアクセス権限が **[フルコントロール（Full Control）]** であることを確認します。
g) 変更を保存します。

**ステップ 2** インスタンスに接続するには、Windows PowerShell を開き、次のコマンドを実行します。

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

ここで、

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

<username> は、Threat Defense Virtual インスタンスのユーザー名です。

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

# PuTTY を使用した Threat Defense Virtual インスタンスへの接続

PuTTY を使用して Windows システムから Threat Defense Virtual インスタンスに接続するには、次の手順を実行します。

**ステップ 1** PuTTY を開きます。

**ステップ 2** **[カテゴリ（Category）]** ペインで、**[セッション（Session）]** を選択し、次の内容を入力します。

- **ホスト名または IP アドレス**：

  **<username>@<public-ip-address>**

  ここで、

  <username> は、Threat Defense Virtual インスタンスのユーザー名です。

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

- **ポート**： 22
- **接続タイプ**： SSH

**ステップ 3** **[カテゴリ（Category）]** ペインで、**[Window]** を展開し、**[変換（Translation）]** を選択します。

**ステップ 4** **[リモート文字セット（Remote character set）]** ドロップダウンリストで、**[UTF-8]** を選択します。

Linuxベースのインスタンスでデフォルトのロケール設定はUTF-8です。これにより、PuTTYは同じロケールを使用するように設定されます。

**ステップ 5** **[カテゴリ（Category）]** ペインで、**[接続（Connection）]**、**[SSH]** の順に展開し、**[認証（Auth）]** をクリックします。

**ステップ 6** **[参照（Browse）]** をクリックして、秘密キーを選択します。

**ステップ 7** **[開く（Open）]** をクリックして、セッションを開始します。

インスタンスに初めて接続する場合は、「サーバーのホストキーがレジストリにキャッシュされていない（the server's host key is not cached in the registry）」というメッセージが表示されることがあります。**[はい（Yes）]** をクリックして、接続を続行します。

# IPv6 のトラブルシューティング

**問題** SSH：IPv6 を使用した Firewall Threat Defense Virtual が機能していない

- **解決法** インターネットゲートウェイ経由の IPv6 パブリックアクセスのルートが追加されていることを確認します。
- **解決法** IPv6 の有効化は、Firewall Threat Defense Virtual の管理構成で設定できます。
- **解決法** 展開された Firewall Threat Defense Virtual に IPv6 関連のアクセス リストが追加されていることを確認します。
- **解決法** 管理インターフェイスで、IPv6 を構成するために「ipv6 address dhcp default」が使用されているかどうかを確認します。「ipv6 address dhcp」のみを使用する場合は、以下のルートを別途追加します。「ipv6 route management ::/0 <IPv6_Gateway_address> 」
- **解決法** 適切な ssh イングレスが許可されているかどうかを確認します。次のコマンドを使用して、すべての「ssh ::/0 management」に対して ssh アクセス許可を設定します。

**問題** 既存のサブネットに IPv6 アドレスを割り当てることができません。

- **解決法** サブネットが属する VCN が IPv6 についてすでに有効になっているかどうかを確認します。
- **解決法** 正しい IPv6 CIDR が使用されていることを確認します。
- **解決法** サブネットには「/64」IPv6 CIDR プレフィックスのみを含めることができます。

**問題** 水平方向のトラフィックが機能していない。

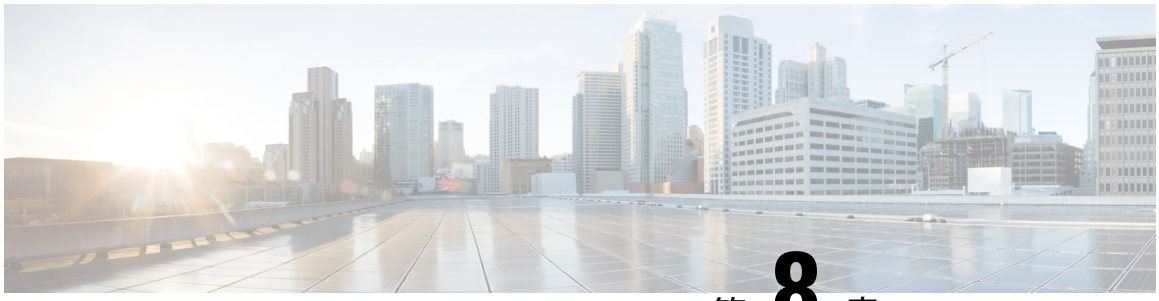
- **解決法** 以下のルートが正しく追加されていることを確認します。

  **解決法** ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

  **解決法** 例：ipv6 route inside 2603:c020:5:5800::/56 fe80::200:17ff:fe96:921b

- **解決法** 正しい IPv6 CIDR が使用されていることを確認します。

- **解決法** IPv6 に適切なアクセスリストが設定されていることを確認します。



第 8 章

# Google Cloud Platform への Threat Defense Virtual の展開

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

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

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

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


- 概要 （346 ページ）
- エンドツーエンドの手順 （348 ページ）
- 前提条件 （348 ページ）
- Threat Defense Virtual および GCP のガイドラインと制限事項 （349 ページ）
- データインターフェイス への NIC マッピング （352 ページ）
- ネットワークトポロジの例 （353 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （354 ページ）
- GCP 環境の設定 （355 ページ）
- ファイアウォールルールの作成 （355 ページ）
- Threat Defense Virtual の導入 （356 ページ）
- 外部 IP を使用した Threat Defense Virtual インスタンスへの接続 （358 ページ）
- シリアルコンソールを使用した Threat Defense Virtual インスタンスへの接続 （359 ページ）
- Gcloud を使用した Threat Defense Virtual インスタンスへの接続 （359 ページ）

- GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開について （360 ページ）
- 診断インターフェイスを使用しない Threat Defense Virtual の展開のガイドラインと制限事項 （360 ページ）
- GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開におけるデータインターフェイスへの NIC マッピング （361 ページ）
- GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開 （361 ページ）
- アップグレードのシナリオ （363 ページ）
- 診断インターフェイスを使用しない Threat Defense Virtual クラスタまたは Auto Scale ソリューションの展開 （363 ページ）
- トラブルシューティング （363 ページ）
- Auto Scale ソリューション （364 ページ）
- 導入パッケージのダウンロード （367 ページ）
- システム要件 （368 ページ）
- 前提条件 （371 ページ）
- Auto Scale ソリューションの展開 （381 ページ）
- Auto Scale ロジック （387 ページ）
- ロギングとデバッグ （388 ページ）
- トラブルシューティング （389 ページ）


# 概要

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

# システム要件

Threat Defense Virtual のニーズに合わせて Google 仮想マシンのタイプとサイズを選択します。現在、Threat Defense Virtual はコンピューティング最適化マシンと汎用マシン（標準タイプ、大容量メモリタイプ、高性能 CPU タイプ）のいずれもサポートしています。

（注） サポートされるマシンタイプは、予告なく変更されることがあります。

表 *26* : サポートされるコンピューティング最適化マシンタイプ

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

表 *27* : サポートされる汎用マシンタイプ

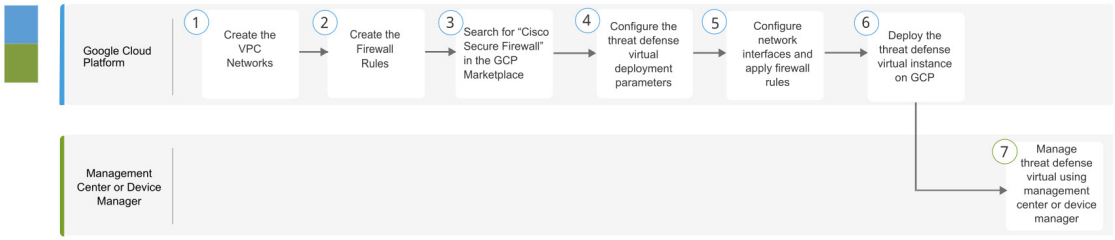
| 汎用マシンタイプ | 属性 | | |
|---|---|---|---|
| | **vCPU** | **RAM（GB）** | **vNIC** |
| n1-standard-4 | 4 | 15 | 4 |
| n1-standard-8 | 8 | 30 | 8 |
| n1-standard-16 | 16 | 60 | 8 |
| n2-standard-4 | 4 | 16 | 4 |
| n2-standard-8 | 8 | 32 | 8 |
| n2-standard-16 | 16 | 64 | 8 |
| n1-highcpu-8 | 8 | 7.2 | 8 |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

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

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

# エンドツーエンドの手順

次のフローチャートは、Google Cloud Platform に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | GCP | GCP 環境の設定：VPC ネットワークを作成します（**[VPCネットワーク（VPC Networks）] > [サブネット（Subnet）] > [リージョン（Region）] > [IPアドレス範囲（IP address range）]**）。 |
| 2 | GCP | ファイアウォールルールの作成：ファイアウォールルールを作成します（**[ネットワーキング（Networking）] > [VPCネットワーク（VPC networks）] > [ファイアウォール（Firewall）] > [ファイアウォールルールの作成（Create Firewall Rule）]**）。 |
| 3 | GCP | Threat Defense Virtual の導入：GCP Marketplace で「Cisco Secure Firewall」を検索します。 |
| 4 | GCP | Threat Defense Virtual の導入：Threat Defense Virtual の展開パラメータを設定します。 |
| 5 | GCP | Threat Defense Virtual の導入：ネットワーク インターフェイスを設定し、ファイアウォールルールを適用します。 |
| 6 | GCP | Threat Defense Virtual の導入：GCP に Threat Defense Virtual を展開します。 |
| 7 | Management Center または Device Manager | Threat Defense Virtual の管理：<br>• Management Center を使用<br>• Device Manager を使用 |

# 前提条件

- https://cloud.google.com で GCP アカウントを作成します。

- GCP プロジェクトを作成します。Google ドキュメントの 『Creating Your Project』を参照してください。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
- Threat Defense Virtual へのライセンス付与。
  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『 Cisco Secure Firewall Management Center アドミニストレーション ガイド』 の「*Licensing*」の章を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - トラフィック インターフェイス（2）：Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。
- 通信パス：
  - Threat Defense Virtual にアクセスするためのパブリック IP。
- Threat Defense Virtual のシステム要件については、『Cisco Firepower Compatibility Guide』を参照してください。

# Threat Defense Virtual および GCP のガイドラインと制限事項

### サポートされる機能

- GCP Compute Engine での展開
- インスタンスあたり最大 16 個の vCPU
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- クラスタリング（7.2 以降）詳細については、『パブリッククラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。

- Cisco Secure Firewall 7.1 以前のバージョンでは、 Management Center のみがサポートされています。Cisco Secure Firewall バージョン 7.2 以降では、Device Manager もサポートされます。

### Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual 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 *28 : Threat Defense Virtual* 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/32 GB | 16 Gbps | 10,000 |

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Licensing」の章を参照してください。

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

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「GCP での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### 送受信キューの割り当て

ネットワークパケットを処理するために、特定の数の受信（RX）および送信（TX）キューが各 vNIC に割り当てられます。Google Cloud では、使用されるネットワーク インターフェイスのタイプ（VirtIO または gVNIC）に基づき、アルゴリズムを使用して、vNIC ごとにデフォルトの数の RX および TX キューが割り当てられます。

vNIC にキューを割り当てるために GCP で使用される方法は次のとおりです。

- VirtIO：vCPU の数が vNIC の数で除算され、残りの値は破棄されます。

  たとえば、VM に 16 個の vCPU と 4 個の vNIC がある場合、vNIC ごとに割り当てられるキューの数は 16/4 = 4 です。

- gVNIC：vCPU の数が vNIC の数で除算され、結果がさらに 2 で除算されます。

  たとえば、VM に 128 個の vCPU と 2 個の vNIC がある場合、割り当てられるキューの数は（128/2）/2 = 2 です。

また、Compute Engine API を使用して新しい VM を作成する場合、各 vNIC に割り当てられるキューの数をカスタマイズできます。ただし、カスタマイズする場合は、次のルールに従う必要があります。

- 最小キュー数：vNIC ごとに 1 つ。
- 最大キュー数：この数は、ドライバタイプに基づいて、vCPU 数または vNIC あたりの最大キュー数のうち、小さい方です。
  - VirtIO またはカスタムドライバを使用している場合、最大キュー数は 32 です。
  - gVNIC を使用している場合、最大キュー数は 16 です。
- VM のすべての vNIC に割り当てられるキューの数をカスタマイズする場合、キューの割り当て総数は、VM インスタンスに割り当てられた vCPU の数以下である必要があります。

デフォルトおよびカスタムキュー割り当ての詳細と例については、「デフォルトキューの割り当て」および「カスタムキューの割り当て」を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

### アップグレード

GCP の Threat Defense Virtual のアップグレードは、Cisco Secure Firewall バージョン 7.1 から 7.2 へはサポートされていません。Cisco Secure Firewall バージョン 7.1 から 7.2 にアップグレードする場合は、再イメージ化を実行します。

### サポートされない機能

- IPv6
- Threat Defense Virtual ネイティブ HA
- トランスペアレント/インライン/パッシブ モード
- ジャンボ フレーム

# データインターフェイス への NIC マッピング

Cisco Secure Firewall バージョン 7.1 以前のリリースにおけるネットワーク インターフェイス カード（NIC）とデータインターフェイスのマッピングは次のとおりです。

- nic0 – 管理インターフェイス
- nic1 – 診断インターフェイス
- nic2 – ギガビットイーサネット 0/0
- nic3 – ギガビットイーサネット 0/1

Cisco Secure Firewall バージョン 7.2 以降、外部ロードバランサ（ELB）はパケットを nic0 にのみ転送するため、North-South トラフィックの移動を容易にするために nic0 にデータインターフェイスが必要です。

Cisco Secure Firewall バージョン 7.2 の NIC とデータインターフェイスのマッピングは次のとおりです。

- nic0 – ギガビットイーサネット 0/0
- nic1 – ギガビットイーサネット 0/1
- nic2 – 管理インターフェイス
- nic3 – 診断インターフェイス
- nic4 – ギガビットイーサネット 0/2

  .

  .

  .

- nic(N-2) – ギガビットイーサネット 0/N-4

- nic(N-1) – ギガビットイーサネット 0/N-3

Cisco Secure Firewall バージョン 7.4.1 以降では、診断インターフェイスを使用せずに Threat Defense Virtual を展開することもできます。そのようなシナリオでは、NIC とデータインターフェイスのマッピングは次のようになります。

- nic0 – ギガビットイーサネット 0/0
- nic1 – ギガビットイーサネット 0/1
- nic2 – 管理インターフェイス
- nic3 – ギガビットイーサネット 0/2
- nic4 – ギガビットイーサネット 0/3

.

.

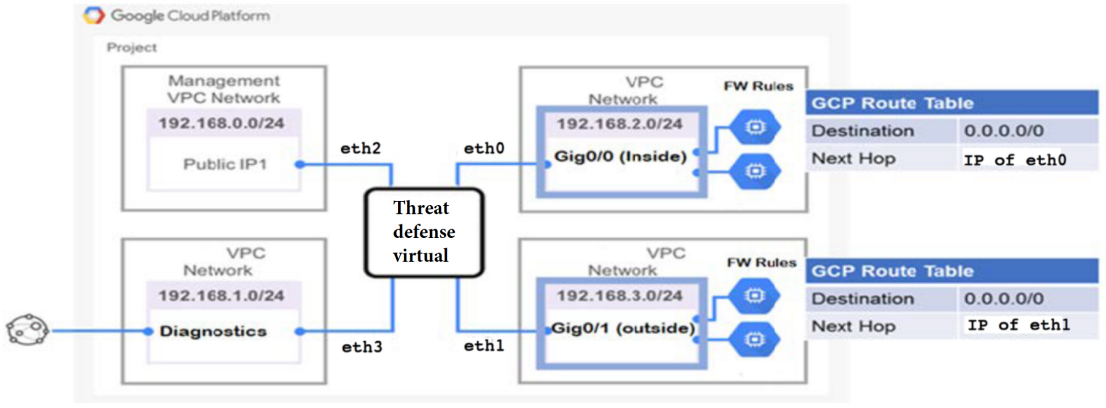
.

- nic(N-2) – ギガビットイーサネット 0/N-3
- nic(N-1) – ギガビットイーサネット 0/N-2

# ネットワークトポロジの例

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

**図 *45 : GCP* 展開での *Threat Defense Virtual* の例**



# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# GCP 環境の設定

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

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

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

**ステップ 1** GCP コンソールで、**[VPC ネットワーク（VPC networks）]** を選択し、**[VPC ネットワークの作成（Create VPC Network）]** をクリックします。

**ステップ 2** **[名前（Name）]** フィールドに、特定の名前を入力します。

**ステップ 3** サブネット作成モードで、[カスタム（Custom）] をクリックします。

**ステップ 4** **新しいサブネット**で **[名前（Name）]** フィールドに、特定の名前を入力します。

**ステップ 5** **[地域（Region）]** ドロップダウンリストから、展開に適した地域を選択します。4 つのネットワークはすべて同じリージョン内にある必要があります。

**ステップ 6** [IPアドレス範囲（IP address range）] フィールドで、最初のネットワークのサブネットを CIDR 形式（10.10.0.0/24 など）で入力します。

**ステップ 7** その他すべての設定はデフォルトのままで、**[作成（Create）]** をクリックします。

**ステップ 8** ステップ 1 ー 7 を繰り返して、残りの 3 つの VPC ネットワークを作成します。

# ファイアウォールルールの作成

Threat Defense Virtual インスタンスの展開中に、管理インターフェイスのファイアウォールルールを適用します（Management Centerとの SSH および SFTunnel 通信を許可するため）。Threat Defense Virtual の導入 （356 ページ） を参照してください。要件に応じて、内部、外部、および診断インターフェイスのファイアウォールルールを作成することもできます。

**ステップ 1** GCP コンソールで、**[ネットワーキング（Networking）]** > **[VPC ネットワーク（VPC network）]** > **[ファイアウォール（Firewall）]**を選択し、**[ファイアウォールルールの作成（Create Firewall Rule）]** をクリックします。

**ステップ 2** **[名前（Name）]** フィールドに、ファイアウォールルールのわかりやすい名前を入力します（例：*vpc-asiasouth-inside-fwrule*）。

**ステップ 3** **[ネットワーク（Network）]** ドロップダウンリストから、ファイアウォールルールを作成する VPC ネットワークの名前を選択します（例：*ftdv-south-inside*）。

**ステップ 4** **[ターゲット（Targets）]** ドロップダウンリストから、ファイアウォールルールに適用可能なオプションを選択します（例：**[ネットワーク内のすべてのインスタンス（All instances in the network）]**）。

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

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

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

**ステップ 7** セキュリティルールを追加します。

**ステップ 8** [作成（Create）] をクリックします。

# Threat Defense Virtual の導入

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

**ステップ 1** GCP コンソールにログインします。

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

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

**ステップ 4** [作成（Launch）] をクリックします。

a) **[展開名（Deployment name）]**：インスタンスの一意の名前を指定します。

b) **[ゾーン（Zone）]**：Threat Defense Virtualを展開するゾーンを選択します。

c) **[マシンタイプ（Machine type）]**：システム要件 （346 ページ）に基づいて正しいマシンタイプを選択します。

d) **[SSH キー（SSH key）]（オプション）**：SSH キーペアから公開キーを貼り付けます。

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

e) このインスタンスにアクセスするためのプロジェクト全体の SSH キーを許可するかブロックするかを選択します。Google ドキュメント『Allowing or blocking project-wide public SSH keys from a Linux instance』を参照してください。

f) **[起動スクリプト（Startup script）]**：インスタンスが起動するたびに自動化されたタスクを実行するために、Threat Defense Virtual インスタンスの起動スクリプトを作成できます。

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

```
{
"AdminPassword": "Cisco@123123",
"Hostname": "ftdv-gcp",
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

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

g) **[ネットワークインターフェイス（Network interfaces）]**：1）管理、2）診断、3）内部、4）外部のインターフェイスを設定します。

（注） インスタンスを作成した後では、インスタンスにインターフェイスを追加できません。不適切なインターフェイス構成でインスタンスを作成した場合は、インスタンスを削除し、適切なインターフェイス構成で再作成する必要があります。

1. **[ネットワーク（Network）]** ドロップダウンリストから、[VPC network（VPC ネットワーク）]（*vpc-asiasouth-mgmt* など）を選択します。
2. **[外部 IP（External IP）]** ドロップダウンリストから、適切なオプションを選択します。

   管理インターフェイスには、[外部 IP からエフェメラルへ（External IP to Ephemeral）] を選択します。内部および外部インターフェイスでは、これはオプションです。
3. [完了（Done）] をクリックします。

h) **[ファイアウォール（Firewall）]**：ファイアウォールルールを適用します。

- **[インターネットからの TCP ポート 22 のトラフィックを許可する（SSH アクセス）（Allow TCP port 22 traffic from the Internet (SSH access)）]** チェックボックスをオンにして、SSH を許可します。
- **[インターネットからの HTTPS のトラフィックを許可する（FMC access）（Allow HTTPS traffic from the Internet (FMC access)）]** チェックボックスをオンにして、Management Centerおよび管理対象デバイスが双方向の SSL 暗号化通信チャネル（SFTunnel）を使用して通信できるようにします。

i) **[詳細（More）]** をクリックしてビューを展開し、**[IP 転送（IP Forwarding）]**が**[オン（On）]**に設定されていることを確認します。

**ステップ 5** [展開（Deploy）] をクリックします。

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

### 次のタスク

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

# 外部 IP を使用した Threat Defense Virtual インスタンスへの接続

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

**ステップ 1** GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]**>**[VM インスタンス（VM instances）]** を選択します。

**ステップ 2** Threat Defense Virtualのインスタンス名をクリックすると、**[VM インスタンスの詳細（VM instance details）]** ページが開きます。

**ステップ 3** **[詳細（Details）]** タブで、**[SSH]** フィールドのドロップダウンメニューをクリックします。

**ステップ 4** **[SSH]** ドロップダウンメニューから、目的のオプションを選択します。

次の方法を使用してThreat Defense Virtualインスタンスに接続できます。

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

# SSH を使用した Threat Defense Virtual インスタンスへの接続

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

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

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

ここで、

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

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

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

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

<username> は、Threat Defense Virtual インスタンスのユーザー名です。

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

# シリアルコンソールを使用した Threat Defense Virtual インスタンスへの接続

**ステップ 1** GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]** > **[VM インスタンス（VM instances）]** を選択します。

**ステップ 2** Threat Defense Virtualのインスタンス名をクリックすると、**[VM インスタンスの詳細（VM instance details）]** ページが開きます。

**ステップ 3** **[詳細（Details）]** タブで、**[シリアルコンソールへの接続（Connect to serial console）]** をクリックします。

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

# Gcloud を使用した Threat Defense Virtual インスタンスへの接続

**ステップ 1** GCP コンソールで、**[コンピューティングエンジン（Compute Engine）]** > **[VM インスタンス（VM instances）]** を選択します。

**ステップ 2** Threat Defense Virtualのインスタンス名をクリックすると、**[VM インスタンスの詳細（VM instance details）]** ページが開きます。

**ステップ 3** **[詳細（Details）]** タブで、**[SSH]** フィールドのドロップダウンメニューをクリックします。

**ステップ 4** **[gcloud コマンドを表示（View gcloud command）]** > **[Cloud Shell で実行（Run in Cloud Shell）]**をクリックします。

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

# GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開について

Cisco Secure Firewall バージョン 7.3 以前では、Threat Defense Virtual は少なくとも 4 つのインターフェイス（1 つの管理インターフェイス、1 つの診断インターフェイス、2 つのデータインターフェイス）で展開されます。

Cisco Secure Firewall バージョン 7.4.1 以降は、診断インターフェイスを削除し、少なくとも 4 つのインターフェイス（1 つの管理インターフェイスと 3 つのデータインターフェイス）で Threat Defense Virtual を展開できます。この機能により、同じマシンタイプに追加のデータインターフェイスを備えた Threat Defense Virtual を展開できます。たとえば、c2-standard-8 マシンタイプでは、1 つの管理インターフェイス、1 つの診断インターフェイス、および 6 つのデータインターフェイスを備えた Threat Defense Virtual を展開する代わりに、1 つの管理インターフェイスと 7 つのデータインターフェイスを備えた Threat Defense Virtual を展開できます。

この機能は、Google Cloud Platform（GCP）上の Threat Defense Virtual インスタンスの新しい展開でのみサポートされます。

（注） サポートされるインターフェイスの最大数は 8 であるため、最大 4 つのインターフェイスを追加して、最大 8 つのインターフェイスを備えた Threat Defense Virtual を展開できます。

# 診断インターフェイスを使用しない Threat Defense Virtual の展開のガイドラインと制限事項

- 診断インターフェイスが削除されると、診断インターフェイスの代わりに Threat Defense Virtual 管理インターフェイスまたはデータインターフェイスを使用して syslog および SNMP がサポートされます。
- この展開では、クラスタリングと Auto Scale がサポートされています。
- 診断インターフェイスポートを持つ Threat Defense Virtual インスタンスと、診断インターフェイスポートを持たない Threat Defense Virtual インスタンスのグループ化はサポートされていません。

（注） ここでの Threat Defense Virtual インスタンスのグループ化は、GCP 上のインスタンスグループ内のインスタンスのグループ化を指します。これは、Management Center Virtual での Threat Defense Virtual インスタンスのグループ化には関係しません。

- CMI はサポートされていません。

# GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開におけるデータインターフェイスへの NIC マッピング

診断インターフェイスを使用せずに Threat Defense Virtual を展開するためのデータインターフェイスへの NIC マッピングを以下に示します。

| Net-Interface | VPC | Port |
|---|---|---|
| NIC0 | outside-vpc | Gig0/0 |
| NIC1 | inside-vpc | Gig0/1 |
| NIC2 | mgmt-vpc | Management |
| NIC3 | diag-vpc | M0/0* |

FTDv-4-NICs

| Net-Interface | VPC | Port |
|---|---|---|
| NIC0 | outside-vpc | Gig0/0 |
| NIC1 | inside-vpc | Gig0/1 |
| NIC2 | mgmt-vpc | Management |

FTDv-3-NICs

# GCP での診断インターフェイスを使用しない Threat Defense Virtual の展開

診断インターフェイスを使用せずに Threat Defense Virtual を展開するには、次の手順を実行します。

**ステップ 1** 新規展開に使用される Day-0 構成スクリプト（GCP コンソールの **Startup script**）でキーと値のペア **Diagnostic: OFF/ON** を使用して、この機能を有効にします。デフォルトでは、キーと値のペアは **Diagnostic: ON** に設定されていて、診断インターフェイスが起動します。キーと値のペアが **Diagnostic: OFF** に設定されている場合、展開は診断インターフェイスを使用せずに起動します。

次に、Day-0 構成スクリプトの例を示します。

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

（注） キーと値のペア "Diagnostic": "ON/OFF" では、大文字と小文字が区別されます。

**ステップ 2** 必要な最小数の NIC（4 枚）を接続します。

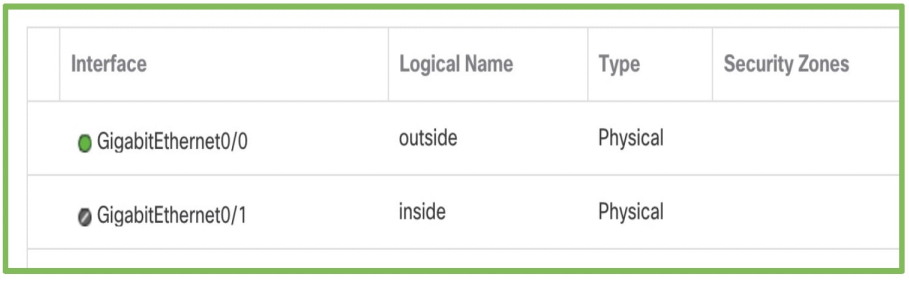
GCP に Threat Defense Virtual を展開する詳細な手順については、「Google Cloud Platform への Threat Defense Virtual の展開」を参照してください。

インターフェイスの詳細については、「Interface Overview」を参照してください。

**ステップ 3** （任意） コンソールで **show interface ip brief** コマンドを使用して、インターフェイスの詳細を表示します。次に示されているように、Management Center Virtual でインターフェイスの詳細を表示することもできます。

Management Center Virtual では、インターフェイスは次のように表示されます。


With Diagnostic Interface




Without Diagnostic Interface

# アップグレードのシナリオ

Threat Defense Virtual インスタンスは、以下のシナリオに従ってアップグレードできます。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできます。
- Cisco Secure Firewall バージョン 7.4 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできます。

次に示すアップグレードシナリオはサポートされていません。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできません。
- Cisco Secure Firewall バージョン 7.4.1 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできません。

（注） NIC の数と順序は、アップグレード後も維持されます。

# 診断インターフェイスを使用しない Threat Defense Virtual クラスタまたは Auto Scale ソリューションの展開

Threat Defense Virtual クラスタ、または診断インターフェイスを使用しない Threat Defense Virtual インスタンスで構成される Auto Scale ソリューションの新しい展開を実行するには、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されていることを確認します。

# トラブルシューティング

Threat Defense Virtual の展開時に診断インターフェイスが削除されない場合は、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されているか確認します。

# Auto Scale ソリューション

次の項では、Auto Scale ソリューションのコンポーネントが GCP の Threat Defense Virtual でどのように機能するかについて説明します。

## 概要

Threat Defense Virtual Auto Scale for GCP は、GCP によって提供されるサーバーレス インフラストラクチャ（クラウド機能、ロードバランサ、Pub/Sub、インスタンスグループなど）を利用した完全なサーバーレス導入です。

Threat Defense Virtual Auto Scale for GCP 導入の主な特徴は次のとおりです。

- GCP Deployment Manager のテンプレートをベースとした導入。
- CPU 使用率などに基づくスケーリングメトリックをサポート。
- Threat Defense Virtual 展開とマルチ可用性ゾーンのサポート。
- Threat Defense Virtual の自動登録および登録解除をサポート。
- 完全に自動化された設定をスケールアウトされた Threat Defense Virtual インスタンスに自動適用。
- NAT ポリシー、アクセスポリシー、およびルートを自動的に Threat Defense Virtual に適用。
- ロードバランサとマルチ可用性ゾーンのサポート。
- 他のプラットフォームで Management Center Virtual をサポート。
- シスコでは、導入を容易にするために、Auto Scale for GCP の導入パッケージを提供しています。

## 注意事項と制約事項

- IPv4 だけがサポートされます。
- ライセンス：BYOL のみをサポートしています。PAYG ライセンスはサポートされていません。
- デバイス機能エラーはログに表示されません。
- サポートされるデバイスの最大数は 25 です。これは、Management Center Virtual インスタンスの上限です。
- すべての Cisco Secure Firewall バージョンで、提供されているテンプレートを使用して、Threat Defense Virtual Auto Scale ソリューションを展開できます。Threat Defense Virtual イ

ンスタンスは、少なくとも 4 つのインターフェイス（1 つの管理インターフェイス、1 つの診断インターフェイス、および 2 つのデータインターフェイス）で展開されます。

Cisco Secure Firewall バージョン 7.4.1 以降では、診断インターフェイスを使用せずに Threat Defense Virtual を展開することもできます。このシナリオでも、展開は少なくとも 4 つのインターフェイス（1 つの管理インターフェイスと 3 つのデータインターフェイス）で実行されます。この展開を実行するには、入力パラメータ （373 ページ）の説明に従って、テンプレートパラメータ（*diagFirewallRule*、*diagSubnetworkName*、*diagVpcName*、および *withDiagnostic*）を変更します。

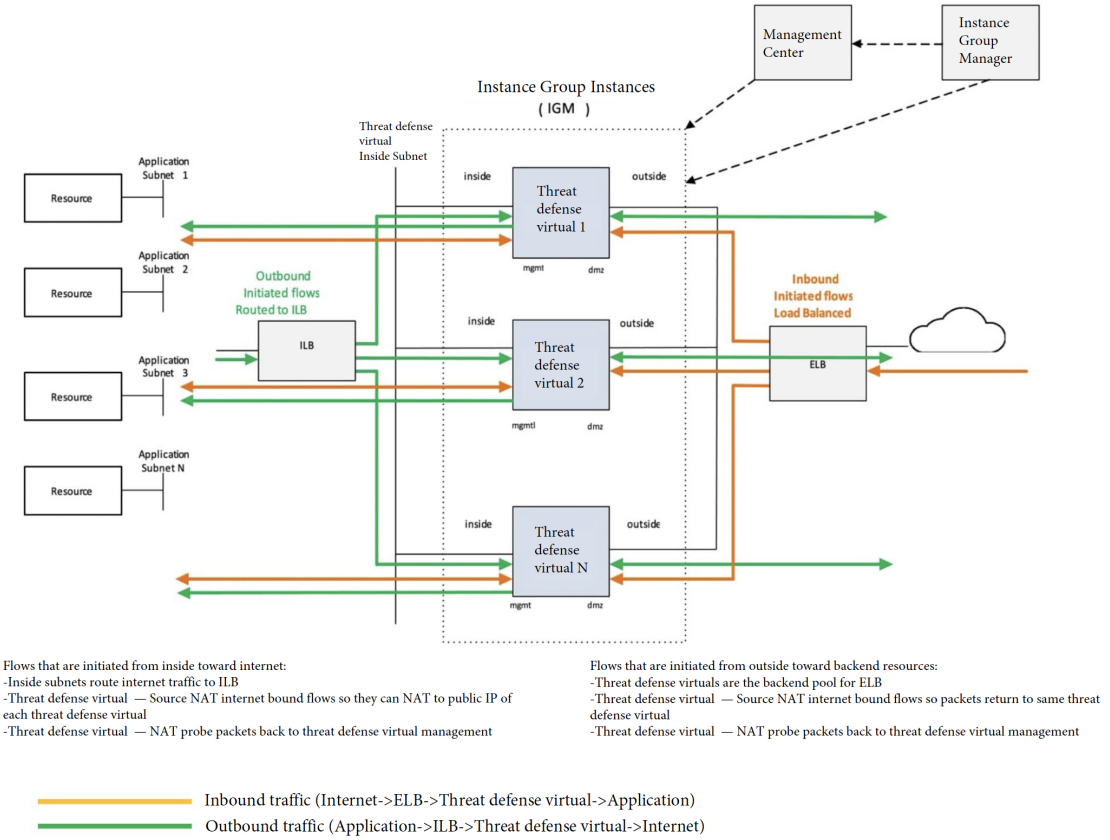
- スケールアウト時間を短縮するコールドスタンバイまたはスナップショットメソッドはサポートされていません。
- スケジュールベースのスケーリングはサポートされていません。
- 平均メモリ使用率に基づく自動スケーリングはサポートされていません。
- スケールイン/スケールアウトにより、インスタンスの数が 1 よりも多く減少/増加する場合がありますが、Management Center Virtual での Threat Defense Virtual インスタンスの登録解除/登録は順次 1 つずつ実行されます。
- スケールイン時に 300 秒の接続ドレイン時間があります。ドレイン時間を必要な時間に手動で設定することもできます。
- 外部ロードバランサは、提供されているテンプレートによって作成されます。ロードバランサのパブリック IP の DNS 要件をカスタマイズすることはできません。
- ユーザーは、既存のインフラストラクチャを導入のサンドイッチモデルに適合させる必要があります。
- スケールアウトおよびスケールインのプロセス中に発生したエラーの詳細については、クライド機能のログを分析してください。
- NAT、デバイスグループに付加されたセキュリティポリシー、および静的ルートは、新しく作成された 脅威に対する防御 ファイルに適用されます。
- ソリューションを複数の Threat Defense Virtual に対して展開する場合、Management Center Virtual は一度に 1 つの登録要求しか処理できないため、展開時間が長くなります。スケールアウトによって複数の Threat Defense Virtual インスタンスが追加されると、展開時間も長くなります。現在、すべての登録と登録解除は連続して実行されます。
- 自動スケーリングを開始する前に、Management Center Virtual でデバイスグループ、NAT ルール、およびネットワークオブジェクトを作成する必要があります。ILB および ELB IP は、ソリューションを展開してからのみ使用できることに注意してください。したがって、ダミーオブジェクトを作成し、実際の IP を取得した後にオブジェクトを更新できます。

# Auto Scale の導入例

Threat Defense Virtual Auto Scale for GCP は、Threat Defense Virtual インスタンスグループを GCP の内部ロードバランサ（ILB）と GCP の外部ロードバランサ（ELB）の間に配置する水平方向の自動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インスタンスグループ内の Threat Defense Virtual インスタンスに分散させます。その後、Threat Defense Virtual がアプリケーションにトラフィックを転送します。
- ILB は、アプリケーションからのインターネットトラフィックをインスタンスグループ内の Threat Defense Virtual インスタンスに分散させます。その後、Threat Defense Virtual がインターネットにトラフィックを転送します。
- ネットワークパケットが、単一の接続で両方（内部および外部）のロードバランサを通過することはありません。
- スケールセット内の Threat Defense Virtual 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 *46 : Threat Defense Virtual* 自動スケールのユースケース**



すべての Cisco Secure Firewall バージョンで、提供されているテンプレートを使用して、Threat Defense Virtual Auto Scale ソリューションを展開できます。Threat Defense Virtual インスタンスは、少なくとも 4 つのインターフェイス（1 つの管理インターフェイス、1 つの診断インターフェイス、および 2 つのデータインターフェイス）で展開されます。

Cisco Secure Firewall バージョン 7.4.1 以降では、診断インターフェイスを使用せずに Threat Defense Virtual を展開することもできます。このシナリオでも、展開は少なくとも 4 つのインターフェイス（1 つの管理インターフェイスと 3 つのデータインターフェイス）で実行されます。この展開を実行するには、入力パラメータ （373 ページ）の説明に従って、テンプレートパラメータ（*diagFirewallRule*、*diagSubnetworkName*、*diagVpcName*、および *withDiagnostic*）を変更します。

# スコープ

このドキュメントでは、Threat Defense Virtual Auto Scale for GCP 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際の詳細な手順について説明します。

**重要**

- 導入を開始する前に、ドキュメント全体をお読みください。
- 導入を開始する前に、前提条件を満たしていることを確認します。
- ここに記載されている手順と実行順序に従っていることを確認します。

# 導入パッケージのダウンロード

Threat Defense Virtual Auto Scale for GCP は、GCP によって提供されるサーバーレス インフラストラクチャ（クラウド機能、ロードバランサ、Pub/Sub、インスタンスグループなど）を利用した GCP Deployment Manager のテンプレートベースの導入です。

Threat Defense Virtual Auto Scale for GCP 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。該当する Threat Defense Virtual バージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

**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。

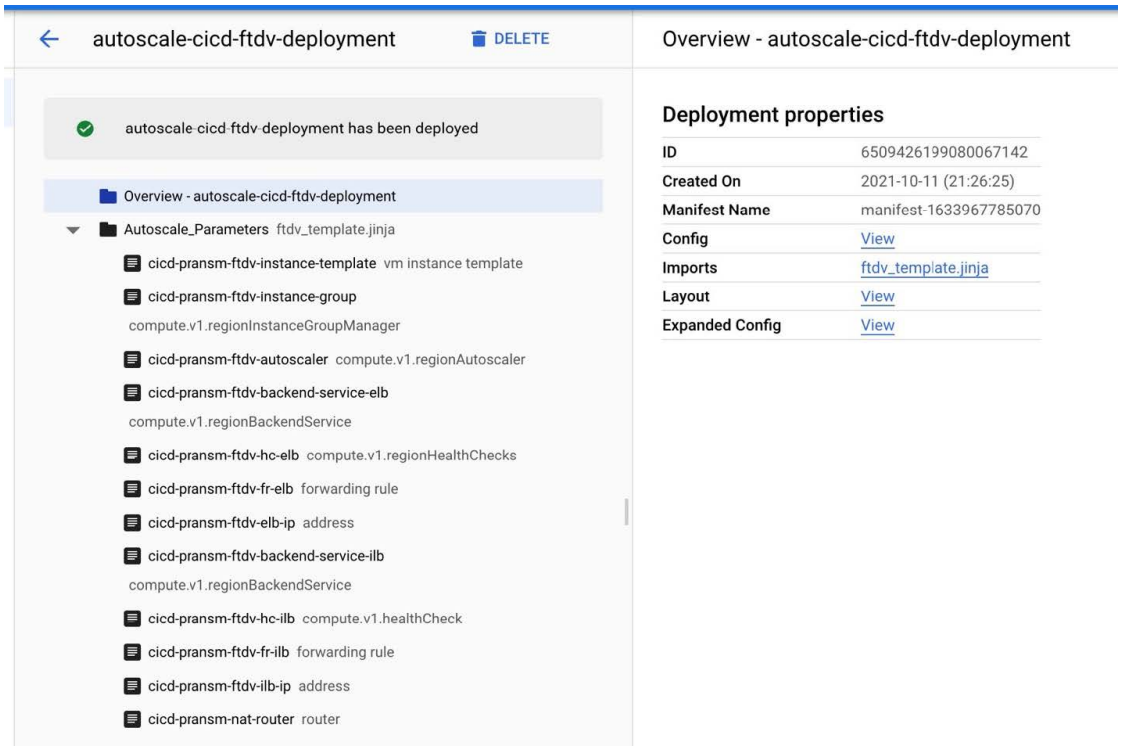
# システム要件

Threat Defense Virtual Auto Scale for GCP 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。

### 導入マネージャ

- 構成をコードとして扱い、反復可能な展開を実行します。Google Cloud Deployment Manager では、YAML を使用して、アプリケーションに必要なすべてのリソースを宣言形式で指定できます。また、Jinja2 テンプレートを使用して構成をパラメータ化し、一般的な導入パラダイムを再利用可能にすることもできます。
- リソースを定義する構成ファイルを作成します。リソースを作成するプロセスを繰り返し実行することで、一貫した結果を得ることができます。詳細については、https://cloud.google.com/deployment-manager/docsを参照してください。

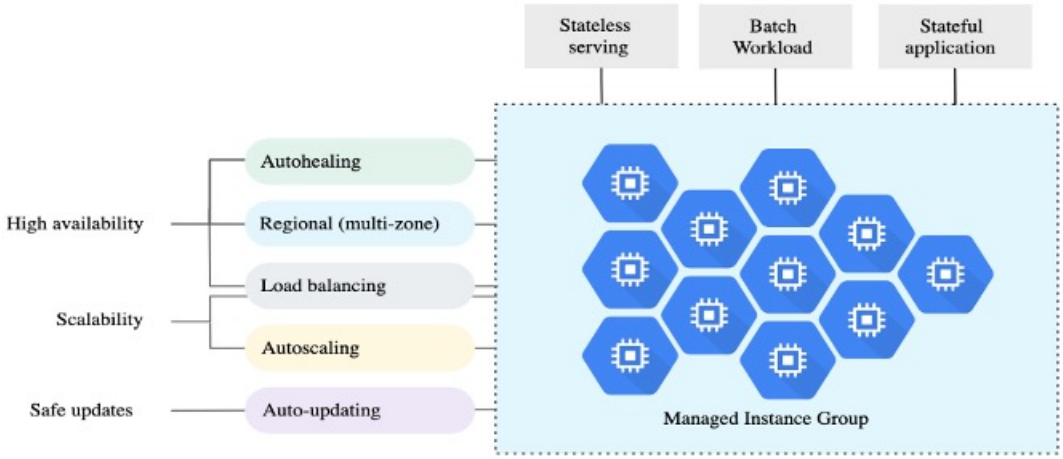
**図 47 : 導入マネージャビュー**




### GCP のマネージドインスタンス グループ

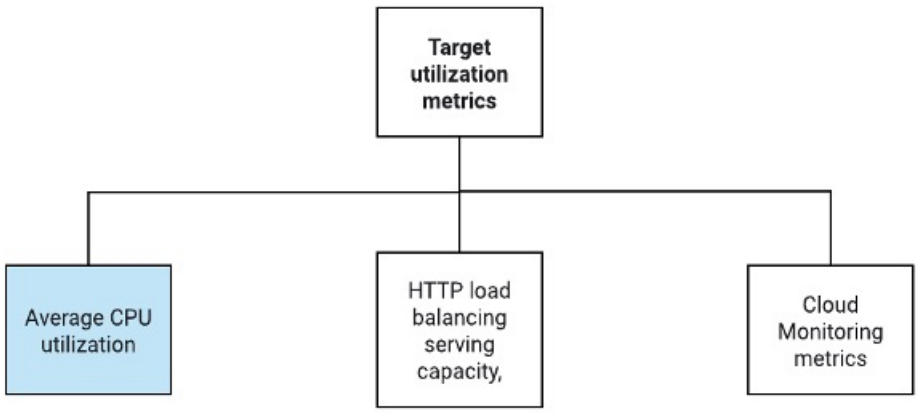
マネージドインスタンス グループ（MIG）は、指定したインスタンステンプレートとオプションのステートフル構成に基づいて、各マネージドインスタンスを作成します。詳細については、https://cloud.google.com/compute/docs/instance-groupsを参照してください。

図 *48* : インスタンスグループの機能




### ターゲット使用率メトリック

- 次の図は、ターゲット使用率のメトリックを示しています。自動スケーリングを決定する際、平均 CPU 使用率メトリックのみが使用されます。
- オートスケーラは、選択された使用率メトリクスに基づいて使用状況の情報を継続的に収集し、実際の使用率を希望するターゲット使用率と比較します。次に、この情報を使用して、グループがインスタンスを削除する必要があるか（スケールイン）またはインスタンスを追加する必要があるか（スケールアウト）を判断します。
- ターゲット使用率レベルとは、仮想マシン（VM）インスタンスをどのレベルで維持するかを示します。たとえば、CPU使用率に基づいてスケーリングする場合、ターゲット使用率レベルを75%に設定すると、オートスケーラは指定されたインスタンスグループで75%またはそれに近いCPU使用率を維持します。各メトリックの使用率レベルは、自動スケーリング ポリシーに基づいてさまざまに解釈されます。詳細については、https://cloud.google.com/compute/docs/autoscalerを参照してください。



### サーバーレスクラウド機能

SSH パスワードの変更、マネージャの設定、Management Center Virtual への Threat Defense Virtual の登録、Management Center Virtual から Threat Defense Virtual の登録解除などのタスクには、サーバーレスの Google Cloud 機能を使用します。

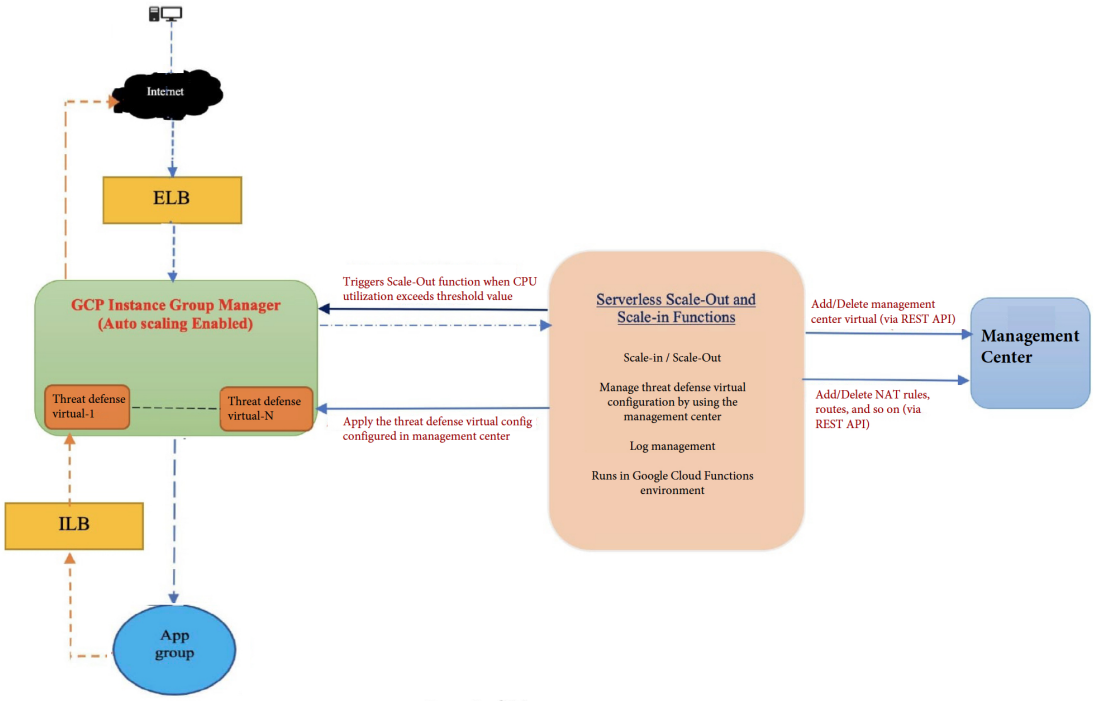
- スケールアウト中に新しい Threat Defense Virtual インスタンスがインスタンスグループに追加された場合、SSH パスワードの変更、マネージャの設定、Management Center Virtual への Threat Defense Virtual の登録、Management Center Virtual から Threat Defense Virtual の登録解除などのタスクを実行する必要があります。
- クラウド機能は、スケールアウトプロセス中にクラウドのパブリック/サブトピックを介してトリガーされます。また、スケールアウト時のインスタンス追加専用のフィルタを備えたログシンクもあります。

### クラウド機能を使用したサーバーレスのライセンス登録解除

- スケールイン時のインスタンス削除中に、Threat Defense Virtual インスタンスからライセンスの登録を解除し、Management Center Virtual から Threat Defense Virtual の登録を解除する必要があります。
- クラウド機能は、クラウドのパブリック/サブトピックを介してトリガーされます。特に削除プロセスについては、スケールイン時のインスタンス削除専用のフィルタを備えたログシンクがあります。
- クラウド機能がトリガーされると、削除対象の Threat Defense Virtual インスタンスに SSH で接続し、ライセンス登録解除のコマンドを実行します。

### Auto Scale ソリューションの概要

図 *49 : Auto Scale* ソリューションの概要




# 前提条件

## GCP リソース

### GCP プロジェクト

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プロジェクトが必要です。

### VPC ネットワーク

4 つの VPC が使用可能/作成されてい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。

既存のサブネットワークに加えて、/28 サブネットワークを使用して管理 VPC ネットワークに新しい VPC コネクタを作成します。クラウド機能はVPC コネクタを使用して、プライベート IP アドレスで Threat Defense Virtual にアクセスします。

Threat Defense Virtual 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。

- 外部トラフィック
- 内部トラフィック
- 管理トラフィック
- 診断トラフィック

### Firewall

VPC間通信を許可し、正常性プローブも許可するファイアウォールルールを作成する必要があります。

内部、外部、管理、および診断インターフェイス用に4つのファイアウォールルールが必要です。また、正常性チェックプローブを許可するファイアウォールルールを作成します。

正常性チェックプローブの IP アドレスは次のとおりです。

- 35.191.0.0/16
- 130.211.0.0/22
- 209.85.152.0/22
- 209.85.204.0/22

Deployment Managerテンプレートで後に使用されるファイアウォールタグに注意する必要があります。

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 Threat Defense Virtual 間の正常性プローブに必要です。サーバーレス機能と Threat Defense Virtual 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）。

# GCP クラウド機能パッケージの構築

Threat Defense Virtual GCP Auto Scale ソリューションでは、圧縮形式の ZIP パッケージでクラウド関数を提供する 2 つのアーカイブファイルを作成する必要があります。

- `ftdv_scalein.zip`
- `ftdv_scaleout.zip`

`ftdv_scalein.zip` および `ftdv_scaleout.zip` パッケージの構築方法については、Auto Scale の導入手順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。

# 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、GCP プロジェクトに GCP Deployment Manager を展開するときに、各パラメータを使用して Threat Defense Virtual デバイスを作成できます。

**表 *29 :* 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 |
|---|---|---|
| resourceNamePrefix | 文字列 | 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。<br>例：demo-test |
| region | GCP でサポートされている有効なリージョン<br>[String] | プロジェクトが展開されるリージョン名。<br>例：us-central1 |
| serviceAccountMailId | 文字列 [ Email Id] | サービスアカウントを識別するメールアドレス。 |
| vpcConnectorName | 文字列 | サーバーレス環境と VPC ネットワーク間のトラフィックを処理するコネクタの名前。<br>例：demo-test-vpc-connector |
| adminPassword | 文字列 | Threat Defense Virtual インスタンスの初期パスワード。後でこのパラメータは「newFtdPasswordSecret」に変更されます。 |
| bucketName | 文字列 | クラウド機能の ZIP パッケージをアップロードする GCP ストレージバケットの名前。<br>例：demo-test-bkt |
| coolDownPeriodSec | 整数 | オートスケーラが新しいインスタンスから情報の収集を開始するまで待機する秒数。<br>例：30 |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| cpuUtilizationTarget | 10 進数 (0,1] | オートスケーラーが維持する必要があるインスタンスグループ内の VM の平均 CPU 使用率。<br>例：0.5 |
| deployUsingExternalIP | ブール値 | Threat Defense Virtual の管理にパブリック IP アドレスが必要かどうかを決定します。<br>例：true<br>true に設定されている場合、Threat Defense Virtual にはパブリック IP アドレスが必要です。false に設定されている場合、パブリック IP アドレスは必要ありません。 |
| diagFirewallRule | 文字列 | 診断 VPC 用に作成されたファイアウォールルールの名前。<br>例：cisco-ftdv-diag-firewall-rule<br>診断インターフェイスを使用せずに Threat Defense Virtual を展開する場合は、このパラメータを空白のままにするか、ダミーの文字列を入力します。 |
| diagSubnetworkName | 文字列 | 診断インターフェイスに使用される VPC サブネットの名前。<br>例：cisco-ftdv-diag-subnet<br>診断インターフェイスを使用せずに Threat Defense Virtual を展開する場合は、このパラメータを空白のままにするか、ダミーの文字列を入力します。 |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| diagVpcName | 文字列 | 診断インターフェイスに使用される VPC の名前。<br>例：custom-ftdv-diag-vpc<br>診断インターフェイスを使用せずに Threat Defense Virtual を展開する場合は、このパラメータを空白のままにするか、ダミーの文字列を入力します。 |
| elbFePorts | 整数 | ELB ファストイーサネットポート。<br>例：80,22 |
| elbIpProtocol | 文字列 | 使用される ELB IP プロトコル。<br>例：TCP |
| elbPort | 整数 | ELB ポート番号。<br>例： 80 |
| elbPortName | 文字列 | ELB ポートの名前。<br>例：tcp |
| elbPortRange | 整数 | ELB ポートの範囲。<br>例：80-80 |
| elbProtocol | 文字列 | 使用される ELB プロトコル。<br>例：TCP |
| elbProtocolName | 文字列 | ELB プロトコルの名前。<br>例：TCP |
| elbTimeoutSec | 整数 | 秒単位の ELB タイムアウト時間。<br>例：5 |
| elbUnhealthyThreshold | 整数 | ヘルスチェック不合格回数のしきい値。<br>例：2。 |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| fmcIP | 文字列 | Management Center の IP アドレス<br>例：10.61.1.2 |
| fmcPasswordSecret と新しい FtdPasswordSecret | 文字列 | 作成されたシークレットの名前。 |
| fmcUsername | 文字列 | Management Center Virtual のユーザー名 |
| ftdvCheckIntervalSec | 整数 | ヘルスチェックの間隔。<br>例：300 |
| ftdvHealthCheckPort | 整数 | Threat Defense Virtual のヘルスチェックのポート番号。<br>例：22 |
| ftdvHealthCheckProtocolName | 文字列 | ヘルスチェックに使用されるプロトコル。<br>例：TCP |
| ftdvPassword | 文字列 | Threat Defense Virtual のパスワード。 |
| ftdvTimeoutSec | 整数 | Threat Defense Virtual 接続のタイムアウト<br>例：300 |
| ftdvUnhealthyThreshold | 整数 | ヘルスチェック不合格回数のしきい値。<br>例：3 |
| grpID | 文字列 | Management Center で作成されたデバイスグループの名前。<br>例：auto-group |
| healthCheckFirewallRule | 文字列 | ヘルスチェックプローブの IP 範囲からのパケットを許可するファイアウォールルールの名前。<br>例：custom-ftdv-hc-firewall-rule |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| healthCheckFirewallRuleName | 文字列 | ヘルスチェックプローブの IP 範囲からのパケットを許可するファイアウォールルールのタグ。<br>例：demo-test-health-allow-all |
| ilbCheckIntervalSec | 整数 | ILB接続をチェックする間隔。<br>例：10 |
| ilbDrainingTimeoutSec | 整数 | 接続ドレインのタイムアウト時間<br>例：60 |
| ilbPort | 整数 | ILB ポート番号。<br>例： 80 |
| ilbProtocol | 文字列 | 使用される ILB プロトコル。<br>例：TCP |
| ilbProtocolName | 文字列 | ILB プロトコル名。<br>例：TCP |
| ilbTimeoutSec | 整数 | ILB タイムアウト時間。<br>例：5 |
| ilbUnhealthyThreshold | 整数 | ヘルスチェック不合格回数のしきい値。<br>例：3 |
| insideFirewallRule | 文字列 | 内部ファイアウォールルールの名前。<br>例：custom-ftdv-in-firewall-rule |
| insideFirewallRuleName | 文字列 | 内部 VPC での通信を許可するファイアウォールルールのタグ。<br>例：demo-test-inside-allowall |
| insideGwName | 文字列 | 内部ゲートウェイの名前。<br>例：inside-gateway |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| insideSecZone | 文字列 | 内部セキュリティゾーンの名前。<br>例：inside-zone |
| insideSubnetworkName | 文字列 | 内部サブネットの名前。<br>例：custom-ftdv-inside-subnet |
| insideVPCName | 文字列 | 内部 VPC の名前。<br>例：demo-test-inside |
| insideVPCSubnet | 文字列 | 内部サブネットの名前。<br>例：demo-test-inside-subnet |
| licenseCAPS | 文字列 | 使用するライセンスの名前<br>例：BASE、MALWARE、URL Filter、THREAT |
| machineType | 文字列 | Threat Defense Virtual VM のマシンタイプ。<br>例：n1-standard-4 |
| maxFTDCount | 整数 | インスタンスグループで許可される Threat Defense Virtual インスタンスの最大数。<br>例：3 |
| maxFTDReplicas | 整数 | 自動スケーリンググループ内の Threat Defense Virtual インスタンスの最大数。<br>例：2。 |
| mgmtFirewallRule | 文字列 | 管理ファイアウォールルールの名前。<br>例：cisco-ftdv-mgmt-firewall-rule |
| mgmtFirewallRuleName | 文字列 | 管理 VPC での通信を許可するファイアウォールルールのタグ。<br>例：demo-test-mgmt-allowall |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| mgmtSubnetworkName | 文字列 | 管理サブネットの名前。<br>例：custom-ftdv-mgmt-subnet |
| mgmtVPCName | 文字列 | 管理 VPC の名前。<br>例：demo-test-mgmt |
| mgmtVPCSubnet | 文字列 | 管理サブネットの名前。<br>例：demo-test-mgmt-subnt |
| minFTDCount | 整数 | 任意の時点でインスタンスグループで使用可能な Threat Defense Virtual の最小インスタンス数。<br>例 1 |
| minFTDReplicas | 整数 | 自動スケーリンググループ内の Threat Defense Virtual インスタンスの最小数。<br>例：2。 |
| natID | 文字列 | 脅威に対する防御 で Management Center を登録するときに必要な一意の NAT ID。 |
| outsideFirewallRule | 文字列 | 外部ファイアウォールルールの名前。<br>例：cisco-ftdv-out-firewall-rule |
| outsideFirewallRuleName | 文字列 | 外部 VPC での通信を許可するファイアウォールルールのタグ。<br>例：demo-test-outside-allowall |
| outsideGwName | 文字列 | 外部ゲートウェイの名前。<br>例：outside-gateway |
| outsideSecZone | 文字列 | 外部セキュリティゾーンの名前。<br>例：outside-zone |
| outsideSubnetworkName | 文字列 | 外部サブネットの名前。<br>例：custom-ftdv-outside-subnet |

| パラメータ名 | 使用できる値/タイプ | 説明 |
|---|---|---|
| outsideVPCName | 文字列 | 外部 VPC の名前。<br>例：demo-test-outside |
| outsideVPCSubnet | 文字列 | 外部サブネットの名前。<br>例：demo-test-outside-subnt |
| policyID | 文字列 | ACL ポリシーの名前。 |
| publicKey | 文字列 | Threat Defense Virtual VM の SSH キー。 |
| sourceImageURL | 文字列 | プロジェクトで使用する Threat Defense Virtual イメージの URL。 |
| sshUsingExternalIP | ブール値 | Google 機能によってパブリック IP アドレスとプライベート IP アドレスのどちらが使用されるかを決定します。<br>例：true<br>true に設定されている場合、Google 機能はパブリック IP アドレスを使用します。false に設定されている場合、Google 機能はプライベート IP アドレスを使用します。 |
| withDiagnostic | ブール | Threat Defense Virtual を診断インターフェイスを使用して展開するか、診断インターフェイスを使用せずに展開するかを決定します。<br>例：true<br>true に設定すると、Threat Defense Virtual は診断インターフェイスを使用して展開されます。false に設定すると、Threat Defense Virtual は診断インターフェイスを使用せずに展開されます。 |

# Auto Scale ソリューションの展開

**ステップ 1** Git リポジトリをローカルフォルダに複製します。

```
git clone git_url -b branch_name
```

**ステップ 2** gcloud CLI でバケットを作成します。

```
gsutil mb -c nearline gs://bucket_name
```

（注） システムにインストールされている Google Cloud Shell または Google Cloud SDK で、この手順の任意の **gsutil** または **gcloud** コマンドを実行します。

**ステップ 3** Zip 形式の圧縮パッケージを作成します。

a) `ftdv_scaleout` および `ftdv_scalein` フォルダから、以下のファイルで構成される Zip 形式の圧縮パッケージを作成します。

- main.py
- basic_functions.py
- fmc_functions.py
- requirements.txt

（注） 内部 IP アドレスを使用する場合は、main.py ファイルで **ssh_ip = response[‘networkInterfaces’] [2] [‘networkIP’]** コマンドを使用します。外部 IP アドレスを使用する場合は、**ssh_ip = response[‘networkInterfaces’] [2] [‘accessConfigs’] [0] [‘natIP’]** コマンドを入力します。また、この関数では2つの静的ルートが追加されます。静的ルートを変更するには、**fmc.create_static_network_route (vm_name, ‘outside’, ‘any_ipv4’, os.getenv(“OUTSIDE_GW_NAME”), metric=1)** および **fmc.create_static_network_route (vm_name, ‘inside’, ‘any_ipv4’, os.getenv(“INSIDE_GW_NAME”), metric=2)** コマンドを使用します。

b) Zip 形式の圧縮パッケージの名前を `ftdv_scaleout.zip` および `ftdv_scalein.zip` に変更します。

（注） フォルダ内を移動して選択するファイルを右クリックし、[圧縮|アーカイブ（compress | archive）] を選択すると、GCP が読み取れる .zip が作成されます。

**ステップ 4** Zip 形式の圧縮パッケージ（`ftdv_scaleout.zip` および `ftdv_scalein.zip`）をクラウドエディタのワークスペースにアップロードします。

**ステップ 5** 以下のファイルを Deployment Manager のテンプレートからクラウドエディタのワークスペースにアップロードします。

- ftdv_predeployment.yaml
- ftdv_predeployment.jinja

- ftdv_parameters.yaml
- ftdv_template.jinja

**ステップ 6** Zip 形式の圧縮パッケージをバケットストレージにコピーします。

- `gsutil cp ftdv_scaleout.zip gs://bucket_name`
- `gsutil cp ftdv_scalein.zip gs://bucket_name`

**ステップ 7** 内部、外部、管理、診断インターフェイス用の VPC とサブネットを作成します。

管理 VPC では、/28 サブネット（例：10.8.2.0/28）が必要です。

**ステップ 8** 内部、外部、管理、診断インターフェイス用に 4 つのファイアウォールルールが必要です。また、正常性チェックプローブを許可するファイアウォールルールが必要です。

**ステップ 9** Secret Manager GUI を使用して、次の 2 つのシークレットを作成します。https://console.cloud.google.com/security/secret-manager を参照してください。

- fmc-password
- ftdv-new-password

**ステップ 10** VPC コネクタを作成します。

```
gcloud beta compute networks vpc-access connectors create <vpc-connector-name>
--region <region> --subnet=</28 subnet name>
```

**例**：

```
gcloud beta compute networks vpc-access connectors create demo-vpc-connector
--region us-central1 --subnet=outside-connect-28
Create request issued for: [demo-vpc-connector]
Waiting for operation [projects/asavgcp-poc-4krn/locations/us-central1/operations/
10595de7-837f-4c19-9396-0c22943ecf15] to complete...done.
Created connector [demo-vpc-connector].
```

**ステップ 11** パブリック IP を持つ任意のパブリック クラウド プラットフォームに Management Center Virtual を展開します。各種パブリック クラウド プラットフォームに Management Center Virtual を展開する方法の詳細については、『Cisco Firepower Management Center Virtual Getting Started Guide』を参照してください。

（注） Management Center Virtual を展開したインスタンスでステップ 12 から 16 を実行します。

**ステップ 12** Management Center Virtual インスタンス：fmcpassword シークレットに保存されているものと同じパスワードを使用して、Management Center Virtual でユーザー restapi を作成します。詳細については、「ユーザー」を参照してください。

**ステップ 13** Management Center Virtual インスタンス：デバイスグループ、アクセス コントロール ポリシー、およびアクセス制御ルールを作成します。詳細については、「デバイスグループの追加」、「基本的なアクセス コントロール ポリシーの作成」、および「アクセスコントロールルールの作成および編集」を参照してください。

**ステップ 14** Management Center Virtual インスタンス：以下のオブジェクトを作成します。Management Center Virtual でオブジェクトを作成する方法の詳細については、「オブジェクト管理」を参照してください。

- ELB-IP

- ILB-IP
- Application-IP
- ヘルスチェックの IP 範囲（4）
- メタデータ（Metadata）

```
object network hc1
  subnet 35.191.0.0 255.255.0.0
object network metadata
  host 169.254.169.254
object network ilb-ip
  host 10.52.1.218
object network hc2
  subnet 130.211.0.0 255.255.252.0
object network elb-ip
  host 34.85.214.40
object network hc3
  subnet 209.85.152.0 255.255.252.0
object network hc4
  subnet 209.85.204.0 255.255.252.0
object network inside-linux
  host 10.52.1.217
object network outside-gateway
  host <>
object network inside-gateway
  host <>
```

**ステップ 15** Management Center Virtual インスタンス：セキュリティゾーン（インターフェイスオブジェクト）を作成します。「Creating Security Zone and Interface Group Objects」を参照してください。

- inside-security-zone
- outside-security-zone

**ステップ 16** Management Center Virtual インスタンス：NAT ポリシーと NAT ルールを作成します。詳細については、「Network Address Translation」を参照してください。

```
nat (inside,outside) source dynamic hc1 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic hc2 interface destination static ilb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (inside,outside) source dynamic any interface
nat (outside,inside) source dynamic hc1 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc2 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc3 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic hc4 interface destination static elb-ip metadata service
SVC_4294968559 SVC_4294968559
nat (outside,inside) source dynamic any interface destination static elb-ip inside-linux
```

| | # | Direction | Type | Source Interface Objects | Destination Interface Objects | Original Sources | Original Destinations | Original Services | Translated Sources | Translated Destinations | Translated Services | Options |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | | D... | inside-zone | outside-zone | hc1 | ilb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 2 | | D... | inside-zone | outside-zone | hc2 | ilb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 3 | | D... | inside-zone | outside-zone | any-ipv4 | | | Interface | | | Dns:false |
| | 4 | | D... | outside-zone | inside-zone | hc1 | elb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 5 | | D... | outside-zone | inside-zone | hc2 | elb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 6 | | D... | outside-zone | inside-zone | hc3 | elb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 7 | | D... | outside-zone | inside-zone | hc4 | elb-ip | Original HTTP | Interface | metadata | Original HTTP | Dns:false |
| | 8 | | D... | outside-zone | inside-zone | any-ipv4 | elb-ip | | Interface | inside-linux | | Dns:false |

**ステップ 17** 導入前および Threat Defense Virtual Auto Scale 導入用の Jinja ファイルと YAML ファイルのパラメータを更新します。

a) `ftdv_predeployment.yaml` ファイルを開き、次のパラメータを更新します。

- **resourceNamePrefix**: <resourceNamePrefix>
- **region**: <region>
- **serviceAccountMailId**: <serviceAccountMailId>
- **vpcConnectorName**: <VPC-Connector-Name>
- **bucketName**: <bucketName>
- **fmcIP**：<Management Center-IP-address>
- **regID**：<registration-ID>
- **natID**：<unique-NAT-ID>
- **grpID**：<device-group-name>
- **policyID**：<acl-policy-name>
- **licenseCAPS**：<licenses>
- **fmcPasswordSecret**：<Management Center-password>
- **newFtdPasswordSecret**：<new-Threat Defense Virtual-password>
- **fmcUsername**：<username>
- **ftdvPassword**：<password>
- **outsideGwName**：<outside-gateway-name>
- **insideGwName**：<inside-gateway-name>
- **outsideSecZone**：<outside-security-zone>
- **insideSecZone**：<inside-security-zone>
- **sshUsingExternalIP**：<true/false>

b) `ftdv_predeployment.jinja` ファイルは、`ftdv_predeployment.yaml` ファイルからパラメータを受け取ります。

c) `ftdv_parameters.yaml` ファイルを開き、以下のパラメータを更新します。

**VPC and Firewall Parameters**

- **mgmtVpcName**：<mgmt-vpc-name>
- **diagVpcName**：<diagnostic-vpc-name>
- **outsideVpcName**：<outside-vpc-name>
- **insideVpcName**：<inside-vpc-name>
- **mgmtSubnetworkName**：<mgmt-subnet-name>
- **diagSubnetworkName**：<diagnostic-subnet-name>
- **outsideSubnetworkName**：<outside-subnet-name>
- **insideSubnetworkName**：<inside-subnet-name>
- **mgmtFirewallRule**：<mgmt-firewall-rule>
- **diagFirewallRule**：<diagnostic-firewall-rule>
- **outsideFirewallRule**：<outside-firewall-rule>
- **insideFirewallRule**：<inside-firewall-rule>
- **healthCheckFirewallRule**：<healthcheck-firewall-rule>
- **adminPassword**：<initial-Threat Defense Virtual-password>
- **deployUsingExternalIP**：<true/false>

**Instance Template parameters**

- **machineType**：<machine-type>
- **sourceImageURL**：<source-image-URL>

**FTDv Health Check**

- **ftdvHealthCheckPort**：<port-number>
- **ftdvCheckIntervalSec**：<interval-in-seconds>
- **ftdvTimeoutSec**：<timeout-in-seconds>
- **ftdvHealthCheckProtocolName**：<protocol-name>
- **ftdvUnhealthyThreshold**：<threshold-count>

**FTDv Autoscaler**

- **cpuUtilizationTarget**：<percentage-in-decimals（例：0.7）>

- **coolDownPeriodSec**：<cooldown-period-in-seconds>
- **minFTDReplicas**：<min-number-of-FTDv-instances>
- **maxFTDReplicas**：<max-number-of-FTDv-instances>

**ELB Services**

- **elbPort**：<port-number>
- **elbPortName**：<port-name>
- **elbProtocol**：<protocol-name>
- **elbTimeoutSec**：<timeout-in-seconds>
- **elbProtocolName**：<protocol-name>
- **elbUnhealthyThreshold**：<threshold-number-for-failed-health-checks>
- **elbIpProtocol**：<IP-Protocol>
- **elbPortRange**：<port-range>
- **elbFePorts**：<fast-ethernet-ports>

**ILB Services**

- **ilbProtocol**: <protocol-name>
- **ilbDrainingTimeoutSec**: <timeout-in-seconds>
- **ilbPort**: <port-number>
- **ilbCheckIntervalSec**: <interval-in seconds>
- **ilbTimeoutSec**：<timeout-in-seconds>
- **ilbProtocolName**：<protocol-name>
- **ilbUnhealthyThreshold**：<threshold-number-for-failed-health-checks>

（注） Threat Defense Virtual Auto Scale の場合、**cpuUtilizationTarget: 0.5** パラメータが設定されており、必要に応じて編集できます。この値は、すべての Threat Defense Virtual インスタンスグループの CPU 使用率が 50% であることを示します。

d) `ftdv_template.jinja` ファイルは、`ftdv_parameters.yaml` ファイルからパラメータを受け取ります。

**ステップ 18** 導入前の YAML 構成を展開します。

```
gcloud deployment-manager deployments create <pre-deployment-name>
--config ftdv_predeployment.yaml
```

**例**：

```
gcloud deployment-manager deployments create demo-predeployment
--config ftdv_predeployment.yaml
```

```
The fingerprint of the deployment is b'9NOy0gsTPgg16SqUEVsBjA=='
Waiting for create [operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c]...done.
Create operation operation-1624383045917-5c55e266e596d-4979c5b6-66d1025c
completed successfully
```

**ステップ 19** Threat Defense Virtual Auto Scale の展開を作成します。

```
gcloud deployment-manager deployments create <deployment-name>
--config ftdv_parameters.yaml
```

**例**：

```
gcloud deployment-manager deployments create demo-asav-autoscale
--config ftdv_parameters.yaml
The fingerprint of the deployment is b'1JCQi7Il-laWOY7vOLza0g=='
Waiting for create [operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16]...done.
Create operation operation-1624383774235-5c55e51d79d01-1a3acf92-4f3daf16
completed successfully.
```

**ステップ 20** 内部アプリケーションからインターネットにパケットを転送する ILB のルートを作成します。

```
gcloud beta compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

**例**：

```
gcloud beta compute routes create demo-ilb --network=sdt-test-asav-inside
--priority=1000 --destination-range=0.0.0.0/0 --next-hop-ilb=demo-asav-fr-ilb
--next-hop-ilb-region=us-central1
Created [https://www.googleapis.com/compute/beta/projects/asavgcp-poc-4krn/global
/routes/demo-ilb].
```

# Auto Scale ロジック

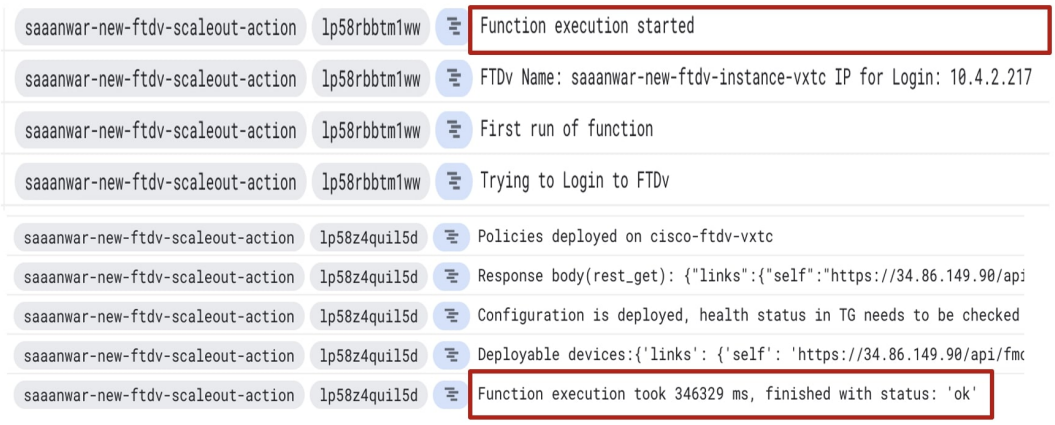
- オートスケーラは、ターゲット CPU 使用率レベルを、インスタンスグループ内の一定期間にわたるすべての vCPU の平均使用量の一部として扱います。
- 合計 vCPU の平均使用率がターゲット使用率を超えると、オートスケーラによって VM インスタンスが追加されます。合計 vCPU の平均使用率がターゲット使用率よりも低い場合、オートスケーラはインスタンスを削除します。
- たとえば、0.75 のターゲット使用率を設定すると、オートスケーラはインスタンスグループ内のすべての vCPU の平均使用率を 75% に維持するように指示されます。
- スケーリングの決定では、CPU 使用率メトリックのみが使用されます。
- このロジックは、ロードバランサがすべての Threat Defense Virtual に接続を均等に分散しようとし、平均してすべての Threat Defense Virtual が均等にロードされるという前提に基づいています。

# ロギングとデバッグ

表示できるクラウド機能のログは以下のとおりです。

- スケールアウト機能のログ

**図 *50* : スケールアウト機能のログ**




上記のスケールアウト機能のログでは、**Function execution started** と **Function execution took 346329 ms, finish with status: 'ok'** のエントリは、機能ログの開始と終了をそれぞれ示しています。初回の機能実行、Threat Defense Virtual へのログイン、ポリシーの展開など、他の操作を追跡することもできます。

- スケールイン機能のログ


上記のスケールアウト機能のログでは、**Function execution started** と **Function execution took 50852 ms, finish with status: 'ok'** のエントリは、機能ログの開始と終了をそれぞれ示しています。登録解除プロセスの開始、登録解除のステータス、新しい認証トークンの取得など、他の操作を追跡することもできます。

# トラブルシューティング

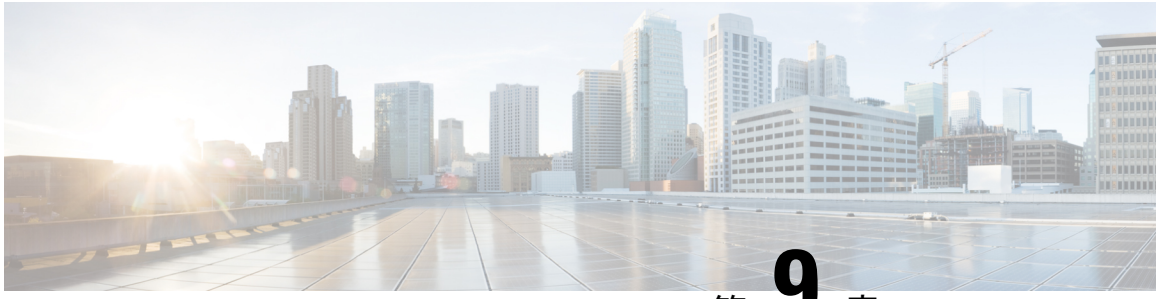
次に、Threat Defense Virtual Auto Scale for GCP の一般的なエラーシナリオとデバッグのヒントを示します。

- `main.py` が見つからない：Zip パッケージがファイルのみから作成されていることを確認します。クラウド機能に移動してファイルツリーを確認できます。フォルダがあってはいけません。
- テンプレートの展開中のエラー：「<>」内のすべてのパラメータ値が Jinja と YAML で入力されていることを確認します。または、同じ展開名が既に存在するかどうかを確認します。
- Google 関数が Threat Defense Virtual に到達できない：VPC コネクタが作成されており、YAML パラメータファイルで同じ名前が指定されていることを確認します。
- Threat Defense Virtual に SSH 接続中に認証に失敗：公開キーと秘密キーのペアが正しいことを確認します。
- 認証トークンが見つからない：シークレットの Management Center Virtual パスワードが正しいことを確認します。
- Threat Defense Virtual の異常とトラフィックの問題：ファイアウォールルールとルートに問題がないことを確認します。
- 手動で Threat Defense Virtual にログインできない：新しいパスワードを使用しているかを確認します。スケールアウト機能により旧パスワードは変更されます。
- Management Center Virtual にデバイスを登録できない：Threat Defense Virtual が Management Center Virtual から到達可能であるかを確認します。Threat Defense Virtual と Management Center Virtual の管理インターフェイスが同じサブネット内に存在する必要があります。
- 保持された接続により ILB と Threat Defense Virtual 間のループが形成されるため、正常性プローブ要求が開始されると CPU 使用率が高くなります。高い CPU 使用率を下げるには、次のいずれかのオプションを使用できます。

  オプション 1：Management Center Virtual でデータインターフェイスを無効にし、正常性プローブの NAT ルールを設定して、データインターフェイスを有効にします。データインターフェイスと NAT の詳細については、「インターフェイスの概要」と「ネットワークアドレス変換」を参照してください。

  オプション 2：正常性プローブの NAT ルールを Management Center Virtual から適用した後、Threat Defense Virtual のコンソールにログインし、**clear conn** コマンドを使用します。クラスタリングを設定している場合は、**cluster exec clear conn** コマンドを使用します。

  Threat Defense Virtual のコンソールで **show cpu** コマンドを使用して、CPU 使用率を確認します。



第 9 章

# Cisco HyperFlex への Threat Defense Virtual の展開

この章では、vCenter サーバーまたはスタンドアロン ESXi ホストの Cisco HyperFlex に Threat Defense Virtual を展開する際の手順について説明します。


- 概要 （391 ページ）
- エンドツーエンドの手順 （392 ページ）
- システム要件 （393 ページ）
- 注意事項と制約事項 （395 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （399 ページ）
- 概要 （400 ページ）
- Threat Defense Virtual の導入 （401 ページ）
- CLI を使用した Threat Defense Virtual のセットアップの実行 （405 ページ）
- ジャンボ フレームの有効化 （406 ページ）
- トラブルシューティング （407 ページ）


## 概要

Cisco Secure Firewall Threat Defense Virtual（旧称 Firepower Threat Defense Virtual）は、Cisco Secure Firewall 機能を仮想化環境にもたらします。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

HyperFlex システムは、あらゆる場所であらゆるアプリケーションにハイパーコンバージェンスを提供します。Cisco Unified Computing System（Cisco UCS）テクノロジーを備える HyperFlex は、Cisco Intersight クラウド運用プラットフォームを通じて管理され、場所を問わずアプリケーションとデータを強力にサポートし、コアデータセンターからエッジ、そしてパブリッククラウドまでの運用を最適化し、DevOps 手法を推進して俊敏性を高めることができます。

この章では、Cisco HyperFlex 環境内における Threat Defense Virtual の機能について説明します。機能のサポート、システム要件、ガイドライン、制限事項などを取り上げます。また、この章では Threat Defense Virtual を管理するためのオプションについても説明します。導入を開始す

る前に、管理オプションを理解しておくことが重要です。Secure Firewall Management Center（旧称 Firepower Management Center）または Secure Firewall Device Manager （旧称 Firepower Device Manager）を使用して Threat Defense Virtual を管理および監視できます。その他の管理オプションを使用できる場合もあります。

# エンドツーエンドの手順

次のフローチャートは、Cisco HyperFlex に Threat Defense Virtual を展開する際のワークフローを示しています。


| | ワークスペース | 手順 |
|---|---|---|
| 1 | HyperFlex | Threat Defense Virtual の導入：Cisco.com から Threat Defense Virtual の VI OVF テンプレートファイルをダウンロードします。 |
| 2 | HyperFlex | Threat Defense Virtual の導入：OVF テンプレート情報を確認します。 |
| 3 | HyperFlex | Threat Defense Virtual の導入：展開設定をカスタマイズします。 |
| 4 | HyperFlex | Threat Defense Virtual の導入：表示される情報に目を通して確認します。[終了（Finish）]をクリックして、OVF テンプレートの展開を開始します。 |
| 5 | Management Center または Device Manager | Threat Defense Virtual の管理：<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

# システム要件

## バージョン

| マネージャバージョン | デバイスバージョン |
|---|---|
| Device Manager 7.0 | Threat Defense 7.0 |
| Management Center 7.0 | |

Threat Defense Virtual のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

### Threat Defense Virtual メモリ、ディスクのサイジング、および vCPU

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入するインスタンス数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

| 設定 | 値 |
|---|---|
| パフォーマンス階層 | **バージョン 7.0 以降**<br>Threat Defense Virtual 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。<br>• FTDv5 4vCPU/8GB（100 Mbps）<br>• FTDv10 4vCPU/8GB（1 Gbps）<br>• FTDv20 4vCPU/8GB（3 Gbps）<br>• FTDv30 8vCPU/16GB（5 Gbps）<br>• FTDv50 12vCPU/24GB（10 Gbps）<br>• FTDv100 16vCPU/32GB（16 Gbps）<br>Threat Defense Virtual 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* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。<br>（注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。 |

| 設定 | 値 |
|---|---|
| ストレージ | ディスク形式の選択に基づきます。<br>• シンプロビジョニングのディスクサイズは 48.24 GB です。 |
| vNIC | Threat Defense Virtual は次の仮想ネットワークアダプタをサポートしています。<br>• **VMXNET3**：VMware 上の Threat Defense Virtual では、仮想デバイスを作成するときに、デフォルトが VMXNET3 インターフェイスになりました。以前は、デフォルトは e1000 でした。（7.1 以降）vmxnet3 ドライバは、最初のイーサネットアダプタを管理に使用します。2番目のアダプタは未使用です。（7.0 以前）<br>VMXNET3 ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つのイーサネット アダプタは、管理インターフェイスとして設定する必要があります。1つはデバイス管理/登録用で、もう 1 つは診断用です。 |

### Threat Defense Virtual ライセンス

- Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
- ライセンスの管理方法の詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Firepower* システムのライセンス」を参照してください。

### HyperFlex HX シリーズの設定とクラスタ

| 設定 | クラスタ |
|---|---|
| HX220c コンバージドノード | • フラッシュクラスタ<br>• 最小 3 ノードクラスタ（データベース、VDI、VSI） |
| HX240c コンバージドノード | • フラッシュクラスタ<br>• 最小 3 ノードクラスタ（VSI：T/Biz アプリケーション、テスト/開発） |
| HX220C とエッジ（VDI、VSI、ROBO）<br>HX240C（VDI、VSI、テスト/開発） | • ハイブリッドクラスタ<br>• 最小 3 ノードクラスタ |
| B200 + C240/C220 | コンピューティング バウンド アプリ/VDI |

HyperFlex HX シリーズの導入オプション：

- ハイブリッドクラスタ
- フラッシュクラスタ
- HyperFlex HX エッジ
- SED ドライブ
- NVME キャッシュ
- GPU

HyperFlex HX クラウドを利用した管理オプションについては、『Cisco HyperFlex システム設置ガイド』の「*HyperFlex* ファブリック インターコネクトに接続されたクラスタの展開」のセクションを参照してください。

### HyperFlex コンポーネントとバージョン

| コンポーネント | バージョン |
|---|---|
| VMware vSphere/VMware ESXI | 7.0<br>Threat Defense Virtual と VMware vSphere/VMware ESXI との互換性の詳細については、「Threat Defense Virtual の互換性：VMware」を参照してください。 |
| HyperFlex Data Platform | 4.5.1a-39020 以降<br>. |

# 注意事項と制約事項

### サポートされる機能

- 展開モード：ルーテッド（スタンドアロン）、ルーテッド（HA）、インラインタップ、インライン、パッシブ、およびトランスペアレント
- ライセンス：BYOL のみ
- IPv6
- Threat Defense Virtual ネイティブ HA
- ジャンボフレーム
- HyperFlex データセンタークラスタ（ストレッチ クラスタを除く）
- HyperFlex Edge クラスタ

- HyperFlex すべての NVMe、オールフラッシュ、およびハイブリッド コンバージド ノード
- HyperFlex コンピューティング専用ノード

### サポートされない機能

SR-IOV を使用した Threat Defense Virtualの実行は、HyperFlex で認定されていません。

（注） HyperFlex は SR-IOV をサポートしていますが、MLOM VIC に加えて PCI-e NIC も必要です。

### 一般的なガイドライン

HyperFlex の vSwitch を設定するには、GUI またはコマンド ライン インターフェイスを使用します。vSwitch を設定すると、複数の ESX サーバーをインストールして、vSwitch 設定のスクリプトを構築する際に便利です。詳細については、『Cisco HyperFlex Systems Network and External Storage Management Guide』の「Configure the vSwitches」の項を参照してください。

Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークに関する用語索引を以下に記載します。

| ネットワーク アダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Management0/0 | 管理 |
| Network adapter 2 | Diagnostic 0-0 | 診断 | 診断 |
| ネットワークアダプタ 3 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部 |
| ネットワークアダプタ 4 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部 |
| ネットワークアダプタ 5 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet 0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ～ネットワーク アダプタ 10 | | | |

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「HyperFlex での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラ

フィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

### vSphere 標準スイッチのセキュリティポリシー設定の変更

vSphere 標準スイッチの場合、レイヤ 2 セキュリティポリシーには、無差別モード、MAC アドレスの変更、不正送信という 3 つの要素があります。Threat Defense Virtual は無差別モードを使用して稼働します。また、Threat Defense Virtual の高可用性が正常に機能するかは、アクティブとスタンバイ間での MAC アドレスの切り替えにかかっています。

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。以下の必須の設定を参照してください。

**表 *30 : vSphere* 標準スイッチのセキュリティ ポリシー オプション**

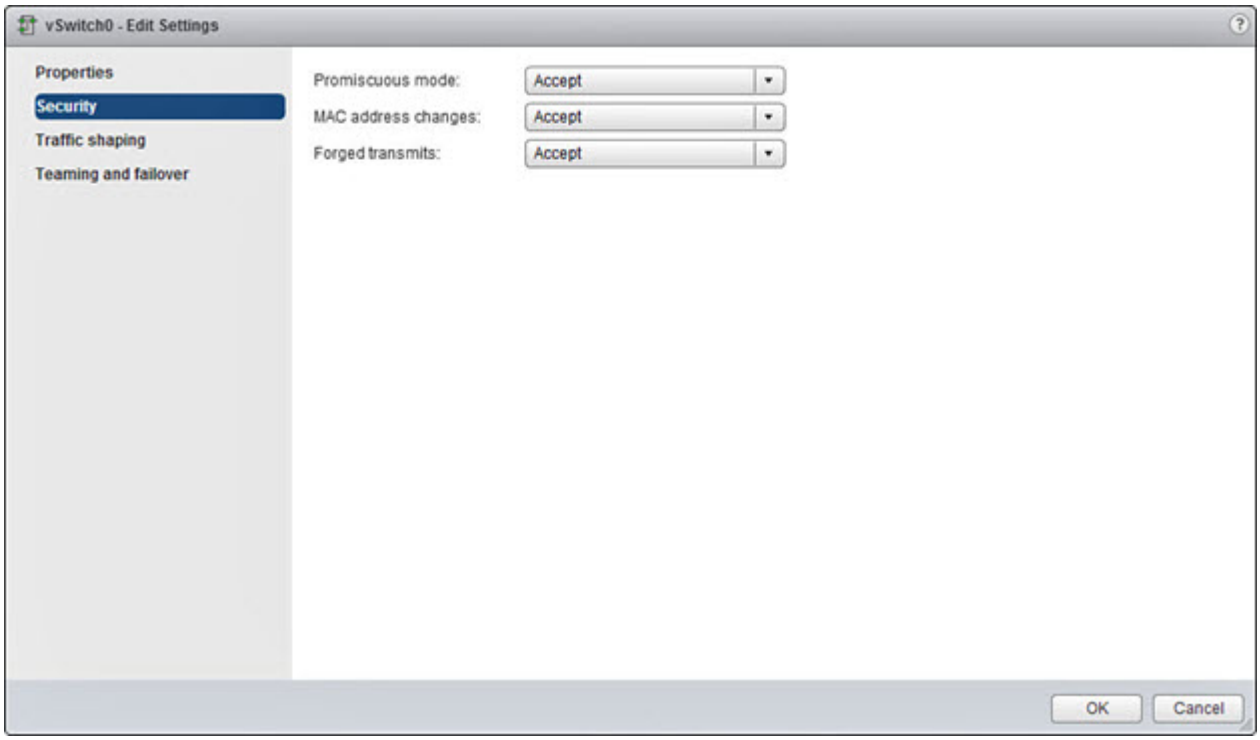
| オプション | 必須の設定 | アクション |
|---|---|---|
| 無差別モード（Promiscuous Mode） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを編集し、[無差別モード（Promiscuous mode）] オプションを [承認（Accept）] に設定する必要があります。<br>ファイアウォール、ポートスキャナ、侵入検知システムなどは無差別モードで実行する必要があります。 |

| オプション | 必須の設定 | アクション |
|---|---|---|
| MAC アドレスの変更（MAC Address Changes） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[MAC アドレスの変更（MAC address changes）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。 |
| 不正送信（Forged Transmits） | 承認（Accept） | vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[不正転送（Forged transmits）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。 |

Threat Defense Virtual を正しく動作させるためのデフォルト設定にするには、次の手順を実行します。

1. vSphere Web クライアントで HyperFlex クラスタに移動します。
2. [管理（Manage）] タブで、[ネットワーク（Networking）] をクリックし、[仮想スイッチ（Virtual switches）] を選択します。
3. リストから標準スイッチを選択し、[設定の編集（Edit settings）] をクリックします。
4. [セキュリティ（Security）] を選択し、現在の設定を表示します。
5. 標準スイッチに接続された仮想マシンのゲスト オペレーティング システムで無差別モードの有効化、MAC アドレスの変更、および不正送信の [承認（Accept）] を選択します。

図 *51 : vSwitch* の編集設定




6. [OK] をクリックします。

（注） これらの設定が、Threat Defense Virtual デバイスの管理インターフェイスおよびフェールオーバー（HA）インターフェイスに設定されているすべてのネットワーク上で同じであることを確認します。

### 関連資料

『Release Notes for Cisco HX Data Platform』

Configuration Guides for Cisco HX Data Platform

Cisco HyperFlex 4.0 for Virtual Server Infrastructure with VMware ESXi

Cisco HyperFlex Systems Solutions Overview

Cisco HyperFlex Systems ドキュメンテーション ロードマップ

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

# 概要

VMware vCenter サーバー上の Cisco HyperFlex に Threat Defense Virtual を展開できます。

Threat Defense Virtual を正常に展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

Cisco HyperFlex 向けの Threat Defense Virtual はオープン仮想化フォーマット（OVF）を使用して配布されます。OVF は、仮想マシンをパッケージ化して展開する標準的な方法です。VMware

では、vSphere 仮想マシンをプロビジョニングするための方法がいくつか用意されています。お使いの環境に最適な方法は、インフラストラクチャの規模やタイプ、達成目標などの要因によって異なります。

VMware vSphere Web クライアントを使用して、Cisco HyperFlex 環境にアクセスできます。

# Threat Defense Virtual の導入

以下の手順を使用して、vSphere vCenter Server 上の Cisco Hyperflex に Threat Defense Virtual アプライアンスを展開します。

### 始める前に

- Cisco HyperFlex を展開してインストール後の構成タスクをすべて実行済みであることを確認します。詳細については、『Cisco HyperFlex Systems Documentation Roadmap』を参照してください。
- Threat Defense Virtual を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。
- Cisco.com から Threat Defense Virtual VI OVF テンプレートファイル（*Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*）をダウンロードします。*X.X.X-xxx* はバージョンとビルド番号です。

---

**ステップ 1** vSphere Web クライアントにログインします。

**ステップ 2** Threat Defense Virtual を展開する HyperFlex クラスタを選択し、**[アクション（ACTIONS）]** > **[OVFテンプレートの展開（Deploy OVF Template）]** の順にクリックします。

**ステップ 3** ファイルシステムで OVF テンプレートソースの場所を参照し、[次へ（NEXT）] をクリックします。

次の Threat Defense Virtual VI OVF テンプレートを選択します。

*Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*

ここで、*X.X.X-xxx* は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

**ステップ 4** Threat Defense Virtual の名前と場所を指定し、[次へ（NEXT）] をクリックします。

**ステップ 5** コンピューティングリソースを選択し、互換性チェックが完了するまで待ちます。

互換性チェックが成功したら、[次へ（NEXT）] をクリックします。

**ステップ 6** OVFテンプレートの情報（製品名、バージョン、ベンダー、ダウンロードサイズ、ディスク上のサイズ、説明）を確認して、[次へ（NEXT）] をクリックします。

**ステップ 7** OVFテンプレート（VIテンプレートのみ）でパッケージ化されたライセンス契約書を確認して承認し、[次へ（NEXT）] をクリックします。

**ステップ 8** 展開の構成（vCPU/メモリ値）を選択し、[次へ（NEXT）] をクリックします。

**ステップ 9** ストレージの場所と仮想ディスク形式を選択し、[次へ（NEXT）] をクリックします。

このウィンドウで、宛先の HyperFlex クラスタですでに設定されているデータストアから選択します。仮想マシンの構成ファイルおよび仮想ディスクファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。

[シックプロビジョン（Thick Provisioned）] を仮想ディスク形式として選択すると、すべてのストレージがただちに割り当てられます。[シンプロビジョン（Thin Provisioned）] を仮想ディスク形式として選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

**ステップ 10** OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ（NEXT）] をクリックします。

Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Management Center または Device Manager から設定できます。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集（Edit Settings）] ダイアログボックスからネットワークを変更できます。展開後、Threat Defense Virtual インスタンスを右クリックして [設定の編集（Edit Settings）] を選択します。ただし、この画面には Threat Defense Virtual の ID は表示されません（ネットワークアダプタ ID のみ）。

以下に示す、Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を参照してください（これらは vmxnet3 デフォルトのインターフェイスです）。

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| Network adapter 1 | Management0-0 | Management0/0 | 管理 |
| Network adapter 2 | Diagnostic 0-0 | Diagnostic 0/0 | 診断 |
| ネットワークアダプタ 3 | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部データ |
| ネットワークアダプタ 4 | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部日付 |
| ネットワークアダプタ 5 | GigabitEthernet0-2 | GigabitEthernet 0/2 | データトラフィック（オプション） |
| ネットワークアダプタ 6 | GigabitEthernet 0-3 | GigabitEthernet 0/3 | データトラフィック（オプション） |
| ネットワークアダプタ 7 | GigabitEthernet 0-4 | GigabitEthernet 0/4 | データトラフィック（オプション） |
| ネットワークアダプタ 8 | GigabitEthernet 0-5 | GigabitEthernet 0/5 | データトラフィック（オプション） |
| ネットワークアダプタ 9 | GigabitEthernet 0-6 | GigabitEthernet 0/6 | データトラフィック（オプション） |

| ネットワークアダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| ネットワークアダプタ 10 | GigabitEthernet 0-7 | GigabitEthernet 0/7 | データトラフィック（オプション） |

Threat Defense Virtual を展開する際には、合計 10 個のインターフェイスを指定できます。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。すべての Threat Defense Virtual インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、Threat Defense Virtual の設定内でそのインターフェイスを無効のままにしておいて構いません。

**ステップ 11** OVF テンプレートでパッケージ化された、ユーザー設定可能なプロパティを設定します。

（注） このステップでは、必須のカスタマイズ項目をすべて設定することを推奨します。必要なすべてのカスタマイズ項目を設定しなかった場合は、展開後に CLI にログインして設定を完了する必要があります。この説明については、CLI を使用した Threat Defense Virtual のセットアップの実行 （405 ページ） を参照してください。

a) **パスワード**

Threat Defense Virtual 管理アクセス用のパスワードを設定します。

b) **ネットワーク**

完全修飾ドメイン名（FQDN）、DNS、検索ドメイン、ネットワークプロトコル（IPv4 または IPv6）などのネットワーク情報を設定します。

c) **管理**

管理モードを設定します。[ローカルマネージャを有効にする（Enable Local Manager） ] のドロップダウン矢印をクリックし、Web ベースの Device Manager 統合設定ツールを使用する場合は [はい（Yes）] を選択します。Management Center を使用してこのデバイスを管理するには、[いいえ（No）] を選択します。

d) **ファイアウォールモード**

初期ファイアウォールモードを設定します。[ファイアウォールモード（Firewall Mode）] のドロップダウン矢印をクリックし、サポートされている 2 つのモードである [ルーテッド（Routed）] または [トランスペアレント（Transparent）] のどちらかを選択します。

[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、[ルーテッド（Routed）] ファイアウォール モードのみを選択できます。ローカルの Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。

e) **登録**

[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、管理を行う Firepower Management Center にこのデバイスを登録するのに必要なクレデンシャルを指定する必要があります。次の情報を入力します。

- [管理を行うDefense Center（Managing Defense Center）]：Management Center のホスト名または IP アドレスを入力します。
- [登録キー（Registration Key）]：登録キーは、ユーザーが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。デバイスを Management Center に追加するときに、この登録キーが必要になります。
- [NAT ID]：Threat Defense Virtual と Management Center がネットワークアドレス変換（NAT）デバイスによって分離されていて、Management Center が NAT デバイスの背後にある場合は、一意の NAT ID を入力します。これは、ユーザーが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。

f) [次へ（NEXT）] をクリックします。

**ステップ 12** 表示された情報を確認して検証します。これらの設定を使用して展開を開始するには、[終了（FINISH）] をクリックします。変更を加えるには、[戻る（BACK）] をクリックして前の各画面に戻ります。

ウィザードが完了すると、vSphere Web Client によって仮想マシンが処理されます。[グローバル情報（Global Information）] 領域の [最近使用したタスク（Recent Tasks）] ペインで [OVF展開の初期設定（Initialize OVF deployment）] ステータスを確認できます。

この手順が終了すると、[OVFテンプレートの展開（Deploy OVF Template）] 完了ステータスが表示されます。

Threat Defense Virtual 仮想インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。新しい VM の起動には、最大 30 分かかることがあります。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、展開後に追加の構成が必要になります。

### 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）」を参照してください。

（注） Threat Defense Virtual の展開時に必要なすべてのカスタマイズ項目を設定しなかった場合は、CLI を使用して設定を完了する必要があります。この説明については、CLI を使用した Threat Defense Virtual のセットアップの実行 （405 ページ） を参照してください。

# CLI を使用した Threat Defense Virtual のセットアップの実行

Threat Defense Virtual の展開時に必要なすべてのカスタマイズ項目を設定しなかった場合は、CLI を使用して設定を完了する必要があります。

**ステップ 1** VMware コンソールを開きます。

**ステップ 2** [firepowerログイン（firepower login）] プロンプトで、ユーザー名 **admin** とパスワード **Admin123** のデフォルトのクレデンシャルでログインします。

**ステップ 3** Threat Defense システムが起動すると、セットアップ ウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理で Device Manager を使用）

**ステップ 4** セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

設定が実装されたときに、VMware コンソールにメッセージが表示される場合があります。

**ステップ 5** プロンプトに従ってシステム設定を行います。

**ステップ 6** コンソールが # プロンプトに戻るときに、設定が正常に行われたことを確認します。

（注） Cisco Licensing Authority に Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

### 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）」を参照してください。

# ジャンボ フレームの有効化

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASAv インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応：MTU を最大 9198 バイトに設定できます。ASAv の最大値は 9000 です。

この手順では、次の環境でジャンボフレームを有効にする方法について説明します。

**vSphere 7.0.1 上の HyperFlex クラスタ > VMware vSphere vSwitch> Cisco UCS ファブリック インターコネクト（FI）**

---

**ステップ 1** ASAv を展開した ASAv ホストの MTU 設定を変更します。

1. vSphere Web クライアントを使用して vCenter サーバーに接続します。
2. HyperFlex ホストの [詳細システム設定（Advanced System Settings）] で、[Net.Vmxnet3NonTsoPacketGtMtuAllowed] の設定パラメータの値を `1` にします。
3. 変更を保存してホストを再起動します。

詳細については、「https://kb.vmware.com/s/article/1038578」を参照してください。

**ステップ 2** VMware vSphere vSwitch の MTU 設定を変更します。

1. vSphere Web クライアントを使用して vCenter サーバーに接続します。
2. VMware vSphere vSwitch のプロパティを編集し、[MTU] の値を `9000` に設定します。

**ステップ 3** Cisco UCS ファブリック インターコネクト（FI）の MTU 設定を変更します。

1. Cisco UCS Management コンソールにログインします。

2. QoS システムクラスを編集するには、**[LAN]** > **[LANクラウド（LAN Cloud）]** > **QoS システム クラス（QoS System Class）** の順に選択します。[全般（General）] タブで、[MTU] の値を 9216 に設定します。
3. vNIC を編集するには、**[LAN]** > **[ポリシー（Policies）]** > **[ルート（root）]** > **[サブ組織（Sub-Organizations）]**

   <your-hyperflex-org>**vNIC テンプレート** <your-vnic> の順に選択します。[全般（General）] タブで、[MTU] の値を 9000 に設定します。

# トラブルシューティング

ここでは、仮想マシンへの Hyperflex 導入に関連する基本的なトラブルシューティング手順について説明します。

### 仮想マシンが HyperFlex を実行しているかどうかを確認

Threat Defense Virtual アプライアンスが ESX OS を搭載した HyperFlex に設置されている場合、HX post_install スクリプトによって作成されたデフォルトの vSphere HA ポリシーにより、Threat Defense Virtual の電源がオンになったときにエラーメッセージが表示されます。エラーメッセージの内容は以下のとおりです。

「電源オンに失敗：vSphere HA 向けに設定されたフェールオーバーレベルを満たすために必要なリソースが不足しています。」

### 回避策

1. VMware vCenter で**[HXクラスタ（HX cluster）** > **[設定（Configure）]** > **[vSphereの可用性（vSphere Availability）]** > **[vSphere HAの編集（Edit vSphere HA）]** > **[アドミッションコントロール（Admission Control）]** > **[ホストのフェールオーバー キャパシティの定義（Define host failover capacity）]** > **[計算済みフェールオーバー キャパシティのオーバーライド（Override Calculated failover capacity）]**に移動します。
2. 予約済みのフェールオーバー CPU とメモリ容量の割合を変更および調整します。
3. Threat Defense Virtual VM の電源を入れます。

第 10 章

# Nutanix への Threat Defense Virtual の展開

この章では、Threat Defense Virtual を Nutanix 環境に展開する際の手順について説明します。


- 概要 （409 ページ）
- Nutanix への Threat Defense Virtual の展開について （409 ページ）
- エンドツーエンドの手順 （410 ページ）
- システム要件 （412 ページ）
- 注意事項と制約事項 （413 ページ）
- Secure Firewall Threat Defense Virtual デバイスの管理方法 （416 ページ）
- Nutanix に展開するための前提条件 （417 ページ）
- Nutanix に Threat Defense Virtual を展開する方法 （417 ページ）


## 概要

Cisco Secure Firewall Threat Defense Virtual（旧称 Firepower Threat Defense Virtual）は、Cisco Secure Firewall 機能を仮想化環境にもたらします。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

この章では、AHV ハイパーバイザを含む Nutanix 環境内における 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 Threat Defense Virtual 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。Secure Firewall Management Center（旧称 Firepower Management Center）または Secure Firewall Device Manager （旧称 Firepower Device Manager）を使用して Threat Defense Virtual を管理および監視できます。

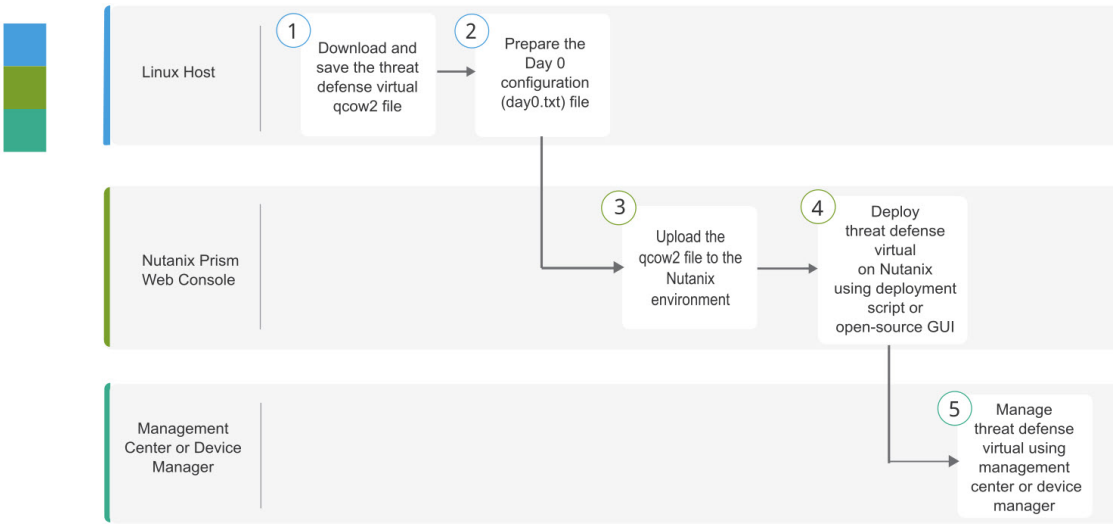
## Nutanix への Threat Defense Virtual の展開について

Nutanix Enterprise Cloud Platform は、仮想マシンのホスティングと格納用に構築された、統合型のスケールアウト対応コンピューティングおよびストレージシステムです。Nutanix AHV を

使用して、修正されていない Threat Defense Virtual の OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

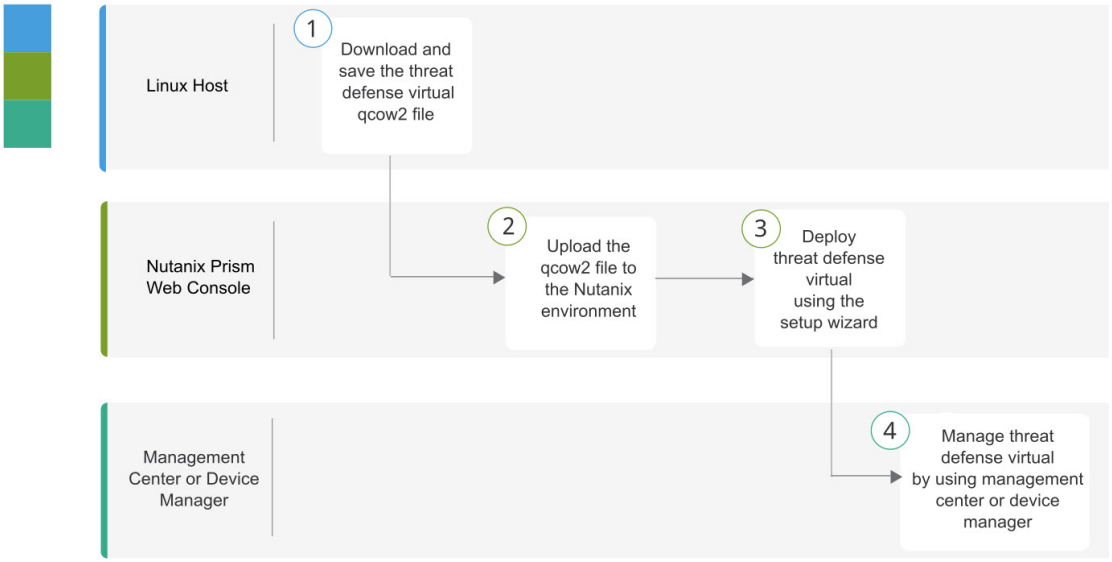
# エンドツーエンドの手順

次のフローチャートは、Day 0 の構成ファイルを使用して Nutanix プラットフォームに Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Linux ホスト | Threat Defense Virtual の導入：Threat Defense Virtual の qcow2 ファイルをダウンロードして保存します。 |
| 2 | Linux ホスト | Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード：qcow2 ファイルを Nutanix 環境にアップロードします。 |
| 3 | Nutanix Prism Web コンソール | 第 0 日のコンフィギュレーション ファイルの準備：Day-0 構成ファイルを準備します（**テキストファイル** > **構成の詳細を入力** > **day0-config.txt のファイル名で保存**）。 |
| 4 | Nutanix Prism Web コンソール | Threat Defense Virtual の導入：Nutanix に Threat Defense Virtual を展開します。 |
| 5 | Management Center または Device Manager | Threat Defense Virtual の管理：<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

次のフローチャートは、Day 0 の構成ファイルを使用せずに Nutanix プラットフォームに Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | Linux ホスト | Threat Defense Virtual の導入：Threat Defense Virtual の qcow2 ファイルをダウンロードして保存します。 |
| 2 | Nutanix Prism Web コンソール | Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード：qcow2 ファイルを Nutanix 環境にアップロードします。 |
| 3 | Nutanix Prism Web コンソール | Threat Defense Virtual の導入：Nutanix に Threat Defense Virtual を展開します。 |
| 4 | Management Center または Device Manager | Threat Defense Virtual の管理：<br>• Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理<br>• Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理 |

# システム要件

### バージョン

| マネージャバージョン | デバイスバージョン |
|---|---|
| Device Manager 7.0 | Threat Defense 7.0 |
| Management Center 7.0 | |

Threat Defense Virtual のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

### Threat Defense Virtual のメモリ、vCPU、およびディスクのサイジング

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

| 設定 | 値 |
|---|---|
| パフォーマンス階層 | **バージョン 7.0 以降**<br>Threat Defense Virtual 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。<br>• FTDv5 4vCPU/8GB（100 Mbps）<br>• FTDv10 4vCPU/8GB（1 Gbps）<br>• FTDv20 4vCPU/8GB（3 Gbps）<br>• FTDv30 8vCPU/16GB（5 Gbps）<br>• FTDv50 12vCPU/24GB（10 Gbps）<br>• FTDv100 16vCPU/32GB（16 Gbps）<br>Threat Defense Virtual 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* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。<br>（注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。 |

| 設定 | 値 |
|---|---|
| ストレージ | 50 GB（調整可能）<br>• virtio ブロック デバイスをサポート |

（注） Threat Defense Virtual 向けネットワークのデータインターフェイスの最小数は 4 つ（管理、診断、外部、内部）です。

### Threat Defense Virtual ライセンス

- Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
- ライセンスの管理方法の詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Firepower* システムのライセンス」を参照してください。

### Nutanix のコンポーネントとバージョン

| コンポーネント | バージョン |
|---|---|
| Nutanix Acropolis OS（AOS） | 5.15.5 LTS 以降 |
| Nutanix クラスタチェック（NCC） | 4.0.0.1 |
| Nutanix AHV | 20201105.12 以降 |
| Nutanix Prism Web コンソール | - |

# 注意事項と制約事項

### サポートされる機能

- 展開モード：ルーテッド（スタンドアロン）、ルーテッド（HA）、インラインタップ、インライン、パッシブ、およびトランスペアレント
- ライセンス：BYOL のみ
- IPv6
- Threat Defense Virtual ネイティブ HA
- Device Manager
- ジャンボフレーム
- VirtIO

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「Nutanix での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

### サポートされない機能

- Nutanix AHV 上の Threat Defense Virtual は、インターフェイスのホットプラグをサポートしていません。Threat Defense Virtual の電源が入っているときに、インターフェイスの追加や削除を試みないでください。
- Nutanix AHV は SR-IOV および DPDK-OVS をサポートしていません。

（注） Nutanix AHV は、VirtIO を使用したゲスト内 DPDK をサポートします。詳細については、「AHV での DPDK サポート」を参照してください。

### 一般的なガイドライン

- ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要合計 10 個のインターフェイスをサポート。

（注）
- Threat Defense Virtual のデフォルト設定では、管理インターフェイス、診断インターフェイス、および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。
- ネットワーク インターフェイスを変更するときは、Threat Defense Virtual デバイスをオフにする必要があります。

- Threat Defense Virtual のデフォルト設定では、管理インターフェイス（管理と診断）および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用すると仮定します（外部インターフェイス経由）。
- Threat Defense Virtual は、少なくとも 4 つのインターフェイスを備え、firstboot で電源がオンになる必要があります。4 つのインターフェイスがなければ展開は実行されません。
- Threat Defense Virtual では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワークインターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。
  1. 管理インターフェイス（必須）
  2. 診断インターフェイス（必須）
  3. 外部インターフェイス（必須）
  4. 内部インターフェイス（必須）
  5. 5 ～ 10 個のデータインターフェイス（オプション）

（注） Threat Defense Virtual 向けネットワークのデータインターフェイスの最小数は 3 つです。

- コンソールアクセスの場合、ターミナルサーバーは telnet を介してサポートされます。
- サポートされている vCPU とメモリのパラメータは次のとおりです。

| CPU | メモリ | Threat Defense Virtual プラットフォームのサイズ |
|---|---|---|
| 4 | 8 GB | 4vCPU/8GB（デフォルト） |
| 8 | 16 GB | 8vCPU/16GB |
| 12 | 24 GB | 12 vCPU/24 GB |
| 16 | 32 GB | 16vCPU/32GB |

- Threat Defense Virtual インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークに関する以下の用語索引を参照してください。

| ネットワーク アダプタ | 送信元ネットワーク | 宛先ネットワーク | 機能 |
|---|---|---|---|
| vnic0* | Management0-0 | Management0/0 | 管理 |
| vnic1 | 診断 | 診断 | 診断 |
| vnic2* | GigabitEthernet0-0 | GigabitEthernet 0/0 | 外部 |
| vnic3* | GigabitEthernet0-1 | GigabitEthernet 0/1 | 内部 |
| * 同じサブネットに接続します。 | | | |

**関連資料**

- Nutanix Release Notes
- Nutanix Field Installation Guide
- Nutanix でのハードウェアのサポート

# Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

## Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

## Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

**重要** Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

# Nutanix に展開するための前提条件

- Cisco.com から Threat Defense Virtual qcow2 ファイルをダウンロードします（https://software.cisco.com/download/navigator.html）。

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

- 「概要 （409 ページ）」の章を確認します。
- Nutanix とシステムの互換性については、『Cisco Firepower Threat Defense Virtual Compatibility Guide』[英語] を参照してください。

# Nutanix に Threat Defense Virtual を展開する方法

| ステップ | タスク | 詳細情報 |
|---|---|---|
| 1 | 前提条件を確認します。 | Nutanix に展開するための前提条件 （417 ページ） |

| ステップ | タスク | 詳細情報 |
|---|---|---|
| 2 | Threat Defense Virtual qcow2 ファイルを Nutanix 環境にアップロードします。 | Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード （418 ページ） |
| 3 | （オプション）仮想マシンの展開時に適用される初期設定データを含む第 0 日の構成ファイルを準備します。 | 第 0 日のコンフィギュレーション ファイルの準備 （419 ページ） |
| 4 | Threat Defense Virtual を Nutanix 環境に展開します。 | Threat Defense Virtual の導入 （420 ページ） |
| 5 | （任意）Threat Defense Virtual のセットアップに Day 0 の構成ファイルを使用しなかった場合は、CLI にログインして、セットアップを完了します。 | Threat Defense Virtual のセットアップの完了 （423 ページ） |

# Threat Defense Virtual QCOW2 ファイルを Nutanix にアップロード

Threat Defense Virtual を Nutanix 環境に展開するには、Prism Web コンソールで Threat Defense Virtual qcow2 ディスクファイルからイメージを作成する必要があります。

### 始める前に

Cisco.com から Threat Defense Virtual qcow2 ディスクファイルをダウンロードします（https://software.cisco.com/download/navigator.html）。

**ステップ 1** Nutanix Prism Web コンソールにログインします。

**ステップ 2** 歯車アイコンをクリックして [設定（Settings）] ページを開きます。

**ステップ 3** 左側のペインで [イメージの設定（Image Configuration）] をクリックします。

**ステップ 4** [Upload Image] をクリックします。

**ステップ 5** イメージを作成します。

1. イメージの名前を入力します。
2. [イメージタイプ（Image Type）] ドロップダウンリストから、[ディスク（DISK）] を選択します。
3. [ストレージコンテナ（Storage Container）] ドロップダウンリストから、目的のコンテナを選択します。
4. Threat Defense Virtual qcow2 ディスクファイルの場所を指定します。

   URL を指定して Web サーバーからファイルをインポートすることも、ワークステーションからファイルをアップロードすることもできます。
5. [保存（Save）] をクリックします。

**ステップ 6** [イメージの設定（Image Configuration）] ページに新しいイメージが表示されるまで待ちます。

# 第 0 日のコンフィギュレーション ファイルの準備

Threat Defense Virtual を展開する前に、Day 0 の構成ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキスト ファイルです。

次の点を考慮してください。

- 導入時に Day 0 の構成ファイルを使用すると、導入プロセスで Threat Defense Virtual アプライアンスの初期設定をすべて実行できます。
- 導入時に Day 0 の構成ファイルを使用しない場合は、起動後にシステムの必須設定を指定する必要があります。詳細については、「Threat Defense Virtual のセットアップの完了（423 ページ）」を参照してください。

次を指定することができます。

- エンド ユーザー ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 最初のファイアウォール モード。最初のファイアウォール モード（**ルーテッド**または**トランスペアレント**）を設定します。

  ローカルの Device Manager を使用して展開を管理する予定の場合は、ファイアウォール モードに**ルーテッド**のみ設定できます。Device Manager を使用してトランスペアレント ファイアウォール モードのインターフェイスは設定できません。
- 管理モード。Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）を参照してください。

  [ローカルに管理（ManageLocally）] を [はい（Yes）] に設定するか、または Management Center フィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に情報を入力することができます。使用していない管理モードでは、フィールドを空のままにします。
- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。

**ステップ 1** 任意のテキストエディタを使用して、新しいテキストファイルを作成します。

**ステップ 2** 次の例に示すように、テキストファイルに構成の詳細を入力します。

**例**：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
```

```
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"Yes"
}
```

（注） 第 0 日の構成ファイルの内容は、JSON 形式である必要があります。JSON 検証ツールを使用してテキストを検証する必要があります。

**ステップ 3** ファイルを「**day0-config.txt**」として保存します。

**ステップ 4** ステップ 1 ～ 3 を繰り返して、展開する Threat Defense Virtual ごとに一意のデフォルト構成ファイルを作成します。

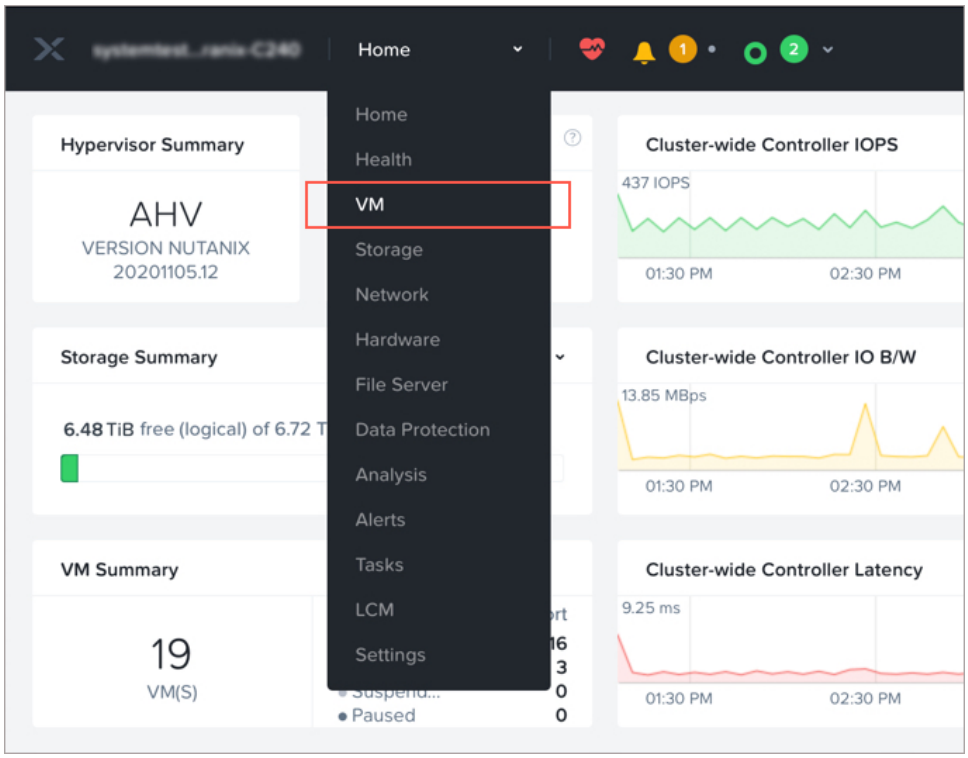
# Threat Defense Virtual の導入

### 始める前に

展開する Threat Defense Virtual のイメージが [イメージの設定（Image Configuration）] ページに表示されていることを確認します。

**ステップ 1** Nutanix Prism Web コンソールにログインします。

**ステップ 2** メインメニューバーで、表示ドロップダウンリストをクリックし、[VM] を選択します。




**ステップ 3** VM ダッシュボードで、[VMの作成（Create VM）] をクリックします。

**ステップ 4** 次の手順を実行します。

1. Threat Defense Virtual インスタンスの名前を入力します。
2. 必要に応じて、Threat Defense Virtual インスタンスの説明を入力します。
3. Threat Defense Virtual インスタンスで使用するタイムゾーンを選択します。

**ステップ 5** コンピューティングの詳細を入力します。

1. Threat Defense Virtual インスタンスに割り当てる仮想 CPU の数を入力します。
2. 各仮想 CPU に割り当てる必要があるコアの数を入力します。
3. Threat Defense Virtual インスタンスに割り当てるメモリの量（GB）を入力します。

**ステップ 6** Threat Defense Virtual インスタンスにディスクを接続します。

1. [ディスク（Disks）] で、[新しいディスクの追加（Add New Disk）] をクリックします。
2. [タイプ（Type）] ドロップダウンリストから、[ディスク（DISK）] を選択します。
3. [操作（Operation）] ドロップダウンリストから、[イメージサービスから複製（Clone from Image Service）] を選択します。
4. [バスタイプ（Bus Type）] ドロップダウンリストから、[PCI] または [SCSI] を選択します。
5. [イメージ（Image）] ドロップダウンリストから、使用するイメージを選択します。

6. [追加（Add）] をクリックします。

**ステップ 7** 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。

[ネットワークアダプタ（NIC）（Network Adapters (NIC)）] で、[新しいNIC の追加（Add New NIC）] をクリックし、ネットワークを選択して、[追加（Add）] をクリックします。

このプロセスを繰り返して、ネットワーク インターフェイスをさらに追加します。

Nutanix 上の Threat Defense Virtual は、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データトラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- vnic0：管理インターフェイス（必須）
- vnic1：診断インターフェイス（必須）
- vnic2：外部インターフェイス（必須）
- vnic3：内部インターフェイス（必須）
- vnic4-9：データ インターフェイス（オプション）

**ステップ 8** Threat Defense Virtual のアフィニティポリシーを設定します。

[VMホストアフィニティ（VM Host Affinity）] で、[アフィニティの設定（Set Affinity）] をクリックし、ホストを選択して、[保存（Save）] をクリックします。

ノードに障害が発生した場合でも Threat Defense Virtual を実行できるようにするには、1 つ以上のホストを選択します。

**ステップ 9** 第 0 日の構成ファイルを準備済みの場合は、次の手順を実行します。

1. [カスタムスクリプト（Custom Script）] を選択します。
2. [ファイルをアップロード（Upload A File）] をクリックし、第 0 日の構成ファイル（**day0-config.txt**）を選択します。

（注） 他のすべてのカスタム スクリプト オプションは、このリリースではサポートされていません。

**ステップ 10** [保存（Save）] をクリックして、Threat Defense Virtual を展開します。VM テーブルビューに Threat Defense Virtual インスタンスが表示されます。

**ステップ 11** VM テーブルビューで、新しく作成した Threat Defense Virtual インスタンスを選択し、[電源オン（Power On）] をクリックします。

### 次のタスク

- Day 0 構成ファイルを使用して Threat Defense Virtual をセットアップした場合、次の手順は選択した管理モードによって異なります。

- [ローカルに管理（ManageLocally）] で [いいえ（No）] を選択した場合は、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 ページ）」を参照してください。

- Threat Defense Virtual のセットアップに Day 0 の構成ファイルを使用しなかった場合は、CLI にログインして、Threat Defense Virtual のセットアップを完了します。この説明については、Threat Defense Virtual のセットアップの完了 （423 ページ） を参照してください。

# Threat Defense Virtual のセットアップの完了

Threat Defense Virtual アプライアンスには Web インターフェイスがないため、Day 0 の構成ファイルを使用せずに導入した場合には、CLI を使用して仮想デバイスを設定する必要があります。

**ステップ 1** Threat Defense Virtual でコンソールを開きます。

**ステップ 2** [firepower ログイン（firepower login）] プロンプトで、ユーザー名 *admin* とパスワード *Admin123* のデフォルトのクレデンシャルでログインします。

**ステップ 3** Threat Defense Virtual システムが起動すると、セットアップウィザードでシステムの設定に必要な次の情報の入力が求められます。

- 使用許諾契約の同意
- 新しい管理者パスワード
- IPv4 または IPv6 の構成
- IPv4 または IPv6 の DHCP 設定
- 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
- システム名
- デフォルトゲートウェイ
- DNS セットアップ
- HTTP プロキシ
- 管理モード（ローカル管理が必要）

**ステップ 4** セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

**ステップ 5** プロンプトに従ってシステム設定を行います。

**ステップ 6** コンソールが # プロンプトに戻るときに、設定が正常に行われたことを確認します。

**ステップ 7** CLI を閉じます。

### 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、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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、「Secure Firewall Threat Defense Virtual デバイスの管理方法 （2 ページ）」を参照してください。

第 11 章

# OpenStack への Threat Defense Virtual の展開


- 概要 （425 ページ）
- エンドツーエンドの手順 （426 ページ）
- 前提条件 （427 ページ）
- 注意事項と制約事項 （428 ページ）
- システム要件 （429 ページ）
- OpenStack 上の Threat Defense Virtual のネットワークトポロジ例 （431 ページ）
- Threat Defense Virtual の導入 （432 ページ）
- OpenStack への Threat Defense Virtual イメージのアップロード （433 ページ）
- OpenStack と Threat Defense Virtual のネットワーク インフラストラクチャの作成 （434 ページ）
- OpenStack への Threat Defense Virtual の展開 （434 ページ）


## 概要

このガイドでは、OpenStack 環境で Threat Defense Virtual を展開する方法について説明します。OpenStack は無料のオープンな標準規格のクラウドコンピューティングプラットフォームであり、ほとんどの場合は、ユーザーが仮想サーバーやその他のリソースを利用できるように Infrastructure-as-a-Service（IaaS）としてパブリッククラウドとプライベートクラウドの両方に展開します。

この展開では、KVM ハイパーバイザを使用して仮想リソースを管理します。KVM は、仮想化拡張機能（Intel VT など）を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネルモジュール（kvm.ko）と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。

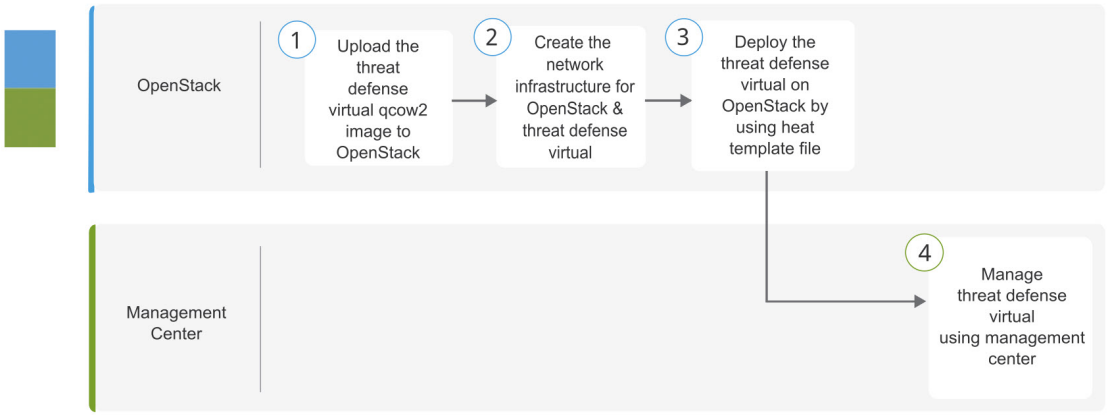
KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

デバイスは KVM ハイパーバイザですでにサポートされているため、OpenStack サポートを有効にするために必要な追加のカーネルパッケージやドライバはありません。

（注） OpenStack の Threat Defense Virtual は、最適化されたマルチノード環境にインストールできます。

# エンドツーエンドの手順

次のフローチャートは、OpenStack に Threat Defense Virtual を展開する際のワークフローを示しています。




| | ワークスペース | 手順 |
|---|---|---|
| 1 | OpenStack | OpenStack への Threat Defense Virtual イメージのアップロード：Threat Defense Virtual のイメージを OpenStack にアップロードします。 |
| 2 | OpenStack | OpenStack と Threat Defense Virtual のネットワーク インフラストラクチャの作成：OpenStack および Threat Defense Virtual のネットワーク インフラストラクチャを作成します。 |
| 3 | OpenStack | OpenStack への Threat Defense Virtual の展開：Threat Defense Virtual の Heat テンプレートファイルを使用して、Threat Defense Virtual を OpenStack に展開します。 |
| 4 | Management Center | Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 |

# 前提条件

- software.cisco.com から qcow2 Threat Defense Virtual イメージを取得します。
- Threat Defense Virtual は、オープンソースの OpenStack 環境と Cisco VIM 管理対象 OpenStack 環境での展開をサポートします。

  OpenStack のガイドラインに従って OpenStack 環境をセットアップします。

  - オープンソースの OpenStack ドキュメントを参照してください。

    Stein リリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html

    Queens リリース：https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/overview.html

  - Cisco Virtualized Infrastructure Manager（VIM）OpenStack のドキュメント（Cisco Virtualized Infrastructure Manager のマニュアル、3.4.3 ～ 3.4.5）を参照してください。

- Cisco スマートアカウント。Cisco Software Central で作成できます。
- Threat Defense Virtual へのライセンス付与。
  - Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
  - ライセンスの管理方法の詳細については、『*Secure Firewall Management Center Admin Guide*』の「Licensing」を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Threat Defense Virtual を Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - 内部インターフェイスと外部インターフェイス：Threat Defense Virtual を内部のホストとパブリックインターフェイスに接続するために使用します。
- 通信パス：
  - Threat Defense Virtual にアクセスするためのフローティング IP。
- サポートされている Threat Defense Virtual の最小バージョン：
  - バージョン 7.0
- OpenStack の要件については、システム要件 （429 ページ）を参照してください。
- Threat Defense Virtual システムの要件については、『Cisco Firepower Compatibility』を参照してください。

# 注意事項と制約事項

## サポートされる機能

OpenStack 上の Threat Defense Virtual は次の機能をサポートします。

- OpenStack 環境のコンピューティングノードで実行されている KVM ハイパーバイザへの Threat Defense Virtual の展開
- OpenStack CLI
- Heat テンプレートベースの展開
- OpenStack Horizon ダッシュボード
- ルーテッド モード（デフォルト）
- IPv6
- ライセンス：BYOL のみをサポート
- Management Center を使用した Threat Defense Virtual の管理
- ドライバ：VirtIO、VPP、および SR-IOV

## Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual 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 *31 : Threat Defense Virtual* 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 | 4 コア/8 GB | 100Mbps | 50 |
| FTDv10 | 4 コア/8 GB | 1Gbps | 250 |
| FTDv20 | 4 コア/8 GB | 3 Gbps | 250 |
| FTDv30 | 8 コア/16 GB | 5 Gbps | 250 |
| FTDv50 | 12 コア/24 GB | 10 Gbps | 750 |
| FTDv100 | 16 コア/32 GB | 16 Gbps | 10,000 |

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『*Secure Firewall Management Center Admin Guide*』の「Licensing」の章を参照してください。

### パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「OpenStack での仮想化の調整と最適化」を参照してください。

**Receive Side Scaling**：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

### Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

### サポートされない機能

OpenStack 上の Threat Defense Virtual は以下をサポートしません。

- 自動スケール
- IPv6

# システム要件

OpenStack 環境は、サポートされているハードウェアとソフトウェアの次の要件に準拠している必要があります。

**表 *32 : Open Source OpenStack* のハードウェアとソフトウェアの要件**

| カテゴリ | サポートされるバージョン | 注記 |
|---|---|---|
| サーバ ハードウェア | UCS C240 M5 | 2 台の UCS サーバーを推奨します。os-controller ノードと os-compute ノードに 1 台ずつです。 |
| ドライバ | VIRTIO、IXGBE、I40E | サポートされているドライバは次のとおりです。 |

| カテゴリ | サポートされるバージョン | 注記 |
|---|---|---|
| オペレーティングシステム | Ubuntu Server 18.04 | これは、UCS サーバーで推奨されている OS です。 |
| OpenStack バージョン | Stein リリース | さまざまな OpenStack リリースの詳細については、次の URL を参照してください。<br>https://releases.openstack.org/ |

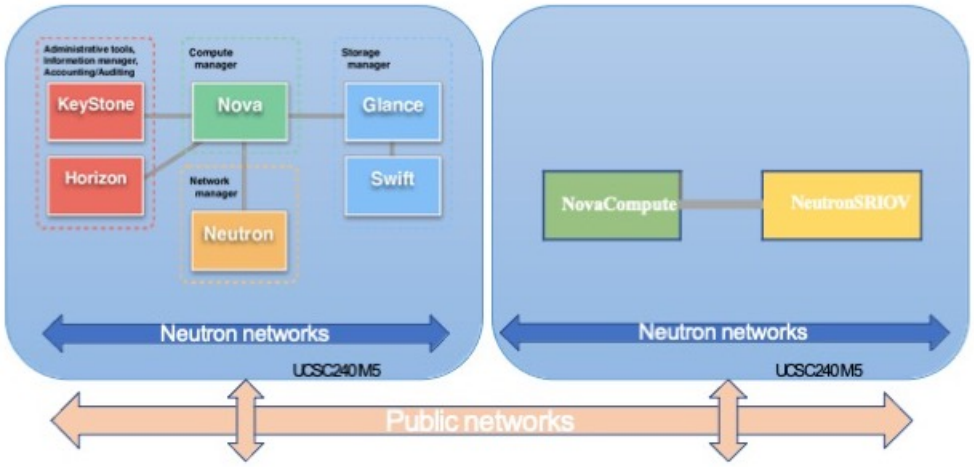
表 *33 : Cisco VIM Managed OpenStack* のハードウェアとソフトウェアの要件

| カテゴリ | サポートされるバージョン | 注記 |
|---|---|---|
| サーバ ハードウェア | UCS C220-M5/UCS C240-M4 | os-controller ノードごとに 3 台、os-compute ノードに 2 台以上で、5 台の UCS サーバーを推奨します。 |
| ドライバ（Drivers） | VIRTIO、SRIOV、および VPP | サポートされているドライバは次のとおりです。 |
| Cisco VIM バージョン | Cisco VIM 3.4.4<br>サポート対象：<br>• オペレーティングシステム - Red Hat Enterprise Linux 7.6<br>• OpenStack バージョン - OpenStack 13.0（Queens リリース） | 詳細については、シスコ仮想インフラストラクチャ マネージャのドキュメント 3.4.3 ～ 3.4.5 を参照してください。<br>さまざまな OpenStack リリースの詳細については、https://releases.openstack.org/ を参照してください。 |
| | Cisco VIM 4.2.1<br>サポート対象：<br>• オペレーティングシステム - Red Hat Enterprise Linux 8.2<br>• OpenStack バージョン - OpenStack 16.1（トレイン リリース） | 詳細については、シスコ仮想インフラストラクチャ マネージャのドキュメント 4.2.1 を参照してください。<br>さまざまな OpenStack リリースの詳細については、https://releases.openstack.org/ を参照してください。 |

### OpenStack プラットフォームトポロジ

次の図に、2 台の UCS サーバーを使用して OpenStack での展開をサポートするための推奨トポロジを示します。

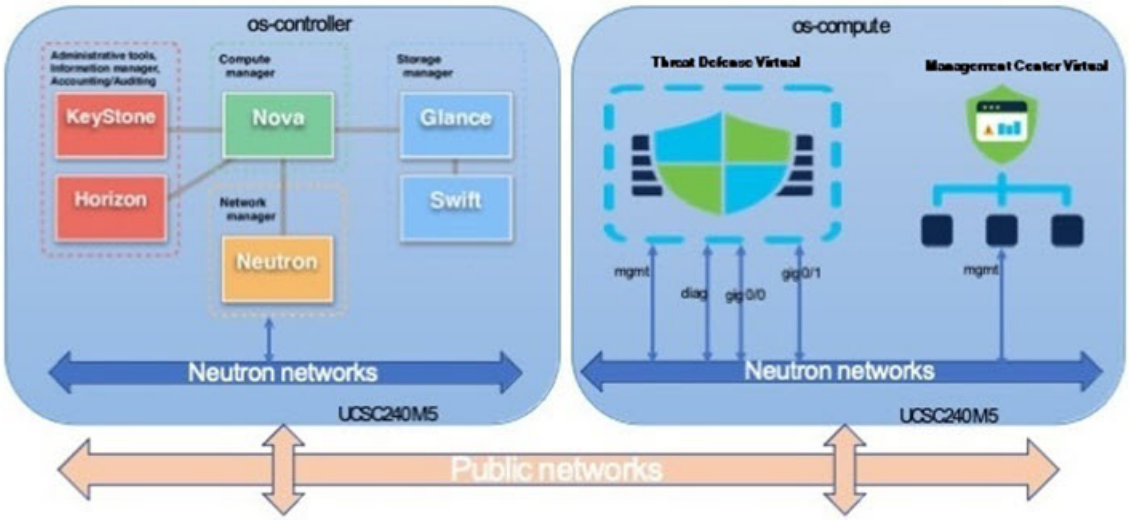
**図 *52 : OpenStack* プラットフォームトポロジ**




# OpenStack 上の Threat Defense Virtual のネットワークトポロジ例

次の図に、Threat Defense Virtual 用の OpenStack に設定された 4 つのサブネット（管理、診断、内部、および外部）を備えたルーテッド ファイアウォール モードの Threat Defense Virtual のネットワークトポロジの例を示します。

図 *53 : OpenStack* で *Threat Defense Virtual* と *Management Center Virtual* を使用したトポロジの例




# Threat Defense Virtual の導入

シスコでは、Threat Defense Virtual を展開するためのサンプルの Heat テンプレートを提供しています。OpenStack インフラストラクチャのリソースを作成する手順は、ネットワーク、サブネット、およびルータインターフェイスを作成するために、Heat テンプレート（`deploy_os_infra.yaml`）ファイルで結合されます。Threat Defense Virtual の展開手順は大まかに次の部分に分類されます。

- Threat Defense Virtual qcow2 イメージを OpenStack Glance サービスにアップロードします。
- ネットワーク インフラストラクチャを作成します。
  - ネットワーク
  - サブネット
  - ルータ インターフェイス
- Threat Defense Virtual インスタンスを作成します。
  - フレーバ
  - セキュリティ グループ
  - フローティング IP
  - インスタンス

次の手順を使用して、OpenStack に Threat Defense Virtual を展開できます。

# OpenStack への Threat Defense Virtual イメージのアップロード

Threat Defense Virtual qcow2 イメージを OpenStack コントローラノードにコピーし、イメージを OpenStack Glance サービスにアップロードします。

### 始める前に

Cisco.com から Threat Defense Virtual qcow2 ファイルをダウンロードし、Linux ホストに格納します。

https://software.cisco.com/download/navigator.html

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

**ステップ 1** qcow2 イメージファイルを OpenStack コントローラノードにコピーします。

**ステップ 2** Threat Defense Virtual イメージを OpenStack Glance サービスにアップロードします。

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

**ステップ 3** Threat Defense Virtual イメージが正常にアップロードされたことを確認します。

root@ucs-os-controller:$ openstack image list

**例**：

```
root@ucs-os-controller:$ openstack image
list+--------------------------------------+------------------+--------+
| ID                                   | Name               | Status
|+--------------------------------------+------------------+--------+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image     | active
|+--------------------------------------+------------------+--------+
```

アップロードしたイメージとそのステータスが表示されます。

### 次のタスク

`deploy_os_infra.yaml` テンプレートを使用してネットワーク インフラストラクチャを作成します。

# OpenStack と Threat Defense Virtual のネットワーク インフラストラクチャの作成

### 始める前に

Heatテンプレートファイルは、フレーバ、ネットワーク、サブネット、ルータインターフェイス、セキュリティグループルールなど、ネットワーク インフラストラクチャと Threat Defense Virtual に必要なコンポーネントを作成するために必要です。

- `deploy_os_infra.yaml`
- `env.yaml`

Threat Defense Virtual バージョンのテンプレートは、GitHub リポジトリの FTDv OpenStack Heat テンプレートから入手できます。

**重要** シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。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。

**ステップ 1** インフラストラクチャ Heat テンプレートファイルを展開します。

**root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>**

例：

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

**ステップ 2** インフラストラクチャ スタックが正常に作成されたかどうかを確認します。

**root@ucs-os-controller:$ openstack stack list**

### 次のタスク

OpenStack で Threat Defense Virtual インスタンスを作成します。

# OpenStack への Threat Defense Virtual の展開

Threat Defense Virtual Heat テンプレートのサンプルを使用して、OpenStack に Threat Defense Virtual を展開します。

### 始める前に

OpenStack で Threat Defense Virtual を展開するには、次の Heat テンプレートが必要です。

- `deploy_ftdv.yaml`

Threat Defense Virtual バージョンのテンプレートは、GitHub リポジトリの FTDv OpenStack Heat テンプレートから入手できます。

**重要** シスコが提供するテンプレートはオープンソースの例として提供しているものであり、通常の Cisco TAC サポートの範囲内では扱われていません。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。

**ステップ 1** Threat Defense Virtual Heat テンプレートファイル（`deploy_ftdv.yaml`）を展開して、Threat Defense Virtual インスタンスを作成します。

**root@ucs-os-controller:$ openstack stack create ftdv-stack -e env.yaml-t deploy_ftdv.yaml**

**例：**

```
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | ftdv-stack                           |
| description         | FTDvtemplate                         |
| creation_time       | 2020-12-07T14:55:05Z                 |
| updated_time        | None                                 |
| stack_status        | CREATE_IN_PROGRESS                   |
| stack_status_reason | Stack CREATE started                 |
+---------------------+--------------------------------------+
```

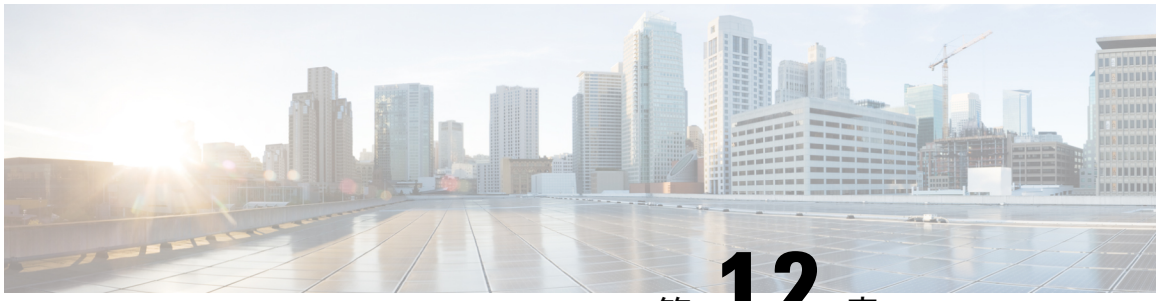
**ステップ 2** Threat Defense Virtual スタックが正常に作成されたことを確認します。

**root@ucs-os-controller:$ openstack stack list**

**例：**

```
+--------------------------------------+------------+----------------------------------+--------------+----------------------+--------+
| ID                                   | Stack Name | Project                          | Stack
Status     | Creation Time        | Updated Time |
+--------------------------------------+------------+----------------------------------+--------------+----------------------+--------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-07T14:55:05Z | None         |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE | 2020-12-03T10:46:50Z | None         |
+--------------------------------------+------------+----------------------------------+--------------+----------------------+--------+
```

OpenStack への Threat Defense Virtual の展開



第 12 章

# Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理

この章では、Management Center を使用して管理されるスタンドアロンの Threat Defense Virtual 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 Threat Defense Virtual 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 Management Center 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。


- Secure Firewall Management Center を備えた Secure Firewall Threat Defense Virtual について （437 ページ）
- Secure Firewall Management Center へのログイン （438 ページ）
- Secure Firewall Management Center へのデバイス登録 （438 ページ）
- 基本的なセキュリティポリシーの設定 （441 ページ）
- Secure Firewall Threat Defense CLI へのアクセス （454 ページ）


## Secure Firewall Management Center を備えた Secure Firewall Threat Defense Virtual について

Secure Firewall Threat Defense Virtual は、Cisco NGFW ソリューションの仮想化コンポーネントです。Threat Defense Virtual 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、マルウェア防御などの次世代ファイアウォールサービスを提供します。

Threat Defense Virtual 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 Management Centerを使用します。Threat Defense Virtual は、Threat Defense

Virtual マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

Threat Defense Virtual は、Threat Defense Virtual マシンに割り当てた管理インターフェイス上の Management Center 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 Threat Defense CLI にアクセスすることも、Management Center の CLI から Threat Defense に接続することもできます。

このガイドでは、Management Center を使用して管理されるスタンドアロンの Threat Defense Virtual デバイスの展開方法について説明します。Management Center での設定の詳細については、Management Center アドミニストレーション ガイド [英語] および Management Center デバイス コンフィギュレーション ガイド [英語] を参照してください。

Management Center のインストールの詳細については、『Cisco Firepower Management Center 1600、2600、4600 ハードウェア設置ガイド』または『Cisco Firepower Management Center Virtual スタートアップガイド』を参照してください。

# Secure Firewall Management Center へのログイン

Management Center を使用して、Threat Defense 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。

**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://***fmcv_ip_address*

*fmc_ip_address* で Management Center の IP アドレスまたはホスト名を指定します。

（注） IPv6 固有の https://[fmcv_ipv6_public_address]

**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。

# Secure Firewall Management Center へのデバイス登録

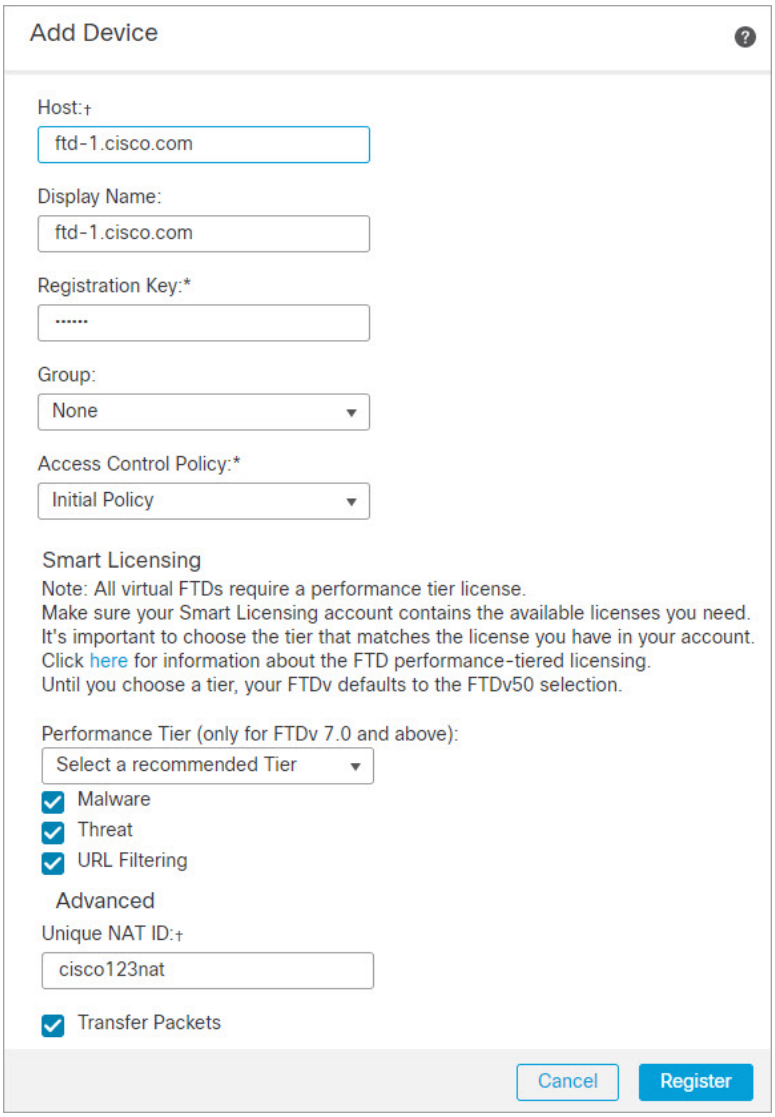
### 始める前に

Threat Defense Virtual 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、Management Center 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。Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

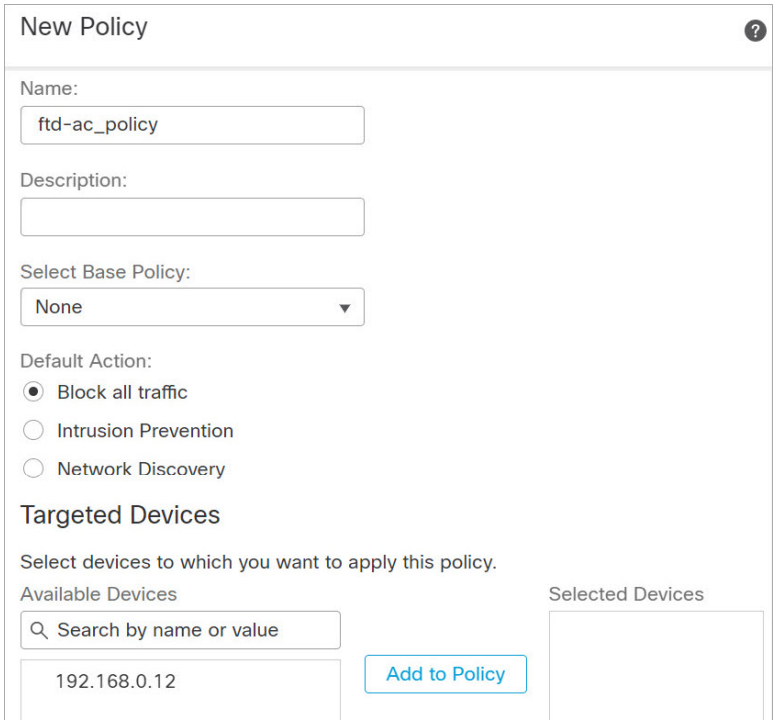
**ステップ 1** **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。

**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。




- [ホスト（Host）]：追加するデバイスの IP アドレス（IPv4 および IPv6）を入力します。IPv6 が有効になっている場合は、ホスト名に IPv4 または IPv6 を使用できます。

- [表示名（Display Name）]：Management Center に表示するデバイスの名前を入力します。
- [登録キー（Registration key）]：Threat Defense Virtual 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 （452 ページ）」を参照してください。




- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（マルウェア防御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行する予定の場合）を割り当てます。
- [一意の NAT ID（Unique NAT ID）]：Threat Defense Virtual 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 Management Center 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 Management Center 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 Management Center 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。Threat Defense Virtual 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：Threat Defense CLI（「Secure Firewall Threat Defense CLI へのアクセス （454 ページ）」）にアクセスし、次のコマンドを使用して Management Center 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。Threat Defense IP アドレスを変更する必要がある場合は、**configure network** {**ipv4** | **ipv6**} **manual or DHCP** 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）]**ページで設定した Management Center サーバーと一致していることを確認します。

- 登録キー、NAT ID、および Management Center 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 DONTRESOLVE<registrationkey> <NATID>** コマンドを使用して、Threat Defense Virtual 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 Management Center 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。

**ステップ 1** インターフェイスの設定 （442 ページ）
**ステップ 2** DHCP サーバーの設定 （445 ページ）
**ステップ 3** デフォルトルートの追加 （446 ページ）

**ステップ 4** NAT の設定 （448 ページ）
**ステップ 5** アクセス制御の設定 （452 ページ）
**ステップ 6** 設定の展開 （453 ページ）

# インターフェイスの設定

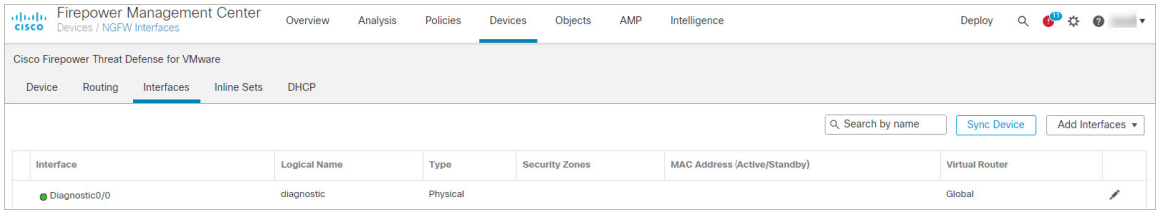
Threat Defense Virtual インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

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。

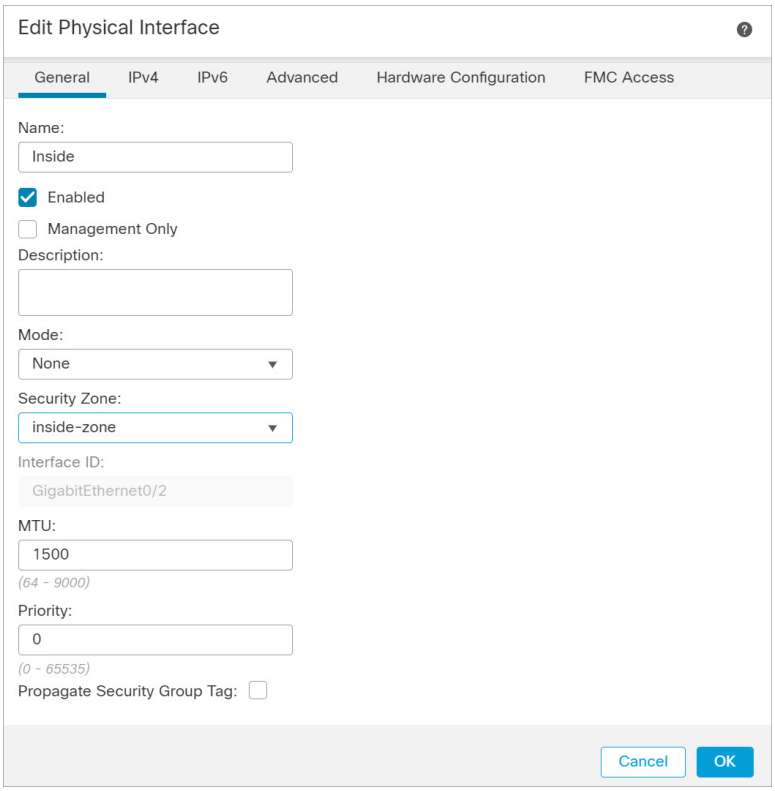
**ステップ 1** **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイス[編集（Edit）]（✎）をクリックします。

**ステップ 2** [インターフェイス（Interfaces）] をクリックします。




**ステップ 3** 「内部」に使用するインターフェイス[編集（Edit）]（✎）をクリックします。

[全般（General）] タブが表示されます。




a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

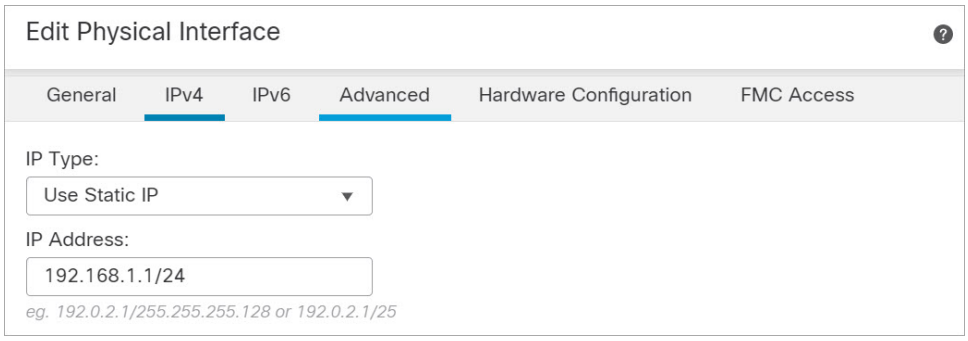
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。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、または [IPv6] タブ、または両方のタブをクリックします。

- [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または DHCP オプションで入力します。

  たとえば、**192.168.1.1/24** などと入力します。

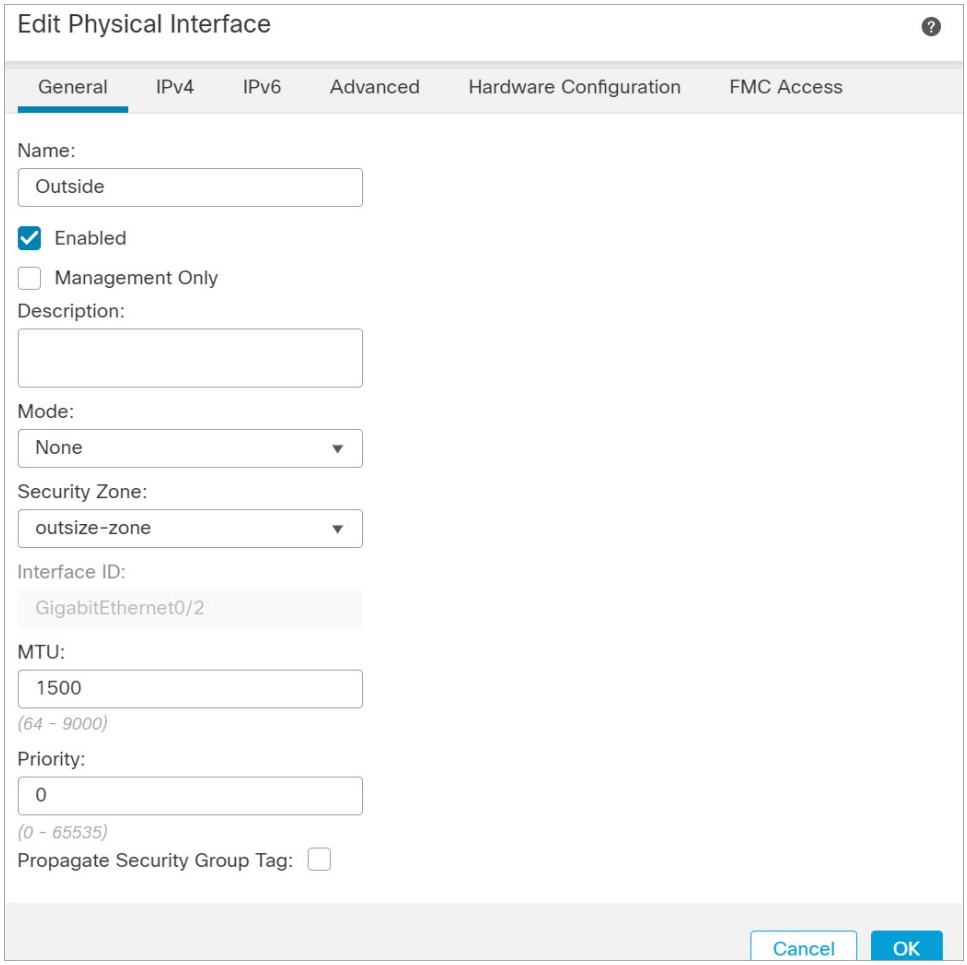



- [IPv6]：ステートレス自動設定を使用し、かつインターフェイスを有効にするために IPv6 DHCP または静的設定を使用する場合は、[自動設定（Autoconfiguration）] チェックボックスをオンにします。

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[編集（Edit）]（✎）をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「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。

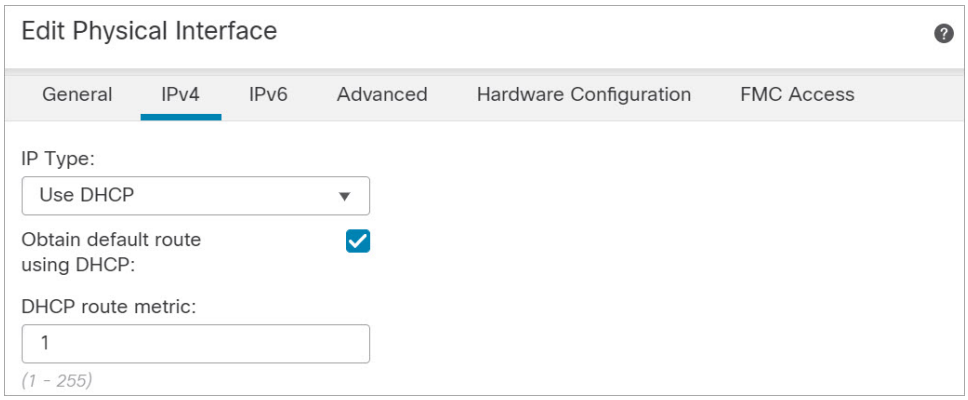
c) [モード（Mode）] は [なし（None）] に設定したままにします。

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、または [IPv6] タブ、または両方のタブをクリックします。

- [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。




- [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

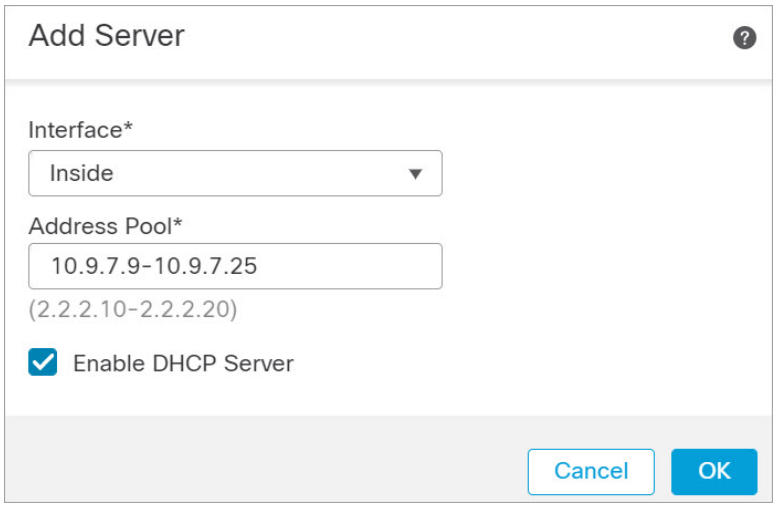
（注） AWS、Azure、GCP、OCI などのパブリッククラウド環境に展開する場合は、この手順をスキップします。

クライアントで DHCP を使用して Threat Defense Virtual 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。

**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[編集（Edit）]（✎）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。




- [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。

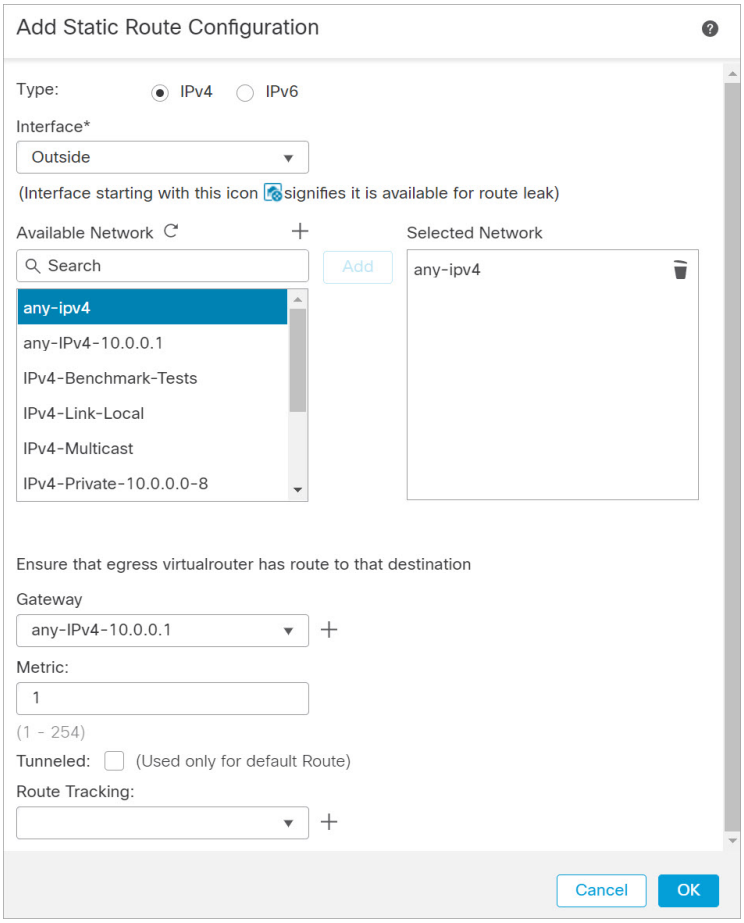
**ステップ 5** [保存（Save）] をクリックします。

# 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。

**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[編集（Edit）]（✎）をクリックします。

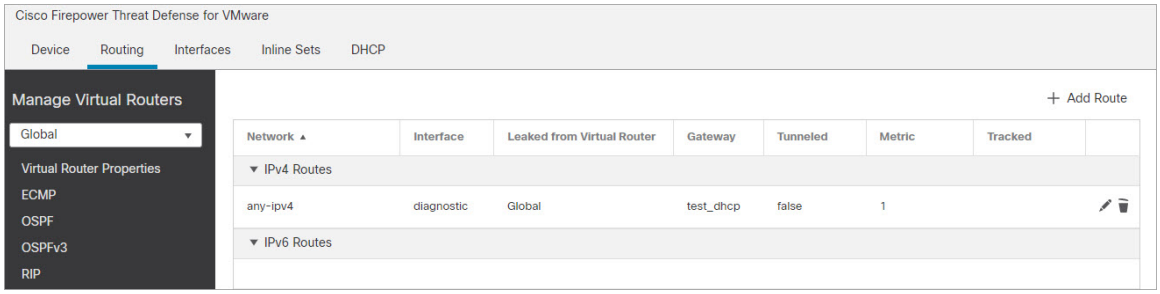
**ステップ 2** **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）]をクリックして、次のように設定します。




- [タイプ（Type）]：追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス（Interface）]：出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク（Available Network）]：IPv4 デフォルト ルートの場合は [any-ipv4]、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。
- [ゲートウェイ（Gateway）] または [IPv6ゲートウェイ（IPv6 Gateway）]：このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

**ステップ 3** [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。



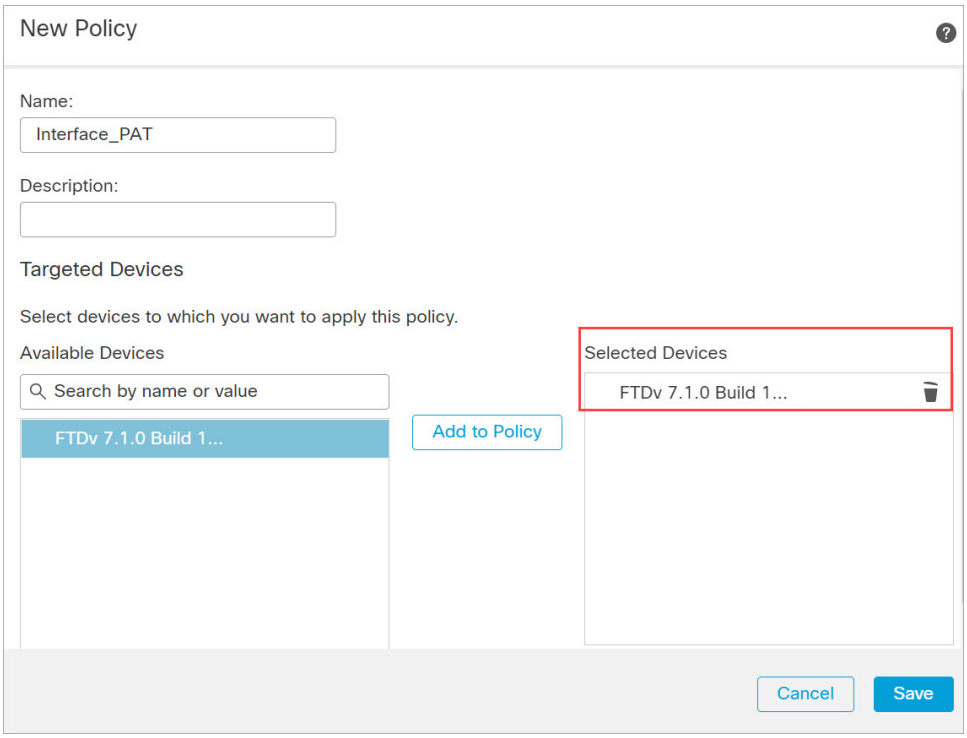

**ステップ 4** [保存（Save）] をクリックします。

# NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

**ステップ 1** **[デバイス（Devices）]** > **[NAT]** をクリックし、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

**ステップ 2** ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。

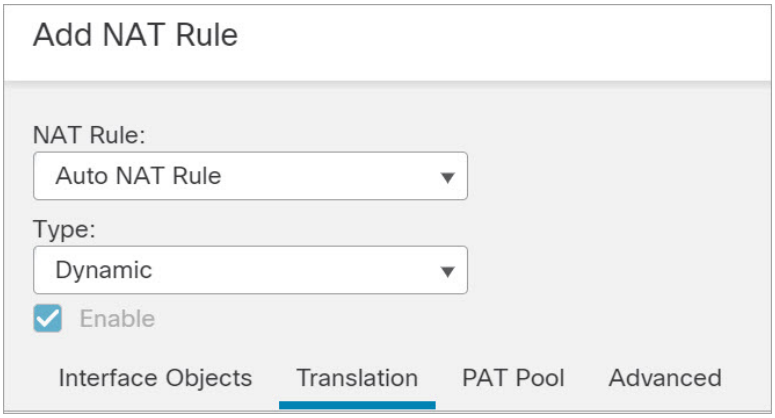



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

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

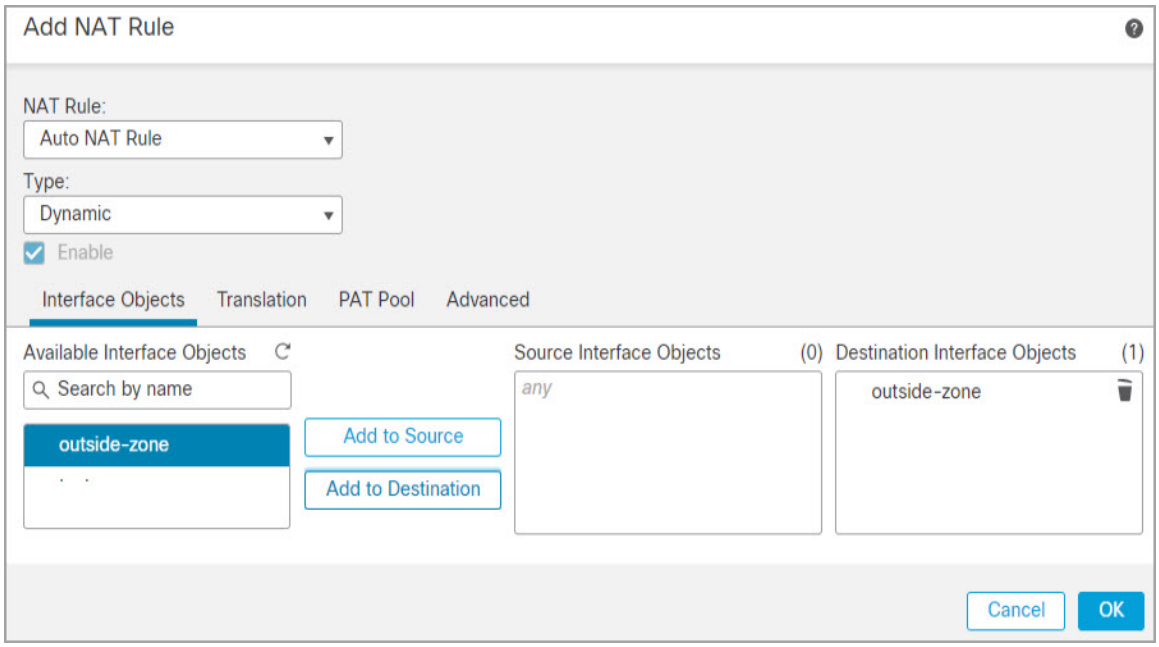
[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

**ステップ 4** 基本ルールのオプションを設定します。

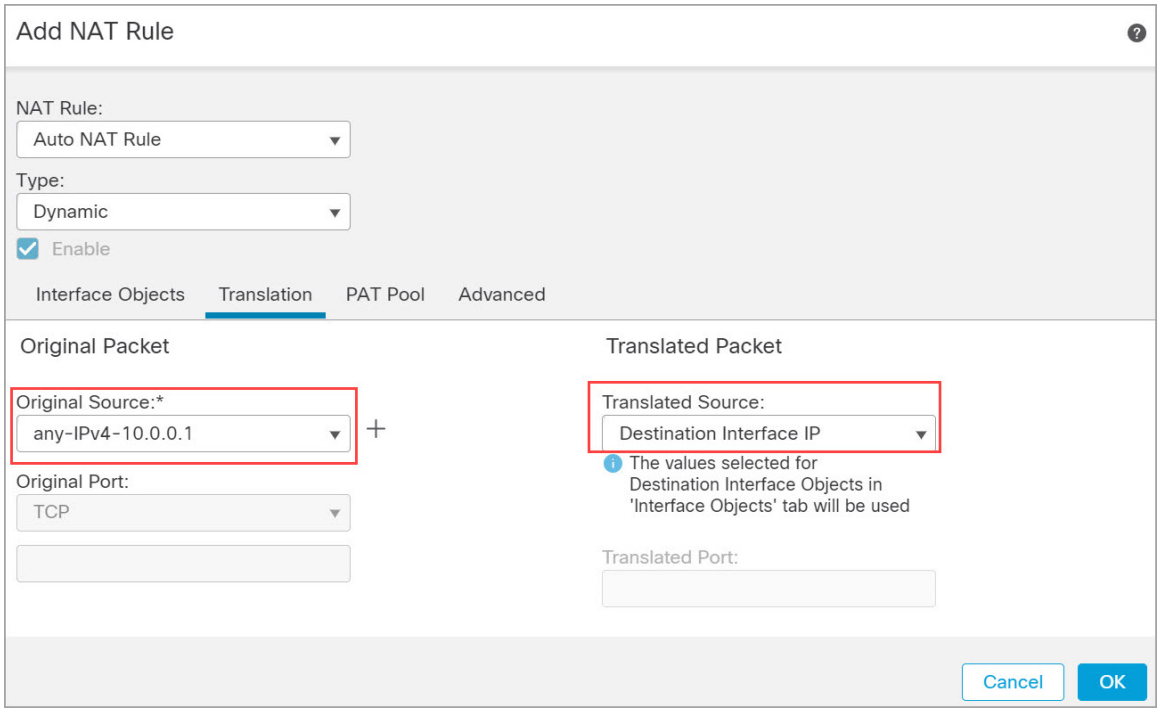



- [NATルール（NAT Rule）]：[自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

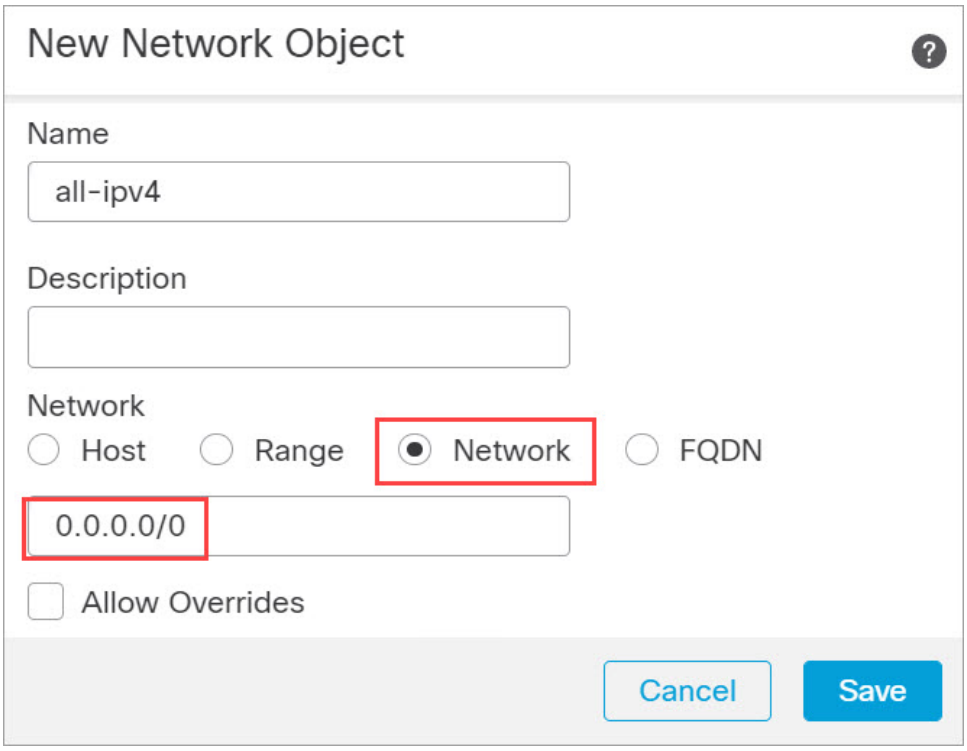
**ステップ 5** [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。




**ステップ 6** [変換（Translation）] ページで、次のオプションを設定します。




- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。



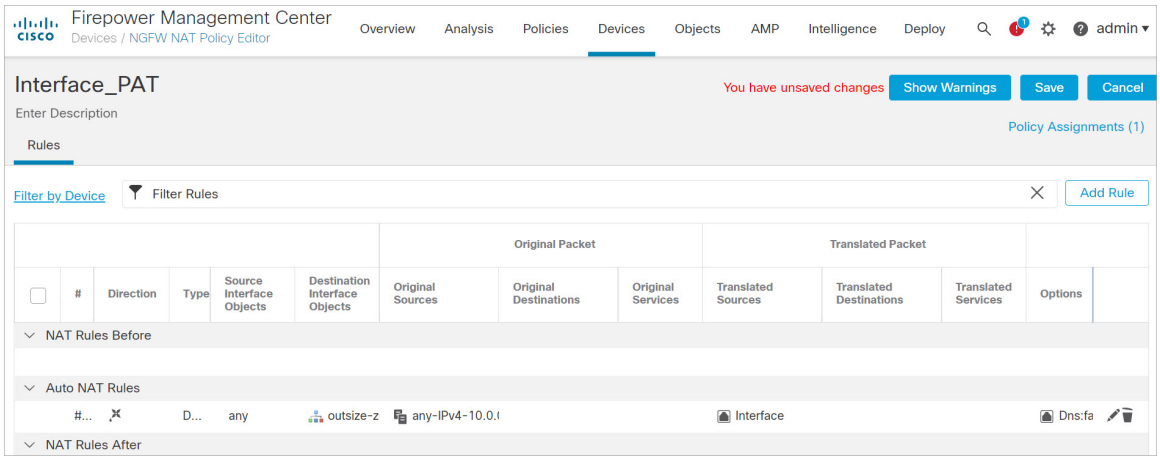

（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

同様に、すべての IPv6 トラフィックに対してデフォルトのホストネットワーク [::/0] を使用して NAT ポリシーを作成できます。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

**ステップ 7** [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。




**ステップ 8** NAT ページで [保存（Save）] をクリックして変更を保存します。

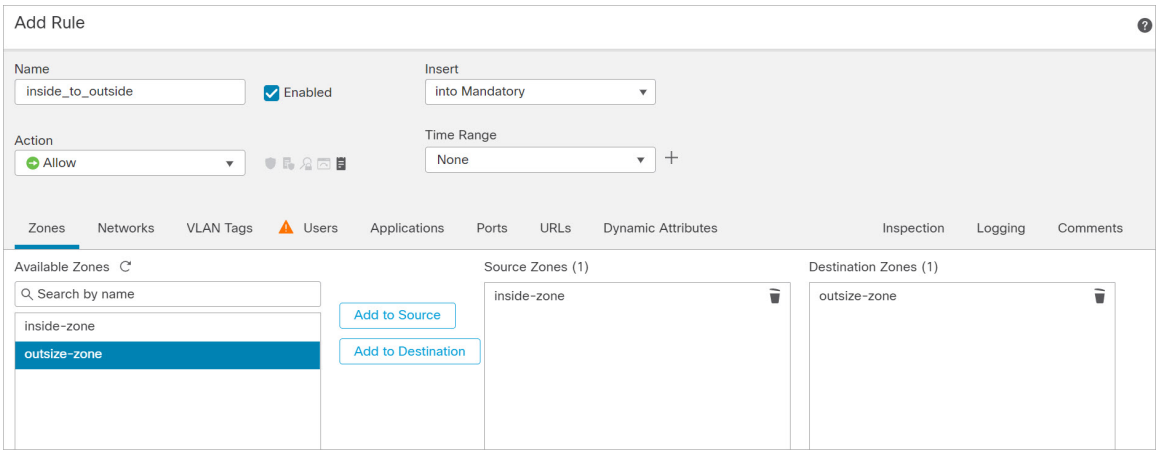
# アクセス制御の設定

Threat Defense Virtual を Management Center 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、Firepower Management Center コンフィギュレーション ガイド のコンフィギュレーション ガイドを参照してください。

**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、Threat Defense 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 [編集（Edit）]（✎）をクリックします。

**ステップ 2** **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

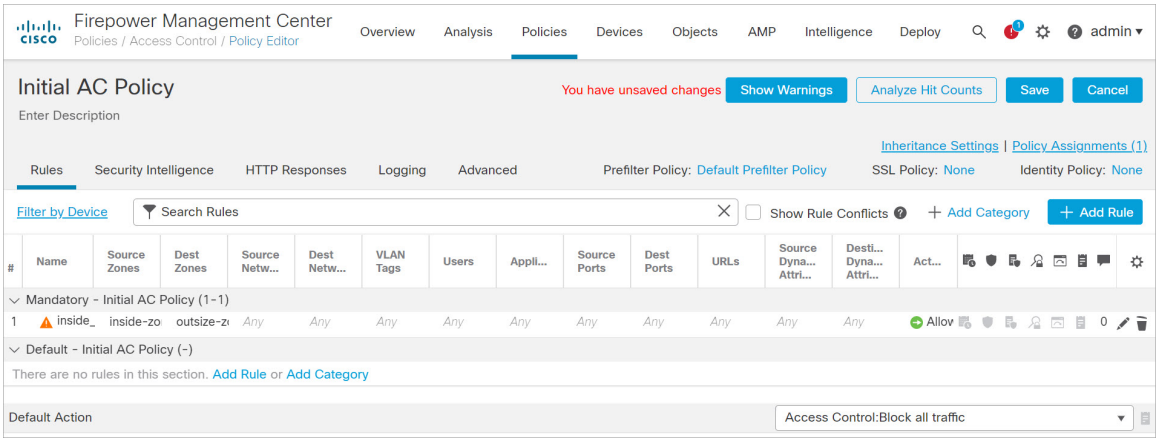



- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

**ステップ 3** [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。

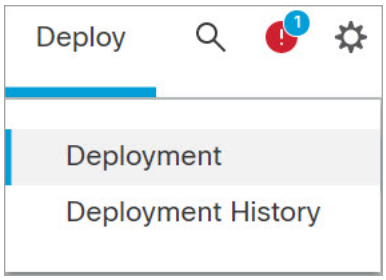



**ステップ 4** [保存（Save）] をクリックします。

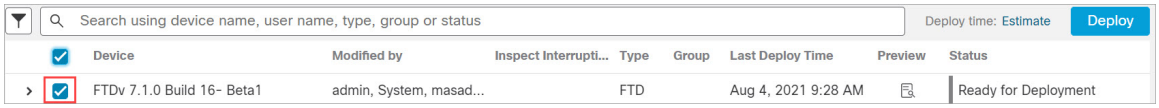
# 設定の展開

設定の変更を Threat Defense Virtual 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。

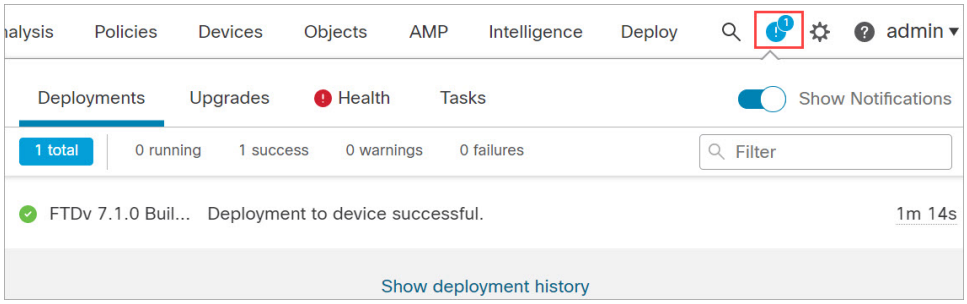
**ステップ 1** 右上の [展開（Deploy）] をクリックします。




**ステップ 2** [ポリシーの展開（Deploy Policies）] ダイアログボックスでデバイスを選択し、[展開（Deploy）] をクリックします。




**ステップ 3** 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。




# Secure Firewall Threat Defense CLI へのアクセス

Threat Defense Virtual 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。

**ステップ 1** （オプション 1）Threat Defense Virtual 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 Threat Defense Virtual にログインします。

**ステップ 2** （オプション 2）VMware コンソールを開き、初期展開時に設定したデフォルトのユーザー名「admin」アカウントとパスワードを使用して ログインします。

第 13 章

# Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理

この章では、Device Manager を使用して管理されるスタンドアロンの Threat Defense Virtual 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、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。


- Secure Firewall Device Manager を備えた Secure Firewall Threat Defense Virtual について （455 ページ）
- 初期設定 （456 ページ）
- Secure Firewall Device Manager でデバイスを設定する方法 （458 ページ）


## Secure Firewall Device Manager を備えた Secure Firewall Threat Defense Virtual について

Secure Firewall Threat Defense Virtual は、Cisco NGFW ソリューションの仮想化コンポーネントです。Threat Defense Virtual 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、マルウェア防御などの次世代ファイアウォールサービスを提供します。

一部の Threat Defense モデルに搭載された Web ベースのデバイス設定ウィザードである Secure Firewall Device Managerを使用して Threat Defense Virtual を管理できます。Device Manager 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 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 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。詳細については、「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理 （437 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 Threat Defense CLI にアクセスすることも、Device Manager の CLI から Threat Defense に接続することもできます。

# デフォルト設定

Threat Defense Virtual 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。

Threat Defense Virtual 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。
- 仮想マシン上の 2 番目のインターフェイス（Diagnostic 0-0）は、診断インターフェイスです。
- 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

Threat Defense Virtual 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。

- Device Manager Web インターフェイスの使用（推奨）。Device Manager 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）。Device Manager 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 Device Manager を使用します。「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。

# Device Manager の起動

Device Manager に初めてログインする際に、デバイス 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。

**ステップ 1** ブラウザを開き、Device Manager にログインします。CLI で初期設定を行っていない場合は、**https://FTDv pubic IPv4 address または [FTDv IPv6 pubic address]** で Device Manager を開きます。

**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 脅威に対する防御 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

- Device Manager を使用してデバイスを設定します。「Secure Firewall Device Manager でデバイスを設定する方法 （458 ページ）」を参照してください。

# Secure Firewall 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。

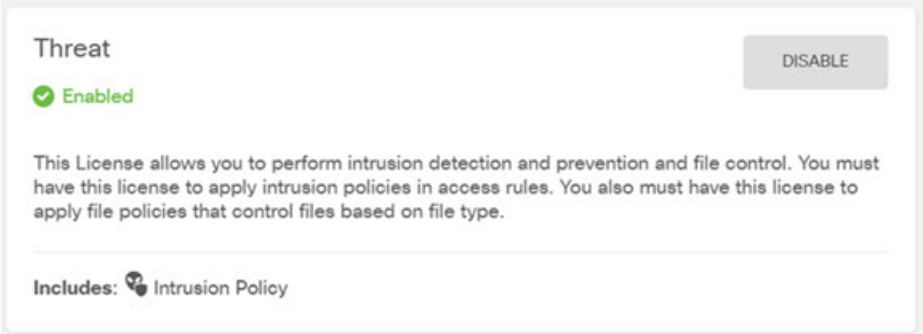
**ステップ 1** [デバイス（Device）] を選択してから、[スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

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

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

たとえば、有効なIPS ライセンスは次のようになります。

**図 *54 :* 有効な *IPS* ライセンス**

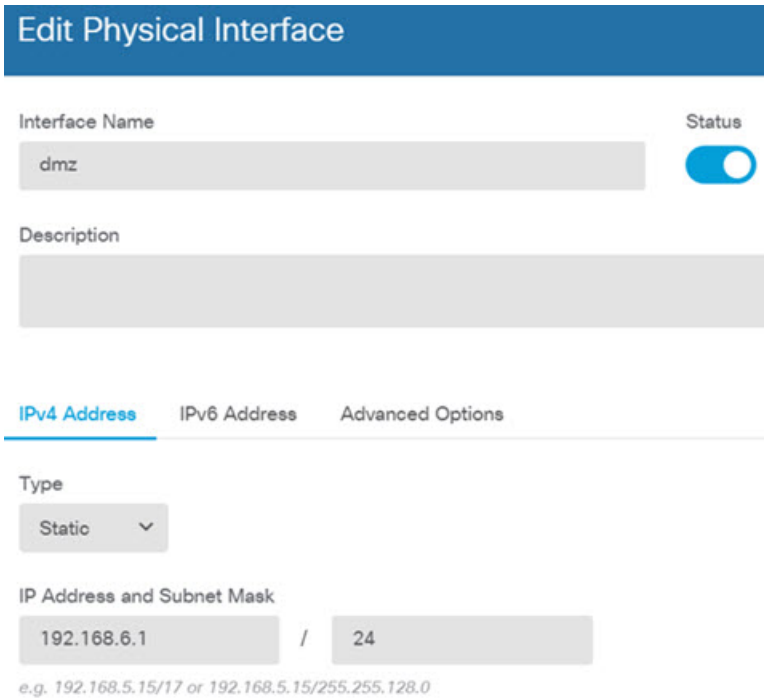



**ステップ 2** 他のインターフェイスを設定した場合は、[デバイス（Device）] を選択してから、[インターフェイス（Interfaces）] グループの [設定の表示（View Configuration）] をクリックして、各インターフェイスを設定します。

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

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

図 *55* : インターフェイスの編集




（注） IPv6 アドレスを有効にするには、[IPv6] タブを選択し、静的アドレスまたは DHCP を使用して IPv6 アドレスを設定します。

**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 *56* : セキュリティ ゾーン オブジェクト


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

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

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

図 *57* : *DHCP* サーバー

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

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 *58 :* デフォルトルート**


（注） 同様に、[IPv6] ラジオボタンを選択して、IPv6 ルートを設定できます。

**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。

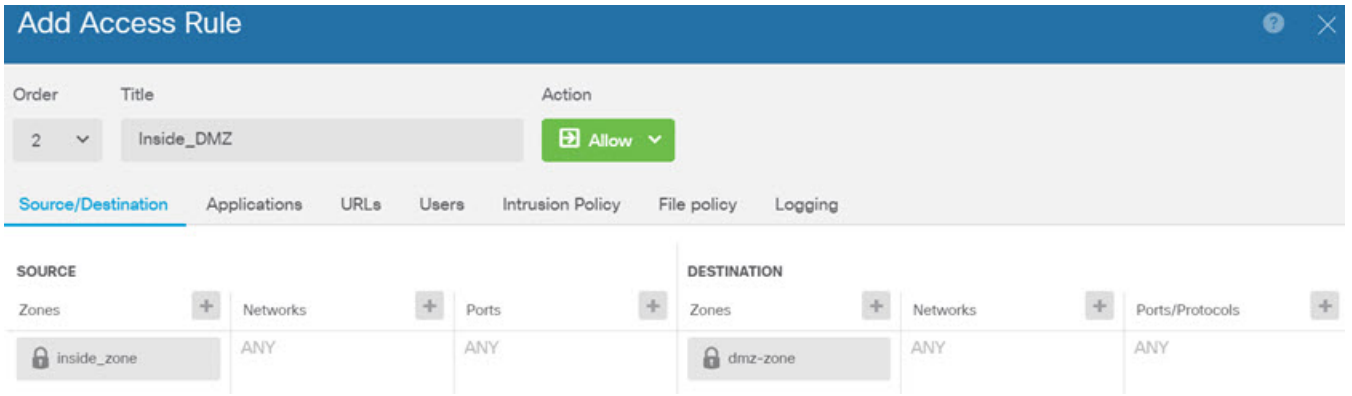
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

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 *59* : アクセス コントロール ポリシー




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

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

**ステップ 8** メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（ ）をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

### 次のタスク

Device Manager による 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 Secure Firewall Device Manager のオンラインヘルプを参照してください。

翻訳について
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。