

Deploy Threat Defense Virtual in a New VPC on Azure

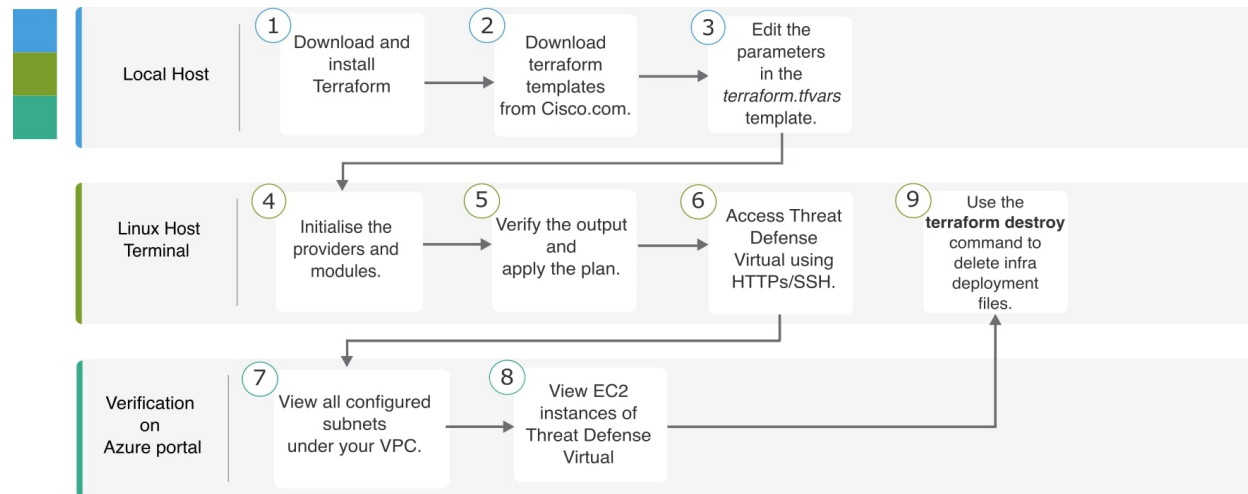
First Published: 2024-02-08

Introduction

This document describes the procedure of deploying Cisco Secure Firewall Threat Defense Virtual and other network components on Azure using a terraform script.

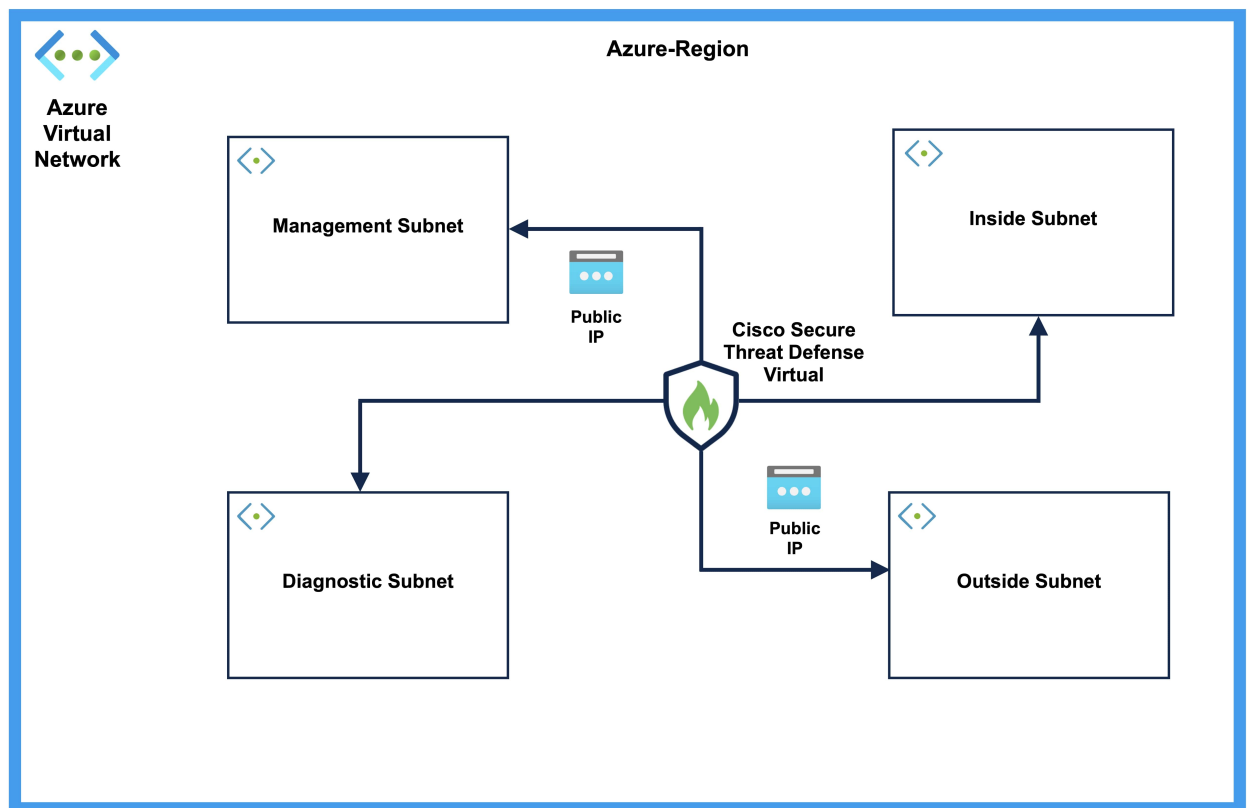
End-to-End Process

The following flowchart illustrates the workflow for deploying Threat Defense Virtual in a new VPC on Azure.



Sample Topology

The following network topology is deployed on Azure.



Prerequisites

- Download and install Terraform on your local machine. For more information, see [Install Terraform](#).
- An Azure account with proper permissions for creating networks and virtual machines (VMs). For more information, see [Assign Azure roles using the Azure portal](#).
- On your local system, ensure that you have logged in using the Azure Command Line Interface (CLI). For more information, see [Get started with Azure CLI](#).

Procedure

Perform the following steps to deploy the required infrastructure in a new VPC.

Procedure

-
- Step 1** Download the terraform scripts from [here](#).
 - Step 2** Extract the zip file and open the folder.
 - Step 3** Open the `terraform.tfvars` file by using a code editor or `vim` and provide inputs.

- Step 4** Add a **prefix** and **location** in the space provided between the double quotes. You have to append a prefix for each new resource.
- Step 5** Optionally, add a password for admin in the **ftd_password** field. By default, the password is Admin123.
- Step 6** If required, change the version of the Threat Defense Virtual in the "**ftd_image_version**" field.
- Step 7** Initialize the providers and modules by using the following command:
- ```
terraform init
```
- Step 8** Submit the terraform plan by using the following command:
- ```
terraform plan --out filename
```
- Step 9** Verify the output of the plan in the terminal and then apply the plan by using the following command:
- ```
terraform apply filename
```
- Step 10** The terraform output displays the IP address of the management interface and the command to SSH into the firewall. Use these to access the Threat Defense Virtual over HTTPs/SSH.
- Step 11** Open the Azure portal after the deployment is complete. Go to your provided region and validate the final configuration.
- Go to **Service > VPC** to view all the configured subnets under your VPC.
  - Go to **Service > EC2** to view the EC2 instance of Threat Defense Virtual with the name - Cisco Threat Defense Virtual.
- Note** Do not delete the **.terraform** folder and **terraform.tfstate** files as they are required for the clean-up process.
- 

## Clean-Up

We recommend that you delete the infrastructure deployment once it's not needed to prevent unnecessary billing on your Azure account.

To delete the infrastructure deployment that was created by terraform, enter the **terraform destroy** command from the same directory in which you entered the **terraform apply** command.

### **terraform destroy**

Type "yes" to delete the infrastructure deployment.

After entering the command, verify that all the resources are deleted from your Azure account.