Security Virtual Image

Cisco SD-WAN Manager uses a Security Virtual Image to enable security features such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) on Cisco IOS XE Catalyst SD-WAN Devices. These features enable application hosting, real-time traffic analysis, and packet logging on IP networks. Once the image file is uploaded to the Cisco SD-WAN Manager Software Repository, you can create policy, profile, and device templates that will push the policies and updates to the correct devices automatically.

Before you use these features, you must first install and configure IPS/IDS, URL-F, or AMP security policies, and then upload the relevant Security Virtual Image to Cisco SD-WAN Manager. After upgrading the software on the device, you must also upgrade the Security Virtual Image.

This chapter describes how to perform these tasks.

Install and Configure IPS/IDS, URL-F, or AMP Security Policies

Installing and configuring IPS/IDS, URL-F, or AMP security policies require the following workflow:

Task 1: Create a Security Policy Template for IPS/IDS, URL-F, or AMP Filtering

Task 2: Create a Feature Template for Security App Hosting

Task 3: Create a Device Template

Task 4: Attach Devices to the Device Template

Create a Security Policy Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** window, select your security scenario from the list of options.
4. Click **Proceed**.

Create a Feature Template for Security App Hosting

The feature profile template configures two functions:

- **NAT:** Enables or disables Network Address Translation (NAT), which protects internal IP addresses when outside the firewall.
- **Resource Profile:** Allocates default or high resources to different subnets or devices.

Note A feature profile template, while not strictly required, is recommended.

To create a feature profile template, follow these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. From the **Select Devices** list, choose the devices that you want to associate with the template.
4. Under **Basic Information**, click **Security App Hosting**.
5. Enter **Template Name** and **Description**.
6. Under **Security Policy Parameters**, customize the security policy parameters if required.
   - Enable or disable the Network Address Translation (NAT) feature, based on your use case. By default, **NAT** is on.
   - Click the drop-down arrow to set boundaries for the policy. The default is **Default**.

     Global: Enables NAT for all devices attached to the template.

     Device Specific: Enables NAT only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default NAT policy for devices attached to the template.
   - Set **Resource Profile**. This option sets the number of snort instances to be used on a router. The default is **Low** that indicates one snort instance. **Medium** indicates two instances and **High** indicates three instances.
   - Click the drop-down arrow to set boundaries for the resource profile. The default is **Global**.

     Global: Enables the selected resource profile for all devices attached to the template.

     Device Specific: Enables the profile only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default resource profile for devices attached to the template.
7. Set **Download URL Database on Device** to **Yes** if you want to download the URL-F database on the device. In this case, the device looks up in the local database before trying the cloud lookup.

8. Click **Save**.

Create a Device Template

To activate the policies you want to apply, you can create a device template that will push the policies to the devices that need them. The available options vary with the device type. For example, Cisco SD-WAN Manager devices require a more limited subset of the larger device template. You will see only valid options for that device model.

To create a security device template, follow this example for vEdge 2000 model routers:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then choose **Create Template** > **From Feature Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Device Model** drop-down list, choose the device model.
4. From the **Device Role** drop-down list, choose the device role.
5. Enter **Template Name** and **Description**.
6. Scroll down the page to the configuration submenus that let you select an existing template, create a new template, or view the existing template. For example, to create a new System template, click **Create Template**.

Attach Devices to the Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then choose **Create Template** > **From Feature Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. In the row of the desired device template, click **...** and choose **Attach Devices**.
4. In the **Attach Devices** window, select the desired devices from the **Available Devices** list, and click the right-pointing arrow to move them to the **Selected Devices** list.
5. Click **Attach**.

Identify the Recommended Security Virtual Image Version

At times, you may want to check the recommended Security Virtual Image (SVI) release number for a given device. To check this using Cisco SD-WAN Manager:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

Step 2 Choose **WAN – Edge**.

Step 3 Choose the device that will run the SVI.

The System Status page displays.

Step 4 Scroll to the end of the device menu, and click **Real Time**.

The System Information page displays.

Step 5 Click the **Device Options** field, and choose **Security App Version Status** from the menu.

Step 6 The image name is displayed in the **Recommended Version** column. It should match the available SVI for your router from the Cisco downloads website.

Upload the Cisco Security Virtual Image to Cisco SD-WAN Manager

Each router image supports a specific range of versions for a hosted application. For IPS/IDS and URL-Filtering, you can find the range of supported versions (and the recommended version) for a device on its Device Options page.

When a security policy is removed from Cisco IOS XE Catalyst SD-WAN devices, the Virtual Image or Snort engine is also removed from the devices.

Procedure

Step 1 From the Software Download page for your router, locate the image **`UTD Engine for IOS XE SD-WAN`**.

Step 2 Click **download** to download the image file.

Step 3 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**

Step 4 Choose **Virtual Images**.

Step 5 Click **Upload Virtual Image**, and choose either **Manager** or **Remote Server – Manager**. The **Upload Virtual Image to Manager** window opens.

Step 6 Drag and drop, or browse to the image file.

Step 7 Click **Upload**. When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

Upgrade a Security Virtual Image

When a Cisco IOS XE Catalyst SD-WAN device is upgraded to a new software image, the security virtual image must also be upgraded so that they match. If there is a mismatch in the software images, a VPN template push to the device will fail.

Note During the UTD Virtual image upgrade, the IPS signature file is installed with version 29.0C, which is the default packaging within the UTD tar container. If the IPS Signature Update option is enabled, the matching IPS signature package is automatically updated as a part of the upgrade. You can enable the setting from **Administration** > **Settings** > **IPS Signature Update**.

To upgrade the application hosting virtual image for a device, follow these steps:

Procedure

Step 1 Follow the steps in *Upload the Correct Cisco Security Virtual Image to Cisco SD-WAN Manager* to download the recommended version of the SVI for your router. Note the version name.

Step 2 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** > **Virtual Images** to verify that the image version listed under the **Recommended Version** column matches a virtual image listed in the Virtual Images table.

Step 3 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 4 Choose the devices you want to upgrade, and check the check boxes in the leftmost column. When you have chosen one or more devices, a row of options display, as well as the number of rows you chose.

Step 5 When you are satisfied with your choices, choose **Upgrade Virtual Image** from the options menu. The Virtual Image Upgrade dialog box displays.

Step 6 For each device you have chosen, choose the correct upgrade version from the **Upgrade to Version** drop-down menu.

Step 7 When you have chosen an upgrade version for each device, click **Upgrade**. When the update completes, a confirmation message displays.