GCP 上の Firepower Threat Defense Virtual の展開

Google Cloud Platform（GCP）上で FTDv 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、FTDv 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、FTDv インスタンスを起動して FTDv を展開する方法について説明します。

VPC ネットワークの作成

FTDv の展開には、FTDv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、FTDv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、FTDv 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、「GCP 上の FTDv のネットワークトポロジの例（Sample Network Topology for FTDv on GCP）」 を参照してください。

手順

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

FTDv 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（FMCとの SSH および SFTunnel 通信を許可するため）。GCP 上の FTDv インスタンスの作成 （3 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。

手順

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。

GCP 上の FTDv インスタンスの作成

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 FTDv インスタンスを展開できます。

手順

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）]**：FTDvを展開するゾーンを選択します。

c) **[マシンタイプ（Machine type）]**：GCP マシンタイプのサポート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、FTDv 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、FMC 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。