Firepower Threat Defense Virtual と AWS の利用開始

Amazon Virtual Private Cloud（VPC）は、お客様が定義する仮想ネットワークで Amazon Web Services（AWS）のリソースを起動できるようにします。この仮想ネットワークは、お客様自身のデータセンターで運用されている可能性がある従来型のネットワークとよく似ているだけでなく、AWS のスケーラブルなインフラストラクチャを活用するというメリットがあります。

このドキュメントでは、AWS に Firepower Threat Defense Virtual を展開する方法について説明します。

FTDv および AWS クラウドについて

AWS はパブリッククラウド環境です。Firepower 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。

（注） 次の表に示すように、Firepower バージョン 6.6 では C5 インスタンスタイプのサポートが追加されています。インスタンスが大きくなるほど、AWS VM により多くの CPU リソースが提供され、パフォーマンスが向上し、さらに多くのネットワークインターフェイスが実現します。

表 *1 : FTDv* の *AWS* サポートインスタンス

インスタンス タイプ	vCPU	メモリ（RAM）	vNIC
C5.xlarge	4	8 GB	4

インスタンス タイプ	vCPU	メモリ（RAM）	vNIC
C 5.2 xlarge	8	16 GB	4
C5.4xlarge	16	32 GB	8
C4.xlarge	4	7.5 GB	4
C3.xlarge	4	7.5 GB	4

Firepower デバイスの管理方法

Firepower Threat Defense 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。

Firepower Device Manager

Firepower Device Manager（FDM）オンボード統合マネージャ。

FDM は、一部の Firepower Threat Defense デバイスに組み込まれている Web ベースの設定インターフェイスです。FDM 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 Firepower 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） FDM をサポートしている Firepower Threat Defense デバイスのリストについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』を参照してください。

Firepower Management Center

Cisco Firepower Management Center（FMC）。

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

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

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、Firepower Management Center Virtual および Firepower 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。

Firepower Threat Defense Virtual の前提条件

- Amazon アカウント。http://aws.amazon.com/ では 1 つ作成できます。
- FTDv コンソールにアクセスするには、SSH クライアント（Windows 場合の PuTTY、Macintosh の場合はターミナルなど）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/
- Firepower Threat Defense Virtual のライセンス。

- Firepower 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。
- ライセンスを管理する方法の詳細については、『Firepower Management Center Configuration Guide』の「Licensing the Firepower System」を参照してください。

- Firepower 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 Firepower Threat Defense Virtual を Firepower Management Center に接続するために使用され、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。

    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 FMC 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の FMC アクセスは、ハイアベイラビリティ展開ではサポートされません。FMC アクセスに対する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、『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）：Firepower 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：
  - Firepower Threat Defense Virtual にアクセスするためのパブリック IP または Elastic IP。

サポートされる機能およびコンポーネント

サポートされる機能

- 仮想プライベート クラウド（VPC）への展開
- 拡張ネットワーク（SR-IOV）（使用可能な場合）
- Amazon マーケットプレイスからの展開
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザ展開
- 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

Firepower Threat Defense Virtual の制限事項

- 推奨されるインスタンスは c4.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） Firepower Threat Defense Virtual は、4 つのインターフェイスがないと起動しません。

- 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 アドレス設定は（CLI から設定したものでも Firepower 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。
- Firepower Threat Defense Virtual を登録した後、インターフェイスを編集し、Firepower 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。
- IPv6 は現時点でサポートされていません。
- 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場合、以下のようにして、AWS コンソールから変更を行う必要があります。
  - Firepower Management Center から登録を解除します。
  - AWS AMI ユーザ インターフェイス経由でインスタンスを停止します。
  - AWS AMI ユーザ インターフェイス経由で、変更するインターフェイスを切り離します。
  - 新しいインターフェイスを接続します（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を起動する必要があることを念頭に置いてください）。
  - AWS AMI ユーザ インターフェイス経由でインスタンスを開始します。
  - Firepower Management Center に再登録します。
  - Firepower 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 アドレスおよび他のパラメータを変更します。
- 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。
- 複製/スナップショットは現時点でサポートされていません。

AWS 環境の設定

Firepower 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、Firepower 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。

はじめる前に

- AWS アカウントを作成します。
- 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。

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。Firepower Management Center Virtual インスタンスや Firepower Threat Defense Virtual インスタンスなどの AWS リソースを VPC で起動できます。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。

手順

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 を識別するユーザ定義の [Nameタグ（Name tag）]。

b) IP アドレスの [CIDRブロック（CIDR block）]。 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) [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

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

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

手順

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 ユーザ定義の [Name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

Firepower Threat Defense Virtual 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。Firepower Threat Defense Virtual の場合、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

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

手順

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定義の [Name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）]。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。

手順

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定義の [Name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 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。

手順

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） Firepower 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、Firepower Management Center Virtual と Firepower 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

静的 IP アドレスを使用して、Firepower Threat Defense Virtual のネットワーク インターフェイスを作成できます。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。

手順

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。Firepower 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。**自動割り当て**ではなく、スタティック IP アドレスを使用することが推奨されています。

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 [はい、作成します（Yes, Create）] 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 [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。

ステップ 9 [無効（Disable）] を選択します。作成したすべてのネットワーク インターフェイスについて、この操作を繰り返します。

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、Firepower 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、Firepower 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。

手順

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

次のセクションの説明に従い、Firepower Threat Defense Virtual を展開します。