Deploy the Firepower Threat Defense Virtual with the VHD

You can create your own custom Cisco Firepower Threat Defense Virtual images using a compressed VHD image available from Cisco. To deploy using a VHD image, you must upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image.

Before You Begin

- Obtain the JSON template and corresponding JSON parameters file for your Cisco Firepower Threat Defense Virtual custom template deployment.
- This procedure requires an existing Linux VM in Azure. We recommended you use a temporary Linux VM to upload the compressed VHD image to Azure. This image will require about 50G of storage when unzipped. Also, your upload times to Azure storage will be faster from a Linux VM in Azure.

  If you need to create a VM, use one of the following methods:

  - Create a Linux virtual machine with the Azure CLI
  - Create a Linux virtual machine with the Azure portal
- In your Azure subscription, you should have a storage account available in the Location in which you want to deploy the Cisco Firepower Threat Defense Virtual.

Procedure

1. Download the Cisco Firepower Threat Defense Virtual compressed VHD image from the Cisco Download Software page:

   a. Navigate to **Products** > **Security** > **Firewalls** > **Next-Generation Firewalls (NGFW)** > **Firepower NGFW Virtual**.

   b. Click **Firepower Threat Defense Software**.

   Follow the instructions for downloading the image.

   For example, Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2
2. Copy the compressed VHD image to your Linux VM in Azure.

   There are many options that you can use to move files up to Azure and down from Azure. This example shows SCP or secure copy.

   ```
   # scp /username@remotehost.com/dir/Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.
   bz2 <linux-ip>
   ```
3. Log in to the Linux VM in Azure and navigate to the directory where you copied the compressed VHD image.
4. Unzip the Firepower Threat Defense Virtual VHD image.

   There are many options that you can use to unzip or decompress files. This example shows the Bzip2 utility, but there are also Windows-based utilities that would work.

   ```
   # bunzip2 Cisco_Firepower_Threat_Defense_Virtual-6.2.3-81.vhd.bz2
   ```
5. Upload the VHD to a container in your Azure storage account. You can use an existing storage account or create a new one. The storage account name can only contain lowercase letters and numbers.

   There are many options that you can use to upload a VHD to your storage account, including AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI, or the Azure Portal. We do not recommend using the Azure Portal for a file as large as the Firepower Threat Defense Virtual VHD.

The following example shows the syntax using Azure CLI:

```
azure storage blob upload \
 --file <unzipped vhd> \
 --account-name <azure storage account> \
 --account-key yX7txxxxxxxx1dnQ== \
 --container <container> \
 --blob <desired vhd name in azure> \
 --blobtype page
```

6. Create a Managed Image from the VHD.

   c. In the Azure Portal, select **Images**.

   d. Click **Add** to create a new image.

   e. Provide the following information:

   - **Name**—Enter a user-defined name for the managed image.
   - **Subscription**—Choose a subscriptions from the drop-down list.
   - **Resource group**—Choose an existing resource group or create a new one.
   - **OS disk**—Select Linux as the OS type.
   - **Storage blob**—Browse to the storage account to select the uploaded VHD.
   - **Account type**—Choose Standard (HDD) from the drop-down list.
   - **Host caching**—Choose Read/write from the drop-down list.
   - **Data disks**—Leave at the default; don't add a data disk.

   f. Click **Create**.

   Wait for the **Successfully created image** message under the **Notifications** tab.

   Note: Once the Managed Image has been created, the uploaded VHD and upload Storage Account can be removed.

7. Acquire the **Resource ID** of the newly created Managed Image.

   Internally, Azure associates every resource with a Resource ID. You'll need the Resource ID when you deploy new Firepower Threat Defense Virtual firewalls from this managed image.

   a. In the Azure Portal, select **Images**.

   b. Select the managed image created in the previous step.

   c. Click **Overview** to view the image properties.

   d. Copy the **Resource ID** to the clipboard.

   The Resource ID takes the form of:
   /subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

8. Build a Firepower Threat Defense Virtual firewall using the managed image and a custom template:

   a. Select **New**, and search for **Template Deployment** until you can select it from the options.

   b. Select **Create**.

   c. Select **Build your own template in the editor**.

   You have a blank template that is available for customizing.

   d. Paste your customized JSON template code into the window, and then click **Save**.

   e. Choose a **Subscription** from the drop-down list.

   f. Choose an existing **Resource group** or create a new one.

   g. Choose a **Location** from the drop-down list.

   h. Paste the Managed Image **Resource ID** from the previous step into the **Vm Managed Image Id** field.

9. Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.

   a. Click **Load file** and browse to the customized Firepower Threat Defense Virtual parameters file.

   b. Paste your customized JSON parameters code into the window, and then click **Save**.

10. Review the Custom deployment details. Make sure that the information in **Basics** and **Settings** matches your expected deployment configuration, including the **Resource ID**.

11. Review the Terms and Conditions, and check the **I agree to the terms and conditions stated above** check box.

12. Click **Purchase** to deploy a Firepower Threat Defense Virtual firewall using the managed image and a custom template.

    If there are no conflicts in your template and parameters files, you should have a successful deployment.

    The Managed Image is available for multiple deployments within the same subscription and region.