AWS の既存の VPC への Threat Defense Virtual の展開

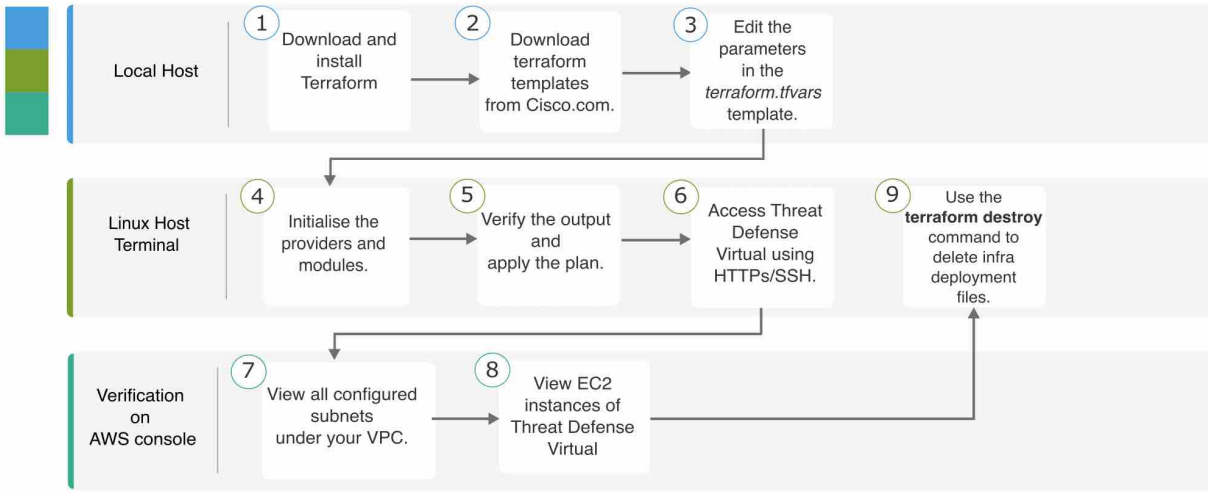
初版：2024 年 1 月 11 日

はじめに

このドキュメントでは、Terraform スクリプトを使用して Cisco Secure Firewall Threat Defense Virtual およびその他のネットワークコンポーネントを AWS に展開する手順について説明します。この手順では、AWS アカウントの既存の VPC 内に必要なすべてのリソースを作成します。新しい VPC で Threat Defense Virtual を AWS に展開する場合は、AWS の新しい VPC への Threat Defense Virtual の展開 [英語] を参照してください。

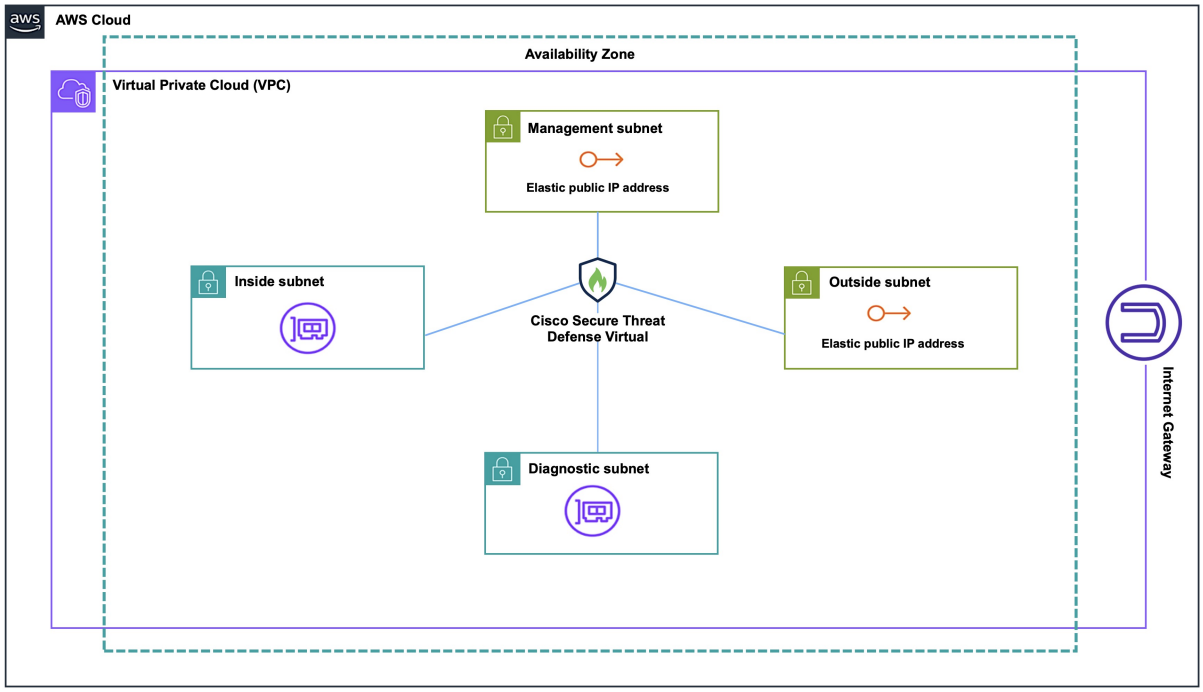
エンドツーエンドのプロセス

次のフローチャートは、AWS の既存の VPC に Threat Defense Virtual を展開するためのワークフローを示しています。



トポロジの例

次のネットワークトポロジが AWS に展開されています。



前提条件

- ローカルマシンに Terraform をダウンロードしてインストールします。詳細については、「Install Terraform」を参照してください。
- VPC および EC2 インスタンスを作成するための適切な権限を持つ AWS アカウント。詳細については、「Amazon VPC policy examples」を参照してください。

手順

AWS アカウントにすでに存在する VPC に必要なインフラストラクチャを展開するには、次の手順を実行します。

手順

ステップ 1 ここから Terraform スクリプトをダウンロードします。

ステップ 2 zip ファイルを解凍し、フォルダを開きます。

ステップ 3 コードエディタまたは「vim」を使用して **terraform.tfvars** ファイルを開き、入力します。

ステップ 4 二重引用符で囲まれたスペースに **aws_access_key**、**aws_secret_key**、および **region** を追加します。たとえば、**region = “us-east-1”** のようになります。アカウントのアクセスキーとシーク

レットアクセスキーを取得する方法については、「Managing access keys for IAM users」を参照してください。

ステップ 5 必要に応じて、**admin_password** フィールドに admin のパスワードを追加します。デフォルトのパスワードは Admin123 です。

ステップ 6 必要に応じて、**"FTD_version"** フィールドで Threat Defense Virtual のバージョンを変更します。

ステップ 7 **vpc_name** および **vpc_cidr** フィールドに VPC の名前と CIDR ブロックを入力します。

ステップ 8 VPC にインターネットゲートウェイが接続されていない場合は、**create_igw** フィールドを **true** に設定します。それ以外の場合は、**false** に設定します。

ステップ 9 4 つの異なるサブネット（**mgmt_subnet, outside_subnet, inside_subnet**、および **diag_subnet**）に適切なサブネット CIDR ブロックを入力します。

（注） 競合の可能性を回避するために、VPC にまだ存在しないサブネット CIDR のみを追加するようにしてください。

ステップ 10 **ftd01_mgmt_ip, ftd01_outside_ip, ftd01_inside_ip** および **ftd01_diag_ip** フィールドに、それぞれのサブネットの CIDR ブロックに対応するプライベート IP アドレスを入力します。

ステップ 11 次のコマンドを使用して、プロバイダーとモジュールを初期化します。

```
terraform init
```

ステップ 12 次のコマンドを使用して、Terraform プランを送信します。

```
terraform plan --out filename
```

ステップ 13 ターミナルでプランの出力を確認し、次のコマンドを使用してプランを適用します。

```
terraform apply filename
```

ステップ 14 Terraform の出力には、管理インターフェイスの IP アドレスと、ファイアウォールに SSH 接続するコマンドが表示されます。それらを使用し、HTTPS/SSH を介して Threat Defense Virtual にアクセスします。

ステップ 15 展開が完了したら、AWS コンソールを開きます。指定したリージョンに移動し、最終的な設定を検証します。

a) [サービス（Service）] > [VPC] の順に選択して、VPC の下に設定されているすべてのサブネットを表示します。

b) [サービス（Service）] > [EC2] の順に選択して、Cisco Threat Defense Virtual という名前の Threat Defense Virtual の EC2 インスタンスを表示します。

（注） **.terraform** フォルダと **terraform.tfstate** ファイルはクリーンアッププロセスに必要なため、削除しないでください。

クリーンアップ

AWS アカウントに関する不要な課金を防ぐために、不要になったインフラストラクチャの展開は削除することを推奨します。

Terraform によって作成されたインフラストラクチャ展開を削除するには、**terraform apply** コマンドを入力したディレクトリと同じディレクトリから **terraform destroy** コマンドを入力します。

```
terraform destroy
Type "yes" to delete the infrastructure deployment.
```

（注） **terraform destroy** コマンドでは、AWS アカウントで手動で設定した内容は削除されません。

コマンドを入力後、すべてのリソースが AWS アカウントから削除されていることを確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。