Cisco FirePOWER Threat Defense Virtual for the AWS Cloud クイック スタート ガイド

初版:2016 年 3 月 21 日

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。

AWS クラウドへの展開の概要

AWS は、プライベート Xen ハイパーバイザを使用するパブリック クラウド環境です。Firepower Threat Defense Virtual は、Xen ハイパーバイザの AWS 環境内でゲストとして実行されます。

AWS 上の Firepower Threat Defense Virtual は、次のインスタンス タイプを使用する必要があります。

- c3.xlarge:4 つの vCPU、7.5 GB、2 つのインターフェイス、1 つの管理インターフェイス

注: Firepower Threat Defense Virtual は AWS 環境外部の Xen ハイパーバイザをサポートしていません。

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。aws.amazon.com [英語]で作成できます。
- Cisco スマート アカウント。Cisco Software Central（https://software.cisco.com/ [英語]）で作成できます。
- Firepower Threat Defense Virtual へのライセンス付与。Firepower Threat Defense Virtual にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。
  - 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）：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/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

- サポートされる唯一のインスタンスは、c3.xlarge です。
- 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 はこの 4 つのインターフェイスがなければ起動しません。
- 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、AWS の使用開始ドキュメント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。

- VPC の作成（4 ページ）
- インターネット ゲートウェイの追加（4 ページ）
- サブネットの追加（5 ページ）
- ルート テーブルの追加（5 ページ）
- セキュリティ グループの作成（6 ページ）
- ネットワーク インターフェイスの作成（7 ページ）
- Elastic IP の作成（7 ページ）

始める前に:

- AWS アカウントを作成します。
- AMI を Firepower Threat Defense Virtual 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

1. aws.amazon.com [英語]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。
2. [サービス（Services）] > [VPC] の順にクリックします。
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。
4. [VPC の作成（Create VPC）] をクリックします。
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。
6. [はい、作成します（Yes, Create）] をクリックして、VPC を作成します。

次の作業

- 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。

始める前に：

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

手順

1. [サービス（Services）] > [VPC] の順にクリックします。
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。
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。
4. 前のステップで作成したゲートウェイを選択します。

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。
6. [はい、作成します(Yes, Create)] 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。

次の作業

- 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。

始める前に:

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

手順

1. [サービス(Services)] > [VPC] の順にクリックします。
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。
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。
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。
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。

次の作業

- 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

1. [サービス(Services)] > [VPC] の順にクリックします。
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。
3. ルート テーブルを識別するユーザ定義の [Name タグ(Name tag)]。
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。
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。
6. 作成したルート テーブルを選択します。
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。
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。
9. [保存(Save)] をクリックします。

次の作業

- 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。AWS では、セキュリティ グループにまだ精通していないお客様のために、この機能に関する詳しい資料を用意しています。

手順

1. [サービス(Services)] > [EC2] の順にクリックします。
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。
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。
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、次のものを入力します。
   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。
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。

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。

次の作業

- 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

1. [サービス(Services)] > [EC2] の順にクリックします。
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。
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。
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、静的 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。
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。
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。
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。
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。
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。

次の作業

- 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。AWS では、Elastic IP にまだ精通していないお客様のために、この機能に関する詳しい資料を用意しています。

(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 2 つの Elastic IP アドレスを作成してください。

手順

1. [サービス(Services)] > [EC2] の順にクリックします。
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。
3. [新規アドレスの割り当て(Allocate New Address)] をクリックします。

   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。
4. [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。
5. 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。

次の作業

- 次のセクションで説明されているように、Firepower Threat Defense Virtual を展開します。

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(3 ページ)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 インスタンスで使用できることを確認します。

手順

1. https://aws.amazon.com/marketplace [英語](Amazon マーケットプレイス)に移動して、サインインします。
2. Amazon マーケットプレイスにログインしたら、Firepower Threat Defense Virtual 用の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。
3. [続行(Continue)] をクリックしてから、[手動開始(Manual Launch)] タブをクリックします。
4. [条件に同意する(Accept Terms)] をクリックします。
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。
6. Firepower Threat Defense Virtual でサポートされる [インスタンス タイプ(Instance Type)] である c3.xlarge を選択します。
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)] の下の [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。
   - 前に作成した ***eth0*** に使用される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。(注)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。その場合、インスタンスを終了して、作成し直す必要があります。

ログイン設定の例:

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<Your_hostname>",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>",
}
```

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。

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。

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。

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。

12. [確認して起動する(Review and Launch)] をクリックします。

13. [起動(Launch)] をクリックします。

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。

15. [インスタンスの起動(Launch Instances)] をクリックします。

16. [起動の表示(View Launch)] をクリックし、プロンプトに従います。

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。

18. AWS 環境の設定(3 ページ)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。これは、Firepower Threat Defense Virtual インスタンス上の ***eth2*** インターフェイスになります。

19. AWS 環境の設定(3 ページ)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。これは、Firepower Threat Defense Virtual インスタンス上の ***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が設定されている必要があります。そうしないと、Firepower Threat Defense Virtual はブート プロセスを完了しません。

20. [EC2 ダッシュボード(Dashboard)] > [インスタンス(Instances)] の順にクリックします。

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)おそらく接続の問題に関する警告が表示されます。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。

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。

ポリシーとデバイス設定の設定

Firepower Threat Defense Virtual をインストールして、デバイスを Firepower Management Center に追加した後、Firepower Management Center ユーザ インターフェイスを使用して、AWS 上で実行する Firepower Threat Defense Virtual のデバイス管理設定の設定や、アクセス制御ポリシーおよび Firepower Threat Defense Virtual インスタンスを使用してトラフィックを管理するその他の関連ポリシーの設定と適用を行うことができます。

セキュリティ ポリシーは、Next Generation IPS のフィルタリングやアプリケーションのフィルタリングなど、FirePOWER Threat Defense Virtual で提供されるサービスを制御します。Firepower Management Center を使用して、Firepower Threat Defense Virtual 上でセキュリティ ポリシーを設定します。セキュリティ ポリシーの設定方法の詳細は、『*FireSIGHT System User Guide*』、または Firepower Management Center のオンライン ヘルプを参照してください。