OCI への Firewall Threat Defense Virtual の導入

Firewall 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、Firewall 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。Firewall 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 （1 ページ）
- エンドツーエンドの手順 （2 ページ）
- 前提条件 （4 ページ）
- 注意事項と制約事項 （5 ページ）
- ネットワークトポロジの例 （7 ページ）
- Cisco Secure Firewall Threat Defense Virtual デバイスの管理方法 （8 ページ）
- OCI 環境の構成 （10 ページ）
- OCI への Threat Defense Virtual の展開 （13 ページ）
- インターフェイスの接続 （15 ページ）
- 接続された VNIC のルートルールの追加 （16 ページ）
- SSH を使用した Firewall Threat Defense Virtual インスタンスへの接続 （16 ページ）
- OpenSSH を使用した Firewall Threat Defense Virtual インスタンスへの接続 （17 ページ）
- PuTTY を使用した Firewall Threat Defense Virtual インスタンスへの接続 （18 ページ）

概要

Cisco Secure Firewall Threat Defense Virtual は、物理的な Cisco Firewall 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。Firewall 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。Firewall Threat Defense Virtual は、次の OCI のシェイプタイプをサポートします。

表 *1 : x86* 展開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.Standard2.4	7.1、7.2.x、および 7.3.x	4	60	最小 4、最大 4
インテル VM.Standard2.8	7.1、7.2.x、および 7.3.x	8	120	最小 4、最大 8

（注） Flex コンピューティングシェーピングを使用することを推奨します。

（注） VM. Standard.A1.Flex シェイプの場合、1 OCPU は 1 vCPU に相当します。

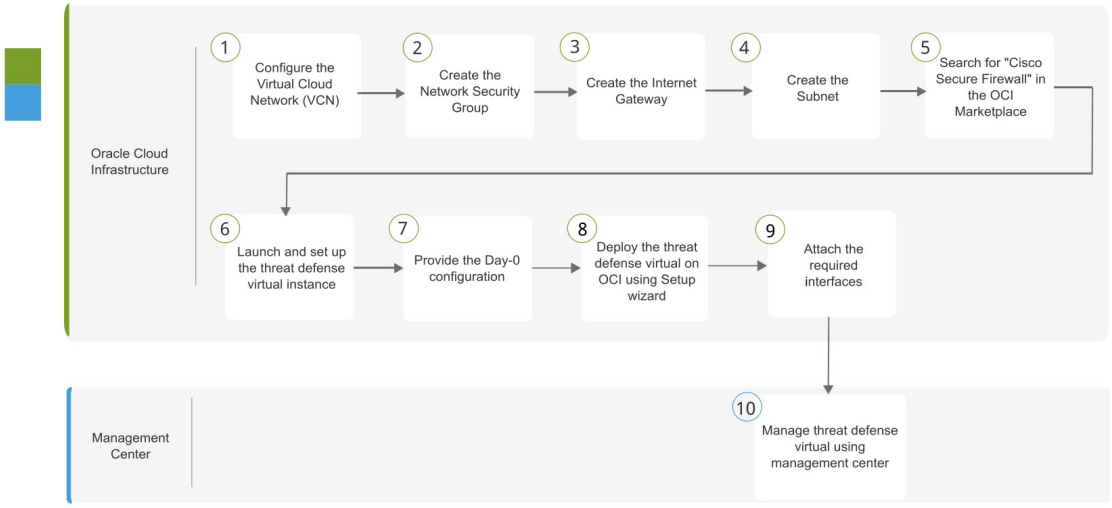
残りのコンピューティングシェイプでは、1 OCPU は 2 vCPU に相当します。

- *SR-IOV モードは、バージョン 7.4.x 以降、Flex シェイプでサポートされています。
- Firewall 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。

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 への Threat Defense Virtual の展開：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	OCI への Threat Defense Virtual の展開：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	OCI への Threat Defense Virtual の展開：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）]**）。
4	Oracle Cloud Infrastructure	OCI への Threat Defense Virtual の展開：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 （13 ページ） ：OCI Marketplace で「Cisco Secure Firewall」を検索します。

	ワークスペース	手順
6	Oracle Cloud Infrastructure	OCI への Threat Defense Virtual の展開 （13 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 （13 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 （13 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	OCI への Threat Defense Virtual の展開：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	Management Center を使用した 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。
- Firewall Threat Defense Virtual へのライセンス付与。
  - Firewall 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。
- 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 Firewall Threat Defense Virtual を Firewall 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） ：Firewall 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：
  - Firewall Threat Defense Virtual にアクセスするためのパブリック IP。

- Firewall Threat Defense Virtual のシステム要件については、『Cisco Secure Firewall Threat Defense 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
- Firewall 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

Firewall 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 *2 : Firewall 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

Firewall 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 Firewall 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

Firewall 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：Firewall 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。

展開

バージョン 7.4.3 以降を実行している Threat Defense 仮想インスタンスでは、最初の起動時にいくつかの初期化タスクが実行され、約 5 分後にコンソールが使用可能になります。この遅延は正常です。最初の起動から約 2 分以内にデバイスの電源がオフになっている場合、重要な初期化手順が中断され、セットアップが不完全になり予期しない動作をする可能性があります。

この問題を解決するには、新しいイメージを使用して仮想プラットフォームを再インストールする必要があります。

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、Firewall 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 Firewall 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

- Firewall Device Manager を介したローカル管理サポート。
- Firewall Threat Defense Virtual ネイティブ HA
- バージョン 7.0 以前の Auto Scale。
- 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
- IPv6

制限事項

- OCI に Firewall 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。
- 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、Firewall 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 Firewall Threat Defense Virtual の推奨トポロジを示しています。

図 *1 : 4* つの *VCN* のサブネットを使用した *OCI* への *Firewall Threat Defense Virtual* の展開の例

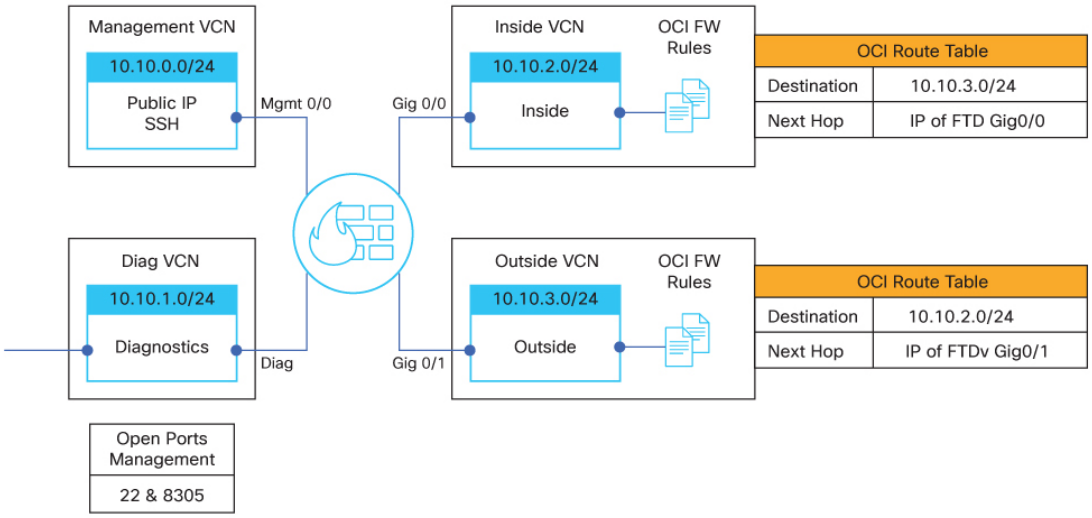
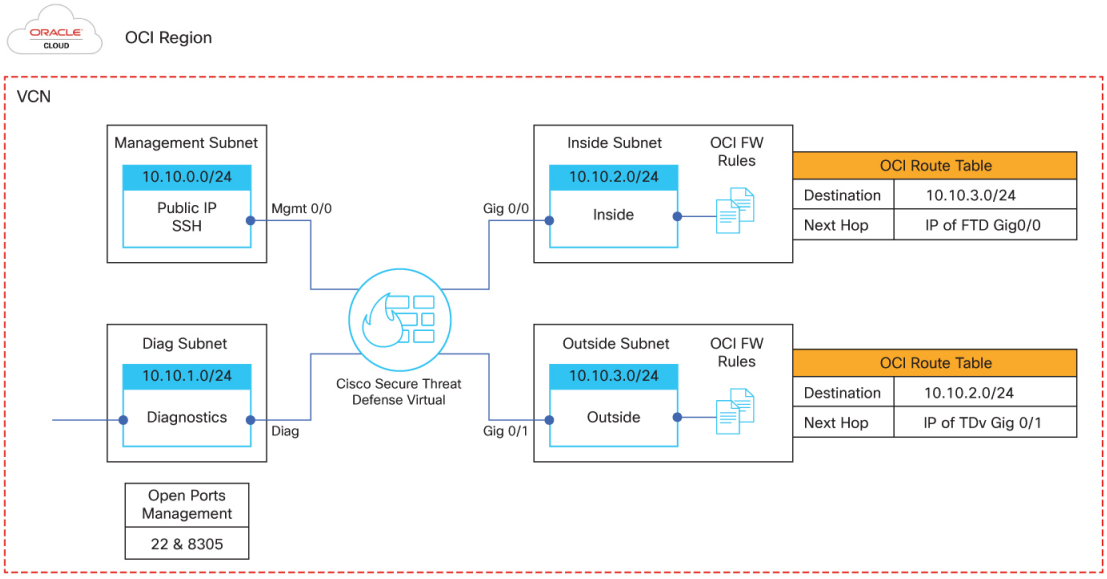


図 *2 : VCN* の *4* つのサブネットを使用した *OCI* への *Firewall Threat Defense Virtual* の展開の例



（注） 単一 VCN の 4 つのサブネットを使用している場合は、サブネットに固有のルートを、そのサブネットに関連付けられたルートテーブルに追加する必要があります。

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

Cisco Secure Firewall Threat Defense Virtual を管理するには、2 つのオプションがあります。

Cisco Secure Firewall Management Center

多数のデバイスを管理している場合、または Firewall 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 Firewall Device Manager の代わりに Firewall Management Center を使用してデバイスを設定します。詳細については、Cisco Secure Firewall Management Center を使用した Cisco Secure Firewall Threat Defense Virtual の管理を参照してください。

重要 Firewall Device Manager と Firewall Management Center の両方を使用して Firewall Threat Defense デバイスを管理することはできません。いったん Firewall 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、Firewall Management Center を使用するように管理を再設定しない限り、Firewall Management Center を使用して Firewall Threat Defense デバイスを管理することはできなくなります。一方、Firewall Threat Defense デバイスを Firewall Management Center に登録すると、Firewall 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 Firewall Device Manager の設定を Firewall 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。Firewall 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。

Cisco Secure Firewall Device Manager

Firewall Device Manager は、ほとんどの Firewall Threat Defense デバイス に含まれる Web インターフェイスです。これを使用して、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的な機能を構成できます。特に、多数のデバイスを含む大規模なネットワークを制御するためのデバイスマネージャを必要としない、1 台もしくは数台のデバイスを含むネットワークを対象としています。詳細については、Cisco Secure Firewall Device Manager を使用した Cisco Secure Firewall Threat Defense Virtual の管理を参照してください。

（注） Firewall Device Manager をサポートしているデバイスのリストについては、*Cisco Secure Firewall Threat Defense* 互換性ガイド を参照してください。

クラウド提供型 Firewall Management Center

クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense Virtual デバイスを一元管理できるクラウドベースの管理プラットフォームです。クラウド提供型 Firewall Management Center は、Cisco Secure Firewall Threat Defense Virtual バージョン 7.0.3、7.2.0 以降でサポートされています。詳細については、クラウド提供型 Firewall Management Center を使用した Cisco Secure Firewall Threat Defense Virtual の管理を参照してください。

重要 クラウド提供型 Firewall Management Center を Firewall Device Manager とともに使用しながら、同じ Cisco Secure Firewall Threat Defense Virtual デバイスを管理することはできません。

OCI 環境の構成

Threat Defense Virtual 展開用の仮想クラウドネットワーク（VCN）は、次のように設定できます。

- **複数の VCN**：少なくとも、Firewall 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。これにより、異なるネットワーク間で分離されたトラフィック検査が可能になります。
- **サブネットを持つ単一の VCN**：または、Threat Defense Virtual の各インターフェイスに 1 つずつ、合計 4 つのサブネットを持つ単一の VCN を設定できます。この設定では、同じ VCN 内のサブネット間のトラフィックを、関連付けられたルートテーブルを使用してファイアウォールで検査および制御できます。これにより、単一の VCN を使用しながらサブネット間トラフィックを効果的に管理できます。

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。

手順

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。

ステップ 5 **[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。

手順

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 8305 を許可するルールを追加します。

Firewall Threat Defense Virtual は Firewall 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。

手順

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) **[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。

g) **[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。

1 つの VCN を使用している場合は、VCN 内に管理サブネット、診断サブネット、内部サブネット、および外部サブネットを作成します。

手順

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。

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。

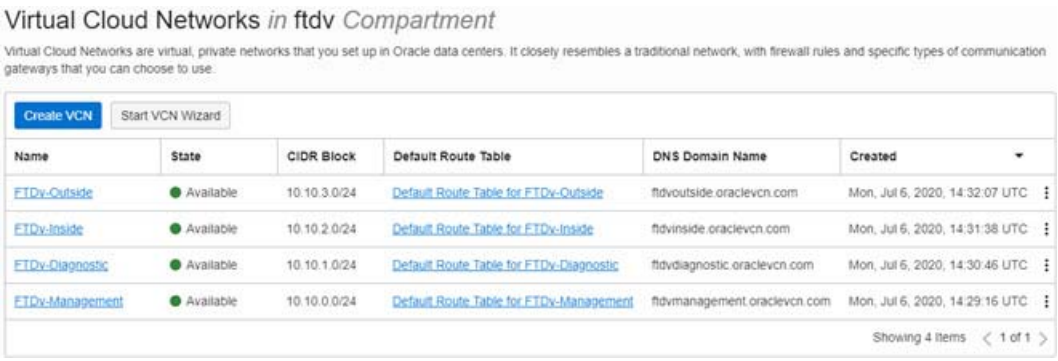
ステップ 8 以前作成した **[セキュリティリスト（Security List）]** を選択します。

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、Firewall Threat Defense Virtual を起動する準備が整います。Firewall 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 *3 : Firewall Threat Defense Virtual* 仮想クラウドネットワーク



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 Firewall 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。

手順

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、Firewall 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 （1 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、Firewall Threat Defense Virtual の day0 構成を指定します。day0 構成は、Firewall 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",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey": "cisco123reg",
"FmcNatId": "cisco123nat"
}
```

- **FmcRegKey**：これは、デバイスを Firewall 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 Firewall 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 Firewall 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。Firewall 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、Firewall 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

Firewall 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。Firewall Threat Defense Virtual が最初のブートを完了する前に、VNIC が Firewall 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。

手順

ステップ 1 新しく起動した Firewall 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。

手順

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。

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。

SSH を使用した Firewall 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 Firewall 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。

手順

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、Firewall 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 Firewall Threat Defense Virtual インスタンスへの接続

Windows システムから Firewall 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。

手順

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、Firewall 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 Firewall 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 Firewall 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。

手順

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、Firewall 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。

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。