Firepower Threat Defense Virtual の OCI への展開

FTDv 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、FTDv 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。FTDv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。

仮想クラウドネットワーク（VCN）の設定

FTDv 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、FTDv 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。

始める前に

（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『コンパートメントの管理（Managing Compartments）』を参照してください。

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。

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。

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 443 を許可するルールを追加します。

FTDv は Firepower 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 CIDR の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。

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**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。

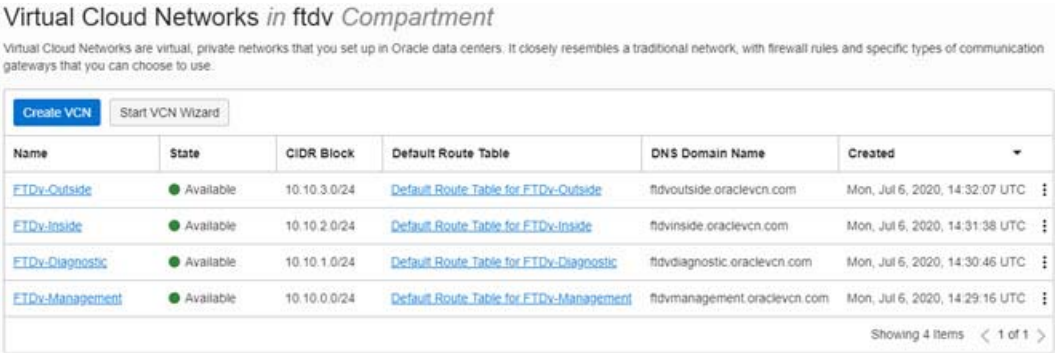
ステップ 8 以前作成した **[セキュリティリスト（Security List）]** を選択します。

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、FTDv を起動する準備が整います。FTDv VCN 構成の例については、次の図を参照してください。

図 *1: FTDv* 仮想クラウドネットワーク



OCI 上の FTDv インスタンスの作成

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 FTDv 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、FTDv 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（OCI への FTDv の展開についてを参照）。

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、FTDv の day0 構成を指定します。day0 構成は、FTDv 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 Firepower 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（ユーザが定義）。ただし、センサーと Defense 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 FTDv インスタンスをモニタします。

重要 ステータスをモニタすることが重要です。FTDv 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、FTDv ブート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

FTDv 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。FTDvが最初のブートを完了する前に、VNICがFTDv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 FTDv 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。