Firepower Threat Defense Virtual の展開

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

- Firepower Threat Defense Virtual インスタンスの展開 （1 ページ）

Firepower 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 Firepower Threat Defense Virtual のインスタンスに使用できることを確認します。

手順

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、Firepower 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 Firepower Threat Defense Virtual でサポートされている [インスタンスタイプ（Instance Type）] を選択します（c4.xlarge を推奨）。

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。
- [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） Firepower 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。

Firepower Management Center を使用して FTDv を管理するためのログイン設定の例：

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

Firepower Device Manager を使用して FTDv を管理するためのログイン設定の例：

```
#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。

デフォルトを受け入れることも、ボリュームを変更することもできます。

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。このインターフェイスが Firepower Threat Defense Virtual インスタンスの 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。このインターフェイスが Firepower Threat Defense Virtual インスタンスの 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、Firepower 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、Firepower Threat Defense Virtual を Firepower Management Center に登録できるようになります。

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、Firepower Management Center を使用して FTDv を管理します。「Firepower Management Center を使用した Firepower Threat Defense Virtual の管理」を参照してください。
- [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 Firepower Device Manager を使用して FTDv を管理します。「Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Firepower デバイスの管理方法」を参照してください。