

---

## Configuring the Security Virtual Image for IPS/IDS and URL Filtering

This section describes how to install, configure, activate, and update the Cisco SD-WAN Release 18.4 IPS/IDS and URL-F Security Policy Virtual Image.

Cisco release 18.4 supports intrusion prevention/intrusion detection systems (IPS/IDS) and URL filtering (URL-F) for IOS XE and IOS XE 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 vManage Software Repository, you can create policy, profile, and device templates that will push the policies and updates to the correct devices automatically.

The following router platforms support the 18.4 security virtual image:

- Cisco Integrated Service Router 4351 (ISR-4351)
- Cisco Integrated Service Router 4331 (ISR-4331)
- Cisco Integrated Service Router 4321 (ISR-4321)
- Cisco Integrated Service Router 4221 (ISR-4221X)
- Cisco Integrated Service Router 4431 (ISR-4431)
- Cisco Integrated Service Router 4451 (ISR-4451)
- Cisco Integrated Service Router 1111X-8P (ISR-1111X-8P)
- Cisco Cloud Services Router 1000v series

IPS/IDS and URL filtering is not supported on ASR platforms for this release.

To install and configure IPS/IDS and URL-F security policies for release 18.4 requires the following workflow:

- Task 1: Upload the Cisco security virtual image to vManage
- Task 2: Create a security policy template for IPS/IDS or URL filtering
- Task 3: Create a feature profile template for IPS/IDS or URL filtering
- Task 4: Create a device template
- Task 5: Attach devices to the device template

---

## Upload the Cisco Security Virtual Image to vManage

The IPS/IDS and URL-F feature set is contained within a TAR file, which can be downloaded from the Cisco website, and uploaded to your vManage software repository as a virtual image.

To download the security virtual image to your vManage software repository:

1. Go to <https://software.cisco.com/download/home> and sign on. The Software Download page displays.
2. Browse to Downloads ► Home ► Routers ► Branch Routers ► XE SD-WAN Routers.



3. From the right-most pane, select your router model. The Software Download page displays for your selected router.
4. From the list of software options, select “**UTD Snort IPS Engine Software.**”
5. From the list on the left-hand side, select an image option, such as Latest Release, or 18.4.x. The page will look similar to the following example. The correct file will begin with “**UTD Engine for...**”



6. Click the  
  
icon on the right-hand side of the window to download the image file.
7. From the vManage dashboard, select Maintenance ► Software Repository.
8. Select **Virtual Images** from the top options.
9. Click **Upload Virtual Image**, and select either **vManage** or **Remote Server – vManage**. The Upload Virtual Image to vManage window opens.
10. Drag and drop, or browse to the image file and select it (your image file will be different).
11. Click **Upload**. When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

---

## Create a Security Policy Template for IPS/IDS or URL-F

Once the image is uploaded, use the Add Security Policy configuration wizard to build your IPS/IDS or URL-F policies. For a complete description of this task, see “[Intrusion Prevention Configuration on SD-WAN](#).”

1. From the vManage dashboard, select Configuration ► Security.



2. Click **Add Security Policy**. The Add Security Policy wizard displays.
3. Select your security scenario from the list of options.

4. Select the scenario that most closely fits your needs, and click **Proceed**.

---

## Create a Feature Profile Template for IPS/IDS or URL-F

The feature profile template configures two functions:

- **NAT** – Enable or disable network address translation, which protects internal IP addresses when outside the firewall.
- **Resource Profile** – Allocate default or high resources to different subnets or devices.

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

To configure a security profile template for IPS/IDS or URL-F:

1. From the vManage dashboard, select Configuration ► Templates.
2. Click **Feature**.
3. Click **Add Template**. The add feature template page displays.
4. From the Select Devices list on the left, select the device(s) you want to associate with the template.
5. In the Select Template ► Basic Information section, click **Security App Hosting**. The Security App Hosting template



page displays.

6. Enter a name for the template in the Template Name field. Make it as descriptive as possible.
7. Optionally, enter a description of the template in the Description field. Scroll to the Security Policy Parameters section.
8. **NAT** – Click **On** to enable network address translation (NAT), or **Off** to disable it. By default, NAT is on.
9. Click the drop-down menu to set boundaries for the policy. The default is **Default**.
  - **Global** – Enable NAT for all devices attached to the template.
  - **Device Specific** – Enable NAT only for specified devices. If you select Device Specific, enter the name of a device key.
  - **Default** – Enable the default NAT policy for devices attached to the template.
10. **Resource Profile** – Choose Default or High to designate the resource profile for devices attached to this template. The default is High.
11. Click the drop-down menu to set boundaries for the resource profile. The default is **Global**.
  - **Global** – Enable the selected resource profile for all devices attached to the template.
  - **Device Specific** – Enable the profile only for specified devices. If you select Device Specific, enter the name of a device key.
  - **Default** – Enable the default resource profile for devices attached to the template.
12. When you have finished, click **Save**. The Feature Profile template displays in the Configuration ► Templates ► Feature page table.

---

## 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, vManage devices require a more limited subset of the larger device template. You will only see valid options for that device model. For information about other template options, see [Templates](#).



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

1. From the vManage dashboard, select Configuration ► Templates ► Device. The device configuration table displays.
2. Click Create Template ► From Feature Template. The add device template page displays.
3. Select the device model from the Select Devices list on the left. The device template page displays.
4. Enter a name for the template in the Template Name field.
5. Optionally, enter a description of the template in the Description field.
6. Scroll down the page to the four configuration sub-menus. Each field allows you to select an existing template, to create a new template, or to view the existing template. For example, to create a new System template, click **Create Template**.

Fields with an asterisk are required.

---

## Basic Information

7. **System** - Use the System template for all Cisco SD-WAN devices, to configure system-wide parameters using vManage templates. For a full description, see [System](#).
8. **Logging** - Use the Logging template for all SD-WAN devices, to configure logging to either the local hard drive or a remote host. For a full description, see [Logging](#).
9. Optionally, from the Additional System Templates section to the right, you can select templates stored in an archive or



NTP system. Click **Archive** or **NTP** to open a menu field where you can browse to the template file.

10. Select templates for the following protocols from the drop-down menus, or leave the defaults:

- **AAA** Authentication, Authorization, and Accounting - For AAA support, in combination with RADIUS and TACACS+. For a full description, see [AAA](#).
- **BFD** Bidirectional Forwarding Detection - The BFD protocol, which detects link failures as part of the Cisco high availability solution, is enabled by default on all vEdge routers, and you cannot disable it. For a full description, see [BFD](#).
- **OMP** Edge Overlay Management Protocol - Use OMP to establish and maintain the SD-WAN control plane. OMP is enabled by default on all SD-WAN vEdge routers, vManage NMSs, and vSmart controllers, so there is no need to explicitly configure or enable OMP. OMP must be operational for the Viptela overlay network to function. If you disable it, you disable the overlay network. For a full description, see [OMP](#).
- **Security** - On vEdge Cloud and vEdge routers and on vBond orchestrators, use this template to configure IPsec for data plane security. On vManage NMSs and vSmart controllers, use this template to configure DTLS or TLS for control plane security. For a full description, see [Intrusion Protection, Intrusion Detection, and URL Filtering](#)

---

## Transport and Management VPN

For a full description of VPN options, see [VPN](#).

The screenshot displays the 'Transport & Management VPN' configuration interface. It is divided into two main sections: 'VPN 0' and 'VPN 512'. Each section contains a dropdown menu for selecting a template and another dropdown menu for selecting a VPN interface. For VPN 0, the template is 'Factory\_Default\_vEdge\_VPN\_0\_Template' and the interface is 'Factory\_Default\_vEdge\_DHCP\_Tunnel\_Interfa...'. For VPN 512, the template is 'Factory\_Default\_vEdge\_VPN\_512\_Template' and the interface is 'Factory\_Default\_vEdge\_Management\_Interfa...'. To the right of these sections are two lists of 'Additional VPN 0 Templates' and 'Additional VPN 512 Templates'. The 'Additional VPN 0 Templates' list includes BGP, OSPF, VPN Interface, VPN Interface GRE, VPN Interface IPsec, and VPN Interface PPP. The 'Additional VPN 512 Templates' list includes VPN Interface. Each option in these lists has a radio button next to it.

10. From the Transport and Management VPN section, select templates for the following virtual private networks (VPNs) from the drop-down menus, or leave the defaults:

- **VPN 0** -- Transport VPN, which carries control traffic via the configured WAN transport interfaces. Initially, VPN 0 contains all of a device's interfaces except for the management interface, and all interfaces are disabled.

11. Optionally, from the Additional VPN 0 Templates section to the right, you can select templates for the following



protocols and interfaces:

- **BGP** Border Gateway Protocol
- **OSPF** Open Shortest Path First
- **VPN Interface** – Optionally, create templates for VPNs 1 through 511, and 513 through 65530.
- **GRE** VPN Interface Generic Routing Encapsulation
- **IPsec** VPN Interface IPsec - IPsec tunnels on vEdge routers running Internet Key Exchange (IKE) sessions.
- **PPP** VPN Interface Point-to-Point Protocol (PPP)

12. Optionally, from the Additional VPN 512 Templates section to the right, you can select templates for the management VPN, and related VPN interfaces. Choose **vEdge DHCP tunnel interface**, or the **default** management interface.

---

## Service VPN

For a full description of VPN options, see [VPN](#).

13. Optionally, from the Service VPN section, click the **+** icon to create a template for service VPNs other than VPN 0 and VPN 512.
14. Optionally, from the Service VPN section to the right, you can select templates for the following protocols and interfaces:
  - **BGP** Border Gateway Protocol
  - **IGMP** Internet Group Message Protocol
  - Multicast routing
  - **OSPF** Open Shortest Path First
  - **PIM** Protocol-Independent Multicast
  - **VPN Interface** – Choose vEdge DHCP tunnel interface, or the default management interface. Optionally, designate a DHCP sub-template.
  - **Bridge** - VPN Interface Bridge. Optionally, designate a DHCP sub-template.




- **GRE** - VPN Interface Generic Routing Encapsulation.
- **IPsec** - VPN Interface IPsec. Optionally, designate a DHCP sub-template.
- **Natpool** - VPN Interface Natpool. Optionally, designate a DHCP sub-template.

The NAT pool defines a range of IP addresses that the firewall can use to translate the source address of connections from VPN clients. The NAT pool translates the addresses in the same way as NAT rules do. Connections that use the NAT Pool must not match any NAT rules.

## Additional Templates

### Additional Templates

Banner	Choose...
Policy	Choose...
SNMP	Choose...
Security Policy	systb_security_default_policy
Container Profile *	Factory_Default_UTD_Template 

15. Optionally, you can create feature templates for the following additional network elements:

- **Banner** – You can configure two different banner text strings, one to be displayed before the CLI login prompt on a Viptela device and the other to be displayed after a successful login to the device. For a full description, see [Banner](#).
- **Policy** –
- **SNMP** – Use the Simple Network Management Protocol (SNMP) template to configure SNMP parameters for all Cisco SD-WAN devices and Cisco IOS XE routers running the SD-WAN software. For a full description, see [SNMP](#).
- **Security Policy** – Select the IPS/IDS or URL-F Security Policy template you created (see [Create a Security Policy Template for IPS/IDS or URL-F](#)). Once you select a Security Policy template, the Container Profile option displays.
- **Container Profile** – Select the IPS/IDS or URL-F Feature Profile template you created (see [Create a Feature Profile Template for IPS/IDS or URL-F](#)).



---

## Bridge Ports

16. For devices that support bridging, optionally, from the Bridge section, click the **+** icon to select the number of bridge profiles you need. Then choose the profile and an ID range between **1-63**.

---

## Create the Device Template

17. When you have finished assigning templates, click **Create**. The new template will display in the Configuration ► Templates ► Device table.

---

## Additional Information

