Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1

First Published: 2019-04-25
Last Modified: 2019-05-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
     800 553-NETS (6387)
Fax: 408 527-0883
CONTENTS

CHAPTER 1 Administration 1
  Cluster Management 1
  Manage Users 4
  Settings 10
  Tenant Management 21

CHAPTER 2 Configuration 25
  Certificates 25
    Configuring WAN Edge Certificates for Hardware 30
    Using Controller Certificates with Cisco PKI 33
  Cloud OnRamp for Colocation 37
    Manage Clusters 38
    Provision and Configure Cluster 39
    Create and Activate Cluster 40
      Cluster Settings 43
    View Cluster 45
    Edit Cluster 45
    Remove Cluster 46
    Reactivate Cluster 47
  Create Service Chain into Service Group 47
  Create Customized Service Chain 51
  View Service Groups 51
  Edit Service Group 52
    Attach and Detach Service Group with Cluster 52
  Cloud onRamp 53
  Cloud OnRamp with AWS 62
Contents

VPN Interface DSL PPPoA  277
VPN Interface DSL PPPoE  285
VPN Interface Ethernet  294
  Open and Name the Template  294
  Changing the Scope for a Parameter Value  295
  Configure Basic Interface Functionality  296
  Create a Tunnel Interface  298
  Configure an Interface as a NAT Device  301
  Configuring VRRP  303
  Apply Access Lists and QoS Parameters  304
  Add ARP Table Entries  305
  Configure IEEE 802.1X Authentication for WANs  305
  Configure Other Interface Properties  308
VPN Interface Ethernet PPPoE  310
VPN Interface GRE  317
VPN Interface IPsec (for vEdge Routers)  321
VPN Interface IPsec (for XE Routers)  327
  Create and Name the Template  327
  Basic Configuration  328
  Configure Dead-Peer Detection  329
  Configure IKE  330
  Configure IPsec Tunnel Parameters  333
VPN Interface Multilink  334
VPN Interface NAT Pool  341
VPN Interface PPP  346
VPN Interface PPP Ethernet  354
VPN Interface SVI  360
VPN Interface T1/E1  365
WiFi Radio  371
WiFi SSID  374
Add Branch Sites  377
Add Data Centers  378
Add Network Circuits  378
Configure Centralized Policy  378
CHAPTER 3  Dashboard  405
    Dashboard  405
    Multitenant Dashboard  410
    RBAC by VPN  416
        RBAC by VPN Overview  416
        VPN Dashboard Overview  416
    Configure and Manage VPN Segments  417
    Configure and Manage VPN Groups  417
    Configure User with User group  418
    Monitor devices for VPN Groups  419

CHAPTER 4  Maintenance  421
    Device Reboot  421
    Software Repository  423
        Upload VNF Images  427
        Create Customized VNF Image  428
    View VNF Images  432
    Delete VNF Images  433
    Software Upgrade  433
        Upgrade CSP Device with NFVIS Upgrade Image  437

CHAPTER 5  Monitor  441
    ACL Log  441
    Geography  442
    Network  446

CHAPTER 6  Security  467
    Security Overview  468
    Configuring SD-WAN Security  469
    Control Plane Security Overview  470
    Data Plane Security Overview  474
Configuring Security Parameters  479
Configuring Single Sign-On Using Okta  485
  Configuring Okta on the vManage UI  485
  Configuring SSO on the Okta website  485
  Assigning Users to the Application in Okta  487
Application-Aware Routing  487
Configuring Firewall Policies  491
Enterprise Firewall with Application Awareness  498
Zone-based Firewall Configuration Examples  499
Configuring Advanced Malware Protection  503
  Configuring an Advanced Malware Protection Policy  504
  Copying an existing Advanced Malware Protection Policy  506
  Applying an Advanced Malware Policy to a Device  507
Configuring Threat Grid API Key  507
  Rekeying the Device Threat Grid API Key  507
  Monitoring Advanced Malware Protection  507
  Monitoring from the Security Dashboard  508
Configuring Unified Threat Defense  508
Configuring Cloud OnRamp for IaaS  534
Configure DHCP  549
Configuring Single Sign-On using Okta  551
License Management  554
IPsec for Cisco IOS XE Routers  560
Configuring IKE-Enabled IPsec Tunnels  569
Intrusion Prevention Configuration on SD-WAN  575
URL Filtering Configuration on vManage  582
Using Umbrella DNS Security  588
Umbrella Configuration on SD-WAN  588
Umbrella Integration Using CLI  596
Configuring Centralized Control Policy  610
  Centralized Control Policy Overview  629
  Centralized Control Policy Configuration Examples  635
Configuring Localized Control Policy  639
  Configuring Localized Data Policy for IPv4  656
Configuring Localized Data Policy for IPv6 676
Configuring Centralized Data Policy 694
Overview 694
Configuring Centralized Data Policy Based on Prefixes and IP Headers 695
General vManage Configuration Procedure 698
Start the Policy Configuration Wizard 698
Step 1: Create Groups of Interest 698
Step 2: Configure the Network Topology 701
Step 3: Configure Traffic Rules 708
Step 4: Apply Policies to Sites and VPNs 712
Step 5: Activate a Centralized Data Policy 712
General CLI Configuration Procedure 712
Structural Components of Policy Configuration for Centralized Data Policy 714
Lists 715
VPN Lists 717
Policer Parameters 718
Sequences 718
Match Parameters 718
Action Parameters 720
Default Action 723
Applying Centralized Data Policy 723
Configuring Deep Packet Inspection 724
Centralized Data Policy Configuration Examples 724
Localized Control Policy 728
Localized Data Policy 728
Localized Data Policy Configuration Examples 729

Chapter 7  Tools  731
Operational Commands 731
Rediscover Network 733
SSH Terminal 735

Chapter 8  vAnalytics 737
Applications 737
Chapter 1

Administration

• Cluster Management, on page 1
• Manage Users, on page 4
• Settings, on page 10
• Tenant Management, on page 21

Cluster Management

Use the Cluster Management screen to create a vManage NMS cluster. In a vManage NMS cluster, all the cluster members communicate and work cooperatively to manage all the vBond orchestrators, vEdge routers, and vSmart controllers in the overlay network. Each vManage server can manage up to about 2,000 vEdge routers in the overlay network.

It is strongly recommended that all members of a vManage NMS cluster be located in the same data center.

Screen Elements

• Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

• Title bar—Includes the title of the screen, Cluster Management.

• Service Configuration bar—Includes tabs for Service Configuration and Service Reachability.
  • Service Configuration tab—Display the configured vManage NMSs and cluster services configured on each vManage NMS. When you first open the Cluster Management screen, the Service Configuration tab is selected.
    • Add vManage button—Add a new vManage NMS to a cluster.
  • Service Reachability tab—Display the reachable cluster services reachable on the vManage NMSs in the cluster.
    • Current vManage—Display the IP address of the vManage NMS you are currently logged into.

• Status legend—Includes colored icons for Normal, Warning, Error, and Disabled.

• Table of vManage NMS cluster members—Click a green check mark in the table to display which cluster members are reporting the status. To re-arrange the columns, drag the column title to the desired position.
Change the IP Address of the Current vManage NMS

It is recommended that you configure the IP address of the vManage server statically, in its configuration file. Configure this IP address on a non-tunnel interface in VPN 0. It is also recommended that you do not configure DHCP in VPN 512.

When you start a vManage NMS for the first time, the default IP address of the vManage server is shown as "localhost". Before you can add a new vManage NMS to a cluster, you must change "localhost" to an IP address:

1. In the Service Configuration tab, click the Add vManage button. The Edit vManage screen opens.
2. From the vManage IP Address drop-down list, select an IP address to assign to the vManage server.
3. Specify a username and password for the vManage server.
4. Click Update.

The vManage server automatically reboots and displays the Cluster Management screen.

Add a vManage NMS

To add a new vManage NMS to the cluster:

1. In the Service Configuration tab, click the Add vManage button. The Add vManage screen opens.
2. Enter the IP address of the vManage NMS you are adding to the cluster.
3. Specify the username and password for the new vManage server.
4. Select the services to run on the vManage server. You can select from the services listed below. Note that the Application Server field is not editable. The vManage Application Server is the local vManage HTTP web server.
• Statistics Database—Stores all real-time statistics from all Viptela devices in the network.
• Configuration Database—Stores all the device and feature templates and configurations for all Viptela devices in the network.
• Messaging Server—Distributes messages and shares state among all vManage NMS cluster members.

5. Click Add. The vManage NMS that you just added then reboots before joining the cluster.

In a cluster, it is recommended that you run at least three instances of each service.

Note: It is strongly recommended that the IP addresses of all members of the vManage cluster be in the same subnet.

Note: The members of a vManage cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, you cannot change the clock time on any one of the vManage servers of the cluster after you create the cluster.

Configure the Statistics Database
To configure the statistics database, which stores all real-time statistics from the local vManage NMS:

1. In the Service Configuration tab, click the Statistics Database Configuration button. The Statistics Database Configuration screen opens. The top of the screen specifies the maximum space available for the database.

2. For each Statistics Type field, assign an the amount of storage to allocate, in gigabytes (GB). The total value of all fields cannot exceed the maximum available space.

3. Click Update.

vManage NMS updates the storage allocations you have assigned once a day, at midnight.

View Statistics Database Space Usage
To view the amount of space available and utilized for the statistics database on the local vManage NMS, in the Service Configuration tab, click the Statistics Database Configuration button. The Statistics Database Configuration screen opens. The top of the screen shows the maximum space available for the database and the total amount of space currently being utilized. The table on this screen shows, for each statistics type, the disk space currently being utilized.

View vManage Service Details
To view detailed information about the services running on a vManage NMS:

1. In the Service Configuration tab, click on the hostname of the vManage server. The IP Address screen opens, with the vManage Details tab selected. This screen displays the process IDs of all the vManage services that are enabled on the vManage NMS.

2. Click Cluster Management in the breadcrumb in the title bar to return to the Cluster Management screen.

View Devices Connected to a vManage NMS
To view a list of devices connected to a vManage NMS:

1. In the Service Configuration tab, click on the hostname of the vManage server. The IP Address screen opens with the vManage Details tab selected.
2. Click the Connected Device tab to view a detailed list of all devices connected to the vManage NMS.

Alternatively:
1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row.
2. Click Device Connected.

Edit a vManage NMS
1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row and click Edit. The Edit vManage screen opens.
2. In the vManage IP Address box, select the IP address to edit.
3. Enter the username and password, and edit the cluster services provided by that vManage NMS.
4. Click Update.

Remove a vManage NMS from the Cluster
1. In the Service Configuration tab, for a vManage NMS, click the More Actions icon to the right of its row and click Remove. The Remove vManage dialog box opens.
2. Enter the username and password to confirm removal of the device from the network.
3. Click Remove.

The vManage NMS is removed from the cluster, the device is invalidated, and the certificates for that device are deleted. The remaining members in the cluster re-balance the NMS services.

View Available Cluster Services
To view the services that are available and reachable on all members in the vManage NMS cluster, click the Service Reachability tab.

Manage Users

Use the Manage Users screen to add, edit, or delete users and user groups from the vManage NMS.

Only a user logged in as the admin user or a user who has Manage Users write permission can add, edit, or delete users and user groups from the vManage NMS.

Screen Elements
• Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
• Title bar—Includes the title of the screen, Manage Users.
• Users tab—Add, edit, or delete users who are allowed to perform operations on the vManage NMS.
  • Add User: Add a new user.
  • Search box: Includes the Search Options drop-down, for a Contains or Match string.
• Refresh icon: Click to refresh data in the device table with the most current data.

• Table with list of users: To re-arrange the columns, drag the column title to the desired position.

• User Groups tab—Add, edit, or delete user groups.
  • Add User Group: Add a user group.
  • Group Name: Search for a user group. The list of user groups are displayed directly beneath Group Name in the left pane.
  • Edit: Edit the privilege levels for the selected user group.
  • Privilege level table: Displays privilege levels for the user group selected in the Group Name field.
Add a User

To perform operations on a Viptela device, you configure usernames and passwords for users who are allowed to access the Viptela device. The Viptela software provides one standard username, **admin**, and you can also create custom usernames, as needed.

To add a user:

1. In the Users tab, click Add User.
2. In the Add User popup window, enter the full name, username, and password for the user. Note that uppercase characters are not allowed in usernames.
3. From the User Groups drop-down list, select the groups that the user will be a member of.
4. Click Add. The user is then listed in the user table.

Delete a User

1. In the Users tab, select the user you wish to delete.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the user.

Edit User Details

1. In the Users tab, select the user whose details you wish to edit.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit login details, and add or remove the user from user groups.
4. Click Update.

Change User Password

1. In the Users tab, select the user whose password you wish to change.
2. Click the More Actions icon to the right of the column and click Change Password.
3. Enter, and then confirm, the new password. Note that the user, if logged in, is logged out.
4. Click Done.

Add a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. The Viptela software provides three standard user groups, and you can also create custom user groups, as needed:

- **basic**—Includes users who have permission to view interface and system information.
- **netadmin**—Includes the admin user, by default, who can perform all operations on the vManage NMS. You can add other users to this group.
- **operator**—Includes users who have permission only to view information.
To add a user group:

1. In the User Groups tab, click Add User Group.

2. In the Add User Group popup window, enter the user group name and select the desired read and write permissions for each feature. Note that uppercase characters are not allowed in user group names.

3. Click OK. The user group is then listed in the left pane.

Each user group can have read or write permission for the features listed below. Write permission includes read permission.

**Table 1:**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Read Permission</th>
<th>Write Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>Set alarm filters and view alarms generated on Viptela devices on the Monitor ► Alarms screen.</td>
<td>No additional permissions.</td>
</tr>
<tr>
<td>Audit Log</td>
<td>Set audit log filters and view a log of all activities on Viptela devices on the Monitor ► Audit Log screen.</td>
<td>No additional permissions.</td>
</tr>
</tbody>
</table>
| Certificates | View a list of vEdge routers in the overlay network on the Configuration ► Certificates ► vEdge List screen.  
               | View a CSR and certificate on the Configuration ► Certificates ► Controllers screen. | Validate and invalidate a vEdge router, stage a vEdge router, and send the serial number of valid controller devices to the vBond orchestrator on the Configuration ► Certificates ► vEdge List screen.  
               |                                                                                   | Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the Configuration ► Certificates ► Controllers screen. |
| Cluster    | View information about services running on a vManage NMS, a list of devices connected to a vManage NMS, and the services that are available and running on all the vManage NMSs in the cluster on the Administration ► Cluster Management screen. | Change the IP address of the current vManage NMS, add a vManage NMS to the cluster, configure the statistics database, edit a vManage NMS, and remove a vManage NMS from the cluster on the Administration ► Cluster Management screen. |
| Device Inventory | View a vEdge router's running and local configuration, a log of template activities, and the status of attaching configuration templates to vEdge routers on the Configuration ► Devices ► vEdge List screen.  
                   | View the running and local configuration of a controller device, a log of template activities, and the status of attaching configuration templates to controller devices on the Configuration ► Devices ► Controllers screen. | Upload the vEdge router authorized serial number file to the vManage NMS, toggle a vEdge router from vManage configuration mode to CLI mode, copy a vEdge router's configuration, and delete a vEdge router from the network on the Configuration ► Devices ► vEdge List screen.  
<pre><code>               |                                                                                   | Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the Configuration ► Devices ► Controllers screen. |
</code></pre>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Read Permission</th>
<th>Write Permission</th>
</tr>
</thead>
</table>
| Device Monitoring | View the geographic location of Viptela devices on the Monitor ▶ Geography screen.  
View events that have occurred on Viptela devices on the Monitor ▶ Events screen.  
View a list of Viptela devices in the network, device status summary, DPI flow information, TLOC loss, latency, and jitter information, control and tunnel connections, system status, and events on the Monitor ▶ Network screen (only if System is selected). | Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the Monitor ▶ Network ▶ Troubleshooting screen (only if System is selected). |
<p>| Device Reboot     | View a list of devices on which the reboot operation can be performed on the Maintenance ▶ Device Reboot screen. | Reboot one or more Viptela device on the Maintenance ▶ Device Reboot screen. |
| Interface         | View information about interfaces on a device on the Monitor ▶ Network ▶ Interface screen (only is Device Monitoring is selected). | Edit Chart Options to select the type of data to display, and edit the time period for which to display data on the Monitor ▶ Network ▶ Interface screen (only if Device Monitoring is selected). |
| Manage Users      | View users and user groups on the Administration ▶ Manage Users screen. | Add, edit, and delete users and user groups from the vManage NMS, and edit user group privileges on the Administration ▶ Manage Users screen. |
| Policy            | View common policies for all vSmart controllers or vEdge routers in the network on the Configuration ▶ Policy screen (only if Policy Configuration and Policy Deploy are selected). | Create, edit, and delete common policies for all vSmart controllers or vEdge routers in the network on the Configuration ▶ Policy screen (only if Policy Configuration and Policy Deploy are selected). |
| Policy Configuration | View list of policies created and details about them on the Configuration ▶ Policy screen (only if Policy is selected). | Create, edit, and delete common policies for all vSmart controllers and vEdge routers in the network on the Configuration ▶ Policy screen (only if Policy is selected). |
| Policy Deploy     | View the current status of the vSmart controllers to which a policy is being applied on the Configuration ▶ Policy screen (only if Policy is selected). | Activate and deactivate common policies for all vSmart controllers in the network on the Configuration ▶ Policy screen (only if Policy is selected). |
| Routing           | View real-time routing information for a device on the Monitor ▶ Network ▶ Real-Time screen (only if Device Monitoring is selected). | Add command filters to speed up the display of information on the Monitor ▶ Network ▶ Real-Time screen (only if Device Monitoring is selected). |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Read Permission</th>
<th>Write Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>View the organization name, vBond DNS/IP address, certificate authorization settings, software version enforced on a vEdge router, custom banner on the vManage login screen, and the current settings for collecting statistics on the Administration ➤ Settings screen.</td>
<td>Edit the organization name, vBond DNS/IP address, certificate authorization settings, software version enforced on a vEdge router, custom banner on the vManage login screen, current settings for collecting statistics, generate a Certificate Signing Request (CSR) for a web server certificate, and install a certificate on the Administration ➤ Settings screen.</td>
</tr>
<tr>
<td>Software Upgrade</td>
<td>View a list of Viptela devices on which software upgrade can be performed and the current software version running on a device on the Maintenance ➤ Software Upgrade screen.</td>
<td>Upload new software images on Viptela devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on a Viptela device on the Maintenance ➤ Software Upgrade screen.</td>
</tr>
<tr>
<td>System</td>
<td>View system-wide parameters configured using vManage templates on the Configuration ➤ Templates ➤ System screen (only if Device Monitoring is selected).</td>
<td>Configure system-wide parameters using vManage templates on the Configuration ➤ Templates ➤ System screen (only if Device Monitoring is selected).</td>
</tr>
<tr>
<td>Template Configuration</td>
<td>View feature and device templates on the Configuration ➤ Templates screen.</td>
<td>Create, edit, delete, and copy a feature or device template on the Configuration ➤ Templates screen.</td>
</tr>
<tr>
<td>Template Deploy</td>
<td>View devices attached to a device template on the Configuration ➤ Templates screen.</td>
<td>Attach a device to a device template on the Configuration ➤ Templates screen.</td>
</tr>
<tr>
<td>Tools</td>
<td>Use the Admin Tech command to collect system status information for a device on the Tools ➤ Operational Commands screen.</td>
<td>Use the Admin Tech command to collect system status information for a device, and use the Interface Reset command to shut down and then restart an interface on a device in a single operation on the Tools ➤ Operational Commands screen.</td>
</tr>
</tbody>
</table>

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed in the vManage Dashboard screen.

**Delete a User Group**

1. In the User Groups tab, click the name of the user group you wish to delete. Note that you cannot delete any of the three standard user groups—basic, netadmin, and operator.

2. Click the Trash icon.
3. Click OK to confirm deletion of the user group.

**Edit User Group Privileges**

1. In the User Groups tab, select the name of the user group whose privileges you wish to edit. Note that you cannot edit privileges for the three standard user groups—basic, netadmin, and operator.
2. Click the Edit button located directly above the privilege level table, and edit privileges as needed.
3. Click Save.

If an `admin` user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

## Settings

Use the Settings screen to view the current settings and configure the setting for vManage NMS parameters, including the organization name, vBond orchestrator's DNS name or IP address, certificate settings, and statistics collection.

The current setting for each item is displayed in the bar for each item, immediately following the name.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, Settings.
- **Organization Name bar**—Click View to view the organization name or Edit to edit the name.
- **vBond bar**—Click View to view the vBond DNS/IP address or Edit to enter new values.
- **Email Notifications bar**—Click View to view the settings for email notifications from the vManage server.
- **Controller Certificate Authorization bar**—Click View to view the certificate authorization settings or Edit to edit the settings.
- **vEdge Cloud Certificate Authorization bar**—Click View to view the vEdge Cloud certification authorization setting or Edit to edit the setting.
- **Web Server Certificate bar**—Click CSR to generate a Certificate Signing Request (CSR) for a web server certificate or Certificate to install the certificate.
- **Enforce Software Version (ZTP) bar**—Click View to view the software version enforced on a vEdge router or Edit to enforce a software version on the router.
- **Banner bar**—Click View to view the custom banner on the vManage login screen or Edit to edit or create a custom banner.
- **Reverse Proxy bar**—Click View to view the current settings for reverse proxy or Edit to edit the settings.
- **Statistics Setting bar**—Click View to view the current settings for collecting device statistics or Edit to edit the settings.
• Cloud onRamp bar—Click View to view the current settings for Cloud onRamp service or Edit to edit the setting.

• vAnalytics bar—Click View to view the current settings for the vAnalytics platform or Edit to edit the setting.

• Client Session Timeout bar—Click View to view the current vManage client session timeout setting or Edit to edit the setting.

• Identity Provider Settings—Click View to view the current vManage identity provider setting or Edit to edit the setting.

• Data Stream bar—Click View to view the current data streaming setting or Edit to edit the setting.

• Tenancy Mode bar—Click View to view the current tenancy setting or Edit to edit the setting.

• Statistics Configuration bar—Click View to view the current time interval for collecting device statistics or Edit to edit the setting.

• Maintenance Window bar—Click Edit to configure a maintenance time window notification.

• Statistics Database Configuration bar—Click View to view the current the vManage statistics database setting or Edit to edit the settings.
**Configure Organization Name**

Before you can generate a CSR, you must configure the name of your organization. The organization name is included in the CSR.

To configure the organization name:

1. Click the Edit button to the right of the Organization Name bar.
2. In the Organization Name field, enter the name of your organization. The organization name must be identical to the name that is configured on the vBond orchestrator.
3. In the Confirm Organization Name field, re-enter and confirm your organization name.
4. Click Save.

Note that once the control connections are up and running, the organization name bar is not editable.

**Configure vBond DNS Name or IP Address**

1. Click the Edit button to the right of the vBond bar.
2. In the vBond DNS/IP Address: Port field, enter the DNS name that points to the vBond orchestrator or the IP address of the vBond orchestrator and the port number to use to connect to it.
3. Click Save.

**Enable Email Notifications**

You can configure the vManage NMS to send email notifications when alarms occur on devices in the overlay network. First configure the SMTP and email recipient parameters on this screen:

1. Click the Edit button to the right of the Email Notifications bar.
2. In the Enable Email Notifications field, click Enabled.
3. Select the security level for sending the email notifications. The security level can be none, SSL, or TLS.
4. In the SMTP Server field, enter the name or IP address of the SMTP server to receive the email notifications.
5. In the SMTP port field, enter the SMTP port number. For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
6. In the From Address field, enter the full email address to include as the sender in email notifications.
7. In the Reply To address, enter the full email address to include in the Reply-To field of the email. This address can be a noreply address, such as noreply@cisco.com.
8. To enable SMTP authentication to the SMTP server, click Use SMTP Authentication. Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. The password that you type is hidden.
9. Click Save.

Then configure the alarms that trigger emails by clicking the Email Notifications button on the Monitor ► Alarms screen.
Configure Controller Certificate Authorization Settings

Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the vManage NMS that you generate these certificates and install them on the controller devices—vBond orchestrators, vManage NMSs, and vSmart controllers. You can use certificates signed by Symantec, or you can use enterprise root certificates.

The controller certification authorization settings establish how the certification generation for all controller devices will be done. They do not generate the certificates.

You need to select the certificate-generation method only once. The method you select is automatically used each time you add a device to the overlay network.

To have the Symantec signing server automatically generate, sign, and install certificates on each controller device:

1. Click the Edit button to the right of the Controller Certificate Authorization bar.
2. Click Symantec Automated (Recommended). This is the recommended method for handling controller signed certificates.
3. In the Confirm Certificate Authorization Change popup, click Proceed to confirm that you wish to have the Symantec signing server automatically generate, sign, and install certificates on each controller device.
4. Enter the first and last name of the requestor of the certificate.
5. Enter the email address of the requestor of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requestor via email; they are also made available though the customer portal.
6. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
8. Confirm your challenge phrase.
9. In the Certificate Retrieve Interval field, specify how often the vManage server checks if the Symantec signing server has sent the certificate.
10. Click Save.

To manually install certificates that the Symantec signing server has generated and signed:

1. Click the Edit button to the right of the Controller Certificate Authorization bar.
2. Click Symantec Manual.
3. In the Confirm Certificate Authorization Change popup, click Proceed to manually install certificates that the Symantec signing server has generated and signed.
4. Click Save.

To use enterprise root certificates:

1. Click the Edit button to the right of the Controller Certificate Authorization bar.
2. Click Enterprise Root Certificate.
3. In the Confirm Certificate Authorization Change popup, click Proceed to confirm that you wish to use enterprise root certificates.

4. In the Certificate box, either paste the certificate, or click Select a file and upload a file that contains the enterprise root certificate.

5. By default, the enterprise root certificate has the following properties: • Country: United States • State: California • City: San Jose • Organizational unit: vIPtela Inc Regression • Organization: vIPtela Inc • Domain name: viptela.com • Email: support@viptela.com To view this information, issue the show certificate signing-request decoded command on a controller device, and check the output in the Subject line. For example:

```
vSmart# show certificate signing-request decoded
...  
  Subject: C=US, ST=California, L=San Jose, OU=vIPtela Inc Regression, O=vIPtela Inc, CN=vsmart-uuid.viptela.com/emailAddress=support@viptela.com
...  
```

6. To change one or more of the default CSR properties:
   1. Click Set CSR Properties.
   2. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).
   3. Enter the organizational unit (OU) to include in the CSR.
   4. Enter the organization (O) to include in the CSR.
   5. Enter the city (L), state (ST), and two-letter country code (C) to include in the CSR.
   6. Enter the email address (emailAddress) of the certificate requestor.
   7. Specify the validity period for the certificate. It can be 1, 2, or 3 years.

6. Click Import & Save.

**Configure vEdge Cloud Certificate Authorization Settings**

Certificates are used to authenticate vEdge Cloud routers in the overlay network. Once authentication is complete, vEdge Cloud routers can establish secure sessions with other devices in the overlay network.

By default, vEdge Cloud certification authorization is automated. This is the recommended setting.

If you use third-party certificate authorization, configure certificate authorization to be manual:

1. Click the Edit button to the right of the vEdge Cloud Certificate Authorization bar.
2. In the vEdge Cloud field, click Manual (Enterprise CA).
3. Click Save.

**Generate Web Server Certificate**

To establish a secure connection between your web browser and the vManage server using authentication certificates, generate a CSR to create a certificate, have it signed by a root CA, and then install it. To do so:

1. Click the CSR button to the right of the Web Server Certificate bar.
2. In the Common Name field, enter the domain name or IP address of the vManage server. For example, the fully-qualified domain name of vManage could be vmanage.org.local.

3. In the Organizational Unit field, enter the unit name within your organization, for example, Network Engineering.

4. In the Organization field, enter the exact name of your organization as specified by your root CA, for example, Viptela Inc.

5. In the City field, enter the name of the city where your organization is located, for example, San Jose.

6. In the State field, enter the state in which your city is located, for example, California.

7. In the 2-Letter Country Code field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.

8. From the Validity drop-down, select the validity period for the certificate.

9. Click Generate to generate the CSR.

10. Send the CSR to Symantec or a root CA for signing.

11. When you receive the signed certificate, click the Certificate button to the right of the Web Server Certificate bar to install the new certificate. The View box displays the current certificate on the vManage server.

12. Copy and paste the new certificate in the box. Or click the Import button, click Select a File to download the new certificate file, and click Import.

13. Once the certificate is installed, reboot the vManage server.

Below is an example of a certificate generated with the above configuration. Note that the certificate is truncated in this example.
View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the vManage server using authentication certificates, you configure the time period for which the certification is valid (in Step 8 in the previous section).
At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

**Enforce Software Version on vEdge Routers**

If you are using the Viptela ZTP hosted service, you can enforce a version of the Viptela software to run on a vEdge router when it first joins the overlay network. To do so:

1. Ensure that the software image for the desired vEdge router software version is present in the vManage software image repository:
   1. In vManage NMS, select the Maintenance ► Software Upgrade screen.
   2. In the Device List drop-down, click Repository. The Software Repository screen opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.
   3. If you need to add a software image, click Add New Software.
   4. Select the location from which to download the software images, either vManage or Remote Server.
   5. Select an x86-based or a MIPS-based software image.
   6. Click Upload or Add to play the image in the repository.

2. In the Administration ► Settings screen, click the Edit button to the right of the Enforce Software Version (ZTP) bar.

3. In the Enforce Software Version field, click Enabled.

4. From the Software Version drop-down, select the version of the software to enforce on vEdge routers when they join the network.

5. Click Save.

If you enable this feature on the vManage NMS, any vEdge router joining the network is configured with the version of the software specified in the Enforce Software Version field regardless of whether the router was running a higher or lower version of Viptela software.

**Create a Custom Banner**

To create a custom banner that is displayed after you log in to the vManage NMS:

1. Click the Edit button to the right of the Banner bar.

2. In the Enable Banner field, click Enabled.

3. In the Banner Infotext box, enter the text string for the login banner or click Select a File to download a file that contains the text string.

4. Click Save.
Enable Reverse Proxy

To enable reverse proxy services in the overlay network:

1. Click the Edit button to the right of the Reverse Proxy bar.
2. Click Enabled.
3. Click Save.

To configure reverse proxy on individual vManage NMS and vSmart controller devices, in vManage NMS select Configuration ► Devices and then click the Controllers tab. For the desired device, click the More Actions icon to the right of the row, and click Add Reverse Proxy. Then configure the private and proxy IP addresses and ports for the device.

For more information, see Enable Reverse Proxy.

Collect Device Statistics

To enable or disable the collection of statistics for devices in the overlay network:

1. Click the Edit button to the right of the Statistics Settings bar. By default, all statistics collection settings are enabled for all Viptela devices.
2. To set statistics collection parameters for all devices in the network, click Disable All for the parameter you wish to disable statistics collection for. To return to the saved settings during an edit operation, click Reset. To return the saved settings to the factory-default settings, click Restore Factory Default.
3. To set statistics collection parameters for individual devices in the network, click Custom to select devices on which to enable or disable statistics collection. The Select Devices popup screen opens listing the hostname and device IP of all devices in the network. Select one or more devices from the Enabled Devices column on the left and click the arrow pointing right to move the device to the Disabled Devices column on the right. To move devices from the Disabled Devices to the Enabled Devices column, select one or more devices and click the arrow pointing left. To select all devices in the Select Devices popup screen, click the Select All checkbox in either window. Click Done when all selections are made.
4. Click Save.

Enable Cloud onRamp Service

1. Click the Edit button to the right of the Cloud onRamp bar.
2. In the Enable Cloud onRamp field, click Enabled.
3. Click Save.

Enable vAnalytics Platform

1. Click the Edit button to the right of the vAnalytics bar.
2. In the Enable vAnalytics field, click Enabled.
3. Click Save.
**Enable vManage Client Session Timeout**

By default, a user's session to a vManage client remains established indefinitely and never times out. To set how long a vManage client session is inactive before a user is logged out:

1. Click the Edit button to the right of the Client Session Timeout bar.
2. In the Session Timeout field, click Enabled.
3. In the Timeout field, enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
4. Click Save.

The client session timeout value applies to all vManage servers in a vManage cluster.

**Enable Single Sign-On**

To enable single sign-on (SSO) for the vManage NMS to allow users to be authenticated using an external identity provider:

1. Ensure that you have enabled NTP on the vManage NMS.
2. Click the Edit button to the right of the Identity Provider Settings bar.
3. In the Enable Identity Provider field, click Enabled,
4. Copy and paste the identity provider metadata in the Upload Identity Provider Metadata box. Or click Select a File to upload the identity provider metadata file.
5. Click Save.

**Enable Data Stream Collection**

By default, collecting streams of data from a network device is not enabled. To use the Packet Capture, Speed Test, and Debug Logs troubleshooting tools, you must enable the collection of data streams.

To collect data streams:

1. Click the Edit button to the right of the Data Stream bar.
2. In the Data Stream field, click Enabled.
3. In the Hostname field, enter the name of the host to which to send the collected data. Enter just the hostname (such as "test") with no domain name. It is recommended that this host be one that is used for out-of-band management and that is located in the management VPN.
4. In the VPN field, enter the number of the VPN in which the host is located. It is recommended that this be the management VPN, which is typically VPN 512.
5. Click Save.

**Set the Tenancy Mode**

By default, the vManage server is in single-tenant mode, which enables it to manage a single overlay network. In single-tenant mode, the vManage server can manage up to 10,000 devices.

To place the vManage server in multitenant mode so that you can manage the overlay networks of multiple tenants:
1. Click the Edit button to the right of the Tenancy Mode bar.

2. In the Tenancy field, click Multitenant.

3. In the Domain field, enter the domain name for the service provider (for example, viptela.com).

4. Click Save. The vManage server reboots and comes back up in multitenant mode.

In multitenant mode, you can configure up to 500 tenants and up to a total of 10,000 devices.

To configure tenants, go to the Administration ► Tenant Management screen.

Note: After you place a vManage server into multitenant mode, you cannot convert it back to single-tenant mode.

Set Interval to Collect Device Statistics

To set the time interval at which vManage NMS should collect statistics for devices in the overlay network:

1. Click the Edit button to the right of the Statistics Configuration bar. By default, statistics is collected for all Viptela devices every 30 minutes.

2. Click the up or down arrow in the Collection Interval drop-down to change the frequency at which to collect device statistics. The minimum time you can specify is 5 minutes and the maximum is 180 minutes.

3. Click Save.

Configure a Maintenance Window

To configure a maintenance window for the vManage server:

1. Click the Edit button to the right of the Maintenance Window bar.

2. Click the Start date and time drop-down, and select the date and time when the maintenance window will start.

3. Click the End date and time drop-down, and select the date and time when the maintenance window will end.

4. Click Save. The start and end times and the duration of the maintenance window are displayed in the Maintenance Window bar.

Two days before the start of the window, the vManage Dashboard displays a maintenance window alert notification.

To cancel a maintenance window for the vManage server:

1. Click the Edit button to the right of the Maintenance Window bar.

2. Click Cancel maintenance window.

Configure the vManage Statistics Database

To configure the vManage statistics database, which stores all real-time statistics from the local vManage NMS:
1. Click the Edit button to the right of the Statistics Database Configuration bar. The Statistics Database Configuration screen opens. The Statistics Database Configuration bar shows the maximum space available for the database.

2. For each Statistics Type row, enter the maximum size of the statistics file, in gigabytes (GB). The total value of all fields cannot exceed the maximum available space.

3. Click Save.

vManage NMS updates the storage allocations you have assigned once a day, at midnight.

To view the actual and maximum size of statistics database on the vManage server:

1. Click the Edit button to the right of the Statistics Database Configuration bar. The Statistics Database Configuration screen opens. The table on this screen shows, for each statistics type, the disk space currently being utilized.

2. Click Close.

**Tenant Management**

Use the Tenant Management screen to add tenants to a vManage server that is operating in multitenant mode.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. In the middle is the name of the provider and the Select Tenant drop-down. On the right are a number of icons and the user profile drop-down.

- **Title bar**—Includes the title of the screen, Tenant Management.

- **Add Tenant button**—Add a new tenant to the provider's domain.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.

- **All tenants**—The left pane lists all the tenants.

- **Tenant**—The right pane shows information for the tenant selected in the left pane.
Add a Tenant

1. In the left pane, click the Add Tenant button.

2. In the Add Tenant window:
   1. Enter a name for the tenant. It can be up to 128 characters and can contain only alphanumeric characters.
   2. Enter a description for the tenant. It can be up to 256 characters and can contain only alphanumeric characters.
   3. Enter the name of the organization. The name is case-sensitive. It is the name in the certificates for all Viptela network devices, and it must be identical on all devices in the overlay network.
   4. In the URL subdomain field, enter the domain name for the tenant. The domain name must include the provider's domain name. For example, for the provider viptela.com, a valid domain name might be plum.viptela.com. You must also configure this same domain name when you enable multitenancy mode, in vManage Administration ➤ Settings ➤ Tenancy Mode.
   5. Click Save.

3. The Create Tenant screen is displayed, and the Status column shows In progress. To view status messages related to the creation of the tenant, click the > to the left of the status column. After about 1 minute, the Status column changes to Success, and the tenant table shows the tenant's system IP address.

View All Tenants

To view a summary of information about all tenants, in the center of the top bar, click the provider name.

View a Single Tenant

To view a summary of information about a single tenant:

1. In the center of the top bar, click the provider name.
2. In the table of tenants, click the tenant name. The summary information displays to the right of the name.
3. To hide the summary information, click the tenant name a second time.

To view the vManage dashboard for a single tenant:

1. In the center of the top bar, click Select Tenant to the right of the provider name.
2. Select the tenant name from the drop-down.

Edit a Tenant

1. In the left pane, click the name of the tenant.
2. In the right pane, click the Pencil icon to the right of the tenant's name.
3. In the Edit Tenant popup, modify the tenant's name, description, or domain name.
4. Click Save.
Remove a Tenant

1. In the left pane, click the name of the tenant.
2. In the right pane, click the Trash icon to the right of the tenant's name.
3. In the Delete Tenant popup, enter your vManage password and click Save.

Related Topics

Multitenant Dashboard, on page 410
CHAPTER 2

Configuration

- Certificates, on page 25
- Cloud OnRamp for Colocation, on page 37
- Cloud onRamp, on page 53
- Cloud OnRamp with AWS, on page 62
- Cloud OnRamp with Azure, on page 66
- Devices, on page 72
- IPv6 Functionality, on page 79
- Network Design, on page 86
- Policies, on page 98
- Templates, on page 106
- Add Branch Sites, on page 377
- Add Data Centers, on page 378
- Add Network Circuits, on page 378
- Configure Centralized Policy, on page 378
- Configure Global Parameters, on page 390
- Configure Localized Policy, on page 390

Certificates

In the 16.11/19.1 release, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously.

See Configuring WAN Edge Certificates for Hardware, on page 30 for more information.

Use the Certificates screen to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Viptela solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the vManage NMS that you generate these certificates and install them on the controller devices—vManage NMSs, vBond orchestrators, and vSmart controllers.

- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Viptela, mark each router as valid or invalid, and then from the vManage NMS, send the file to the controller devices in the network.
You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Viptela overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

**Note**

For purposes of certificate management, the term *controller* is used to collectively refer to the vManage NMS, the vSmart controller, and the vBond orchestrator.

### Screen Elements

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- **Title bar**—Includes the title of the screen, Certificates.

- **WAN Edge List tab**—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - **Send to Controllers**—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - **Table of WAN edge routers in the overlay network**—To re-arrange the columns, drag the column title to the desired position.

- **Controllers tab**—Install certificates and download the device serial numbers to the vBond orchestrator.
  - **Send to vBond**—Send the controller serial numbers to the vBond orchestrator.
  - **Install Certificate**—Install the signed certificates on the controller devices. This button is available only if you select Manual in Administration ▶ Settings ▶ Certificate Signing by Symantec.
  - **Export Root Certificate**—Display a copy of the root certificate for the controller devices that you can download to a file.
  - **Table of controller devices in the overlay network**—To re-arrange the columns, drag the column title to the desired position.

- **Certificate status bar**—Located at the bottom of the screen, this bar is available only if you select Server Automated in Administration ▶ Settings ▶ Certificate Authorization. It displays the states of the certificate installation process:
  - **Device Added**
  - **Generate CSR**
  - **Waiting for Certificate**
  - **Send to Controllers**

A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.
- **Refresh icon**—Click to refresh data in the device table with the most current data.
• Export icon—Click to download all data to a file, in CSV format.

• Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.

Check the WAN Edge Router Certificate Status

In the WAN Edge List tab, check the Validate column. The status can be one of the following:

• Valid (shown in green)—The router's certificate is valid.

• Staging (shown in yellow)—The router is in the staging state.

• Invalid (shown in red)—The router's certificate is not valid.

Validate a WAN Edge Router

When you add vEdge and WAN routers to the network using the Configuration ► Devices screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the WAN Edge List tab, select the router to validate.

2. In the Validate column, click Valid.

3. Click OK to confirm the move to the valid state.

4. Repeat Steps 1 to 3 for each router you wish to validate.
5. Click the Send to Controllers button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

### Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the vManage NMS. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the vSmart controller and the vManage NMS.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the Validate column, click Staging.
3. Click OK to confirm the move to the staging state.
4. Click Send to Controllers in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

### Invalidate a WAN Edge Router

1. In the WAN Edge List tab, select the router to invalidate.
2. In the Validate column, click Invalid.
3. Click OK to confirm the move to the invalid state.
4. Repeat Steps 1 to 3 for each router you wish to invalidate.
5. Click the Send to Controllers button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

### Send the Controller Serial Numbers to vBond Orchestrator

To determine which controllers in the overlay network are valid, the vBond orchestrator keeps a list of the controller serial numbers. The vManage NMS learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the vBond orchestrator:

1. In the Controllers tab, check the certificate status bar at the bottom of the screen. If the Send to Controllers check mark is green, all serial numbers have already been sent to the vBond orchestrator. If it is grey, you can send one or more serial numbers to the vBond orchestrator.

2. Click the Send to vBond button in the Controllers tab. A controller's serial number is sent only once to the vBond orchestrator. If all serial numbers have been sent, when you click the Send to vBond button, an error message is displayed. To resend a controller's serial number, you must first select the device and then select Invalid in the Validity column.

After the serial numbers have been sent, click the Tasks icon in the vManage toolbar to display a log of the file download and other recent activities.
Install Signed Certificate

If in Administration ► Settings ► Certificate Signing by Symantec, you selected the Manual option for the certificate-generation process, use the Install Certificate button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the Controllers tab, click the Install Certificate button.
2. In the Install Certificate window, select a file, or copy and paste the certificate text.
3. Click Install to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps 1 to 3 to install additional certificates.

Export Root Certificate

1. In the Controllers tab, click the Export Root Certificate button.
2. In the Export Root Certificate window, click Download to export the root certificate to a file.
3. Click Close.

View the CSR

1. In the WAN Edge List or Controllers tab, select a device.
2. Click the More Actions icon to the right of the row, and click View CSR to view the certificate signing request (CSR).

View the Certificate

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click View Certificate.

Generate the CSR

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Generate CSR.
3. In the Generate CSR window, click Download to download the file to your local PC (that is, to the PC you are using to connect to the vManage NMS).
4. Repeat Steps 1 to 4 for each controller for which you are generating a CSR.

Reset the RSA Key Pair

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Reset RSA.
3. Click OK to confirm resetting of the device's RSA key and to generate a new CSR with new public/private keys.

**Invalid a Device**

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm invalidation of the device.

**View Log of Certificate Activities**

To view the status of certificate-related activities:

1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

---

**Configuring WAN Edge Certificates for Hardware**

Enterprise certificates allow organizations to use their own private certificate signing authority rather than having to rely on public certificate signing authorities. You can also apply custom certificate properties using the Set CSR Properties field.

---

**Note**

In the 16.11/19.1 release, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously. An independent organization handles the signing of enterprise certificates.

Use the Configuration ► Certificates screen to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the vManage NMS that you generate these certificates and install them on the controller devices—vManage NMSs, vBond orchestrators, and vSmart controllers.

- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Plug and Play (PnP), mark each router as valid or invalid, and then from the vManage NMS, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.
For purposes of certificate management, the term controller is used to collectively refer to the vManage NMS, the vSmart controller, and the vBond orchestrator.

Once you reset a WAN edge device, you have to install the enterprise root certificate manually on the device. If you perform an upgrade, your certificate is retained.

Support is provided in Base64 format, which contains only signed certificates. The base needs to be in Base64 PEM certificate format.

The PEM extension is used for different types of X.509v3 files that contain ASCII (Base64) armored data prefixed with a --BEGIN ... line.

### Enterprise Certificate Supported Devices

The following are the supported enterprise supported devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>vManage</td>
<td>Yes</td>
</tr>
<tr>
<td>vBond</td>
<td>Yes</td>
</tr>
<tr>
<td>vSmarts</td>
<td>Yes</td>
</tr>
<tr>
<td>Edges</td>
<td>All hardware WAN edges (vEdge/IOS-XE-SD-WAN except ASR1002-X, ISRv, CSR1000v)</td>
</tr>
</tbody>
</table>

---

**Configuring Enterprise Certificates**

1. Navigate to Administration ➤ Settings Hardware WAN Edge Certificate Authority and select Edit.
2. Click Enterprise Certification (signed by Enterprise CA).
   Security: On Box Certificate (TPM/SUDI Certificate) is the default option.

3. Click Set CSR Properties if you want to specify custom certificate properties. Properties are listed under the CSR Properties checkbox.

   **Note**
   Organization Unit is a non-editable field. Organization Unit needs to be the same as Organization Name on vManage.

4. Choose Select a file to upload a root certificate authority file.
   The uploaded root certificate authority displays in the text box.

5. Select Save.


7. Select the Upload WAN Edge List tab.

8. Browse to the location of the vEdge list and click Upload.

9. At the Configuration ► Certificates page, using the More options, select the appropriate action, View Enterprise CSR, View Enterprise Certificate, Renew Enterprise CSR, or Revoke Enterprise Certificate.
   - **View Enterprise CSR (certificate signing request)** - Copy the CSR and sign it using the enterprise root certificate, and upload the signed certificate on vManage using the Install Certificate operation. vManage automatically discovers on which hardware edge the certificate needs to be installed on.
   - **View Enterprise Certificate** - Once the certificate is installed, you can see the installed certificate and download it.
   - **Renew Enterprise CSR** - In case you need to install a new certificate on the hardware device, you can use the Renew Enterprise CSR option. The Renew Enterprise CSR option generates the CSR. You can then view the certificate (View Enterprise CSR option) and install the certificate (Install Certificate option). This step flips the control connections as a new serial number. You can see the new serial number and expiry data on the Configuration ► Certificates page.
• Revoke Enterprise Certificate - This option removes the enterprise certificate from the device and moves it back to pre-staging. The device has only vBond and vManage controls up.

10. Select Install Certificates to upload the signed certificate.
    The certificate has to be a signed certificate. Initially, the state is CSR Generated.
    The state changes to Certificate Installed when successfully installed.

11. At the Configuration ► Certificates page, you can see enterprise certificate columns, including the
    device type, chassis-id, enterprise serial number, and enterprise certificate date.

Generating a Bootstrap Configuration

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable
USB drive or from internal boot flash to a device that supports SD-WAN. When the device boots, it uses the
information in the configuration file to come up on the network.

1. If you need to generate a bootstrap configuration, use the Configuration ► Devices page, and select
Generate Bootstrap Configuration under More options.

Deleting a WAN Edge Device

Before deleting a WAN edge device, invalidate the device on the Configuration ► Certificates page.

Using Controller Certificates with Cisco PKI

From software release 19.x and onwards, there is an option to use Cisco as the certificate authority (CA)
instead of Symantec/Digicert for the controller certificates.

This section goes through the different deployment types, scenarios to administer, install, and troubleshoot
controller certificates using Cisco public key infrastructure (PKI). Cisco PKI provides certificate management
to support security protocols such IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

The major difference between Symantec/Digicert and Cisco PKI certificates is that Cisco PKI certificates are
linked to a customer's Smart Account (SA) and Virtual Account (VA) in Plug and Play (PnP) and do not
require manual approval using a portal like Digicert. Each VA has a limit of 100 certificates; that is, each
overlay has a limit of 100 certificates and once the certificate signing request (CSR) is generated, the approval
and installation happens automatically if the vManage Settings are set correctly.

Devices are added and certificates are installed automatically from the Cisco PKI servers. There is no human
intervention required to approve the certificate.

Supported Devices for Cisco PKI Certificates

The following are the supported devices for using Cisco PKI certificates.

<table>
<thead>
<tr>
<th>Device</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>vManage</td>
<td>Yes</td>
</tr>
<tr>
<td>vBond</td>
<td>Yes</td>
</tr>
<tr>
<td>vSmart</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Use Cases for Cisco PKI Controller Certificates

#### Use Case 1

**Cisco-Hosted Cloud Overlays with Software Version 19.x and Above**

#### Prerequisites

vManage and the controllers should all be running the same 19.x software version.

You can verify the software version for the new or expired overlays without having control connections using SSH.

1. SSH to each of the controllers and the version should show during the SSH process.
2. You do not need to actually have the credentials work, therefore you can run this on a controller where the credentials do not work.

Repeat this process for all the controllers in the overlay to make sure.

3. Customer Smart Account credentials need to be ready using either of the following methods:
   1. Email and request the customer contact from PnP trigger notifications to individually email you and provide the Smart Account credentials.
   2. Email and request the customer contact to log on to vManage and add them. Also ensure that you ask the customer for their IPs to whitelist.

Ensure that if asking the customer to provide their customer contact to log on, this step is done after asking the customer for their IPs to whitelist, so that they can reach the vManage GUI, be able to log on, and input their Smart Account credentials.

You can find your Smart Account credentials in the vManage GUI in Administration ► Settings ► Smart Account Credentials at the very bottom of the page.

Enter the user name and password and select **Save**.

#### Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
2. Navigate to Administration ► Settings ► Controller Certificate Authorization and press **Edit**.
3. Select the radio button **Cisco Automated (Recommended)**. You get an error if the Smart Account credentials are not added. Check the prerequisites.
4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press **Save**.

---

### Use Device Support

<table>
<thead>
<tr>
<th>Device</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>vEdges</td>
<td>No</td>
</tr>
</tbody>
</table>
Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the vManage GUI.

Navigate to the Configuration ► Certificates ► Controllers tab. Click on the More (dot) menu on the right ► Generate CSR.

The operation status shows the CSR sent for signing, the certificate signed and installed automatically without needing human intervention.

7. The certificates get installed automatically and shows the expiration date and status of a successful install. The operation status shows Installed for vBonds and vBond Updated for vSmarts and vManage along with the certificate serial number.

8. Ensure that the control connections have come up to the controllers on the vManage dashboard.

Use Case 2

Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal

Prerequisites

vManage, controllers, and vEdges should all have their control connections up.

1. Verify that the control connections to controllers and vEdges are up in the vManage GUI dashboard.

   If the control connections are not up, let the customer know that migrating from Digicert to Cisco PKI cannot proceed until the control is up.

   If the control connections are only partially up, that is some vEdges are control down, then let the customer know that those vEdges will not be able to automatically reconnect to the controllers if their control comes up once the certificates have been moved to Cisco PKI.

   If it is a case of expired certificates and control connections are down, then certificates need to be renewed on Digicert first and control connections need to be brought up before migrating them to the Cisco PKI controller certificates.

2. Verify that the software version of the controllers is 19.x.

   **How to Verify the Software Version for the Active Existing Overlays (with Valid Control Connections to Controllers) Using the vManage GUI**

   1. Navigate to the Maintenance ► Software Upgrade in the vManage GUI menu.

   2. Select the vManage tab and look for the column Current Version. Verify that it is 19.x or above.

      If the control connections are up and vManage and controller versions are not 19.x, then let the customer know to upgrade them to 19.x first (vEdges need not be upgraded) before migration to Cisco PKI can be done.
It is mandatory that controllers upgraded to 19.x should immediately have their certificates renewed with Cisco PKI as part of the upgrade; they cannot be allowed to run with the existing Symantec certificates even if those certificates are going to remain valid.

3. Once the prerequisites are verified, check that the Cisco PKI root-CA has been propagated to all the controllers and the vEdges.
   
   This requires SSH access to the controllers.
   
   1. SSH into the vManage and controllers and run the following command: `show certificate root-ca-cert | include Cisco`.
      
      If the output is blank or does not show the result, escalate to the cloud infrastructure team.

4. Customer Smart Account credentials need to be ready by either of the following methods:
   
   1. Email and request the customer contact from a PnP trigger notification to individually email you and provide the Smart Account credentials.
      
      or

   2. Email and request your customer contact to log on to the vManage themselves and add them. Also ensure that you ask for the customer IPs to whitelist.

      Ensure that if asking the customer to provide, this step is done after asking the customer for their IPs to whitelist, so that they can reach the vManage GUI, be able to log on, and input the Smart Account Credentials.

      You can find the Smart Account credentials in the vManage GUI at Administration ▶ Settings ▶ Smart Account Credentials (at the very bottom).

3. Enter the username and password and press Save.

   Once all the prerequisites have been satisfied, follow the Runbook to Request and Install Cisco PKI Certificates to request CSRs and get the Cisco certificates installed. Verify that all the control connections to the controllers and the vEdges have come back up. If not, then escalate to the cloud infrastructure team.

**Use Case 3:**

**Submitting CSRs and Downloading Certificates on On-Premises Controllers**

The following steps require access to PnP and to the SA/VA in question. Customers have access to their own SA/VA.

**Prerequisites**

The prerequisites are the same in the above cases, except that you use the manual method for installing the certificates.

**Runbook**

2. Generate the CSRs for the controllers.
   Navigate to the Configuration ► Certificates ► Controllers tab. Click on the More (dot) menu on the right and then select Generate CSR.
   Download each CSR to a file with a filename .csr and keep it ready to submit to the PnP portal for getting the signed certificates.

3. Log on to the PnP portal to the required SA/VA and select the Certificates tab.

4. Click on Generate Certificate and follow the steps to give a name for the certificate file, paste the CSR, and download the signed certificate.
   The finished certificate is ready for download. Repeat this process for each CSR and download all the required certificates.

5. You can install the downloaded certificates in the vManage GUI by navigating to Configuration ► Certificates ► Controllers ► Install Certificate button (top right).
   Once installed, verify that the control connections are up.

**Debugging and Log Information**

1. Check the vBond profile under the VA in PnP to verify that the correct organization name exists.

2. Check the output at /var/log/nms/vmanage-server.log on the vManage for logs of the entire certificate process.

3. vManage should have internet connectivity to reach the Cisco PKI servers.

---

**Cloud OnRamp for Colocation**

The Cloud OnRamp for Colocation solution securely connects enterprise applications that are hosted in an enterprise data center, in either a public, private or hybrid cloud, to the enterprise's employees, devices, customers, and partners.

A colocation is a stack of compute and networking fabric that brings up multiple virtual networking functions and multiple service chains on them. A Cloud OnRamp for Colocation cluster consists of a collection of two to eight Cloud Services Platform (CSP) devices and two switches.

**Screen Elements**

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- Title bar—Includes the title of the screen, Cloud OnRamp for Colocation.

- Cluster and Service Group tabs—When you first open the Cloud OnRamp for Colocation screen, the Cluster tab is selected.
  - Cluster tab—Click to create a cluster.
  - Service Group tab—Click to create a service group.
• Cluster table—If you have created at least one cluster, it is listed in the table. If you have not created any cluster, click the Configure & Provision Cluster button.

Related Topics
   Software Repository, on page 423

Manage Clusters

Use the Cloud OnRamp for Colocation screen to configure a Cloud OnRamp for Colocation cluster and service groups that can be used with the cluster.

The three steps to configure Cloud OnRamp for Colocation devices are:

• Create a cluster. See Create and Activate Cluster, on page 40.

• Create a service group. See Create Service Chain into Service Group, on page 47.

• Attach a cluster with a service group. See Attach and Detach Service Group with Cluster, on page 52.

A Cloud OnRamp for Colocation cluster is a collection of two to eight CSP devices and two switches. The supported cluster templates are:

• Small cluster—2 Catalyst 9500+2 CSP
• Medium Cluster—2 Catalyst 9500+4 CSP
• Large Cluster—2 Catalyst 9500+6 CSP
• X-Large Cluster—2 Catalyst 9500+8 CSP

**Note**

Ensure that you add a minimum of two CSP devices one-by-one to a cluster. You can keep adding three, four, and so on, up to a maximum of eight CSP devices. You can edit a Day-N configuration of any cluster, and add pairs of CSP devices to each site up to a maximum of eight CSP devices.

Ensure that all devices that you bring into a cluster have the same software version.

Following are the cluster states:

• Incomplete—When a cluster is created from the vManage interface without providing the minimum requirement of two CSP devices and two switches. Also, cluster activation is not yet triggered.

• Inactive—When a cluster is created from the vManage interface after providing the minimum requirement of two CSP devices and two Switches, and cluster activation is not yet triggered.

• Init—When the cluster activation is triggered from the vManage interface and Day-0 configuration push to the end devices is pending.

• Inprogress—When one of the CSP devices within a cluster comes up with control connections, the cluster moves to this state.

• Pending—When the Day-0 configuration push is pending or VNF install is pending.

• Active—When a cluster is activated successfully and NCS has pushed the configuration to the end device.
• Failure—If Cisco Colo Manager (CCM) has not been brought up or if any of the CSP devices that failed to receive an UP event.

A cluster transitioning to an active state or failure state is as follows:

- Inactive > Init > Inprogress > Pending > Active—Success
- Inactive > Init > Inprogress > Pending > Failure—Failure

**Provision and Configure Cluster**

This topic describes about activating a cluster that enable deployment of service chains.

To provision and configure a cluster, perform the following:

1. Create a cluster by adding two to eight CSP devices and two switches.

   CSP devices can be added to a cluster and configured through vManage before bringing them up. You can configure CSP devices and Catalyst 9K switches with the global features such as, AAA, default user (admin) password, NTP, syslog, and more.

2. Configure cluster parameters including IP address pool input such as, service chain VLAN pool, VNF management IP address pool, management gateway, VNF data plane IP pool, and system IP address pool.

3. Configure a service group.

   A service group consists of one or more service chains.

   **Note**
   You can add a service chain by selecting one of the predefined or validated service chain template, or create a custom one. For each service chain, configure input and output VLAN handoff and service chain throughput or bandwidth, as mentioned.

4. Configure each service chain by selecting each VNF from the service template. Choose a VNF image that is already uploaded to the VNF repository to bring up the VM along with required resources (CPU, memory, and disk). Provide the following information for each VNF in a service chain:
   - The specific VM instance behavior such as, HA, shared VM can be shared across service chains.
   - Day-0 configuration values for tokenized keys and not part of the VLAN pool, management IP address, or data HA IP address. The first and last VMs handoff-related information such as peering IP and autonomous system values must be provided. The internal parameters of a service chain are automatically filled by the orchestrator from the VLAN or Management or Data Plane IP address pool provided.

5. Add the required number of service chains for each service group and create the required number of service groups for a cluster.

6. To attach a cluster to a site or location, activate the cluster after all configuration has been completed.

   You can watch the cluster status change from in progress to active or error.

To edit a cluster, perform the following:

1. Modify the activated cluster by adding or deleting service groups or service chains.
2. Modify the global features configuration such as, AAA, system setting, and more.

You can predesign a service group and service chain before creating a cluster. They can be attached with a cluster after the cluster is active.

Create and Activate Cluster

This topic provides the steps about how a cluster can be formed with CSP devices, Catalyst 9K switches as single unit, and provision the cluster with cluster-specific configuration.

Before you begin

Ensure that the clock on Cisco vManage and CSP devices are synchronized.

| Step 1 | In vManage NMS, choose Configuration > Cloud OnRamp for Colocation. The CLOUD ONRAMP FOR COLOCATION screen appears, and the Configure & Provision Cluster button is highlighted. In the CLOUD ONRAMP FOR COLOCATION screen, perform the following tasks:
| a) | In the Cluster tab, click the Configure & Provision Cluster button.
A graphical representation of the default cluster, which consists of two switches each connected to two Cloud Services Platform (CSP) devices is displayed in the design view window.
| b) | Provide cluster name, description, site id, and location information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The cluster name can be up to 128 characters and can contain only alphanumeric characters.</td>
</tr>
<tr>
<td>Description</td>
<td>The description can be up to 2048 characters and can contain only alphanumeric characters.</td>
</tr>
<tr>
<td>Site ID</td>
<td>Specifies overlay network site identifier. This entry can be a value from 1 through 4294967295 (2^{32} - 1).</td>
</tr>
<tr>
<td>Location</td>
<td>The location can be up to 128 characters and can contain only alphanumeric characters.</td>
</tr>
</tbody>
</table>

| c) | From the graphical representation, to configure a switch, click a switch icon, the Edit Switch dialog box is displayed. Provide a name and choose the switch serial number. Click Save.

The switch name can be up to 128 characters and can contain only alphanumeric characters.

When you order Cisco SD-WAN Cloud OnRamp for Colocation solution PID on CCW and buy the Catalyst 9500 switches, a serial number is assigned for the switches. These serial numbers are integrated with vManage through PNP.

| Note | You can keep the serial number field blank, design your cluster, and edit the cluster later to include the serial number after you have bought the switches. |
| d) | To configure another switch, repeat the previous step. |
e) From the graphical representation, to configure CSP, click a CSP icon in the CSP box. The **Edit CSP** dialog box is displayed. Provide a hostname and choose the CSP serial number. Click **Save**.

The hostname can be up to 128 characters and can contain only alphanumeric characters.

**Note** You can keep the serial number field blank, design your cluster, and edit the cluster later to include the serial number after you have bought CSP devices. However, you cannot activate a cluster, where the serial number of CSP devices are not being included.

f) To add remaining CSP devices, repeat step e.

After you design a cluster, an ellipse that is enclosed in a yellow circle next to the device appears if a serial number has not been assigned for a device.

g) To edit a CSP device configuration, click a CSP from the graphical representation, and follow the process that is mentioned in substep e.

h) For mandatory and optional global parameters to be set for a cluster, click and choose from **Cluster Settings** drop-down.

The dialog boxes for each of the global parameters are displayed. Enter values for the cluster settings parameters and click **Save**. See **Cluster Settings**, on page 43.

i) Click the **Save Cluster** button.

**Step 2** In the **Cluster** tab, to activate a cluster, click a cluster, click the **More Actions** icon to the right of its row, click **Activate** against the cluster.

When you click Activate, vManage establishes a DTLS tunnel with CSP devices in the cluster where it connects with the switches through CCM. After the DTLS connection is running, a CSP device in the cluster is chosen to host the CCM. CCM is brought up and vManage sends global parameter configurations to the CSP devices and switches. To verify if a cluster has been activated, you can view the task progress as shown.
To verify if cluster has been activated from the CSP end, you can view the task progress as shown.

If the CCM status does not go to "HEALTHY" after "STARTING", see Troubleshoot Cisco Colo Manager Issues.

If the status of CCM goes to "HEALTHY" after "STARTING" but the status of CCM shows IN-PROGRESS for more than 20 minutes after the switch configurations are already complete, see Switch devices are not calling home to PNP or CCM.

If the status of the tasks running on a CSP device does not show success for more than five minutes after the activation through OTP, see Troubleshoot Cisco Colo Manager Issues.

Note

If a cluster goes into a "PENDING" state, click the More Actions icon to the right of its row, and then click the Sync button. This action moves a cluster back to an "ACTIVE" state.

To view if a cluster moves back to an "ACTIVE" state, you can view the successful activation as shown.
To determine the service groups present on CSP devices, navigate to Monitor > Network > Colocation Cluster.

Choose a cluster and then choose a CSP device as shown in the following image. You can choose and view other CSP devices.

**Cluster Settings**

The cluster settings parameters are:

- Configure login credentials for the cluster:
  1. In the Cluster Settings drop-down, click **Credentials**. The Credentials dialog box is displayed. Enter the values for the following fields:
     - (Mandatory) Template Name: The template name can be up to 128 characters and can contain only alphanumeric characters.
     - (Optional) Description: The description can be up to 2048 characters and can contain only alphanumeric characters.
  2. Click **New User**.
     - Provide name, password, and role of a user.

- Configure the Resource pool for the cluster:
  1. In the Cluster Settings drop-down, click **Resource Pool**. The Resource Pool dialog box is displayed. Enter the values for the following fields:
     - (Mandatory) Name: Name of the IP address pool. The name can be up to 128 characters and can contain only alphanumeric characters.
     - (Optional) Description: IP address pool description. The description can be up to 2048 characters and can contain only alphanumeric characters.
     - (Mandatory) DTLS Tunnel IP: IP addresses to be used for the DTLS tunnel. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 1.1.1.1-1.1.1.4).
(Mandatory) Service Chain VLAN Pool: Numbers of the VLAN to be used for service chains. To enter multiple numbers, separate them by commas. To enter a numeric range, separate the numbers with a hyphen (for example, 20-30).

**Note**  
A VLAN range brings up VNFs, so that each circuit has VLAN configured when it comes up. The VLAN pool can only start from 1021 as switch reserves the VLANs until 1021. We recommend you to enter VLAN pools between 1021-2021.

(Mandatory) VNF Data Plane IP Pool: IP addresses to be used for auto configuring data plane on a VNF interface. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 1.1.1.1-1.1.1.4).

(Mandatory) VNF Management IP Pool: IP addresses to be used for the VNF. To enter multiple IP addresses, separate them by commas. To enter a range, separate the IP addresses with a hyphen (for example, 20-30).

**Note**  
These addresses are IP addresses for secure interfaces.

(Mandatory) Management Gateway Prefix: IP address of the gateway to the management network. It enables DNS to exit the cluster.

(Mandatory) Management Mask: Mask value for the failover cluster. For example, /24 and not 255.255.255.0

(Mandatory) Switch PNP Server IP: IP address of the switch device.

**Note**  
The IP address of the switch is automatically picked from the management pool, which is the first IP address. You can change it if a different IP is configured in the DHCP server for the switch.

- Optionally, configure NTP servers for the cluster:
  1. In the Cluster Settings drop-down, select NTP. The NTP configuration box is displayed. Enter the values for the following fields:
     - Template Name: Name of the NTP template. The name can be up to 128 characters and can contain only alphanumeric characters.
     - Description: The description can be up to 2048 characters and can contain only alphanumeric characters.
     - Preferred server: IP address of the primary NTP server.
     - Backup server: IP address of the secondary NTP server.

- Optionally, configure syslog parameters for the cluster:
  1. In the Cluster Settings drop-down, select Syslog. The System Log configuration box is displayed. Enter the values for the following fields:
TemplateName: Name of the System Log template. The name can be up to 128 characters and can contain only alphanumeric characters.

Description: The description can be up to 2048 characters and can contain only alphanumeric characters.

Severity drop-down: Select the severity of syslog messages to be logged.

2. To configure a syslog server, click New Server.
3. Type the IP address of a syslog server.

If all global parameters are set through cluster settings, you can verify if the cluster has been activated successfully, as shown.

View Cluster

To view a cluster configuration, perform the following steps:

Step 1 In vManage, choose Configuration > Cloud OnRamp for Colocation. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the Configure & Provision Cluster button is highlighted.

Step 2 In the Cluster tab, click a cluster, click the More Actions icon to the right of its row, and click View against the cluster. The Cluster window opens, displaying the switches and CSP devices in the cluster and showing which cluster settings have been configured.

Step 3 You can only view the global parameters being set, configuration of switches and CSP devices.

Step 4 Click the Cancel button to return to the CLOUD ONRAMP FOR COLOCATION Cluster screen.

Edit Cluster

To modify any existing cluster configuration such as global parameters, perform the following steps:

Step 1 In vManage, select Configuration > Cloud OnRamp for Colocation. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the Configure & Provision Cluster button is highlighted.

Step 2 In the Cluster tab, click a cluster, click the More Actions icon to the right of its row, and click Edit against the cluster. The Cluster window opens, displaying the switches and CSP devices in the cluster and showing which cluster settings have been configured.

Step 3 In the cluster design window, you can modify some of the global parameters. Based on whether a cluster is in active or inactive state, following are the restrictions for editing a cluster:

1. Inactive state.
   - Edit all global parameters, and the Resource pool parameter.
• Add more CSP devices (up to eight).
• Cannot edit the name or serial number of a switch or CSP device. Instead, delete the CSP or switch and add another switch or CSP with a different name and serial number.
• Delete an entire cluster configuration.

2. Activate state.
• Edit all global parameters, except the Resource pool parameter.

   Note  The Resource pool parameter cannot be changed when the cluster is activated. However, the only way to change the Resource pool parameter is to delete the cluster and recreate it again with the correct Resource pool parameter.

• Cannot edit the name or serial number of a switch or CSP device. Instead, delete the CSP or switch and add another switch or CSP with a different name and serial number.
• Cannot delete a cluster in active state.

**Step 4**  Click the **Save Cluster** button.

---

## Remove Cluster

To decommission an entire cluster, perform the following steps:

**Step 1**  In Cisco vManage, in the **Configuration > Certificates** screen, locate and verify status of devices to be deleted, and click **Invalid** against the devices.

**Step 2**  In the **Configuration|Certificates** screen, click **Send to Controllers**.

**Step 3**  In vManage, click **Configuration > Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted.

**Step 4**  In the **Cluster** tab, locate the cluster that has invalid devices, click the **More Actions** icon to the right of its row, and click **Deactivate** against the cluster.

If the cluster is attached to one or more service groups, you are prompted with a message that service chains hosting the VMs are running on this device and whether you can continue with the cluster deletion. However, although you confirm deletion of a cluster, you are not allowed to remove the cluster without detaching the service groups that are hosted on this device. If the cluster is not attached to any service group, you are prompted with a message to confirm the cluster deletion.

   Note  You can delete the cluster, if necessary, or can keep it in deactivated state.

**Step 5**  To delete the cluster, select **Delete**.

**Step 6**  Click the **Cancel** button to return to the CLOUD ONRAMP FOR COLOCATION Cluster screen without deleting the cluster.

**Step 7**  To decommission invalid devices, in vManage, click **Configuration > Devices**.

**Step 8**  Locate the devices that are in the deactivated cluster, click the **More Actions** icon to the right of the device row, and click **Decommission WAN Edge**.
This action provides new tokens to your devices.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Reset the devices to the factory default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>Log into NFVIS by using <strong>admin</strong> as the login name and <strong>Admin123#</strong> as the default password.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Reset switch configuration and reboot switches.</td>
</tr>
</tbody>
</table>

### Reactivate Cluster

To add new CSP devices or when CSP devices are considered for RMA process, perform the following steps:

| Step 1 | In Cisco vManage, in the **Configuration > Devices** screen, locate the devices that are in the deactivated cluster. |
| Step 2 | Get new token from vManage for the devices. |
| Step 3 | Log into NFVIS by using **admin** as the login name and **Admin123#** as the default password. |
| Step 4 | Use the **request activate chassis-number chassis-serial-number token token-number** command. |
| Step 5 | From vManage, configure the system configuration and then activate the cluster. See [Create and Activate Cluster, on page 40](#). |

If the cluster has been deleted, recreate and then activate it.

| Step 6 | In Cisco vManage, in the **Configuration > Certificates** screen, locate, and verify status of devices. |
| Step 7 | To validate the devices, click **Valid** if it is invalid. |
| Step 8 | In the **Configuration/Certificates** screen, click **Send to Controllers**. |

### Create Service Chain into Service Group

A service group consists of one or more service chains.

In vManage, click **Configuration > Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab, and then click the **Create Service Group** button. Provide service group name and description.

   The service group name can be up to 128 characters and can contain only alphanumeric characters.

   The service group description can be up to 2048 characters and can contain only alphanumeric characters.

b) Click **Add Service Chain**.

c) In the Add Service Chain dialog box, provide the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, and service chain configuration.

   The service chain name can be up to 128 characters and can contain only alphanumeric characters.

   The service chain description can be up to 2048 characters and can contain only alphanumeric characters.
For service chain configuration, you can choose any of the four validated service chains such as, Router - Firewall - Router, Firewall, Firewall - Router. See Validated Service Chains. You can also create a customized service chain. See Create Customized Service Chain, on page 51.

The Input VLAN handoff and output VLAN handoff can be comma separated values (10, 20) or a range between 10-20.

d) In the Add Service Chain definition box, click Add.
   Based on the service chain configuration information, a graphical representation of the service group with all the service chains and its VNFs are automatically displayed in the design view window. It shows all the configured service chains within each service group. A check against the service chain indicates that all configuration information for the service chain has been completed.

e) In the design view window, to configure a VNF, click a VNF in the service chain.
   The Configure VNF dialog box appears.

f) Configure the VNF with the following information and perform the actions, as appropriate:

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Package</td>
<td>Mandatory</td>
<td>Choose a router or firewall package.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>VNF image name</td>
</tr>
<tr>
<td>CPU</td>
<td>Optional</td>
<td>Specifies the number of virtual CPUs that are required for a VNF.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter,</td>
<td>If you do not enter, the default value is considered, which is 1 vCpu.</td>
</tr>
<tr>
<td></td>
<td>the default value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is considered, which</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is 1024 MB.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Optional</td>
<td>Specifies the maximum primary memory in MB that the VNF can use.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter,</td>
<td>If you do not enter, the default value is considered, which is 8 GB.</td>
</tr>
<tr>
<td></td>
<td>the default value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is considered, which</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is 8 GB.</td>
<td></td>
</tr>
<tr>
<td>Disk</td>
<td>Optional</td>
<td>Specifies disk in GB required for the VM.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter,</td>
<td>If you do not enter, the default value is considered, which is 8 GB.</td>
</tr>
<tr>
<td></td>
<td>the default value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is considered, which</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is 8 GB.</td>
<td></td>
</tr>
</tbody>
</table>

You are prompted with any custom tokenized variables from Day-0 that requires your input. Provide the values.

In the following image, all IP addresses, VLAN, and AS within the green box are system generated (from the VLAN, IP pools provided for the cluster) and automatically populated into Day-0 configurations of VMs.
The following images provide an example of the configuration for VNF IP addresses and AS numbers in vManage.
For edge VMs such as first and last VM in a service chain, user must provide the following addresses as they peer with a branch and provider.

**Table 4: VNF Options for First VM in Service Chain**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Mode</td>
<td>Mandatory</td>
<td>Choose Routed or Transparent mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Firewall mode is applicable only for firewall VMs and not other VMs.</td>
</tr>
<tr>
<td>Enable HA</td>
<td>Optional</td>
<td>HA enabled or not for VNF.</td>
</tr>
<tr>
<td>Termination mode</td>
<td>Mandatory</td>
<td>Specifies the following modes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• L3 mode selection with subinterfaces that are trunked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;val help=&quot;L3 Mode With Sub-interfaces(Trunked)&quot; display=&quot;VNF-Tagged&quot;&gt;vlan&lt;/val&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• L3 mode with IPSEC termination from a consumer and routed to a provider gateway.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;val help=&quot;L3 Mode With IPSEC Termination From Consumer and Routed to Provider GW&quot; display=&quot;Tunneled&quot;&gt;vpn&lt;/val&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• L3 mode with access mode (nontrunked).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;val help=&quot;L3 Mode In Access Mode (Non-Trunked)&quot; display=&quot;Hypervisor-Tagged&quot;&gt;routed&lt;/val&gt;</td>
</tr>
</tbody>
</table>

- g) Click **Configure**. The service chain is configured with VNF configuration.
- h) To add another service chain, repeat step b.
Create Customized Service Chain

You can customize service chains:

- By including extra VNFs or add other VNF types
- By creating new VNF sequence that is not part of the predefined service chains.

Step 1
Create a service group and service chains within the service group. See Create Service Chain into Service Group, on page 47.

Step 2
In the Add Service Chain dialog box, provide the service chain name, description, bandwidth, input VLAN handoff, output VLAN handoff, and service chain configuration. Click Add.

For service chain configuration, choose Create Custom from the drop-down. An empty service group in the design view window is available.

Step 3
To add a VNF such as a router, load balancer, firewall, and others, click a VNF icon on the left bar, and drag the icon to its proper location within the service group box. After adding all required VNFs and forming the VNF service chain, configure each of the VNFs. Click a VNF in the service group box. The Configure VNF dialog box is displayed. Enter the following parameters:

a) Select the software image to load from the Image Package drop-down.
b) Click Fetch VNF Properties.
c) Enter a name of the VNF in the Name field.
d) Enter the number of virtual CPUs required for the VNF in the CPU field.
e) Enter the amount of memory in megabytes to be allocated for the VNF in the Memory field.
f) Enter the amount of memory for storage in gigabytes to be allocated for the VNF in the Disk field.
g) Enter VNF-specific parameters, as required.

Note These VNF details are the custom variables that are required for Day-0 operations of the VNF.

h) Click Configure.
i) To delete the VNF or cancel the VNF configuration, click Delete or Cancel respectively.

The customized service chains are added to a service group.

Note You can customize a VNF sequence with only up to four VNFs in a service chain.

View Service Groups

To view service groups, perform the following steps:
In vManage, click **Configuration > Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLOCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab.
b) To view the service chains in the design view window, click a service chain box.

---

**Edit Service Group**

Before attaching a service group, you can edit all parameters. However, after attaching a service group, you can only add new service chains but not edit or attach a service chain. To edit and delete a service group, perform the following steps:

In vManage, click **Configuration > Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. In the CLOUD ONRAMP FOR COLOCATION Cluster screen, perform the following tasks:

a) Click the **Service Group** tab.
b) To modify either service chain configuration or modify VNF configuration, click a router or firewall VNF icon.
c) To add new service chains, click a service chain button.

---

**Attach and Detach Service Group with Cluster**

To complete the Cisco SD-WAN Cloud OnRamp for Colocation configuration, you must attach service groups to a cluster. To attach or detach a service group from a cluster, perform the following steps:

**Step 1**

In vManage, click **Configuration > Cloud OnRamp for Colocation**. The CLOUD ONRAMP FOR COLOCATION Cluster screen appears, and the **Configure & Provision Cluster** button is highlighted. To attach a service group with a cluster, perform the following steps:

a) In the **Cluster** tab, click a cluster from the table, click the **More Actions** icon to the right of its row, and click **Attach Service Groups**.

**Step 2**

In the **Attach Service Groups** dialog box, select a service group from the available service groups.

**Step 3**

Click the right arrow to move the chosen service groups to the selected box.

**Step 4**

Click **Attach**.

**Step 5**

To detach a service group from a cluster, perform the following action:

a) In the **Cluster** tab, click a cluster from the table, click the **More Actions** icon to the right of its row.
b) Click **Detach Service Groups**.

You cannot attach or detach individual service chain within a group.

**Step 6**

To verify if service groups have been attached and detached, you can view from the following vManage screen:
If the status of the tasks are "FAILURE" or in "PENDING" state for long duration, see Troubleshoot Service Chain Issues. If CCM task fails, see Troubleshoot Cisco Colo Manager Issues.

Note

If a cluster goes into "PENDING" state, click the More Actions icon to the right of its row and then click the Sync button. This action moves the cluster back to "ACTIVE" state.

Cloud onRamp

Use the Cloud onRamp dashboard to configure the Cloud onRamp for SaaS service and to view the performance of cloud applications for which you have enabled Cloud onRamp service.

Cloud onRamp service calculates a value called the Viptela Quality of Experience (vQoE). The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best. Cloud onRamp service computes vQoE values for applications and paths, then assigns applications to the paths that best match their vQoE value. Cloud onRamp service periodically recalculates vQoE values for paths to ensure ongoing optimal application performance.

Screen Elements

• Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

• Title bar—Includes the title of the screen, Cloud onRamp.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.

• Application panes—Display performance of individual applications.

• Legend—Indicates quality of experience levels for cloud applications.

• Manage Cloud onRamp—Manage Cloud onRamp applications, client sites, gateways, and Direct Internet Access (DIA) sites.
**View Application Performance**

Each pane in the Cloud onRamp dashboard displays the performance of a cloud application. Each application pane displays the number of vEdge routers accessing the application and the quality of the connection:

- The bottom status bar displays green for devices experiencing good quality.
- The middle status bar displays yellow for devices experiencing average quality.
- The top status bar displays red for devices experiencing bad quality.
The number to the right of each status bar indicates how many devices are experiencing that quality of connection.

**View Details about an Application**

1. Click in an application's pane. vManage NMS displays a list of sites accessing the application.
2. Click a graph icon in the vQoE Score column to display vQoE history for that site.
   - Click the time duration links to adjust the data the chart displays.
   - Hover over a point on the chart to display vQoE details for that point in time.

**Manage Cloud onRamp Applications**

Select Manage Cloud onRamp ➤ Applications. The screen changes and displays the following elements:

- Add Applications and VPN—Add applications to Cloud onRamp service.
- Applications table—Display applications and VPNs configured for Cloud onRamp service.
To edit the VPN configured for an application, click the Edit icon for that application, then enter the new VPN. You can enter any VPN other than 0, which is the transport VPN, or 512, which is the management VPN.

To add applications to Cloud onRamp service:

1. From the Manage Cloud onRamp drop-down, located to the right of the title bar, select Applications.
2. Click the Add Applications and VPN button. The Add Applications & VPN popup window displays.
3. In the Applications field, select an application.
4. In the VPN field, enter the service VPN in which that application runs. You can enter any VPN other than 0 and 512.
5. Click Add.
6. Repeat Steps 2 through 4 for each application you want to add.
7. Click Save Changes.

**Manage Cloud onRamp Client Sites**

Client sites in Cloud onRamp service choose the best gateway site for each application to use for accessing the internet.

In the title bar, select Manage Cloud onRamp ► Client Sites. The screen changes and displays the following elements:

- Attach Sites—Add client sites to Cloud onRamp service.
- Detach Sites—Remove client sites from Cloud onRamp service.
- Client sites table—Display client sites configured for Cloud onRamp service.
To display details about a client site, select the site from the Client Sites Table and click the forward arrow located to the right of the row.

To detach a client site, select the site from the Client Sites Table and click Detach Sites.

To add client sites to Cloud onRamp service:

1. Click Attach Sites. The Attach Sites popup window displays all sites in your overlay network, with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.

2. In the Available Sites pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.

3. Click Attach to push the new template to the vEdge routers.
Manage Cloud onRamp Gateways

Gateway sites in Cloud onRamp service choose the best network path for application traffic that originates at client sites.

In the title bar, select Manage Cloud onRamp ► Gateways. The screen changes and displays the following elements:

- Attach Gateways—Attach gateway sites.
- Detach Sites—Remove gateway sites from Cloud onRamp service.
- Edit Sites—Edit interfaces on gateway sites.
- Gateways table—Display gateway sites configured for Cloud onRamp service.
To display details about a gateway site, select the site from the Gateways Table and click the forward arrow located to the right of the row.

To detach a gateway site, select the site from the Gateways Table and click Detach Gateways.

To attach gateways:

1. Click Attach Gateways. The Attach Gateways screen displays. The Site List shows all available sites in your overlay network. For a site to be available, all devices at that site must be running in vManage mode.

2. In the Available Gateways pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.

3. If you would like to specify GRE interfaces for Cloud onRamp service to use:
   1. Click Add Interfaces to Selected Sites.
   2. In the Interfaces drop-downs, add GRE interfaces.

If you do not specify interfaces for Cloud onRamp service to use, the system will select a NAT-enabled physical interface from VPN 0.

1. Click Attach to push the new template to the vEdge routers.

To edit Cloud onRamp interfaces on gateway sites:

1. Select the sites you want to edit and click Edit Gateways.

2. In the Edit Interfaces of Selected Sites screen, select a site to edit.
   • To add interfaces, click the Interfaces field to select available interfaces.
   • To remove an interface, click the X beside its name.

3. Click Save Changes to push the new template to the vEdge routers.

**Manage Cloud onRamp DIA Sites**

In Cloud onRamp service, DIA sites choose the best internet path for the application to use. They also consider paths that exit to the internet through gateway sites.

In the title bar, select Manage Cloud onRamp ► DIA. The screen changes and displays the following elements:

• Attach DIA Sites—Attach DIA sites.
• Detach DIA Sites—Remove DIA sites.
• Edit DIA Sites—Edit interfaces on DIA sites.
• Sites table—Display sites configured for Cloud onRamp service.
To display details about a site, select the site from the Sites Table and click the forward arrow located to the right of the row.

To detach a DIA site, select the site from the Sites Table and click Detach DIA Sites.

To attach DIA sites:

1. Click Attach DIA Sites. The Attach DIA Sites screen displays. The Site List shows all sites in your overlay network, with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.

2. In the Available Sites pane, select a site to attach and click the right arrow. If you wish to remove a site from the Selected Sites pane, select the site and click the left arrow.

3. If you would like to specify GRE interfaces for Cloud onRamp service to use:
1. Click Add Interfaces to Selected Sites.
2. In the Interfaces drop-downs, add GRE interfaces.

If you do not specify interfaces for Cloud onRamp service to use, the system will select a NAT-enabled physical interface from VPN 0.

1. Click Save Changes to push the new template to the vEdge routers.

To edit Cloud onRamp interfaces on DIA sites:
1. Select the sites you want to edit and click Edit DIA Sites.
2. In the Edit Interfaces of Selected Sites screen, select a site to edit.
   • To add interfaces, click the Interfaces field to select available interfaces.
   • To remove an interface, click the X beside its name.
3. Click Save Changes to push the new template to the vEdge routers.

Cloud OnRamp with AWS

Use the Cloud OnRamp screen to create virtual private cloud (VPC) instances for hosting vEdge Cloud routers in different AWS regions in the public internet. A Cloud OnRamp setup comprises three components:

• A transit VPC, which connects a Viptela overlay network to one or more cloud-based applications.
• A host VPC, which is where cloud-based applications reside.
• The connections, or mappings, between the transit VPC and one or more host VPCs.

Screen Elements

• Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
• Title bar—Includes the title of the screen, Cloud OnRamp.
• Add New Cloud Instance—Click to create a Cloud OnRamp VPC instance using the cloud instance configuration wizard.
• Cloud OnRamp Dashboard—Displays after you add at least one region in an Account.
  • VPC panes—Located on the Cloud OnRamp Dashboard, directly under the Add New Cloud Instance button, is a pane for each region corresponding to an account that has been created. Each pane shows:
    • Account number or account name used for logging in to AWS
    • Number of up and down IPsec connections for mapped host VPCs
    • Number of up and down control connections for vEdge router instances within the transit VPCs
Create a Cloud Instance

1. Click Add New Cloud Instance.

2. In the Add Cloud Instance–Log In to a Cloud Server popup:
   1. In the Cloud drop-down, select the cloud type to be AWS.
   2. Click IAM Role or Key to log in to the cloud server. It is recommended that you use IAM Role.
   3. If you select IAM Role:
      1. In the Role ARN field, enter the role ARN of the IAM role.
      2. In the External ID field, enter external ID created for the role ARN. It is recommended that the external ID include 10 to 20 characters in random order. To authenticate to the vManage NMS using an IAM role, vManage NMS must be hosted by Viptela on AWS and have the following attributes: • Trusts the AWS account, 200235630647, that hosts the vManage NMS. • Have all permissions for EC2 and VPC resources. • A default timeout of at least one hour. If vManage NMS is not hosted by Viptela on AWS, assign an IAM role with permissions to AssumeRole to the vManage server running the Cloud OnRamp process. Refer to the AWS documentation for details.

4. If you select Key:
   1. In the API Key field, enter your Amazon API key.
   2. In the Secret Key field, enter the password associated with the API key.

3. Click Login to log in to the cloud server. The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a region and discover hosts VPCs, add transit VPC, and map host VPCs to transit VPCs. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

4. Select a region and discover host VPCs:
   1. In the Choose Region drop-down, select a geographical region.
   2. Click Discover Host VPCs. A list of host VPCs discovered in that region is displayed.
   3. Select the desired VPCs.
   4. Click Next.

5. Add a transit VPC:
   1. In the Transit VPC Name field, type a name for the transit VPC. The name can be up to 128 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   2. Under Device Information, enter information about the transit VPC:
      1. In the vEdge Version drop-down, select the Viptela software version to run on the VPC transit.
      2. In the Size of Transit vEdge drop-down, select how much memory and how many CPUs to create on the VPC transit.
3. In the Device 1 drop-down, select the serial number to use.

4. In the Device 2 drop-down, select the serial number to use.

5. Click Advanced if you wish to enter more specific configuration options:
   1. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.
   2. In the SSH PEM Key drop-down, select a PEM key pair to log in to an instance. Note that the key pairs are region-specific. Refer to the AWS documentation for instructions on creating key pairs.
   3. Click Save and Finish to create the transit VPC. Or click Proceed to Mapping to continue with the wizard.

3. Click Next.

6. Map the host VPCs to transit VPCs:
   1. In the table of host VPCs, select the desired host VPCs.
   2. Click Map VPCs. The Map Host VPCs popup opens.
   3. In the Transit VPC drop-down, select the transit VPC to map to the host VPCs.
   4. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
   5. Click Map VPCs.
   6. Click Save and Complete.

**Display Host VPCs**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default. In the bar below this, Mapped Host VPCs is selected by default, and the table on the screen lists the mapping between host and transit VPCs, the state of the transit VPC, and the VPN ID.

2. To list unmapped host VPCs, click Unmapped Host VPCs. Then click Discover Host VPCs.

3. To display the transit VPCs, click Transit VPCs.

**Map Host VPCs to a Transit VPC**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens.

2. Click Unmapped Host VPCs.

3. Click Discover Host VPCs.

4. From the list of discovered host VPCs, select the desired host VPCs.

5. Click Map VPCs. The Map Host VPCs popup opens.
6. In the Transit VPC drop-down, select the desired transit VPC.

7. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.

8. Click Map VPCs.

**Unmap Host VPCs**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens.

2. Click Mapped Host VPCs.

3. From the list of VPCs, select the desired host VPCs.

4. Click Unmap VPCs.

5. Click OK to confirm the unmapping.

Unmapping host VPCs deletes all VPN connections to the VPN gateway in the host VPC, and then deletes the VPN gateway. When you make additional VPN connections to a mapped host VPC, they will be terminated as part of the unmapping process.

**Display Transit VPCs**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.

2. Click Transit VPCs.

The table at the bottom of the screen lists the transit VPCs.

**Add a Transit VPC**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.

2. Click Transit VPCs.

3. Click Add Transit VPC.

**Delete a Transit VPC**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VPC. The Host VPCs/Transit VPCs screen opens, and Host VPCs is selected by default.

2. Click Mapped Host VPCs.

3. Select the desired host VPC, and click Unmap VPCs.

4. Click OK to confirm the unmapping.

5. Click Transit VPCs.

6. Click the Trash icon to the left of the row for the transit VPC.

7. Click OK to confirm.
Cloud OnRamp with Azure

Use the Cloud OnRamp screen to create transit virtual networks (VNets) for hosting vEdge Cloud router instances in different Azure locations in the public internet. A Cloud OnRamp setup comprises three components:

- A transit VNet, which connects a Viptela overlay network to one or more cloud-based applications.
- A host VNet, which is where cloud-based applications reside.
- The connections, or mappings, between the transit VNet and one or more host VNets.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Cloud OnRamp.
- Add New Cloud Instance—Click to create a Cloud OnRamp VNet instance using the cloud instance configuration wizard.
- Cloud OnRamp Dashboard—Displays after you add at least one cloud instance.
  - VNet panes—Located on the Cloud OnRamp Dashboard, directly under the Add New Cloud Instance button, is a pane for each VNet that has been created. For each VNet, the pane shows:
    - Credential value for the VNet
    - Name of the VNet
    - Type of VNet
    - Number of up and down connections for mapped host VNets
    - Number of up and down connections for transit VNets
Create a Cloud Instance

1. Click Add New Cloud Instance:
2. In the Add Cloud Instance–Log In to a Cloud Server popup:
   1. In the Cloud drop-down, select the cloud type to be Azure.
   2. To give vManage programmatic access to your Azure Subscription, log in to the cloud server:
      1. In the Subscription ID field, enter the ID of the Azure subscription you want to use as part of the Cloud onRamp workflow.
      2. In the Client ID field, enter the ID of an existing application or create a new application in Azure. To create a new application, go to your Azure Active Directory ► App Registrations ► New Application Registration.
      3. In the Tenant ID field, enter the ID of your Azure account. To find the tenant ID, go to your Azure Active Directory and click Properties.
4. In the Secret Key field, enter the password associated with the client ID.

3. Click Log In. The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a location and discover host VNets, add transit VNet, and map host VNets to transit VNets. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

4. Select a location and discover host VNets:
   1. In the Choose Location drop-down, select a geographical location.
   2. Click Discover Host VNets. A list of host VNets discovered in that location is displayed.
   3. Select the desired VNet.
4. Click Next.

5. Add a transit VNet:
   1. In the Transit VNet Name field, type a name for the transit VNet. The name can be up to 32 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   2. Under Device Information, enter information about the transit VNet:
      1. In the WAN Edge Version drop-down, select the Viptela software version to run on the VNet transit. The drop-down lists the published versions of the Viptela software in the Azure marketplace.
      2. In the Size of Transit VNet drop-down, select how much memory and how many CPUs to create on the VNet transit.
      3. In the Device 1 drop-down, select the serial number to use.
      4. In the Device 2 drop-down, select the serial number to use.
   3. Click Advanced if you wish to enter more specific configuration options.
   4. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.

3. Click Next.

6. Map the host VNets to transit VNets:
   1. In the table of host VNets, select the desired host VNet.
   2. Click Map VNs. The Map Host VNs popup opens.
   3. In the Transit VNet drop-down, select the transit VNet to map to the host VNs.
   4. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
   5. In the IPSec Tunnel CIDR section, enter two pairs of interface IP addresses for each vEdge Cloud router to configure IPSec tunnels to reach the Azure virtual network transit. The IP addresses must be network addresses in the /30 subnet, be unique across the overlay network, and not be a part of the host VNet CIDR. If they are part of the host VNet CIDR, Azure will return an error while attempting to create VPN connections to the transit VNet.
   6. In the Azure Information section:
      1. In the BGP ASN field, enter the ASN that will be configured on the Azure Virtual Network Transit that is spun up within the host VNet. Use an ASN that is not part of an existing configuration on Azure. For acceptable ASN values, refer to Azure documentation.
      2. In the Host VNet Gateway Subnet field, enter a host VNet subnet in which the Virtual Network Gateway can reside. It is recommended you use a /28 subnet or higher. You must not provide a subnet that is already created in the VNet.

7. Click Map VNs.
8. Click Save and Complete.
When you configure the two vEdge Cloud routers that form the transit VNet, ensure that the color you assign to the tunnel interface in the VPN feature configuration template for VPN 0, is a public color, not a private color. Public colors are 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, public-internet, red, and silver.

Display Host VNets
1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default. In the bar below this, Mapped Host VNets is selected by default, and the table on the screen lists the mapping between host and transit VNets, the state of the transit VNet, and the VPN ID.
2. To list unmapped host VNets, click Unmapped Host VNets.
3. To display the transit VNets, click Transit VNets.

Map Host VNets to an Existing Transit VNet
1. In the Cloud OnRamp Dashboard, click the pane for the desired location of the required account. The Host VNets/Transit VNets screen opens.
2. Click Unmapped Host VNets.
3. Click Discover Host VNets.
4. From the list of discovered host VNets, select the desired host VNet.
5. Click Map VNets. The Map Host VNets popup opens.
6. In the Transit VNet drop-down, select the desired transit VNet.
7. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
8. Click Map VNets.

Unmap Host VNets
1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens.
2. Click Mapped Host VNets.
3. From the list of VNets, select the desired host VNets. It is recommended that you unmap one vNet at a time. If you want to unmap multiple vNets, do not select more than three in a single unmapping operation.
4. Click Unmap VNets.
5. Click OK to confirm the unmapping.

Display Transit VNets
1. In the Cloud OnRamp Dashboard, click the pane for the desired VNets. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Transit VNets.
The table at the bottom of the screen lists the transit VNets.

**Add a Transit VNet**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Transit VNets.
3. Click Add Transit VNet.

**Delete a Transit VNet**

1. In the Cloud OnRamp Dashboard, click the pane for the desired VNet. The Host VNets/Transit VNets screen opens, and Host VNets is selected by default.
2. Click Mapped Host VNets.
3. Select the desired host VNet, and click Unmap VNets.
4. Click OK to confirm the unmapping.
5. Click Transit VNets.
6. Click the Trash icon to the left of the row for the transit VNet.
7. Click OK to confirm.

**Related Topics**

Cloud OnRamp with AWS, on page 62

---

**Devices**

Use the Devices screen to add or delete WAN Edge routers and controller devices from the overlay network. WAN Edge routers are vEdge and other WAN routers. Controller devices are the vManage NMS, the vSmart controller, and the vBond orchestrator.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, Devices.
- **WAN Edge List tab**—Upload the WAN Edge authorized serial number file to the vManage NMS. When you first open the Devices screen, the WAN Edge List tab is selected.
  - **Change mode**—Switch between vManage and CLI mode.
  - **Upload WAN Edge List**—Upload the WAN edge router authorized serial number file to the vManage NMS.
  - **Export Bootstrap Configuration**—Generate and download a bootstrap configuration for multiple vEdge Cloud routers.
• Sync Smart Account—Download the updated device list to vManage NMS and send it to the vBond orchestrator.

• Table of routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.

• Controllers tab—Add controllers to the overlay network.
  • Add Controller drop-down—Add controllers to the overlay network.
  • Change mode drop-down—Switch between vManage and CLI mode.
  • Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.

• Refresh icon—Click to refresh data in the device table with the most current data.

• Export icon—Click to download all data to a file, in CSV format.

• Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
### Change Configuration Modes

To toggle a router from vManage mode to CLI mode:

1. In WAN Edge List tab, select a device.
2. Click the Change Mode drop-down and select CLI mode.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

To toggle a controller device from vManage mode to CLI mode:
1. In the Controllers tab, select a device.

2. Click the Change Mode drop-down.

3. Select CLI mode and then select the device type. The Change Mode CLI window opens.

4. From the vManage mode pane, select the device and click the right arrow to move the device to the CLI mode pane.

5. Click Update to CLI Mode.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

**Upload WAN Edge Router Authorized Serial Number File**

The WAN Edge router authorized serial number file contains the chassis and serial numbers of all valid vEdge routers in the overlay network. You receive this file from Viptela. Then, from the vManage NMS, you send it to the controllers in the network. This file is required to allow the Viptela overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

To upload the WAN edge router authorized serial number file to the vManage NMS and then download it to all the controllers in the overlay network:

1. In the WAN Edge List tab, click Upload WAN Edge List.

2. In the Upload WAN Edge List window:
   1. Click Choose File and select the WAN edge router authorized serial number file you received from Viptela.
   2. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.

3. Click Upload.

A list of routers in the network is displayed in the router table, with details about each router.

**Upload WAN Edge Router Serial Numbers from Cisco Smart Account**

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to the vManage NMS and then download it to all the controllers in the overlay network:

1. In the WAN Edge List tab, click Sync Smart Account.

2. In the Sync Smart Account window:
   1. Enter the username and password for your Smart account.
   2. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the checkbox Validate the Uploaded WAN Edge List and Send to Controllers is selected. (It is selected by default.) If you do not select this option, you must individually validate each router in Configuration ► Certificates ► WAN Edge List.

3. Click Sync.
A list of routers in the network is displayed in the router table, with details about each router.

**Generate Bootstrap Configuration for a vEdge Cloud Router**

For vEdge Cloud routers, you need to generate a bootstrap configuration file that you use when you create vEdge cloud VM instances.

To generate and download a bootstrap configuration for one or more vEdge Cloud routers:

1. In the WAN Edge List tab, click the Export Bootstrap Configuration button.
2. In the Export Bootstrap Configuration window, in the Bootstrap Configuration field, click Cloud-Init or Encoded String, depending the Hypervisor you are using to bring up the vEdge Cloud router.
3. Select the devices to configure from the Available Devices pane, or click Select All to select all devices.
4. Click the right arrow to move the devices to the Selected Devices pane.
5. Click Generate Configuration. The configurations are downloaded to the vManage NMS.
6. Provision the vEdge Cloud router instance in AWS, KVM, or ESXi with the bootstrap configuration. By default, ge0/0 is the device's tunnel interface and is a DHCP client. To use an interface other than ge0/0 as the tunnel interface or to use a static IP as the IP address, reconfigure the device through the CLI. For more information about configuring interfaces, see Configure Network Interfaces.

After you provision the vEdge Cloud router instance, vManage NMS installs a certificate on the device and the device's token changes to a serial number. After the device's control connections to vManage NMS come up, any templates attached to the device are automatically pushed to the device.

**Export Device Data in CSV Format**

To export data for all devices to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named viptela_download.csv.

**View a Device's Running Configuration**

To view a device's running configuration:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Running Configuration.

**View a Device's Configuration**

To view a device's configuration created using Configuration ► Templates:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Local Configuration.
**Delete a WAN Edge Router**

Deleting a router removes its serial and chassis numbers from the WAN edge router serial number list and permanently removes the router's configuration from the vManage NMS.

1. In the Configuration ► Certificates screen, mark the WAN Edge router as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the router.
3. Click the More Actions icon to the right of the row and click Delete WAN Edge.
4. Click OK to confirm deletion of the device.
5. In the Configuration ► Certificates screen, click Send to Controller.

**Copy Router Configuration**

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

To copy the configuration from the old router to the new router:

1. In the Configuration ► Certificates screen, mark the new vEdge router as invalid.
2. In the Configuration ► Devices screen, in the WAN Edge List tab, select the old router.
3. Click the More Actions icon to the right of the row and click Copy Configuration.
4. In the Copy Configuration window, select the new router.
5. Click Update to confirm the copy of the configuration.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

1. In the Configuration ► Certificates screen, mark the new router as valid.
2. Click Send to Controller.

**Decommission a vEdge Cloud Router**

Decommissioning a vEdge Cloud router removes the device's serial number from vManage NMS and generates a new token for the device. To do so:

1. In the WAN Edge List tab, select a vEdge Cloud router.
2. Click the More Actions icon to the right of the row and click Decommission WAN Edge.
3. Click OK to confirm the decommissioning of the router.

**View Log of Template Activities**

To view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Template Log.
**View Status of Device Bringup**

To view the status of the operations involved in bringing a router or controller up in the overlay network:

1. In the WAN Edge List or Controllers tab, select the device.
2. Click the More Actions icon to the right of the row and click Device Bring Up.

**Add a vBond Orchestrator**

1. In the Controllers tab, click the Add Controller drop-down and select vBond.
2. In the Add vBond window:
   1. Enter the management IP address of the vBond controller.
   2. Enter the username and password to access the vBond orchestrator.
   3. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.
   4. Click Add.

3. Repeat Steps 1 and 2 to add additional vBond orchestrators.

The new vBond orchestrator is added to the list of controllers in the Controllers screen.

**Add a vSmart Controller**

1. In the Controllers tab, click the Add Controller drop-down and select vSmart.
2. In the Add vSmart window:
   1. Enter the system IP address of the vSmart controller.
   2. Enter the username and password to access the vSmart controller.
   3. Select the protocol to use for control-plane connections. The default is DTLS.
   4. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   5. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.
   6. Click Add.

3. Repeat Steps 1 and 2 to add additional vSmart controllers. The vManage NMS can support up to 20 vSmart controllers in the network.

The new vSmart controller is added to the list of controllers in the Controllers screen.

**Edit Controller Details**

To edit the IP address and login credentials of a controller device:

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Edit window, edit the IP address and the login credentials.
4. Click Save.

**Delete a Controller**

1. In the Controllers tab, select the controller.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm the removal of the device and all its control connections.

**Configure Reverse Proxy on Controllers**

To configure reverse proxy on an individual vManage NMS and vSmart controller device:

1. In the Controllers tab, select the device.
2. Click the More Actions icon to the right of the row, and click Add Reverse Proxy. The Add Reverse Proxy popup is displayed.
3. Click Add Reverse Proxy.
4. Configure the private IP address and port number for the device. The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.
5. Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.
6. If the vManage NMS or vSmart controller has multiple cores, repeat Steps 4 and 5 for each core.
7. Click Add.

To enable reverse proxy in the overlay network, in vManage NMS select Administration ► Settings. Then click Edit to the right of the Reverse Proxy bar, click Enabled, and click Save.

**IPv6 Functionality**

This article describes the options for enabling IPv6 functionality for Cisco SD-WAN templates and policies.

**Configure IPv6 Functionality for an Interface or Subinterface Template**

To configure IPv6 functionality for an interface or subinterface template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
2. Select Feature ► Add Template and then select an appropriate device model.
3. Select VPN Interface Ethernet from the list of templates.
4. In the Basic Configuration area, click the IPv6 button and configure the parameters that the following table describes.
Table 5:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>This radio button is selected by default because IPv6 addresses are static.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Enter the IPv6 address of the interface or subinterface.</td>
</tr>
</tbody>
</table>

Configure IPv6 Functionality for an OMP Template

To configure IPv6 functionality for an Overlay Management Protocol (OMP) template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
2. Select Feature ► Add Template and then select an appropriate device model.
3. Select OMP from the list of templates.
4. In the Basic Configuration area, click the IPv6 button in the ADVERTISE area and configure the parameters that the following table describes.

Table 6:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Click On to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.</td>
</tr>
<tr>
<td>Connected</td>
<td>Click Off to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.</td>
</tr>
<tr>
<td>Static</td>
<td>Click Off to disable advertising static routes to OMP. By default static routes are advertised to OMP.</td>
</tr>
</tbody>
</table>

Configure IPv6 Functionality for a BGP Template

To configure IPv6 functionality for a Border Gateway Protocol (BGP) template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
2. Select Feature ► Add Template and then select an appropriate device model.
3. Select BGP from the list of templates.
4. In the Unicast Address Family area, click the IPv6 button and configure the parameters that the following table describes.
Table 7:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum Paths</td>
<td>Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing. Range: 0 to 32</td>
</tr>
<tr>
<td></td>
<td>Address Family</td>
<td>Enter the BGP IPv6 unicast address family.</td>
</tr>
</tbody>
</table>
| RE-DISTRIBUTE        | Protocol           | Click the **Redistribute** tab, and then click **Add New Redistribute**. Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following:  
  - For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.  
  - For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors. |
|                      | Route Policy       | Enter the name of the route policy to apply to redistributed routes. Click **Add** to save the redistribution information.                                                                         |
| NETWORK              | Network Prefix     | Click the **Network** tab, and then click **Add New Network**. Enter a network prefix, in the format of `prefix/length`, to be advertised by BGP.                                                    |
|                      | Click **Add** to save the network prefix. |
| AGGREGATE ADDRESS    | Aggregate Prefix   | Click the **Aggregate Address** tab, and then click **Add New Aggregate Address**. Enter the prefix of the addresses to aggregate for all BGP sessions, in the format `prefix/length`. |
|                      | AS Set Path        | Click **On** to generate set path information for the aggregated prefixes.                                                                                                                         |
|                      | Summary Only       | Click **On** to filter out more specific routes from BGP updates. Click **Add** to save the aggregate address.                                                                                      |

1. In the Neighbor area, click the **IPv6** button, create a new neighbor or edit an existing one, and then configure the parameters that the following table describes.

Parameters marked with an asterisk are required.
Table 8:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address*</td>
<td>Specify the IPv6 address of the BGP neighbor.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the BGP neighbor.</td>
</tr>
<tr>
<td>Remote AS*</td>
<td>Enter the AS number of the remote BGP peer.</td>
</tr>
<tr>
<td>Address Family</td>
<td>Select Global from the drop-down list, click On and select the address family. Enter the address family information.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>To shut down a BGP neighbor when you push the template, select Global from the drop-down list and then click Yes. Default: Off</td>
</tr>
</tbody>
</table>

Configure IPv6 Functionality for a VRRP Template

To configure IPv6 functionality for a Virtual Router Redundancy Protocol (VRRP) template, follow these steps:

1. In Cisco vManage NMS, select the Configuration ► Templates screen.
2. Select Feature ► Add Template and then select an appropriate device model.
3. Select VPN Interface Ethernet from the list of templates.
4. In the VRRP area, click the IPv6 button and then click New VRRP.
5. Configure the parameters that the following table describes.

Table 9:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Enter a virtual router ID, which represents a group of routers. Range: 1 through 255</td>
</tr>
</tbody>
</table>
| Priority       | Enter the priority level of the router within a VRRP group.  
|                 | • Range: 1 through 254  
|                 | • Default: 100 |
| Timer          | Not used. |
| Track OMP      | Select On to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the VRRP master virtual router. Default: Off |
| Track Prefix List | Enter a value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy. |
### Configure IPv6 Functionality for an SNMP Template

To configure IPv6 functionality for an SNMP template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **SNMP** from the list of templates.
4. In the SNMP Version area, click the **SNMP Version** button ► TRAP TARGET SERVER and create or edit an SNMP trap target.

1. Configure the parameters that the following table describes.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN ID</td>
<td>Enter the number of the VPN to use to reach the trap server. <em>Range: 0 through 65530</em></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the SNMP server.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>Enter the UDP port number for connecting to the SNMP server. <em>Range: 1 through 65535</em></td>
</tr>
<tr>
<td>Trap Group Name</td>
<td>Select the name of a trap group that was configured under the Group tab.</td>
</tr>
<tr>
<td>User Name</td>
<td>Select the name of a community that was configured under the Community tab.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Enter the interface to use to send traps to the SNMP server that is receiving the trap information.</td>
</tr>
</tbody>
</table>

Note: Make sure that you have already configured the SNMP community and trap target group.

### Configure IPv6 Functionality for a DHCP Relay Agent Template

To configure IPv6 functionality for a DHCP Relay Agent template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button.

5. Click **Add** next to DHCP Helper.

6. Configure the parameters that the following table describes.

**Table 11:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Helper #</td>
<td>IP address of the DHCP helper</td>
</tr>
<tr>
<td>DHCPv6 Helper VPN</td>
<td>VPN ID of the VPN source interface for the DHCP helper.</td>
</tr>
</tbody>
</table>

**Configure IPv6 Functionality for an ACL Template or a QoS Template**

To configure IPv6 functionality for an ACL and QoS template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the ACL/QoS area, configure the parameters that the following table describes.

**Table 12:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click on to enable the IPv6 ingress access list.</td>
</tr>
<tr>
<td>IPv6 Ingress Access List</td>
<td>Enter the name of the IPv6 ingress access list.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click on to enable the IPv6 egress access list.</td>
</tr>
<tr>
<td>IPv6 Egress Access List</td>
<td>Enter the name of the IPv6 egress access list.</td>
</tr>
</tbody>
</table>

**Configure IPv6 Functionality for a Logging Template**

To configure IPv6 functionality for a Logging template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **Logging** from the list of templates.
4. In the Server area, click the **IPv6** button.
5. Configure the parameters that the following table describes.
Table 13:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Hostname/IPv6 Address</td>
<td>Host name or IP address of the server to direct the logging information.</td>
</tr>
<tr>
<td>VPN ID</td>
<td>VPN ID of the VPN source interface.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Name of the source interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Choose the maximum severity of messages that are logged.</td>
</tr>
</tbody>
</table>

**Configure IPv6 Functionality for a New Prefix List**

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration ▶ Policies**.
2. From the Custom Options drop-down menu, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy.
3. Select **Prefix** from the list on the left and then select **New Prefix List**.
4. Select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

**Configure IPv6 Functionality for a Data Prefix**

To configure an IPv6 address for a new prefix list, follow these steps:

1. In Cisco vManage NMS, select **Configuration ▶ Policies**.
2. From the Custom Options drop-down menu, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy.
3. Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.
4. In the Internet Protocol area, select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

**Configure IPv6 Functionality for a Centralized Policy**

To configure a centralized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select **Configuration ▶ Policies**.
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select the **Traffic Data** tab.
4. Select Add Policy ▶ Create New.
5. Click the **Sequence Type** button and then select **Traffic Engineering**.
6. Click the **Sequence Rule** button.
7. From the Protocol drop-down list, select IPv6 to apply the policy only to IPv6 address families, or select Both to apply the policy IPv4 and IPv6 address families.

8. Click the Sequence Type button and then select QoS.

9. Click the Sequence Rule button.

10. From the Protocol drop-down list, select IPv6 to apply the policy only to IPv6 address families, or select Both to apply the policy IPv4 and IPv6 address families.

**Configure IPv6 Functionality for a Localized Policy**

To configure a localized policy to apply to IPv6 address families, follow these steps:

1. In Cisco vManage NMS, select Configuration ► Policies.

2. From the Custom Options drop-down menu, select Access Control Lists under Localized Policy.

3. Click the Add Access Control List Policy button and choose Add IPv6 ACL Policy. The policy you create will apply only to IPv6 address families.

---

**Network Design**

Use the Network Design screen to create and manage an overlay network topology. From this screen, you can add circuits, data centers, and branch sites to a network topology, configure LAN, WAN, and management options for elements in the topology, review the topology, and perform related tasks. The network design operations are particularly useful for smaller-scale deployments that include data centers and branch sites.

Network design consists of these major workflows:

- Create network topology—Create circuits, data centers, and branch sites, in this order. A network topology must include at least one circuit and one data center.

- Configure device profiles—Configure global parameters and options for LAN, WAN, and management settings.

- Attach devices profiles—Attach device profiles to devices.

- Ongoing management—Add elements to the network topology and modify the configuration settings for elements as needed.

**Access Network Design Options**

To access options for creating or updating a network design, select Configuration ► Network Design.

The Network Design screen displays. This screen includes the following items:

- Create Network Design button—Displays if you have not yet created a network topology. Click to create elements for the network. For more information, see Configure Network Design Elements.

- Manage Network Design button—Displays if you have created a network topology. Click to modify configuration setting for elements in the network. For more information, see Configure Network Design Elements.
• **Attach Devices** button—Click to access options for attaching a device profile to a device, detach a device profile from a device, export device profile configuration values to a CSV file, or modify values in a device profile. For more information, see Attach, Detach, Export, Update Device Profiles.

• Last modified information—Date and time that the network design was last modified.

• Device Attached Task option—Displays if the system is in the process of attaching a device profile to devices or updating device profile configuration information. For more information, see Attach Device Profile or Change Device Profile Values.

• Network design topology diagram—Displays if you have created a network topology. Figure 1 shows an example diagram.

Figure 1. Network Design Topology Display
Table 14:

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Custom device profile for a device in a data center. Custom profiles are indicated by a solid border and the icon at the top left corner. If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name. If a device profile is attached to 1 or more devices, the following icons and information display:</td>
</tr>
<tr>
<td></td>
<td>- Indicates the number of devices that the profile is successfully attached to.</td>
</tr>
<tr>
<td></td>
<td>- Indicates the number of devices that the profile failed to attach to. If there are failed attachments, the device is out of sync.</td>
</tr>
<tr>
<td></td>
<td>- Indicates the number of devices that the profile is in the process of attaching to.</td>
</tr>
<tr>
<td>2</td>
<td>Name of a data center. If the partial name of a data center displays, hover your mouse pointer over the name to see the full name.</td>
</tr>
<tr>
<td>3</td>
<td>Standard device profile for a device in a data center. Standard profiles are indicated by a dashed border. If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name. If a device profile is attached to 1 or more devices, icons and information display as described in Row 1 of this table.</td>
</tr>
<tr>
<td>4</td>
<td>Number of segments that are assigned to a data center or branch site. Hover your mouse pointer over the segment display to see the name of each segment.</td>
</tr>
<tr>
<td>5</td>
<td>TLOC connections between elements in the topology. A custom device profile does not display TLOC connections to other elements because its settings, such as LAN, WAN, and circuit configurations, have been converted to feature templates.</td>
</tr>
<tr>
<td>6</td>
<td>Circuit.</td>
</tr>
<tr>
<td>7</td>
<td>Name of a branch site. If the partial name of a branch site displays, hover your mouse pointer over the name to see the full name.</td>
</tr>
<tr>
<td>8</td>
<td>Standard device profiles for a device in a branch site. Standard profiles are indicated by a dashed border. If the partial name of a device profile displays, hover your mouse pointer over the name to see the full name. If a device profile is attached to 1 or more devices, icons and information display as described in Row 1 of this table.</td>
</tr>
<tr>
<td>9</td>
<td>A blue shaded icon with white arrows indicates that the device profile has been attached to 1 or more devices. Shaded circle with white arrows.</td>
</tr>
<tr>
<td>10</td>
<td>An unshaded icon with blue arrows indicates that the device profile has not been attached to any devices.</td>
</tr>
</tbody>
</table>
Configure Network Design Elements

With the network design feature, you can create a new overlay network topology and modify existing elements in a topology. You perform these activities from the Network Design screen.

Creating a new network topology involves performing the following procedures in the order shown:

Table 15:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add circuits.</td>
<td>See Configure Circuits</td>
</tr>
<tr>
<td>2</td>
<td>Add data centers.</td>
<td>See Configure Data Centers</td>
</tr>
<tr>
<td>3</td>
<td>Add branch sites.</td>
<td>See Configure Branch Sites</td>
</tr>
<tr>
<td>4</td>
<td>Configure global parameters.</td>
<td>See Configure Global Parameters</td>
</tr>
<tr>
<td>5</td>
<td>Configure device profiles.</td>
<td>See Configure Device Profiles</td>
</tr>
<tr>
<td>6</td>
<td>Attach device profiles.</td>
<td>See Attach Device Profile</td>
</tr>
</tbody>
</table>

A network topology must include at least one circuit and one data center. After a network topology is created, you can modify its elements directly.

Configure Circuits

Each network topology must have at least 1 circuit and can have up to 18 circuits.

To configure circuits for a network topology, follow these steps:

1. Select Configuration ► Network Design and then click Create Network Design (which displays if you have not yet created a network topology) or Manage Network Design (which displays if you have created a network topology).

2. Click Circuits near the top of the Network Design screen.

A screen for configuring circuits displays. If any circuits have been created, this screen lists them. You can remove a circuit by clicking its corresponding delete icon.

1. Click Add New Circuit.

2. Select the Private or the Public radio button to indicate whether the circuit is private or public.

3. From the Circuit Color drop-down list, choose a predefined color to uniquely identify the transport location (TLOC) in a circuit.

The color can be default, 3g, biz-internet, blue, bronze, custom1, custom2, custom3, gold, green, lte, metro-ethernet, mpls, private1, private2, public-internet, red, or silver. The color you choose cannot be used for a TLOC in any other circuit in the topology.

1. Repeat Steps 2 through 5 as needed to add more circuits.
To remove a circuit that you added, click its corresponding **Delete** icon.

1. Click Finish.
2. Click Save on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel**.

**Configure Data Centers**

Configuring a data center involves assigning a name and adding device profiles and segments to the data center. Each network topology must have at least one data center.

To configure data centers for a network topology, follow these steps:

1. Select **Configuration ► Network Design** and then click **Create Network Design** (which displays if you have not yet created a network topology) or **Manage Network Design** (which displays if you have created a network topology).

2. Click **Data Center** near the top of the Network Design screen.

This option appears dimmed if you have not added at least one circuit as described in Configure Circuits.

A screen for configuring data centers displays. If any data centers have been created, this screen lists them. If you are creating a network topology for the first time, skip to Step 4.

1. If any data centers are listed on the screen that displays, you can take any of these actions:

   - To add another data center, click **Add Data Center** and then continue to Step 4.
   - To view information about device profiles that have been added to a data center, click the **Devices** button to the right of the data center name.
   - To view information about segments that have been added to a data center, click the **Segments** button to the right of the data center name.
   - To update configuration items for a data center, including its name, device profiles, and segments, click the pencil icon to the right of the data center name and then continue to Step 4.
   - To remove a data center from the network topology, click the trash can icon to the right of the data center name and then skip to Step 8. You cannot delete a data center that includes any device profiles that are attached to one or more devices. To delete a data center in this situation, first detach the device profiles from devices. For instructions, see Detach Device Profile.

1. In the Data Center Name field, enter a unique name for the data center.

This name cannot be used for any other data center, branch site, or device profile in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

1. Take the following actions to add device profiles to the data center or to update device profile configuration settings:
Each data center must have at least one device profile. A device profile is associated with a specific device type in the data center and provides configuration settings that are pushed to those device types.

1. If you are adding a new device profile, click Add a Device Profile.

2. In the Name field, enter a name for the device profile. This name cannot be used for any other device profile, data center, or branch site in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

3. From the Device Model drop-down list, choose the device type with which to associate the device profile.

4. Click the Circuits field to display a list of circuits that you created as described in Configure Circuits and then check the box next to each circuit that the device profile should be associated with. The circuit names that you check appear in the Circuits field. You can remove a circuit from this field by unchecking its check box or by clicking the X next to its name. You can use the same circuit in multiple data centers and branch sites.

5. Repeat Steps 5a through 5d as needed to add more device profiles.

6. Click Next.

1. Take the following actions to add one or more segments.

Each data center must have at least one segment. A segment is a service side VPN that is associated with all device profiles in the data center. You can use the same segment in multiple data centers and branch sites.

1. Click Add Segment and choose one of these options:

   • New Segment—Creates a new segment with a new name and VPN ID
   • Existing Segment—Lets you choose a segment that you already created

1. In the Segment Name field, take one of these actions:

   • If you chose New Segment, enter a name for the segment. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.
   • If you chose Existing Segment, choose a segment from the drop-down list. The VPN Number field populates automatically with the VPN ID that was configured for the segment.

1. If you chose New Segment, in the VPN Number field, enter a LAN side VPN ID to associate with the segment. This value cannot be used for any other VPN number in the topology. Valid values are 1 through 65535, except 512.

2. Repeat Steps 6a through 6c as needed to add more segments. To remove a segment that you added, click its corresponding Delete icon.

3. Click Add.

The system displays a list of data centers.

1. Repeat Steps 2 through 6 as needed to add more data centers.
2. Click Finish.

3. Click Save on the Network Design screen.

Or, if you do not want to save the updates that you made, click Cancel.

**Configure Branch Sites**

Configuring a branch site involves assigning a name and adding device profiles and segments to the branch site. A network topology does not require branch sites.

To configure branch sites for a network topology, follow these steps:

1. Select Configuration ► Network Design and then click Create Network Design (which displays if you have not yet created a network topology) or Manage Network Design (which displays if you have created a network topology).

2. Click Branch Sites near the top of the Network Design screen.

This option appears dimmed if you have not added at least one circuit when you added a data center as described in Configure Data Center.

A screen for configuring branch sites displays. If any circuits have been created, this screen lists them. If you are creating a network design for the first time, skip to Step 4.

1. If any branch sites are listed on the screen that displays, you can take any of these actions:

   • To add another branch site, click Add Branch and then continue to Step 4.

   • To view information about device profiles that have been added to a branch site, click the Devices button to the right of the branch site name.

   • To view information about segments that have been added to a branch site, click the Segments button to the right of the branch site name.

   • To update configuration items for a branch site, including its name, device profiles, circuits, and segments, click the pencil item to the right of the branch site name and then continue to Step 4.

   • To remove a branch site from the network topology, click the trash can icon to the right of the branch site name and then skip to Step 8. You cannot delete a branch site that includes any device profiles that are attached to one or more devices. To delete a branch site in this situation, first detach device profiles from devices. For instructions, see Detach Device Profile.

1. In the Branch Name field, enter a name for the branch site.

   This name cannot be used for any other branch site, data center, or device profile in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

1. Take the following actions to add or update device profiles.

Each branch site must have at least one device profile. A device profile is associated with a specific device type in the branch site and provides configuration settings that are pushed to those device types.

1. If you are adding a new device profile, click Add a Device Profile.
2. In the Name field, enter a name for the device profile. This name cannot be used for any other device profile, data center, or branch site in the topology. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.

3. From the Device Model drop-down list, choose the device type with which to associate the device profile.

4. Click the Circuits field to display a list of circuits that you created as described in Configure Circuits and then check the box next to each circuit that the device profile should be associated with. The circuit names that you check appear in the Circuits field. You can remove a circuit from this field by unchecking its check box or by clicking the X next to its name. You can use the same circuit in multiple data centers and branch sites.

5. Repeat Steps 5a through 5d as needed to add more device profiles.

6. Click Next.

1. Take the following actions to add one or more segments.

Each branch site must have at least one segment. A segment is a service side VPN that is associated with all device profiles in the branch site. You can use the same segment in multiple branch sites and data centers.

1. Click Add Segment and choose one of these options:

   - New Segment—Creates a new segment with a new name and VPN ID
   - Existing Segment—Lets you choose a segment that you already created

1. In the Segment Name field, take one of these actions:

   - If you chose New Segment, enter a name for the segment. The name can include letters, numbers, underscores, and hyphens, but no spaces or special characters.
   - If you chose Existing Segment, choose a segment from the drop-down list. The VPN Number field populates automatically with the VPN ID that was configured for the segment.

1. If you chose New Segment, in the VPN Number field, enter a LAN side VPN ID to associate with the segment. This value cannot be used for any other VPN number in the topology. Valid values are 1 through 65535, except 512.

2. Repeat Steps 6a through 6c as needed to add more segments. To remove a segment that you added, click its corresponding Delete icon.

3. Click Add.

The system displays a list of branch sites.

1. Repeat Steps 2 through 6 as needed to add more branch sites.

2. Click Finish.

3. Click Save on the Network Design screen.

Or, if you do not want to save the updates that you made, click Cancel.
Configure Global Parameters

Global parameters are configuration settings that are used in all device profiles in a network topology. If you do not configure global parameters, factory default configuration settings are used for device profiles.

To configure global parameters, follow these steps:

1. Select Configuration ► Network Design and then click Create Network Design (which displays if you have not yet created a network topology) or Manage Network Design (which displays if you have created a network topology).

2. Click Global Parameters near the top of the Network Design screen and choose the desired template from the drop-down list that displays.

   A screen for configuring the selected template displays.

   1. Configure the template as described in the “Create a Device Template” section in Templates.

   The template name and description are filled in automatically and cannot be changed. There is no option for selecting a device type because the template is used for all devices throughout your network.

   1. Click Update.

   2. Click Save on the Network Design screen.

   Or, if you do not want to save the updates that you made, click Cancel.

Configure Device Profiles

You must configure a device profile for each router in a data center or branch site before the device profile can be attached to the router. Configuring a profile involves configuring its TLOC, LAN side, and management interfaces, and configuring related settings.

There are two types of device profiles:

- Standard device profile—Contains basic LAN, WAN, and management interface configuration options
- Custom device profile—Contains more advanced configuration options for a variety of items such as routing and other services for the interfaces

Each new device profile that you create is saved as a standard type. After you create a standard device profile and attach it to a device, you can convert it to a custom device profile as described in the following instructions.

To configure a device profile for a router in a network topology, follow these steps:

1. Select Configuration ► Network Design and then click Create Network Design (which displays if you have not yet created a network topology) or Manage Network Design (which displays if you have created a network topology).

1. In the network diagram that displays on the Network Design screen, click the image that represents the device for which you want to build or modify a device profile.

The image of the device displays in one of these ways:

- Blue shaded icon—Indicates that the device has a profile. When you hover your mouse pointer over this image, “Manage profile” displays.
If you choose this option for a standard device profile, the Manage Profile screen displays. From this screen, you can modify configuration settings for the device profile or convert it to a custom device profile. Continue to Step 3.

If you choose this option for a custom device profile, a template screen displays. Skip to Step 4.

- Unshaded icon—Indicates that the device does not yet have a profile. When you hover your mouse pointer over this image, “Build profile” displays.

If you choose this option, the Build Profile screen displays. From this screen, you can create a standard device profile. Skip to Step 5.

1. If you chose to manage a device profile for a standard device profile, take one of these actions:
   - To update existing options for the standard device profile, click the pencil icon that appears near the top right of the screen for managing a profile. The Build Profile screen displays. Skip to Step 5.
   - To convert the standard device profile to a custom device profile, click Custom Profile and then click Proceed in the dialog box that pops up. A template screen displays with some options pre-populated based on options that you have already configured for this device profile. Configure the options as desired. (For information about configuring a template, see the “Create a Device Template” section in Templates.) When you are finished, click Update and then skip to Step 17.

1. If you chose to manage a custom device profile, configure the options as desired. (For information about configuring a template, see the “Create a Device Template” section in Templates.) When you are finished, click Done and then skip to Step 17.

2. If you chose to build a device profile or to manage a standard device profile, In the Interface Name field, enter the name of a TLOC interface to associate with the circuit that is associated with this router.

3. Click one of these radio buttons:
   - DHCP—Selects a dynamic IP address for the interface
   - Static—Indicates that you will assign a static IP address to the interface and a prefix and next hop to the VPN later, as described in Attach Device Profile

1. (Optional) In the DNS server field, enter the IP address of the primary DNS server in the network.

2. Click Next.

3. In the Interface Name field, enter the name of a LAN side interface to associate with the segment.

4. (Optional) In the VLAN field, enter a sub-interface, if needed for your deployment.

5. Click one of these radio buttons:
   - None—Indicates that you will assign a static IP address to this interface later, as described in Attach Device Profile
   - DHCP—Indicates that you will assign a DHCP address pool to this interface later, as described in Attach Device Profile
   - DHCP Relay—Indicates that you will assign a DHCP helper address to this interface later, as described in Attach Device Profile

1. Click Next.
2. In the Interface Name field, enter the name for the management interface to associate with the device.

3. Click one of these radio buttons:
   - **DHCP**—Selects a dynamic IP address for the interface
   - **Static**—Indicates that you will assign a static IP address to the interface and a prefix and next hop to the VPN later, as described in Attach Device Profile

1. (Optional) In the DNS server field, enter the IP address of the primary DNS server in the network.
2. Click **Done**.
3. Click **Save** on the Network Design screen.

Or, if you do not want to save the updates that you made, click **Cancel**.

**Attach, Detach, Export, Update Device Profiles**

From the Network Design screen, you can perform the following tasks for existing device profiles.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach a device profile to devices.</td>
<td>Makes the devices available to be controlled and configured through the SD-WAN.</td>
<td>See Attach Device Profile.</td>
</tr>
<tr>
<td>Detach a device profile from devices.</td>
<td>Puts the devices into CLI mode.</td>
<td>See Detach Device Profile.</td>
</tr>
<tr>
<td>Export device profile settings</td>
<td>Creates a CSV file that contains configuration information of a selected device profile. This task is useful for backing up of device profile configuration information.</td>
<td>See Export Device Profile Settings.</td>
</tr>
<tr>
<td>Change configuration information for a device profile.</td>
<td>Updates device profile configuration information on the devices to which the profile is attached.</td>
<td>See Change Device Profile Values.</td>
</tr>
</tbody>
</table>

For information about creating a device profile, see Configure Device Profiles.

**Attach Device Profile**

Attaching a device profile to devices makes the devices available to be controlled and configured through the SD-WAN. A device to which a device profile is not attached is in CLI mode.

A device can have only one device profile. The same device profile can be attached to multiple devices.

To attach a device profile to devices, follow these steps:

1. Select **Configuration ► Network Design** and then click **Attach Device**.
2. In the network diagram that displays, click the device profile that you want to attach to devices and then choose **Attach Devices** from the pop-up list.
The Attach Devices window displays.

Configure options on this window as described in the “Attach Devices to a Device Template” section in Templates.

If, when you configured a device profile, if you configured static for a TLOC interface, or DHCP or DCHP relay for a VLAN subinterface, make sure to configure the static IP address, DHCP IP address, prefix information, and next hop information, as applicable.

After you configure devices, the Network Design screen displays and the configuration updates are pushed to the selected devices.

You can click the **Device Attached Task** option near the top right of the screen to view the progress of the configuration push operation.

**Detach Device Profile**

Detaching a device profile puts the devices to which it was attached into CLI mode.

To detach a device, follow these steps:

1. Select **Configuration ► Network Design** and then click **Detach Device**.
2. In the network diagram that displays, click the device profile that you want to detach from devices and then choose **Detach Devices** from the pop-up list.

The Detach Device window displays.

1. In the Available Devices column on the left, either select a group and search for one or more devices, select a device from the list, or click **Select All**.
2. Click the arrow pointing right to move the device to the Selected Devices column on the right.
3. Click **Detach**.

The device profile is detached from the devices that you selected.

**Export Device Profile Settings**

Exporting device profile settings creates a CSV file that contains the configuration information of a selected device profile. You can save this CSV file in the location of your choice. This export feature is useful for creating a backup of device profile configuration information.

A device profile must be attached to at least one device before you can export its configuration information.

To export a CSV file, follow these steps:

1. Select **Configuration ► Network Design** and then click **Export**.
2. In the network diagram that displays, click the device profile whose configuration information you want to export and then choose **Export CSV** from the pop-up list.
3. Follow the on-screen prompts to create the CSV file and save it to the location of your choice.

**Change Device Profile Values**

Changing device profile values updates device profile configuration information on the devices to which the profile is attached.
A device profile must be attached to at least one device before you can update its configuration information. To change device values, follow these steps:

1. Select Configuration ► Network Design and then click Profile.
2. In the network diagram that displays, click the device profile whose configuration values you want to update and then choose Change Device Values from the pop-up list.
3. In the window that displays, use the Search field and options to locate a device to which the profile is attached.
4. Click the More Actions icon to the right of the row for the applicable device and select Edit Device Template.
5. In the Update Device Template window that pops-up, modify values as desired, and then click Update.
6. Click Next.
7. Select a device from the list of devices that displays at the left of the window.
8. Click Configure Devices to push the configuration to all devices that the device profile is attached to.

The Network Design screen displays and the configuration updates are pushed to the selected devices. You can click the Device Attached Task option near the top right of the screen to view the progress of the configuration push operation.

Policies

Use the Policies screen to create and activate centralized and localized control and data policies for vSmart controllers and vEdge routers.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Policies, and the following:
  - Custom Options—Click to display, create, and edit a components for use in policy. For centralized policy, the components are CLI policies, lists, topologies, and traffic policies. For localized policy, the components are CLI policies, lists, forwarding class/QoS definitions, access control lists (ACLs), and route policies.
- Centralized Policy tab—Create a centralized policy. When you first open the Policies screen, the Centralized Policy tab is selected.
  - Add Policy—Click to create a centralized policy using a policy configuration wizard.
- Localized Policy tab—Create a localized policy.
  - Add Policy—Click to create a localized policy using a policy configuration wizard.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the policies table with the most current data.
- Show Table Columns icon—Click to display or hide columns from the policies table. By default, all columns are displayed.
- Policies table—To re-arrange the columns, drag the column title to the desired position.

**Configure Policies**

- Configure Centralized Policy
- Configure Localized Policy
**View a Policy**

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click View. Policies created with the UI policy builder are displayed in graphical format. Policies created using the CLI are displayed in text format.
3. Click Cancel to return to the policies table.

For a policy created using the vManage policy configuration wizard, you can view the policy in text format:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Preview.
3. Click Cancel to return to the policies table.

**Copy a Policy**

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.
4. Click Copy.

**Edit a Policy**

For policies created using the vManage policy configuration wizard:

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

For polices created using the CLI:

1. In the Custom Options drop-down, click CLI Policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Update.

**Edit or Create a Policy Component**

You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard:

1. In the Title bar, click the Custom Options drop-down.
2. For centralized policy, select the policy component:
• CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.

• Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.

• Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.

• Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.

1. For localized policy, select the policy component:

   • CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.

   • Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.

   • Forwarding Class/QoS—Create QoS mappings and rewrite rules to import in the Forwarding Classes/QoS screen in the policy configuration wizard.

   • Access Control Lists—Create ACLs of interest to import in the Configure Access Lists screen in the policy configuration wizard.

   • Route Policy—Create route policies to import in the Configure Route Policies screen in the policy configuration wizard.

Delete a Policy

1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the policy.

Activate a Centralized Policy on vSmart Controllers

1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Activate.
3. In the Activate Policy popup, click Activate to push the policy to all reachable vSmart controllers in the network.
4. Click OK to confirm activation of the policy on all vSmart controllers.

Deactivate a Centralized Policy on vSmart Controllers

1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Deactivate.
3. In the Deactivate Policy popup, click Deactivate to confirm that you want to remove the policy from all reachable vSmart controllers.
Configuring and Monitoring Forward Error Correction

Forward Error Correction is a mechanism to recover lost packets on a link by sending extra “parity” packets for every group (N) of packets. As long as the receiver receives a subset of packets in the group (at-least N-1) and the parity packet, up to a single lost packet in the group can be recovered.

Configuring Forward Error Correction for a Policy

To configure FEC, follow these steps:

Step 1  Select Configuration > Policies.
Step 2  Select Centralized Policy.
Step 3  Select Centralized Policy at the top of the page and then click Add Policy.
Step 4  Click Next twice to select Configure Traffic Rules
Step 5  Select Traffic Data, and from the Add Policy drop-down menu select click Create New.
Step 6  Click Sequence Type in the left panel.
Step 7  From the Add Data Policy pop-up menu, select QoS.
Step 8  Click Sequence Rule.
Step 9  Click Applications/Application Family List/Data Prefix.
Step 10 Select one or more applications or lists.
Step 11 Click Actions and select Loss Correction.
Step 12 In the Actions area, select one of the following:
  • FEC Adaptive—Only send FEC information only when the system detects packet loss
  • FEC Always—Always send FEC information with every transmission
  • Packet Duplication check box—Duplicates packets through secondary links to reduce packet loss if one link goes down
Step 13 Click Save Match and Actions.
Step 14 Click Save Data Policy.
Step 15 Click Next and take these actions to create a Centralized Policy:
  a) Enter a Name and Description.
  b) Select Traffic Data Policy.
  c) Choose VPNs/site list for the policy.
  d) Save the policy.

Monitoring Forward Error Correction Tunnel Information

To monitor FEC tunnel information, follow these steps:

Step 1  Select Monitor > Network.
Step 2  Select a device group.
Step 3

In the left panel, click **Tunnel**, which displays under WAN.

The WAN tunnel information includes the following:

- A graph that shows the total tunnel loss for the selected tunnels.
- A graph that shows the FEC loss recovery rate for the selected tunnels. The system calculates this rate by dividing the total number of reconstructed packets by the total number of lost packets on FEC.
- A table that provides the following information for each tunnel endpoint:
  - Name of the tunnel endpoint
  - Communications protocol that the endpoint uses
  - State of the endpoint
  - Jitter, in ms, on the endpoint
  - Packet loss percentage for the endpoint
  - FEC loss recovery percentage for the endpoint
  - Latency, in ms, on the endpoint
  - Total bytes transmitted from the endpoint
  - Total bytes received by the endpoint
  - Application usage link

---

**Monitoring Forward Error Application Family Information**

To monitor FEC application family information, follow these steps:

**Step 1**
Select **Monitor > Network**.

**Step 2**
Select a device group.

**Step 3**
In the left panel, click **DPI**, which displays under WAN.

The FEC application information includes the following:

- A graph for which you can select any of the following perspectives:
  - Application Usage—Usage of various types of traffic for the selected application families, in KB.
  - Application Goodput—Goodput metadata for the selected application families.
  - Mean Opinion Score (MOS)—MOS for the selected application families.
  - FEC Recovery Rate—FEC loss recovery rate for the selected application families. The system calculates this rate by dividing the total number of reconstructed packets by the total number of lost FEC-enabled packets.
- A table that provides the following for each application family:
  - Name of the application family.
• Goodput, in kbps, for the application family.
• MOS for the selected application family.
• FEC loss recovery percentage for the application family.
• Traffic usage, in MB, for the selected application family.

Integrating with Cisco ACI

Cisco ACI release 4.1(1) adds support for WAN SLA policies. This feature enables tenant administrator to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for tenant traffic over the WAN. When a WAN SLA policy is applied to tenant traffic, the Cisco APIC sends the configured policies to a vManage controller. The vManage controller, which is configured in Cisco ACI as an external device manager that provides Cisco SD-WAN capabilities, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy.

The WAN SLA policies are applied to tenant traffic through contracts.

Integrating with Cisco ACI Overview and Guidelines

The general steps that you perform in vManage to configure the integration are:

1. Verify that Cisco ACI has registered the desired controller as a partner with a vManage controller, as described in the Verify Cisco ACI Registration section.

2. Attach devices to the vManage controller, as described in the Map ACI Sites section.

The following guidelines apply when integrating vManage with Cisco ACI:

• Only new SD-WAN deployments support this integration.

• Make sure that any devices to which the Cisco APIC sends policies do not have any application-aware routing policies configured for them.

• Make sure each device to which the Cisco APIC sends policies has an attached template.

• Before you begin the integration, use the CLI policy builder to create a centralized policy and activate it by using the vManage policy builder.

• Before you apply WAN SLA policies, establish a connection between the vManage controller and the Cisco APIC. For instructions, see Cisco ACI and SDWAN Integration.

• Before you attach devices, configure Cisco ACI for this integration. For more information and instructions, see the Cisco ACI Integrations documentation.

Verifying Cisco ACI Registration

After you configure Cisco ACI for integration with vManage, perform the following steps in vManage to verify that Cisco ACI has registered the desired controller as a vManage partner:
Step 1  In vManage, select **Administration > Integration Management**.
The Integration Management page displays.

Step 2  On the Integration Management page, verify that “ACI Partner Registration” appears in the Description for the controller to which the Cisco APIC is to send policies.

**Mapping ACI Sites**

Mapping ACI sites designates the controller devices to which the policies from Cisco APIC apply.

Before you begin, review the guidelines in the Integration Overview and Guidelines section.

To attach devices to a controller, follow these steps:

Step 1  In vManage, select **Administration > Integration Management**.
The Integration Management page displays.

Step 2  Click the **More Actions** icon to the right of the row for the applicable site and select **Attach Devices**.

Step 3  In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.

Step 4  Click the arrow pointing right to move the device to the Selected Devices column on the right.

To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click **Select All**, and then click the arrow pointing left.

Step 5  Click **Attach**.

**Unmapping ACI Sites**

Unmapping ACI sites stops Cisco APIC policies from being applied to the unmapped devices.

To detach devices from a controller, follow these steps:

Step 1  In vManage, select **Administration > Integration Management**.
The Integration Management page displays.

Step 2  Click the **More Actions** icon to the right of the row for the applicable site and select **Detach Devices**.

Step 3  In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.

Step 4  Click the arrow pointing right to move the device to the Selected Devices column on the right.

To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click **Select All**, and then click the arrow pointing left.
Deleting a Controller

Deleting a controller removes it as a partner with Cisco ACI.

If you want to remove a controller as a partner with Cisco ACI, we recommend that you remove its registration by using Cisco ACI instead of deleting it in vManage.

Step 5  Click **Detach**.

---

Templates

Use the Templates screen to configure all Viptela devices in the overlay network that are managed by the vManage NMS. To do so:

1. Create a device template.
2. Attach Viptela devices to the device template.

Note: To create and modify a device's configuration, use vManage templates, along with other configuration-related screens in the vManage Configuration and Administration menus. Do not modify configurations from the command-line interface (CLI) unless you are explicitly directed to do so.

Screen Elements

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, Templates.
- **Device tab**—Create device templates for configuring Viptela devices.
  - **Create Template drop-down**—Click to create device templates from feature template or the CLI.
  - **Device template table**—Table of all device templates. To re-arrange the columns, drag the column title to the desired position.
- **Feature tab**—Create feature templates for configuring software features that you can enable on a Viptela device.
  - **Add Template button**—Click to create feature templates.
• Feature template table—Table of all feature templates. To re-arrange the columns, drag the column title to the desired position.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.

• Refresh icon—Click to refresh data in the templates table with the most current data.

• Show Table Columns icon—Click to display or hide columns from the templates table. By default, all columns are displayed.

• Templates table—To re-arrange the columns, drag the column title to the desired position.
Create a Device Template

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Viptela software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones too, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_{feature-name}_Template) or you can create a custom feature template.

Create a Device Template from Feature Templates

To create a device template:

1. In the Device tab, click the Create Template drop-down and select From Feature Template.
2. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.
6. To create a custom template for a feature, select the desired factory-default feature template and click Create Template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.
7. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
8. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.
9. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.
10. When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 17:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Use Variable Values in Configuration Templates. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

1. For some groups of parameters, you can mark the entire group as device-specific. To do this, click the Mark as Optional Row box. These parameters are then grayed out so that you cannot enter a value for them in the feature template. You enter the value or values when you attach a Viptela device to a device template.

2. Click Save.

3. Repeat Steps 7 through 13 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in Available Feature Templates.

4. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see Available Feature Templates.

1. From the Templates title bar, select Feature.

2. Click the Add Template button.

3. In the left pane, from Select Devices, select the type of device for which you are creating a template. You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

4. In the right pane, select the feature template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters. If the
feature has optional parameters, the bottom of the template form shows a plus sign (+) after the required parameters.

5. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter's value box.

8. Click the plus sign (+) below the required parameters to set the values of optional parameters.

9. Click Save.

10. Repeat Steps 2 to 9 for each additional feature template you wish to create.

11. From the Templates title bar, select Device.

12. Click the Create Template drop-down and select From Feature Template.

13. From the Device Model drop-down, select the type of device for which you are creating the device template. vManage NMS displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

14. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

15. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

16. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.

17. To use the factory-default configuration, click Create to create the device template. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

18. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.

19. Repeat Step 18 for each factory-default feature template you wish to modify.

20. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a Device Template from the CLI

To create a device template by entering a CLI text-style configuration directly on the vManage NMS:

1. In the Device tab, click the Create Template drop-down and select CLI Template.
2. From the Device Type drop-down, select the type of device for which you are creating the template.

3. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

5. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

6. To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format {{variable-name}}; for example, {{hostname}}.

7. Click Add. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

**Edit a Template**

1. In the Device or Feature tab, select a template.

2. Click the More Actions icon to the right of the row and click Edit.

You cannot change the name of a device or feature template when that template is attached to a device.

Note that you can edit templates simultaneously from one or more vManage servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

**View a Template**

1. In the Device or Feature tab, select a template.

2. Click the More Actions icon to the right of the row and click View.

**Delete a Template**

1. In the Device or Feature tab, select a template.

2. Click the More Actions icon to the right of the row and click Delete.

3. Click OK to confirm deletion of the template.
View Device Templates Attached to a Feature Template

1. In the Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Device Templates. The View Attached Device Templates popup window opens, displaying the names of the device templates to which the feature template is attached.

View Devices Attached to a Device Template

For a device template that you created from feature templates:
1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices.
3. In the Attach Devices window, click the Attached Devices tab.

For a device template that you created from a CLI template:
1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Devices.

Perform Parallel Template Operations

On Viptela devices in the overlay network, you can perform the same operations, in parallel, from one or more vManage servers. You can perform the following template operations in parallel:

- Attach devices to a device template
- Detach devices from a device template
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click Update Configure Devices, all other template operations—including attach devices, detach devices, and edit device values—are locked on all vManage servers until the update operation completes. This means that a user on another vManage server cannot perform any template operations until the update completes.

- You can perform the attach and detach device template operations on different devices, from one or more vManage servers, at the same time. However, if any one of these operations is in progress on one vManage server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Attach Devices to a Device Template

To attach one or more devices to a device template:
1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices. The Attach Devices dialog box opens with the Select Devices tab selected.
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.

4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

5. Click Attach.

6. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking the More Actions icon to the right of the row and clicking Edit Device Template. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.

1. Click Update

2. Click Next. If any devices have the same system IP address, a pop-up or an error message is displayed when you click Next. Modify the system IP addresses so that there are no duplicates, and click Save. Then click Next again.

3. In the left pane, select the device, to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the Config Preview tab in the upper right corner is selected. Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the Back button to edit the variable values entered in the previous screen.

4. If you are attaching a vEdge router, click Configure Device Rollback Timer located at the bottom of the left pane, to configure the time interval at which the device rolls back to its previous configuration if the router loses its control connection to the overlay network. The Configure Device Rollback Time dialog box is displayed.
   1. From the Devices drop-down, select a device.
   2. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
   3. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password field pops up. Enter the password that you used to log in to the vManage NMS.
   4. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.
   5. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.
   6. The table at the bottom of the Configure Device Rollback Time dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the Trash icon to right right of the device name.
   7. Click Save.
5. Click Configure Devices to push the configuration to the devices. The Status column displays whether
the configuration was successfully pushed. Click the right angle bracket to the left of the row to display
details of the push operation.

**Copy a Template**

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Copy.
3. Enter a new template name and description.
4. Click Copy.

**Edit a CLI Device Template**

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Device CLI Template window, edit the template.
4. Click Update.

**Export a Variables Spreadsheet in CSV Format for a Template**

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Export CSV.

**Change the Device Rollback Timer**

By default, when you attach a vEdge router to a configuration template, if the router is unable to successfully
start after 5 minutes, it returns to, or rolls back to, the previous configuration For a configuration that you
have created from the CLI, you can change the device's rollback timer:

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane
displays the device's configuration, and the Config Preview tab in the upper right corner is selected.
3. In the left pane, click the name of a device.
4. Click Configure Device Rollback Timer located at the bottom of the left pane. The Configure Device
Rollback Time dialog box is displayed.
5. From the Devices drop-down, select a device.
6. To enable the rollback timer, in the Set Rollback slider beneath the Devices drop-down, drag the slider
to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.
7. To disable the rollback timer, click the Enable Rollback slider. When you disable the timer, the Password
field pops up. Enter the password that you used to log in to the vManage NMS.
8. In the Device Rollback Time slider, drag the slider to the desired value. The default time is 5 minutes.
You can configure a time from 6 to 15 minutes.
9. To exclude a device from the rollback timer setting, click Add Exception and select the devices to exclude.

10. The table at the bottom of the Configure Device Rollback Time dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the Trash icon to right right of the device name.

11. Click Save.

12. Click Configure Devices to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

**Preview the Configuration and View Configuration Differences**

For a configuration that you have created from the CLI:

1. In the Device tab, select a device template.

2. Click the More Actions icon to the right of the row and click Change Device Values. The right pane displays the device's configuration, and the Config Preview tab in the upper right corner is selected.

3. In the left pane, click the name of a device.

4. Click the Config Diff tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the Back button to edit the variable values entered in the previous screen.

5. Click Configure Devices to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

**Change Variable Values for a Device**

For a configuration that you have created from device configuration templates, if the templates contain variables, the vManage NMS can automatically populate the variables with actual values when you attach the templates to the devices. To do this, you create an Excel file that lists the variable values for each device and save the file in CSV format. You can also enter values for these variables manually.

After you have pushed the configuration to a device, you can change the value assigned to any variable:

1. In the Device tab, select the device template.

2. Click the More Actions icon to the right of the row, and click Change Device Values. The screen displays a table of all the devices that are attached to that device template.

3. For the desired device, click the More Actions icon to the right of the row, and click Edit Device Template.

4. In the Update Device Template pop-up, enter values for the items in the variable list.

5. Click Update.

6. Click Next.

7. Click Configure Devices to push the configuration to the device. The Status column displays if the configuration was successfully pushed or not. Click the right angle bracket to the left of the row to display details of the push operation.
Available Feature Templates

vManage NMS provides the following feature templates to configure Viptela devices in the overlay network:

- AAA
- Archive
- Banner
- BFD
- BGP
- Bridge
- Cellular Controller
- Cellular Profile
- DHCP Server
- EIGRP
- GPS
- IGMP
- Logging
- Multicast
- NTP
- OMP
- OSPF
- PIM
- Security
- SNMP
- Switch Port
- System
- T1/E1 Controller
- VPN
- VPN Interface Bridge
- VPN Interface Cellular
- VPN Interface DSL PPPoA
- VPN Interface DSL PPPoE
- VPN Interface Ethernet
- VPN Interface GRE
• VPN Interface IPsec
• VPN Interface Multilink
• VPN Interface NAT Pool
• VPN Interface PPP
• VPN Interface PPP Ethernet
• VPN Interface SVI
• VPN Interface T1/E1
• WiFi Radio
• WiFi SSID

AAA

Use the AAA template for vBond controllers, vManage NMSs, vSmart controllers, vEdge routers, and Cisco IOS XE routers.

Viptela devices support configuration of authentication, authorization, and accounting (AAA) in combination with RADIUS and TACACS+.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Select the Basic Information tab.
6. To create a custom template for AAA, select the Factory_Default_AAA_Template and click Create Template. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 18:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure Authentication Order and Fallback

To configure AAA authentication order and authentication fallback on a Viptela device, select the Authentication tab and configure the following parameters:

Table 19:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Order</td>
<td>The default order is local, then radius, and then tacacs. To change the default order of authentication methods that the software tries when verifying user access to a Viptela device: 1. Click the dropdown arrow to display the list of authentication methods. 2. In the list, click the up arrows to change the order of the authentication methods and click the boxes to select or deselect a method. If you select only one authentication method, it must be <code>local</code>.</td>
</tr>
<tr>
<td>Authentication Fallback</td>
<td>Click On to configure authentication to fall back from RADIUS or TACACS+ to the next priority authentication method if the user cannot be authenticated or if the RADIUS or TACACS+ servers are unreachable. With the default configuration (Off), authentication falls back only if the RADIUS or TACACS+ servers are unreachable.</td>
</tr>
</tbody>
</table>
### Table 20: Configure Local Access for Users and User Groups

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, <em>The YANG 1.1 Data Modeling Language</em>. Each username must have a password. Each user is allowed to change their own password. The default password for the admin user is admin. It is strongly recommended that you change this password.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the user.</td>
</tr>
</tbody>
</table>
Select from the list of configured groups. You must assign the user to at least one group. The admin user is automatically placed in the netadmin group and is the only member of this group.

Click Add to add the new user. Click Add New User again to add additional users.

To configure local access for user groups, you first place the user into either the basic or operator group. The admin is automatically placed in the netadmin group. Then you configure user groups. To do this, select the Local tab, select the User Group tab, click Add New User Group, and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of an authentication group. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. The Viptela software provides three standard user groups, basic, netadmin, and operator. The user admin is automatically placed in the group netadmin and is the only user in this group. All users learned from a RADIUS or TACACS+ server are placed in the group basic. All users in the basic group have the same permissions to perform tasks, as do all users in the operator group. The following groups names are reserved, so you cannot configure them: adm, audio, backup, bin, cdrom, dialout, dip, disk, fax, floppy, games, gnats, input, irc, kmem, list, lp, mail, man, news, nogroup, plugdev, proxy, quagga, quaggavty, root, sasl, shadow, src, sshd, staff, sudo, sync, sys, tape, tty, uucp, users, utmp, video, voice, and www-data. Also, group names that start with the string viptela-reserved are reserved.</td>
</tr>
</tbody>
</table>

Click Add to add the new user group.

To add another user group, click Add New User Group again.

To delete a user group, click the trash icon at the right side of the entry. You cannot delete the three standard user groups, basic, netadmin, and operator.

**CLI equivalent:**
```
system
  aaa
    user username
      group group-name
    password password usergroup group-name
    task (interface | policy | routing | security | system) (read | write)
```

**Configure RADIUS Authentication**

To configure RADIUS authentication, select the RADIUS tab and configure the following parameters:
Table 22:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Retransmit Count       | Specify how many times to search through the list of RADIUS servers while attempting to locate a server.  
                         | Range: 1 through 1000 Default: 3                                            |
| Timeout                | Specify how long to wait to receive a reply form the RADIUS server before retransmitting a request.  
                         | Range: 1 through 1000 Default: 5 seconds                                     |

To configure a connection to a RADIUS server, select the RADIUS tab, click Add New Radius Server, and configure the following parameters:

Table 23:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the RADIUS server host.</td>
</tr>
<tr>
<td>Tag</td>
<td>Enter a text string to identify the RADIUS server. The tag can be 4 to 16 characters long. The tag allows you to configure authentication for AAA, IEEE 802.1X, and IEEE 802.11i to use a specific RADIUS server or servers. For Cisco routers running Viptela software, this field is ignored.</td>
</tr>
</tbody>
</table>
| Authentication Port    | Enter the UDP destination port to use for authentication requests to the RADIUS server.  
                         | If the server is not used for authentication, configure the port number to be 0.Default: Port 1812 |
| Accounting Port        | Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server.Range: 0 through 65535 Default: 1813 |
| Key (Deprecated)       | This field is deprecated. Use the Secret Key field instead.                 |
| Secret Key             | Enter the key the Viptela device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server. |
| Source Interface       | Enter the name of the interface on the local device to use to reach the RADIUS server. |
| VPN ID                 | Enter the number of the VPN in which the RADIUS server is located or through which the server can be reached. If you configure multiple RADIUS servers, they must all be in the same VPN. |
| Priority               | Enter the priority of a RADIUS server. A server with a lower number is given priority. Range: 0 through 7 Default: 0 |

Click Add to add the new RADIUS server.

To add another RADIUS server, click Add New RADIUS Server again.
To remove a server, click the trash icon on the right side of the line.

**CLI equivalent:**

```bash
system radius
  retransmit number
  server ip-address
    acct-port port-number
    auth-port port-number
    priority number
    secret-key key
    source-interface interface-name
    tag tag
    vpn vpn-id
    timeout seconds
```

### Configure TACACS+ Authentication

To configure the device to use TACACS+ authentication, select the TACACS tab and configure the following parameters:

**Table 24:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Timeout        | Enter how long to wait to receive a reply from the TACACS+ server before retransmitting a request.  
*Range:* 1 through 1000  
*Default:* 5 seconds |
| Authentication  | Set the type of authentication to use for the server password. The default authentication type is PAP. You can change it to ASCII. |

To configure a connection to a TACACS+ server, select the TACACS tab, click Add New TACSCS Server, and configure the following parameters:

**Table 25:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address of the TACACS+ server host.</td>
</tr>
</tbody>
</table>
| Authentication Port| Enter the UDP destination port to use for authentication requests to the TACACS+ server. If the server is not used for authentication, configure the port number to be 0.  
*Default:* Port 49 |
| Key (Deprecated)  | This field is deprecated. Use the Secret Key field instead. |
| Secret Key        | Enter the key the Viptela device passes to the TACACS+ server for authentication and encryption. You can type the key as a text string from 1 to 32 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS+ server. |
| Source Interface  | Enter the name of the interface on the local device to use to reach the TACACS+ server. |
### Parameter Name | Description
---|---
VPN ID | VPN in which the TACACS+ server is located or through which the server can be reached. If you configure multiple TACACS+ servers, they must all be in the same VPN.
Priority | Set the priority of a TACACS+ server. A server with lower priority number is given priority over one with a higher number. Range: 0 through 7. Default: 0

Click Add to add the new TACACS server.

To add another TACACS server, click Add New TACACS Server again.

To remove a server, click the trash icon on the right side of the line.

**CLI equivalent:**
```bash
system tacacs
    authentication password-authentication
    server ip-address
    auth-port port-number
    priority number
    key key
    source-interface interface-name
    vpn vpn-id
    timeout seconds
```

**Release Information**

Introduced in vManage NMS in Release 15.2. In Release 17.1, add Disable Netconf Logs and Disable Audit Logs fields.

## Archive

Use the Archive template for vBond controllers, vManage NMSs, vSmart controllers, and vEdge routers.

You can configure a Viptela device to periodically archive a copy of the full running configuration to an archival file. The running configuration that is archived is viewable by the user "admin".

### Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Under Additional System Templates, located to the right of the screen, click Archive.
6. From the Archive drop-down, click Create Template. The Archive template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Archive parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 26:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure Configuration Archive Configuration

To configure archiving of running configurations, configure the following parameters:

Table 27:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archival Interval</td>
<td>Specify how often to archive the full running configuration. In addition, the running configuration is archived each time you issue the commit command on the device. <strong>Range:</strong> 5 minutes through 525600 minutes (about one year) <strong>Default:</strong> 10080 minutes (7 days)</td>
</tr>
<tr>
<td>Path to Archive File Directory</td>
<td>Specify the path to the directory in which to store the archival file and the base name of the file. The path can be one of the following: • ftp: file-path—Path to a file on an FTP server. • scp: user@host: file-path • path file-path/filename</td>
</tr>
<tr>
<td>SSH Key File</td>
<td>Enter the name of the SSH private key file on the local Viptela device. This file is used to SCP into a remote file server. The Viptela software automatically generates a public and a private key and places the public key in the SSH key file archive_id_rsa.pub, which is located in /home/admin directory on the Viptela device. If you do not enter the name of an SSH private key file, the software uses the automatically generated private key.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>VPN ID</td>
<td>Enter the ID for the VPN in which the archival file server is located or through which the server can be reached. On vEdge routers, <em>vpn-id</em> can be a value from 0 through 65530. On vSmart controllers, <em>vpn-id</em> can be either 0 or 512.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```
system archive
    interval minutes
    path file-path
    ssh-id-file filename
    vpn vpn-id
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**Banner**

Use the Banner template for vBond controllers, vManage NMSs, vSmart controllers, vEdge routers, and Cisco IOS XE routers.

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.

- To configure the banner text for login screens using vManage templates, create a Banner feature template to configure PIM parameters, as described in this article.

- To configure a login banner for the vManage NMS system, see the Administration ➤ Settings help file.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ➤ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. From the Banner drop-down, click Create Template. The Banner template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Banner parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 28:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
  When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.  
  To change the default key, type a new string and move the cursor out of the Enter Key box.  
  Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.                                                                 |
| Global (indicated by a globe icon)       | Enter a value for the parameter, and apply that value to all devices.  
  Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.                                                                                     |

Configure the Banner

To set a banner, configure the following parameters:

Table 29:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Banner</td>
<td>Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n.</td>
</tr>
<tr>
<td>MOTD Banner</td>
<td>Enter message-of-the-day text to display after a successful login. The string can be up to 2048 characters long. To insert a line break, type \n.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:

```bash
banner
  login "text"
  motd "text"
```

Release Information

Introduced in vManage NMS in Release 15.2.
BFD

Use the BFD template for vEdge routers and Cisco IOS XE routers.

The BFD protocol, which detects link failures as part of the Viptela high availability solution, is enabled by default on all vEdge routers, and you cannot disable it.

Navigate to the Template Screen
1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for BFD, select the Factory_Default_BFD_Template and click Create Template. The BFD template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining BFD parameters. You may need to click a tab or the plus sign (+) to display additional fields.
6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 30:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure BFD for Application-Aware Routing

To configure the BFD timers used by application-aware routing, click the Basic Configuration tab and configure the following parameters:

Table 31:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplier</td>
<td>Specify the value by which to multiply the poll interval, to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet configured SLAs. \textit{Range:} 1 through 6 \textit{Default:} 6</td>
</tr>
<tr>
<td>Poll Interval</td>
<td>Specify how often BFD polls all data plane tunnels on a vEdge router to collect packet latency, loss, and other statistics used by application-aware routing. \textit{Range:} 1 through 4,294,967,296 \textit{(2^{32} – 1) milliseconds} \textit{Default:} 600,000 milliseconds (10 minutes)</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:

```
bfd app-route
  multiplier number
  poll-interval milliseconds
```
Configure BFD on Transport Tunnels

To configure the BFD timers used on transport tunnels, click the Color tab, click Add New Color, and configure the following parameters:

Table 32:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>From the drop-down, choose the color of the transport tunnel for data traffic moving between vEdge routers. The color identifies a specific WAN transport provider. Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver Default: default</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Specify how often BFD sends Hello packets on the transport tunnel. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel. Range: 100 through 60000 milliseconds Default: 1000 milliseconds (1 second)</td>
</tr>
<tr>
<td>Multiplier</td>
<td>Specify how many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time. Range: 1 through 60 Default: 7 (for hardware vEdge routers), 20 (for vEdge Cloud software routers)</td>
</tr>
<tr>
<td>Path MTU Discovery</td>
<td>Click On to enable path MTU discovery for the transport tunnel, or Off to disable. When PMTU discovery is enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. When PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes, but the effective tunnel MTU is 1468 bytes. Default: Enabled</td>
</tr>
<tr>
<td>Add</td>
<td>Click Add to save the data traffic transport tunnel color.</td>
</tr>
</tbody>
</table>

To add another color, click Add New Color.

A table lists the transport tunnel colors.

To edit a color, click the Pencil icon. The Update Color popup is displayed. After you make the desired changes, click Save Changes.

To remove a color, click the trash icon to the right of the entry.

To save the feature template, click Save.

**CLI equivalent:**

```
bfd  color color
    hello-interval  milliseconds
    multiplier  number
    pmtu-discovery
```

**Release Information**

Introduced in vManage NMS in Release 15.2.
Configuring BGP

Use the Border Gateway Protocol (BGP) template for all vEdge Cloud and vEdge router devices.

To configure the BGP routing protocol using vManage templates:

1. Create a BGP feature template to configure BGP parameters, as described in this article. BGP can be used for service-side routing, to provide reachability to networks at the local site, and it can be used for transport-side routing, to enable communication between the vEdge router and other SD-WAN devices when the router is not directly connected to the WAN cloud. Create separate BGP templates for the two BGP routing types.

2. Create a VPN feature template to configure VPN parameters for either service-side BGP routing (in any VPN other than VPN 0 or VPN 512) or transport-side BGP routing (in VPN 0).

Find and Name the Template

**Step 1**  
In vManage NMS, select the Configuration ► Templates screen.

**Step 2**  
In the Device tab, click Create Template.

**Step 3**  
From the Create Template drop-down, select From Feature Template.

**Step 4**  
From the Device Model drop-down, select the type of device for which you are creating the template.

**Step 5**  
To create a template for VPN 0 or VPN 512:

a) Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

b) Under Additional VPN 0 Templates, located to the right of the screen, click BGP.

c) From the BGP drop-down, click Create Template. The BGP template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP parameters.

**Step 6**  
To create a template for VPNs 1 through 511, and 513 through 65530:

a) Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

b) Click the Service VPN drop-down.

c) Under Additional VPN Templates, located to the right of the screen, click BGP.

d) From the BGP drop-down, click Create Template. The BGP template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining BGP parameters.
Step 7  In the **TemplateName** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8  In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

## Configuring Basic BGP

To configure Border Gateway Protocol (BGP), select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure BGP.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shutdown</strong></td>
<td>Click <strong>No</strong> to enable BGP on the interface.</td>
</tr>
<tr>
<td><strong>AS number</strong></td>
<td>Enter the local AS number.</td>
</tr>
<tr>
<td><strong>Router ID</strong></td>
<td>Enter the BGP router ID, in decimal four-part dotted notation.</td>
</tr>
<tr>
<td><strong>Propagate AS Path</strong></td>
<td>Click <strong>On</strong> to carry BGP AS path information into OMP.</td>
</tr>
</tbody>
</table>
| **Internal Routes Distance** | Enter a value to apply as the BGP route administrative distance for routes coming from one AS into another.  
  Range: 0 through 255  
  Default: 0 |
| **Local Routes Distance** | Specify the BGP route administrative distance for routes within the local AS.  
  By default, a route received locally from BGP is preferred over a route received from OMP.  
  Range: 0 through 255  
  Default: 0 |
| **External Routes Distance** | Specify the BGP route administrative distance for routes learned from other sites in the overlay network.  
  Range: 0 through 255  
  Default: 0 |

For service-side BGP, you might want to configure Overlay Management Protocol (OMP) to advertise to the vSmart controller any BGP routes that the vEdge router learns. By default, a vEdge router advertises to OMP both the connected routes on the vEdge router and the static routes that are configured on the vEdge router, but it does not advertise BGP external routes learned by the vEdge router. You configure this route advertisement in the OMP template for vEdge routers or vEdge software. See [OMP](#).

For transport-side BGP, you must also configure a physical interface and a loopback interface in VPN 0. In addition, you should create a policy for BGP to advertise the loopback interface address to its neighbors, and apply the policy in the BGP instance or to a specific neighbor. See the [Configuring Unicast Overlay Routing](#) article for your software release.

To save the feature template, click **Save**.
CLI Equivalent

```
vpn  vpn-id  router  bgp  local-as-number  distance  external  number  internal  number  local  number  propagate-aspath  router-id  ip-address  [no]  shutdown
```

Configuring the Unicast Address Family

To configure global BGP address family information, select the IPv4 Unicast Address Family tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Tab/Parameter</th>
<th>Option</th>
<th>Sub-Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 / IPv6</td>
<td>Click IPv4 to configure an IPv4 VPN interface. Click IPv6 to configure an IPv6 interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Paths</td>
<td>Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing.</td>
<td>Range: 0 to 32</td>
<td></td>
</tr>
<tr>
<td>Mark as Optional Row</td>
<td>Check Mark as Optional Row to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redistribute</td>
<td>Click the Redistribute tab, and then click New Distribute.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mark as Optional Row</td>
<td>Check Mark as Optional Row to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>static  Redistribute static routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>connected  Redistribute connected routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospf  Redistribute Open Shortest Path First routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>omp  Redistribute Overlay Management Protocol routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>nat  Redistribute Network Address Translation routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>natpool-outside  Redistribute outside NAT routes into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>At a minimum, select the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Route Policy</td>
<td>Enter the name of the route policy to apply to redistributed routes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click Add to save the redistribution information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To save the feature template, click **Save**.

**CLI Equivalent**

```
vpn vpn-id router bgp local-as-number  address-family ipv4-unicast aggregate-address prefix/length [as-set] [summary-only] maximum-paths paths number network prefix/length redistribute (connected | nat | omp | ospf | static)
```

### Configuring Neighbors

To configure a neighbor, select the Neighbor tab, click **New Neighbor**, and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Sub-Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 / IPv6</td>
<td>Click IPv4 to configure IPv4 neighbors. Click IPv6 to configure IPv6 neighbors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address/IPv6 Address</td>
<td>Specify the IP address of the BGP neighbor.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Advanced Parameters

To configure advanced parameters for BGP, click the Advanced tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Hold Time      | Specify the interval after not receiving a keepalive message that the local BGP session considers its peer to be unavailable. The local router then terminates the BGP session to that peer. This hold time is the global hold time.  
Range: 0 through 65535 seconds  
Default: 180 seconds (three times the keepalive timer) |
| Keepalive      | Specify the frequency at which keepalive messages are advertised to a BGP peer. These messages indicate to the peer that the local router is still active and should be considered to be available. This keepalive time is the global keepalive time.  
Range: 0 through 65535 seconds  
Default: 60 seconds (one-third the hold-time value) |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare MED</td>
<td>Click <strong>On</strong> to compare the router IDs among BGP paths to determine the active path.</td>
</tr>
<tr>
<td>Deterministic MED</td>
<td>Click <strong>On</strong> to compare multiple exit discriminators (MEDs) from all routes received from the same AS, regardless of when the route was received.</td>
</tr>
<tr>
<td>Missing MED as Worst</td>
<td>Click <strong>On</strong> to consider a path as the worst path if the path is missing a MED attribute.</td>
</tr>
<tr>
<td>Compare Router ID</td>
<td>Click <strong>On</strong> to always compare MEDs regardless of whether the peer ASs of the compared routes are the same.</td>
</tr>
<tr>
<td>Multipath Relax</td>
<td>Click <strong>On</strong> to have the BGP best-path process select from routes in different in ASs. By default, when you are using BGP multipath, the BGP best path process selects from routes in the same AS to load-balance across multiple paths.</td>
</tr>
</tbody>
</table>

To save the feature, click **Save**.

**CLI Equivalent**

```
vpn vpn-id
router
bgp local-as-number
best-path
as-path multipath-relax
compare-router-id
med (always-compare | deterministic | missing-as-worst)
timers
holdtime seconds
keepalive seconds
```

**Bridge**

Use the Bridge template for all vEdge Cloud and vEdge router devices.

To have a vEdge router act as a transparent bridge, configure bridging domains on the router. A router can have up to 16 bridging domains.

To configure the bridging domains using vManage templates:

1. Create a Bridge feature template, as described in this article.
2. Create a VPN Interface Bridge feature template to enable integrated routing and bridging (IRB). See the VPN Interface Bridge help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. Click the plus sign (+) next to Bridge.

7. From the Bridge drop-down, click Create Template. The Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Bridge parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 33:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.</td>
</tr>
<tr>
<td></td>
<td>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.</td>
</tr>
<tr>
<td></td>
<td>To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure Bridging Domains**

To configure bridging domains, select the Basic Configuration tab and configure the following parameters. For bridging to work, you must also associate interfaces with the bridging domain. Parameters marked with an asterisk are required to configure bridging.

**Table 34:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Name*</td>
<td>Enter a text description of the bridging domain. It can be up to 32 characters.</td>
</tr>
<tr>
<td>VLAN ID*</td>
<td>Enter the VLAN identifier to associate with the bridging domain.Range: 0 through 4095</td>
</tr>
<tr>
<td>Maximum MAC Addresses</td>
<td>Specify the maximum number of MAC addresses that the bridging domain can learn.Range: 0 through 4096Default: 1024</td>
</tr>
<tr>
<td>Age-Out Time</td>
<td>Specify how long to store an entry in the MAC table before it ages out.Range: 10 through 4096 secondsDefault: 300 seconds (5 minutes)</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

*CLI equivalent:*
Associate Interfaces with the Bridge Domain

To associate an interface with the bridge domain, click the Interface tab and click Add New Interface:

Table 35:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name*</td>
<td>Enter the name of the interface to associate with the bridging domain, in the format ge slot/port.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a text description of the interface.</td>
</tr>
<tr>
<td>Native VLAN Support</td>
<td>Click Enabled to configure the interface to carry untagged traffic. By default, native VLAN is disabled.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Click No to enable the interface. By default, an interface in a bridge domain is disabled.</td>
</tr>
<tr>
<td>Static MAC Address</td>
<td>Click Add Static MAC Address, and in the MAC Static Address field that appears, enter a static MAC address entry for the interface in the bridge domain. Click Add MAC Address to add another static MAC address entry for the interface. Click Save to save the MAC address or addresses.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:

```
bridge bridge-id interface interface-name
  description "text description"
  native-vlan
  [no] shutdown
  static-mac-address mac-address
```

Release Information

Introduced in vManage NMS in Release 15.3.

Cellular Controller

Use the Cellular Controller template for Cisco IOS XE routers running the SD-WAN software.

To use vManage templates to configure a cellular controller for a 4G network interface module (NIM) installed in a router, create a Cellular Controller template to configure cellular controller properties. This template is mandatory if the 4G NIM module is installed in the router.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.

5. Select the Cellular tab.

6. To create a cellular controller template, in the Cellular Controller drop-down click Create Template. The Cellular Controller template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining cellular controller parameters.

7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 36:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| **Device Specific** (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template.  
For more information, see Create a Template Variables Spreadsheet.  
To change the default key, type a new string and move the cursor out of the Enter Key box.  
Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| **Global** (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.  
Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

**Configure a Cellular Controller**

To configure a cellular controller, configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

**Table 37:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellular ID*</td>
<td>Enter the interface slot and port number in which the cellular NIM card is installed. Currently, it can be 0/1/0 or 0/2/0.</td>
</tr>
<tr>
<td>Primary SIM Slot*</td>
<td>Enter the number of the primary SIM slot. It can be 0 or 1. The other slot is automatically set to be the secondary. If there is a single SIM slot, this parameter is not applicable.</td>
</tr>
</tbody>
</table>
| SIM Failover Retries    | Specify the maximum number of times to retry connecting to the secondary SIM when service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.  
*Range: 0 through 65535*  
*Default: 10* |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| SIM Failover Timeout | Specify how long to wait before switching from the primary SIM to the secondary SIM if service on the primary SIM becomes unavailable. If there is a single SIM slot, this parameter is not applicable.  
Range: 3 to 7 minutes  
Default: 3 minutes |

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS Release 18.1.1.

**Cellular Profile**

Use the Cellular Profile feature template to configure the profiles used by cellular modems on vEdge routers and Cisco IOS XE routers running the SD-WAN software.

To configure a cellular profile using vManage templates:

1. Create a Cellular Profile template to configure the profiles used by the cellular modem, as described in this article.
2. Create a VPN-Interface-Cellular feature template to configure cellular module parameters. See the VPN-Interface-Cellular help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. Click the plus sign (+) next to Cellular-Profile.
7. From the Cellular-Profile drop-down, click Create Template. The Cellular-Profile template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Cellular-Profile parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 38:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure a Cellular Profile

To configure a cellular profile, in the Basic Configuration tab, configure the following parameters. Parameters marked with an asterisk are required to configure the cellular profile.

Table 39:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name*</td>
<td>Enter the name of the cellular interface, which must be cellular0.</td>
</tr>
<tr>
<td>Profile ID*</td>
<td>Enter the identification number of the profile to use on the router. You use this profile identification number when you configure for the cellular interface in the VPN-Interface-Cellular template.Range: 1 through 15</td>
</tr>
<tr>
<td>Access Point Name</td>
<td>Enter the name of the gateway between the service provider network and the public Internet. It can be up to 32 characters long.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select the authentication method used for the connection to the cellular network. It can be CHAP, None, PAP, or PAP/CHAP.</td>
</tr>
<tr>
<td>IP Address (on vEdge routers)</td>
<td>Enter the static IP address assigned to the cellular interface. This field is used when the service provider requires that a static IP address be preconfigured before attaching to the network.</td>
</tr>
<tr>
<td>Profile Name (on vEdge routers)</td>
<td>Enter a name to identify the cellular profile. It can be up to 14 characters long.</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
--- | ---
Packet Data Network Type | Select the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv46.
Profile Username | Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password | Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES encrypted key.
Primary DNS Address (on vEdge routers) | Enter the IP addresses of the primary DNS servers in the service provider network, in decimal four-part dotted notation.
Overwrite (on IOS XE routers) | Click On to overwrite the profile on the cellular modem.

To save the feature template, click Save.

**CLI equivalent:**
```
cellular cellular0
  profile number
  apn name
  auth auth-method
  ip-addr ip-address
  name profile-name
  pdn-type type
  primary-dns ip-address
  secondary-dns ip-address
  user-name user-name
  user-pass password
```

**Release Information**
Introduced in vManage NMS in Release 16.1.

---

**CLI Templates for Cisco XE SD-WAN Routers**

The CLI Templates for Cisco XE SD-WAN Routers features allows you to configure intent-based CLI templates for Cisco XE SD-WAN routers using vManage. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, vManage enables pushing vEdge syntax-based commands to Cisco XE SD-WAN Routers in Cisco IOS XE Syntax.

Using vManage CLI templates significantly reduces the effort to configure feature templates.
Feature Information for CLI Template for Cisco XE SD-WAN Routers

Table 40: Feature Information for CLI Template for Cisco XE SD-WAN Routers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Template for Cisco XE SD-WAN Routers</td>
<td>Cisco IOS XE Gibraltar 16.11.1a/Cisco SD-WAN release 19.1</td>
<td>The CLI Templates for Cisco XE SD-WAN Routers features allows to you configure intent-based CLI templates for Cisco XE SD-WAN routers using vManage.</td>
</tr>
</tbody>
</table>

Benefits of CLI Templates

- You can reuse any Cisco vEdge-specific vManage feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, vManage displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SD-WAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

Configuring CLI Templates in vManage

1. In vManage, select Configuration ► Templates.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select CLI Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
6. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
7. The configuration of the CLI template must be intent-based. You can upload a configuration file using the Select a File field or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```system```
These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

8. To save the feature template, click Add.

---

**Note**

See the Attach Devices to a Device Template section in this topic to know more about attaching a device to a template and reusing a template for multiple devices of the same device model.

---

**Sample Configurations for CLI Template**

**System Level Configuration**

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td>host-name pm4</td>
<td>host-name pm4</td>
</tr>
<tr>
<td>system-ip 172.16.255.14</td>
<td>system-ip 172.16.255.14</td>
</tr>
<tr>
<td>overlay-id 1</td>
<td>overlay-id 1</td>
</tr>
<tr>
<td>site-id 400</td>
<td>site-id 400</td>
</tr>
<tr>
<td>control-session-pps 300</td>
<td>control-session-pps 300</td>
</tr>
<tr>
<td>admin-tech-on-failure</td>
<td>admin-tech-on-failure</td>
</tr>
<tr>
<td>sp-organization-name &quot;XYZ Inc Regression&quot;</td>
<td>sp-organization-name &quot;XYZ Inc Regression&quot;</td>
</tr>
<tr>
<td>organization-name &quot;XYZ Regression&quot;</td>
<td>organization-name &quot;XYZ Regression&quot;</td>
</tr>
<tr>
<td>console-baud-rate 115200</td>
<td>console-baud-rate 11520</td>
</tr>
<tr>
<td>vbond 10.0.12.26 port 12346</td>
<td>vbond 10.0.12.26 port 12346</td>
</tr>
</tbody>
</table>
### AAA Configuration - Authentication, authorization, and accounting (AAA) with RADIUS and TACACS+

**Table 42: AAA Configuration**

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa</code></td>
<td><code>aaa group server tacacs+ server-10.0.1.1</code></td>
</tr>
<tr>
<td><code>auth- order local radius tacacs</code></td>
<td><code>server-private 10.0.1.1 timeout 5 key $8$vs5h2Vg/Z6Eeu9dNHTz0wWP6tUv97/50xmcRfShWp3YI=</code></td>
</tr>
<tr>
<td><code>usergroup basic</code></td>
<td><code>ip tacacs source-interface GigabitEthernet0/0/1</code></td>
</tr>
<tr>
<td><code>task system read write</code></td>
<td><code>aaa group server radius server-10.99.144.200</code></td>
</tr>
<tr>
<td><code>task interface read write</code></td>
<td><code>server-private 10.99.144.200 auth-port 1812 timeout 5 retransmit 3</code></td>
</tr>
<tr>
<td><code>usergroup netadmin</code></td>
<td><code>ip radius source-interface GigabitEthernet0/0/1</code></td>
</tr>
<tr>
<td><code>usergroup operator</code></td>
<td><code>aaa group server radius server-10.99.144.201</code></td>
</tr>
<tr>
<td><code>task system read</code></td>
<td><code>server-private 10.99.144.201 auth-port 1812 timeout 5 retransmit 3</code></td>
</tr>
<tr>
<td><code>task interface read</code></td>
<td><code>ip radius source-interface GigabitEthernet0/1/0</code></td>
</tr>
<tr>
<td><code>task policy read</code></td>
<td><code>aaa authentication login default local group radius group tacacs+</code></td>
</tr>
<tr>
<td><code>task routing read</code></td>
<td><code>aaa authorization exec default local group radius group tacacs+</code></td>
</tr>
<tr>
<td><code>task security read</code></td>
<td><code>aa session-id common --- added by default</code></td>
</tr>
<tr>
<td><code>!</code></td>
<td><code>username admin password $6$nbbLkA==$ae/DO78l/wluPuhbhBU2L6h/ P.LkuryGvx3JRLS9OBh9rTfWSGbf6Qh5w6AHRHOCe59QAOHv6FJN1Wy2/3H5/</code></td>
</tr>
<tr>
<td><code>! ! radius</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>server 10.99.144.200</code></td>
<td><code>aaa authentication login default local group radius group tacacs+</code></td>
</tr>
<tr>
<td><code>source-interface GigabitEthernet0/0/1</code></td>
<td><code>aaa authorization exec default local group radius group tacacs+ </code></td>
</tr>
<tr>
<td><code>exit</code></td>
<td><code>aa session-id common --- added by default</code></td>
</tr>
<tr>
<td><code>server 10.99.144.201</code></td>
<td><code>username admin password $6$nbbLkA==$ae/DO78l/wluPuhbhBU2L6h/ P.LkuryGvx3JRLS9OBh9rTfWSGbf6Qh5w6AHRHOCe59QAOHv6FJN1Wy2/3H5/</code></td>
</tr>
<tr>
<td><code>source-interface GigabitEthernet0/1/0</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>exit</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>tacacs</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>server 10.0.1.1</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>auth-port 50</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>vpn 0</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>source-interface GigabitEthernet0/0/1</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>key 1</code></td>
<td><code>!</code></td>
</tr>
<tr>
<td><code>secret-key $8$KcuvaO8M671E8czE5wV5g/YX4Q8p1L05K/+P1DrtCg= exit</code></td>
<td><code>!</code></td>
</tr>
</tbody>
</table>

---

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
Logging configuration - Configures logging to either the local hard drive or a remote host

Table 43: Logging Configuration

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging</code></td>
<td><code>logging</code></td>
</tr>
<tr>
<td><code>disk</code></td>
<td><code>disk</code></td>
</tr>
<tr>
<td><code>enable</code></td>
<td><code>enable</code></td>
</tr>
<tr>
<td><code>file size 12</code></td>
<td>!</td>
</tr>
<tr>
<td><code>file rotate 6</code></td>
<td>!</td>
</tr>
<tr>
<td><code>server 192.168.13.1</code></td>
<td><code>server 192.168.13.1</code></td>
</tr>
<tr>
<td><code>vpn 0</code></td>
<td><code>vpn 0</code></td>
</tr>
<tr>
<td><code>source-interface Loopback1</code></td>
<td><code>source-interface Loopback1</code></td>
</tr>
<tr>
<td><code>priority alert</code></td>
<td><code>priority alert</code></td>
</tr>
<tr>
<td><code>exit</code></td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td><code>logging persistent size 75497472 filesize 12582912</code></td>
</tr>
<tr>
<td></td>
<td><code>logging buffered 512000</code></td>
</tr>
<tr>
<td></td>
<td><code>logging host 192.168.13.1</code></td>
</tr>
<tr>
<td></td>
<td><code>no logging rate-limit</code></td>
</tr>
<tr>
<td></td>
<td><code>logging source-interface Loopback1</code></td>
</tr>
<tr>
<td></td>
<td><code>logging persistent</code></td>
</tr>
</tbody>
</table>

Switch Port and VLAN configuration

Table 44: Switch Port Configuration

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface GigabitEthernet0/1/4</code></td>
<td><code>interface GigabitEthernet0/1/4</code></td>
</tr>
<tr>
<td><code>switchport</code></td>
<td><code>switchport</code></td>
</tr>
<tr>
<td><code>mode trunk</code></td>
<td><code>mode trunk</code></td>
</tr>
<tr>
<td><code>access vlan vlan 10</code></td>
<td><code>access vlan vlan 10</code></td>
</tr>
<tr>
<td><code>access vlan name &quot;DHCP Vlan&quot;</code></td>
<td><code>access vlan name &quot;DHCP Vlan&quot;</code></td>
</tr>
<tr>
<td><code>trunk allowed vlan 10</code></td>
<td><code>trunk allowed vlan 10</code></td>
</tr>
<tr>
<td></td>
<td><code>no shutdown</code></td>
</tr>
<tr>
<td><code>vpn 10</code></td>
<td><code>vpn 10</code></td>
</tr>
<tr>
<td><code>name &quot;DHCP VPN&quot;</code></td>
<td><code>name &quot;DHCP VPN&quot;</code></td>
</tr>
<tr>
<td><code>interface Vlan10</code></td>
<td><code>interface Vlan10</code></td>
</tr>
<tr>
<td><code>description &quot;Vlan 10 Mgmt interface&quot;</code></td>
<td><code>description &quot;Vlan 10 Mgmt interface&quot;</code></td>
</tr>
<tr>
<td><code>ip address 10.29.35.1/24</code></td>
<td><code>ip address 10.29.35.1/24</code></td>
</tr>
<tr>
<td></td>
<td><code>no shutdown</code></td>
</tr>
<tr>
<td></td>
<td><code>no shutdown</code></td>
</tr>
<tr>
<td></td>
<td><code>arp timeout 1200</code></td>
</tr>
<tr>
<td></td>
<td><code>vrf forwarding 10</code></td>
</tr>
<tr>
<td></td>
<td><code>ip address 10.29.35.1 255.255.255.0</code></td>
</tr>
<tr>
<td></td>
<td><code>ip mtu 1500</code></td>
</tr>
<tr>
<td></td>
<td><code>exit</code></td>
</tr>
</tbody>
</table>

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
## Cellular Configuration

**Table 45: Cellular Configuration - Configures cellular controllers and cellular interfaces**

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn 0</td>
<td>interface Cellular0/2/0</td>
</tr>
<tr>
<td>interface Cellular0/2/0</td>
<td>description Cellular interface</td>
</tr>
<tr>
<td>description &quot;Cellular interface&quot;</td>
<td>no shutdown</td>
</tr>
<tr>
<td>no shutdown</td>
<td>ip address negotiated</td>
</tr>
<tr>
<td></td>
<td>ip mtu 1428</td>
</tr>
<tr>
<td></td>
<td>mtu 1500</td>
</tr>
<tr>
<td></td>
<td>exit</td>
</tr>
<tr>
<td>controller cellular 0/2/0</td>
<td>controller Cellular 0/2/0</td>
</tr>
<tr>
<td>lte sim max-retry 1</td>
<td>lte sim max-retry 1</td>
</tr>
<tr>
<td>lte failovertimer 7</td>
<td>lte failovertimer 7</td>
</tr>
<tr>
<td>profile id 1 apn Broadband</td>
<td>profile id 1 apn Broadband authentication</td>
</tr>
<tr>
<td></td>
<td>none pdn-type ipv4</td>
</tr>
</tbody>
</table>
### Table 46: BGP, OSPF, and EIGRP Configuration

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
</table>

BGP, OSPF, and EIGRP - Configures BGP, OSPF, and EIGRP Routing Protocols under Transport or Service VPN
Configuration on the Device

### CLI Template Configuration

**vpn1**
- **bgp 2**
  - shutdown
  - distance external 30
  - distance internal 250
  - distance local 10
  - address-family ipv4-unicast
    - network 10.0.100.0/24
    - redistribute static route-policy
  - route_map
    - redistribute connected route-policy

**route_map**

- neighbor 10.0.100.1
  - no shutdown
  - remote-as 3
  - timers
    - keepalive 12
    - holdtime 20
    - connect-retry 300
    - advertisement-interval 123
  - update-source GigabitEthernet0/0/1
  - ebgp-multihop 1
  - password $8$pou4PH9b60B072hcw3MmSSdLCfJk8bVys12LMB+08=
  - address-family ipv4-unicast

**vpn 1**
- router
  - ospf
    - router-id 172.16.255.15
    - compatible rfc1583
    - timers spf 200 1000 10000
    - redistribute connected route-policy
  - route_map
    - max-metric router-lsa administrative
      - area 23
      - stub
      - interface GigabitEthernet0/0/1
        - cost 23
        - authentication type message-digest
        - authentication authentication-key key1
    - exit
    - exit
    - !

**vpn 1**
- router
  - eigrp 1
    - af-interface GigabitEthernet0/0/2
    - no split-horizon
    - exit-af-interface
    - !
  - address-family ipv4 network 10.1.10.1/32
  - address-family ipv4 topology base
  - redistribute omp
  - exit-af-topology
CLI Template Configuration | Configuration on the Device
--- | ---
router bgp 2  
  bgp log-neighbor-changes  
  distance bgp 30 250 10  
  address-family ipv4 unicast vrf 1  
  neighbor 10.0.100.1 remote-as 3  
  neighbor 10.0.100.1 activate  
  neighbor 10.0.100.1 ebgp-multihop 1  
  neighbor 10.0.100.1 maximum-prefix 2147483647 100  
  neighbor 10.0.100.1 password 0 password  
  neighbor 10.0.100.1 send-community both  
  neighbor 10.0.100.1 timers 12 20  
  neighbor 10.0.100.1 update-source GigabitEthernet0/0/1  
  network 10.0.100.0 mask 255.255.255.0  
  redistribute connected  
  redistribute static route-map route_map  
  exit-address-family  
  !
  timers bgp 60 180

router ospf 1 vrf 1  
  auto-cost reference-bandwidth 100  
  max-metric router-lsa  
  timers throttle spf 200 1000 10000  
  router-id 172.16.255.15  
  default-information originate  
  distance ospf external 110  
  distance ospf inter-area 110  
  distance ospf intra-area 110  
  redistribute connected subnets route-map route_map  
  !
  interface GigabitEthernet0/0/1  
  no shutdown  
  arp timeout 1200  
  vrf forwarding 1  
  ip address 10.1.100.14 255.255.255.0  
  ip redirects  
  ip mtu 1500  
  ip ospf 1 area 23  
  ip ospf network broadcast  
  mtu 1500  
  negotiation auto  
  exit  
  !
  router eigrp eigrp-name  
  address-family ipv4 vrf 1 autonomous-system 1  
  af-interface GigabitEthernet0/0/2  
  hello-interval 5  
  hold-time 15  
  no split-horizon  
  exit-af-interface  
  !
  network 10.1.10.1 0.0.0.0  
  topology base  
  redistribute omp  
  exit-af-topology  
  !
  exit-address-family

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
Configuration on the Device

```
Configuration on the Device

! 
```

VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces

**Table 47: VPN, Interface, and Tunnel Configuration**

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn 0</td>
<td>ip route 0.0.0.0 0.0.0.0 10.1.14.13 1</td>
</tr>
<tr>
<td>interface GigabitEthernet0/2/0</td>
<td>interface GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>tunnel-interface</td>
<td>no shutdown</td>
</tr>
<tr>
<td>encapsulation ipsec weight 1</td>
<td>arp timeout 1200 - added by default</td>
</tr>
<tr>
<td>color lte</td>
<td>ip address 10.1.14.14 255.255.255.0</td>
</tr>
<tr>
<td>no allow-service bgp</td>
<td>ip redirects --&gt; added by default</td>
</tr>
<tr>
<td>allow-service dhcp</td>
<td>ip mtu 1500</td>
</tr>
<tr>
<td>allow-service dns</td>
<td>mtu 1500</td>
</tr>
<tr>
<td>allow-service icmp</td>
<td>negotiation auto --&gt; added by default</td>
</tr>
<tr>
<td>no allow-service netconf</td>
<td>exit</td>
</tr>
<tr>
<td>no allow-service ntp</td>
<td>interface Tunnel20 ---&gt; based on the interface 0/2/0</td>
</tr>
<tr>
<td>no allow-service ospf</td>
<td>no shutdown</td>
</tr>
<tr>
<td>no allow-service stun</td>
<td>ip unnumbered GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>allow-service https</td>
<td>no ip redirects</td>
</tr>
<tr>
<td>! autonegotiate</td>
<td>ipv6 unnumbered GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>! no shutdown</td>
<td>no ipv6 redirects</td>
</tr>
<tr>
<td>! ip route 0.0.0.0/0 10.1.14.13</td>
<td>tunnel source GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>vpm 512</td>
<td>tunnel mode sdwan</td>
</tr>
<tr>
<td>interface GigabitEthernet0</td>
<td>sdwan</td>
</tr>
<tr>
<td>ip dhcp-client</td>
<td>interface GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>ipv6 dhcp-client</td>
<td>tunnel-interface</td>
</tr>
<tr>
<td>autonegotiate</td>
<td>encapsulation ipsec weight 1</td>
</tr>
<tr>
<td>! no shutdown</td>
<td>color lte</td>
</tr>
<tr>
<td>! !</td>
<td>no last-resort-circuit</td>
</tr>
<tr>
<td></td>
<td>vm-manager-connection-preference 5</td>
</tr>
<tr>
<td></td>
<td>no allow-service all</td>
</tr>
<tr>
<td></td>
<td>no allow-service bgp</td>
</tr>
<tr>
<td></td>
<td>allow-service dhcp</td>
</tr>
<tr>
<td></td>
<td>allow-service dns</td>
</tr>
<tr>
<td></td>
<td>allow-service icmp</td>
</tr>
<tr>
<td></td>
<td>no allow-service sshd</td>
</tr>
<tr>
<td></td>
<td>no allow-service netconf</td>
</tr>
<tr>
<td></td>
<td>no allow-service ntp</td>
</tr>
<tr>
<td></td>
<td>no allow-service ospf</td>
</tr>
<tr>
<td></td>
<td>no allow-service stun</td>
</tr>
<tr>
<td>interface GigabitEthernet0</td>
<td>ip route 0.0.0.0 0.0.0.0 10.1.14.13 1</td>
</tr>
<tr>
<td>no shutdown</td>
<td>interface GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>arp timeout 1200</td>
<td>tunnel-interface</td>
</tr>
<tr>
<td>vrf forwarding Mgmt-intf</td>
<td>encapsulation ipsec weight 1</td>
</tr>
<tr>
<td>ip address dhcp client-id GigabitEthernet0</td>
<td>color lte</td>
</tr>
<tr>
<td>ip redirects</td>
<td>no last-resort-circuit</td>
</tr>
<tr>
<td>ip mtu 1500</td>
<td>vm-manager-connection-preference 5</td>
</tr>
<tr>
<td>mtu 1500</td>
<td>no allow-service all</td>
</tr>
<tr>
<td>negotiation auto</td>
<td>no allow-service bgp</td>
</tr>
<tr>
<td>allow-service dhcp</td>
<td>allow-service sshd</td>
</tr>
<tr>
<td>allow-service dns</td>
<td>no allow-service netconf</td>
</tr>
<tr>
<td>allow-service icmp</td>
<td>no allow-service ntp</td>
</tr>
<tr>
<td>no allow-service ospf</td>
<td>no allow-service sshd</td>
</tr>
<tr>
<td>no allow-service stun</td>
<td>no allow-service ntp</td>
</tr>
<tr>
<td>allow-service sshd</td>
<td>no allow-service ospf</td>
</tr>
<tr>
<td>no allow-service stun</td>
<td>no allow-service stun</td>
</tr>
<tr>
<td>interface GigabitEthernet0</td>
<td>interface GigabitEthernet0/2/0</td>
</tr>
<tr>
<td>no shutdown</td>
<td>tunnel-interface</td>
</tr>
<tr>
<td>arp timeout 1200</td>
<td>encapsulation ipsec weight 1</td>
</tr>
<tr>
<td>vrf forwarding Mgmt-intf</td>
<td>color lte</td>
</tr>
<tr>
<td>ip address dhcp client-id GigabitEthernet0</td>
<td>no last-resort-circuit</td>
</tr>
<tr>
<td>ip redirects</td>
<td>vm-manager-connection-preference 5</td>
</tr>
<tr>
<td>ip mtu 1500</td>
<td>no allow-service all</td>
</tr>
<tr>
<td>mtu 1500</td>
<td>no allow-service bgp</td>
</tr>
<tr>
<td>negotiation auto</td>
<td>allow-service dhcp</td>
</tr>
<tr>
<td>allow-service dns</td>
<td>allow-service sshd</td>
</tr>
<tr>
<td>allow-service icmp</td>
<td>no allow-service netconf</td>
</tr>
<tr>
<td>no allow-service ospf</td>
<td>no allow-service ntp</td>
</tr>
<tr>
<td>no allow-service stun</td>
<td>no allow-service sshd</td>
</tr>
<tr>
<td>allow-service sshd</td>
<td>no allow-service ntp</td>
</tr>
<tr>
<td>no allow-service ostf</td>
<td>no allow-service stun</td>
</tr>
<tr>
<td>no allow-service stun</td>
<td>negotiation auto</td>
</tr>
</tbody>
</table>
Network Address Translation (NAT) over Direct Internet Access (DIA)

Table 48: NAT over DIA

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn 201</td>
<td>interface GigabitEthernet0/0/2.2901</td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
</tr>
<tr>
<td></td>
<td>encapsulation dot1Q 2901</td>
</tr>
<tr>
<td></td>
<td>vrf forwarding 201</td>
</tr>
<tr>
<td></td>
<td>ip address 10.201.201.1/24</td>
</tr>
<tr>
<td></td>
<td>mtu 1496</td>
</tr>
<tr>
<td></td>
<td>vrrp 100</td>
</tr>
<tr>
<td></td>
<td>track-omp</td>
</tr>
<tr>
<td></td>
<td>ipv4 10.201.201.3</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>dhcp-server</td>
</tr>
<tr>
<td></td>
<td>address-pool 10.201.201.0/24</td>
</tr>
<tr>
<td></td>
<td>exclude 10.201.201.1-10.201.201.10</td>
</tr>
<tr>
<td></td>
<td>offer-time 600</td>
</tr>
<tr>
<td></td>
<td>lease-time 86400</td>
</tr>
<tr>
<td></td>
<td>admin-state up</td>
</tr>
<tr>
<td></td>
<td>options</td>
</tr>
<tr>
<td></td>
<td>default-gateway 10.201.201.1</td>
</tr>
<tr>
<td></td>
<td>dns-servers 10.99.139.201</td>
</tr>
<tr>
<td></td>
<td>tftp-servers 10.99.139.201</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>ip route 0.0.0.0/0 vpn 0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td>vpn 0</td>
<td>interface GigabitEthernet0/0/0/0</td>
</tr>
<tr>
<td></td>
<td>ip address 172.16.10.1/24</td>
</tr>
<tr>
<td></td>
<td>nat</td>
</tr>
<tr>
<td></td>
<td>udp-timeout 3</td>
</tr>
<tr>
<td></td>
<td>tcp-timeout 40</td>
</tr>
<tr>
<td></td>
<td>respond-to-ping</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>ip route 0.0.0.0/0 vpn 0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
</tbody>
</table>

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
NAT64 Configuration

Table 49: NAT64 Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>v4 pool pool1</td>
<td>interface GigabitEthernet3</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>no shutdown</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>arp timeout 1200</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>vrf forwarding 1</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>ip address 10.1.19.15 255.255.255.0</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>negotiation auto</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 enable</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 prefix stateful 2001::F/64 vrf 1</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 v4 pool pool1 10.1.1.10 10.1.1.100</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 v6v4 list global-list pool pool1 vrf 1</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 translation timeout tcp 60</td>
</tr>
<tr>
<td>v4 pool pool2</td>
<td>nat64 translation timeout udp 1</td>
</tr>
</tbody>
</table>

Multilink and T1/E1 - Configures T1/E1 Controller and Serial, Multilink Interfaces

Table 50: Configuring Multilink

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>card type t1 0 2</td>
<td>interface Multilink1</td>
</tr>
<tr>
<td>controller T1 0/2/0</td>
<td>ip address 10.1.10.30/24 shutdown</td>
</tr>
<tr>
<td>framing esf</td>
<td>controller T1 0/2/0</td>
</tr>
<tr>
<td>clock source internal</td>
<td>linecode b8zs</td>
</tr>
<tr>
<td>linecode b8zs</td>
<td>channel-group 1</td>
</tr>
<tr>
<td>cablelength long 0db</td>
<td>channel-group 3</td>
</tr>
<tr>
<td>channel-group 1 timeslots 15</td>
<td>channel-group 1 timeslots 12</td>
</tr>
<tr>
<td>channel-group 3 timeslots 10</td>
<td>channel-group 4 timeslots 10</td>
</tr>
<tr>
<td>channel-group 4 timeslots 10</td>
<td></td>
</tr>
</tbody>
</table>
| interface Multilink1 | !
| no shutdown | ppp pap sent-username admin password admin |
| encapsulation ppp | ppp authentication pap |
| ip address 10.1.10.30 255.255.255.0 | ppp multilink |
| ppp pap sent-username admin password admin | ppp multilink group 1 |
| ppp authentication pap | |
| ppp multilink | |
| ppp multilink group 1 | |
| ppp multilink links minimum 1 | |
| ppp multilink fragment disable | |
| ppp multilink group 1 | |
| exit | |
| interface Serial0/2/0:1 | |
| no shutdown | |
| encapsulation ppp | |
| bandwidth 1536 | |
| no ip address | |
| load-interval 30 | |
| ppp pap sent-username admin password admin | |
| ppp authentication pap | |
| ppp multilink | |
| ppp multilink group 1 | |
| exit | |
Local QoS Policy

Table 51: Local QoS Policy

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>CLI Template Configuration</td>
<td>Configuration on the Device</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>vpn 1</td>
<td>interface GigabitEthernet0/0/1</td>
</tr>
<tr>
<td></td>
<td>access-list MyACL in</td>
</tr>
<tr>
<td></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>class-map match-any</td>
</tr>
<tr>
<td></td>
<td>match best-effort</td>
</tr>
<tr>
<td></td>
<td>match qos-group 3</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class-map match-any</td>
</tr>
<tr>
<td></td>
<td>match any bulk-data</td>
</tr>
<tr>
<td></td>
<td>match qos-group 2</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class-map match-any</td>
</tr>
<tr>
<td></td>
<td>match any critical-data</td>
</tr>
<tr>
<td></td>
<td>match qos-group 1</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class-map match-any voice</td>
</tr>
<tr>
<td></td>
<td>match qos-group 0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>policy-map MyQoSMap</td>
</tr>
<tr>
<td></td>
<td>class best-effort</td>
</tr>
<tr>
<td></td>
<td>random-detect bandwidth</td>
</tr>
<tr>
<td></td>
<td>percent 20</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class bulk-data</td>
</tr>
<tr>
<td></td>
<td>random-detect bandwidth</td>
</tr>
<tr>
<td></td>
<td>percent 20</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class critical-data</td>
</tr>
<tr>
<td></td>
<td>random-detect bandwidth</td>
</tr>
<tr>
<td></td>
<td>percent 40</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>class voice</td>
</tr>
<tr>
<td></td>
<td>priority percent 20</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>policy</td>
</tr>
<tr>
<td></td>
<td>no app-visibility</td>
</tr>
<tr>
<td></td>
<td>no flow-visibility</td>
</tr>
<tr>
<td></td>
<td>no implicit-acl-logging</td>
</tr>
<tr>
<td></td>
<td>log-frequency 1000</td>
</tr>
<tr>
<td></td>
<td>class-map</td>
</tr>
<tr>
<td></td>
<td>class best-effort</td>
</tr>
<tr>
<td></td>
<td>class bulk-data</td>
</tr>
<tr>
<td></td>
<td>class critical-data</td>
</tr>
<tr>
<td></td>
<td>class critical-data</td>
</tr>
<tr>
<td></td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>dscp 22</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>sequence 40</td>
</tr>
<tr>
<td></td>
<td>action accept</td>
</tr>
<tr>
<td></td>
<td>class best-effort</td>
</tr>
<tr>
<td></td>
<td>set</td>
</tr>
<tr>
<td></td>
<td>dscp 0</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>default-action accept</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>qos-scheduler be-scheduler</td>
</tr>
<tr>
<td></td>
<td>class best-effort</td>
</tr>
<tr>
<td></td>
<td>bandwidth-percent 20</td>
</tr>
<tr>
<td></td>
<td>buffer-percent 20</td>
</tr>
<tr>
<td></td>
<td>drops red-drop</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>qos-scheduler bulk-scheduler</td>
</tr>
<tr>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### CLI Template Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class bulk-data</td>
<td></td>
</tr>
<tr>
<td>bandwidth-percent 20</td>
<td></td>
</tr>
<tr>
<td>buffer-percent 20</td>
<td></td>
</tr>
<tr>
<td>drops red-drop</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler critical-scheduler</td>
<td></td>
</tr>
<tr>
<td>class critical-data</td>
<td></td>
</tr>
<tr>
<td>bandwidth-percent 40</td>
<td></td>
</tr>
<tr>
<td>buffer-percent 40</td>
<td></td>
</tr>
<tr>
<td>drops red-drop</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler voice-scheduler</td>
<td></td>
</tr>
<tr>
<td>class voice</td>
<td></td>
</tr>
<tr>
<td>bandwidth-percent 20</td>
<td></td>
</tr>
<tr>
<td>buffer-percent 20</td>
<td></td>
</tr>
<tr>
<td>scheduling 11q</td>
<td></td>
</tr>
<tr>
<td>qos-map MyQoSMap</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler be-scheduler</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler bulk-scheduler</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler critical-scheduler</td>
<td></td>
</tr>
<tr>
<td>qos-scheduler voice-scheduler</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration on the Device

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>sequence 30</td>
<td></td>
</tr>
<tr>
<td>match</td>
<td></td>
</tr>
<tr>
<td>destination-ip 192.168.20.0/24</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>action accept</td>
<td></td>
</tr>
<tr>
<td>class critical-data</td>
<td></td>
</tr>
<tr>
<td>set</td>
<td></td>
</tr>
<tr>
<td>dscp 22</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>sequence 40</td>
<td></td>
</tr>
<tr>
<td>action accept</td>
<td></td>
</tr>
<tr>
<td>class best-effort</td>
<td></td>
</tr>
<tr>
<td>set</td>
<td></td>
</tr>
<tr>
<td>dscp 0</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>default-action accept</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
</tbody>
</table>
Security Policy (ZBFW, IPS/IDS, URL-Filtering) Configuration

Table 52: Security Policy (ZBFW, IPS/IDS, URL-Filtering)

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td></td>
</tr>
<tr>
<td>zone internet</td>
<td></td>
</tr>
<tr>
<td>vpn 0</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone zone1</td>
<td></td>
</tr>
<tr>
<td>vpn 1</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone zone2</td>
<td></td>
</tr>
<tr>
<td>vpn 2</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone-pair ZP_zone1_internet_fw_policy</td>
<td></td>
</tr>
<tr>
<td>source-zone zone1</td>
<td></td>
</tr>
<tr>
<td>destination-zone internet</td>
<td></td>
</tr>
<tr>
<td>zone-policy fw_policy</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone-pair ZP_zone1_zone2_fw_policy</td>
<td></td>
</tr>
<tr>
<td>source-zone zone1</td>
<td></td>
</tr>
<tr>
<td>destination-zone zone2</td>
<td></td>
</tr>
<tr>
<td>zone-policy fw_policy</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone-based-policy fw_policy</td>
<td></td>
</tr>
<tr>
<td>sequence 1</td>
<td></td>
</tr>
<tr>
<td>match</td>
<td></td>
</tr>
<tr>
<td>source-data-prefix-list subnet1</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>action inspect</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>default-action pass</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>zone-to-nozone-internet deny lists</td>
<td></td>
</tr>
<tr>
<td>data-prefix-list subnet1</td>
<td></td>
</tr>
<tr>
<td>ip-prefix 10.0.10.0/24</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>url-filtering url_filter</td>
<td></td>
</tr>
<tr>
<td>web-category-action block</td>
<td></td>
</tr>
<tr>
<td>web-categories games</td>
<td></td>
</tr>
<tr>
<td>block-threshold moderate-risk</td>
<td></td>
</tr>
<tr>
<td>block text</td>
<td></td>
</tr>
<tr>
<td>&quot;&lt;![CDATA[&amp;lt;h3&amp;gt;Access&quot; to the requested page has been denied]]&gt;&quot;</td>
<td></td>
</tr>
<tr>
<td>target-vpns 1</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>intrusion-prevention intrusion_policy</td>
<td></td>
</tr>
<tr>
<td>security-level connectivity</td>
<td></td>
</tr>
<tr>
<td>inspection-mode protection</td>
<td></td>
</tr>
<tr>
<td>log-level err</td>
<td></td>
</tr>
<tr>
<td>target-vpns 1</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>failure-mode open</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
</tbody>
</table>
### CLI Template Configuration

<table>
<thead>
<tr>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list extended fw_policy-seq-1-acl_</code></td>
</tr>
<tr>
<td><code>11 permit object-group</code></td>
</tr>
<tr>
<td><code>fw-policy-seq-1-service-og_ object-group</code></td>
</tr>
<tr>
<td><code>subnet1 any</code></td>
</tr>
<tr>
<td><code>ip access-list extended utd-nat-acl</code></td>
</tr>
<tr>
<td><code>10 permit ip any any</code></td>
</tr>
<tr>
<td><code>class-map type inspect match-all</code></td>
</tr>
<tr>
<td><code>fw_policy-seq-1-cm_</code></td>
</tr>
<tr>
<td><code>match access-group name</code></td>
</tr>
<tr>
<td><code>fw_policy-seq-1-acl_</code></td>
</tr>
<tr>
<td><code>policy-map type inspect fw_policy</code></td>
</tr>
<tr>
<td><code>class fw_policy-seq-1-cm_</code></td>
</tr>
<tr>
<td><code>inspect</code></td>
</tr>
<tr>
<td><code>class class-default</code></td>
</tr>
<tr>
<td><code>pass</code></td>
</tr>
<tr>
<td><code>object-group service</code></td>
</tr>
<tr>
<td><code>fw_policy-seq-1-service-og_</code></td>
</tr>
<tr>
<td><code>ip</code></td>
</tr>
<tr>
<td><code>parameter-map type inspect-global</code></td>
</tr>
<tr>
<td><code>alert on</code></td>
</tr>
<tr>
<td><code>log dropped-packets</code></td>
</tr>
<tr>
<td><code>multi-tenancy</code></td>
</tr>
<tr>
<td><code>vpn zone security</code></td>
</tr>
<tr>
<td><code>parameter-map type umbrella global</code></td>
</tr>
<tr>
<td><code>token</code></td>
</tr>
<tr>
<td><code>A5EA676087BF66A42DC4F722C2AFD10D00256274</code></td>
</tr>
<tr>
<td><code>dnsresolver</code></td>
</tr>
<tr>
<td><code>vrf 1</code></td>
</tr>
<tr>
<td><code>dns-resolver umbrella</code></td>
</tr>
<tr>
<td><code>match-local-domain-to-bypass</code></td>
</tr>
<tr>
<td><code>zone security internet</code></td>
</tr>
<tr>
<td><code>vpn 0</code></td>
</tr>
<tr>
<td><code>zone security zone1</code></td>
</tr>
<tr>
<td><code>vpn 1</code></td>
</tr>
<tr>
<td><code>zone security zone2</code></td>
</tr>
<tr>
<td><code>vpn 2</code></td>
</tr>
<tr>
<td><code>zone-pair security</code></td>
</tr>
<tr>
<td><code>ZP_zone1_internet_fw_policy source zone1 destination internet</code></td>
</tr>
<tr>
<td><code>service-policy type inspect fw_policy</code></td>
</tr>
<tr>
<td><code>zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2</code></td>
</tr>
<tr>
<td><code>service-policy type inspect fw_policy</code></td>
</tr>
<tr>
<td><code>app-hosting appid utd</code></td>
</tr>
<tr>
<td><code>app-resource package-profile cloud-low</code></td>
</tr>
<tr>
<td><code>app-vnic gateway0 virtualportgroup 0</code></td>
</tr>
<tr>
<td>CLI Template Configuration</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>guest-interface 0</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
|                          | text &lt;![CDATA[&lt;h3&gt;Access to the requested page has been denied&lt;/h3&gt;&lt;p&gt;Please contact your Network Administrator&lt;/p&gt;]]&gt;
|                          | ! web-filter url profile url_filter |
|                          | categories block games       |
|                          | ! block page-profile block-url_filter |
|                          | log level error reputation   |
|                          | block-threshold moderate-risk |
|                          | ! threat-inspection profile intrusion_policy |
|                          | threat protection policy connectivity logging level err |
|                          | ! utd global                 |
|                          | ! policy utd-policy-vrf-1    |
|                          | all-interfaces vrf 1 thr   |
|                          | threat-inspection profile intrusion_policy |
|                          | web-filter url profile url_filter |
|                          | exit                        |
Configuring NTP

Table 53: Configuring NTP

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>ntp</td>
<td>ntp server 198.51.241.229 source</td>
</tr>
<tr>
<td>server 10.29.43.1</td>
<td>GigabitEthernet1 version 4</td>
</tr>
<tr>
<td>source-interface GigabitEthernet1</td>
<td>exit</td>
</tr>
<tr>
<td>version 4</td>
<td>!</td>
</tr>
<tr>
<td>exit</td>
<td>!</td>
</tr>
</tbody>
</table>

IPv6 Configuration

Table 54: IPv6 Configuration

<table>
<thead>
<tr>
<th>CLI Template Configuration</th>
<th>Configuration on the Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface GigabitEthernet3</td>
<td>interface GigabitEthernet3</td>
</tr>
<tr>
<td>shutdown</td>
<td>shutdown</td>
</tr>
<tr>
<td>arp timeout 1200</td>
<td>arp timeout 1200</td>
</tr>
<tr>
<td>vrf forwarding 1</td>
<td>vrf forwarding 1</td>
</tr>
<tr>
<td>no ip address</td>
<td>no ip address</td>
</tr>
<tr>
<td>ip redirects</td>
<td>ip redirects</td>
</tr>
<tr>
<td>mtu 1500</td>
<td>mtu 1500</td>
</tr>
<tr>
<td>ipv6 address 2671:123A::1/128</td>
<td>ipv6 address 2671:123A::1/128</td>
</tr>
<tr>
<td>ipv6 redirects</td>
<td>ipv6 redirects</td>
</tr>
<tr>
<td>mtu 1500</td>
<td>mtu 1500</td>
</tr>
<tr>
<td>negotiation auto</td>
<td>negotiation auto</td>
</tr>
<tr>
<td>exit</td>
<td>exit</td>
</tr>
<tr>
<td>vrf definition 1</td>
<td>vrf definition 1</td>
</tr>
<tr>
<td>rd 1:1</td>
<td>rd 1:1</td>
</tr>
<tr>
<td>address-family ipv4</td>
<td>address-family ipv4</td>
</tr>
<tr>
<td>exit-address-family</td>
<td>exit-address-family</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
</tbody>
</table>

DHCP Server

Use the DHCP-Server template for all vEdge Cloud and vEdge router devices.

You enable DHCP server functionality on a vEdge router interface so it can assign IP addresses to hosts in the service-side network.

To configure a vEdge router to act as a DHCP server using vManage templates:

1. Create a DHCP-Server feature template to configure DHCP server parameters, as described in this article.
2. Create one or more interface feature templates, as described in the VPN-Interface-Ethernet and the VPN-Interface-PPP-Ethernet help topics.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.
To configure a vEdge router interface to be a DHCP helper so that it forwards broadcast DHCP requests that it receives from DHCP servers, in the DHCP Helper field of the applicable interfaces template, enter the addresses of the DHCP servers.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface.
8. From the Sub-Templates drop-down, select DHCP Server.
9. From the DHCP Server drop-down, click Create Template. The DHCP-Server template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining DHCP Server parameters.
10. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

11. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 55:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Minimum DHCP Server Configuration

To configure DHCP server functionality, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk as required to configure DHCP servers.

Table 56:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Pool*</td>
<td>Enter the IPv4 prefix range, in the format $prefix/length$, for the pool of addresses in the service-side network for which the vEdge router interface acts as DHCP server.</td>
</tr>
<tr>
<td>Exclude Addresses</td>
<td>Enter one or more IP addresses to exclude from the DHCP address pool. To specify multiple individual addresses, list them separated by a comma (for example, 1.1.1.1, 2.2.2.2, 3.3.3.3). To specify a range of addresses, separate them with a hyphen (for example, 1.1.1.1-1.1.1.10).</td>
</tr>
<tr>
<td>Maximum Leases</td>
<td>Specify the number of IP addresses that can be assigned on this interface. $Range$: 0 through 4294967295</td>
</tr>
<tr>
<td>Lease Time</td>
<td>Specify how long a DHCP-assigned IP address is valid. $Range$: 0 through 4294967295 seconds</td>
</tr>
<tr>
<td>Offer Time</td>
<td>Specify how long the IP address offered to a DHCP client is reserved for that client. By default, an offered IP address is reserved indefinitely, until the DHCP server runs out of addresses. At that point, the address is offered to another client. $Range$: 0 through 4294967295 seconds $Default$: 600 seconds</td>
</tr>
</tbody>
</table>
DHCP Server

Table 57:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address of the client to which the static IP address is being assigned.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the static IP address to assign to the client.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the hostname of the client device.</td>
</tr>
</tbody>
</table>

To edit a static lease, click the pencil icon to the right of the entry.

To remove a static lease, click the trash icon to the right of the entry.

To save the feature template, click Save.

CLI equivalent:

```bash
vpn vpn-id
interface ge.slot/port
dhcp-server address-pool prefix/length admin-state (down | up)
    exclude ip-address
    lease-time seconds
    max-leases number
    offer-time minutes
```

Configure Advanced Options

To configure advanced DHCP server options, click the Advanced tab and then configure the following parameters:

Table 58:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface MTU</td>
<td>Specify the maximum MTU size of packets on the interface. <em>Range</em>: 68 to 65535 bytes</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specify the domain name that the DHCP client uses to resolve hostnames.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the IP address of a default gateway in the service-side network.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Enter one or more IP address for a DNS server in the service-side network. Separate multiple entries with a comma. You can specify up to eight addresses.</td>
</tr>
<tr>
<td>TFTP Servers</td>
<td>Enter the IP address of a TFTP server in the service-side network. You can specify one or two addresses. If two, separate them with a comma.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id
tunnel interface ge slot/port
dhcp-server options
default-gateway ip-address
dns-servers ip-address
domain-name domain-name
interface-mtu mtu
tftp-servers ip-address
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**Configuring EIGRP**

Cisco release 19.1 supports Enhanced Interior Gateway Routing Protocol (EIGRP) on Cisco IOS XE devices. EIGRP is an open standard IGP routing protocol that provides advantages such as:

- Increased network width from 15 to 100 hops
- Fast convergence
- Incremental updates, minimizing bandwidth
- Protocol-independent neighbor discovery
- Easy scaling

**Note**

If your EIGRP network includes vEdge routers, you may need additional software. Refer to SD-WAN 19.1 release notes for configuration information.

To configure EIGRP routing protocol using vManage templates:

1. Create an EIGRP feature template to configure EIGRP parameters, described here.
2. Create a VPN feature template to configure VPN parameters for service-side routing (any VPN other than VPN 0 or VPN 512). See VPN.
3. Create a device template and apply the templates to the correct devices. See Templates.
Create and Name an EIGRP Template

Step 1  From the vManage menu, select Configuration > Templates.
Step 2  Click Feature.
Step 3  Click Add Template.
Step 4  Select a Cisco IOS XE device from the list.
Step 5  From the Other Templates section, click EIGRP.

The EIGRP Feature template opens. The top of the form contains fields for naming the template, and the bottom contains fields for defining EIGRP parameters.

Step 6  In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
Step 7  In the Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Basic Configuration

Click the Basic Configuration tab to configure the local autonomous system (AS) number for the template.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous System ID *</td>
<td>Enter the local AS number.</td>
</tr>
<tr>
<td></td>
<td>• Range: 1-65,535</td>
</tr>
<tr>
<td></td>
<td>• Default: None</td>
</tr>
</tbody>
</table>
Equivalent CLI Commands

```
vpn  vpn-id
router
eigrp name
    address-family ipv4 vrf vrf-name autonomous-system number
```

**IP4 Unicast Address Family**

To configure the global EIGRP address family, click the **Unicast Address Family** tab.

**Redistribute Tab**

To redistribute routes from one protocol (routing domain) into a EIGRP routing domain, click **New Redistribute** and enter the following parameter values:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mark as Optional Row</strong></td>
<td></td>
<td>Click <strong>Optional</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
</tr>
<tr>
<td>Protocol *</td>
<td></td>
<td>Select the protocols from which to redistribute routes into EIGRP, for all EIGRP sessions.</td>
</tr>
<tr>
<td>bgp</td>
<td></td>
<td>Redistribute Border Gateway Protocol (BGP) routes into EIGRP.</td>
</tr>
<tr>
<td>connected</td>
<td></td>
<td>Redistribute connected routes into EIGRP.</td>
</tr>
<tr>
<td>nat-route</td>
<td></td>
<td>Redistribute network address translation (NAT) routes into EIGRP.</td>
</tr>
<tr>
<td>omp</td>
<td></td>
<td>Redistribute Overlay Management Protocol (OMP) routes into EIGRP.</td>
</tr>
<tr>
<td>ospf</td>
<td></td>
<td>Redistribute Open Shortest Path First (OSPF) routes into EIGRP.</td>
</tr>
<tr>
<td>static</td>
<td></td>
<td>Redistribute static routes into EIGRP.</td>
</tr>
<tr>
<td><strong>Route Policy</strong></td>
<td>*</td>
<td>Enter the name of the route policy to apply to redistributed routes.</td>
</tr>
</tbody>
</table>

Click **Add** to save the redistribution information.

**Network Tab**

To advertise a prefix into the EIGRP routing domain, click the **Network** tab, and then click **New Network** and enter the following parameter values:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mark as Optional Row** | Click **Optional** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.
**Advanced Parameters**

To configure advanced parameters for EIGRP, click the **Advanced** tab and configure the following parameter values:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Hold Time (seconds)** | Set the interval after which EIGRP considers a neighbor to be down. The local router then terminates the EIGRP session to that peer. This acts as the global hold time.  
  - **Range**: 0 through 65,535  
  - **Default**: 15 seconds |

| **Hello Interval (seconds)** | Set the interval at which the router sends EIGRP hello packets.  
  - **Range**: 0 through 65,535  
  - **Default**: 5 seconds |

| **Route Policy Name** | Enter the name of an EIGRP route policy.                                    |

### Equivalent CLI Commands

```
vpn vpn-id
  router
eigrp
    address-family ipv4-unicast
    maximum-paths paths number
    network prefix/mask
    redistribute (bgp | connected | nat-route | ospf | static)
```

---

**Network Prefix**

Enter the network prefix you want EIGRP to advertise in the format of `prefix/mask`.

Click **Add** to save the network prefix.

### Equivalent CLI Commands

```
vpn vpn-id
  router
eigrp
  address-family ipv4-unicast
  network prefix/mask
  redistribute (bgp | connected | nat-route | ospf | static)
```

---

### Advanced Parameters

- **Hold Time (seconds)**: Set the interval after which EIGRP considers a neighbor to be down. The local router then terminates the EIGRP session to that peer. This acts as the global hold time.
  - **Range**: 0 through 65,535
  - **Default**: 15 seconds

- **Hello Interval (seconds)**: Set the interval at which the router sends EIGRP hello packets.
  - **Range**: 0 through 65,535
  - **Default**: 5 seconds

- **Route Policy Name**: Enter the name of an EIGRP route policy.
Route Authentication Parameters

The IP Enhanced IGRP Route Authentication feature supports MD5 or HMAC-sha-256 authentication of routing updates from the EIGRP routing protocol. To configure authentication for EIGRP routes:

1. Click the Authentication tab.
2. Click Authentication to open the Authentication Type field.
3. Select global parameter scope.
4. From the drop-down list, select md5 or hmac-sha-256.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>MD5 Key ID</td>
<td>Enter an MD5 key ID to compute an MD5 hash over the contents of the EIGRP packet using that value.</td>
</tr>
<tr>
<td></td>
<td>MD5 Authentication Key</td>
<td>Enter an MD5 authentication key to use an encoded MD5 checksum in the transmitted packet.</td>
</tr>
<tr>
<td></td>
<td>Authentication Key</td>
<td>A 256-byte unique piece of information that is used to compute the HMAC and is known both by the sender and the receiver of the message.</td>
</tr>
</tbody>
</table>

Click Add to save the authentication parameters.

To use a preferred route map, specify both an MD5 key (ID or auth key) and a route map.

Equivalent CLI Commands

```
vpn vpn-id
router
eigrp name
   address-family ipv4 [vrf vrf-name] autonomous-system number
   af-interface intf-name
   authentication key-chain keychain-name
   authentication mode {hmac-sha-256 | md5}
```

Interface Parameters

To configure interface parameters for EIGRP routes, click the Interface tab, click Interface, and enter the following parameter values:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Optional Row</td>
<td>Click Optional to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.</td>
</tr>
<tr>
<td>Interface name</td>
<td>Enter the interface name(s) on which EIGRP should run.</td>
</tr>
</tbody>
</table>
Summary Addresses

To configure a summary IP address from the Interface tab:

**Parameter Name** | **Description**
--- | ---
Shutdown | No (the default) enables the interface to run EIGRP. Yes, disables the interface.

Click Add to save the interfaces.

**Step 1** Click Interface to open the Interface menu.
**Step 2** Click Add Summary Address
**Step 3** If you have no configured summary addresses, click Add Summary Address from the pop-up message.
**Step 4** Enter the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary address prefix</td>
<td>Enter the address prefix you want to apply to the summary address.</td>
</tr>
</tbody>
</table>

Click Add to add the summary address.

**Step 5** Click Add to save the interfaces.
**Step 6** Click Save to save the feature template.

---

**What to do next**

**Equivalent CLI Commands**

vpn  
vpn-id

router
eigrp
name
address-family ipv4 vrf vrf-name autonomous-system number
af-interface intf-name
summary-address prefix/mask

**GPS**

Use the GPS template for all Cisco cellular routers running Viptela software.

For Cisco devices running Viptela software, you can configure the GPS and National Marine Electronics Association (NMEA) streaming. You enable both these features to allow 4G LTE routers to obtain GPS coordinates.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ➤ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.

4. From the Device Model drop-down, select the type of device for which you are creating the template.

5. Select the Cellular tab.

6. In Additional Cellular Controller Templates, click GPS.

7. To create a custom template for GPS, click the GPS drop-down and then click Create Template. The GPS template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining GPS parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 59:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure GPS**

To configure GPS parameters for the cellular router, configure the following parameters. Parameters marked with an asterisk are required to configure the GPS feature.
Table 60:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS</td>
<td>Click On to enable the GPS feature on the router.</td>
</tr>
<tr>
<td>GPS Mode</td>
<td>Select the GPS mode:</td>
</tr>
<tr>
<td></td>
<td>• MS-based—Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, cell tower data is used to enhance the quality and precision in determining location, which is useful when satellite signals are poor.</td>
</tr>
<tr>
<td></td>
<td>• Standalone—Use satellite information when determining position.</td>
</tr>
<tr>
<td>NMEA</td>
<td>Click On to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE NIM to any marine device, such as a Windows-based PC, that is running a commercially available GPS-based application.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Enter the IP address of the interface that connects to the router's NIM.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Enter the IP address of the marine NMEA server.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the number of the port to use to send NMEA data to the server.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS Release 18.1.1.

**IGMP**

Use the IGMP template for all vEdge Cloud and vEdge router devices.

Internet Group Management Protocol (IGMP) allows vEdge routers to join multicast groups within a particular VPN.

To configure IGMP using vManage templates:

1. Create an IGMP feature template to configure IGMP parameters, as described in this article.
2. Create the interface in the VPN to use for IGMP. See the VPN-Interface-Ethernet help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.

7. Under Additional VPN Templates, located to the right of the screen, click IGMP.

8. From the IGMP drop-down, click Create Template. The IGMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IGMP parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 61:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure IGMP**

To configure IGMP, select the Basic Configuration tab to enable IGMP. Then, select the Interface tab and click Add New Interface to configure IGMP interfaces. All parameters listed below are required to configure IGMP.

**Table 62:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown</td>
<td>Ensure that No is selected to enable IGMP.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Enter the name of the interface to use for IGMP. To add another interface, click the plus sign (+). To delete an interface, click the trash icon to the right of the entry.</td>
</tr>
<tr>
<td>Join Group Address</td>
<td>Click Add Join Group Address, and enter the address of a multicast group for the interface to join. Click Add to add the new interface</td>
</tr>
</tbody>
</table>
To save the feature template, click Save.

**CLI equivalent:**
```
vpn vpn-id
router
   igmp interface interface-name join-group group-address
   [no] shutdown
```

**Release Information**
Introduced in vManage NMS in Release 15.2.

## Logging

Use the Logging template for all Viptela devices to configure logging to either the local hard drive or a remote host.

### Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for Logging, select the Factory_Default_Logging_Template and click Create Template. The Logging template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Logging parameters. You may need to click a tab or the plus sign (+) to display additional fields.
6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

7. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 63:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the keys (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Minimum Logging Configuration

The following logging parameters are configured by default on all Viptela devices:

- Log event notification system log (syslog) messages are logged to a file on the local device's hard disk, at a priority level of "information."
- Log files are placed in the directory /var/log on the local device.
- Log files are readable by the "admin" user.

Configure Logging to the Local Disk

To configure logging of event notification system log messages to the local device's hard disk, select the Disk tab and configure the following parameters:

Table 64:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Disk</td>
<td>Click On to allow syslog messages to be saved in a file on the local hard disk, or click Off to disallow it. By default, logging to a local disk file is enabled on all Viptela devices.</td>
</tr>
<tr>
<td>Maximum File Size</td>
<td>Enter the maximum size of syslog files. Syslog files are rotated on an hourly basis based on the file's size. When the file size exceeds configured value, the file is rotated and the syslogd process is notified. <em>Range:</em> 1 through 20 MB <em>Default:</em> 10 MB</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
---|---
Rotations | Enter the number of syslog files to create before discarding the oldest files. \textit{Range:} 1 through 10 \textit{Default:} 10

Priority | Select the priority level of the syslog message to save to the log files. The severity indicates the seriousness of the event that generated the message. The default priority value is "informational", so, by default, all syslog messages are recorded. The priority level can be one of the following (in order of decreasing severity): • Emergency—System is unusable (corresponds to syslog severity 0). • Alert—Action must be taken immediately (corresponds to syslog severity 1). • Critical—Critical: A serious condition (corresponds to syslog severity 2). • Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • Warning—A minor error condition (corresponds to syslog severity 4). • Notice—A normal, but significant condition (corresponds to syslog severity 5). • Informational—Routine condition (the default) (corresponds to syslog severity 6).

To save the feature template, click Save.

**CLI equivalent:**
```
system
logging
disk
   enable
   file
      rotate number
      size megabytes
      priority priority
```

**Configure Logging to Remote Servers**

To configure logging of event notification system log messages to a remote server, click the Server tab. Then click Add New Server and configure the following parameters:

#### Table 65:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.</td>
</tr>
<tr>
<td>VPN ID</td>
<td>Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. \textit{Range:} 0 through 65530</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Priority</td>
<td>Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. <strong>priority</strong> can be one of the following: • Emergency—System is unusable (corresponds to syslog severity 0). • Alert—Action must be taken immediately (corresponds to syslog severity 1). • Critical—Critical: A serious condition (corresponds to syslog severity 2). • Error—An error condition that does not fully impair system usability (corresponds to syslog severity 3). • Warning—A minor error condition (corresponds to syslog severity 4). • Notice—A normal, but significant condition (corresponds to syslog severity 5). • Informational—Routine condition (the default) (corresponds to syslog severity 6).</td>
</tr>
</tbody>
</table>

Click Add to save the logging server.

To edit a logging server, click the pencil icon to the right of the entry.

To remove a logging server, click the trash icon to the right of the entry.

To save the feature template, click Save.

**CLI equivalent:**
```plaintext
system
logging
   server (dns-name | hostname | ip-address)
   priority priority
   source-interface interface-name
   vpn vpn-id
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**Multicast**

Use the Multicast template for all vEdge Cloud and vEdge router devices.

To configure a vEdge router to be a multicast replicator using vManage templates:

1. Create a multicast feature template to configure multicast replicator parameters, as described in this article.
2. Create a PIM feature template to enable PIM on each VPN that participates in a multicast domain. See the PIM help topic.
3. Create a VPN feature template to configure parameters for the VPN that is running PIM. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.

7. Under Additional VPN Templates, located to the right of the screen, click Multicast.

8. From the Multicast drop-down, click Create Template. The Multicast template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Multicast parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

Table 66:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure a Multicast Replicator

To configure a vEdge router to be a multicast replicator, in the Basic Configuration tab, configure the following parameters:

Table 67:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Click On to configure the local router as a multicast replicator.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Specify the number of joins per group that the router can accept. For each join, the router can accept 256 outgoing tunnel interfaces (OILs). Range: 0 through 1000 Default: 0. A value of 0 means that the router can accept any number of (*,G) and (S,G) joins.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:

```
vpn vpn-id router
multicast-replicator local [threshold number]
```
Release Information

Introduced in vManage NMS in Release 15.2.

NTP

Use the NTP template for all Viptela devices.

Configure network time protocol (NTP) servers on your Viptela devices in order to synchronize time across all devices in the Viptela overlay network. You can configure up to four NTP servers, and they must all be located or reachable in the same VPN.

Other devices are allowed to ask a Viptela device for the time, but no devices are allowed to use the Viptela device as an NTP server.

To configure NTP using vManage templates:

1. Create an NTP feature template to configure NTP parameters, as described in this article.
2. Configure the timezone in the System template. See the System help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ▶ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Select the Basic Information tab.
6. Under Additional System Templates, located to the right of the screen, click NTP.
7. From the NTP drop-down, click Create Template. The NTP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining NTP parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
### Configure NTP Servers

To configure NTP servers, select the Server tab and click Add New Server. Then configure the following parameters. Parameters marked with an asterisk are required to configure NTP.

#### Table 69:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address*</td>
<td>Enter the IP address of an NTP server or of a DNS server that knows how to reach the NTP server.</td>
</tr>
<tr>
<td>Authentication Key*</td>
<td>Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the Trusted Keys field, under the Authentication tab (discussed below).</td>
</tr>
</tbody>
</table>
| VPN ID*               | Enter the number of the VPN to use to reach the NTP server or the VPN in which the NTP server is located. If you configure multiple NTP servers, they must all be located or reachable in the same VPN.  
*Range*: 0 through 65530 |
| Version*              | Enter the version number of the NTP protocol software.  
*Range*: 1 through 4  
*Default*: 4 |
| Source Interface      | Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored. |
To add the NTP server, click Add.

To add another NTP server, click Add New Server. You can configure up to four NTP servers. The Viptela software uses the server at the highest stratum level.

To edit an NTP server, click the pencil icon to the right of the entry.

To delete an NTP server, click the trash icon to the right of the entry.

To save the feature template, click Save.

**CLI equivalent:**

```
system ntp
  server (dns-server-address | ip-address)
    key key-id
    prefer
    source-interface interface-name
    version number
    vpn vpn-id
```

## Configure NTP Authentication

To configure authentication keys used to authenticate NTP servers, in the Authentication tab, click the Authentication Key tab. Then click Add New Authentication Key, and configure the following parameters. Parameters marked with an asterisk are required to configure NTP.

### Table 70:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authentication Key* | Select the following values:  
  • Authentication Key—Enter an MD5 key ID. It can be a number from 1 through 65535.  
  • Authentication Value—Enter either a cleartext key or an AES-encrypted key. |
| Authentication Value*| Enter an MD5 authentication key. For the key to be used, you must designate it as trusted. To associate a key with a server, enter the same value as you use for the the Authentication Key field on the Server tab. |

To configure trusted keys used to authenticate NTP servers, in the Authentication tab, click the Trusted Keys tab and configure the following parameters;

### Table 71:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enter the MD5 authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value as you use for the the Authentication Key field on the Server tab.

**CLI equivalent:**

```
system
tp
  keys
    authentication key-id md5 md5-key
    trusted key-id
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**OMP**

Use the OMP template to configure OMP parameters for all vEdge Cloud and vEdge router devices, and for vSmart controllers.

The Viptela Overlay Management Protocol (OMP) establishes and maintains the Viptela control plane.

OMP is enabled by default on all 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.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for OMP, select the Factory_Default_OMP_Template and click Create Template. The OMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OMP parameters. You may need to click a tab or the plus sign (+) to display additional fields.
6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 72:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.  
To change the default key, type a new string and move the cursor out of the Enter Key box.  
Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon)       | Enter a value for the parameter, and apply that value to all devices.  
Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

Configure Basic OMP Options

To configure basic OMP options, select the Basic Configuration tab and configure the following parameters. All parameters are optional.

Table 73:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful Restart for OMP</td>
<td>Ensure that Yes is selected to enable graceful restart. By default, graceful restart for OMP is enabled.</td>
</tr>
<tr>
<td>Overlay AS Number (on vEdge routers only)</td>
<td>Specify a BGP AS number that OMOP advertises to the router's BGP neighbors.</td>
</tr>
<tr>
<td>Graceful Restart Timer</td>
<td>Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 through 604800 seconds (168 hours, or 7 days) Default: 43200 seconds (12 hours)</td>
</tr>
<tr>
<td>Number of Paths Advertised per Prefix</td>
<td>Specify the maximum number of equal-cost routes to advertise per prefix. vEdge routers advertise routes to vSmart controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A vEdge router can have up to four TLOCs, and by default advertises each route-TLOC tuple to the vSmart controller. If a local site has two vEdge routers, a vSmart controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 through 16 Default: 4</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ECMP Limit (on vEdge routers only)</td>
<td>Specify the maximum number of OMP paths received from the vSmart controller that can be installed in the vEdge router's local route table. By default, a vEdge router installs a maximum of four unique OMP paths into its route table. <em>Range:</em> 1 through 32  <em>Default:</em> 4</td>
</tr>
<tr>
<td>Send Backup Paths (on vSmart Controllers only)</td>
<td>Click On to have OMP advertise backup routes to vEdge routers. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Ensure that No is selected, to enable to Viptela overlay network. Click Yes to disable OMP and disable the Viptela overlay network. OMP is enabled by default.</td>
</tr>
<tr>
<td>Discard rejected (on vSmart controllers only)</td>
<td>Click Yes to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes are not discarded.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```plaintext
omp discard-rejected (on vSmart controllers only)
ecmp-limit number (on vEdge routers only)
graceful-restart
  overlay-as as-number (on vEdge routers only)
send-backup-paths (on vSmart controllers only)
send-path-limit number
[no] shutdown
```

### Configure OMP Timers

To configure OMP timers, select the Timers tab and configure the following parameters:

**Table 74:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Advertisement Interval | Specify the time between OMP Update packets.  
*Range:* 0 through 65535 seconds  *Default:* 1 second |
| Hold Time | Specify how long to wait before closing the OMP connection to a peer. If the peer does not receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed.  
*Range:* 0 through 65535 seconds  *Default:* 60 seconds |
| EOR Timer | Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that were not refreshed after the OMP session came back up are considered to be stale and are deleted from the route table.  
*Range:* 1 through 3600 seconds (1 hour)  *Default:* 300 seconds (5 minutes) |

To save the feature template, click Save.

**CLI equivalent:**

```plaintext
```

---

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
Configure OMP Advertisements

To advertise routes learned locally by the vEdge router to OMP, select the Advertise tab and configure the following parameters:

Table 75:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertise (on vEdge routers only)</td>
<td>Click On or Off to enable or disable the vEdge router advertising to OMP the routes that it learns locally:</td>
</tr>
<tr>
<td></td>
<td>• BGP—Click On to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.</td>
</tr>
<tr>
<td></td>
<td>• Connected—Click Off to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.</td>
</tr>
<tr>
<td></td>
<td>• OSPF—Click On and click On again in the External field that appears to advertise external OSPF routes to OMP. OSPF inter-area and intra-area routes are always advertised to OMP. By default, external OSPF routes are not advertised to OMP.</td>
</tr>
<tr>
<td></td>
<td>• Static—Click Off to disable advertising static routes to OMP. By default static routes are advertised to OMP.</td>
</tr>
</tbody>
</table>

To configure per-VPN route advertisements to OMP, use the VPN feature template.

To save the feature template, click Save.

**CLI equivalent:**

```
omp advertise (bgp | connected | ospf | static) (on vEdge routers only)
```

**Release Information**

Introduced in vManage NMS in Release 15.2. In Release 17.1, add Overlay AS Number field.

---

**OSPF**

Use the OSPF template for all vEdge Cloud and vEdge router devices.

To configure OSPF on vEdge routers using vManage templates:

1. Create an OSPF feature template to configure OSPF parameters, as described in this article. OSPF can be used for service-side routing, to provide reachability to networks at the local site, and it can be used for transport-side routing, to enable communication between the vEdge router and other Viptela devices when the router is not directly connected to the WAN cloud. Create separate OSPF templates for the two OSPF routing types.
2. Create a VPN feature template to configure VPN parameters for either service-side OSPF routing (in any VPN other than VPN 0 or VPN 512) or transport-side OSPF routing (in VPN 0). See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click OSPF.
   3. From the OSPF drop-down, click Create Template. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.

6. To create a template for VPNs 1 through 511, and 513 through 65530:
   1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
   2. Click the Service VPN drop-down.
   3. Under Additional VPN Templates, located to the right of the screen, click OSPF.
   4. From the OSPF drop-down, click Create Template. The OSPF template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining OSPF parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 76:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific                     | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box.
Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon)  | Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

Configure Basic OSPF

To configure basic OSPF, select the Basic Configuration tab and then configure the following parameters. All these parameters are optional. For OSPF to function, you must configure area 0, as described below.

Table 77:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Enter the OSPF router ID, in decimal four-part dotted notation. This is the IP address associated with the router for OSPF adjacencies.</td>
</tr>
</tbody>
</table>
| Distance for External Routes | Specify the OSPF route administration distance for routes learned from other domains.  
  
  Range: 0 through 255  
  Default: 110 |
| Distance for Inter-Area Routes | Specify the OSPF route administration distance for routes coming from one area into another.  
  
  Range: 0 through 255  
  Default: 110 |
| Distance for intra-Area routes | Specify the OSPF route administration distance for routes within an area.  
  
  Range: 0 through 255  
  Default: 110 |

To save the feature template, click Save.

CLI equivalent:
Redistribute Routes into OSPF

To redistribute routes learned from other protocols into OSPF on vEdge routers, select the Redistribute tab. Click Add New Redistribute and configure the following parameters:

**Table 78:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the protocol from which to redistribute routes into OSPF. Select from BGP, Connected, NAT, OMP, and Static.</td>
</tr>
<tr>
<td>Route Policy</td>
<td>Enter the name of a localized control policy to apply to routes before they are redistributed into OSPF.</td>
</tr>
</tbody>
</table>

To add another OSPF route redistribution policy, click the plus sign (+).

To remove an OSPF route redistribution policy from the template configuration, click the trash icon to the right of the entry.

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id
router ospf
   redistribute (bgp | connected | nat | omp | static) route-policy policy-name
```

Configure OSPF To Advertise a Maximum Metric

To configure OSPF to advertise a maximum metric so that other routers do not prefer this vEdge router as an intermediate hop in their Shortest Path First (SPF) calculation, select the Maximum Metric (Router LSA) tab. Then click Add New Router LSA and configure the following parameters:

**Table 79:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select a type:</td>
</tr>
<tr>
<td></td>
<td>• Administrative—Force the maximum metric to take effect immediately, through operator intervention.</td>
</tr>
<tr>
<td></td>
<td>• On-Startup—Advertise the maximum metric for the specified time.</td>
</tr>
</tbody>
</table>
**Advertisement Time**

If you selected On-Startup, specify the number of seconds to advertise the maximum metric after the router starts up.

*Range: 0, 5 through 86400 seconds
Default: 0 seconds (the maximum metric is advertised immediately when the router starts up)*

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id router ospf
    max-metric
    router-lsa (administrative | on-startup seconds)
```

---

### Configure OSPF Areas

To configure an OSPF area within a VPN on a vEdge router, select the Area tab and click Add New Area. For OSPF to function, you must configure area 0.

**Table 80:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Area Number    | Enter the number of the OSPF area.  
*Range: 32-bit number* |
| Set the Area Type | Select the type of OSPF area, Stub or NSSA. |
| No Summary     | Select On to not inject OSPF summary routes into the area. |
| Translate      | If you configured the area type as NSSA, select when to allow vEdge routers that are ABRs (area border routers) to translate Type 7 LSAs to Type 5 LSAs:  
always—Router always acts as the translator for Type 7 LSAs. That is, no other router, even if it is an ABR, can be the translator. If two ABRs are configured to always be the translator, only one of them actually ends up doing the translation. candidate—Router offers translation services, but does not insist on being the translator. never—Translate no Type 7 LSAs |

To save the new area, click Add.

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id
    router ospf area number nssa
    no-summary
    translate (always | candidate | never)
    stub
    no-summary
```
### Configure Interfaces in an OSPF Area

To configure the properties of an interface in an OSPF area, select the Area tab and click Add New Area. Then, in Interface, click Add Interface. In the Add Interface popup, configure the following parameters:

#### Table 81:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Enter the name of the interface, in the format ge slot/port or loopback number.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Specify how often the router sends OSPF hello packets.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>Specify how often the vEdge router must receive an OSPF hello packet from its neighbor. If no packet is received, the vEdge router assumes that the neighbor is down.</td>
</tr>
<tr>
<td>LSA Retransmission Interval</td>
<td>Specify how often the OSPF protocol retransmits LSAs to its neighbors.</td>
</tr>
<tr>
<td>Interface Cost</td>
<td>Specify the cost of the OSPF interface.</td>
</tr>
</tbody>
</table>

To configure advanced options for an interface in an OSPF area, in the Add Interface popup, click Advanced Options and configure the following parameters:

#### Table 82:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated Router Priority</td>
<td>Set the priority of the router to be elected as the designated router (DR). The router with the highest priority becomes the DR. If the priorities are equal, the node with the highest router ID becomes the DR or the backup DR. Range: 0 through 255 Default: 1</td>
</tr>
</tbody>
</table>
| OSPF Network Type     | Select the OSPF network type to which the interface is to connect:  
  - Broadcast network—WAN or similar network.  
  - Point-to-point network—Interface connects to a single remote OSPF router.  
  Default: Broadcast |
| Passive Interface     | Select On or Off to specify whether to set the OSPF interface to be passive. A passive interface advertises its address, but does not actively run the OSPF protocol. Default: Off |
| Authentication        | Specify the authentication and authentication key on the interface, to allow OSPF to exchange routing update information securely:  
  - Authentication Type: Simple  
  - Authentication Key: ExampleKey |

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authentication Type</td>
<td>Select the authentication type:</td>
</tr>
<tr>
<td></td>
<td>• Simple authentication—Password is sent in clear text.</td>
</tr>
<tr>
<td></td>
<td>• Message-digest authentication—MD5 algorithm generates the password.</td>
</tr>
<tr>
<td>• Authentication Key</td>
<td>Enter the authentication key. Plain text authentication is used when devices within an area cannot support the more secure MD5 authentication. The key can be 1 to 32 characters.</td>
</tr>
<tr>
<td>Message Digest</td>
<td>Specify the key ID and authentication key if you are using message digest (MD5):</td>
</tr>
<tr>
<td>• Message Digest Key ID</td>
<td>Enter the key ID for message digest (MD5 authentication). It can be 1 to 32 characters.</td>
</tr>
<tr>
<td>• Message Digest Key</td>
<td>Enter the MD5 authentication key, in clear text or as an AES-encrypted key. It can be from 1 to 255 characters.</td>
</tr>
</tbody>
</table>

To save the interface configuration, click Save.

To save the new area, click Add.

To save the feature template, click Save.

**CLI equivalent:**

```bash
vpn vpn-
  id
  router ospf area number
  interface interface-name
  authentication
    authentication-key key
    message-digest key
    type (message-digest | simple)
    cost number
  dead-interval seconds
  hello-interval seconds
  network (broadcast | point-to-point)
  passive-interface
  priority number retransmit-interval seconds
```

**Configure an Interface Range for Summary LSAs**

To configure the properties of an interface in an OSPF area, select the Area tab and click Add New Area. Then, in Range, click Add Range. In the Area Range popup, click Add Area Range and configure the following parameters:

**Table 83:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the IP address and subnet mask, in the format prefix/length, for the IP addresses to be consolidated and advertised.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Cost</td>
<td>Specify a number for the Type 3 summary LSA. OSPF uses this metric during its SPF calculation to determine the shortest path to a destination. <em>Range:</em> 0 through 16777215</td>
</tr>
<tr>
<td>No Advertise</td>
<td>Select On to not advertise the Type 3 summary LSAs or Off to advertise them.</td>
</tr>
</tbody>
</table>

To save the area range, click Save.

To save the new area, click Add.

To save the feature template, click Save.

**CLI equivalent:**
```
vpn vpn- id
  router ospf area number range prefix/length
  cost number
  no-advertise
```

### Configure Other OSPF Properties

To configure other OSPF properties, select the Advanced tab and configure the following properties:

**Table 84:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Bandwidth</td>
<td>Specify the reference bandwidth for the OSPF auto-cost calculation for the interface.</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 1 through 4294967 Mbps</td>
</tr>
<tr>
<td></td>
<td><em>Default:</em> 100 Mbps</td>
</tr>
<tr>
<td>RFC 1538 Compatible</td>
<td>By default, the OSPF calculation is done per RFC 1583. Select Off to calculate the cost of summary routes based on RFC 2328.</td>
</tr>
<tr>
<td>Originate</td>
<td>Click On to generate a default external route into an OSPF routing domain:</td>
</tr>
<tr>
<td></td>
<td>• Always—Select On to always advertise the default route in an OSPF routing domain.</td>
</tr>
<tr>
<td></td>
<td>• Default metric—Set the metric used to generate the default route. <em>Range:</em> 0 through 16777215</td>
</tr>
<tr>
<td></td>
<td>• Metric type—Select to advertise the default route as an OSPF Type 1 external route or an OSPF Type 2 external route.</td>
</tr>
<tr>
<td>SPF Calculation Delay</td>
<td>Specify the amount of time between when the first change to a topology is received until performing the SPF calculation.</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 0 through 600000 milliseconds (60 seconds)</td>
</tr>
<tr>
<td></td>
<td><em>Default:</em> 200 milliseconds</td>
</tr>
<tr>
<td>Initial Hold Time</td>
<td>Specify the amount of time between consecutive SPF calculations.</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 0 through 600000 milliseconds (60 seconds)</td>
</tr>
<tr>
<td></td>
<td><em>Default:</em> 1000 milliseconds</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Hold Time</td>
<td>Specify the longest time between consecutive SPF calculations.</td>
</tr>
<tr>
<td></td>
<td><em>Range: 0 through 600000</em></td>
</tr>
<tr>
<td></td>
<td><em>Default: 10000 milliseconds (60 seconds)</em></td>
</tr>
<tr>
<td>Policy Name</td>
<td>Enter the name of a localized control policy to apply to routes coming from OSPF neighbors.</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**CLI equivalent:**

```cl
vpn vpn-id
router
ospf auto-cost reference-bandwidth mbps
compatible rfc1583
default-information
  originate (always | metric metric | metric-type type)
route-policy policy-name in
timers
  spf delay initial-hold-time maximum-hold-time
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**PIM**

Use the PIM template for all vEdge Cloud and vEdge router devices.

To configure the PIM Sparse Mode (PIM-SM) protocol using vManage templates so that a router can participate in the Viptela multicast overlay network:

1. Create a PIM feature template to configure PIM parameters, as described in this article.
2. Optionally, create an IGMP feature template to allow individual hosts on the service side to join multicast groups within a particular VPN. See the IGMP help topic.
3. Optionally, create a Multicast feature template to configure a vEdge router to be a multicast replicator. See the Multicast help topic.
4. Create a VPN feature template to configure parameters for the VPN that is running PIM. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

6. Click the Service VPN drop-down.

7. Under Additional VPN Templates, located to the right of the screen, click PIM.

8. From the PIM drop-down, click Create Template. The PIM template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PIM parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 85:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific                  | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
  When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.  
  To change the default key, type a new string and move the cursor out of the Enter Key box.  
  Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global                            | Enter a value for the parameter, and apply that value to all devices.  
  Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

**Configure Basic PIM**

To configure PIM, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure PIM.

**Table 86:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Ensure that No is selected, to enable PIM.</td>
</tr>
<tr>
<td>Auto-RP</td>
<td>Click On to enable auto-RP to enable automatic discovery of rendezvous points (RPs) in the PIM network so that the router receivea group-to-RP mapping updates. By default, auto-RP is disabled.</td>
</tr>
<tr>
<td>SPT Threshold</td>
<td>Specify the traffic rate, in kbps, at which to switch from the shared tree to the shortest-path tree (SPT). Configuring this value forces traffic to remain on the shared tree and travel via the RP instead of via the SPT.</td>
</tr>
</tbody>
</table>
| Replicator      | For a topology that includes multicast replicators, determine how the replicator for a multicast group is chosen:  
  • Random—Choose the replicator at random.  
  • Sticky—Always use the same replicator. This is the default. |
To save the feature template, click Save.

**CLI equivalent:**
```
vpn vpn-id
router
  pim auto-rp replicator-selection
    [no] shutdown spt-threshold kbps
```

**Configure PIM Interfaces**

If the router is just a multicast replicator and is not part of a local network that contains either multicast sources or receivers, you do not need to configure any PIM interfaces. The replicator learns the locations of multicast sources and receivers from the OMP messages it exchanges with the vSmart controller. These control plane messages are exchanged in the transport VPN (VPN 0). Similarly, other vEdge routers discover replicators dynamically, through OMP messages from the vSmart controller.

To configure PIM interfaces, select the Interface tab. Then click Add New Interface and configure the following parameters:

**Table 87:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of an interface that participates in the PIM domain, in the format ge slot/port.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Specify how often the interface sends PIM hello messages. Hello messages advertise that PIM is enabled on the router. <em>Range:</em> 1 through 3600 seconds <em>Default:</em> 30 seconds</td>
</tr>
<tr>
<td>Join/Prune Interval</td>
<td>Specify how often PIM multicast traffic can join or be removed from a rendezvous point tree (RPT) or shortest-path tree (SPT). vEdge routers send join and prune messages to their upstream RPF neighbor. <em>Range:</em> 10 through 600 seconds <em>Default:</em> 60 seconds</td>
</tr>
</tbody>
</table>

To edit an interface, click the pencil icon to the right of the entry.

To delete an interface, click the trash icon to the right of the entry.

To save the feature template, click Save.

**CLI equivalent:**
```
vpn vpn-id
router
  pim interface interface-name
  hello-interval seconds
  join-prune-interval seconds
```

**Release Information**

Introduced in vManage NMS in Release 15.2.

**Security**

Use the Security screen to create security policies to implement the Cisco SD-WAN security solution on IOS XE SD-WAN routers in the overlay network. The Cisco SD-WAN security solution provides an integrated...
security solution that address all key enterprise security profiles: Compliance, Guest Access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).

You can configure the following Cisco SD-WAN security mechanisms:

- Application-Aware Enterprise Firewall
- Intrusion prevention and detection (IPS/IDS)
- URL filtering
- Umbrella DNS security

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- Title bar—Includes the title of the screen, Security, and the following:
  - Custom Options—Click to display, create, and edit a components for use in security policy. These components are Lists, which include signatures, whitelist URLs, blacklist URLs, and zones; zone-based firewall policies; intrusion prevention policies; URL-filtering policies, and Umbrella DNS policies.

- Security wizard—When you have not yet configured any security policies, the Security pages displays a security configuration wizard, which consists a security icon and an Add Security Policy button. Click this button to start the security policy wizard.

- Add Security Policy—When you have configured one or more security policies, the Add Security Policy button is displayed. Click to create a firewall policy using the security policy configuration wizard.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.

- Refresh icon—Click to refresh data in the policies table with the most current data.

- Show Table Columns icon—Click to display or hide columns from the security policies table. By default, all columns are displayed.

- Security policy table—To re-arrange the columns, drag the column title to the desired position.
Configure Security Policies

You configure security policies with a configuration wizard. The wizard is a UI policy builder that consists of screens to guide you through the creation and modification of the following security policy components:

- Enterprise firewall—Allows you to filter data packets, to match allowed data traffic and drop unwanted traffic. You enable enterprise firewalls by configuring zones. Zone configuration consists of the following components:
  - Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
• **Destination zone**—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.

• **Firewall policy**—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.

• **Zone pair**—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

• **Intrusion prevention policy**—Protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

• **URL filtering policy**—Allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on whitelists, blacklists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blacklist, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the whitelist, the traffic is allowed without further URL filtering inspection.

• **DNS security policy**—Directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella uses DNS to stop threats over all ports and protocols and over direct-to-IP connections.

### Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Security Policy.
3. From the Add Security Policy popup, select the desired security policy type:

   • **Compliance policy**—Consists of an application firewall policy and an intrusion prevention policy.
   • **Guest access policy**—Consists of an application firewall policy and a URL-filtering policy.
   • **Direct cloud access policy**—Consists of an application firewall policy, an intrusion prevention policy, and an Umbrella DNS security policy.
   • **Direct internet access policy**—Consists of an application firewall policy, an intrusion prevention policy, a URL-filtering policy, and an Umbrella DNS security policy.
   • **Custom security policy**—Consists of an application firewall policy and your choice of the remaining security policy components (intrusion prevention, Umbrella DNS, and URL filtering).

1. Click Proceed.
The security policy configuration wizard opens, and the Firewall screen displays.

**Step 2: Configure Application Firewall Policy**

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
   1. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
   2. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
   3. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
   - Click Add Sequence Rule.
   - Click Match to add a match condition. You can match the following: - Source Data Prefix - Source Port - Destination Data Prefix - Destination Port - Protocol - Application/Application Family List
   - Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions: - Inspect: Inspect the packet's header to determine its source address and port. - Log: Log the packet headers. - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.
   - Click Save Match and Actions.
   - Add additional sequence rules as needed.
   - Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which they are defined in the policy.
7. Click Save Firewall Policy.
8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Firewall popup:
1. In the Policy field, select a policy.
2. In the Policy Name field, select a policy name.
3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

Step 3: Configure Security Policy Components

Step 3a: Configure Intrusion Prevention

To create a new intrusion prevention policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Click Create New. The Add Intrusion Prevention Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Signature Set field, select the desired signature set:

   - Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
     - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
     - Exploit-kit—Rules that are designed to detect exploit kit activity.
     - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
     - SQL Injection—Rules that are designed to detect SQL Injection attempts.
   - Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.
   - Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
     - App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
• Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

• Exploit-kit—Rules that are designed to detect exploit kit activity.

• Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.

• SQL Injection—Rules that are designed to detect SQL Injection attempts.

1. In the Inspection Mode field, select the desired inspection mode:
   • Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
   • Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

1. In the Advanced ► Signature Whitelist field, select the desired signature list.

2. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.

3. Configure the VPNs to which to apply the intrusion prevention policy:
   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   3. Click Save Changes.

4. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.

5. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Intrusion Prevention Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

Step 3b: Configure Umbrella DNS

To create a new Umbrella DNS policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Umbrella Registration Status field:
   1. Click Manage Umbrella Registration.
   2. In the Manage Umbrella Registration pop-up, enter your Umbrella registration token.
   3. Click Save Changes.
5. By default, the DNS security policy applies to all VPNs, so the Match All VPN field is selected. To apply the DNS security policy to a custom set of VPNs:
   1. Select the Custom VPN Configuration field.
   2. In the Target field, click Add Target VPNS.
   3. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNS, separate the numbers with commas.
   4. Click Save Changes.
6. In the Local Domain Bypass List field, select the web domain list that lists the websites domains that are allowed by bypass DNS lookups. To create a domain list:
   1. Click in the Local Domain Bypass List field and then click Add New Domain List.
   2. In the Domain List Name field, enter a name for the domain list.
   3. In the Domain field, enter one or more web domains. Examples of website domains are cisco.com and *.cisco.com. Separate lists with a comma. The first item in the list cannot start with an asterisk (*).
   4. Click Save.
7. In the DNS Server IP field, select the IP address of the DNS server. By default, traffic using Umbrella as the DNS server. To use a different DNS server, select Custom DNS and enter the IP address of the DNS server.
8. In the Advanced ▶ DNSCrypt field, configure the encryption of DNS traffic. By default, encryption is enabled. To disable DNS traffic encryption, move the slider to the left.
9. Click Save DNS Security Policy. The intrusion prevention policy is then listed in the policy table.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing DNS Security Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. Click Copy. The copied policy is listed in the Security Policy Firewall table.


**Step 3c: Configure URL Filtering**

To create a new URL-filtering policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.
2. Click Create New. The Add URL Filtering Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Web Categories field:
   1. In the Block drop-down, define the action to take if a URL matches a website category. Select Block (the default) to block access to the website category, or select Allow to allow access to the website category.
   2. In the Web Category field, select one or more webpage categories to block or accept. A category defines websites that contain a certain type of content. When you configure category-based or reputation-based URL filtering, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. To check a website's reputation, use the Webroot BrightCloud URL/IP Lookup tool.
5. In the Web Reputation field, select the reputation level of the website to block or accept. Each URL has a reputation score associated with it. The score ranges from 0 through 100 and is labeled as follows:
   - High Risk—Reputation score 0 through 20
   - Suspicious—Reputation score 0 through 40
   - Moderate Risk—Reputation score 0 through 60. This is the default reputation setting.
   - Low Risk—Reputation score 0 through 80.
   - Trustworthy—Reputation score 0 through 100.

   1. In the Advanced ▶ Whitelist URL List field, select a URL list to include in the URL filtering policy. A URL whitelist allows the specified URLs and blocks URLs not included in the list. For each URL filtering policy, you can configure only one whitelist URL list. To create a new list of URLs to whitelist:
      1. Click in the Advanced ▶ Whitelist URL List field.
      2. Click Add New Whitelist URL List.
      3. In the Whitelist URL List Name field, enter a name for the whitelist.
4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as \*\.cisco\.com.

5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.

6. Click Save.

2. In the Advanced ► Blacklist URL List field, select one or more URL blacklists to include in the URL filtering policy. A URL blacklist blocks the specified URLs and allows URLs not included in the list. For each URL filtering policy, you can configure only one blacklist URL list. To create a new list of URLs to blacklist:
   1. Click in the Advanced ► Blacklist URL List field.
   2. Click Add New Blacklist URL List.
   3. In the Blacklist URL List Name field, enter a name for the blacklist.
   4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as \*\.cisco\.com.
   5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.
   6. Click Save.

3. In the Advanced ► Block Page Server section, configure how to handle blocked HTTP URLs. For blocked HTTPS websites, no blocking or redirection is performed. Instead, all traffic is dropped.
   1. To block and not display the content of a webpage, click Block Page Content. Then, type the message to display to the user indicated why the webpage is not displayed. This is the default method for handling blocked URLs. In the Default Content Header field, type the title of the message, which is displayed in bold letters. The default header is, "Access to the requested page has been denied." In the Content Body field, type the content of the blocked page message. The default message is, "Please contact your network administrator".
   2. To redirect to another URL, click Redirect URL. Then, enter the URL to which to redirect the user.

4. In the Advanced ► Alerts and Logs section, configure when to send alerts and syslog messages:
   1. Click Blacklist to send alerts when a blacklisted URL is blocked.
   2. Click Whitelist to send alerts when a whitelisted URL is allowed.
   3. Click Reputation/Category to send alerts when a URL is blocked because of its category or reputation.

5. Configure the VPNs to which to apply the URL filtering policy:
   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the URL filtering policy. To specify multiple VPNs, separate the numbers with commas.
   3. Click Save Changes.

6. Click Save URL Filtering Policy. The URL filtering policy is then listed in the policy table.

7. Click Next. The Policy Summary screen displays.
To copy an existing URL filtering policy into the guest access policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing URL Filtering Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the URL Filtering table.

**Step 4: Configure Additional Policy Settings**

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).
2. In the Security Policy Description field,
3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.
5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.
6. By default, system logging (syslog) is enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.
7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.
9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.
10. Click Save Policy. The policy is listed in the table on the Configuration ➤ Policy screen.

Step 5: Apply the Security Policy to an IOS XE SD-WAN Router

1. In vManage NMS, select the Configuration ➤ Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.
   4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
   5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.
   6. Click Create (for a new template) or Update (for an existing template).

View a Security Policy

1. In the security policy table, select a policy. Or, click the Custom Options drop-down and select the security policy component.

2. Click the More Actions icon to the right of the column and click View.

3. Click Cancel to return to the policies table.

For a policy created using the security policy configuration wizard, you can view the policy in graphical format:

1. In the security policy table, select a policy. Or, click the Custom Options drop-down and select the security policy component.

2. Click the More Actions icon to the right of the column and click Graphical Preview.
3. Click Dismiss to return to the policies table.

**Edit a Security Policy**

1. In the security policy table, select a policy. Or, click the Custom Options drop-down and select the security policy component.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

**Edit or Create a Security Policy Component**

You can create individual zone-based firewall components directly and then use them or import them when you are using the security policy configuration wizard:

1. In the Title bar, click the Custom Options drop-down.
2. Select the security policy component:
   - Lists, which include signatures, whitelist URLs, blacklist URLs, and zones; zone-based firewall policies
   - Intrusion prevention policies
   - URL-filtering policies
   - Umbrella DNS policies.

**Delete a Security Policy**

1. In the security policy table, select a policy.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the policy.

---

**Security**

Use the Security template for all Viptela devices. 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.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ➤ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for Security, select the Factory_Default_Security_Template and click Create Template. The Security template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Security parameters.

6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

7. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 88:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure Control Plane Security

To configure the control plane connection protocol on a vManage NMS or a vSmart controller, select the Basic Configuration tab and configure the following parameters:

Table 89:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select the protocol to use on control plane connections to a vSmart controller: • DTLS (Datagram Transport Layer Security). This is the default. • TLS (Transport Layer Security)</td>
</tr>
<tr>
<td>Control TLS Port</td>
<td>If you selected TLS, configure the port number to use: Range: 1025 through 65535 Default: 23456</td>
</tr>
</tbody>
</table>

To save the feature template, click Save

CLI equivalent:

```plaintext
security control
  protocol (dtls | tls)
  tls-port port-number
```
Configure Data Plane Security

To configure data plane security on a vBond controller or vEdge router, select the Basic Configuration and Authentication Type tabs, and configure the following parameters:

Table 90:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rekey Time</td>
<td>Specify how often a vEdge router changes the AES key used on its secure DTLS connection to the vSmart controller. If OMP graceful restart is enabled, the rekeying time must be at least twice the value of the OMP graceful restart timer. <strong>Range:</strong> 10 through 1209600 seconds (14 days) <strong>Default:</strong> 86400 seconds (24 hours)</td>
</tr>
<tr>
<td>Replay Window</td>
<td>Specify the size of the sliding replay window. <strong>Values:</strong> 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets <strong>Default:</strong> 512 packets</td>
</tr>
</tbody>
</table>
| Authentication Type | Select the authentication types from the Authentication List, and click the arrow to move them to the Selected List:  
  - ah-no-id—Enable a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the packet's outer IP header.  
  - ah-sha1-hmac—Enable AH-SHA1 HMAC and ESP HMAC-SHA1.  
  - none—Select no authentication.  
  - sha1-hmac—Enable ESP HMAC-SHA1. |

To save the feature template, click Save.

CLI equivalent:

```
security ipsec authentication-type type rekey seconds replay-window number
```

Release Information

Introduced in vManage NMS in Release 15.2.

SNMP

Use the SNMP template to configure SNMP parameters for all Viptela devices and Cisco IOS XE routers running the SD-WAN software.

Note: A single device template can contain only one SNMP feature template. So in a single device template you can configure either SNMPv2 or SNMPv3, but not both.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.

5. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.

6. From the SNMP drop-down, click Create Template. The SNMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining SNMP parameters.

7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 91:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon)           | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
  
  When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.  
  
  To change the default key, type a new string and move the cursor out of the Enter Key box.  
  
  Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon)                   | Enter a value for the parameter, and apply that value to all devices.  
  
  Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

**Configuring Basic SNMP**

To configure basic SNMP, select the SNMP tab and configure the following parameters. All parameters are required.

**Table 92:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown</td>
<td>Click No to enable SNMP. By default, SNMP is disabled.</td>
</tr>
<tr>
<td>Name of Device for SNMP</td>
<td>Enter a name for the Viptela device to identify it in SNMP notifications.</td>
</tr>
<tr>
<td>Contact Person</td>
<td>Enter the name of the network management contact person in charge of managing the Viptela device. It can be a maximum of 255 characters.</td>
</tr>
<tr>
<td>Location of Device</td>
<td>Enter a description of the location of the device. It can be a maximum of 255 characters.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**
Configure SNMPv2

To configure SNMPv2, select the SNMP Version tab and click V2. For SNMPv2, you can configure communities and trap information.

To configure SNMP views, in the View & Community section, select the View tab. Then click Add New View, and configure the following parameters:

**Table 93:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all views before adding a community.</td>
</tr>
</tbody>
</table>

Object Identifiers

Click Add Object Identifiers and configure the following parameters:

- Exclude OID—Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Viptela MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name.

- On/Odd—Click Off to include the OID in the view or click On to exclude the OID from the view.

To save the object identifiers, click Save.

To remove an OID from the list, click the minus sign to the right of the entry.

To add the SNMP view, click Add.

To configure the SNMP community, select the Community tab. Then click Add New Community, and configure the following parameters:

**Table 94:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the community. The name can be from 1 through 32 characters and can include angle brackets (&lt; and &gt;).</td>
</tr>
<tr>
<td>Authorization</td>
<td>Select read-only from the dropdown list. The MIBs supported by the Viptela software do not allow write operations, so you can configure only read-only authorization.</td>
</tr>
<tr>
<td>View</td>
<td>Select a view to apply to the community. The view specifies the portion of the MIB tree the community can access.</td>
</tr>
</tbody>
</table>
To add the SNMP community, click Add.

To configure trap, in the Trap section, select the Trap Group tab. Then click Add New Trap Group, and configure the parameters below.

Note that an IOS XE router has no trap groups. As such, you must create a dummy trap group before you can configure the trap target server.

**Table 95:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter a name for the trap group. It can be from 1 to 32 characters long.</td>
</tr>
</tbody>
</table>
| Trap Type Modules | Click Add Trap Type Modules, and configure the following parameters: In Severity Levels, select one or more severity levels for the trap—critical, major, or minor. In Module Name, select the type of traps to include in the trap group:  
  - all—All trap types.  
  - app-route—Traps generated by application-aware routing.  
  - bfd—Traps generated by BFD and BFD sessions.  
  - control—Traps generated by DTLS and TLS sessions.  
  - dhcp—Traps generated by DHCP.  
  - hardware—Traps generated by Viptela hardware.  
  - omp—Traps generated by OMP.  
  - routing—Traps generated by BGP, OSPF, and PIM.  
  - security—Trap generated by certificates, vSmart and vEdge serial number files, and IPsec.  
  - system—Traps generated by system-wide functions.  
  - vpn—Traps generated by VPN-specific functions, including interfaces and VRRP. |

To save the trap type module, click Save.

To configure trap target servers, in the Trap section, select the Trap Target Server tab. Then click Add New Trap Group, and configure the parameters below.

Note that on a vEdge router, you can bind a different source interface to each trap target server. On an IOS XE router, however, the last occurrence of the source interface is chosen as the global source interface.

**Table 96:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN ID</td>
<td>Enter the number of the VPN to use to reach the trap server. Range: 0 through 65530</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the SNMP server.</td>
</tr>
</tbody>
</table>
## Table 97: Description

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Port</td>
<td>Enter the UDP port number for connecting to the SNMP server. Range: 1 though 65535.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Select the name of a trap group that was configured under the Group tab.</td>
</tr>
<tr>
<td>Community Name</td>
<td>Select the name of a community that was configured under the Community tab.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>Enter the interface to use to send traps to the SNMP server that is receiving the trap information.</td>
</tr>
</tbody>
</table>

To save the trap target, click Add.

To save the feature template, click Save.

**CLI equivalent:**
```
snmp community name
    authorization {read-only | read-write}
    view string
    trap
    group group-name
    trap-type
    level severity target vpn vpn-id ip-address udp-port
    community-name community-name
    group-name name view string
    oid oid-number [exclude]
```

### Configure SNMPv3

To configure SNMPv3, in SNMP Version, click V3. For SNMPv3, you can configure groups, users, and trap information. Configure groups and trap information as described above.

To configure SNMPv3 users, in the User section, click Add New User and enter the following parameters:

**Table 97:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Select the authentication mechanism for the user:</td>
</tr>
<tr>
<td></td>
<td>• MD5—Use message digest 5.</td>
</tr>
<tr>
<td></td>
<td>• SHA—Use SHA-2 message digest.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Enter the authentication password either in cleartext or as an AES-encrypted key.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>Select the privacy type for the user:</td>
</tr>
<tr>
<td></td>
<td>• AES-CFB-128—Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Enter the authentication password either in cleartext or as an AES-encrypted key.</td>
</tr>
</tbody>
</table>
To save the user, click Add.

To save the feature template, click Save. **CLI equivalent:**

```plaintext
snmp group group-name authentication
  view string
  trap
    group group-name
    trap-type
      level severity target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name name user username
      auth authentication
      auth-password password
      group group-name
      priv privacy
      priv-password password
```

**Release Information**

Introduced in vManage NMS in Release 15.2. In Release 16.2, add support for SNMPv3. In Release 17.2, remove support for DES privacy for the SNMP user.

**Switch Port**

Use the Switch Port template for Cisco IOS XE routers.

To have a vEdge router act as a transparent bridge, configure bridging domains on the router. A router can have up to 16 bridging domains.

To configure the switch ports using vManage templates:

1. Create a Switch Port feature template, as described in this article.
2. To use the switch port for routing, associate it with an SVI. See the VPN Interface SVI help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Additional Templates tab located directly beneath the Description field, or scroll to the Additional Templates section.
6. Click the plus sign (+) next to Switch Port.
7. In the Switch Port drop-down, select the port number.
8. From the lower Switch Port drop-down, click Create Template. The Switch Port template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining switch port parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 98:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure Basic Switch Port Parameters

To configure basic switch port parameters, select the Basic Configuration tab and configure the following parameters:

Table 99:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>Enter the number of the slot in which the Layer 2 switch port module is installed.</td>
</tr>
<tr>
<td>Module</td>
<td>Select the switch port module type, either 4 port or 8 port.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

Associate Interfaces with the Switch Port

To associate an interface with the switch port, click the Interface tab and click Add New Interface. The Wlan-GigabitEthernet0/1/8 interface applies only to C1111-8PW and C1111-8PLTExxW routers. When you configure this interface, select either C1111-8PW or C1111-8PLTExxW when you create a switch port, and select 8 port from the Module drop-down list. In addition, from the New Interface drop-down menu, make sure to select Wlan-GigabitEthernet0/1/8.
Table 100:

<table>
<thead>
<tr>
<th><strong>Parameter Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Enter the name of the interface to associate with the bridging domain, in the format ge slot/port.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Click No to enable the interface. By default, an interface is disabled.</td>
</tr>
<tr>
<td>Switch Port</td>
<td>Select the switch port mode:</td>
</tr>
<tr>
<td></td>
<td>• Access—Configure the interface as an access port. You can configure only one VLAN on an access port, and the port can carry traffic for only one VLAN.</td>
</tr>
<tr>
<td></td>
<td>• VLAN Name—Enter a description for the VLAN.</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID—Enter the VLAN number, which can be a value from 1 through 4094.</td>
</tr>
<tr>
<td></td>
<td>• Trunk—Configure the interface as a trunk port. You can configure one or more VLANs on a trunk port, and the port can carry traffic for multiple VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Allowed VLANs—Enter the numbers of the VLANs for which the trunk can carry traffic. A description for the VLAN.</td>
</tr>
<tr>
<td></td>
<td>• Native VLAN ID—Enter the number of the VLAN allowed to carry untagged traffic.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 101:

<table>
<thead>
<tr>
<th><strong>Parameter Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Age-Out Time</td>
<td>Enter how long an entry is in the MAC table before it ages out. Set the value to 0 to prevent entries from timing out. \textit{Range}: 0, 10 through 1000000 seconds \textit{Default}: 300 seconds</td>
</tr>
<tr>
<td>Static MAC Address</td>
<td>Click Add Static MAC Address to map a MAC address to a switch port. In the MAC Static Address field that appears, enter the following:</td>
</tr>
<tr>
<td></td>
<td>• MAC Address—Enter the static MAC address to map to the switch port interface.</td>
</tr>
<tr>
<td></td>
<td>• Switch Port Interface Name—Enter the name of the switch port interface.</td>
</tr>
<tr>
<td></td>
<td>• VLAN ID—Enter the number of the VLAN for the switch port.</td>
</tr>
<tr>
<td></td>
<td>Click Add to save the static MAC access mapping.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.
**Release Information**

Introduced in vManage NMS in Release 18.3.

**System**

Use the System template for all Viptela devices.

To configure system-wide parameters using vManage templates:

1. Create a System feature template to configure system parameters, as described in this article.
2. Create an NTP feature template to configure NTP servers and authentication. See the NTP help topic.
3. Configure the organization name and vBond orchestrator IP address on the vManage NMS. See the Settings help topic. These settings are appended to the device templates when the templates are pushed to devices.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ➤ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a custom template for System, select the Factory_Default_System_Template and click Create Template. The System template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining System parameters.
6. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
**Table 102:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Specific</strong> (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td><strong>Global</strong> (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Basic System-Wide Configuration**

To set up system-wide functionality on a Viptela device, select the Basic Configuration tab and then configure the following parameters. Parameters marked with an asterisk are required.

**Table 103:**

<table>
<thead>
<tr>
<th>Parameter Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site ID* (on vEdge routers, vManage NMSs, and vSmart controllers)</td>
<td>Enter the identifier of the site in the Viptela overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Viptela devices that reside in the same site. Range: 1 through 4294967295 ((2^{32} - 1))</td>
</tr>
<tr>
<td>System IP*</td>
<td>Enter the system IP address for the Viptela device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.</td>
</tr>
<tr>
<td>Timezone*</td>
<td>Select the timezone to use on the device.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter a name for the Viptela device. It can be up to 32 characters.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter a description of the location of the device. It can be up to 128 characters.</td>
</tr>
<tr>
<td>Parameter Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Groups</td>
<td>Enter the names of one or more groups to which the device belongs, separated by commas.</td>
</tr>
<tr>
<td>Controller Groups (on vEdge routers only)</td>
<td>List the vSmart controller groups to which the vEdge router belongs.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter any additional descriptive information about the device.</td>
</tr>
<tr>
<td>Console Baud Rate (vEdge routers only)</td>
<td>Select the baud rate of the console connection on the vEdge router. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps) Default: 115200 bps</td>
</tr>
<tr>
<td>Maximum OMP Sessions (on vEdge routers only)</td>
<td>Set the maximum number of OMP sessions that a vEdge router can establish to a vSmart controller. Range: 0 through 100 Default: 2</td>
</tr>
<tr>
<td>Dedicated Core for TCP Optimization (optional, on vEdge 1000 and 2000 routers only)</td>
<td>Click on to carve out a separate CPU core to use for performing TCP optimization.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:
```
system clock
timezone timezone
console-baud-rate rate controller-group-list numbers description text device-groups
host-name string location string max-omp-sessions number site-id site-id system-ip
ip-address tcp-optimization-enabled
```

To configure the DNS name or IP address of the vBond orchestrator in your overlay network, go to the Administration ➤ Settings screen and click vBond.

**Configure the GPS Location**

To configure a device's location, select the GPS tab and then configure the following parameters. This location is used to place the device on the vManage NMS network map. Setting the location also allows the vManage NMS to send a notification if the device is moved to another location.

**Table 104:**
<table>
<thead>
<tr>
<th>Parameter Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latitude</td>
<td>Enter the latitude of the device, in the format decimal-degrees.</td>
</tr>
<tr>
<td>Longitude</td>
<td>Enter the longitude of the device, in the format decimal-degrees.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:
```
system gps-location (latitude decimal-degrees | longitude decimal-degrees)
```
Configure Interface Trackers

To Track the status of transport interfaces that connect to the internet, click the Tracker tab. Then click Add New Tracker and configure the following parameters:

**Table 105:**

<table>
<thead>
<tr>
<th>Parameter Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.</td>
</tr>
<tr>
<td>Threshold</td>
<td>How long to wait for the probe to return a response before declaring that the transport interface is down. <em>Range:</em> 100 through 1000 milliseconds <em>Default:</em> 300 milliseconds</td>
</tr>
<tr>
<td>Interval</td>
<td>How often probes are sent to determine the status of the transport interface. <em>Range:</em> 10 through 600 seconds <em>Default:</em> 60 seconds (1 minute)</td>
</tr>
<tr>
<td>Multiplier</td>
<td>Number of times to resend probes before declaring that the transport interface is down. <em>Range:</em> 1 through 10 <em>Default:</em> 3</td>
</tr>
<tr>
<td>End Point Type: IP Address</td>
<td>IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address.</td>
</tr>
<tr>
<td>End Point Type: DNS Name</td>
<td>DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. For each tracker, you must configure either one DNS name or one IP address.</td>
</tr>
</tbody>
</table>

To save a tracker, click Add.

To save the feature template, click Save.

**CLI equivalent:**

```text
system tracker tracker-name
    endpoint-dns-name dns-name
    endpoint-ip ip-address
    interval seconds
    multiplier number
    threshold milliseconds
```

To apply a tracker to an interface, configure it in & the VPN Interface Cellular, VPN Interface Ethernet, VPN Interface NAT Pool, or VPN Interface PPP configuration template. You can apply only one tracker to an interface.

**Configure Advanced Options**

To configure additional system parameters, click the Advanced tab:
<table>
<thead>
<tr>
<th><strong>Parameter Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Session Policer Rate</strong></td>
<td>Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic. <em>Range:</em> 1 through 65535 pps <em>Default:</em> 300 pps</td>
</tr>
<tr>
<td><strong>MTU of DTLS Tunnel</strong></td>
<td>Specify the MTU size to use on the DTLS tunnels that send control traffic between Viptela devices. <em>Range:</em> 500 through 2000 bytes <em>Default:</em> 1024 bytes</td>
</tr>
<tr>
<td><strong>Port Hopping</strong></td>
<td>Click On to enable port hopping, or click Off to disable it. When a Viptela device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Viptela devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. <em>Default:</em> Enabled (on vEdge routers); disabled (on vManage NMSs and vSmart controllers)</td>
</tr>
<tr>
<td><strong>Port Offset</strong></td>
<td>Enter a number by which to offset the base port number. Configure this option when multiple Viptela devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. <em>Values:</em> 0 through 19</td>
</tr>
<tr>
<td><strong>DNS Cache Timeout</strong></td>
<td>Specify when to timeout the vBond orchestrator addresses that have been cached by the device. <em>Range:</em> 1 through 30 minutes <em>Default:</em> 30 minutes</td>
</tr>
<tr>
<td><strong>Track Transport</strong></td>
<td>Click On to regularly check whether the DTLS connection between the device and a vBond orchestrator is up. Click Off to disable checking. By default, transport checking is enabled</td>
</tr>
<tr>
<td><strong>Local vBond (only on vEdge routers acting as vBond orchestrators)</strong></td>
<td>Click On to configure the vEdge router to act as a vBond orchestrator. Then specify the DNS name for the vBond orchestrator or its IP address, in decimal four-part dotted notation.</td>
</tr>
<tr>
<td><strong>Track Interface (on vEdge routers only)</strong></td>
<td>Set the tag string to include in routes associated with a network that is connected to a non-operational interface. <em>Range:</em> 1 through 4294967295</td>
</tr>
<tr>
<td><strong>Multicast Buffer (on vEdge routers only)</strong></td>
<td>Specify the percentage of interface bandwidth that multicast traffic can use. <em>Range:</em> 5% through 100% <em>Default:</em> 20%</td>
</tr>
<tr>
<td><strong>USB Controller (on vEdge 1000 and 2000 series routers only)</strong></td>
<td>Click On to enable or click Off to disable the USB controller, which drives the external USB ports. If you enable the USB controller, the vEdge router reboots when you attach the device template to the device. <em>Default:</em> Disabled</td>
</tr>
<tr>
<td><strong>Gateway Tracking</strong></td>
<td>Click On to enable or click Off to Disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. <em>Default:</em> Enabled</td>
</tr>
<tr>
<td><strong>Host Policer Rate (on vEdge routers only)</strong></td>
<td>Specify the maximum rate at which a policer delivers packets to the control plane. <em>Range:</em> 1000 through 20000 pps <em>Default:</em> 5000 pps</td>
</tr>
</tbody>
</table>
### Parameter Name

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Error Rate (on vEdge routers only)</td>
<td>Specify how many ICMP error messages a policer can generate or receive. <strong>Range:</strong> 1 through 200 pps</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 100 pps</td>
</tr>
<tr>
<td>Allow Same-Site Tunnel (on vEdge routers only)</td>
<td>Click On to allow tunnels to be formed between vEdge routers in the same site. Note that no BFD sessions are established between the two collocated vEdge routers. <strong>Default:</strong> Off</td>
</tr>
<tr>
<td>Route Consistency Check (on vEdge routers only)</td>
<td>Click On to check whether the IPv4 routes in the device's route and forwarding table are consistent.</td>
</tr>
<tr>
<td>Collect Admin Tech on Reboot</td>
<td>Click On to collect admin-tech information when the device reboots.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. <strong>Range:</strong> 0 through 300 seconds <strong>Default:</strong> CLI session does not time out</td>
</tr>
<tr>
<td>Eco-Friendly Mode (on vEdge Cloud routers only)</td>
<td>Click On to configure a vEdge Cloud router not to use its CPU minimally or not at all when the router is not processing any packets.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```plaintext
system
    admin-tech-on-failure allow-same-site-tunnels {on vEdge routers only}
    control-session-pps rate eco-friendly-mode {on vEdge Cloud routers only}
    host-policer-pps rate {on vEdge routers only}
    icmp-error-pps rate {on vEdge routers only}
    idle-timeout seconds multicast-buffer-percent percentage {on vEdge routers only}
    port-hop port-offset number route-consistency-check {on vEdge routers only}
    system-tunnel-mtu bytes timer
    dns-cache-timeout minutes track-default-gateway
    track-interface-tag number {on vEdge routers only}
    track-transport upgrade-confirm minutes [no] usb-controller {vEdge 1000 and 2000 routers only}
    vbond (dns-name | ip-address) local {on vEdge routers acting as vBond controllers}
```

**Release Information**

Introduced in vManage NMS in Release 15.2. In Releases 15.3.8 and 15.4.3, add Track Interface field. In Release 17.1.0, add Route Consistency Check and Collect Admin Tech on Reboot fields. In Release 17.2.0, add support for CLI idle timeout and ecofriendly mode. In Release 17.2.2, add support for interface status tracking.

### T1/E1 Controller

Use the T1/E1 Controller template for Cisco IOS XE routers running the SD-WAN software.

To configure the T1/E1 interfaces in a VPN using vManage templates:

1. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters, as described in this article.
2. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters. See the VPN Interface T1/E1 help topic.

3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
   3. From the VPN Interface drop-down, click Create Template. The VPN Interface T1/E1 template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.

6. To create a template for VPNS 1 through 511, and 513 through 65530:
   1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
   2. Click the Service VPN drop-down.
   3. Under Additional VPN templates, located to the right of the screen, click VPN Interface.
   4. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 107:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.

When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.

To change the default key, type a new string and move the cursor out of the Enter Key box.

Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.

Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

Configure a T1 Controller

To configure a T1 controller, click the T1 radio button and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

Table 108:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Slot* | Enter the number of the slot in which the T1 NIM is installed.  
\textit{Range}: 0 through 6 |
| Framing* | Enter the T1 frame type:  
\begin{itemize}  
\item \textit{esf}—Send T1 frames as extended superframes. This is the default.  
\item \textit{sf}—Send T1 frames as superframes. Superframing is sometimes called D4 framing.  
\end{itemize} |
| Line Code | Select the line encoding to use to send T1 frames:  
\begin{itemize}  
\item \textit{ami}—Use alternate mark inversion (AMI) as the linecode. AMI signaling uses frames grouped into superframes.  
\item \textit{b8zs}—Use bipolar 8-zero substitution as the linecode. This is the default. B8ZS uses frames that are grouping into extended superframes.  
\end{itemize} |
### Parameter Name | Description
---|---
Clock Source | Select the clock source:
  - internal—Use the controller framer as the clock master.
  - line—Use phase-locked loop (PLL) on the interface. This is the default. When both T1 ports use line clocking and neither port is configured as the primary, by default, port 0 is the primary clock source and port 1 is the secondary clock source.
Line Mode | If you choose the Line clock source, select whether the line is a primary or a secondary line.
Description | Enter a description for the controller.
Channel Group | Enter the number of the channel group. If you do so, you must enter a timeslot in the Time Slot field. Range: 0 through 30
Time Slot | Enter the timeslot or timeslots that are part of the channel group. Range: 1 through 24
Cable Length | Select the cable length to configure the attenuation
  - long—Attenuate the pulse from the transmitter using pulse equalization and line buildout. You can configure a long cable length for cables longer that 660 feet.
  - short—Set the transmission attenuation for cables that are 660 feet or shorter.
  There is no default length.
Length | If you specify a value in the Cable Length Field, enter the length of the cable.
  For short cables, the length values can be:
  - 110—Length from 0 through 110 feet
  - 220—Length from 111 through 220 feet
  - 330—Length from 221 through 330 feet
  - 440—Length from 331 through 440 feet
  - 550—Length from 441 through 550 feet
  - 660—Length from 551 through 660 feet
  For long cables, the length values can be:
  - 0 dB
  - –7.5 dB
  - –15 dB
  - –22.5 dB

To save the feature template, click Save.
Configure an E1 Controller

To configure an E1 controller, click the E1 radio button and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

**Table 109:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Slot*          | Enter the number of the slot in which the E1 NIM is installed.  
*Range:* 0 through 6 |
| Framing*       | Enter the E1 frame type:  
• **crc4**—Use cyclic redundancy check 4 (CRC4). This is the default.  
• **no-crc4**—Do no use CRC4. |
| Line Code*     | Select the line encoding to use to send E1 frames:  
• **ami**—Use alternate mark inversion (AMI) as the linecode.  
• **hdb3**—Use high-density bipolar 3 as the linecode. This is the default. |
| Clock Source   | Select the clock source:  
• **internal**—Use the controller framer as the clock master.  
• **line**—Use phase-locked loop (PLL) on the interface. This is the default. |
| Line Mode      | If you choose the Line clock source, select whether the line is a primary or secondary line.  
If you configure both a primary and a secondary line, if the primary line fails, the PLL automatically switches to the secondary line. When the PLL on the primary line becomes active again, the PLL automatically switches back to the primary line. |
| Description    | Enter a description for the controller. |
| Channel Group  | To configure the serial WAN on the E1 interface, enter a channel group number. *Range:* 0 through 30 |
| Time Slot      | For a channel group, configure the timeslot. *Range:* 1 through 31 |

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS Release 18.1.1.

**VPN**

Use the VPN template for all Viptela devices and Cisco IOS XE routers running the SD-WAN software. To configure VPNs for network segmentation using vManage templates, follow this general workflow:
1. Create VPN feature templates to configure VPN parameters, as described in this topic. You create a separate VPN feature template for each VPN. For example, create one feature template for VPN 0, a second for VPN 1, and a third for VPN 512.

For vManage Network Management Systems and vSmart controllers, you can configure only VPNs 0 and 512. Create templates for these VPNs only if you want to modify the default settings for the VPN. For vEdge routers, you can create templates for these two VPNs and for additional VPN feature templates to segment service-side user networks.

- **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.

- **VPN 512**—*Management VPN*, which carries out-of-band network management traffic among the Viptela devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all vEdge routers except for vEdge 100. For controller devices, by default, VPN 512 is not configured.

- **VPNs 1–511, 513–65530**—*Service VPNs*, for service-side data traffic on vEdge routers.

2. Create interface feature templates to configure the interfaces in the VPN. See [VPN-Interface-Ethernet](#).

---

## Open and Name the Template

**Step 1**
In vManage NMS, select the Configuration ➤ Templates screen.

**Step 2**
In the Device tab, click **Create Template**.

**Step 3**
From the Create Template drop-down, select **From Feature Template**.

**Step 4**
From the **Device Model** drop-down, select the type of device for which you are creating the template.

**Step 5**
To create a template for VPN 0 or VPN 512:

1. Click the **Transport & Management** VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

2. From the VPN 0 or VPN 512 drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.

**Step 6**
To create a template for VPNs 1 through 511, and 513 through 65530:

1. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the Service VPN section.

2. Click the **Service VPN** drop-down.

3. From the VPN drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.
Step 7  
In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8  
In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

**Changing the Scope for a Parameter Value**

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (a 🔄), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄 Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>✌️ Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

## Configure Basic VPN Parameters

To configure basic VPN parameters, select the Basic Configuration tab and then configure the following parameters. Parameters marked with an asterisk are required to configure a VPN.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN*</td>
<td>Enter the numeric identifier of the VPN. Range for vEdge routers: 0 through 65530 Values for vSmart and vManage devices: 0, 512</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the VPN.</td>
</tr>
<tr>
<td>Enhance ECMP keying (vEdge routers only)</td>
<td>Click On to enable the use in the ECMP hash key of Layer 4 source and destination ports, in addition to the combination of the source IP address, destination IP address, protocol, and DSCP field, as the ECMP hash key. ECMP keying is Off by default.</td>
</tr>
</tbody>
</table>
Configure DNS and Static Hostname Mapping

To configure DNS addresses and static hostname mapping, select the DNS tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DNS Address</td>
<td>Select either IPv4 or IPv6, and enter the IP address of the primary DNS server in this VPN.</td>
<td></td>
</tr>
<tr>
<td>New DNS Address</td>
<td>Click <strong>New DNS Address</strong> and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address.</td>
<td></td>
</tr>
<tr>
<td>Mark as Optional Row</td>
<td>Check <strong>Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the hostname of the DNS server. The name can be up to 128 characters.</td>
<td></td>
</tr>
<tr>
<td>List of IP Addresses</td>
<td>Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.</td>
<td></td>
</tr>
</tbody>
</table>

To save the DNS server configuration, click **Add**.

To save the feature template, click **Save**.

**CLI Equivalent**

```bash
evpn vpn-id
dns ip-address {primary | secondary}
host hostname ip ip-address
```

Configure Route Advertisements to OMP

To configure route advertisements to OMP for this VPN, select the Advertise OMP tab and configure the parameters listed below. Route advertisements that you configure here apply to the specific VPN. If you configure route advertisements to OMP for both the VPN and the entire vEdge router (using the OMP feature template), both configurations are applied.
### Configure Route Advertisements to OMP

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 / IPv6</td>
<td>Click IPv4 or IPv6 to select the address type.</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>Click On to advertise BGP routes from this VPN to OMP.</td>
<td></td>
</tr>
<tr>
<td>Static</td>
<td>Click On to advertise static routes from this VPN to OMP.</td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>Click On to advertise connected routes from this VPN to OMP.</td>
<td></td>
</tr>
<tr>
<td>OSPF External (IPv4 only)</td>
<td>Click On to advertise OSPF routes from this VPN to OMP. By default OSPF interarea and intra-areas routes are advertised to OMP. Click On again to advertise external OSPF routes.</td>
<td></td>
</tr>
<tr>
<td>Network (IPv4)</td>
<td>Click the Network tab and click On to advertise a specific prefix to OMP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>New Network</strong></td>
<td><strong>Check Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
</tr>
<tr>
<td></td>
<td><strong>Prefix</strong></td>
<td>Enter the new IP prefix and click Add to add the prefix.</td>
</tr>
<tr>
<td>Aggregate (IPv4)</td>
<td>Click the Aggregate tab and click On to aggregate a prefix before advertising it to OMP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>New Aggregate</strong></td>
<td><strong>Check Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
</tr>
<tr>
<td></td>
<td><strong>Prefix</strong></td>
<td>Enter the new IP prefix and click Add to add the prefix.</td>
</tr>
<tr>
<td></td>
<td><strong>Aggregate Only</strong></td>
<td>Click On to advertise only the aggregated prefix, and click Add.</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

### CLI Equivalent

```
vpn vpn-id
  omp
    advertise (aggregate prefix [aggregate-only] | bgp | connected | network prefix | ospf type | static)
```
Configure Route Advertisements to OMP

To configure route advertisements to OMP for this VPN, select the Advertise OMP tab and configure the parameters listed below. Route advertisements that you configure here apply to the specific VPN. If you configure route advertisements to OMP for both the VPN and the entire vEdge router (using the OMP feature template), both configurations are applied.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 / IPv6</td>
<td>Click IPv4 or IPv6 to select the address type.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>Click On to advertise BGP routes from this VPN to OMP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static</td>
<td>Click On to advertise static routes from this VPN to OMP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td>Click On to advertise connected routes from this VPN to OMP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPF External</td>
<td>Click On to advertise OSPF routes from this VPN to OMP. By default OSPF interarea and intra-areas routes are advertised to OMP. Click On again to advertise external OSPF routes.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network (IPv4)

Click the Network tab and click On to advertise a specific prefix to OMP.

- **New Network**
  - **Mark as Optional Row**
  - **Prefix** Enter the new IP prefix and click Add to add the prefix.

Aggregate (IPv4)

Click the Aggregate tab and click On to aggregate a prefix before advertising it to OMP.

- **New Aggregate**
  - **Mark as Optional Row**
  - **Prefix** Enter the new IP prefix and click Add to add the prefix.
  - **Aggregate Only** Click On to advertise only the aggregated prefix, and click Add.

To save the feature template, click Save.
Configure NAT64 Address Pools

To use Stateful Network Address Translation 64 (NAT64) as a transition tool for IPv4 and IPv6 network addresses running on Cisco IOS XE routers running SD-WAN software, select the NAT tab. Then click New NAT64 v4 Pool and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT64 Pool name</td>
<td>Enter a name for the NAT64 pool. The string can be any combination of letters, numbers, spaces, and characters.</td>
</tr>
<tr>
<td>NAT64 v4 Pool Range Start</td>
<td>Enter a valid IPv4 address to designate the start of the NAT64 pool.</td>
</tr>
<tr>
<td>NAT64 v4 Pool Range End</td>
<td>Enter a valid IPv4 address to designate the end of the NAT64 pool.</td>
</tr>
<tr>
<td>NAT64 Overload</td>
<td>True - Enable overloading, allowing a device to use one global address for many local addresses. False - Disable overloading.</td>
</tr>
</tbody>
</table>

CLI Equivalent

```
nat64 v4 pool pool_name start_address end_address
nat64 v6v4 list global-list pool pool_name vrf vrf_no
```

Configure IPv4 and IPv6 Static Routes

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>More Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Optional Row</td>
<td>Check Mark as Optional Row</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter the address or prefix, in decimal four-point-dotted notation, and the prefix length of the static route to configure in the VPN.</td>
<td></td>
</tr>
</tbody>
</table>
### Configure IPv4 and IPv6 Static Routes

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>More Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>Select one of the following options to configure the next hop to reach the static route.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Hop</td>
<td>Configure next hops for the route. Click <strong>Add Next Hop</strong>. If you have no existing Next Hops, click <strong>Add Next Hop</strong> again.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Enter the IP address of the next-hop router to use to reach the static route.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance</td>
<td>Enter the administrative distance for the route. Default is 1.</td>
<td>1-255</td>
<td></td>
</tr>
<tr>
<td>Add Next Hop</td>
<td>Open another pair of Next Hop <strong>Address</strong> and <strong>Distance</strong> fields.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Click **Add** to add the Next Hops.

<table>
<thead>
<tr>
<th>Gateway (cont.)</th>
<th>Enable Null0</th>
<th>To enable the Null0 gateway (off by default), change the scope from default to <strong>global</strong>.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Click <strong>On</strong> to set the next hop to be the null interface. All packets sent to this interface are dropped without sending any ICMP messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distance</td>
<td>Enter the administrative distance for the route. Default is 1.</td>
<td>1-255</td>
</tr>
</tbody>
</table>

Click **Add** to add the null gateway.

<table>
<thead>
<tr>
<th>Gateway (cont.)</th>
<th>VPN</th>
<th>Configure a VPN gateway</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable VPN</td>
<td>To enable a VPN gateway (off by default), change the scope from default to <strong>global</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>On</strong> to direct packets to the transport VPN. If NAT is enabled on the WAN interface, the packets can be forwarded to an Internet destination or other destination outside of the overlay network, effectively converting the vEdge router into a local Internet exit point. You must also enable NAT on a transport interface in VPN 0.</td>
<td></td>
</tr>
</tbody>
</table>

Click **Add** to add the VPN gateway.

To save the configured static routes, click **Add**.

To save the feature template, click **Save**.

### CLI Equivalent (IPv4)

```text
vpn vpn-id
ip route ip-address/subnet next-hop-address [administrative-distance]
```
CLI Equivalent (IPv6)

```
vpn 0
ipv6 route ip-address/subnet next-hop-address [administrative-distance]
```

## Configure GRE-Specific Static Routes

To create a Generic Routing Encapsulation (GRE)-specific static route for a service VPN on a vEdge router, select the GRE Route tab. Then click **New GRE Route** and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Optional Row</td>
<td>Check <strong>Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See <a href="#">Create a Template Variables Spreadsheet</a>.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the GRE-specific static route.</td>
</tr>
<tr>
<td>VPN</td>
<td>Enter the number of the VPN to reach the service. This must be VPN 0.</td>
</tr>
<tr>
<td>GRE Interface</td>
<td>Enter the name of one or two GRE tunnels to use to reach the service.</td>
</tr>
</tbody>
</table>

To save a GRE-specific static route, click **Add**.

To save the feature template, click **Save**.

### CLI Equivalent

```
vpn vpn-id
ip gre-route prefix/length vpn 0 interface grenumber [grenumber2]
```

## Configure IPsec-Specific Static Routes

To configure IPsec-specific static routes in a service VPN (any VPN except VPN 0 and VPN 512 on a vEdge router), select the IPsec Route tab. Then click **Add New IPsec Route**, and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Optional Row</td>
<td>Check <strong>Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See <a href="#">Create a Template Variables Spreadsheet</a>.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.</td>
</tr>
<tr>
<td>VPN ID</td>
<td>Enter the number of the VPN to reach the IPsec tunnel. This must be VPN 0.</td>
</tr>
<tr>
<td>IPsec Interface</td>
<td>Enter the name of one or two IPsec tunnel interfaces. If you configure two interfaces, the first is the primary IPsec tunnel, and the second is the backup. All packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.</td>
</tr>
</tbody>
</table>

To save an IPsec-specific static route, click **Add**.

To save the feature template, click **Save**.
**Configure Services**

For VPNs other than VPN 0 and VPN 512 (service VPNs), you can configure services that are either present on the router's local network or available on a device at a remote site that is reachable through a Generic Routing Encapsulation (GRE) tunnel.

To configure a service in a VPN, select the Service tab. Then click **New Service**, and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Type</strong></td>
<td></td>
<td>Select the service available in the local VPN.</td>
</tr>
<tr>
<td>FW</td>
<td>Firewall service.</td>
<td></td>
</tr>
<tr>
<td>IDP</td>
<td>Intrusion detection and prevention service.</td>
<td></td>
</tr>
<tr>
<td>netsvc1, netsvc2, netsvc3, netsvc4</td>
<td>Net services 1 through 4.</td>
<td></td>
</tr>
<tr>
<td>TE</td>
<td>Traffic engineering service.</td>
<td></td>
</tr>
<tr>
<td><strong>IP Address or Interface</strong></td>
<td>Enter the location of the service.</td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter up to four IP addresses, separated by commas. The service is advertised to the vSmart controller only if one of the addresses can be resolved locally, at the local site, not via routes learned through OMP.</td>
<td></td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Enter one or two GRE interfaces. If you configure two, the first interface is the primary GRE tunnel, and the second is the backup tunnel.</td>
<td></td>
</tr>
</tbody>
</table>

To save the service configuration, click **Add**.

To save the feature template, click **Save**.

**CLI Equivalent**

```
vpn vpn-id
  ip ipsec-route prefix/length
vpn 0 interface ipsecnumber [ipsecnumber2]
```

---

**VPN Interface Bridge**

Use the VPN Interface Bridge template for all vEdge Cloud and vEdge router devices.

Integrated routing and bridging (IRB) allows vEdge routers in different bridge domains to communicate with each other. To enable IRB, create logical IRB interfaces to connect a bridge domain to a VPN. The VPN provides the Layer 3 routing services necessary so that traffic can be exchanged between different VLANs. Each bridge domain can have a single IRB interface and can connect to a single VPN, and a single VPN can connect to multiple bridge domains on a vEdge router.

To configure a bridge interface using vManage templates:
1. Create a VPN Interface Bridge feature template to configure parameters for logical IRB interfaces, as described in this article.

2. Create a Bridge feature template for each bridging domain, to configure the bridging domain parameters. See the Bridge help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface Bridge.

8. From the VPN Interface Bridge drop-down, click Create Template. The VPN Interface Bridge template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Bridge parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

Table 110:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Create a Bridging Interface

To configure an interface to use for bridging servers, select the Basic Configuration tab and click configure the following parameters. Parameters marked with an asterisk are required to configure bridging.

Table 111:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td>Interface name*</td>
<td>Enter the name of the interface, in the format irb number. The IRB interface number can be from 1 through 63, and must be the same as the VPN identifier configured in the Bridge feature template for the bridging domain that the IRB is connected to.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>Enter the IPv4 address of the router.</td>
</tr>
<tr>
<td>DHCP Helper</td>
<td>Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.</td>
</tr>
</tbody>
</table>
To save the template, click Save.

**CLI equivalent:**
```
vpn vpn-id interface irbnumber description "text description" dhcp-helper ip-addresses
ip address prefix/length mac-address mac-address mtu bytes secondary-address ipv4-address
[no] shutdown tcp-mss-adjust bytes
```

### Apply Access Lists

To apply access lists to IRB interfaces, select the ACL tab and configure the following parameters:

**Table 112:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of an IPv4 access list to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of an IPv4 access list to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**
```
vpn vpn-id interface irbnumber access-list acl-name (in | out)
```

### Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

**Table 113:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter the priority level of the router. There router with the highest priority is elected as master. If two vEdge routers have the same priority, the one with the higher IP address is elected as master. Range: 1 through 254 Default: 100</td>
</tr>
</tbody>
</table>
**Parameter Name** | **Description**
---|---
Timer | Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. *Range*: 1 through 3600 seconds. *Default*: 1 second.

**Track OMP | Track Prefix List** | By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which vEdge router is the master virtual router. If a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:

Track OMP—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the master VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.

Track Prefix List—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the master VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.

**IP Address** | Enter the IP address of the virtual router. This address must be different from the configured interface IP addresses of both the local vEdge router and the peer running VRRP.

To save the VRRP configuration, click Add.

To save the feature template, click Save.

**CLI equivalent:**
```plaintext
vpn vpn-id
interface irbnumber\.subinterface
  vrrp group-number
  ipv4 ip-address
  priority number
  timer seconds
  (track-omp | track-prefix-list list-name)
```

**Add ARP Table Entries**
To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

**Table 114:**
<table>
<thead>
<tr>
<th><strong>Parameter Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address in colon-separated hexadecimal notation.</td>
</tr>
</tbody>
</table>
To save the ARP configuration, click Add.
To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id interface irbnumber arp
    ip address ip-address mac mac-address
```

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

**Table 115:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. <em>Range:</em> 576 through 1804. <em>Default:</em> 1500 bytes</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range:</em> 552 to 1460 bytes. <em>Default:</em> None</td>
</tr>
<tr>
<td>Clear-Dont-Fragment</td>
<td>Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>ARP Timeout</td>
<td>Specify how long it takes for a dynamically learned ARP entry to time out. <em>Range:</em> 0 through 2678400 seconds (744 hours). <em>Default:</em> 1200 seconds (20 minutes)</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id interface irbnumber arp-timeout seconds clear-dont-fragment
icmp-redirect-disable mac-address mac-address mtu bytes tcp-mss-adjust bytes
```

### Release Information

Introduced in vManage NMS in Release 15.3. In Release 18.2, add support for disabling ICMP redirect messages.

### VPN Interface Cellular

Use the VPN Interface Cellular feature template to configure cellular module parameters on vEdge routers and Cisco IOS XE routers running the SD-WAN software.
To configure cellular interfaces using vManage templates:

1. Create a VPN Interface Cellular feature template to configure cellular module parameters, as described in this article.
2. Create a Cellular Profile template to configure the profiles used by the cellular modem. See the Cellular Profile help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

**Navigate to the Template Screen**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Cellular.
7. From the VPN Interface Cellular drop-down, click Create Template. The VPN Interface Cellular template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Cellular parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 116:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure Basic Cellular Interface Functionality

To configure basic cellular interface functionality, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface. You must also configure a tunnel interface for the cellular interface.

Table 117:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td>Technology</td>
<td>Cellular technology. The default is lte. Other values are auto and cdma. For ZTP to work, the technology must be auto.</td>
</tr>
<tr>
<td>Interface Name*</td>
<td>Enter the name of the interface. It must be cellular0.</td>
</tr>
<tr>
<td>Profile ID*</td>
<td>Enter the identification number of the cellular profile. This is the profile identifier that you configure in the Cellular-Profile template. Range: 1 through 15</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the cellular interface.</td>
</tr>
<tr>
<td>IPv4 Configuration</td>
<td>To configure a static address, click Static and enter an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.</td>
</tr>
</tbody>
</table>
Table 118:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Configuration</td>
<td>To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.</td>
</tr>
<tr>
<td>DHCP Helper</td>
<td>Enter up to four IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.</td>
</tr>
<tr>
<td>Block Non-Source IP</td>
<td>Click Yes to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.</td>
</tr>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through ((2^{32} / 2) – 1) kbps</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. Range: 1 through ((2^{32} / 2) – 1) kbps</td>
</tr>
<tr>
<td>IP MTU*</td>
<td>Enter 1428 to set the MTU size, in bytes. This value must be 1428. You cannot use a different value.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**
```bash
vpn 0
  interface cellular0
    bandwidth-downstream kbps bandwidth-upstream kbps block-non-source-ip ( ip address ip-address/length | ip dhcp-client [dhcp-distance number]) ( ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] {dhcp-rapid-commit})
  mtu 1428
  profile number
  no shutdown
```

**Create a Tunnel Interface**

To configure an interface in VPN 0 to be a WAN transport connection, you must configure a tunnel interface on the cellular interface. The tunnel, which provides security from attacks, is used to send the phone number. At a minimum, select On and select a color for the interface, as described in the previous section. You can generally accept the system defaults for the remainder of the tunnel interface settings.

To configure a tunnel interface, select the Tunnel tab and configure the following parameters. Parameters marked with an asterisk are required to configure a cellular interface.

Table 119:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface*</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Color*</td>
<td>Select a color for the TLOC. The color typically used for cellular interface tunnels is <strong>lte</strong>.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>The default is On, which establishes a control connection for the TLOC. If the router has multiple TLOCs, click No to have a tunnel not establish a TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Set the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2</td>
</tr>
<tr>
<td>vBond As STUN Server</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Control Group List</td>
<td>Set the identifiers of one or more vSmart controller groups that this tunnel is not allowed to establish control connections with. Range: 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Set the preference for using the tunnel to exchange control traffic with the vManage NMS. Range: 0 through 9 Default: 5</td>
</tr>
<tr>
<td>Low-Bandwidth Link</td>
<td>Click On to set the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>Click On or Off for each service to allow or disallow the service on the cellular interface.</td>
</tr>
</tbody>
</table>

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

*Table 119:*

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec Preference</td>
<td>Enter a value to set the preference for directing traffic to the tunnel. A higher value is preferred over a lower value. Range: 0 through 4294967295 Default: 0</td>
</tr>
<tr>
<td>IPsec Weight</td>
<td>Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. Range: 1 through 255 Default: 1</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
--- | ---
Carrier | Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default. Default: default

**Bind Loopback Tunnel** | Enter the name of a physical interface to bind to a loopback interface. The interface name has the format ge slot/port.

**Last-Resort Circuit** | Use the tunnel interface as the circuit of last resort.

**NAT Refresh Interval** | Set the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds. Default: 5 seconds

**Hello Interval** | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds. Default: 1000 milliseconds (1 second)

**Hello Tolerance** | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds. Default: 12 seconds

To save the feature template, click Save.

**CLI equivalent:**

```bash
vpn 0
   interface cellular0
      tunnel-interface allow-service service-name
      bind interface-name carrier carrier-name
      color color encapsulation (gre | ipsec)
      preference number
      weight number exclude-controller-group-list number hello-interval milliseconds
      hello-tolerance seconds hold-time milliseconds low-bandwidth-link
      max-control-connections number last-resort-circuit nat-refresh-interval seconds
      vbond-as-stun-server vmanage-connection-preference number
```

### Configure the Cellular Interface as a NAT Device

To configure a cellular interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

**Table 120:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Click On to have the interface act as a NAT device.</td>
</tr>
<tr>
<td>Refresh Mode</td>
<td>Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound</td>
</tr>
<tr>
<td>UDP Timeout</td>
<td>Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes. Default: 1 minutes</td>
</tr>
</tbody>
</table>
TCP Timeout | Specify when NAT translations over TCP sessions timeout. *Range*: 1 through 65536 minutes. *Default*: 60 minutes (1 hour)
---|---
Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. *Default*: Off
Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

**Table 121:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Start Range</td>
<td>Enter a port number to define the port or first port in the range of interest. <em>Range</em>: 0 through 65535</td>
</tr>
<tr>
<td>Port End Range</td>
<td>Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. <em>Range</em>: 0 through 65535</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.</td>
</tr>
<tr>
<td>VPN</td>
<td>Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. <em>Range</em>: 0 through 65530</td>
</tr>
<tr>
<td>Private IP</td>
<td>Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.</td>
</tr>
</tbody>
</table>

To save a port forwarding rule, click Add.

To save the feature template, click Save.

**CLI equivalent:**

```
vpn 0
interface cellular0
    nat block-icmp-error port-forward port-start port-number1 port-end port-number2 proto (tcp | udp) private-ip-address ip address private-vpn vpn-id refresh (bi-directional | outbound)
    respond-to-ping tcp-timeout minutes udp-timeout minutes
```

**Apply Access Lists**

To configure a shaping rate to a cellular interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL/QoS tab and configure the following parameters:
Table 122:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of an IPv4 access list to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of an IPv4 access list to packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of an IPv6 access list to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of an IPv6 access list to packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```
vpn 0
interface cellular0
  access-list acl-name (in | out)
  ipv6 access-list acl-name (in | out)
  policer policer-name (in | out)
  qos-map name rewrite-rule name shaping-rate name
```

### Add ARP Table Entries

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

Table 123:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address in colon-separated hexadecimal notation.</td>
</tr>
</tbody>
</table>

To save the ARP configuration, click Add.
To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id interface irbnumber arp
    ip address ip-address mac mac-address
```

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters.

*Table 124:*

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMTU Discovery</td>
<td>Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range: 552 to 1460 bytes</em></td>
</tr>
<tr>
<td>Clear-Dont-Fragment</td>
<td>Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>Static Ingress QoS</td>
<td>Select a queue number to use for incoming traffic. <em>Range: 0 through 7</em></td>
</tr>
<tr>
<td>ARP Timeout</td>
<td>Specify how long it takes for a dynamically learned ARP entry to time out. <em>Range: 0 through 2678400 seconds (744 hours)</em> <em>Default: 1200 seconds (20 minutes)</em></td>
</tr>
<tr>
<td>Autonegotiate</td>
<td>Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Tracker</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

*CLI equivalent:*

```
vpn 0
    interface cellular0
    arp-timeout seconds
    [no] autonegotiate clear-dont-fragment icmp-redirect-disable mtu 1428
    pmitu static-ingress-qos number tcp-mss-adjust bytes
```
Release Information

VPN Interface DSL IPoE

Use the IPoE template for Cisco IOS XE routers.
You configure IPoE on routers with DSL interfaces, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:
1. Create a VPN Interface DSL IPoE feature template to configure IP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Screen and Name the Template
1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select "From Feature Template."
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL IPoE.
7. From the VPN Interface DSL IPoE drop-down, click Create Template. The VPN Interface DSL IPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining IPoE Interface parameters.
8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 125:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure IPoE Functionality

To configure basic IPoE functionality, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

Table 126:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the VDSL controller interface.</td>
</tr>
<tr>
<td>Controller VDSL Slot*</td>
<td>Enter the slot number of the controller VDSL interface, in the format slot/subslot/port (for example, 0/2/0).</td>
</tr>
</tbody>
</table>
Select the operating mode of the VDSL controller from the drop-down:

- **Auto**—Default mode.
- **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.
- **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.
- **ADSL2+**—Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.
- **ANSI**—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.
- **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.

Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed.

**VDSL Modem Configuration**

**SRA**

Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

To save the feature template, click Save.

**Configure the Ethernet Interface**

To configure an Ethernet interface on the VDSL controller, select the Ethernet tab and configure the following parameters. You must configure all parameters.

**Table 127:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Interface Name</td>
<td>Enter a name for the Ethernet interface, in the format subslot/port (for example 2/0). You do not need to enter the slot number, because it must always be 0.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Enter the VLAN identifier of the Ethernet interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>Dynamic/Static</td>
<td>Assign a dynamic or static IPv4 address to the Ethernet interface.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>Enter the static IPv4 address of the Ethernet interface.</td>
</tr>
</tbody>
</table>
To save the feature template, click Save.

### Create a Tunnel Interface

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

**Table 128:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.</td>
</tr>
<tr>
<td></td>
<td><em>Range</em>: 0 through 8  <em>Default</em>: 2</td>
</tr>
<tr>
<td>vBond As STUN Server</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Controller Group List</td>
<td>Set the vSmart controllers that the tunnel interface is not allowed to connect to. <em>Range</em>: 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS. <em>Range</em>: 0 through 8  <em>Default</em>: 5</td>
</tr>
<tr>
<td>Port Hop</td>
<td>Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. <em>Default</em>: Enabled</td>
</tr>
</tbody>
</table>
To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low-Bandwidth Link</td>
<td>Select to characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>Select On or Off for each service to allow or disallow the service on the interface.</td>
</tr>
</tbody>
</table>

**Table 129:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec Preference</td>
<td>Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295 Default: 0</td>
</tr>
<tr>
<td>IPsec Weight</td>
<td>Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255 Default: 1</td>
</tr>
<tr>
<td>Carrier</td>
<td>Select the carrier name or private network identifier to associate with the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default</td>
</tr>
<tr>
<td>Bind Loopback Tunnel</td>
<td>Enter the name of a physical interface to bind to a loopback interface.</td>
</tr>
<tr>
<td>Last-Resort Circuit</td>
<td>Select to use the tunnel interface as the circuit of last resort.</td>
</tr>
<tr>
<td>NAT Refresh Interval</td>
<td>Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)</td>
</tr>
<tr>
<td>Hello Tolerance</td>
<td>Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds</td>
</tr>
</tbody>
</table>
Configure the Interface as a NAT Device

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Click On to have the interface act as a NAT device.</td>
</tr>
<tr>
<td>Refresh Mode</td>
<td>Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). <em>Default: Outbound</em></td>
</tr>
<tr>
<td>UDP Timeout</td>
<td>Specify when NAT translations over UDP sessions time out. <em>Range: 1 through 65536 minutes Default: 1 minutes</em></td>
</tr>
<tr>
<td>TCP Timeout</td>
<td>Specify when NAT translations over TCP sessions time out. <em>Range: 1 through 65536 minutes Default: 60 minutes (1 hour)</em></td>
</tr>
<tr>
<td>Block ICMP</td>
<td>Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. <em>Default: Off</em></td>
</tr>
<tr>
<td>Respond to Ping</td>
<td>Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.</td>
</tr>
</tbody>
</table>

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a port number to define the port or first port in the range of interest. <em>Range: 0 through 65535</em></td>
</tr>
<tr>
<td>Port End Range</td>
<td>Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. <em>Range: 0 through 65535</em></td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.</td>
</tr>
<tr>
<td>VPN</td>
<td>Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. <em>Range: 0 through 65530</em></td>
</tr>
<tr>
<td>Private IP</td>
<td>Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.</td>
</tr>
</tbody>
</table>

To save a port forwarding rule, click Add.
To save the feature template, click Save.
Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

Table 132:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policier</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policier</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 133:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. Range: 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. Range: 576 through 1804. Default: 1500 bytes</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range: 552 to 1460 bytes Default: None</em></td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Tracker</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
<tr>
<td>IP Directed-Broadcast</td>
<td>Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS in Release 18.4.1.

**VPN Interface DSL PPPoA**

Use the VPN Interface DSL PPPoA template for Cisco IOS XE routers.

You configure PPP-over-ATM interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface DSL PPPoA feature template to configure ATM interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ▶ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoA.

7. From the VPN Interface DSL PPPoA drop-down, click Create Template. The VPN Interface DSL PPPoA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.  
When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.  
To change the default key, type a new string and move the cursor out of the Enter Key box.  
Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.  
Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

**Configure VDSL Controller Functionality**

To configure basic VDSL controller functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the VDSL controller interface.</td>
</tr>
<tr>
<td>Controller VDSL Slot*</td>
<td>Enter the slot number of the controller VDSL interface, in the format slot/subslot/port (for example, 0/2/0).</td>
</tr>
</tbody>
</table>
**Mode***
Select the operating mode of the VDSL controller from the drop-down:
• Auto—Default mode.
• ADSL1—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.
• ADSL2—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.
• ADSL2+—Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.
• ANSI—Operate in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.
• VDSL2—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.

**VDSL Modem Configuration**
Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed.

**SRA**
Enabled by default. Click No to disable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

To save the feature template, click Save.

**Configure the ATM Interface**
To configure an ATM interface on the VDSL controller, select the ATM tab and configure the following parameters. You must configure all parameters.

**Table 136:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM Interface Name</td>
<td>Enter a name for the ATM interface, in the format subslot/port (for example 2/0). You do not need to enter the slot number, because it must always be 0.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>VPI and VCI</td>
<td>Create an ATM permanent virtual circuit (PVC), in the format vpi/vci. Enter values for the virtual path identifier (VPI) and the virtual channel identifier (VCI).</td>
</tr>
</tbody>
</table>
### Encapsulation
Select the ATM adaptation layer (AAL) and encapsulation type to use on the ATM PVC from the drop-down:
- **AAL5 MUX**—Dedicate the PVC to a single protocol.
- **AAL5 NLPID**—Use NLPID multiplexing.
- **AAL5 SNAP**—Multiplex two or more protocols on the same PVC.

### Dialer Pool Member
Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.

### VBR-NRT
Configure variable bit rate non-real-time parameters:
- **Peak Cell Rate**—Enter a value from 48 through 25000 Kbps.
- **Sustainable Cell Rate**—Enter the sustainable cell rate, in Kbps.
- **Maximum Burst Size**—This size can be 1 cell.

### VBR-RT
Configure variable bit rate real-time parameters:
- **Peak Cell Rate**—Enter a value from 48 through 25000 Kbps.
- **Average Cell Rate**—Enter the average cell rate, in Kpbs.
- **Maximum Burst Size**—This size can be 1 cell.

To save the feature template, click Save.

### Configure the PPP Authentication Protocol
To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

**Table 137:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authentication Protocol | Select the authentication protocol used by the MLP:  
  - **CHAP**—Enter the hostname and password provided by your Internet Service Provider (ISP). *hostname* can be up to 255 characters.  
  - **PAP**—Enter the username and password provided by your ISP. *username* can be up to 255 characters.  
  - **PAP and CHAP**—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP. |

To save the feature template, click Save.
Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

**Table 138:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the vEdge router has multiple TLOCs, click No to have the tunnel not</td>
</tr>
<tr>
<td></td>
<td>establish a TLOC. The default is On, which establishes a control connection</td>
</tr>
<tr>
<td></td>
<td>for the TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Specify the maximum number of vSmart controllers that the WAN tunnel</td>
</tr>
<tr>
<td></td>
<td>interface can connect to. To have the tunnel establish no control connections,</td>
</tr>
<tr>
<td></td>
<td>set the number to 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Range:</strong> 0 through 8 <strong>Default:</strong> 2</td>
</tr>
<tr>
<td>vBond As STUN Server</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the</td>
</tr>
<tr>
<td></td>
<td>tunnel interface to discover its public IP address and port number when the</td>
</tr>
<tr>
<td></td>
<td>vEdge router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Controller Group List</td>
<td>Set the vSmart controllers that the tunnel interface is not allowed to</td>
</tr>
<tr>
<td></td>
<td>connect to. <strong>Range:</strong> 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Set the preference for using a tunnel interface to exchange control traffic</td>
</tr>
<tr>
<td></td>
<td>with the vManage NMS. <strong>Range:</strong> 0 through 8 <strong>Default:</strong> 5</td>
</tr>
<tr>
<td>Port Hop</td>
<td>Click On to enable port hopping, or click Off to disable it. When a router</td>
</tr>
<tr>
<td></td>
<td>is behind a NAT, port hopping rotates through a pool of preselected OMP port</td>
</tr>
<tr>
<td></td>
<td>numbers (called base ports) to establish DTLS connections with other routers</td>
</tr>
<tr>
<td></td>
<td>when a connection attempt is unsuccessful. The default base ports are 12346,</td>
</tr>
<tr>
<td></td>
<td>12366, 12386, 12406, and 12426. To modify the base ports, set a port offset</td>
</tr>
<tr>
<td></td>
<td>value. <strong>Default:</strong> Enabled</td>
</tr>
<tr>
<td>Low-Bandwidth Link</td>
<td>Select to characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>Select On or Off for each service to allow or disallow the service on the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
</tbody>
</table>

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:
### Table 139:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
</tbody>
</table>
| IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.  
*Range*: 0 through 4294967295  
*Default*: 0 |
| IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.  
*Range*: 1 through 255  
*Default*: 1 |
| Carrier | Select the carrier name or private network identifier to associate with the tunnel.  
*Values*: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default  
*Default*: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface. |
| Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort. |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.  
*Range*: 1 through 60 seconds  
*Default*: 5 seconds |
| Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.  
*Range*: 100 through 10000 milliseconds  
*Default*: 1000 milliseconds (1 second) |
| Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.  
*Range*: 12 through 60 seconds  
*Default*: 12 seconds |

### Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:
Table 140:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 141:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMTU Discovery</td>
<td>Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None</td>
</tr>
<tr>
<td>Clear Dont Fragment</td>
<td>Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>Static Ingress QoS</td>
<td>Select a queue number to use for incoming traffic. Range: 0 through 7</td>
</tr>
<tr>
<td>Autonegotiate</td>
<td>Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS in Release 18.3.

**VPN Interface DSL PPPoE**

Use the VPN Interface DSL PPPoE template for Cisco IOS XE routers.

You configure PPP-over-Ethernet interfaces on routers with DSL NIM modules, to provide support for service provider digital subscriber line (DSL) functionality.

To configure DSL interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface DSL PPPoE feature template to configure PPP-over-Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface DSL PPPoE.
7. From the VPN Interface DSL PPPoE drop-down, click Create Template. The VPN Interface DSL PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining PPPoE Interface parameters.
8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 142:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure VDSL Controller Functionality

To configure basic VDSL controller functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

Table 143:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the VDSL controller interface.</td>
</tr>
<tr>
<td>Controller VDSL Slot*</td>
<td>Enter the slot number of the controller VDSL interface, in the format slot/subslot/port (for example, 0/2/0).</td>
</tr>
</tbody>
</table>
Select the operating mode of the VDSL controller from the drop-down:

- **Auto**—Default mode.
- **ADSL1**—Use ITU G.992.1 Annex A full-rate mode, which provides a downstream rate of 1.3 Mbps and an upstream rate of 1.8 Mbps.
- **ADSL2**—Use ITU G.992.3 Annex A, Annex L, and Annex M, which provides a downstream rate of 12 Mbps and an upstream rate of 1.3 Mbps.
- **ADSL2+**—Use ITU G.992.5 Annex A and Annex M, which provides a downstream rate of 24 Mbps and an upstream rate of 3.3 Mbps.
- **ANSI**—Operating in ADSL2/2+ mode, as defined in ITU G.991.1, G.992.3, and G992.5, Annex A and Annex M, and in VDSL2 mode, as defined in ITU-T G993.2.
- **VDSL2**—Operate in VDSL2 mode, as defined in ITU-T G.993.2, which uses frequencies of up to 30 MHz to provide a downstream rate of 200 Mbps and an upstream rate of 100 Mbps.

Enter a command to send to the DSL modem in the NIM module. If the command is valid, it is executed and the results are returned to the vManage NMS. If the command is not valid, it is not executed.

Click Yes to enable seamless rate adaptation on the interface. SRA adjusts the line rate based on current line conditions.

Configure the Ethernet Interface

To configure an Ethernet interface on the VDSL controller, select the Ethernet tab and configure the following parameters. You must configure all parameters.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Interface Name</td>
<td>Enter a name for the Ethernet interface, in the format subslot/port (for example 2/0). You do not need to enter the slot number, because it must always be 0.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Enter the VLAN identifier of the Ethernet interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>Dialer Pool Member</td>
<td>Enter the number of the dialer pool to which the interface belongs. It can be a value from 1 through 255.</td>
</tr>
<tr>
<td>PPP Max Payload</td>
<td>Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation. Range: 64 through 1792 bytes</td>
</tr>
</tbody>
</table>
**Configure the IP prefix of the dialer interface.** This prefix is that of the node in the destination that the interface calls.

- **Negotiated**—Use the address that is obtained during IPCP negotiation.

To save the feature template, click Save.

### Configure the PPP Authentication Protocol

To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

**Table 145:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Select the authentication protocol used by the MLP:</td>
</tr>
<tr>
<td>Protocol</td>
<td>CHAP—Enter the hostname and password provided by your Internet Service</td>
</tr>
<tr>
<td></td>
<td>Provider (ISP). <em>hostname</em> can be up to 255 characters.</td>
</tr>
<tr>
<td></td>
<td>PAP—Enter the username and password provided by your ISP. <em>username</em> can</td>
</tr>
<tr>
<td></td>
<td>be up to 255 characters.</td>
</tr>
<tr>
<td></td>
<td>PAP and CHAP—Configure both authentication protocols. Enter the login</td>
</tr>
<tr>
<td></td>
<td>credentials for each protocol. To use the same username and password for</td>
</tr>
<tr>
<td></td>
<td>both, click Same Credentials for PAP and CHAP.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

### Create a Tunnel Interface

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

**Table 146:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
</tbody>
</table>
To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

**Table 147:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec Preference</td>
<td>Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. <em>Range: 0 through 4294967295</em> <em>Default: 0</em></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IPsec Weight         | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.  
  Range: 1 through 255  
  Default: 1            |
| Carrier              | Select the carrier name or private network identifier to associate with the tunnel.  
  Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default  
  Default: default      |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface.      |
| Last-Resort Circuit  | Select to use the tunnel interface as the circuit of last resort.            |
| NAT Refresh Interval  | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.  
  Range: 1 through 60 seconds  
  Default: 5 seconds       |
| Hello Interval       | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.  
  Range: 100 through 10000 milliseconds  
  Default: 1000 milliseconds (1 second) |
| Hello Tolerance      | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.  
  Range: 12 through 60 seconds  
  Default: 12 seconds       |

**Configure the Interface as a NAT Device**

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

**Table 148:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Click On to have the interface act as a NAT device.</td>
</tr>
</tbody>
</table>
| Refresh Mode   | Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).  
  Default: Outbound |
| UDP Timeout    | Specify when NAT translations over UDP sessions time out.  
  Range: 1 through 65536 minutes  
  Default: 1 minutes            |
| TCP Timeout    | Specify when NAT translations over TCP sessions time out.  
  Range: 1 through 65536 minutes  
  Default: 60 minutes (1 hour)  |
| Block ICMP      | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages.  
  Default: Off                 |
| Respond to Ping| Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection. |
To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

**Table 149:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Start Range</td>
<td>Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535</td>
</tr>
<tr>
<td>Port End Range</td>
<td>Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.</td>
</tr>
<tr>
<td>VPN</td>
<td>Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65530</td>
</tr>
<tr>
<td>Private IP</td>
<td>Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.</td>
</tr>
</tbody>
</table>

To save a port forwarding rule, click Add.

To save the feature template, click Save.

**Apply Access Lists**

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

**Table 150:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>
Click On, and specify the name of the policer to apply to packets being received on the interface.

Click On, and specify the name of the policer to apply to packets being transmitted on the interface.

To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:

*Table 151:*

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. <em>Range:</em> 576 through 1804 <em>Default:</em> 1500 bytes</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range:</em> 552 to 1460 bytes <em>Default:</em> None</td>
</tr>
<tr>
<td>Clear Dont Fragment</td>
<td>Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Tracker</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS in Release 18.3.
VPN Interface Ethernet

Use the VPN Interface Ethernet template for all Viptela devices and Cisco IOS XE routers running the SD-WAN software.

To configure the Ethernet interfaces in a VPN using vManage templates:

1. Create a VPN Interface Ethernet feature template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See VPN.
3. Optionally, to enable DHCP server functionality on a vEdge router interface, create a DHCP Server feature template.

Open and Name the Template

**Step 1**
In vManage NMS, select the Configuration ► Templates screen.

**Step 2**
In the Device tab, click Create Template.

**Step 3**
From the Create Template drop-down, select From Feature Template.

**Step 4**
From the Device Model drop-down, select the type of device for which you are creating the template.

**Step 5**
To create a template for VPN 0 or VPN 512:

1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
3. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form displays The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.

**Step 6**
To create a template for VPNS 1 through 511, and 513 through 65530:

1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
2. Click the Service VPN drop-down.
3. Under Additional VPN templates, located to the right of the screen, click VPN Interface.
4. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.
Step 7  In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8  In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Changing the Scope for a Parameter Value

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (a ✔), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
</tbody>
</table>

Once you have created and named the template, enter the following values. Parameters marked with an asterisk are required.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Note: Parameters marked with an asterisk are required to configure an interface.
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>IPv4 or IPv6</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| Interface name*      |              |         | Enter a name for the interface. For IOS XE routers, you must:  
|                      |              |         | • Spell out the interface names completely (for example, GigabitEthernet0/0/0).  
|                      |              |         | • Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured. |
| Description          |              |         | Enter a description for the interface. |
| IPv4 / IPv6          |              |         | Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface. |
| Dynamic              |              |         | Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server. |
| DHCP Distance        | Both         |         | Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1. |
| DHCP Rapid Commit    | IPv6         |         | Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments.  
|                      |              |         | Click **On** to enable DHCP rapid commit  
|                      |              |         | Click **Off** to continue using the regular commit process. |
| Static               |              |         | Click **Static** to enter an IP address that doesn't change. |
| IPv4 Address         | IPv4         |         | Enter a static IPv4 address. |
| IPv6 Address         | IPv6         |         | Enter a static IPv6 address. |
| Secondary IP Address | IPv4         |         | Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface. |
| IPv6 Address         | IPv6         |         | Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface. |
| DHCP Helper          | Both         |         | To designate the interface as a DHCP helper on a vEdge router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers. |
| Block Non-Source IP  | Yes / No     |         | Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic. |
| Bandwidth Upstream   |              |         | For vEdge routers and vManage NMSs:  
|                      |              |         | For transmitted traffic, set the bandwidth above which to generate notifications.  
|                      |              |         | Range: 1 through (232 / 2) – 1 kbps |
Create a Tunnel Interface

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs. On vSmart controllers and vManage NMSs, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>vEdge Routers Only</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>No</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>No</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>Yes</td>
<td>If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Yes</td>
<td>Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>vEdge Routers Only</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vBond As Stun Server</td>
<td>Yes</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Controller Group List</td>
<td>Yes</td>
<td>Set the vSmart controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Yes</td>
<td>Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS. Range: 0 through 8 Default: 5</td>
</tr>
<tr>
<td>Port Hop</td>
<td>No</td>
<td>Click On to enable port hopping, or click Off to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template. vEdge router default: Enabled vManage NMS and vSmart controller default: Disabled</td>
</tr>
<tr>
<td>Low-Bandwidth Link</td>
<td>Yes</td>
<td>Select to characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>No</td>
<td>Select On or Off for each service to allow or disallow the service on the interface.</td>
</tr>
</tbody>
</table>

To configure additional tunnel interface parameters, click Advanced Options:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>vEdge Routers Only</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Yes</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Yes</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>vEdge Routers Only</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPsec Preference</td>
<td>Yes</td>
<td>Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>IPsec Weight</td>
<td>Yes</td>
<td>Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 through 255</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1</td>
</tr>
<tr>
<td>Carrier</td>
<td>No</td>
<td>Select the carrier name or private network identifier to associate with the tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: default</td>
</tr>
<tr>
<td>Bind Loopback</td>
<td>Yes</td>
<td>Enter the name of a physical interface to bind to a loopback interface.</td>
</tr>
<tr>
<td>Tunnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last-Resort Circuit (on vEdge routers)</td>
<td>Yes</td>
<td>Select to use the tunnel interface as the circuit of last resort.</td>
</tr>
<tr>
<td>NAT Refresh</td>
<td>No</td>
<td>Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
<td>Range: 1 through 60 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 5 seconds</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>No</td>
<td>Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 100 through 10000 milliseconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1000 milliseconds (1 second)</td>
</tr>
<tr>
<td>Hello Tolerance</td>
<td>No</td>
<td>Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 12 through 60 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 12 seconds</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**CLI Equivalent**

```
vpn 0
  interface interface-name
    tunnel-interface
    allow-service service-name
```
Configure an Interface as a NAT Device

You can configure IPv4 and IPv6 interfaces to act as a network address translation (NAT) device for applications such as port forwarding. To configure a NAT device:

1. Click the NAT tab, and select either **IPv4** or **IPv6**.
2. Change the scope from Default (blue check) to **Global** (green globe).
3. Click **On** to enable NAT (IPv4) or NAT64 (IPv6). The correct set of parameters will display.
4. Enter the following parameter values:

### IPv4 NAT

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Mode</td>
<td>Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound</td>
</tr>
<tr>
<td>Log NAT flow creations or deletions</td>
<td>Enable logging when NAT flows are created or deleted. Default: Off</td>
</tr>
<tr>
<td>UDP Timeout</td>
<td>Specify when NAT translations over UDP sessions time out.</td>
</tr>
<tr>
<td>TCP Timeout</td>
<td>Specify when NAT translations over TCP sessions time out.</td>
</tr>
</tbody>
</table>

**Parameter Name**  
**Description**  
Refresh Mode  
Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). Default: Outbound  
Log NAT flow creations or deletions  
Enable logging when NAT flows are created or deleted. Default: Off  
1. Change the scope from Default to **Global**.  
2. Click **On**.  
UDP Timeout  
Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minutes  
TCP Timeout  
Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)
### Block ICMP
Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages.

Default: Off

### Respond to Ping
Select On to have the vEdge router respond to ping requests to the NAT interface’s IP address that are received from the public side of the connection.

### NAT Pool Range Start
Enter a starting IP address for the NAT pool.

1. Change the scope from Default to Global to enable the field.
2. Enter the starting IP address for the NAT pool.

### NAT Pool Range End
Enter a closing IP address for the NAT pool.

1. Change the scope from Default to Global to enable the field.
2. Enter the last IP address for the NAT pool.

### CLI Equivalent
```
vpn vpn-id
  interface interface-name
    nat
      block-icmp-error
      refresh (bi-directional | outbound)
      respond-to-ping
      tcp-timeout minutes
      udp-timeout minutes
```

### IPv6 NAT

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| UDP Timeout    | Enter the timeout value for User Datagram Protocol (UDP) traffic  
  1. Change the scope from Default to Global to enable the field.  
  2. Enter a timeout value.  
  Range: 1–536870 seconds  
  Default: 1 second |
| TCP Timeout    | Enter the timeout value for Transmission Control Protocol (TCP) traffic.  
  1. Change the scope from Default to Global to enable the field.  
  2. Enter a timeout value.  
  Range: 1–536870 seconds  
  Default: 60 seconds |

To save the feature template, click **Save**.
CLI Equivalent

```
interface interface-name
  nat64 enable
    tcp-timeout minutes
    udp-timeout minutes
```

CLI Equivalent

Optionally, click either Port Forward or Static NAT to enable those parameters.

Configuring VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. Range: 1 through 255</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter the priority level of the router. The router with the highest priority is elected as master. If two vEdge routers have the same priority, the one with the higher IP address is elected as master. Range: 1 through 254 Default: 100</td>
</tr>
<tr>
<td>Timer</td>
<td>Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. Range: 1 through 3600 seconds Default: 1 second</td>
</tr>
<tr>
<td>Track OMP</td>
<td>By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which vEdge router is the master virtual router. If a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:</td>
</tr>
<tr>
<td>Track Prefix List</td>
<td>By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which vEdge router is the master virtual router. If a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:</td>
</tr>
</tbody>
</table>

  **Track OMP**—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the master VRRP router loses all its OMP sessions, VRRP elects a new default gateway from those that have at least one active OMP session.

  **Track Prefix List**—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the master VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.
**Apply Access Lists and QoS Parameters**

To configure a shaping rate to a vEdge router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a vEdge router interface, select the ACL/QoS tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS Map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI Equivalent**

```bash
vpn vpn-id
  interface interface-name
    vrrp group-number
    ipv4 ip-address
    priority number
    timer seconds
    (track-omp | track-prefix-list list-name)
```

```bash
vpn vpn-id
  interface interface-name
    access-list acl-list (in | out)
    policer policer-name (in | out)
    qos-map name
```
**Add ARP Table Entries**

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click **Add New ARP** and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address in colon-separated hexadecimal notation.</td>
</tr>
</tbody>
</table>

To save the ARP configuration, click **Add**.

To save the feature template, click **Save**.

**CLI Equivalent**

```
vpn vpn-id
tunnel interface interface-name
  arp
    ip ip-address mac mac-address
```

**Configure IEEE 802.1X Authentication for WANs**

To configure IEEE 802.1X authentication for WANs on the interface, select the 802.1X tab, and click **On**. Then enter values for the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>Click On to enable IEEE 802.1X on the interface.</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>Enter the tag of the RADIUS server to use for 802.1X authentication. It can be from 4 through 16 characters long. Use the AAA feature template to configure.</td>
</tr>
<tr>
<td>Account Interim Interval</td>
<td>Enter how often to send 802.1X interim accounting updates to the RADIUS server. Range: 0 through 7200 seconds Default: 0 (no interim accounting updates are sent)</td>
</tr>
<tr>
<td>NAS Identifier</td>
<td>Enter the NAS identifier of the local router. It can be a string from 1 to 255 characters long. This identifier is sent to the RADIUS server.</td>
</tr>
<tr>
<td>NAS IP</td>
<td>Enter the NAS IP address of the local router. This address is sent to the RADIUS server.</td>
</tr>
<tr>
<td>Wake On LAN</td>
<td>Enable a client to be powered up when the router receives an Ethernet magic packet frame.</td>
</tr>
<tr>
<td>Control Direction</td>
<td>Select how an 802.1X interface that is using wake on LAN handles packets from unauthorized clients:</td>
</tr>
</tbody>
</table>
  • In and Out—Send and receive packets with unauthorized clients. This is the default |
  • In Only—Send but do not receive packets with unauthorized clients. |
### Parameter Name | Description
--- | ---
Reauthentication | Enter how often to reauthenticate 802.1X clients. By default, no reauthentication attempts are made after the initial LAN access request. 
Range: 0 through 1440 minutes

Inactivity | Enter how long to wait before revoking an 802.1X client's network access. 
Range: 0 through 1440 minutes (24 hours) 
Default: 60 minutes (1 hour)

Host Mode | Select whether an 802.1X interface grants access to a single client or to multiple clients: 
- Multi Auth—Grant access to one client on a voice VLAN and multiple clients on data VLANs. 
- Multi Host—Grant access to multiple clients 
- Single Host—Grant access only to the first authenticated client. This is the default.

To configure other IEEE 802.1X authentication properties, click **Advanced Options** and configure the following parameters:

### Parameter Name | Description
--- | ---
Authentication Order | Set the order of authentication methods to use when authenticating devices for connection to the 802.1X WAN. The default authentication order is RADIUS, then MAC authentication bypass (MAB).

**VLAN**

Authentication Fail VLAN | Configure network access when RADIUS authentication or the RADIUS server fails. An authentication-fail VLAN is similar to a critical VLAN.

Guest VLAN | Configure a guest VLAN to provide limited services 50 802.1X–compliant clients.

Authentication Reject VLAN | Configure limited services to 802.1X–compliant clients that failed RADIUS authentication. An authentication-reject VLAN is similar to a restricted VLAN.

Default VLAN | Configure network access for 802.1X–compliant clients that are successfully authenticated by the RADIUS server. If you do not configure a default VLAN on the router, successfully authenticated clients are placed into VLAN 0, which is the VLAN associated with an untagged bridge.

**Dynamic Authentication Server**

DAS Port | Configure the UDP port number to listen for CoA requests from the RADIUS server. 
Range: 1 through 65535 
Default: 3799
### Parameter Name | Description
--- | ---
Client | Set the IP address of the RADIUS or other authentication server from which to accept CoA requests.
Secret Key | Set the password that the RADIUS or other authentication server uses to access the router's 802.1X interface.
Time Window | Set how long a CoA request is valid.  
Range: 0 through 1000 seconds  
Default: 300 seconds (5 minutes)
Require Timestamp | Enable to require the DAS client to timestamp CoA messages.
VPN | Set the VPN through which the RADIUS or other authentication server is reachable.

#### MAC Authentication Bypass

| Parameter | Description |
--- | --- |
Server | Select to enable MAC authentication bypass (MAB) on the RADIUS server and to authentication non-802.1X–compliant clients using a RADIUS server.
Allow | Specify the MAC addresses of one or more devices so that authentication checks for these devices are performed using the RADIUS server.

#### Request Attributes

| Type | Description |
--- | --- |
Authentication | Click Authentication, then click Add New Authentication Entry to configure RADIUS authentication attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.  
To save the entry, click Add.
Accounting | Click Accounting, then click Add New Accounting Entry to configure RADIUS accounting attribute–value (AV) pairs to send to the RADIUS server during an 802.1X session.  
To save the entry, click Add.

To save the feature template, click Save.

### CLI Equivalent

```cli
vpn 0
  interface interface-name
dot1x
  accounting-interval minutes
  acct-req-attr attribute-number (integer integer | octet octet | string string)
  auth-fail-vlan vlan-id
  auth-order (mab | radius)
  auth-reject-vlan vlan-id
  auth-req-attr attribute-number (integer integer | octet octet | string string)
  control-direction direction
das
  client ip-address
  port port-number
  require-timestamp
  secret-key password
  time-window seconds
```
### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Supported routers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplex</td>
<td>vEdge and IOS XE routers</td>
<td>Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. Default: full</td>
</tr>
<tr>
<td>MAC Address</td>
<td>vEdge and IOS XE routers</td>
<td>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.</td>
</tr>
<tr>
<td>IP MTU</td>
<td>vEdge and IOS XE routers</td>
<td>Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes</td>
</tr>
<tr>
<td>PMTU Discovery</td>
<td>vEdge and IOS XE routers</td>
<td>Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>vEdge and IOS XE routers</td>
<td>Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. Values: autonet, both, egress, ingress, none Default: autoneg</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>vEdge and IOS XE routers</td>
<td>Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Supported routers</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Speed</td>
<td>vEdge and IOS XE routers</td>
<td>Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, or 1000 Mbps. Default: Autonegotiate (10/100/1000 Mbps).</td>
</tr>
<tr>
<td>Clear-Don't-Fragment</td>
<td>vEdge and IOS XE routers</td>
<td>Click <strong>On</strong> to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>Static Ingress QoS</td>
<td>vEdge routers</td>
<td>Specify a queue number to use for incoming traffic. Range: 0 through 7.</td>
</tr>
<tr>
<td>ARP Timeout</td>
<td>vEdge routers</td>
<td>Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours). Default: 1200 (20 minutes).</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>vEdge and IOS XE routers</td>
<td>Click <strong>Off</strong> to turn off autonegotiation. By default, an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>vEdge and IOS XE routers</td>
<td>Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN. Note that TLOC extension over L3 is only supported for Cisco IOS XE routers. If configuring TLOC extension over L3 for a Cisco IOS XE router, enter the IP address of the L3 interface.</td>
</tr>
<tr>
<td>Power over Ethernet</td>
<td>vEdge 100m and vEdge 100wm routers</td>
<td>Click <strong>On</strong> to enable PoE on the interface.</td>
</tr>
<tr>
<td>Tracker</td>
<td>vEdge routers</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>vEdge routers</td>
<td>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</td>
</tr>
<tr>
<td>GRE Tunnel Source IP</td>
<td>IOS XE routers</td>
<td>Enter the IP address of the extended WAN interface.</td>
</tr>
<tr>
<td>Xconnect (on IOS XE routers)</td>
<td>IOS XE routers</td>
<td>Enter the name of a physical interface on the same router that connects to the WAN transport.</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.
CLI Equivalent

```
vpn vpn-id
  interface interface-name
  arp-timeout seconds (on vEdge routers only)
  [no] autonegotiate
  clear-dont-fragment
duplex (full | half)
  flow-control control
  icmp-redirect-disable (on vEdge routers only)
  mac-address mac-address
  mtu bytes
  pmtu
  pppoe-client (on vEdge 100m and vEdge 100wm routers only)
  ppp-interface pppnumber
  speed speed
  static-ingress-qos number (on vEdge routers only)
tcp-max-adjust bytes
tloc-extension interface-name (on vEdge routers only)
  tracker tracker-name (on vEdge routers only)
```

VPN Interface Ethernet PPPoE

Use the PPPoE template for Cisco IOS XE routers.

You configure PPPoE over GigabitEthernet interfaces on Cisco IOS XE routers, to provide PPPoE client support.

To configure interfaces on Cisco routers using vManage templates:

1. Create a VPN Interface Ethernet PPPoE feature template to configure Ethernet PPPoE interface parameters, as described in this article.
2. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select "From Feature Template."
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Ethernet PPPoE.
7. From the VPN Interface Ethernet PPPoE drop-down, click Create Template. The VPN Interface Ethernet PPPoE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Ethernet PPPoE parameters.
8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure PPPoE Functionality**

To configure basic PPPoE functionality, select the Basic Configuration tab and configure the following parameters. Required parameters are indicated with an asterisk.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the GigabitEthernet interface.</td>
</tr>
<tr>
<td>Ethernet Interface Name</td>
<td>Enter the name of a GigabitEthernet interface. For IOS XE routers, you must spell out the interface names completely (for example, GigabitEthernet0/0/0).</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN tag of the sub-interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the Ethernet-PPPoE-enabled interface.</td>
</tr>
</tbody>
</table>
**VPN Interface Ethernet PPPoE**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialer Pool Member</td>
<td>Enter the number of the dialer pool to which the interface belongs.</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 100 to 255.</td>
</tr>
<tr>
<td>PPP Maximum Payload</td>
<td>Enter the maximum receive unit (MRU) value to be negotiated during PPP Link Control Protocol (LCP) negotiation.</td>
</tr>
<tr>
<td></td>
<td><em>Range:</em> 64 through 1792 bytes</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**Configure the PPP Authentication Protocol**

To configure the PPP Authentication Protocol, select the PPP tab and configure the following parameters. Required parameters are indicated with an asterisk.

**Table 154:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP Authentication Protocol</td>
<td>Select the authentication protocol used by the MLP:</td>
</tr>
<tr>
<td></td>
<td>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <strong>hostname</strong> can be up to 255 characters.</td>
</tr>
<tr>
<td></td>
<td>• PAP—Enter the username and password provided by your ISP. <strong>username</strong> can be up to 255 characters.</td>
</tr>
<tr>
<td></td>
<td>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**Create a Tunnel Interface**

On IOS XE routers, you can configure up to four tunnel interfaces. This means that each router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

**Table 155:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2</td>
</tr>
<tr>
<td>vBond As STUN Server</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Controller Group List</td>
<td>Set the vSmart controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS. Range: 0 through 8 Default: 5</td>
</tr>
<tr>
<td>Port Hop</td>
<td>Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled</td>
</tr>
<tr>
<td>Low-Bandwidth Link</td>
<td>Select to characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>Select On or Off for each service to allow or disallow the service on the interface.</td>
</tr>
</tbody>
</table>

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

Table 156:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IPSec Preference     | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.  
                         \* Range: 0 through 4294967295 \* Default: 0                              |
| IPSec Weight         | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.  
                         \* Range: 1 through 255 \* Default: 1                                          |
| Carrier              | Select the carrier name or private network identifier to associate with the tunnel.  
                         \* Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default \* Default: default |
| Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface.        |
| Last-Resort Circuit  | Select to use the tunnel interface as the circuit of last resort.             |
| NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection.  
                         \* Range: 1 through 60 seconds \* Default: 5 seconds                     |
| Hello Interval       | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection.  
                         \* Range: 100 through 10000 milliseconds (1 second) \* Default: 1000 milliseconds (1 second) |
| Hello Tolerance      | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.  
                         \* Range: 12 through 60 seconds \* Default: 12 seconds                  |

**Configure the Interface as a NAT Device**

To configure an interface to act as a NAT device for applications such as port forwarding, select the NAT tab, click On and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT</td>
<td>Click On to have the interface act as a NAT device.</td>
</tr>
<tr>
<td>Refresh Mode</td>
<td>Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound). * Default: Outbound</td>
</tr>
</tbody>
</table>
| UDP Timeout    | Specify when NAT translations over UDP sessions time out.  
                         \* Range: 1 through 65536 minutes \* Default: 1 minutes                |
| TCP Timeout    | Specify when NAT translations over TCP sessions time out.  
                         \* Range: 1 through 65536 minutes \* Default: 60 minutes (1 hour)     |
Block ICMP | Select On to block inbound ICMP error messages. By default, a router acting as a NAT device receives these error messages. Default: Off
---|---
Respond to Ping | Select On to have the router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

**Table 158:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Start Range</td>
<td>Enter a port number to define the port or first port in the range of interest. Range: 0 through 65535</td>
</tr>
<tr>
<td>Port End Range</td>
<td>Enter the same port number to apply port forwarding to a single port, or enter a larger number to apply it to a range of ports. Range: 0 through 65535</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules.</td>
</tr>
<tr>
<td>VPN</td>
<td>Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network. Range: 0 through 65530</td>
</tr>
<tr>
<td>Private IP</td>
<td>Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule.</td>
</tr>
</tbody>
</table>

To save a port forwarding rule, click Add.

To save the feature template, click Save.

**Apply Access Lists**

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

**Table 159:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
</tbody>
</table>
To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:

**Table 160:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through ((2^{32} / 2) – 1) kbps</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through ((2^{32} / 2) – 1) kbps</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. <em>Range:</em> 576 through 1804. <em>Default:</em> 1500 bytes</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range:</em> 552 to 1460 bytes. <em>Default:</em> None</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Tracker</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
--- | ---
IP Directed-Broadcast | Enables translation of a directed broadcast to physical broadcasts. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a node that is not itself part of that destination subnet.

To save the feature template, click Save.

**Release Information**

Introduced in vManage NMS in Release 18.4.1.

---

**VPN Interface GRE**

Use the VPN Interface GRE template for all vEdge Cloud and vEdge router devices.

When a service, such as a firewall, is available on a device that supports only GRE tunnels, you can configure a GRE tunnel on the vEdge router to connect to the remote device by configuring a logical GRE interface. You then advertise that the service is available via a GRE tunnel, and you create data policies to direct the appropriate traffic to the tunnel. GRE interfaces come up as soon as they are configured, and they stay up as long as the physical tunnel interface is up.

To configure GRE interfaces using vManage templates:

1. Create a VPN Interface GRE feature template to configure a GRE interface, as described in this article.
2. Create a VPN feature template to advertise a service that is reachable via a GRE tunnel, to configure GRE-specific static routes, and to configure other VPN parameters. See the VPN help topic.
3. Create a data policy on the vSmart controller that applies to the service VPN, including a set service service-name local command. See the Policies help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface GRE.
   3. From the VPN Interface GRE drop-down, click Create Template. The VPN Interface GRE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface GRE parameters.
6. To create a template for VPNs 1 through 511, and 513 through 65530:
1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

2. Click the Service VPN drop-down.

3. Under Additional VPN templates, located to the right of the screen, click VPN Interface GRE.

4. From the VPN Interface GRE drop-down, click Create Template. The VPN Interface GRE template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface GRE parameters.

7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configuring a Basic GRE Interface

To configure a basic GRE interface, select the Basic Configuration and then configure the following parameters. Parameters marked with an asterisk are required to configure a GRE interface.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click Off to enable the interface.</td>
</tr>
<tr>
<td>Interface Name*</td>
<td>Enter the name of the GRE interface, in the format gre number. number can be from 1 through 255.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the GRE interface.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Source*        | Enter the source of the GRE interface:  
  • GRE Source IP Address—Enter the source IP address of the GRE tunnel interface. This address is on the local router.  
  • Tunnel Source Interface—Enter the physical interface that is the source of the GRE tunnel. |
| Destination*   | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device |
| GRE Destination IP Address* | Enter the destination IP address of the GRE tunnel interface. This address is on a remote device |
| IPv4 Address   | Enter an IPv4 address for the GRE tunnel. |
| IP MTU         | Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes |
| Clear-Dont-Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. |
| TCP MSS        | Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None |
| Keepalive Interval | Specify how often the GRE interface sends keepalive packets on the GRE tunnel. Because GRE tunnels are stateless, sending of keepalive packets is the only way to determine whether the remote end of the tunnel is up. The keepalive packets are looped back to the sender. Receipt of these packets by the sender indicates that the remote end of the GRE tunnel is up. Range: 0 through 65535 seconds Default: 10 seconds |
| Keepalive Retries | Specify how many times the GRE interface tries to resend keepalive packets before declaring the remote end of the GRE tunnel to be down. Range: 0 through 255 Default: 3 |

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id interface gre number clear-dont-fragment description text ip address ipv4-prefix/length keepalive seconds retries mtu bytes policer policer-name (in |out) qos-map name rewrite-rule name shaping-rate name [no] shutdown tcp-mss-adjust bytes tunnel-destination ip-address ( tunnel-source ip-address | tunnel-source-interface interface-name)```

### Configure Interface Access Lists

To configure access lists on a GRE interface, select the ACL tab and configure the following parameters:
Table 163:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

**CLI equivalent:**
```
vpn vpn-id interface gre number access-list acl-list (in | out)
policer policer-name (in | out)
qos-map name rewrite-rule name shaping-rate name
```

**Release Information**

Introduced in vManage NMS Release 15.4.1.

**VPN Interface IPsec (for vEdge Routers)**

Use the VPN Interface IPsec feature template to configure IPsec tunnels on vEdge routers that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels in the transport VPN (VPN 0) and in service VPNs (VPN 1 through 65530, except for 512).

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
6. Click the Service VPN drop-down.
7. Under Additional VPN Templates, located to the right of the screen, click VPN Interface IPsec.

8. From the VPN Interface IPsec drop-down, click Create Template. The VPN Interface IPsec template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface IPsec parameters.

9. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

10. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 164:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.

When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.

To change the default key, type a new string and move the cursor out of the Enter Key box.

Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices.

Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

**Configure a Basic IPsec Tunnel Interface**

To configure an IPsec tunnel to use for IKE sessions, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an IPsec tunnel.

**Table 165:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td>Interface Name*</td>
<td>Enter the name of the IPsec interface, in the format <code>ipsec number. number</code> can be from 1 through 256.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the IPsec interface.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>Enter the IPv4 address of the IPsec interface, in the format <code>ipv4-prefix/length</code>. The address must be a /30.</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
---|---
Source* | Set the source of the IPsec tunnel that is being used for IKE key exchange:
- Click IP Address—Enter the IPv4 address that is the source tunnel interface. This address must be configured in VPN 0.
- Click Interface—Enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in VPN 0.

Destination: IPsec Destination IP Address/FQDN* | Set the destination of the IPsec tunnel that is being used for IKE key exchange. Enter either an IPv4 address or the fully qualified DNS name that points to the destination.

TCP MSS | Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range:** 552 to 1460 bytes **Default:** None

IP MTU | Specify the maximum MTU size of packets on the interface. **Range:** 576 through 1804 **Default:** 1500 bytes

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id
  interface ipsec number ip address ipv4-prefix/length mtu bytes
  no shutdown
tcp-mss-adjust bytes tunnel-destination ipv4-address
  { tunnel-source ip-address | tunnel-source-interface interface-name}
```

### Configure Dead-Peer Detection

To configure IKE dead-peer detection to determine whether the connection to an IKE peer is functional and reachable, select the DPD tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD Interval</td>
<td>Specify the interval for IKE to send Hello packets on the connection. <strong>Range:</strong> 0 through 65535 seconds (1 hour through 14 days) <strong>Default:</strong> 10 seconds</td>
</tr>
<tr>
<td>DPD Retries</td>
<td>Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer. <strong>Range:</strong> 0 through 255 <strong>Default:</strong> 3</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```
vpn vpn-id interface ipsec number dead-peer-detection seconds retries number
```
**Configure IKE**

To configure IKE, select the IKE tab and configure the parameters discussed below.

When you create an IPsec tunnel on a vEdge router, IKE Version 1 is enabled by default on the tunnel interface. The following properties are also enabled by default for IKEv1:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours
- SA establishment mode—Main

To modify IKEv1 parameters, configure the following:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>Enter 1 to select IKEv1.</td>
</tr>
<tr>
<td>IKE Mode</td>
<td>Specify the IKE SA establishment mode. Values: Aggressive mode, Main mode</td>
</tr>
<tr>
<td></td>
<td>Default: Main mode</td>
</tr>
<tr>
<td>IPsec Rekey Interval</td>
<td>Specify the interval for refreshing IKE keys. Values: 1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td>Default: 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Cipher Suite</td>
<td>Specify the type of authentication and encryption to use during IKE key</td>
</tr>
<tr>
<td>IKE Diffie-Hellman Group</td>
<td>Specify the Diffie-Hellman group to use in IKE key exchange. Values:</td>
</tr>
<tr>
<td></td>
<td>1024-bit modulus, 2048-bit modulus, 3072-bit modulus, 4096-bit modulus</td>
</tr>
<tr>
<td></td>
<td>Default: 4096-bit modulus</td>
</tr>
<tr>
<td>IKE Authentication: Preshared Key</td>
<td>To use preshared key (PSK) authentication, enter the password to use</td>
</tr>
<tr>
<td></td>
<td>with the preshared key.</td>
</tr>
<tr>
<td>IKE ID for Local End Point</td>
<td>If the remote IKE peer requires a local end point identifier, specify</td>
</tr>
<tr>
<td></td>
<td>it. Values: Default: Tunnel's source IP address</td>
</tr>
<tr>
<td>IKE ID for Remote End Point</td>
<td>If the remote IKE peer requires a remote end point identifier, specify</td>
</tr>
<tr>
<td></td>
<td>it. Values: 1 through 64 characters Default: Tunnel's destination IP address</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

*CLI equivalent:*

```
vpn vpn-id interface ipsec number ike authentication-type type local-id id
temporary pre-shared-secret password
remote-id id cipher-suite suite group number mode mode rekey-interval seconds
version 1
```

To configure IKEv2, configure the following parameters:
Table 168:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>Enter 2 to select IKEv2.</td>
</tr>
<tr>
<td>IPsec Rekey Interval</td>
<td>Specify the interval for refreshing IKE keys. <em>Range:</em> 3600 through 1209600 seconds (1 hour through 14 days) <em>Default:</em> 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Cipher Suite</td>
<td>Specify the type of authentication and encryption to use during IKE key exchange. <em>Values:</em> aes128-cbc-sha1, aes256-cbc-sha1 <em>Default:</em> aes256-cbc-sha1</td>
</tr>
<tr>
<td>IKE Authentication: Preshared Key</td>
<td>To use preshared key (PSK) authentication, enter the password to use with the preshared key.</td>
</tr>
<tr>
<td>IKE ID for Local End Point</td>
<td>If the remote IKE peer requires a local end point identifier, specify it. <em>Range:</em> Tunnel's source IP address</td>
</tr>
<tr>
<td>IKE ID for Remote End Point</td>
<td>If the remote IKE peer requires a remote end point identifier, specify it. <em>Range:</em> 1 through 64 characters <em>Default:</em> Tunnel's destination IP address</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

*CLI equivalent:*
```
vpn vpn-id interface ipsec number ike authentication-type type
    local-id id
    pre-shared-secret password
    remote-id id cipher-suite suite group number rekey-interval seconds
version 2
```

**Configure IPsec Tunnel Parameters**

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

Table 169:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Rekey Interval</td>
<td>Specify the interval for refreshing IKE keys. <em>Range:</em> 3600 through 1209600 seconds (1 hour through 14 days) <em>Default:</em> 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Replay Window</td>
<td>Specify the replay window size for the IPsec tunnel. <em>Values:</em> 64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes <em>Default:</em> 32 bytes</td>
</tr>
<tr>
<td>IPsec Cipher Suite</td>
<td>Specify the authentication and encryption to use on the IPsec tunnel. <em>Values:</em> aes256-cbc-sha1, aes256-gem, null-sha1 <em>Default:</em> aes256-gem</td>
</tr>
</tbody>
</table>
Perfect Forward Secrecy | Specify the PFS settings to use on the IPsec tunnel. *Values:* • `group-2`—Use the 1024-bit Diffie-Hellman prime modulus group. • `group-14`—Use the 2048-bit Diffie-Hellman prime modulus group. • `group-15`—Use the 3072-bit Diffie-Hellman prime modulus group. • `group-16`—Use the 4096-bit Diffie-Hellman prime modulus group. • `none`—Disable PFS. *Default:* `group-16`

To save the feature template, click Save.

*CLI equivalent:*

```bash
vpn vpn-id interface ipsec number ipsec cipher-suite suite perfect-forward-secrecy pfs-setting rekey-interval seconds replay-window number
```

**Release Information**

Introduced in vManage NMS in Release 17.2. In Release 17.2.3, add support for PFS. In Release 18.2, support support for IPsec tunnels in VPN 0. In Release 18.4, standard IPsec support for IOS XE routers.

**VPN Interface IPsec (for XE Routers)**

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

**Create and Name the Template**

**Step 1** From the vManage menu, select Configuration ► Templates.

**Step 2** Click Feature.

**Step 3** Click Add Template.

**Step 4** Select a Cisco IOS XE device from the list.

**Step 5** From the VPN section, click VPN Interface IPsec. The VPN Interface IPsec template displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining IPsec parameters.
Step 6 In the **TemplateName** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 7 In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

---

**Basic Configuration**

To configure a basic IPsec tunnel interface select the Basic Configuration tab and configure the following parameters.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options/Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Yes / No</td>
<td>Click <strong>No</strong> to enable the interface; click <strong>Yes</strong> to disable.</td>
</tr>
<tr>
<td>Interface Name*</td>
<td>*ipsec number (1…255)</td>
<td>Enter the name of the IPsec interface. <em>Number</em> can be from 1 through 255.</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Enter a description of the IPsec interface.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>*ipv4-prefix/length</td>
<td>Enter the IPv4 address of the IPsec interface. The address must have a /30 subnet.</td>
</tr>
<tr>
<td>Source*</td>
<td></td>
<td>Set the source of the IPsec tunnel that is being used for IKE key exchange:</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in <strong>VPN 0</strong>.</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
<td>Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in <strong>VPN 0</strong>.</td>
</tr>
</tbody>
</table>
## Configure Dead-Peer Detection

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, select the DPD tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD Interval</td>
<td>Specify the interval for IKE to send Hello packets on the connection.</td>
</tr>
<tr>
<td></td>
<td>Range: 10 through 3600 seconds</td>
</tr>
<tr>
<td></td>
<td>Default: Disabled</td>
</tr>
<tr>
<td>DPD Retries</td>
<td>Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.</td>
</tr>
<tr>
<td></td>
<td>Range: 2 through 60</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.
**Configure IKE**

To configure IKE, select the IKE tab and configure the following parameters:

**Note**

When you create an IPsec tunnel on a Cisco IOS XE router, IKE Version 1 is enabled by default on the tunnel interface.

**IKE Version 1**

To modify IKEv1 parameters, configure the following values:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>1 IKEv1</td>
<td>Enter 1 to select IKEv1.</td>
</tr>
<tr>
<td></td>
<td>2 IKEv2</td>
<td>Default: IKEv1</td>
</tr>
<tr>
<td>IKE Mode</td>
<td>Aggressive mode</td>
<td>Specify the IKE SA establishment mode.</td>
</tr>
<tr>
<td></td>
<td>Main mode</td>
<td>Default: Main mode</td>
</tr>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Cipher Suite</td>
<td>AES128-CBC-SHA1</td>
<td>Specify the type of authentication and encryption to use during IKE key exchange.</td>
</tr>
<tr>
<td></td>
<td>AES256-CBC-SHA1</td>
<td>Default: AES256-CBC-SHA1</td>
</tr>
<tr>
<td>IKE Diffie-Hellman</td>
<td>1024-bit modulus</td>
<td>Specify the Diffie-Hellman group to use in IKE key exchange.</td>
</tr>
<tr>
<td>Group</td>
<td>2048-bit modulus</td>
<td>Default: 4096-bit modulus</td>
</tr>
<tr>
<td></td>
<td>3072-bit modulus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4096-bit modulus</td>
<td></td>
</tr>
</tbody>
</table>
### Configure IKE Authentication

**Parameter Name** | **Options** | **Description**
--- | --- | ---
IKE Authentication | Configure IKE authentication. |  
Preshared Key | Enter the password to use with the preshared key. |  
IKE ID for Local End Point | If the remote IKE peer requires a local end point identifier, specify it.  
*Range:* 1 through 64 characters  
*Default:* Tunnel's source IP address |  
IKE ID for Remote End Point | If the remote IKE peer requires a remote end point identifier, specify it.  
*Range:* 1 through 64 characters  
*Default:* Tunnel's destination IP address |  

To save the feature template, click **Save**.

#### CLI Equivalent

```
crypto
  isakmp
    keepalive 60-86400 2-60 {on-demand | periodic}
  policy policy_num
    encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
    hash {sha384 | sha256 | sha}
    authentication pre-share
    group {2 | 14 | 16 | 19 | 20 | 21}
    lifetime 60-86400
  profile ikev1_profile_name
    match identity address ip_address [mask]
    keyring keyring_name
  profile ipsec_profile_name
    set transform-set transform_set_name
    set isakmp-profile ikev1_profile_name
    set security-association
      lifetime {kilobytes disable | seconds 120-2592000}
      replay {disable | window-size [64 | 128 | 256 | 512 | 1024]}
      set pfs group {14 | 16 | 19 | 20 | 21}
      keyring keyring_name
      pre-shared-key address ip_address [mask] key key_string
      ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 | esp-sha384-hmac | esp-sha256-hmac} mode tunnel
```

### IKE Version 2

To configure the IPsec tunnel that carries IKEv2 traffic, select the IPsec tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| IKE Version | 1 IKEv1  
2 IKEv2 | Enter 2 to select IKEv2.  
Default: IKEv1 |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Mode</td>
<td>Aggressive, Main</td>
<td>Aggressive mode -- Negotiation is quicker, and the initiator and responder ID pass in the clear.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Main mode -- Establishes an IKE SA session before starting IPSec negotiations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Main</td>
</tr>
<tr>
<td>IPsec Rekey</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
<td>Range: 1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Cipher Suite</td>
<td>AES128-CBC-SHA1, AES256-CBC-SHA1</td>
<td>Specify the type of authentication and encryption to use during IKE key exchange.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: AES256-CBC-SHA1</td>
</tr>
<tr>
<td>IKE Diffie-Hellman</td>
<td>2 1024-bit modulus, 14 2048-bit modulus, 15 3072-bit modulus, 16 4096-bit modulus</td>
<td>Specify the Diffie-Hellman group to use in IKE key exchange.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
<td>Default: 16 4096-bit modulus</td>
</tr>
<tr>
<td>IKE Authentication</td>
<td>Configure IKE authentication.</td>
<td></td>
</tr>
<tr>
<td>Pre-shared Key</td>
<td>Enter the password to use with the pre-shared key.</td>
<td></td>
</tr>
<tr>
<td>IKE ID for Local End Point</td>
<td>If the remote IKE peer requires a local end point identifier, specify it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 64 characters</td>
<td>Default: Tunnel’s source IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE ID for Remote End Point</td>
<td>If the remote IKE peer requires a remote end point identifier, specify it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 64 characters</td>
<td>Default: Tunnel’s destination IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To save the feature template, click **Save**.

**CLI Equivalent**

```bash
crypto
ikev2
    proposal proposal_name
        encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
        integrity {sha256 | sha384 | sha512}
        group {2 | 14 | 15 | 16}
        keyring idev2_keyring_name
        peer peer_name
        address tunnel_dest_ip [mask]
        pre-shared-key key_string
        profile ikev2_profile_name
```
Conf

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 hour through 14 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3600 seconds</td>
</tr>
<tr>
<td>IKE Replay Window</td>
<td>64, 128, 256, 512, 1024, 2048, 4096, 8192</td>
<td>Specify the replay window size for the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 512</td>
</tr>
<tr>
<td>IPsec Cipher Suite</td>
<td>aes256-cbc-sha1</td>
<td>Specify the authentication and encryption to use on the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>aes256-gcm</td>
<td>Default: aes256-gcm</td>
</tr>
<tr>
<td></td>
<td>null-sha1</td>
<td></td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>2 1024-bit modulus</td>
<td>Specify the PFS settings to use on the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>14 2048-bit modulus</td>
<td>Select one of the following Diffie-Hellman prime modulus groups:</td>
</tr>
<tr>
<td></td>
<td>15 3072-bit modulus</td>
<td>1024-bit – group-2</td>
</tr>
<tr>
<td></td>
<td>16 4096-bit modulus</td>
<td>2048-bit – group-14</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>3072-bit – group-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096-bit – group-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none – disable PFS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: group-16</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI Equivalent**

```
crypto ipsec
  profile ipsec_profile_name
  set ikev2-profile ikev2_profile_name
  set security-association
    lifetime {seconds 120-2592000 | kilobytes disable}
    replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}}
  set pfs group {2 | 14 | 15 | 16 | none}
  set transform-set transform_set_name
```
Release Information

Introduced in vManage NMS for Cisco IOS XE routers in release 19.1.

VPN Interface Multilink

Use the VPN Interface Multilink template for Cisco IOS XE routers running the SD-WAN software.

Multilink Point-to-Point Protocol (MLP) is used to combine multiple physical links into a single logical connection, called an MLP bundle.

To configure multilink on IOS XE routers using vManage templates:

1. Create a VPN Interface Multilink feature template to configure multilink interface properties.
2. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. If you are configuring the multilink interface in the transport VPN (VPN 0):
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface Multilink Controller.
6. If you are configuring the multilink interface in a service VPN (VPNs other than VPN 0):
   1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
   2. In the Service VPN drop-down, enter the number of the service VPN.
   3. Under Additional VPN Templates, located to the right of the screen, click VPN Interface Multilink Controller.
7. From the VPN Interface Multilink Controller drop-down, click Create Template. The VPN Multilink template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining multilink Interface parameters.
8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 170:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure a Multilink Interface

To configure a multilink interface, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

Note, if you are creating a VPN Interface Multilink template, you do not need to create a T1/E1 Controller template or a VPN Interface T1/E1 template.

Table 171:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the multilink interface.</td>
</tr>
<tr>
<td>Multilink Interface Name*</td>
<td>Enter the number of the MLP interface. It can be a number from 1 through 65,535.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the multilink interface.</td>
</tr>
<tr>
<td>Multilink Group Number*</td>
<td>Enter the number of the multilink group. It can be a number from 1 through 65,535 but it must be the same as the number you enter in the Multilink Interface Name parameter.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>To configure a static address, click Static and enter an IPv4 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.</td>
</tr>
</tbody>
</table>
To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.

To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address*</td>
<td>To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address. To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.</td>
</tr>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. <em>Range:</em> 1 through (2^{32}/2) – 1 kbps</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. MLP encapsulation adds 6 extra bytes (4 header, 2 checksum) to each outbound packet. These overhead bytes reduce the effective bandwidth on the connection; therefore, the throughput for an MLP bundle is slightly less than an equivalent bandwidth connection that is not using MLP. <em>Range:</em> 576 through 1804 <em>Default:</em> 1500 bytes</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Configure the PPP Authentication Protocol**

To configure the PPP authentication protocol, select the PPP tab and configure the following parameters:

<p>| Table 172: |</p>
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Protocol</td>
<td>Select the authentication protocol used by the MLP:</td>
</tr>
<tr>
<td>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). <em>hostname</em> can be up to 255 characters.</td>
<td></td>
</tr>
<tr>
<td>• PAP—Enter the username and password provided by your ISP. <em>username</em> can be up to 255 characters.</td>
<td></td>
</tr>
<tr>
<td>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</td>
<td></td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**Create a Tunnel Interface**

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.
To configure a tunnel interface for the multilink interface, select the Tunnel Interface tab and configure the following parameters:

**Table 173:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
</tbody>
</table>
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.  
**Range:** 0 through 8  
**Default:** 2 |
| vBond As STUN Server    | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT. |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.  
**Range:** 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.  
**Range:** 0 through 8  
**Default:** 5 |
| Port Hop                | Click On to enable port hopping, or click Off to disable it. When a router is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other routers when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value.  
**Default:** Enabled |
| Low-Bandwidth Link      | Select to characterize the tunnel interface as a low-bandwidth link. |
| Allow Service           | Select On or Off for each service to allow or disallow the service on the interface. |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

**Table 174:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| GRE            | Use GRE encapsulation on the tunnel interface. By default, GRE is disabled.  
If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation. |
### Parameter Name | Description
--- | ---
IPsec | Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.
IPsec Preference | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value. 
*Range:* 0 through 4294967295  
*Default:* 0
IPsec Weight | Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel. 
*Range:* 1 through 255  
*Default:* 1
Carrier | Select the carrier name or private network identifier to associate with the tunnel. 
*Values:* carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default  
*Default:* default
Bind Loopback Tunnel | Enter the name of a physical interface to bind to a loopback interface.
Last-Resort Circuit | Select to use the tunnel interface as the circuit of last resort.
NAT Refresh Interval | Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. 
*Range:* 1 through 60 seconds  
*Default:* 5 seconds
Hello Interval | Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. 
*Range:* 100 through 10000 milliseconds  
*Default:* 1000 milliseconds (1 second)
Hello Tolerance | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. 
*Range:* 12 through 60 seconds  
*Default:* 12 seconds

### Apply Access Lists
To apply a rewrite rule, access lists, and polices to a router interface, select the ACL tab and configure the following parameters:

### Table 175:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
</tbody>
</table>
Parameter Name | Description
--- | ---
Ingress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.
Ingress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.
Egress ACL – IPv4 | Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.
Egress ACL – IPv6 | Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.
Ingress Policer | Click On, and specify the name of the policer to apply to packets being received on the interface.
Egress Policer | Click On, and specify the name of the policer to apply to packets being transmitted on the interface.

To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:

Table 176:

Parameter Name | Description
--- | ---
PMTU Discovery | Click On to enable path MTU discovery on the interface, to allow the router to determine the largest MTU size supported without requiring packet fragmentation.
TCP MSS | Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. *Range: 552 to 1460 bytes* *Default: None*
Clear Dont Fragment | Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.
Static Ingress QoS | Select a queue number to use for incoming traffic. *Range: 0 through 7*
Autonegotiate | Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.
TLOC Extension | Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.

To save the feature template, click Save.
VPN Interface NAT Pool

Create NAT Pool Interfaces in a VPN

Use the VPN Interface NAT Pool template for all vEdge routers, to create Network Address Translation (NAT) pools of IP addresses in virtual private networks (VPNs). To configure NAT pool interfaces in a VPN using vManage templates:

1. Create a VPN Interface NAT Pool template to configure Ethernet interface parameters, as described in this article.
2. Create a VPN feature template to configure parameters for a service-side VPN. See the VPN help topic.
3. Optionally, create a data policy to direct data traffic to a service-side NAT. See Create a Device Template.

Create and Name a VPN Interface NAT Pool Template

You can open a new VPN Interface NAT Pool template from the Service VPN section of a device template.

1. From the vManage menu, select Configuration > Templates.
2. Click Feature.
3. Click Add Template.
4. Select a vEdge device from the list.
5. From the VPN section, click VPN Interface NATPool.

The VPN Interface NATPool template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface NAT Pool parameters.
1. In the required Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

2. In the optional Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

**Parameter Menus and Options**

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a ☑), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you <a href="#">attach a Viptela device to a device template</a>. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see <a href="#">Create a Template Variables Spreadsheet</a>. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>☑ Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure a NAT Pool Interface**

To configure a NAT pool interface, configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

**Basic Configuration**

Enter the following basic configuration parameters:
Table 178:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Yes</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Interface Name</td>
<td>1-31</td>
<td>Enter a number for the NAT pool interface to use for service-side NAT. For example, natpool22.</td>
</tr>
<tr>
<td>(1…31)*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>Enter the IPv4 address of the interface. The address length determines the number of NAT addresses that the router use at the same time. A vEdge router can support a maximum of 250 NAT IP addresses.</td>
<td></td>
</tr>
<tr>
<td>Refresh Mode</td>
<td>Select how NAT mappings are refreshed:</td>
<td></td>
</tr>
<tr>
<td>bi-directional</td>
<td>Keep active the NAT mappings for inbound and outbound traffic.</td>
<td></td>
</tr>
<tr>
<td>outbound</td>
<td>Keep active the NAT mappings for outbound traffic. This is the default.</td>
<td></td>
</tr>
<tr>
<td>UDP Timeout</td>
<td>1-65536 minutes</td>
<td>Enter the time when NAT translations over UDP sessions time out. Default: 1 minute</td>
</tr>
<tr>
<td>TCP Timeout</td>
<td>1-65536 minutes</td>
<td>Enter the time when NAT translations over TCP sessions time out. Default: 60 minutes (1 hour)</td>
</tr>
<tr>
<td>Block ICMP</td>
<td>On</td>
<td>Select whether a vEdge router that is acting as a NAT device should receive inbound ICMP error messages. By default, the router blocks these error messages. Click Off to receive the ICMP error messages.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Direction</td>
<td>Select the direction in which the NAT interface performs address translation:</td>
<td></td>
</tr>
<tr>
<td>inside</td>
<td>Translate the source IP address of packets that are coming from the service side of the vEdge router and that are destined to transport side of the router. This is the default.</td>
<td></td>
</tr>
<tr>
<td>outside</td>
<td>Translate the source IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined to a service-side device.</td>
<td></td>
</tr>
</tbody>
</table>
Tracker

1. To create one or more tracker interfaces, select the Tracker tab and click New Tracker.
2. Select one or more interfaces to track the status of service interfaces.
3. To save the tracker interfaces, click Add. To save the feature template, click Save.

CLI Equivalent Commands

Use the following commands to configure NAT Pool interfaces.

```
vpn vpn-id
  interface natpool
    ip address prefix/length
    nat
    tracker tracker-name1, tracker-name2, tracker-name3
    direction (inside | outside)
    [no] overload
    refresh (bi-directional | outbound)
    static source-ip ip-address1 translate-ip ip-address2 (inside | outside)
    tcp-timeout minutes
    udp-timeout minutes
    [no] shutdown
```

Configure Port-Forwarding Rules

To create port-forwarding rules to allow requests from an external network to reach devices on the internal network:

1. Select the Port Forward tab.
2. Click **New Port Forwarding Rule**, and configure the following parameters. You can create up to 128 rules.

Table 179:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Start Range</td>
<td>Enter the starting port number. This number must be less than or equal to the ending port number.</td>
<td></td>
</tr>
<tr>
<td>Port End Range</td>
<td>Enter the ending port number. To apply port forwarding to a single port, specify the same port number for the starting and ending numbers. When applying port forwarding to a range of ports, the range includes the two port numbers that you specify.</td>
<td></td>
</tr>
</tbody>
</table>
Select the protocol to apply the port-forwarding rule to. To match the same ports for both TCP and UDP traffic, configure two rules.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>0-65535</td>
<td></td>
</tr>
<tr>
<td>Private IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enter an IP address to use within the firewall. A best practice is to specify the IP address of a service-side VPN.

1. To save the rule, click Add.

2. To save the feature template, click Save.

**CLI Equivalent Commands**

```plaintext
vpn vpn-id
  interface natpoolnumber
    nat
      port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
      private-ip-address ip address private-vpn vpn-id
```

**Configure Static NAT**

To configure a static NAT of service-side source IP addresses:

1. Select the Static NAT tab. Then click New Static NAT and configure the following parameters to add a static NAT mapping:

**Table 180:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as Optional Row</td>
<td>Check <strong>Mark as Optional Row</strong> to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables. See Create a Template Variables Spreadsheet.</td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>Enter the NAT private source IP address.</td>
<td></td>
</tr>
<tr>
<td>Translate IP</td>
<td>To map a public IP address to a private source address, enter the public IP address.</td>
<td></td>
</tr>
<tr>
<td>Static NAT Direction</td>
<td>Select the direction in which to perform network address translation.</td>
<td></td>
</tr>
<tr>
<td>inside</td>
<td>Translate the IP address of packets that are coming from the service side of the vEdge router and that are destined for the transport side of the router.</td>
<td></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>outside</td>
<td>Translate the IP address of packets that are coming to the vEdge router from the transport side of the vEdge router and that are destined for a service-side device.</td>
<td></td>
</tr>
</tbody>
</table>

2. To save the NAT mapping, click Add.
3. To save the feature template, click Save.

**CLI Equivalent Commands**

```
vpn vpn-id
   interface natpoolnumber
      nat
         port-forward port-start port-number1 port-end port-number2 proto (tcp | udp)
         private-ip-address ip address private-vpn vpn-id
```

**Release Information**

Introduced in vManage NMS Release 16.3. In Release 17.2.2, add support for tracker interface status. In Release 18.4, updated images; add support for multiple tracker interfaces.

**VPN Interface PPP**

Use the VPN Interface PPP template for vEdge Cloud and vEdge router devices.

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. PPP properties are associated with a PPPoE-enabled interface on vEdge routers to connect multiple users over an Ethernet link.

To configure PPPoE on vEdge routers using vManage templates:

1. Create a VPN Interface PPP feature template to configure PPP parameters for the PPP virtual interface, as described in this article.
2. Create a VPN Interface PPP Ethernet feature template to configure a PPPoE-enabled interface. See the VPN Interface PPP Ethernet help topic.
3. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface PPP.

7. From the VPN Interface PPP drop-down, click Create Template. The VPN Interface PPP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 181:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
</table>
| Device Specific (indicated by a host icon) | Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template.

When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet.

To change the default key, type a new string and move the cursor out of the Enter Key box.

Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID. |
| Global (indicated by a globe icon) | Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs. |

### Configure a PPP Virtual Interface

To configure a PPP virtual interface, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface. You must also configure an authentication protocol and a tunnel interface for the PPP interface, and you must ensure that the maximum MTU for the PPP interface is 1492 bytes.

**Table 182:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the PPP virtual interface.</td>
</tr>
<tr>
<td>PPP Interface Name*</td>
<td>Enter the number of the PPP interface. It can be a number from 1 through 31.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the PPP virtual interface.</td>
</tr>
<tr>
<td>Bandwidth Upstream</td>
<td>For transmitted traffic, set the bandwidth above which to generate notifications. ( \text{Range: } 1 \text{ through } \left(2^{32} / 2\right) - 1 \text{ kbps} )</td>
</tr>
<tr>
<td>Bandwidth Downstream</td>
<td>For received traffic, set the bandwidth above which to generate notifications. ( \text{Range: } 1 \text{ through } \left(2^{32} / 2\right) - 1 \text{ kbps} )</td>
</tr>
</tbody>
</table>
To have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range.

To save the feature template, click Save.

**CLI equivalent:**

```bash
cisco
network

vpn 0
interface pppnumber bandwidth-downstream kbps bandwidth-upstream kbps block-non-source-ip ppp
no shutdown
```

**Configure the Access Concentrator Name and Authentication Protocol**

To configure the access concentrator name, select the PPP tab and configure the following parameters:

**Table 183:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the access concentrator used by PPPoE to route connections to the Internet.</td>
<td>AC Name</td>
</tr>
<tr>
<td>Select the authentication protocol used by PPPoE:</td>
<td>Authentication Protocol</td>
</tr>
<tr>
<td>• CHAP—Enter the hostname and password provided by your Internet Service Provider (ISP). hostname can be up to 255 characters.</td>
<td></td>
</tr>
<tr>
<td>• PAP—Enter the username and password provided by your ISP. username can be up to 255 characters.</td>
<td></td>
</tr>
<tr>
<td>• PAP and CHAP—Configure both authentication protocols. Enter the login credentials for each protocol. To use the same username and password for both, click Same Credentials for PAP and CHAP.</td>
<td></td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```bash
vpn 0
interface pppnumber ppp
ac-name name
authentication chap hostname name password password
pap password password sent-username name
```

**Create a Tunnel Interface**

On vEdge routers, you can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface for the PPP interface, select the Tunnel Interface tab and configure the following parameters:
Table 184:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the vEdge router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
</tbody>
</table>
| Maximum Control Connections | Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0.  
  Range: 0 through 8 Default: 2 |
| vBond As STUN Server    | Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT.             |
| Exclude Controller Group List | Set the vSmart controllers that the tunnel interface is not allowed to connect to.  
  Range: 0 through 100 |
| vManage Connection Preference | Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS.  
  Range: 0 through 8 Default: 5 |
| Low-Bandwidth Link      | Select to characterize the tunnel interface as a low-bandwidth link.                                                                                                                                 |
| Allow Service           | Select On or Off for each service to allow or disallow the service on the interface.                                                                                                           |

To configure additional tunnel interface parameters, click Advanced Options and configure the following parameters:

Table 185:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Use GRE encapsulation on the tunnel interface. By default, GRE is disabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>Use IPsec encapsulation on the tunnel interface. By default, IPsec is enabled. If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
</tbody>
</table>
| IPsec Preference       | Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.  
  Range: 0 through 4294967295 Default: 0 |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPsec Weight</strong></td>
<td>Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.</td>
</tr>
<tr>
<td><strong>Range</strong>: 1 through 255</td>
<td><strong>Default</strong>: 1</td>
</tr>
<tr>
<td><strong>Carrier</strong></td>
<td>Select the carrier name or private network identifier to associate with the tunnel.</td>
</tr>
<tr>
<td><strong>Values</strong>: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default</td>
<td><strong>Default</strong>: default</td>
</tr>
<tr>
<td><strong>Bind Loopback Tunnel</strong></td>
<td>Enter the name of a physical interface to bind to a loopback interface.</td>
</tr>
<tr>
<td><strong>Last-Resort Circuit</strong></td>
<td>Select to use the tunnel interface as the circuit of last resort.</td>
</tr>
<tr>
<td><strong>NAT Refresh Interval</strong></td>
<td>Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. <strong>Range</strong>: 1 through 60 seconds <strong>Default</strong>: 5 seconds</td>
</tr>
<tr>
<td><strong>Hello Interval</strong></td>
<td>Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. <strong>Range</strong>: 100 through 10000 milliseconds <strong>Default</strong>: 1000 milliseconds (1 second)</td>
</tr>
<tr>
<td><strong>Hello Tolerance</strong></td>
<td>Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.</td>
</tr>
<tr>
<td><strong>Range</strong>: 12 through 60 seconds</td>
<td><strong>Default</strong>: 12 seconds</td>
</tr>
</tbody>
</table>

**CLI equivalent:**

```bash
vpn 0
  interface interface-name tunnel-interface allow-service service-name
  bind interface-name
    carrier carrier-name
  color color encapsulation (gre | ipsec)
  preference number
  weight number hello-interval milliseconds hello-tolerance seconds last-resort-circuit
  max-control-connections number nat-refresh-interval seconds vbond-as-stun-server
```

**Configure the Interface as a NAT Device**

To configure an interface to act as a NAT device, select the NAT tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAT</strong></td>
<td>Click On to have the interface act as a NAT device.</td>
</tr>
<tr>
<td><strong>Refresh Mode</strong></td>
<td>Select how NAT mappings are refreshed, either outbound or bidirectional (outbound and inbound).</td>
</tr>
<tr>
<td><strong>Default</strong>: Outbound</td>
<td></td>
</tr>
</tbody>
</table>

---

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
Specify when NAT translations over UDP session times out.

**Range:** 1 through 65536 minutes  
**Default:** 1 minutes

**RFC Timeout**

Specify when NAT translations over TCP session times out.

**Range:** 1 through 65536 minutes  
**Default:** 60 minutes (1 hour)

**Block ICMP**

Select On to block inbound ICMP error messages. By default, a vEdge router acting as a NAT device receives these error messages.

**Default:** Off

**Respond to Ping**

Select On to have the vEdge router respond to ping requests to the NAT interface's IP address that are received from the public side of the connection.

To create a port forwarding rule, click Add New Port Forwarding Rule and configure the following parameters. You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

**Table 187:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port Start Range | Enter a port number to define the port or first port in the range of interest.  
**Range:** 0 through 65535 |
| Port End Range | Enter the same port number to apply port forwarding to a single port, or enter the larger number to apply it to a range or ports.  
**Range:** 0 through 65535 |
| Protocol | Select the protocol to which to apply the port-forwarding rule, either TCP or UDP. To match the same ports for both TCP and UDP traffic, configure two rules. |
| VPN | Specify the private VPN in which the internal server resides. This VPN is one of the VPN identifiers in the overlay network.  
**Range:** 0 through 65535 |
| Private IP | Specify the IP address of the internal server to which to direct traffic that matches the port-forwarding rule. |

To save a port forwarding rule, click Add.

To save the feature template, click Save.

**CLI equivalent:**

```console
vbp vpn vpn-id  
interface interface-name nat block-icmp-error port-forward port-start port-number1 port-end port-number2 proto (tcp | udp) private-ip-address ip-address private-vpn vpn-id refresh (bi-directional | outbound) respond-to-ping tcp-timeout minutes udp-timeout minutes
```
**Apply Access Lists**

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

*Table 188:*

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

*CLI equivalent:*

```plaintext
vpn 0
  interface pppnumber access-list acl-name (in | out)
    ipv6 access-list acl-name (in | out)
    policer policer-name (in | out)
    rewrite-rule name
```

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:

*Table 189:*

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. <em>Range: 576 through 1804</em> <em>Default: 1500 bytes</em></td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TPC SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None</td>
</tr>
<tr>
<td>Clear Don't Fragment</td>
<td>Click On to clear the Don't Fragment bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of the physical interface on the same router that connects to the WAN transport circuit. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Tracker</td>
<td>Enter the name of a tracker to track the status of transport interfaces that connect to the internet.</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```bash
cipher
vpn vpn-id interface interface-name clear-dont-fragment icmp-redirect-disable mac-address mac-address mtu bytes tcp-mss-adjust bytes tloc-extension interface-name tracker tracker-name
```

**Release Information**


**VPN Interface PPP Ethernet**

Use the VPN Interface PPP Ethernet template for vEdge Cloud and vEdge router devices.

Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two nodes. PPP properties are associated with a PPPoE-enabled interface on vEdge routers to connect multiple users over an Ethernet link.

To configure PPPoE on vEdge routers using vManage templates:

1. Create a VPN Interface PPP Ethernet feature template to configure a PPPoE-enabled interface as described in this article.
2. Create a VPN Interface PPP feature template to configure PPP parameters for the PPP virtual interface. See the VPN Interface PPP help topic.
3. Optionally, create a VPN feature template to modify the default configuration of VPN 0. See the VPN help topic.
Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
6. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface PPP.
7. From the VPN Interface PPP Ethernet drop-down, click Create Template. The VPN Interface PPP Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface PPP parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure a Basic PPPoE-Enabled Interface**

To create a PPPoE-enabled interface on a vEdge router, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure the interface.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the PPPoE-enabled interface.</td>
</tr>
</tbody>
</table>
**Parameter Name** | **Description**
---|---
Interface Name* | Enter the name of the physical interface in VPN 0 to associate with the PPP interface. For IOS XE routers, you must spell out the interface names completely (for example, GigabitEthernet0/0/0), and you must configure all the router's interfaces even if you are not using them so that they are configured in the shutdown state and so that all default values for them are configured.

Description | Enter a description of the PPPoE-enabled interface.

IPv4 Configuration* | To configure a static address, click Static and enter an IPv4 address.
To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1.

IPv6 Configuration* | To configure a static address for an interface in VPN 0, click Static and enter an IPv6 address.
To set the interface as a DHCP client so that the interface to receive its IP address from a DHCP server, click Dynamic. You can optionally set the DHCP distance to specify the administrative distance of routes learned from a DHCP server. The default DHCP distance is 1. You can optionally enable DHCP rapid commit, to speed up the assignment of IP addresses.

DHCP Helper | Enter up to eight IP addresses for DHCP servers in the network, separated by commas, to have the interface be a DHCP helper. A DHCP helper interface forwards BOOTP (Broadcast) DHCP requests that it receives from the specified DHCP servers.

Bandwidth Upstream | For transmitted traffic, set the bandwidth above which to generate notifications. Range: 1 through \((2^{32} / 2) - 1\) kbps

Bandwidth Downstream | For received traffic, set the bandwidth above which to generate notifications. Range: 1 through \((2^{32} / 2) - 1\) kbps

To save the feature template, click Save.

**CLI equivalent:**
```bash
vpn 0
  interface pppnumber bandwidth-downstream kbps bandwidth-upstream kbps description text
dhcp-helper ip-address
  ( ip address ipv4-prefix/length | ip-dhcp-client [dhcp-distance number])
  ( ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number] [dhcp-rapid-commit])
  pppoe-client ppp-interface pppnumber
  [no] shutdown
```

**Apply Access Lists**

To configure a shaping rate to a PPPoE-enabled interface and to apply a QoS map, a rewrite rule, access lists, and policers to the interface, select the ACL/QOS tab and configure the following parameters:
### Table 192:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping Rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS Map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
<tr>
<td>Rewrite Rule</td>
<td>Click On, and specify the name of the rewrite rule to apply on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress ACL – IPv6</td>
<td>Egress ACL – IPv6</td>
</tr>
<tr>
<td>Egress ACL – IPv6</td>
<td>Egress ACL – IPv6</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature temp

**CLI equivalent:**

```
vpn 0
  interface pppnumber access-list acl-list (in | out)
  policer policer-name (in | out)
  qos-map name rewrite-rule name shaping-rate name
```

### Configure Other Interface Properties

To configure other interface properties, select the Advanced tab and configure the following properties:

### Table 193:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplex</td>
<td>Choose full or half to specify whether the interface runs in full-duplex or half-duplex mode. Default: Full</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specify a MAC address to associate with the interface, in colon-separated hexadecimal notation.</td>
</tr>
<tr>
<td>IP MTU</td>
<td>Specify the maximum MTU size of packets on the interface. Range: 576 through 1804 Default: 1500 bytes</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PMTU Discovery</td>
<td>Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Select a setting for bidirectional flow control, which is a mechanism for temporarily stopping the transmission of data on the interface. Values: autonet, both, egress, ingress, none. Default: autoneg.</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes. Default: None.</td>
</tr>
<tr>
<td>Speed</td>
<td>Specify the speed of the interface, for use when the remote end of the connection does not support autonegotiation. Values: 10, 100, or 1000 Mbps. Default: Autonegotiate (10/100/1000 Mbps).</td>
</tr>
<tr>
<td>Static Ingress QoS</td>
<td>Specify a queue number to use for incoming traffic. Range: 0 through 7.</td>
</tr>
<tr>
<td>ARP Timeout</td>
<td>Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours). Default: 1200 seconds (20 minutes).</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
<tr>
<td>Power over Ethernet</td>
<td>Click On to enable PoE on the interface.</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Click Disable to disable ICMP redirect messages on the interface. By default, an interface allows ICMP redirect messages.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI equivalent:**

```sh
test 0
  interface pppnumber arp-timeout seconds
  [no] autonegotiate duplex (full | half)
  flow-control control icmp-redirect-disable mac-address mac-address mtu bytes pmtu
  pppoe-client
  ppp-interface pppnumber speed speed
  static-ingress-qos number tcp-mss-adjust bytes tloc-extension interface-name
```
**Release Information**


**VPN Interface SVI**

Use the VPN Interface SVI template for Cisco IOS XE routers running the SD-WAN software. You configure a switch virtual interface (SVI) to configure a VLAN interface.

To configure DSL interfaces on Cisco routers using vManage templates, create a VPN Interface SVI feature template to configure VLAN interface parameters, as described in this article.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ▶ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. If you are configuring the SVI in the transport VPN (VPN 0):
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface SVI.
6. If you are configuring the SVI in a service VPN (VPNs other than VPN 0):
   1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.
   2. In the Service VPN drop-down, enter the number of the service VPN.
   3. Under Additional VPN Templates, located to the right of the screen, click VPN Interface SVI.
7. From the VPN Interface SVI drop-down, click Create Template. The VPN Interface SVI template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VLAN Interface parameters.
8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 194:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>
Apply Access Lists

To apply a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.</td>
</tr>
<tr>
<td>Egress ACL – IPv4</td>
<td>Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.</td>
</tr>
<tr>
<td>Ingress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being received on the interface.</td>
</tr>
<tr>
<td>Egress Policer</td>
<td>Click On, and specify the name of the policer to apply to packets being transmitted on the interface.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

Configure VRRP

To have an interface run the Virtual Router Redundancy Protocol (VRRP), which allows multiple routers to share a common virtual IP address for default gateway redundancy, select the VRRP tab. Then click Add New VRRP and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>Enter the virtual router ID, which is a numeric identifier of the virtual router. You can configure a maximum of 24 groups. \textit{Range:} 1 through 255</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter the priority level of the router. There router with the highest priority is elected as master. If two vEdge routers have the same priority, the one with the higher IP address is elected as master. \textit{Range:} 1 through 254 \textit{Default:} 100</td>
</tr>
<tr>
<td>Timer</td>
<td>Specify how often the VRRP master sends VRRP advertisement messages. If slave routers miss three consecutive VRRP advertisements, they elect a new master. \textit{Range:} 1 through 3600 seconds \textit{Default:} 1 second</td>
</tr>
</tbody>
</table>
By default, VRRP uses the state of the service (LAN) interface on which it is running to determine which vEdge router is the master virtual router. If a vEdge router loses all its WAN control connections, the LAN interface still indicates that it is up even though the router is functionally unable to participate in VRRP. To take WAN side connectivity into account for VRRP, configure one of the following:

- **Track OMP**—Click On for VRRP to track the Overlay Management Protocol (OMP) session running on the WAN connection. If the master VRRP router loses all its OMP sessions, VRRP selects a new default gateway from those that have at least one active OMP session.

- **Track Prefix List**—Track both the OMP session and a list of remote prefixes, which is defined in a prefix list configured on the local router. If the master VRRP router loses all its OMP sessions, VRRP failover occurs as described for the Track OMP option. In addition, if reachability to one of the prefixes in the list is lost, VRRP failover occurs immediately, without waiting for the OMP hold timer to expire, thus minimizing the amount of overlay traffic is dropped while the vEdge routers determine the VRRP master.

**Add ARP Table Entries**

To configure static Address Resolution Protocol (ARP) table entries on the interface, select the ARP tab. Then click Add New ARP and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the ARP entry in dotted decimal notation or as a fully qualified host name.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address in colon-separated hexadecimal notation.</td>
</tr>
</tbody>
</table>

To save the ARP configuration, click Add.

To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following properties:
Table 199:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TPCSYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 552 to 1460 bytes Default: None</td>
</tr>
<tr>
<td>ARP Timeout</td>
<td>Specify how long it takes for a dynamically learned ARP entry to time out. Range: 0 through 2678400 seconds (744 hours) Default: 1200 (20 minutes)</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

Release Information

Introduced in vManage NMS in Release 18.3.

VPN Interface T1/E1

Use the VPN Interface T1/E1 template for Cisco IOS XE routers running the SD-WAN software.

To configure the T1/E1 interfaces in a VPN using vManage templates:

1. Create a VPN Interface T1/E1 feature template to configure T1/E1 interface parameters, as described in this article.
2. Create a T1/E1 Controller template to configure the T1 or E1 network interface module (NIM) parameters. See the T1/E1 Controller help topic.
3. Create a VPN feature template to configure VPN parameters. See the VPN help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the template.
5. To create a template for VPN 0 or VPN 512:
   1. Click the Transport & Management VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.
   2. Under Additional VPN 0 Templates, located to the right of the screen, click VPN Interface.
   3. From the VPN Interface drop-down, click Create Template. The VPN Interface T1/E1 template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.

6. To create a template for VPNs 1 through 511, and 513 through 65530:
1. Click the Service VPN tab located directly beneath the Description field, or scroll to the Service VPN section.

2. Click the Service VPN drop-down.

3. Under Additional VPN templates, located to the right of the screen, click VPN Interface.

4. From the VPN Interface drop-down, click Create Template. The VPN Interface Ethernet template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN Interface Ethernet parameters.

7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

**Table 200:**

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

**Configure Basic Interface Functionality**

To configure basic interface functionality in a VPN, select the Basic Configuration tab and configure the following parameters. Parameters marked with an asterisk are required to configure an interface.

**Table 201:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td>Interface name*</td>
<td>Enter a name for the interface. The name should be in the format <code>serial slot / subslot / port : channel-group</code>. You must also configure a number for the channel group in the T1/E1 Controller feature configuration template.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>Enter an IPv4 address.</td>
</tr>
</tbody>
</table>
Create a Tunnel Interface

You can configure up to four tunnel interfaces. This means that each vEdge router can have up to four TLOCs. For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0.

To configure a tunnel interface, select the Interface Tunnel tab and configure the following parameters:

**Table 202:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Interface</td>
<td>Click On to create a tunnel interface.</td>
</tr>
<tr>
<td>Color</td>
<td>Select a color for the TLOC.</td>
</tr>
<tr>
<td>Control Connection</td>
<td>If the router has multiple TLOCs, click No to have the tunnel not establish a TLOC. The default is On, which establishes a control connection for the TLOC.</td>
</tr>
<tr>
<td>Maximum Control Connections</td>
<td>Specify the maximum number of vSmart controllers that the WAN tunnel interface can connect to. To have the tunnel establish no control connections, set the number to 0. Range: 0 through 8 Default: 2</td>
</tr>
<tr>
<td>vBond As Stun Server</td>
<td>Click On to enable Session Traversal Utilities for NAT (STUN) to allow the tunnel interface to discover its public IP address and port number when the vEdge router is located behind a NAT.</td>
</tr>
<tr>
<td>Exclude Controller Group List</td>
<td>Set the vSmart controllers that the tunnel interface is not allowed to connect to. Range: 0 through 100</td>
</tr>
<tr>
<td>vManage Connection Preference</td>
<td>Set the preference for using a tunnel interface to exchange control traffic with the vManage NMS. Range: 0 through 8 Default: 5</td>
</tr>
</tbody>
</table>
### Description

Click On to enable port hopping, or click Off to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template. Default: Enabled (on vEdge routers); disabled (on vManage NMSs and vSmart controllers).

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Hop</td>
<td>Select to characterize the tunnel interface as a low-bandwidth link.</td>
</tr>
<tr>
<td>Allow Service</td>
<td>Select On or Off for each service to allow or disallow the service on the interface.</td>
</tr>
</tbody>
</table>

To configure additional tunnel interface parameters, click Advanced Options:

### Table 203:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation</td>
<td>Select the encapsulation type to use on the tunnel interface, either IPsec or GRE. The default is IPsec.</td>
</tr>
<tr>
<td></td>
<td>If you select both IPsec and GRE encapsulations, two TLOCs are created for the tunnel interface that have the same IP addresses and colors, but that differ by their encapsulation.</td>
</tr>
<tr>
<td>IPsec</td>
<td>By default, IPsec is enabled on the tunnel interface. To disable IPsec, click Off.</td>
</tr>
<tr>
<td>IPsec Preference</td>
<td>Specify a preference value for directing traffic to the tunnel. A higher value is preferred over a lower value.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 through 4294967295 Default: 0</td>
</tr>
<tr>
<td>IPsec Weigh</td>
<td>Enter a weight to use to balance traffic across multiple TLOCs. A higher value sends more traffic to the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 255 Default: 1</td>
</tr>
<tr>
<td>Carrier</td>
<td>Select the carrier name or private network identifier to associate with the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default</td>
</tr>
<tr>
<td>Bind Loopback</td>
<td>Enter the name of a physical interface to bind to a loopback interface.</td>
</tr>
<tr>
<td>Tunnel</td>
<td></td>
</tr>
<tr>
<td>Last-Resort</td>
<td>Select to use the tunnel interface as the circuit of last resort.</td>
</tr>
<tr>
<td>Circuit</td>
<td></td>
</tr>
<tr>
<td>NAT Refresh Interval</td>
<td>Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Hello Tolerance      | Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down.  
  *Range*: 12 through 60 seconds  
  *Default*: 12 seconds |

To save the feature template, click Save.

**Apply Access Lists and QoS Parameters (on vEdge Routers)**

To configure a shaping rate to a router interface and to apply a QoS map, a rewrite rule, access lists, and policers to a router interface, select the ACL tab and configure the following parameters:

**Table 204:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shaping Rate</td>
<td>Configure the aggregate traffic transmission rate on the interface to be less than line rate, in kilobits per second (kbps).</td>
</tr>
<tr>
<td>QoS Map</td>
<td>Specify the name of the QoS map to apply to packets being transmitted out the interface.</td>
</tr>
</tbody>
</table>
| Rewrite Rule   | Click On, and specify the name of the rewrite rule to apply on the interface.  
  Click On, and specify the name of the access list to apply to IPv4 packets being received on the interface.  
  Click On, and specify the name of the access list to apply to IPv4 packets being transmitted on the interface.  
  Click On, and specify the name of the access list to apply to IPv6 packets being received on the interface.  
  Click On, and specify the name of the access list to apply to IPv6 packets being transmitted on the interface.  
  Click On, and specify the name of the policer to apply to packets received on the interface.  
  Click On, and specify the name of the policer to apply to packets being transmitted on the interface. |

To save the feature template, click Save.

**Configure Other Interface Properties**

To configure other interface properties, select the Advanced tab and configure the following parameters:

**Table 205:**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMTU Discovery</td>
<td>Click On to enable path MTU discovery on the interface. PMTU determines the largest MTU size that the interface supports so that packet fragmentation does not occur.</td>
</tr>
<tr>
<td><strong>Parameter Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>TCP MSS</td>
<td>Specify the maximum segment size (MSS) of TCP SYN packets passing through the vEdge router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. <em>Range</em>: 552 to 1460 bytes <em>Default</em>: None</td>
</tr>
<tr>
<td>Clear-Dont-Fragment</td>
<td>Click On to clear the Don't Fragment (DF) bit in the IPv4 packet header for packets being transmitted out the interface. When the DF bit is cleared, packets larger than that interface's MTU are fragmented before being sent.</td>
</tr>
<tr>
<td>Static Ingress QoS</td>
<td>Specify a queue number to use for incoming traffic. <em>Range</em>: 0 through 7</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>Click Off to turn off autonegotiation. By default, an interface runs in autonegotiation mode.</td>
</tr>
<tr>
<td>TLOC Extension</td>
<td>Enter the name of a physical interface on the same router that connects to the WAN transport. This configuration then binds this service-side interface to the WAN transport. A second vEdge router at the same site that itself has no direct connection to the WAN (generally because the site has only a single WAN connection) and that connects to this service-side interface is then provided with a connection to the WAN.</td>
</tr>
</tbody>
</table>

**Release Information**

Introduced in vManage NMS Release 18.2.

**WiFi Radio**

Use the WiFi Radio template for all vEdge router devices that support wireless LANs (WLANs), including the vEdge 100wm router.

To configure WLAN radio parameters using vManage templates:

1. Create a WiFi Radio template to configure WLAN radio parameters, as described in this article.
2. Create a Wifi SSID template to configure an SSID and related parameters. See the WiFi SSID help topic.

**Navigate to the Template Screen and Name the Template**

1. In vManage NMS, select the Configuration ▶ Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select the vEdge router model that supports wireless LANs (WLANs).
5. Click the WLAN tab located directly beneath the Description field, or scroll to the WLAN section.
6. From the WiFi Radio drop-down, click Create Template. The WiFi Radio template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining WiFi Radio parameters.
7. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

8. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 206:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Configure the WLAN Radio Frequency

To configure the WLAN radio frequency, in the Basic Configuration tab, configure the following parameters. Parameters marked with an asterisk are required to configure the radio.

Table 207:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Radio*</td>
<td>Select the radio band. It can be 2.4 GHz or 5 GHz.</td>
</tr>
<tr>
<td>Country*</td>
<td>Select the country where the router is installed.</td>
</tr>
<tr>
<td>Channel Bandwidth</td>
<td>Select the IEEE 802.11n and 802.11ac channel bandwidth. For a 5-GHz radio band, the default value is 80 MHz, and for 2.4 GHz, the default is 20 MHz.</td>
</tr>
<tr>
<td>Channel</td>
<td>Select the radio channel. The default is &quot;auto&quot;, which automatically selects the best channel. For 5-GHz radio bands, you can configure dynamic frequency selection (DFS) channels.</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>Select the guard interval. For a 5-GHz radio band, the default value is the short guard interval (SGI) of 400 ns, and for 2.4 GHz, the default is 800 ns.</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI equivalent:
WiFi SSID

You can use the WiFi SSID template for all vEdge router devices that support wireless LANs (WLANs), including vEdge 100v routers.

To configure SSIDs on the WLAN radio using vManage templates:

1. Create a WiFi SSID template to configure the VAP interfaces to use as SSIDs, as described in this article.
2. Create a WiFi Radio template to configure WLAN radio parameters. See the Configuration ► Templates ► WiFi Radio help topic.
3. Create a Bridge template to assign the VAP interface to a bridging domain. See the Configuration ► Templates ► Bridge help topic.
4. Create a device template that incorporates the WiFi Radio feature template and the Wifi SSID feature template. See the Configuration ► Templates help topic.

Navigate to the Template Screen and Name the Template

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, click Create Template.
3. From the Create Template drop-down, select From Feature Template.
4. From the Device Model drop-down, select a vEdge router model that supports wireless LANs (WLANs).
5. Click the WLAN tab located directly beneath the Description field, or scroll to the WLAN section.
6. Under Additional WiFi Radio Templates, located to the right of the screen, click WiFi SSID.
7. From the WiFi SSID drop-down, click Create Template. The WiFi SSID template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining WiFi SSID parameters.

8. In the Template Name field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

9. In the Template Description field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 208:

<table>
<thead>
<tr>
<th>Parameter Scope</th>
<th>Scope Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Specific (indicated by a host icon)</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>Global (indicated by a globe icon)</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

WLAN SSID Configuration

To configure SSIDs on a vEdge router, configuring the following parameters in the Basic Configuration tab. Parameters marked with an asterisk are required to configure the SSIDs.

Table 209:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name*</td>
<td>Select the VAP interface name.</td>
</tr>
<tr>
<td>Shutdown*</td>
<td>Click No to enable the interface.</td>
</tr>
<tr>
<td>Description (optional)</td>
<td>Enter a description for the interface.</td>
</tr>
<tr>
<td>SSID*</td>
<td>Enter the name of the SSID. It can be a string from 4 through 32 characters. The SSID must be unique. You can configure up to four SSIDs. Each SSID is called a virtual access point (VAP) interface. To a client, each VAP interfaces appears as a different access point (AP) with its own SSID. To provide access to different networks, assign each VAP to a different VLAN.</td>
</tr>
<tr>
<td>Maximum Clients</td>
<td>Enter the maximum number of clients allowed to connect to the WLAN. Range: 1 through 50 Default: 25</td>
</tr>
</tbody>
</table>
### Parameter Name | Description
--- | ---
Data Security | Select the security type to enable user authentication or enterprise WPA security. For user authentication, select from WPA Personal, WPA/WPA2 Personal, or WPA2 Personal, and then enter a clear text or an AES-encrypted key. For enterprise security, select from WPA Enterprise, WPA/WPA2 Enterprise, or WPA2 Enterprise, and then enter a RADIUS server tag.

RADIUS Server | If you select one of the enterprise security methods based on using a RADIUS authentication server, enter the RADIUS server tag.

WPA Personal Key | If you select one of the personal security methods based on preshared keys, enter either a clear text or an AES-encrypted password.

Management Security | If you select one of the WPA2 security methods, select the encryption of management frames to be none, optional, or required.

To save the feature template, click Save.

**CLI equivalent:**

```
wlan frequency interface vapnumber data-security security
description text mgmt-security security radius-servers tag
no shutdown
  ssid ssid wpa-personal-key password
```

**Release Information**

Introduced in vManage NMS Release 16.3.

---

**Add Branch Sites**

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.
Add Data Centers

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

Add Network Circuits

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

Configure Centralized Policy

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs
You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

For more information about the centralized policy components, see Configuring Centralized Control Policy. For information about application-aware routing policy components, see Configuring Application-Aware Routing.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen.
2. Select the Centralized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen displays.

**Step 2: Configure Groups of Interest**

In Create Groups of Interest, create lists of groups to use in centralized policy:
1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:

   - Application
   - Color
   - Data Prefix
   - Policer
   - Prefix
   - Site
   - SLA Class
• TLOC
• VPN

1. In the right pane, click the New button. The New List portion of the screen opens. For example:

2. Enter a name for the list, and enter or select the components to include in the list. For application lists, note that the Google_Apps and Microsoft_Apps lists are preconfigured, and you cannot edit or delete them. For example:
3. Click Add to create the new list.

4. Repeat Steps 1 through 4 to create additional lists.

5. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

6. Click Next to move to Configure Topology and VPN Membership in the wizard.

**Step 3: Configure Topology and VPN Membership**

When you first open the Configure Topology and VPN Membership screen, the Topology tab is selected by default:
To configure topology and VPN membership:

1. To configure a topology policy component:
   1. In the Topology tab, click the Add Topology drop-down.
   2. Select the desired network topology:
3. Enter a name and description for the topology, and select the VPN list to which the topology applies.
4. Click the New button, and enter the information for the topology component.
5. Enter a name for the topology component, and enter or select the components to include in it.
6. Click Save.

2. To configure a VPN membership policy component:
   1. In the VPN Membership tab, click Add VPN Membership Policy:
2. In the Update VPN Membership Policy popup, enter a name and description of the VPN membership, and select site lists and VPN lists. To create new lists, click Add List.

3. Click Save.

3. To edit, copy, or delete an existing topology or VPN membership policy, select it and click the Edit, Copy, or Trash Bin icon in the Action column.

4. Click Next to move to Configure Traffic Rules in the wizard.

**Step 4: Configure Traffic Rules**

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default:
To configure traffic rules:

1. In the Application-Aware Routing tab, select the desired policy type—Application-Aware Routing, Traffic Data, or Cflowd.

2. Click the Add Policy drop-down.

3. To import an existing policy, select Import Existing. In the Import Existing Data Policy popup, select the name of the file containing the data policy. Then click Import.

4. To create a new policy, select Create New, and in the left pane, click Sequence Type.

5. For an application-aware routing policy:
1. In the right pane, click Sequence Rule.

2. Add the match and action rules. You can select the modifiers OR, AND, or EXACT to focus the scope of a rule. OR applies to multiple community lists and is valid for all platforms; AND and EXACT apply to only one community list at a time and are not valid for vEdge devices.

3. Add additional sequences as needed. Drag and drop sequences to re-order them.

4. Click Save Application-Aware Routing Policy.

6. For a traffic data policy:

1. From the Add Data Policy popup, select the policy type:

   - Application Firewall
     - Direct application traffic to a firewall.
   - QoS
     - Class/GoS maps for packet forwarding.
   - Service Chaining
     - Rerouting data traffic through firewalls, load balancers, and other devices.
   - Traffic Engineering
     - Direct control traffic along a desired path.
   - Custom
     - Create a custom policy.

   2. In the right pane, click Sequence Rule.

   3. Add the match and action rules.
4. Add additional sequences as needed. Drag and drop sequences to re-order them.

5. Click Save Data Policy.

7. For cflowd policy:
   1. To configure the cflowd template, enter values for the active flow timeout, inactive flow timeout, flow refresh interval, and sampling interval.
   2. To configure a collector list, click Add New Collector. Enter the VPN ID where the collector is located, its IP address, port number, transport protocol, and source interface. Click Add.
   3. Click Save Cflowd Policy.

8. Click Next to move to Apply Policies to Sites and VPNs in the wizard.

**Step 5: Apply Policy to Sites and VPNs**

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs:
1. Enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. Enter a description of the policy. This field is mandatory, and it can contain any characters and spaces. It can contain up to 2048 characters.

3. From the Topology bar, select the tab that corresponds to the type of policy block—Topology, Application-Aware Routing, Traffic Data, or Cflowd. The table then lists policies that you have created for that type of policy block.

4. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:
1. For a Topology policy block, click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Select one or more site lists, and select one or more VPN lists. Click Add.

2. For an Application-Aware Routing policy block, click Add New Site List and VPN list. Select one or more site lists, and select one or more VPN lists. Click Add.

3. For a Traffic Data policy block, click Add New Site List and VPN List. Select the direction for applying the policy (From Tunnel, From Service, or All), select one or more site lists, and select one or more VPN lists. Click Add.

4. For a cflowd policy block, click Add New Site List. Select one or more site lists, Click Add.

5. Click Preview to view the configured policy. The policy is displayed in CLI format.

6. Click Save Policy. The Configuration Policies screen opens, and the policies table includes the newly created policy.

## Configure Global Parameters

You configure centralized policy with a configuration wizard. The wizard is a UI policy builder that consists of four screens to configure and modify the following centralized policy components:

- Groups of interest, also called lists
- Topologies and VPN membership
- Traffic rules
- Applying policies to sites and VPNs

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply centralized policies by activating them, as described later in the article, to push the policies to all reachable vSmart controllers.

## Configure Localized Policy

You configure localized policy with a configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

- Groups of interest, also called lists
- Forwarding classes to use for QoS
- Access control lists (ACLs)
- Route policies
- Policy settings
You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

You apply localized policies to specific vEdge router interfaces. You associate a localized policy with an interface in the VPN Interface Bridge, VPN Interface Ethernet, VPN Interface GRE, VPN Interface PPP, or VPN Interface PPP Ethernet feature configuration template.

For more information about the localized policy components, see Configuring Localized Data Policy for IPv4 and Configuring Localized Data Policy for IPv6.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen.
2. Select the Localized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen displays.

**Step 2: Configure Groups of Interest**

In the Create Groups of Interest screen, create lists to use in localized policy:
1. In the left pane, select the type of list to use with the localized policy. It can be one of the following:

   - AS Path
   - Community
   - Data Prefix
   - Extended Community
   - Mirror
   - Policer
- Prefix

1. In the right pane, click the New button. The New List portion of the screen opens. For example:

2. Enter a name for the list, and enter or select the components to include in the list. For information entering AS path, community and extended community, and data prefix and prefix values, see Configuring Localized Control Policy . For information about entering mirroring and policer parameters, see Configuring Localized Data Policy for IPv4 .

3. Click Add to create the new list.

4. Repeat Steps 1 through 4 to create additional lists.

5. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.
6. Click Next to move to Configure Forwarding Classes/QoS in the wizard. When you first open this screen, the QoS tab is selected by default.

**Step 3: Configure Forwarding Classes for QoS**

When you first open the Forwarding Classes/QoS screen, the QoS tab is selected by default:

To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
   1. In the QoS tab, click the Add QoS drop-down.
2. Select Create New.
3. Enter a name and description for the QoS mapping.
4. Click Add Queue. The Add Queue popup displays:

![Add Queue popup]

5. Select the queue number from the Queue drop-down.
6. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.
7. Click Save.

2. To import an existing QoS mapping:
1. In the QoS tab, click the Add QoS drop-down.
2. Select Import Existing.
3. Select a QoS mapping.
4. Click Import.

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the More Actions icon to the right of the row, and select the desired action.

4. To configure policy rewrite rules for the QoS mapping:
   1. In the QoS tab, click the Add Rewrite Policy drop-down.
   2. Select Create New.
   3. Enter a name and description for the rewrite rule.
   5. Select a class from the Class drop-down.
   6. Select the priority (Low or High) from the Priority drop-down.
   7. Enter the DSCP value (0 through 63) in the DSCP field.
   8. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field to include an 802.1p marking in the packet.
   9. Click Save.

5. To import an existing rewrite rule:
   1. In the QoS tab, click the Add Rewrite Policy drop-down.
   2. Select Import Existing.
   3. Select a rewrite rule.
   4. Click Import.

6. Click Next to move to Configure Access Lists in the wizard.

**Step 4: Configure ACLs**

In the Configure Access Control Lists screen, configure ACLs:
1. To create a new IPv4 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv4 ACL Policy:
2. To create a new IPv6 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv6 ACL Policy.

3. Enter a name and description for the ACL.

4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.

5. Double-click the Access Control List box, and type a name for the ACL.

6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.

7. Click a match condition.

8. On the left, enter the values for the match condition.

9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
   1. Click Default Action in the left pane.
   2. Click the Pencil icon.
   3. Change the default action to Accept.
   4. Click Save Match and Actions.
17. Click Next to move to Configure Route Policy in the wizard.

**Step 5: Configure Route Policies**

In Configure Route Policy, configure route policies:
1. In the Add Route Policy tab, select Create New.
2. Enter a name and description for the route policy.
3. In the left pane, click Add Sequence Type. A Route box is displayed in the left pane.
4. Double-click the Route box, and type a name for the route policy.
5. In the right pane, click Add Sequence Rule to create a single sequence in the policy. The Match tab is selected by default.
6. Click a match condition.
7. On the left, enter the values for the match condition. You can select the modifiers OR, AND, or EXACT to focus the scope of a rule. OR applies to multiple community lists and is valid for all platforms; AND and EXACT apply to only one community list at a time and are not valid for vEdge devices.

8. On the right enter the action or actions to take if the policy matches.

9. Repeat Steps 6 through 8 to add match–action pairs to the route policy.

10. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.

11. To remove a match–action pair from the route policy, click the X in the upper right of the condition.

12. Click Save Match and Actions to save a sequence rule.

13. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.

14. To copy, delete, or rename an route policy sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.

15. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
   1. Click Default Action in the left pane.
   2. Click the Pencil icon.
   3. Change the default action to Accept.
   4. Click Save Match and Actions.

16. Click Next to move to Policy Overview in the wizard.

**Step 6: Configure Policy Settings**

In Policy Overview, configure policy settings:
1. Enter a name and description for the route policy.

2. To enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN, click Netflow.

3. To enable application visibility so that a vEdge router can monitor and track the applications running on the LAN, click Application.

4. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from transport-side interfaces, click Cloud QoS.

5. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from service-side interfaces, click Cloud QoS Service Side.

6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.
7. To configure how often packets flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

8. Click Preview to view the full policy in CLI format.

9. Click Save Policy.
## Dashboard

Use the dashboard screen to monitor, at a glance, the overall health of the Viptela overlay network.

### Top Bar

The top bar is located at the top of every vManage screen and includes the following screen elements:

- **Menu icon**—Click the icon to expand or collapse the vManage menu. The vManage menu is closed by default.

- **vManage application server logo.** To change the logo, see How to Load a Custom Logo onto the vManage Web Application Server.

- **Cloud onRamp icon**—Enables Cloud onRamp service to optimize access to cloud applications. When Cloud onRamp service is enabled, the icon turns blue.

- **Tasks icon**—Click on the icon to see a list of all active and completed tasks started from the vManage NMS. While the task is in progress, the Tasks tab displays a counter on the top. When the task is completed, the count disappears and Completed Tasks count is incremented. To view details about any task, click the task to display its Status screen.

- **Alarm bell icon**—Displays the total count of all active alarms. Click on the icon to see a list of all active and cleared alarms. To view details about any alarm, click the alarm to display its Alarms Details screen.

- **Help**—Links to product help, software version information about the vManage NMS software, and current time and timezone on the vManage server.

- **Hostname**—Hostname of the vManage NMS that you are logged into.

- **User profile drop-down**—Click to sign out or edit user-related options in your profile.
Device Pane

The Device pane, which runs across the top of the Dashboard screen, displays all control connections from the vManage NMS to the vSmart controllers, WAN Edge routers, and vBond orchestrators in the overlay network. It also displays the status of the vManage NMSs in the network.

For each device, the Device pane shows:

- Total number of connections.
- Number of up connections.
- Number of down connections.
Click the number or the Up or Down arrow to display a table with detailed information for each connection. The Dashboard page automatically refreshes when the status of the members of a vManage cluster changes.

Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or to access the Tools ► SSH Terminal screen.

**Reboot Pane**

The Reboot pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Click the Reboot pane to open the Reboot popup window which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than each, each reboot option is reported separately.

In the Reboot popup window, click the Crashes tab to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

**Certificates Pane**

The Certificates pane displays the state of all certificates on all controller devices, and it shows a count of all expired or invalidated certificates. Click the Certificates pane to open the Certificate Details popup window, which displays the hostname and system IP of the device on which the certificate is installed, the certificate serial number, and its expiration date and status.

**Control Status Pane**

The Control Status pane displays whether vSmart and WAN Edge devices are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each WAN Edge router must connect to the configured maximum number of vSmart controllers.

The Control Status pane shows three counts:

- **Control Up**—Total number of devices with the required number of operational control plane connections to a vSmart controller.

- **Partial**—Total number of devices with some, but not all, operational control plane connections to vSmart controllers.

- **Control Down**—Total number of devices with no control plane connection to a vSmart controller.

Click any row to display a table with device details. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen.

**Site Health View Pane**

The Site Health View pane displays the state of a site's data connections. When a site has multiple WAN Edge routers, this pane displays the state for the entire site, not for individual devices. The Site Health View pane displays three states:

- **Full WAN Connectivity**—Total number of sites where all BFD sessions on all WAN Edge routers are in the up state.

- **Partial WAN Connectivity**—Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
• No WAN Connectivity—Total number of sites where all BFD sessions on all WAN Edge routers are in the down state. These sites have no data plane connectivity.

Click a row to display a popup window with detailed information on each site, node, or tunnel. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

**Transport Interface Distribution**

The Transport Interface Distribution pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

**WAN Edge Inventory Pane**

The WAN Edge Inventory pane provides four counts:

• Total—Total number of WAN Edge routers whose authorized serial number has been uploaded on the vManage server. The serial number is uploaded in the Configuration ► Devices screen.

• Authorized—Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid in the Configuration ► Certificates ► WAN Edge List screen.

• Deployed—Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.

• Staging—Total number of WAN Edge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These routers do not take part in any routing decisions nor do they affect network monitoring through the vManage NMS.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

**WAN Edge Health Pane**

The WAN Edge Health pane displays an aggregated view for each router state and a count of how many WAN Edge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

• Normal—Number of routers with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as normal.

• Warning—Number of routers with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as a warning.

• Error—Number of routers with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as an error.

Click the number or the state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

**Transport Health Pane**

The Transport Health pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).
From the Type drop-down, select loss, latency, or jitter.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Transport Health pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the displayed type and time period as described above.

**Top Applications Pane**

The Top Applications pane displays DPI flow information for traffic transiting WAN Edge routers in the overlay network.

Click the Filter icon to select a time period for which to display data. From the VPN drop-down list, select a VPN to display DPI information for all flows in that VPN.

Click the Expand icon to open the Top Applications pop-up window. This full-screen window displays a more detailed view of the same information. You can change the VPN and time period as described above.

**Application-Aware Routing Pane**

The Application-Aware Routing pane displays the 10 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter. So, if you choose loss, this pane shows the ten tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click Custom to display a drop-down for specifying a custom time period.

Click the Expand icon to open the Application-Aware Routing pop-up window. This full-screen window displays the 25 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter.

**FireWall Enforcement Pane**

The FireWall Enforcement pane displays the number of sessions that were inspected or dropped over the specified time period.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the FireWall Enforcement pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

**Top Signature Hits Pane**

The Top Signature Hits pane displays the Intrusion Prevention System (IPS) signature violations by severity or by count over the specified time period.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Top Signature Hits pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

**URL Filtering Pane**

The URL Filtering pane displays the number and types of URLs that were blocked or allowed over the specified time period.
Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the URL Filtering pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

**Web Server Certificate Expiration Date Notification**

When you establish a secure connection between your web browser and the vManage server using authentication certificates, you configure the time period for which the certification is valid, in the Administration ► Settings screen. At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

**Maintenance Window Alert Notification**

If an upcoming maintenance window is configured on the vManage server, in the Administration ► Settings screen, the vManage Dashboard displays a maintenance window alert notification two days before the start of the window.

**Multitenant Dashboard**

Use the multitenant dashboard screen to monitor, at a glance, the overall health of all tenants being managed by a single vManage NMS server.

**Top Bar**

The top bar is located at the top of every vManage multitenant screen and includes the following screen elements:

- **Menu icon**—Click the icon to expand or collapse the vManage menu. The vManage menu is closed by default.
- **vManage application server logo.** To change the logo, see How to Load a Custom Logo onto the vManage Web Application Server.
- **Provider Name**—Displays the service provider name. Click the Select Tenant drop-down to display information for a single tenant.
- **Alarm bell icon**—Displays the total count of all active alarms. Click on the icon to see a list of all active and cleared alarms. To view details about any alarm, click the alarm to display its Alarms Details screen.
- **Tasks icon**—Click on the icon to see a list of all active and completed tasks started from the vManage NMS. While the task is in progress, the Tasks tab displays a counter on the top. When the task is completed, the count disappears and Completed Tasks count is incremented. To view details about any task, click the task to display its Status screen.
- **Help**—Links to product help, software version information about the vManage NMS software, and current time and timezone on the vManage server.
- **Hostname**—Hostname of the vManage NMS that you are logged into.

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
• User profile drop-down—Click to sign out or edit user-related options in your profile.
Multitenant Dashboard

Dashboard

Menu

Dashboard

Monitor

Configuration

Tools

Maintenance

Administration

Tenant | Control Status
--- | ---
orange | ✅
mango | ✅
apple | ✅
**Provider Dashboard**

If you click Provider Name in the Top Bar, the Multitenant Dashboard shows the following components:

- **Device Pane**—Runs across the top of the Multitenant Dashboard screen. The Device pane displays the total number control connections from the vManage NMS to the vBond orchestrators and vManage NMSs in the overlay networks of all the tenants, and the number of up and down connections. Click the number or the Up or Down arrow to display a table with detailed information for each connection. This pane also displays the number of warning messages and the number of invalid certificates.

- **Tenants Pane**—Displays the total number of tenants and a summary of the control status, site health, vEdge router health, and vSmart controller status for all tenants.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.

- **Table of tenants in the overlay network**—To re-arrange the columns, drag the column title to the desired position.

**Tenant Dashboard**

If you select a tenant from the Provider Name drop-down in the Top Bar, the Multitenant Dashboard shows the components described below.

**Device Pane**

The Device pane, which runs across the top of the Dashboard screen, displays all control connections from the vManage NMS to the vSmart controllers and vEdge routers in the tenant’s overlay network. It also displays the status of the vManage NMSs in the network.

For each device, the Device pane shows:

- Total number of connections.
- Number of up connections.
- Number of down connections.

Click the number or the Up or Down arrow to display a table with detailed information for each connection. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or to access the Tools ► SSH Terminal screen.

**Reboot Pane**

The Reboot pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Click the Reboot pane to open the Reboot popup window which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than each, each reboot option is reported separately.

In the Reboot popup window, click the Crashes tab to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.
**Control Status Pane**

The Control Status pane displays whether vSmart and vEdge devices are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each vEdge router must connect to the configured maximum number of vSmart controllers.

The Control Status pane shows three counts:

- Control Up—Total number of devices with the required number of operational control plane connections to a vSmart controller.
- Partial—Total number of devices with some, but not all, operational control plane connections to vSmart controllers.
- Control Down—Total number of devices with no control plane connection to a vSmart controller.

Click any row to display a table with device details. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen.

**Site Health View Pane**

The Site Health View pane displays the state of a site's data connections. When a site has multiple vEdge routers, this pane displays the state for the entire site, not for individual devices. The Site Health View pane displays three states:

- Full Connectivity—Total number of sites where all BFD sessions on all vEdge routers are in the up state.
- Partial Connectivity—Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- No Connectivity—Total number of sites where all BFD sessions on all vEdge routers are in the down state. These sites have no data plane connectivity.

Click a row to display a popup window with detailed information on each site, node, or tunnel. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

**Transport Interface Distribution Pane**

The Transport Interface Distribution pane displays interface usage in the last 24 hours for all vEdge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

**vEdge Inventory Pane**

The vEdge Inventory pane provides four counts:

- Total—Total number of vEdge routers whose authorized serial number has been uploaded on the vManage server. The serial number is uploaded in the Configuration ► Devices screen.
- Authorized—Total number of authorized vEdge routers in the overlay network. These are routers marked as Valid in the Configuration ► Certificates ► vEdge List screen.
- Deployed—Total number of deployed vEdge routers. These are routers marked as Valid that are now operational in the network.
- Staging—Total number of vEdge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network. These
routers do not take part in any routing decisions nor do they affect network monitoring through the vManage NMS.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

vEdge Health Pane

The vEdge Health pane displays an aggregated view for each router state and a count of how many vEdge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- Normal—Number of routers with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as normal.
- Warning—Number of routers with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as a warning.
- Error—Number of routers with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as an error.

Click the number or the state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor ► Network screen or the Tools ► SSH Terminal screen.

Transport Health Pane

The Transport Health pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the Type drop-down, select loss, latency, or jitter.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Transport Health pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the displayed type and time period as described above.

Top Applications Pane

The Top Applications pane displays DPI flow information for traffic transiting vEdge routers in the overlay network.

Click the Filter icon to select a time period for which to display data. From the VPN drop-down list, select a VPN to display DPI information for all flows in that VPN.

Click the Expand icon to open the Top Applications pop-up window. This full-screen window displays a more detailed view of the same information. You can change the VPN and time period as described above.

Application-Aware Routing Pane

The Application-Aware Routing pane displays the 10 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter. So, if you choose loss, this pane shows the ten tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click Custom to display a drop-down for specifying a custom time period.
Click the Expand icon to open the Application-Aware Routing pop-up window. This full-screen window displays the 25 worst tunnels based on criteria you specify from the Type drop-down list, including loss, latency, and jitter.

Related Topics
Tenant Management, on page 21

RBAC by VPN

RBAC by VPN Overview

The Role-Based Access By VPN feature allows the network administrator to define VPN groups with one or more network segments. Network administrator can associate user to a VPN group which restricts user access to devices in the network and features of vManage.

RBAC by VPN provides the following restricted access to Users configured with a VPN group:

• Access to VPN Dashboard
• Monitor devices, network, and application status via VPN dashboard
• VPN dashboard information restricted to devices with segments in the VPN group
• Monitor option restricted to devices with segments in the VPN group
• Interface monitoring on each device restricted to interfaces of segments in the VPN group

VPN Dashboard Overview

Users configured with VPN group can access only the VPN Dashboard, and it is read-only access. User with Admin access can create the VPN groups and has access to both Admin Dashboard and VPN Dashboard(s). Admin user can view these dashboards in the left panel as shown in the following figures:
Configure and Manage VPN Segments

To configure VPN Segments:

1. Navigate to Administration > VPN Segments in vManage. The following web page displays with the list of segments that are configured.

2. To edit or delete an existing segment, click the Edit or Delete in the More Info (…) column on the right side.

3. To add new segment, click Add Segment. Add Segment window appears.

4. Enter the name of the segment in the Segment Name field.

5. Enter the number of VPNS you want to configure in VPN Number field.

6. Click Add to add a new segment.

Configure and Manage VPN Groups

To configure VPN Groups:

1. Navigate to Administration > VPN Groups in vManage. The following web page displays with the list of segments that are configured.

2. To edit or delete an VPN group, click the Edit or Delete in the More Info (…) column on the right side.

3. To view the existing VPN in the dashboard, click on View Dashboard in the More Info column. The VPN Dashboard displays the device details of the VPN device configured.

4. To add new VPN group, click Add Group. Add VPN Group window appears.
5. In the Create VPN Group pane, Enter VPN group name in the **VPN Group Name** field.
6. Enter a brief description of the VPN in the **Description** field.
7. Enable the user group access checkbox and enter the User Group Name.
8. In the Assign Segment pane, click on Add Segment drop-down to add new or existing segment to the VPN group.
9. Enter the Segment Name and VPN Number in the respective fields.
10. Click **Add** to add the configure VPN group to a device.

**Configure User with User group**

To create users with user group that is associated with the VPN group:

1. Navigate to **Administration > Manage Users**. The manage Users window appears.
2. To edit, delete, or change password for an existing user, click the **Edit, Delete, or Change Password** in the More Info (…) column on the right side.
3. Click on **Add User** to add a new user.
4. In the Add New User page, add **Full Name, Username, Password, and Confirm Password details**.
5. In the User Group drop-down, select the user group where you want to add a user.
6. If you want to add a User Group, click on **Add User Group** button.
7. Enter the user group name in the **Group Name** field.
8. Select the Read or Write checkbox that you want to assign to a user group as shown in the figure.

**Monitor devices for VPN Groups**

To monitor devices:

1. Navigate to **Monitor > Network** in vManage.
2. Select the VPN Group and VPN Segment for which you want to monitor the network.

The following web page displays with the list of VPN groups and segments that are configured to a device.
CHAPTER 4

Maintenance

- Device Reboot, on page 421
- Software Repository, on page 423
- Software Upgrade, on page 433

Device Reboot

Use the Device Reboot screen to reboot one or more Viptela devices.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Device Reboot.
- vEdge tab bar—Includes the Controller and vManage tabs.
- Reboot button—Select a device from the table to activate the button and reboot the device. The Rows Selected box displays the number of rows selected in the table.
- Device Group drop-down—List of all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
Reboot a Device

To reboot one or more Viptela device in the overlay network:

1. In the title bar, click vEdge, Controller, or vManage.
2. Select one or more devices.
3. Click the Reboot button.

View Active Devices

To view a list of devices on which the reboot operation has been performed:
1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.

2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

## Software Repository

Use the Software Repository screen to download software images to the vManage software repository.

### Screen Elements

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- **Title bar**—Includes the title of the screen, Software Repository.

- **Add New Software drop-down (on Repository screen)**—Upload new software images to the vManage or remote server.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.

- **Refresh icon**—Click to refresh data in the device table with the most current data.

- **Show Table Fields icon**—Click to display or hide columns from the device table. By default, all columns are displayed.

- **Software repository table**—List the images in the vManage software repository.
View Software Images

When you open the Software Repository screen, the images in the repository are displayed in the table. To filter the list, search or type a string in the Search box.

The Software Version column lists the version of the software image, and the Controller Version column lists the version of controller software that is equivalent to the software version. The controller version is the minimum supported vManage controller version. The software image can operate with the listed controller version or with a higher controller version. In the following example:
The software version is 16.8.55, and the controller version is 18.1.x. Reading these two columns together tells you that software version 16.8.55 is compatible with vManage controller software versions 18.1.x and later. This means that devices running version 16.8.55 can operate with vManage servers running Releases 18.1, 18.2, and 18.3, and with later software releases, and they cannot operate with vManage servers running Release 17.2 or Release 17.1.

The Software Location column indicates where the software images are stored, either in the repository on the vManage server or in a repository in a remote location.

The Available Files column lists the names of the software image files.

The Update On column shows when the software image was added to the repository.

In the More Actions column, you can delete a software image from the repository.

Add Software Images to the Repository

Before you can upgrade the software on a vEdge router, vSmart controller, or vManage NMS to a new software version, you need to add the software image to the vManage software repository. The repository allows you to store software images on the local vManage server and on a remote file server.

The vManage software repository allows you to store images in three ways:

• On the local vManage server, to be downloaded over a control plane connection—Here, the software images are stored on the local vManage server, and they are downloaded to the Viptela devices over a control plane connection. The receiving device generally throttles the amount of data traffic it can receive over a control plane connection, so for large files, the vManage server might not be able to monitor the software installation on the device even though it is proceeding correctly.

• On the local vManage server, to be downloaded over an out-of-band connection—Here, the software images are stored on the local vManage server, and they are downloaded to the Viptela devices over an out-of-band management connection. For this method to work, you specify the IP address of the out-of-band management interface when you copy the images to the software repository. This method is recommended when the software image files are large, because it bypasses any throttling that the device might perform and so the vManage server is able to monitor the software installation.

• On a remote server—Here, the software images remain on a remote file server that is reachable through an FTP or HTTP URL. As part of the software upgrade process, the vManage server sends this URL to the Viptela device, which then establishes a connection to the file server over which to download the software images.

To add software images to the vManage software repository:

1. Click Add New Software.

2. Select the location to store the software image:

   1. To store the software image or on the local vManage server and have it be downloaded to Viptela devices over a control plane connection, select vManage. The Upload Software to vManage dialog box opens.
1. Drag and drop the software image file to the dialog box, or click Browse to select the software image from a directory on the local vManage server.

2. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

---

**Note**

The local vManage server is available for storing NFVIS upgrade images and no other locations are available.

2. To store the software image on a remote server, select Remote Server. The Location of Software on Remote Server dialog box opens.
   1. In the Version box, enter the version number of the software image.
   2. In the URL box, enter the FTP or HTTP URL of the software image.
   3. Click Add to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

3. To store the image on a remote vManage server and have it be downloaded to Viptela devices over an out-of-band management connection, select Remote Server - vManage. The Upload Software to Remote Server - vManage dialog box opens.
   1. In the vManage Hostname box, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).
   2. Drag and drop the software image file to the dialog box, or click Browse to select the software image from a directory on the local vManage server.
   3. Click Upload to add the image to the software repository. The Software Repository tables displays the added software image, and it is available for installing on the devices.

**Upload VNF Images in Software Repository**

See Upload VNF Images, on page 427.

**Create Customized VNF Image**

See Create Customized VNF Image, on page 428.

**View VNF Images**

See View VNF Images.

**Delete a Software Image from the Repository**

To delete a software image from the vManage software repository:

1. In the software repository table, select the software image.
2. In the More actions icon to the right of the line, click Delete.
If a software image is being download to a router, you cannot delete the image until the download process completes.

**Delete VNF Image**

See [Delete VNF Images](#).

**Related Topics**

[Cloud OnRamp for Colocation](#), on page 37

---

# Upload VNF Images

The VNF images are stored in software repository. These VNF images are referenced during service chain deployment, and then they are pushed to NFVIS during service chain attachment.

In vManage, click **Maintenance > Software Repository**. The Maintenance|Software Repository screen appears, and the **Add New Software** button is highlighted. To upload VNF images, use the **Virtual Images** tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To add a prepackaged VNF image, click the **Virtual Images** tab, and then click the **Upload Virtual Images** button.  
b) Choose the location to store the virtual image.

   • To store the virtual image on the local vManage server and then get it downloaded to CSP devices over a control plane connection, click **vManage**. The **Upload Software to vManage** dialog box appears.

   1. Drag and drop the virtual image file to the dialog box or click **Browse** to choose the virtual image from the local vManage server. For example, CSR.tar.gz, ASA.tar.gz.

   2. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

   • To store the image on a remote vManage server and then get it downloaded to CSP devices over an out-of-band management connection, click **Remote Server - vManage**. The **Upload Virtual Image to Remote Server - vManage** dialog box appears.

   1. In **vManage Hostname/IP Address**, enter the IP address of an interface on the vManage server that is in a management VPN (typically, VPN 512).

   2. Drag and drop the virtual image file to the dialog box, or click **Browse** to choose the virtual image from the local vManage server.

   3. Click **Upload** to add the image to the virtual image repository. The virtual image repository table displays the added virtual image, and it is available for installing on the CSP devices.

c) Click **Submit**.

---

You can have multiple VNF entries such as a firewall from same or different vendors. Also, different versions of VNF that are based on the release of the same VNF can be added. However, ensure that the VNF name is unique.
Create Customized VNF Image

Before you begin

You can upload one or more qcow2 images in addition to a root disk image as an input file along with VM-specific properties, bootstrap configuration files (if any), and generate a compressed TAR file. Through custom packaging, you can:

• Create a custom VM package along with image properties and bootstrap files (if needed) into a TAR archive file.
• Tokenize custom variables and apply system variables that are passed with the bootstrap configuration files.

Ensure that the following custom packaging requirements are met:

• Root disk image for a VNF–qcow2
• Day-0 configuration files–system and tokenized custom variables
• VM configuration–CPU, memory, disk, NICs
• HA mode–If a VNF supports HA, specify Day-0 primary and secondary files, NICs for a HA link
• Additional Storage–If additional storage is required, specify predefined disks (qcow2), storage volumes (NFVIS layer)

Step 1
In the Maintenance > Software Repository screen, click the Add Custom VNF Package button from the Virtual Images tab.

Step 2
Configure the VNF with the following VNF package properties and click Save.

Table 210: VNF Package Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Name</td>
<td>Mandatory</td>
<td>Specifies the filename of the target VNF package. It is the NFVIS image name with .tar or .gz extensions.</td>
</tr>
<tr>
<td>App Vendor</td>
<td>Mandatory</td>
<td>Specifies whether Cisco VNFs or third-party VNFs.</td>
</tr>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Specifies name of the VNF image.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional</td>
<td>Specifies version number of the program.</td>
</tr>
<tr>
<td>Type</td>
<td>Mandatory</td>
<td>Choose VNF type. Supported VNF types are: Router, Firewall, Load Balancer, and Other.</td>
</tr>
</tbody>
</table>

Step 3
To package a VM qcow2 image, click File Upload under Image, and browse to choose a qcow2 image file.

Step 4
To choose a bootstrap configuration file for VNF, if any, click the Bootstrap Files button under Day 0 Configuration, click File Upload, and then browse to choose a bootstrap file.
Include the following Day-0 configuration properties:

**Table 211: Day-0 Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount</td>
<td>Mandatory</td>
<td>Specifies the path where the bootstrap file gets mounted.</td>
</tr>
<tr>
<td>Parseable</td>
<td>Mandatory</td>
<td>Specifies whether a Day-0 configuration file can be parsed or not.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options are: true or false. By default, it is true.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Mandatory</td>
<td>Choose high availability of a Day-0 configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported values are: Standalone, HA Primary, HA Secondary.</td>
</tr>
</tbody>
</table>

**Note** If any bootstrap configuration is required for a VNF, you must create `bootstrap-config` or `day0-config`.

**Step 5**

To add a Day-0 configuration, click **Add**, and then click **Save**. The Day-0 configuration appears in the **Day 0 Config File** table. You can tokenize the bootstrap configuration variables with system and custom variables. To tokenize variables of a Day-0 configuration file, click **View Configuration File** against the configuration file. In the **Day 0 configuration file** dialog box, perform the following tasks:

**Note** The bootstrap configuration file is an XML or a text file, and contains properties specific to a VNF and the environment. These VNF properties can have tokens, which can be populated during deploying a VNF. vManage automatically sets the tokens such as system variables. However, values of custom variables must be provided when creating a customized service chain, if they are defined as mandatory.

a) To add a system variable, in the **CLI configuration** dialog box, select and highlight a property from the text fields. Click **System Variable**. The **Create System Variable** dialog box appears.

b) Choose a system variable from the **Variable Name** drop-down, and click **Done**. The highlighted property is replaced by the system variable name.

c) To add a custom variable, in the **CLI configuration** dialog box, select and highlight a custom variable attribute from the text fields. Click **Custom Variable**. The **Create Custom Variable** dialog box appears.

d) Enter custom variable name and choose a type from **Type** drop-down.

e) To set the custom variable attribute, do the following:

   - To ensure that the custom variable is mandatory when creating a service chain, check the **Type** check box against **Mandatory**.
   - To ensure that a VNF includes both primary and secondary Day-0 files, check the **Type** check box against **Common**.

f) Click **Done**, and then click **Save**. The highlighted custom variable attribute is replaced by the custom variable name.

**Step 6**

To upload extra VM images, expand **Advance Options**, click **Upload Image**, and then browse to choose an additional qcow2 image file. Choose the root disk, Ephemeral disk 1, or Ephemeral disk 2, and click **Add**. The newly added VM image appears in the **Upload Image** table.

**Note** Ensure that you do not combine ephemeral disks and storage volumes when uploading extra VM images.
Step 7
To add the storage information, expand **Add Storage**, and click **Add volume**. Provide the following storage information and click **Add**. The added storage details appear in the **Add Storage** table.

**Table 212: Storage Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Mandatory</td>
<td>Specifies the disk size that is required for the VM operation. The maximum disk size can be 256 if the size unit is GiB.</td>
</tr>
<tr>
<td>Size Unit</td>
<td>Mandatory</td>
<td>Choose size unit. Supported units are: MIB, GiB, TiB.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Optional</td>
<td>Choose a disk or CD-ROM. Default is a disk.</td>
</tr>
<tr>
<td>Location</td>
<td>Optional</td>
<td>Specifies location of the disk or CD-ROM. By default, it is local.</td>
</tr>
<tr>
<td>Format</td>
<td>Optional</td>
<td>Choose a disk image format. Supported formats are: qcow2, raw, and vmdk. Buy default, it is raw.</td>
</tr>
<tr>
<td>Bus</td>
<td>Optional</td>
<td>Choose a value from the drop-down. Supported values for a bus are: virtio, scsi, and ide. By default, it is virtio.</td>
</tr>
</tbody>
</table>

Step 8
To add VNF image properties, expand **Image Properties** and provide the following image information.

**Table 213: VNF Image Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR-IOV Mode</td>
<td>Mandatory</td>
<td>Specifies enabling or disabling SR-IOV support. By default, it is enabled.</td>
</tr>
<tr>
<td>Monitored</td>
<td>Mandatory</td>
<td>VM health monitoring for those VMs that can be bootstrapped. Options are: enable or disable. By default, it is enabled.</td>
</tr>
<tr>
<td>Bootup Time</td>
<td>Mandatory</td>
<td>Specifies monitoring timeout period for a monitored VM. By default, it is 600 seconds.</td>
</tr>
<tr>
<td>Field</td>
<td>Mandatory or Optional</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Serial Console</td>
<td>Optional</td>
<td>Specifies serial console that is supported or not. Options are: enable or disable. By default, it is disabled.</td>
</tr>
<tr>
<td>Privileged Mode</td>
<td>Optional</td>
<td>Allows special features like promiscuous mode and snooping. Options are: enable or disable. By default, it is disabled.</td>
</tr>
<tr>
<td>Dedicate Cores</td>
<td>Mandatory</td>
<td>Facilitates allocation of a dedicated resource (CPU) to supplement a VM's low latency (for example, router and firewall). Otherwise, shared resources are used. Options are: enable or disable. By default, it is enabled.</td>
</tr>
</tbody>
</table>

**Step 9**

To add VM resource requirements, expand **Resource Requirements** and provide the following information.

**Table 214: VM Resource Requirements**

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CPU</td>
<td>Mandatory</td>
<td>Specifies CPUs supported by a VM. The maximum numbers of CPUs supported are 8.</td>
</tr>
<tr>
<td>Default RAM</td>
<td>Mandatory</td>
<td>Specifies RAM supported by a VM. The RAM can range from 2–32.</td>
</tr>
<tr>
<td>Disk Size</td>
<td>Mandatory</td>
<td>Specifies disk size in GB supported by a VM. The disk size can range from 4–256.</td>
</tr>
<tr>
<td>Max number of VNICs</td>
<td>Optional</td>
<td>Specifies maximum number of VNICs allowed for the VM. The number of VNICs can range from 8–32 and the default value is 8.</td>
</tr>
<tr>
<td>Management VNIC ID</td>
<td>Mandatory</td>
<td>Specifies the management VNIC ID corresponding to the management interface. Valid range is from 0 to maximum number of VNICs.</td>
</tr>
<tr>
<td>Number of Management VNICs ID</td>
<td>Mandatory</td>
<td>Specifies number of VNICs.</td>
</tr>
</tbody>
</table>
### Table 215: Day-0 Configuration Drive Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Label</td>
<td>Mandatory</td>
<td>Displays the volume label of the Day-0 configuration drive. Options are: V1 or V2. By default, it is V2. V2 is the config-drive label config-2. V1 is config-drive label cidata.</td>
</tr>
<tr>
<td>Init Drive</td>
<td>Optional</td>
<td>Mounts the Day-0 configuration file as a disk. The default drive is CD-ROM.</td>
</tr>
<tr>
<td>Init Bus</td>
<td>Optional</td>
<td>Choose an init bus. Supported values for a bus are: virtio, scsi, and ide. By default, it is ide.</td>
</tr>
</tbody>
</table>

The Software Repository table displays the customized VNF image, and it is available for choosing while creating a custom service chain.

### View VNF Images

In vManage, click Maintenance > Software Repository. The Maintenance|Software Repository screen appears, and the Add New Software button is highlighted. To view VNF images, use the Virtual Images tab. In the Maintenance|Software Repository screen, perform the following tasks:

- a) To view VNF images, click the Virtual Images tab. The images in the repository are displayed in the table.
- b) To filter the list, search or type a string in the Search box.
The Software Version column provides the version of the software image.
The Software Location column indicates where the software images are stored. It can be stored either in the repository on the vManage server or in a repository in a remote location.
The Version Type Name column provides the type of firewall.
The Available Files column lists the names of the VNF image files.
The Update On column displays when the software image was added to the repository.

c) To view details of a VNF image, click a VNF image, click the More Actions icon, and click Show Info against the VNF image.

Delete VNF Images

In vManage, click Maintenance > Software Repository. The Maintenance|Software Repository screen appears, and the Add New Software button is highlighted. To upload VM images, use the Virtual Images tab. In the Maintenance|Software Repository screen, perform the following tasks:

a) To delete a VM image, click the Virtual Images tab. The images in the repository are displayed in the table.
b) In the repository table, click a VM image.
c) Click the More Actions icon to the right of its row, and click Delete against the VM image.

Note If a VNF image is being download to a router, you cannot delete the VNF image until the download process completes.

Note If the VNF image is referenced by a service chain, it cannot be deleted.

Software Upgrade

Use the Software Upgrade screen to download new software images and to upgrade the software image running on a Viptela device.

From a centralized vManage NMS, you can upgrade the software on Viptela devices in the overlay network and reboot them with the new software. You can do this for a single device or for multiple devices simultaneously.

When you upgrade a group of vBond orchestrators, vSmart controllers, and vEdge routers, the software upgrade and reboot is performed first on the vBond orchestrator, next on the vSmart controllers, and finally on the vEdge routers. For vEdge routers, up to five routers can be upgraded and rebooted in parallel at the same time.

You cannot include the vManage NMS in a group software upgrade operation. You must upgrade and reboot the vManage server by itself.
It is recommended that you perform all software upgrades from the vManage NMS rather than from the CLI.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- **Title bar**—Includes the title of the screen, Software Upgrade.

- **Device List drop-down**—Displays the list of devices in the overlay network. When you first open the Software Upgrade screen, Device List is selected by default.
  - **WAN Edge tab bar**—Includes the Controller and vManage tabs.
  - **Rows Selected**—Displays the number of rows selected from the table. Includes:
    - **Upgrade button**—Installs a new software version on the device. Includes:
    - **Activate button**—Reboots the device and activates the new software version.
    - **Delete Available Software button**—Delete a software version from a device.
    - **Set Default Version button**—Set a software image to be the default image on the device.
  - **Device Group drop-down**—List of all configured device groups in the network.
  - **Table of devices in the overlay network**—To re-arrange the columns, drag the column title to the desired position.

- **Repository drop-down**—Click Repository from the Device List drop-down to display the list of software images on the vManage or remote server.
  - **Add New Software drop-down** (on Repository screen)—Upload new software images to the vManage or remote server.

  - **Table of software images**—To re-arrange the columns, drag the column title to the desired position.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.

- **Refresh icon**—Click to refresh data in the device table with the most current data.

- **Export icon**—Click to download all data to a file, in CSV format (on Device List screen only).

- **Show Table Fields icon**—Click to display or hide columns from the device table. By default, all columns are displayed.
View Software Images

To view a list of software images in the repository on the vManage server or on a remote server, from the Device List drop-down, click Repository.

Upgrade a Software Image

To upgrade the software image on a device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices on which to upgrade the software image.
3. Click the Upgrade button. The Software Upgrade dialog box opens.
4. Select the software version to install on the device. If the software is located on a Remote Server, select the VPN in which the software image is located.

5. To automatically activate the new software version and reboot the device, select the Activate and Reboot checkbox.

6. Click Upgrade. A progress bar indicates the status of the software upgrade.

If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Viptela devices to come up after a software upgrade is 5 minutes, except for vEdge 100 routers, which have a default time of 12 minutes.

Note: If you upgrade the vEdge software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first, before upgrading the vEdge software.

**Activate a New Software Image**

If you did not select the Activate and Reboot checkbox when upgrading the software image, the device continues to use the existing configuration. To activate the new software image:

1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which to activate the new software image.
3. Click the Activate button. The Activate Software dialog box opens.
4. Select the software version to activate on the device.
5. Click Activate. vManage NMS reboots the device and activates the new software image.

If the control connection to the vManage NMS does not come up within the configured time limit, vManage NMS automatically reverts the device to the previously running software image. The configured time limit for all Viptela devices to come up after a software upgrade is 5 minutes, except for the vEdge 100 routers, which have a default time of 12 minutes.

**Upgrade CSP device with NFVIS Upgrade Image**

See Upgrade CSP Device with NFVIS Upgrade Image, on page 437.

**Delete a Software Image**

To delete a software image from a Viptela device:

1. In the title bar, click the WAN Edge, Controller, or vManage tab.
2. Select one or more devices from which to delete a software image.
3. Click the Delete Available Software button. The Delete Available Software dialog box opens.
4. Select the software version to delete.
5. Click Delete.
Set the Default Software Version

You can set a software image to be the default image on a Viptela device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on the device and in your network.

To set a software image to be the default image on a device:
1. In the title bar, click the vEdge, Controller, or vManage tab.
2. Select one or more devices on which you wish to change the default software image.
3. Click the Set Default Version button. The Set Default Version dialog box opens.
4. From the Version drop-down, select the software image to use as the default.
5. Click Set Default.

Export Device Data in CSV Format

To export data for all devices to a file in CSV format, click the Export button. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named viptela_download.csv.

View Log of Software Upgrade Activities

To view the status of software upgrades and a log of related activities:
1. Click the Tasks icon located in the vManage toolbar. vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

Upgrade CSP Device with NFVIS Upgrade Image

Before you begin

Ensure that the NFVIS software versions are the files that have .nfvispkg extension.

Step 1 In the Maintenance > Software Upgrade > WAN Edge screen, view the list of all CSP devices along with their current and available versions.
Step 2 Select one or more devices, and click Upgrade.
Step 3 Choose a CSP device on which to upgrade the NFVIS software image.
Step 4 Click the Upgrade button. The Software Upgrade dialog box appears.
Step 5 Choose the NFVIS software version to install on the CSP device. If software is located on a remote server, choose the appropriate remote version.
Step 6 To automatically upgrade and activate with the new NFVIS software version and reboot the CSP device, check the Activate and Reboot checkbox.
If you do not check the **Activate and Reboot** checkbox, the CSP device downloads and verifies the software image. However, the CSP device continues to run the old or current version of the software image. To enable the CSP device to run the new software image, you must manually activate the new NFVIS software version by selecting the device again and clicking the **Activate** button on the **Software Upgrade** page. For more information about activation, see the "Activate a New Software Image" topic in Cisco SD-WAN documentation about Software Upgrade.

**Step 7**

Click **Upgrade**.

To view the status of software upgrades, the task view page displays a list of all running tasks along with total number of successes and failures. The page periodically refreshes and displays messages to indicate the progress or status of the upgrade. You can easily access the software upgrade status page by clicking the Tasks icon located in the vManage toolbar.

**Note** If two or more CSP devices belonging to the same cluster are upgraded, the software upgrade for the CSP devices happen in a sequence.

---

The CSP device reboots and the new NFVIS version is activated on it. This reboot happens during the **Activate** phase. The activation can either happen immediately after upgrade if you check the **Activate and Reboot** check box, or by manually selecting the activate button after selecting the device again.

To verify if CSP device has rebooted and is running, vManage polls your entire network every 90 seconds up to 30 times.

**Note** The **Set the Default Software Version** option is not available for NFVIS images.
You can delete an NFVIS software image from a CSP device if the image version is not the active version that is running on the device.
Upgrade CSP Device with NFVIS Upgrade Image
CHAPTER 5

Monitor

- ACL Log, on page 441
- Geography, on page 442
- Network, on page 446

ACL Log

Use the ACL Log screen to view logs for access lists (ACLs) configured on a vEdge router. Routers collect ACL logs every 10 minutes.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, ACL Log.
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for ACL logs. Click a predefined or custom time period for which to display data.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the ACL logs table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the ACL logs table. By default, all columns are displayed.
- Table of ACL logs—To re-arrange the columns, drag the column title to the desired position.
Set ACL Log Filters

To set filters for searching ACL logs:

1. Click the Filter drop-down menu.
2. In the VPN drop-down, select the entity for which you are collecting ACL logs. You can select only one VPN.
3. Click Search to search for logs that match the filter.

vManage NMS displays a log of activities in table format.

Geography

Use the Geography screen to view information about the Viptela devices and links in the overlay network. The Geography screen provides a map displaying the geographic location of the Viptela devices.

Note: The browser on which you are running vManage NMS must have Internet access. If you do not have Internet access, ensure that the browser has access to "*.openstreetmaps.org."

Screen Elements

• Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
• Title bar—Includes the title of the screen, Geography.
  • No Geographic Coordinates—Located to the right of the title bar, it displays the number of devices for which geographic coordinates are not configured.
• Filter bar—Includes the Filter button and the following tabs which reflect the default Filter selections:
  • All Groups for the device group.
  • vEdge, vEdge-vBond, vBond, vSmart, and vManage for the device types.
  • Control Up, Data Up, and Data Down for the link states.
• Map—Displays the geographic location of Viptela devices based on the latitude and longitude configured on the devices. The map includes the following elements:
  • Search box—Includes the Search Options drop-down, for a Contains or Match string. The search applies to all devices, including those that have no geographic coordinates defined.
  • + (plus) and – (minus) zoom icons.
  • Map provider icon, to choose any open source map provider.
  • Device icons for the Viptela devices:
• Device clusters—A green circle with a number in the center indicates a cluster of devices located in an area. Click the cluster to display the individual device icons on the map.
Set Map Filters

To select the devices and links you want to display on the map:

1. Click the Filter button to display a pull-down menu.

2. Select the device group from the pull-down menu which includes all configured device groups. By default, the group "All" is selected and displays all Viptela devices in the overlay network. The group "No Groups" includes the devices that are not part of a device group. If all devices are in a group, the "No Groups" group is not displayed.
3. Select the Vipteladevicestodisplayonthemap. By default, the map displays all devicetypesincluding vEdge, vEdge-vBond, vSmart, and vManage.

4. Selectthestateofcontrolanddatalinks. By default, the map displays all control and data connections.

5. Close the Filter box by moving the cursor outside the box.

The map is dynamically updated to reflect your selections. Also, as you make the device group, device type, and link selections, the tabs next to the Filter button are updated.

**View Device Information**

To display basic information for a device, hover over the device icon. A hover box displays the system IP, hostname, site ID, device type, and device status.

To display detailed information for a device, double-click the device icon to open the View More Details hover box. Click Device Dashboard, Device Details, SSH Terminal, or Links to get further details for the device.

**View Link Information**

By default, control and data connections are not displayed on the map. To see control and data connections for a device:

1. Double-click the device icon to open a hover box with details about the device.

2. Click Links.

Note the following:

- An active control connection between two devices is displayed on the map as a thin blue line. Multiple active connections between devices are displayed by a bold blue line. A control connection that is down is displayed on the map as a dotted red line. Multiple control connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.

- An active data connection between two devices is displayed on the map as a thin green line. Multiple active data connections are displayed by a bold green line. A data connection that is down is displayed on the map as a dotted red line. Multiple data connections that are down are displayed by a bold dotted red line. If you hover over the line, a hover box tells you if the connection is up or down.

- An active consolidated control and data connection between two devices is displayed on the map as a thick grey line.

**Configure Geographic Coordinates for a Device**

To configure the geographic coordinates for a device, use the Configuration ► Templates ► System feature template.

If the Viptela device is not attached to a configuration template, you can configure the latitude and longitude directly on the device:

1. Select the Tools ► SSH Terminal screen.

2. Select the device from the left pane. The SSH Terminal screen opens in the right pane.

3. Enter the username and password to log in to the device.
4. Determine whether the device is attached to a configuration template:

Viptela#

**show system status** Check the values in the vManaged and Configuration template output fields. For example:

```
...  
Personality: vedge  
Model name: vedge-cloud  
Services: None  
vManaged: false  
Commit pending: false  
Configuration template: None
```

If the vManaged field is false, the device is not attached to a configuration template, and the Configuration template field says None. For such a device, you can configure the GPS coordinates directly from the CLI. If the vManaged field is true, the device's configuration has been downloaded by the vManage server, and the Configuration template field shows the name of the configuration template. For such a device, you cannot configure the GPS coordinates directly from the CLI. If you attempt to do so, the `validate` or `commit` command fails, with the following message:

```
Aborted: 'system is-vmanaged': This device is being managed by the vManage. Configuration through the CLI is not allowed.
```

5. Enter configuration mode:

Viptela# config
Viptela(config)#

6. Configure the latitude and longitude on the device:

Viptela(config)# `system gps-location latitude
degrees.minutes.seconds`
Viptela(config-system)# `gps-location longitude
degrees.minutes.seconds`

7. Save the configuration:

Viptela(config-system)# commit
Viptela(config-system)#

# Network

Use the Network screen to display a list of Viptela devices in the overlay network and to display detailed information about individual devices.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, Network.
- **WAN Edge and Colocation Clusters tabs**—When you first open the Network screen, the WAN Edge tab is selected.
  - **WAN Edge tab**—Click to display a table of the overlay network devices in the network.
• Colocation Clusters tab—Click to display a table of the Colocation clusters in the network.

• Device Groups drop-down—Lists all configured device groups in the network.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.

• Refresh icon—Click to refresh data in the device table with the most current data.

• Export icon—Click to download all data to a file, in CSV format.

• Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.

• Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
**View List of Devices**

The Network screen lists the Viptela devices in the overlay network. When you first come to the Network screen, the device group "All" is selected, and the screen shows status information for all Viptela devices in the overlay network.

To see a list of devices in a particular group, select that device group.

To filter the devices by reachability, hostname, system IP address, site ID, and device model, select from the sort options in the drop-down or type a string in the Search box.

To display information about an individual device, click its hostname.

**Export Device Data in CSV Format**

To export data for all devices to a file in CSV format, click the Export button. This button is located to the right of the filter criteria.

vManage NMS downloads all data from the device table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named viptela_download.csv.

**View Information about a Device**

To view high-level information about a device, select the device from the Monitor ▶ Network screen:

1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.

2. Select the device by clicking its hostname. The left pane lists the information categories about the device. In the right pane, the System Status category is selected, which displays status information about the device.

To select a different device, either click the Select Device drop-down located at the top of the left pane, or click Network in the title bar and then select a device by clicking its hostname.

After you select a device by clicking its hostname, the screen changes and displays the following elements:

- **Select Device bar**—A horizontal bar that includes these elements:
  - Select Device drop-down
  - Device name
  - Device IP address
  - Device site location
  - Device model
  - More Info drop-down

- **Left pane**—A vertical pane that lists the categories of information you can display about the device:
  - Applications—DPI flow information.
  - Interface—Interface status and statistics.
  - TCP Optimization—Statistics related to find-tuning the processing of TCP data traffic.
  - WAN—TLOC and tunnel status and statistics.
• Control Connections—Status and statistics for control connections.

• System Status—Reboot and crash information, hardware component status, and CPU and memory usage.

• Events—Latest syslog events.

• ACL Logs—Logging files for access lists (ACLs).

• Troubleshooting—Ping and traceroute traffic connectivity tools.

• Real Time—Real-time device information for feature-specific operational commands.

• Right pane—Displays information about the selected category.
View Device Status Summary

To view summary status information about a device:

1. From the Monitor►Network screen, select a device.

2. From the Select Device bar, click the More Info drop-down located to the right of the bar. vManage NMS opens a drop box with summary information about the device.

To close the device status summary, click More Info again or click anywhere on the screen outside the drop-down.
View DPI Flows

To view DPI flow information on a vEdge router:

1. From the Monitor ▶ Network screen, select a device.
2. Click Applications in the left pane. The right pane displays DPI flow information for the device.

The upper part of the right pane contains:

- Filter bar—Located directly under the device name, this bar includes the Filter icon and time periods. Click the Filter icon to display a drop-down menu to select the desired VPN and TLOC. Click a predefined or custom time period for which to display data.
- DPI flow information in graphical format.
- DPI flow graph legend—Select an application family to display information for just that flow. Click the Total Network Traffic checkbox to display flow information as a proportion of total network traffic.

The lower part of the right pane contains:

- Filter criteria.
- DPI flow information table that lists all application families sorted by usage. By default, the top six application families are selected. The graphical display in the upper part of the right pane plots the flow and usage of the selected application families.
  - Click the checkbox to the left to select and deselect application families. You can select and display information for a maximum of six application families at one time.
  - Click an application family to display applications within the family.
  - Click an application to display the source IP addresses of the devices accessing the application. The Traffic per TLOC pie chart next to the graph displays traffic distribution per TLOC (color).
  - To re-arrange the columns, drag the column title to the desired position.
  - To return to the list of application families, click Applications in the title bar or click the Back button in the browser.

View VNF Status

To view performance specifications, required resources for each VNF, and component network functions for each VNF. Reviewing this information can help you to determine which VNF to use when you are designing a network service.

1. In vManage, click Monitor ▶ Network.
   The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.
2. Click a CSP device from the table.
3. From the left pane, click VNF Status.
4. In the table, click the VNF name. The right pane displays information about the specific VNF. You can click the network utilization, CPU utilization, memory utilization, disk utilization to monitor the resources utilization of a VNF.

The primary part of the right pane contains:

- Chart Options bar that includes the following options:
  - Chart Options drop-down—Click Chart Options to select the type of data to display.
  - Time periods—Click either a predefined time period, or a custom time period for which to display data.

- VNF information in graphical format.

- VNF graph legend—Select a VNF to display information for just that VNF.

The detail part of the right pane contains:

- Filter criteria

- VNF table that lists information about all VNFs. By default, the first six VNFs are selected. The graphical display in the upper part of the right pane plots information for the selected VNFs.
  - Check or uncheck the checkbox at the left to select and deselect VNFs. You can select and display information for a maximum of six VNFs at one time.
  - To change the sort order of a column, click the column title.

**View Interfaces**

To view information about interfaces on a device:

1. From the Monitor ► Network screen, select a device.
2. Click Interface in the left pane. The right pane displays interface information for the device.

The upper part of the right pane contains:

- Chart Options bar—Located directly under the device name, this bar includes:
  - Chart Options drop-down—Click Chart Options to select the type of data to display.
  - IPv4 & IPv6 drop-down—Click IPv4 & IPv6 to select the type of interfaces to display. The information is displayed in graphical format. By default, the graph is Combined, showing interfaces on which both IPv4 and IPv6 addresses are configured. To display IPv4 and IPv6 interfaces in separate graphs, select the Separated toggle button.
  - Time periods—Click either Real Time, a predefined time period, or a custom time period for which to display data.

- Interface information in graphical format.

- Interface graph legend—Select an interface to display information for just that interface.

The lower part of the right pane contains:
• Filter criteria.

• Interface table that lists information about all interfaces. By default, the first six interfaces are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  • Click the checkbox to the left to select and deselect interfaces. You can select and display information for a maximum of 30 interfaces at one time.
  • To re-arrange the columns, drag the column title to the desired position.
  • For cellular interfaces, click the interface name to display a screen that shows detailed information about the cellular interface.

View TCP Optimization Information

If TCP optimization is enabled on a router, you can view information about how the optimization is affecting the processing and throughput of TCP data traffic on the router:

1. From the Monitor ► Network screen, select a vEdge router.
2. Click TCP Optimization–WAN Throughput in the left page. The right pane displays the WAN throughput, in megabits per second.

The upper part of the right pane contains the following elements:
  • Chart Options bar—Located directly under the device name, this bar includes the Filter Options drop-down and time periods. Click Filter to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
  • Average optimized throughput information in graphical format.
  • WAN graph legend—Identifies non-optimized and TCP optimized packet throughput.

The lower part of the right pane shows the hourly average throughput and the total optimized throughput, both in megabits per second.

Click TCP Optimization–Flows in the left pane to display information about TCP-optimized traffic flows. The upper part of the right pane contains the following elements:
  • Chart Options bar—Located directly under the device name, this bar includes the Filter drop-down and time periods. Click Filter to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
  • Average optimized throughput information in graphical format.
  • Flows graph legend—Identifies traffic flows.

The lower part of the right pane contains the following elements:
  • Set perspective—Select the flow direction.
  • Search box—Includes the Search Options drop-down, for a Contains or Match string.
  • Flow table that lists the flow destination, usage, and percentage of total traffic for all TCP-optimized flows. By default, the first six flows are selected. Click the checkbox to the left to select and deselect
flows to display. The graphical display in the upper part of the right pane plots information for the selected flows.

Click TCP Optimization–Connections in the left pane to display status information about all the tunnels over which the most TCP-optimized traffic is flowing. The upper part of the right pane contains the following elements:

- TCP Optimization Connections in graphical format
- Connection State boxes—Select the connection state or states to display TCP optimization information about.

The lower part of the right pane contains the following elements:

- Filter criteria.
- Flow table that lists information about each of the tunnels, including the tunnel's connection state.

**View TLOC Loss, Latency, and Jitter Information**

To view information about TLOC loss, latency, and jitter:

1. From the Monitor ► Network screen, select a device.
2. Click WAN–TLOC in the left pane. The right pane displays the aggregated average loss or latency/jitter information for all TLOC colors.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- TLOC information in graphical format. The time interval in the graph is determined by the value of the BFD application-aware routing poll interval.
- TLOC graph legend—Select a TLOC color to display information for just that TLOC.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- TLOC color table that lists average jitter, loss, and latency data about all TLOCs. By default, the first six colors are selected. The graphical display in the upper part of the right pane plots information for the selected interfaces.
  - Click the checkbox to the left to select and deselect TLOC colors. You can select and display information for a maximum of 30 TLOCs at one time.
  - Click Application Usage to the right to display DPI flow information for that TLOC.

**View Tunnel Connections**

To view all tunnel connections for a device:

1. From the Monitor ► Network screen, select a device.
2. Click WAN–Tunnel in the left pane. The right pane displays information about all tunnel connections.

The upper part of the right pane contains the following elements:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- Tunnel information in graphical format.
- Tunnel graph legend—Select a tunnel to display information for just that tunnel.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
- Tunnel table that lists average latency, loss, and jitter data about all tunnel end points. By default, the first six tunnels are selected. The graphical display in the upper part of the right pane plots information for the selected tunnels.
  - Click the arrow to the left to view the tunnel end points for that TLOC color.
  - Click the checkbox to the left to select and deselect tunnels. You can select and display information for a maximum of 30 tunnels at one time.
  - Click Application Usage to the right to display DPI flow information for that TLOC.

View WiFi Configuration

To view WiFi configuration for Viptela routers that support wireless LANs (WLANs), such as the vEdge 100wm routers:

1. From the Monitor ► Network screen, select a device.
2. Click WiFi in the left pane. The right pane displays information about WiFi configuration on the router.

The upper part of the right pane contains the following elements:

- AP Information bar—Located directly under the device name, it displays access point information and the Clients Details button. Click the Clients Details button to view information about clients connected to the WiFi access point during the selected time period.
- Radio frequency parameters for access points.
- SSID parameters for virtual access points (VAPs).

The lower part of the right pane contains the following elements:

- VAP receive and transmit statistics bar—Includes the time periods. Click a predefined or custom time period for which to display data.
- VAP receive and transmit statistics information in graphical format.
- VAP statistics graph legend—Select a VAP interface to display information for just that interface. Click the VAP interface again to return to the previous display.
View Client Details

To view details of clients connected to the WiFi access point, click the Clients Details button on the WiFi screen.

The upper part of the Clients Info right pane contains the following elements:

- Clients Details title bar—Includes the Clients Usage tab.
- Time periods—Click a predefined or custom time period for which to display data.
- Information of clients connected to the WiFi access point in graphical format. Select a column to display information for just those clients in tabular format in the lower part of the screen.

The lower part of the Clients Info right pane contains the following elements:

- Filter criteria.
- Table of clients connected to the WiFi access point.

View Client Usage

To view data usage details of all clients connected to the WiFi access point, click the Clients Usage tab.

The upper part of the Clients Usage right pane contains the following elements:

- Time periods—Click a predefined or custom time period for which to display data.
- Data usage of all clients connected to the WiFi access point in graphical format.
- Data usage information graph legend—Select a client MAC address to display information for just that client.

The lower part of the Clients Usage right pane contains the following elements:

- Filter criteria.
- Data usage information table. By default, the first six clients are selected.

View Control Connections

To view all control connections for a device:

1. From the Monitor ➤ Network screen, select a device. If you select a controller device—a vBond orchestrator, a vManage NMS, or a Smart controller—the Control Connections screen opens by default.

2. If you select a vEdge router, click Control Connections in the left pane. The right pane displays information about all control connections that the device has with other controller devices in the network.

The upper part of the right pane contains the following elements:

- Expected and actual number of connections.
- Control connection data in graphical format. If the device has multiple interfaces, vManage NMS displays a graphical topology of all control connections for each color.

The lower part of the right pane contains the following elements:

- Search box—Includes the Search Options drop-down, for a Contains or Match.
• Control connections data in tabular format. By default, the first six control connections are selected. The graphical display in the upper part of the right pane plots information for the selected control connections.
  • Click the arrow to the left to view the control connections for that TLOC color.
  • Click the checkbox to the left to select and deselect control connections. You can select and display information for a maximum of six control connections at one time.

**View System Status**

To view system status about a device:

1. From the Monitor ► Network screen, select a device. When you select a vEdge router, the System Status screen opens by default.

2. Click System Status in the left pane. The right pane displays information about the device.

The right pane contains the following elements:

  • Reboot—Number of times the device has rebooted. For details about each reboot, click Reboot. The Reboot screen opens and contains the following elements:
    • Search box—Includes the Search Options drop-down, for a Contains or Match.
    • Table listing all the reboots on the device along with the time and reason for the reboot. If the device is down for 90 seconds or longer, the reason shows as "Unknown". The Last Updated column displays the time when the vManage NMS retrieved the reboot data from the device.

  • Crash—Number of times the device has crashed. For details about each crash, click Crash. The Crash screen opens and contains the following elements:
    • Search box—Includes the Search Options drop-down, for a Contains or Match.
    • Table listing all the crashes on the device along with the time of crash and name of the core file created as a result of the crash.

  • Status of hardware components, applicable only if the selected device is a hardware vEdge router:
    • Module
    • Temperature sensors
    • USB
    • Power supply
    • Fans

The status of a hardware component is represented in one of the following ways:

  • Green check mark—Component is operational.
  • Red circle with an X—Component is down.
  • Orange triangle with an exclamation point—Component has an error.
  • N/A—Not applicable since the selected device is not a hardware vEdge router.
• CPU & Memory—To the right are the time periods. Click a predefined or custom time period for which to display data.
  • CPU usage—Displays the CPU usage, as a percentage of available CPU, over the selected time range.
  • Memory usage—Displays the memory usage, as a percentage of available memory, over the selected time period.

**View Cisco Colo Manager Health**

To view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state.

1. In vManage, click **Monitor > Network**.

   The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

2. Click a CSP device from the table.

3. From the left pane, click **Colo Manager**.

   The right pane displays information about the memory usage, CPU usage, uptime, and so on, of the colo manager.

**View Events**

To view the number of critical, major, or minor events on a device:

1. From the Monitor►Network screen, select a device.

2. Click Events in the left pane. The right pane displays information about all events on the device.

   The upper part of the right pane contains the following elements:
   • Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching events by severity, component, and event name. Click a predefined or custom time period for which to display data.
   • Events Histogram—Displays a graphical representation of all events. To hide the events histogram, click the Events Histogram title or the down angle bracket to the right of it.

   The lower part of the right pane has the following elements:
View ACL Logs

To view logs for access lists (ACLs) configured on a vEdge router:

1. From the Monitor ► Network screen, select a vEdge router.
2. Click ACL Logs in the left pane. The right pane displays information about all localized data policy (ACL) logs on the router. You configure these logs by including the log action in an ACL.

The upper part of the right pane contains the following elements:
- Filter bar—Includes the Filter drop-down and time periods. Click the Filter icon to display a drop-down menu to add filters for searching logs by VPN. Click a predefined or custom time period for which to display data.
- Search box—Includes the Search Options drop-down, for a Contains or Match.

The lower part of the right pane contains the following elements:
- Logs table.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

Troubleshoot a Device

You can troubleshoot connectivity or traffic health for all devices in the overlay network.

Check Device Connectivity

To troubleshoot connectivity for a device in the network, you can do the following:
- Check device bringup
- Ping the device
- Run a speed test
- Run a traceroute
- View control connections in real time

Check Device Bringup

To verify the status of a device bringup (available on vEdge routers only):
1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.

3. From the Connectivity pane, click Device Bringup.

The Device Bringup screen opens and displays:

- Troubleshooting drop-down—Located to the right of the Select Device drop-down. Click an option to view troubleshooting information. To close the drop-down, click the Troubleshooting button again.

- Device bringup state—Indicated by one of the following states:
  - Green check mark—Indicates that the device has successfully established control-plane connections with the controller devices in the network and is up and running.
  - Gray check mark—Indicates that ZTP was disabled in the Administration ► Settings screen when the device initially came up. You will see this state for the Software Image Update box only.
  - Red check mark—Indicates that the device failed to establish control-plane connections with the controller devices in the network and is not up and running.
  - Yellow exclamation point—Indicates that vManage NMS could not find the reason for a failure on the device.

**Ping a Device**

To verify that a device is reachable on the network, ping the device to send ICMP ECHO_REQUEST packets to it:

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Ping.
4. In the Destination IP field, enter the IP address of the device to ping.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send the ping packets.
7. In the Probes field, select the protocol type to use to send the ping packets.
8. In the Source Port field, enter the number of the source port.
9. In the Destination Port field, enter the number of the destination port.
10. In the Type of Service field, enter the value for the type of service (ToS) field to include in the ping packets.
11. In the Time to Live field, enter the round-trip time for sending this ping packet and receiving a response, in milliseconds.
12. Click the Don't Fragment slider to set the Don't Fragment bit in the ping packets.
13. Click Advanced Options to specify additional parameters:
   1. In the Count field, enter the number of ping requests to send. The range is 1 through 30. The default is 5.
2. In the Payload Size field, enter the size of the packet to send. The default is 64 bytes, which comprises 56 bytes of data and 8 bytes of ICMP header. The range for data is 56 through 65507 bytes.

3. Click the Rapid slider to send 5 ping requests in rapid succession and to display statistics only for packets transmitted and received, and the percentage of packets lost.

14. Click Ping.

### Run a Speed Test

To check the actual bandwidth of a circuit from one device to another:

1. In the Administration ► Settings screen, ensure that Data Stream is enabled.
2. From the Monitor ► Network screen, select the device.
3. Click Troubleshooting in the left pane.
4. From the Connectivity pane, click Speed Test.
5. In the Source Circuit drop-down, select the color of tunnel interface on the local device.
6. In the Destination Device drop-down, select the remote device by the device's name and system IP address.
7. In the Destination Circuit drop-down, select the color of the tunnel interface on the remote device.
8. Click Start Test. The speed test sends a single packet from the source to the destination and receives the acknowledgement from the destination.

The middle part of the right pane reports the results of the speed test. The clock reports the circuit’s speed based on the round-trip time. The download speed shows the speed from the source to the destination, and the upload speed shows the speed from the destination to the source, both in Mbps. The configured downstream and upstream bandwidths for the circuit are also displayed.

When a speed test completes, the test results are added to the table at the lower part of the right pane.

### Run a Traceroute

To display the path that packets take to reach a host or IP address on the network:

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Trace Route.
4. In the Destination IP field, enter the IP address of a device on the network.
5. In the VPN drop-down, select the VPN to use to reach the device.
6. In the Source/Interface drop-down, select the interface to use to send traceroute probe packets.
7. Click Advanced Options.
8. In the Size field, enter the size of the traceroute probe packets, in bytes.
9. Click Start to trigger a traceroute to the requested destination.

The lower part of the right pane displays:
Output—Raw output of the path the traceroute probe packets take to reach the destination.
Graphical depiction of the path the traceroute probe packets take to reach the destination.

View Control Connections in Real Time

To display a real-time view the control plane connections on a vEdge router:

1. From the Monitor ► Network screen, select the device. The device must be a vEdge router.
2. Click Troubleshooting in the left pane.
3. From the Connectivity pane, click Control Connections.

The control plane connection screen is updated automatically, every 15 seconds.

The upper part of the right pane shows figures illustrates the operational control plane tunnels between the vEdge router and vManage and vSmart controllers.

The lower part of the lower pane contains a table that shows details for each of the control plane tunnels, including the remote device's IP address and the status of the tunnel end points, including the reason for the failure of an end point.

Check Traffic Health

To check traffic health for a vEdge router in the network:

- View tunnel health
- View traffic path information
- Packet capture
- Simulate flows

View Tunnel Health

To view the health of a tunnel from both directions (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click Tunnel Health.
4. From the Local TLOC drop-down, select a source TLOC.
5. From the Remote Device drop-down, select a remote device.
6. From the Remote TLOC drop-down, select a destination TLOC.
7. Click Go. The lower part of the screen displays:

- Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
- App-route data (either loss, latency, or jitter) in graphical format for all tunnels between the two devices in each direction.
- App-route graph legend—Identifies selected tunnels from both directions.

Select a TLOC to display information for just that TLOC.

**Check Application-Aware Routing Traffic**

To check application-aware routing traffic from the source device to the destination device (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click App Route Visualization.
4. From the Remote Device drop-down, select a destination device.
5. Click Go. The lower part of the screen displays:
   - Chart Options bar—Located directly under the device name, this bar includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to display. Click a predefined or custom time period for which to display data.
   - Application-aware routing data (either loss, latency, or jitter), along with octets, in graphical format for all tunnels between the two devices.
   - Application-aware routing graph legend—Identifies source and destination TLOC.

**Capture Packets**

To capture control plane and data plane packets in real time, similar to a UNIX tcpdump operation, and to save these packets to a file (available on vEdge routers only):

1. From the Monitor ► Network screen, select the device.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click App Packet Capture.
4. From the VPN drop-down, select the VPN in which to capture packets.
5. From the Interface drop-down, select the interface over which to capture packets.
6. Optionally, click Traffic Filter to filter the packets to capture based on values in their IP headers. Enter values for one or more of these fields:
   1. In Source IP, enter the packets' source IP address.
   2. In Source Port, enter the packets' source port number.
   3. In Protocol, enter the packets' protocol number
   4. In Destination IP, enter the packets' destination IP address.
   5. In Destination Port, enter the packets' destination port number.
7. Click Start. The packet capture begins, and displays its progress:
   1. Packet Capture in Progress—Packet capture stops after 5 minutes, after the file of collected packets reaches 5 MB, or when you click the Stop button.
   2. Preparing file to download—vManage NMS creates a file in libpcap format (a .pcap file).
   3. File ready, click to download the file—Click the download icon to download the generated file.

Simulate Flows

To display the next-hop information for an IP packet (available on vEdge routers only):

1. From the Monitor ▶ Network screen, select the vEdge router.
2. Click Troubleshooting in the left pane.
3. From the Traffic pane, click Simulate Flows.
4. To specify the data traffic path, select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are: • VPN—VPN in which the data tunnel is located. • Source Interface—Interface from which the cflowd flow originates. • Source IP—IP address from which the cflowd flow originates. • Destination IP—Destination IP address of the cflowd flow. • Protocol (under Advanced Options)—Number of the protocol being used to transmit the cflowd flow. The optional fields are: • Application—Application running on the router. • Source Port (under Advanced Options)—Port from which the cflowd flow originates. • Destination Port (under Advanced Options)—Destination port of the cflowd flow. • DSCP (under Advanced Options)—DSCP value in the cflowd packets.
5. Click Advanced Options:
   1. In the Path toggle field, select whether the data traffic path information comes from the service side of the router or from the tunnel side.
   2. Select values or enter data in the required fields (marked with an asterisk [*]) and optional fields. The required fields are: • Protocol—Number of the protocol being used to transmit the cflowd flow. The optional fields are: • Source Port—Port from which the cflowd flow originates. • Destination Port—Destination port of the cflowd flow. • DSCP—DSCP value in the cflowd packets.
   3. Check the All Paths checkbox to display all possible paths for a packet.
6. Click Simulate to determine the next hop that a packet with the specified headers would take.

Check Device Syslog Files

To display the contents of a device's syslog files:

1. In the Administration ▶ Settings screen, ensure that Data Stream is enabled.
2. From the Monitor ▶ Network screen, select the vEdge router.
3. Click Troubleshooting in the left pane.
4. From the Logs pane, click Debug Log.
5. In the Log Files field, select the name of the log file. The lower part of the screen displays the log information.
**View Real-Time Data**

To view real-time data for a device:

1. From the Monitor > Network screen, select a device.
2. Click Real Time. The right pane displays system information about the device.

The right pane contains the following elements:

- Command drop-down—Located directly under the device name, this drop-down allows you to select a feature-specific operational command to display real-time device information for the selected command. The commands in the drop-down are listed alphabetically. The commands available vary depending on the device selected. When you first select Real Time, the System Information command is selected, and real-time system information about the device is displayed in tabular format. For some commands, you can add filters to speed up the display of information. When you select these commands from the drop-down, the Select Filter window is displayed prompting you to either Show Filters or Do Not Filter.
  - Show Filters—Displays the available filters. Fill in the desired fields and click Search to display real-time device information corresponding just to those fields. Clicking Search without filling any of the fields displays the entire information for the selected command.
  - Do Not Filter—Displays the entire real-time device information for the selected command.

- Filter criteria.
- Table with real-time information for the selected command.
  - To re-arrange the columns, drag the column title to the desired position.
  - To change the sort order in a column, click the Up or Down arrow in the column title.

**View Colocation Cluster Information**

To view the cluster information and their health states. Reviewing this information can help you to determine which CSP device is responsible for hosting each VNF in a service chain.

1. In vManage, click Monitor > Network.
2. To monitor clusters, click the Colocation Clusters tab.
   - All clusters with relevant information are displayed in a tabular format. Click a cluster name.

   From the primary part of the left pane, you can view the cluster topology. In the right pane, you can view the cluster information such as the available and total CPU resources, available and allocated memory, and so on, based on Cloud OnRamp for Colocation size.

   The detail part of the left pane contains:
   - Filter criteria—select the fields to be displayed from the search options drop-down.
   - A table that lists information about all devices in the cluster (CSP devices and switches).

   Click a CSP cluster. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, and other core parameters that define performance of a network service.

3. Click the Services tab.
In this tab, you can view:

- All service groups that are attached to the cluster in a tabular format. The first two columns display the name and description of the service chain within the service group.
- Click the **Diagram** button and view the service group with all its service chains and VNFs in the design view window.
- Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
- Select a service group from the **Service Groups** drop-down. The design view displays the selected service group with all its service chains and VNFs.
CHAPTER 6

Security

• Security Overview, on page 468
• Configuring SD-WAN Security, on page 469
• Control Plane Security Overview, on page 470
• Data Plane Security Overview, on page 474
• Configuring Security Parameters, on page 479
• Configuring Single Sign-On Using Okta, on page 485
• Application-Aware Routing, on page 487
• Configuring Firewall Policies, on page 491
• Enterprise Firewall with Application Awareness, on page 498
• Zone-based Firewall Configuration Examples, on page 499
• Configuring Advanced Malware Protection, on page 503
• Configuring Unified Threat Defense, on page 508
• Configuring Cloud OnRamp for IaaS, on page 534
• Configure DHCP, on page 549
• Configuring Single Sign-On using Okta, on page 551
• License Management, on page 554
• IPsec for Cisco IOS XE Routers, on page 560
• Configuring IKE-Enabled IPsec Tunnels, on page 569
• Intrusion Prevention Configuration on SD-WAN, on page 575
• URL Filtering Configuration on vManage, on page 582
• Using Umbrella DNS Security, on page 588
• Umbrella Configuration on SD-WAN, on page 588
• Umbrella Integration Using CLI, on page 596
• Configuring Centralized Control Policy, on page 610
• Configuring Localized Control Policy, on page 639
• Configuring Centralized Data Policy, on page 694
• Centralized Data Policy Configuration Examples, on page 724
• Localized Control Policy, on page 728
• Localized Data Policy, on page 728
• Localized Data Policy Configuration Examples, on page 729
Security Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing. There are multiple problems with the traditional ways of securing networks, including:

- Very little emphasis is placed on ensuring the authenticity of the devices involved in the communication.
- Securing the links between a pair of devices involves tedious and manual setup of keys and shared passwords.
- Scalability and high availability solutions are often at odds with each other.

Cisco SD-WAN Security Components

The Cisco SD-WAN solution takes a fundamentally different approach to security, basing its core design around the following precepts:

- Authentication—The solution ensures that only authentic devices are allowed to send traffic to one another.
- Encryption—All communication between each pair of devices is automatically secure, completely eliminating the overhead involved in securing the links.
- Integrity—No group keys or key server issues are involved in securing the infrastructure.

These three components—authentication, encryption, and integrity—are key to securing the Cisco SD-WAN overlay network infrastructure.

The articles on Control Plane Security Overview and Data Plane Security Overview examine how authentication, encryption, and integrity are implemented throughout the Cisco SD-WAN overlay network. The security discussion refers to the following illustration of the components of the Cisco SD-WAN network—the vSmart controller, the vBond orchestrator, and the vEdge routers. The connections between these devices form the control plane (in orange) and the data plane (in purple), and it is these connections that need to be protected by appropriate measures to ensure the security of the network devices and all network traffic.

Security Provided by NAT Devices

While the primary purpose of NAT devices is to allow devices with private IP addresses in a local-area network (LAN) to communicate with devices in public address spaces, such as the Internet, NAT devices also inherently
provide a level of security, functioning as hardware firewalls to prevent unwanted data traffic from passing through the Cisco SD-WAN edge routers and to the LAN networks in the service-side networks connected to the vEdge router.

To enhance the security at branch sites, you can place the vEdge router behind a NAT device. The vEdge router can interact with NAT devices configured with the following Session Traversal Utilities for NAT (STUN) methods, as defined in RFC 5389:

- **Full-cone NAT, or one-to-one NAT**—This method maps an internal address and port pair to an external address and port. Any external host can send packets to LAN devices behind the vEdge router by addressing them to the external address and port.

- **Address-restricted cone NAT, or restricted-cone NAT**—This method also maps an internal address and port to an external address and port. However, an external host can send packets to the internal device only if the external address (and any port at that address) has received a packet from the internal address and port.

- **Port-restricted cone NAT**—This method is a stricter version of restricted-cone NAT, in which an external host can send packets to the internal address and port only if the external address and port pair has received a packet from that internal address and port. The external device must send packets from the specific port to the specific internal port.

- **Symmetric NAT**—With this method, each request from the same internal IP address and port to an external IP address and port is mapped to a unique external source IP address and port. If the same internal host sends a packet with the same source address and port but to a different destination, the NAT device creates a different mapping. Only an external host that receives a packet from an internal host can send a packet back. vEdge routers support symmetric NAT only on one side of the WAN tunnel. That is, only one of the NAT devices at either end of the tunnel can use symmetric NAT. When a vEdge router operates behind a NAT device running symmetric NAT, only one of the NAT devices at either end of the tunnel can use symmetric NAT. The vEdge router that is behind a symmetric NAT cannot establish a BFD tunnel with a remote vEdge router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT. To allow a vEdge router to function behind a symmetric NAT, you must configure the vManage NMS and vSmart controller control connections to use TLS. DTLS control connections do not work through a symmetric NAT.

### Security for Connections to External Devices

Cisco SD-WAN vEdge routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote user. The Cisco SD-WAN software supports IKE version 2, which performs mutual authentication and establishes and maintains security associations (SAs). IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

### Configuring SD-WAN Security

**Tags recommended by the template:** article:topic-guide

The Cisco SD-WAN security solution provides an integrated security solution that address all key enterprise security profiles: Compliance, Guest Access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).

The Cisco SD-WAN security solution provides an integrated security solution that address all key enterprise security profiles: Compliance, Guest Access, Direct Cloud Access (DCA), and Direct Internet Access (DIA).
Control Plane Security Overview

The control plane of any network is concerned with determining the network topology and defining how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods for providing security are highly manual and do not scale. As examples, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a very secure approach for providing device security.

The Viptela control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The vSmart controller, which is the centralized brain of the Viptela solution, establishes and maintains DTLS or TLS connections to all Viptela devices in the overlay network: to the vEdge routers, the vBond orchestrators, to vManage NMSs, and to other vSmart controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Viptela devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the connections.

The privacy and encryption in the control plane offered by DTLS and TLS provide a safe and secure foundation for the other two security components, authentication and integrity. To perform authentication, the Viptela devices exchange digital certificates. These certificates, which are either installed by the software or hard-coded into the hardware, depending on the device, identify the device and allow the devices themselves to automatically determine which ones belong in the network and which are imposters. For integrity, the DTLS or TLS connections run SHA-1 or SHA-2, a cryptographic secure hash algorithm which ensures that all control and data traffic sent over the connections has not been tampered with.

The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

- **AES-256** encryption algorithm provides encryption services.
- **Digital certificates** are used for authentication.
- **SHA-1 or SHA-2** is responsible for ensuring integrity.

### DTLS and TLS Infrastructure

Security protocols derived from SSL provide the foundation for the Viptela control plane infrastructure.

The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Viptela control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security for TCP-based traffic. (TLS itself evolved from SSL.) The Viptela infrastructure design uses DTLS running over UDP to avoid some
of the issues with TCP, including the delays associated with stream protocols and some security issues. However, because UDP performs no handshaking and sends no acknowledgments, DTLS has to handle possible packet re-ordering, loss of datagrams, and data larger than the datagram packet size.

The control plane infrastructure can also be configured to run over TLS. This might be desirable in situations where the protections of TCP outweigh its issues. For example, firewalls generally offer better protection for TCP servers than for UDP servers.

The Viptela software implements the standard version of DTLS with UDP, which is defined in RFC 6347. DTLS for use with other protocols is defined in a number of other RFCs. For TLS, the Viptela software implements the standard version defined in RFC 5246.

In the Viptela architecture, the Viptela devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the vSmart controllers, vBond orchestrators, vManage NMSs, and vEdge routers join the network, they create provisional DTLS or TLS tunnels between them as part of the device authentication process. After the authentication process completes successfully, the provisional tunnels between the vEdge routers and vSmart controllers, and those between the vBond orchestrators and vSmart controllers, become permanent and remain up as long as the devices are active in the network. It is these authenticated, secure DTLS or TLS tunnels that are used by all the protocol applications running on the Viptela devices to transport their traffic. For example, an OMP session on a vEdge router communicates with an OMP session on a vSmart controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. (The Overlay Management Protocol is the Viptela control protocol used to exchange routing, policy, and management information among Viptela devices, as described in Overlay Routing Overview.)

A Viptela daemon running on each vSmart controller and vEdge router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called vdaemon and is discussed later in this article. After the control plane DTLS or TLS connections are established between these devices, multiple protocols can create sessions to run and route their traffic over these connections—including OMP, Simple Network Management Protocol (SNMP), and Network Configuration Protocol (Netconf)—without needing to be concerned with any security-related issues. The session-related traffic is simply directed over the secure connection between the vEdge routers and vSmart controllers.
Control Plane Authentication

The Viptela control plane uses digital certificates with 2048-bit RSA keys to authenticate the Viptela devices in the network. The digital certificates are created, managed, and exchanged by standard components of the public key infrastructure, or PKI:

- **Public keys**—These keys are generally known.
- **Private keys**—These keys are private. They reside on each Viptela device and cannot be retrieved from the device.
- **Certificates** signed by a root certification authority (CA)—The trust chain associated with the root CA needs to be present on all Viptela devices.

In addition to standard PKI components, the Viptela device serial numbers and the vEdge router chassis numbers are used in the authentication processes.

Let's first look at the PKI components that are involved in device authentication. On vEdge routers, the public and private keys and the certificates are managed automatically, by a Trusted Board ID chip that is built into the router. When the routers are manufactured, this chip is programmed with a signed certificate, which includes the device's public key and its serial number, and the device's private key. When the vEdge routers boot up and join the network, they exchange their certificates (including the device's public key and serial number) with other Viptela devices as part of the device authentication process. For networks with thousands or tens of thousands of vEdge routers, providing an automated process for managing keys and certificates greatly simplifies the task of maintaining security across the edge devices in the network. (Note that the vEdge router's private key always remains embedded in the router's Trusted Board ID chip, and it is never distributed, nor can it ever be retrieved from the device. In fact, any brute-force attempt to read the private key causes the Trusted Board ID chip to fail, thereby disabling all access to the router.)

For vSmart controllers, vBond orchestrators, and vManage NMS systems, the public and private keys and the certificates are managed manually. When you boot these devices for the first time, the Viptela software generates a unique private key–public key pair for each software image. The public key needs to be signed by the CA root. The network administrator then requests a signed certificate and manually installs it and the certificate chains on the vSmart controllers, vBond orchestrators, and vManage NMS systems. A typical network might have only a small handful of vSmart controllers, vBond orchestrators, and vManage NMSs, so the burden of manually managing the keys and certificates on these devices is small.

To augment these standard PKI components, the Viptela software uses the device serial numbers in performing automatic device authentication. Specifically, it uses the vEdge and vSmart serial numbers and the vEdge chassis numbers. When a batch of vEdge routers is shipped, the manufacturer sends a text file that lists the serial numbers of the vEdge routers and the corresponding chassis numbers. For the vSmart controllers, when the network administrator receives the signed certificate, they should extract the serial numbers from the certificates and place them into a single text file, one serial number per line. Then the network administrator manually installs these two files. The file received from the manufacturer that lists all valid vEdge serial and chassis numbers is uploaded and installed on vSmart controllers. Both the vEdge authorized serial number file and the file listing the vSmart serial numbers are uploaded and installed on vBond orchestrators. Then, during the automatic authentication process, as pairs of devices are establishing DTLS control connections between them, each device compares the serial numbers (and for vEdge routers, the chassis numbers) to those in the files installed on the device. A device allows a connection to be established only if the serial number or serial–chassis number combination (for a vEdge router) matches.

You can display the installed vSmart authorized serial numbers using the `show control valid-vsmarts` command on a vSmart controller or a vEdge router and the `show orchestrator valid-vsmarts` command on a vBond orchestrator. You can display the installed vEdge authorized serial and chassis number associations...
using the **show control valid-vedges** command on a vSmart controller and the **show orchestrator valid-devices** command on a vBond orchestrator

Now, let's look at how the PKI authentication components and the device serial and chassis numbers are used to authenticate devices on the Viptela overlay network. When vSmart controllers, vBond orchestrators, and vEdge routers first boot up, they establish secure DTLS or TLS connections between them. Over these connections, the devices authenticate each other, using the public and private keys, the signed certificates, and the device serial numbers and performing a series of handshake operations to ensure that all the devices on the network are valid and not imposters. The following figure illustrates the key and certificate exchange that occurs when the Viptela devices boot. For details about the authentication that occurs during the bringup process, see Bringup Sequence of Events.

**Control Plane Encryption**

Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocol encrypt the control plane traffic that is sent across the connections between Viptela devices to validate the integrity of the data. TLS uses asymmetric cryptography for authenticating key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

A single Viptela device can have DTLS or TLS connections to multiple Viptela devices, so vdaemon creates a kernel route for each destination. For example, a vEdge router would typically have one kernel route, and hence one DTLS or TLS connection, for each vSmart controller. Similarly, a vSmart controller would have one kernel route and one DTLS or TLS connection for each vEdge router in its domain.
Control Plane Integrity

The Viptela design implements control plane integrity by combining two security elements: SHA-1 or SHA-2 message digests, and public and private keys.

SHA-1 and SHA-2 are cryptographic hash functions that generate message digests (sometimes called simply digests) for each packet sent over a control plane connection. SHA-1 generates a 160-bit message digest. SHA-2 is a family that consists of six hash functions with digests that are 224, 256, 384, or 512 bits. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. Both SHA-1 and SHA-2 allow verification that the packet's contents have not been tampered with.

The second component of control plane integrity is the use of public and private keys. When a control plane connection is being established, a local Viptela device sends a challenge to a remote device. The remote device encrypts the challenge by signing it with its private key, and returns the signed challenge to the local device. The local device then uses the remote device's public key to verify that the received challenge matches the sent challenge.

Then, once a control plane connection is up, keys are used to ensure that packets have been sent by a trusted host and were not inserted midstream by an untrusted source. The authenticity of each packet is verified through encryption and decryption with symmetric keys that were exchanged during the process of establishing the control connection.

Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the vEdge routers in the Viptela overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone would be able to sniff the traffic, and it would be easy to implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Viptela data plane is the security of the control plane. Because the control plane is secure—all devices are validated, and control traffic is encrypted and cannot be tampered with—we can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of vEdge routers.

The data plane provides the infrastructure for sending data traffic among the vEdge routers in the Viptela overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Viptela data plane implements the key security components of authentication, encryption, and integrity in the following ways:
Authentication—As mentioned above, the Viptela control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:

- RSA encryption with 2048-bit keys.
- Two standard protocols from the IPsec security suite framework, Encapsulation Security Payload (ESP) and Authentication Header (AH), are used to authenticate the origin of data traffic.

Encryption—The standard ESP protocol protects the data packet’s payload, and the standard AH protocol protects both the payload and the non-mutable header fields. Key exchange encryption is done using the AES-256 cipher.

Integrity—To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:

- The ESP protocol encapsulates the payload of data packets.
- The HMAC-SHA1 algorithm, which is used by the IPsec AH protocol, combines a keyed-hash authentication code with SHA-1 cryptography to ensure data integrity. AH encapsulates the non-mutable fields in the outer IP header and the payload of data packets. You can configure the integrity methods supported on each vEdge router, and this information is exchanged in the router's TLOC properties. If two vEdge peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
- The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

Data Plane Authentication and Encryption

Before a pair of vEdge routers can exchange data traffic, they establish an IPsec connection between them, which they use as a secure communications channel, and then the routers authenticate each other over this connection. As with the control plane, the data plane uses keys to perform Viptela device authentication.

In a traditional IPsec environment, key exchange is handled by the Internet Key Exchange (IKE) protocol. IKE first sets up secure communications channels between devices and then establishes security associations (SAs) between each pair of devices that want to exchange data. IKE uses a Diffie-Hellman key exchange algorithm to generate a shared key that encrypts further IKE communication. To establish SAs, each device exchanges keys with every other device in the network and creates per-pair keys, generating a unique key for each remote device. This scheme means that in a fully meshed network, each device has to manage n² key exchanges and (n-1) keys. As an example, in a 1,000-node network, 1,000,000 key exchanges are required to authenticate the devices, and each node is responsible for maintaining and managing 999 keys.

The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- The handshaking required to set up the communications channels is both time consuming and resource intensive.
The processing required for the key exchange, especially in larger networks, can strain network resources and can take a long time.

The Viptela implementation of data plane authentication and encryption establishes SAs between each pair of devices that want to exchange data, but it dispenses with IKE altogether. Instead, to provide a scalable solution to data plane key exchange, the Viptela solution takes advantage of the fact that the DTLS control plane connections in the Viptela overlay network are known to be secure. Because the Viptela control plane establishes authenticated, encrypted, and tamperproof connections, there is no need in the data plane to set up secure communications channels to perform data plane authentication.

In the Viptela network, data plane encryption and key generation are done by AES-256, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each vEdge router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the vEdge router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other vEdge routers in the network. In this way, the AES keys for all the vEdge routers are distributed across the network. Even though the key exchange is symmetric, Viptela devices use it in an asymmetric fashion. The result is a simple and scalable key exchange process that does not use per-pair keys.

If control policies configured on a vSmart controller limit the communications channels between network devices, the reachability advertisements sent by the vSmart controller contain information only for the vEdge routers that they are allowed to exchange data with. So, a vEdge router learns the keys only for those vEdge routers that they are allowed to communicate with.

To further strengthen data plane authentication and encryption, vEdge routers regenerate their AES keys aggressively (by default, every 24 hours). Also, the key regeneration mechanism ensures that no data traffic is dropped when keys change.

In the Viptela overlay network, the liveness of SAs between vEdge router peers is tracked by monitoring BFD packets, which are periodically exchanged over the IPsec connection between the peers. IPsec relays the connection status to the vSmart controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the vSmart controller learns that the connection has been lost.

The Viptela IPsec software has no explicit SA idle timeout, which specifies the time to wait before deleting SAs associated with inactive peers. Instead, an SA remains active as long as the IPsec connection between two vEdge routers is up, as determined by the periodic exchange of BFD packets between them. Also, the frequency with which SA keys are regenerated obviates the need to implement an implicit SA idle timeout.

In summary, the Viptela data plane authentication offers the following improvements over IKE:
• Because only \( n + 1 \) keypaths are required rather than \( n^2 \) required by IKE, the Viptela solution scales better as the network grows large.

• Keys are generated and refreshed locally, and key exchange is performed over a secure control plane.

• No key server is required, and thus there is no need to worry about high availability requirements of a key server.

Data Plane Integrity
A number of components contribute to the integrity of data packets in the Viptela data plane:

• ESP, which is the standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets.

• AH, which is the standard IPsec authentication protocol, protects (via authentication) the entire data packet, including the inner and outer headers, data packet payload, and ESP trailer.

• Anti-replay, which is also part of the standard IPsec software suite, provides a mechanism to number all data packets and to ensure that receiving routers accept only packets with unique numbers.

The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet’s payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet's payload and inner header fields and places the resultant hash (also called a digest) into a 12-byte HMAC-SHA1 field at the end of the packet. (A hash is a one-way compression.) The receiving device performs the same checksum and compares its calculated hash with that in the packet. If the two checksums match, the packet is accepted. Otherwise, it is dropped. In the figure below, the left stack illustrates the ESP/UDP encapsulation. ESP encrypts and authenticates the inner headers, payload, MPLS label (if present), and ESP trailer fields, placing the HMAC-SHA1 hash in the ICV checksum field at the end of the packet. The outer header fields added by ESP/UDP are neither encrypted nor authenticated.

A second component that contributes to data packet integrity is AH, the standard IPsec authentication protocol, which protects all fields in a data packet via authentication. AH performs a checksum process similar to that done by ESP, except that instead of calculating the checksum over just the payload and inner IP header fields, it calculates it over all the fields in the packet—the payload, the inner header, and all the non-mutable fields in the outer IP header. AH places the resultant HMAC-SHA1 hash into the last field of the packet. As with ESP, AH on the receiving device performs the same checksum, and accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by AH, in combination with ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now AH authenticates the entire packet—the outer IP and UDP headers, the ESP header, the MPLS label (if present), the original packet, and the ESP trailer—and places its calculated HMAC-SHA1 hash into the ICV checksum field at the end of the packet.

For situations in which data packet authentication is not required, you can disable data packet authentication altogether. In this case, data packets are processed just by ESP, which encrypts the original packet, the MPLS label (if present), and the ESP trailer. This scheme is illustrated in the right stack in the figure below.
Note that Viptela devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the HMAC-SHA1 digest. Both are distributed as part of the TLOC properties for a vEdge router.

Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this type of attack, an adversary tampers with the data traffic by inserting a copy of a message that was previously sent by the source. If the destination cannot distinguish the replayed message from a valid message, it may authenticate the adversary as the source or may incorrectly grant to the adversary unauthorized access to resources or services.

As a counter to such attacks, the Viptela overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, and it drops all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.

When the destination receives a packet whose sequence number is larger than the highest number in the sliding window, it slides the window to the right, thus changing the range of valid sequences numbers it will accept. This scheme protects against an MITM type of attack because, by choosing the proper window size, you can ensure that if a duplicate packet is inserted into the traffic stream, its sequence number will either be within the current range but will be a duplicate, or it will be smaller than the lowest current value of the sliding window. Either way, the destination will drop the duplicate packet. So, the sequence numbering combined with a sliding window provide protection against MITM type of attacks and ensure the integrity of the data stream flowing within the IPsec connection.
Carrying VPN Information in Data Packets

For enterprise-wide VPNs, Viptela devices support MPLS extensions to data packets that are transported within IPsec connections. The figure to the right shows the location of the MPLS information in the data packet header. These extensions provide the security for the network segmentation (that is, for the VPNs) that is needed to support multi-tenancy in a branch or segmentation in a campus. The Viptela implementation uses IPsec UDP-based overlay network layer protocol encapsulation as defined in RFC 4023. The security is provided by including the Initialization Vector (IV) at the beginning of the payload data in the ESP header. The IV value is calculated by the AES-256 cipher block chaining (CBC).

Configuring Security Parameters

How to change security parameters for the control plane and the data plane in the Viptela overlay network. This article describes how to change security parameters for the control plane and the data plane in the Viptela overlay network.

Configure Control Plane Security Parameters

By default, the control plane uses DTLS as the protocol that provides privacy on all its tunnels. DTLS runs over UDP.

You can change the control plane security protocol to TLS, which runs over TCP. The primary reason to use TLS is that, if you consider the vSmart controller to be a server, firewalls protect TCP servers better than UDP servers.

You configure the control plane tunnel protocol on a vSmart controller:

```
vSmart(config)# security control protocol tls
```
With this change, all control plane tunnels between the vSmart controller and vEdge routers and between the controller and vManage NMSs use TLS. Control plane tunnels to vBond orchestrators always use DTLS, because these connections must be handled by UDP.

In a domain with multiple vSmart controllers, when you configure TLS on one of the vSmart controllers, all control plane tunnels from that controller to the other controllers use TLS. Said another way, TLS always takes precedence over DTLS. However, from the perspective of the other vSmart controllers, if you have not configured TLS on them, they use TLS on the control plane tunnel only to that one vSmart controller, and they use DTLS tunnels to all the other vSmart controllers and to all their connected vEdge routers. To have all vSmart controllers use TLS, configure it on all of them.

By default, the vSmart controller listens on port 23456 for TLS requests. To change this:

```
vSmart(config)# security control tls-port number
```

The port can be a number from 1025 through 65535.

To display control plane security information, use the `show control connections` command on the vSmart controller. For example:

```
vSmart-2# show control connections

<table>
<thead>
<tr>
<th>PEER</th>
<th>SITE</th>
<th>DOMAIN</th>
<th>PEER</th>
<th>PRIVATE</th>
<th>PORT</th>
<th>PUBLIC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>dtls</td>
<td>172.16.255.11</td>
<td>100</td>
<td>1</td>
<td>10.0.5.11</td>
<td>12346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12346</td>
<td>lte</td>
<td>up</td>
<td>0:07:48:58</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>dtls</td>
<td>172.16.255.21</td>
<td>100</td>
<td>1</td>
<td>10.0.5.21</td>
<td>12346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12346</td>
<td>lte</td>
<td>up</td>
<td>0:07:48:51</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>dtls</td>
<td>172.16.255.14</td>
<td>400</td>
<td>1</td>
<td>10.1.14.14</td>
<td>12360</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.1.14.14</td>
<td>12360</td>
<td>up</td>
<td>0:07:49:02</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>dtls</td>
<td>172.16.255.15</td>
<td>500</td>
<td>1</td>
<td>10.1.15.15</td>
<td>12346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.1.15.15</td>
<td>12346</td>
<td>up</td>
<td>0:07:47:18</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>dtls</td>
<td>172.16.255.16</td>
<td>600</td>
<td>1</td>
<td>10.1.16.16</td>
<td>12346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.1.16.16</td>
<td>12346</td>
<td>up</td>
<td>0:07:41:52</td>
<td></td>
</tr>
<tr>
<td>vsmart</td>
<td>tls</td>
<td>172.16.255.19</td>
<td>100</td>
<td>1</td>
<td>10.0.5.19</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12345</td>
<td>default</td>
<td>up</td>
<td>0:00:01:44</td>
<td></td>
</tr>
<tr>
<td>vbond</td>
<td>dtls</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>10.1.14.14</td>
<td>12346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12346</td>
<td>default</td>
<td>up</td>
<td>0:07:49:08</td>
<td></td>
</tr>
</tbody>
</table>

vSmart-2 control connections

<table>
<thead>
<tr>
<th>PEER</th>
<th>SITE</th>
<th>DOMAIN</th>
<th>PEER</th>
<th>PRIVATE</th>
<th>PORT</th>
<th>PUBLIC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>tls</td>
<td>172.16.255.11</td>
<td>100</td>
<td>1</td>
<td>10.0.5.11</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12345</td>
<td>lte</td>
<td>up</td>
<td>0:00:01:18</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>tls</td>
<td>172.16.255.21</td>
<td>100</td>
<td>1</td>
<td>10.0.5.21</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12345</td>
<td>lte</td>
<td>up</td>
<td>0:00:01:18</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>tls</td>
<td>172.16.255.14</td>
<td>400</td>
<td>1</td>
<td>10.1.14.14</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.1.14.14</td>
<td>12345</td>
<td>up</td>
<td>0:00:01:18</td>
<td></td>
</tr>
<tr>
<td>vedge</td>
<td>tls</td>
<td>172.16.255.15</td>
<td>500</td>
<td>1</td>
<td>10.1.15.15</td>
<td>12345</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.1.15.15</td>
<td>12345</td>
<td>up</td>
<td>0:00:01:18</td>
<td></td>
</tr>
</tbody>
</table>
Configure DTLS on vManage NMS

If you configure the vManage NMS to use TLS as the control plane security protocol, you must enable port forwarding on your NAT. If you are using DTLS as the control plane security protocol, you do not need to do anything.

The number of ports forwarded depends on the number of vdaemon processes running on the vManage NMS. To display information about these processes and about the number of ports that are being forwarded, use the `show control summary` command shows that four vdaemon processes are running:

```
vManage# show control summary

<table>
<thead>
<tr>
<th>INSTANCE</th>
<th>VBOND COUNTS</th>
<th>VMANAGE COUNTS</th>
<th>VSMART COUNTS</th>
<th>VEDGE COUNTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
```

To see the listening ports, use the `show control local-properties` command:

```
vManage# show control local-properties

organization-name       vP tela Inc Test
certificate-status      Installed
root-ca-chain-status   Installed

certificate-validity    Valid
certificate-not-valid-before May 20 00:00:00 2015 GMT
certificate-not-valid-after  May 20 23:59:59 2016 GMT

dns-name     vbond.viptela.com
site-id       5000
domain-id     0
protocol      dtls
tls-port      23456
...

number-active-wan-interfaces 1

<table>
<thead>
<tr>
<th>INDEX</th>
<th>INTERFACE</th>
<th>IP</th>
<th>CARRIER</th>
<th>ADMIN</th>
<th>OPERATION</th>
<th>LAST</th>
<th>PRIVATE</th>
<th>VSMARTS</th>
<th>MANAGES</th>
<th>COLOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>eth0</td>
<td>72.28.108.37</td>
<td>default</td>
<td>up</td>
<td>up</td>
<td>0:00:00:08</td>
<td>silver</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

This output shows that the listening TCP port is 23456. If you are running vManage NMS behind a NAT, you should open the following ports on the NAT device:

- 23456 (base - instance 0 port)
- 23456 + 100 (base + 100)
- $23456 + 200 \text{ (base + 200)}$
- $23456 + 300 \text{ (base + 300)}$

Note that the number of instances is the same as the number of cores you have assigned for the vManage NMS, up to a maximum of 8.

**Configure Data Plane Security Parameters**

In the data plane, IPsec is enabled by default on all vEdge routers, and by default IPsec tunnel connections use the AH-SHA1 HMAC for authentication on the IPsec tunnels. On vEdge routers, you can change the type of authentication, and you can modify the IPsec rekeying timer and the size of the IPsec anti-replay window.

**Configure Allowed Authentication Types**

By default, IPsec tunnel connections use AH-SHA1 HMAC and ESP HMAC-SHA1 for authentication, choosing whichever authentication method is stronger. To modify the negotiated authentication types or to disable authentication, use the following command:

```
vEdge(config)# security ipsec authentication-type (ah-no-id | ah-shal-hmac | none | sha1-hmac)
```

Configure each authentication type with a separate `security ipsec authentication-type` command. The command options map to the following authentication types, which are listed in order from most strong to least strong:

- **ah-shal-hmac** enables AH-SHA1 HMAC and ESP HMAC-SHA1.
- **ah-no-id** enables a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1. This option accommodates some non-Viptela devices, including the Apple AirPort Express NAT, that have a bug that causes the ID field in the IP header, a non-mutable field, to be modified. Configure the **ah-no-id** option in the list of authentication types to have the Viptela AH software ignore the ID field in the IP header so that the Viptela software can work in conjunction with these devices.
- **sha1-hmac** enables ESP HMAC-SHA1.
- **none** maps to no authentication. You can choose this option in situations where data plane authentication and integrity are not a concern.

For information about which data packet fields are affected by these authentication types, see the "Data Plane Integrity" section in Data Plane Security Overview.

vEdge routers advertise their configured authentication types in their TLOC properties. The two routers on either side of an IPsec tunnel connection negotiate the authentication to use on the connection between them, using the strongest authentication type that is configured on both of the routers. For example, if one vEdge router advertises AH-HMAC-SHA1, ESP HMAC-SHA1, and none, and a second vEdge router advertises ESP HMAC-SHA1 and none, the two routers negotiate to use ESP HMAC-SHA1 on the IPsec tunnel connection between them. If no common authentication types are configured on the two vEdge peers, no IPsec tunnel is established between them.

The encryption algorithm on IPsec tunnel connections is either AES-256-GCM or AES-256-CBC. For unicast traffic, if the remote side supports AES-256-GCM, that encryption algorithm is used. Otherwise, AES-256-CBC is used. For multicast traffic, the encryption algorithm is AES-256-CBC. You cannot modify the choice made by the software.

When the IPsec authentication type is changed, the AES key for the data path is changed.
Change the Rekeying Timer

Before vEdge routers can exchange data traffic, they set up a secure authenticated communications channel between them. The vEdge routers use the DTLS or TLS control plane connection between them as the channel, and they use the AES-256 cipher to perform encryption. Each vEdge router generates a new AES key for its data path periodically.

By default, a key is valid for 86400 seconds (24 hours), and the timer range is 10 seconds through 1209600 seconds (14 days). To change the rekey timer value:

```
vdEdge(config)# security ipsec
                        rekey
                                    seconds
```

The configuration looks like this:

```
security
    ipsec
        rekey seconds
    !
```

When the IPsec keys are compromised, you can generate new keys immediately, without modifying the configuration of the vEdge router. To do this, issue the `request security ipsec-rekey` command on the compromised vEdge router.

For example, the following output shows that the local SA has a SPI (key) of 256:

```
vEdge# show ipsec local-sa
TLOC ADDRESS TLOC COLOR  SPI  SOURCE SOURCE IP PORT KEY HASH
--------------------------------------------------------------------
172.16.255.15 lte 256 10.1.15.15 12346 *****b93a
```

If this key is compromised, use the `request security ipsec-rekey` command to generate a new key immediately. This command increments the existing key, so in our example the SPI changes to 257:

```
vEdge# request security ipsec-rekey
vEdge# show ipsec local-sa
TLOC ADDRESS TLOC COLOR  SPI  SOURCE SOURCE IP PORT KEY HASH
--------------------------------------------------------------------
172.16.255.15 lte 257 10.1.15.15 12346 *****b93a
```

After the new key is generated, the vEdge router sends it immediately to all its DTLS or TLS peers, and they begin using it as soon as they receive it. Note that the old compromised SPI (256) will continue to be used for a short period of time, until it times out.

To stop using the compromised key immediately, issue the `request security ipsec-rekey` command twice, in quick succession. This sequence of commands removes both SPI 256 and 257, and sets the key to 258. Note, however, that some packets will be dropped for a short period of time, until all the remote vEdge routers learn the new key.

```
vEdge# request security ipsec-rekey
vEdge# request security ipsec-rekey
vEdge# ipsec local-sa
```
Change the Size of the Anti-Replay Window

IPsec authentication provides anti-replay protection by assigning a unique sequence number to each packet in a data stream. This sequence numbering protects against an attacker duplicating data packets. With anti-replay protection, the sender assigns monotonically increasing sequence numbers, and the destination checks these sequence numbers to detect duplicates. Because packets often do not arrive in order, the destination maintains a sliding window of sequence numbers that it will accept.

Packets with sequence numbers that fall to the left of the sliding window range are considered old or duplicates, and the destination drops them. The destination tracks the highest sequence number it has received, and adjusts the sliding window when it receives a packet with a higher value.

By default, the sliding window is set to 512 packets. It can be set to any value between 64 and 8192 that is a power of 2 (that is, 64, 128, 256, 512, 1024, 2048, 4096, or 8192). To modify the anti-replay window size, use the `replay-window` command, specifying the size of the window:

```
vEdge(config)# security ipsec replay-window number
```

The configuration looks like this:

```
security
  ipsec
    replay-window number
  !
!```
ones. This occurs because QoS reorders packets, giving higher-priority packets preferential treatment and delaying lower-priority packets. To minimize or prevent this situation, increase the size of the anti-replay window.

**Configuring Single Sign-On Using Okta**

Okta provides secure identity management software that lets you connect any person with any application on any device using Single Sign-On (SSO).

**Configuring Okta on the vManage UI**

**Step 1**  
In vManage, click **Administration > Settings > Identify Provider Settings > Edit.**

**Step 2**  
Click **Enabled.**

**Step 3**  
Navigate to **Click here to download the SAML metadata** and save the content in a file. This data is used for configuring Okta.

**Step 4**  
In Metadata, you need the following information to configure Okta with vManage:

- Entity ID
- Signing certificate
- Encryption certificate
- Logout URL
- Login URL

**Configuring SSO on the Okta website**

**Step 1**  
Log on to the Okta website.

**Step 2**  
Create a username using your email address.

**Step 3**  
Make sure you are using the Classic UI view on Okta. If not, change your view to the Classic UI view by clicking on the **Admin** button in the upper-right corner. On the next page in the upper-left corner, switch from the Developer Console view to the Classic UI view.

**Step 4**  
Navigate to **Add applications > Add application.**

**Step 5**  
Select **SAML 2.0** and click **Create.**

**Step 6**  
Use a string for **Application name.**

**Step 7**  
(Optional) Upload a logo and then click **Next.**

**Step 8**  
At **SAML Settings,** add the SSO URL using the **samlLoginResponse** URL from the downloaded metadata from the vManage UI.

**Step 9**  
Copy the entityID string and paste it in the **Service Provider ID** field.

**Step 10**  
For **Name ID format,** select **Email Address** and then click **Enter.**
Step 11  
For **Application username**, select **Okta username**.

Step 12  
For **Show Advanced Settings**, enter the fields as indicated below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Value</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Assertion Signature</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>RSA-SHA256</td>
<td></td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>SHA256</td>
<td></td>
</tr>
<tr>
<td>Assertion Encryption</td>
<td>Encrypted</td>
<td></td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES256-CBC</td>
<td></td>
</tr>
<tr>
<td>Encryption Certificate</td>
<td></td>
<td><strong>1.</strong> Copy the encryption certificate from the metadata you downloaded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2.</strong> Go to <a href="http://www.samltool.com">www.samltool.com</a> and click on <strong>X.509 CERTS</strong>, paste there. Click <strong>Format X.509 Certificate</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>3.</strong> Make sure to remove the last empty line and then save the output (<strong>X.509.cert with header</strong>) into a text file <strong>encryption.cer</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>4.</strong> Upload the file. The Firefox browser may not allow you to do the upload. You can use the Chrome browser, however. You should see the certificate information after uploading to Okta.</td>
</tr>
<tr>
<td>Enable Single Logout</td>
<td></td>
<td>Make sure this is checked.</td>
</tr>
<tr>
<td>Single Logout URL</td>
<td></td>
<td>Get from the metadata.</td>
</tr>
<tr>
<td>SP Issuer</td>
<td></td>
<td>Use the entityID from the metadata.</td>
</tr>
<tr>
<td>Signature Certificate</td>
<td></td>
<td><strong>1.</strong> Obtain from the metadata. Format the signature certificate using <a href="http://www.samltool.com">www.samltool.com</a> as done above.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>2.</strong> Save to a file, for example, <strong>signing.cer</strong> and upload.</td>
</tr>
<tr>
<td>Authentication context class</td>
<td>X.509 Certificate</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Value</td>
<td>Configuration</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Honor Force Authentication</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SAML issuer ID string</td>
<td>SAML issuer ID string</td>
<td></td>
</tr>
<tr>
<td>Attributes Statements (optional)</td>
<td>Name &gt; Username</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name format (optional) &gt; Unspecified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value &gt; user.login</td>
<td></td>
</tr>
<tr>
<td>Group Attribute Statements (optional)</td>
<td>Name &gt; Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name format (optional) &gt; Unspecified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filter &gt; &quot;Regex&quot;.~.&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**Note** It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

**Step 13** Click Next.
**Step 14** For **App type**, check **This is an internal app that we have created** (optional).
**Step 15** Click **Finish**.

This brings you to the Okta application page.

**Step 16** Click on **View Setup Instructions**.
**Step 17** Copy the IDP metadata.
**Step 18** Navigate back to the vManage UI.
**Step 19** Click on **Identity Provider Settings**.
**Step 20** Paste the IDP metadata that you copied on to **Upload Identity Provider Metadata**, and then click **Save**.

**Assigning Users to the Application in Okta**

**Step 1** On the Okta application page, navigate to **Assignments > People > Assign**.
**Step 2** Select **Assign to people** from the drop-down menu.
**Step 3** Click on **Assign** next to the users(s) you selected and click **Done**.
**Step 4** Click **Done**.
**Step 5** To add a user, click on **Directory > Add > Person > Save**.

**Application-Aware Routing**

Application-aware routing tracks network and path characteristics of the data plane tunnels between vEdge routers and uses the collected information to compute optimal paths for data traffic. These characteristics
include packet loss, latency, and jitter, and the load, cost and bandwidth of a link. The ability to consider factors in path selection other than those used by standard routing protocols—such as route prefixes, metrics, link-state information, and route removal on the edge router—offers a number of advantages to an enterprise:

- In normal network operation, the path taken by application data traffic through the network can be optimized, by directing it to WAN links that support the required levels of packet loss, latency, and jitter defined in an application’s SLA.

- In the face of network brownouts or soft failures, performance degradation can be minimized. The tracking of network and path conditions by application-aware routing in real time can quickly reveal performance issues, and it automatically activates strategies that redirect data traffic to the best available path. As the network recovers from the brownout or soft failure conditions, application-aware routing automatically readjusts the data traffic paths.

- Network costs can be reduced because data traffic can be more efficiently load-balanced.

- Application performance can be increased without the need for WAN upgrades.

Components of Application-Aware Routing

The Viptela Application-Aware Routing solution consists of three elements:

- **Identification**—You define the application of interest, and then you create a centralized data policy that maps the application to specific SLA requirements. You single out data traffic of interest by matching on the Layer 3 and Layer 4 headers in the packets, including source and destination prefixes and ports,

Each vEdge router supports up to eight TLOCs, allowing a single vEdge router to connect to up to eight different WAN networks. This capability allows path customization for application traffic that has different needs in terms of packet loss and latency.
protocol, and DSCP field. As with all centralized data policies, you configure them on a vSmart controller, which then passes them to the appropriate vEdge routers.

• **Monitoring and measuring**—The Viptela software uses BFD packets to continuously monitor the data traffic on the data plane tunnels between vEdge routers, and periodically measures the performance characteristics of the tunnel. To gauge performance, the Viptela software looks for traffic loss on the tunnel, and it measures latency by looking at the one-way and round-trip times of traffic traveling over the tunnel. These measurements might indicate a blackout or brownout condition.

• **Mapping application traffic to a specific transport tunnel**—The final step is to map an application’s data traffic to the data plane tunnel that provides the desired performance for the application. The mapping decision is based on two criteria: the best-path criteria computed from measurements performed on the WAN connections and on the constraints specified in a policy specific to application-aware routing.

To create data policy based on the Layer 7 application itself, use configure deep packet inspection with a centralized data policy. With deep packet inspection, you can direct traffic to a specific tunnel, based on the remote TLOC, the remote TLOC, or both. You cannot direct traffic to tunnels based on SLA classes.

**Classification of Tunnels into SLA Classes**

The process of classifying tunnels into one or more SLA classes for application-aware routing has three parts:

• Measure loss, latency, and jitter information for the tunnel.

• Calculate the average loss, latency, and jitter for the tunnel.

• Determine the SLA classification of the tunnel.
**Measure Loss, Latency, and Jitter**

When a data plane tunnel in the overlay network is established, a BFD session automatically starts on the tunnel. In the overlay network, each tunnel is identified with a color that identifies a specific link between a local TLOC and a remote TLOC. The BFD session monitors the liveness of the tunnel by periodically sending Hello packets to detect whether the link is operational. Application-aware routing uses the BFD Hello packets to measure the loss, latency, and jitter on the links.

By default, the BFD Hello packet interval is 1 second. This interval is user-configurable (with the `bfd color interval` command). Note that the BFD Hello packet interval is configurable per tunnel.

**Calculate Average Loss, Latency, and Jitter**

BFD periodically polls all the tunnels on the vEdge router to collect packet latency, loss, jitter, and other statistics for use by application-aware routing. At each poll interval, application-aware routing calculates the average loss, latency, and jitter for each tunnel, and then calculates or recalculates each tunnel's SLA. Each poll interval is also called a "bucket."

By default, the poll interval is 10 minutes. With the default BFD Hello packet interval at 1 second, this means that information from about 600 BFD Hello packets is used in one poll interval to calculate loss, latency, and jitter for the tunnel. The poll interval is user-configurable (with the `bfd app-route poll-interval` command). Note that the application-aware routing poll interval is configurable per vEdge router; that is, it applies to all tunnels originating on a router.

Reducing the poll interval without reducing the BFD Hello packet interval may affect the quality of the loss, latency, and jitter calculation. For example, setting the poll interval to 10 seconds when the BFD Hello packet interval is 1 second means that only 10 Hello packets are used to calculate the loss, latency, and jitter for the tunnel.

The loss, latency, and jitter information from each poll interval is preserved for six poll intervals. At the seventh poll interval, the information from the earliest polling interval is discarded to make way for the latest information. In this way, application-aware routing maintains a sliding window of tunnel loss, latency, and jitter information.

The number of poll intervals (6) is not user-configurable. Each poll interval is identified by an index number (0 through 5) in the output of the `show app-route statistics` command.

**Determine the SLA Classification**

To determine the SLA classification of a tunnel, application-aware routing uses the loss, latency, and jitter information from the latest poll intervals. The number of poll intervals used is determined by a multiplier. By default, the multiplier is 6, so the information from all the poll intervals (specifically, from the last six poll intervals) is used to determine the classification. For the default poll interval of 10 minutes and the default multiplier of 6, the loss, latency, and jitter information collected over the last hour is considered when classifying the SLA of each tunnel. These default values have to be chosen to provide damping of sorts, as a way to prevent frequent reclassification (flapping) of the tunnel.

The multiplier is user-configurable (with the `bfd app-route multiplier` command). Note that the application-aware routing multiplier is configurable per vEdge router; that is, it applies to all tunnels originating on a router.

If there is a need to react quickly to changes in tunnel characteristics, you can reduce the multiplier all the way down to 1. With a multiplier of 1, only the latest poll interval loss and latency values are used to determine whether this tunnel can satisfy one or more SLA criteria.
Based on the measurement and calculation of tunnel loss and latency, each tunnel may satisfy one or more user-configured SLA classes. For example, a tunnel with a mean loss of 0 packets and mean latency of 10 milliseconds would satisfy a class that has been defined with a maximum packet loss of 5 and a minimum latency of 20 milliseconds, and it would also satisfy a class that has been defined with a maximum packet loss of 0 and minimum latency of 15 milliseconds.

Regardless of how quickly a tunnel is reclassified, the loss, latency, and jitter information is measured and calculated continuously. You can configure how quickly application-aware routing reacts to changes by modifying the poll interval and multiplier.

### Configuring Firewall Policies

This article provides procedures for configuring firewall policies on XE SD-WAN Routers. You provision firewall policies to direct traffic between two zones, which are referred to as a source zone and a destination zone. Each zone consists of one or more VPNs in the overlay network.

In vManage NMS, you configure firewall policies from the Configuration ► Security screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the XE SD-WAN Router.

#### Configuration Components

For firewall policies, you configure zones and a policy to apply to those zones.

Each zone consists of one or more VPNs in the overlay network. You define a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the policy sequences, you define a default action to be taken on the packet.

The following figure illustrates the configuration components for firewall policies:

![Firewall Policy Configuration Components Diagram]

To create a firewall policy, you include the following components in the configuration for a XE SD-WAN Router:
Table 216:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match portion of the zone-based firewall configuration.</td>
<td>Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Data Prefix Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Zones</td>
<td>policy lists policy zone</td>
</tr>
<tr>
<td>Numbered sequences of match-action pairs</td>
<td>Sequences establish the order in which the policy components are applied.</td>
<td>Configuration ▶ Security ▶ Add Security Policy ▶ &lt;Scenario&gt; ▶ Add Firewall Policy ▶ Sequence Rule ▶ Match</td>
<td>policy zone-based-policy sequence</td>
</tr>
<tr>
<td>L3/4 Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration ▶ Security ▶ Add Security Policy ▶ &lt;Scenario&gt; ▶ Add Firewall Policy ▶ Sequence Rule ▶ Match</td>
<td>policy zone-based-policy sequence match</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching packets, and how to process matching items.</td>
<td>Configuration ▶ Security ▶ Add Security Policy ▶ &lt;Scenario&gt; ▶ Add Firewall Policy ▶ Sequence Rule ▶ Action</td>
<td>policy zone-based-policy sequence action</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped.</td>
<td>Configuration ▶ Security ▶ Add Security Policy ▶ &lt;Scenario&gt; ▶ Add Firewall Policy</td>
<td>policy zone-based-policy default-action</td>
</tr>
<tr>
<td>Apply firewall policy to a zone pair</td>
<td>For a firewall policy to take effect, you include it in the definition of a zone pair.</td>
<td>Configuration ▶ Security ▶ Add Security Policy ▶ &lt;Scenario&gt; ▶ Apply Policy</td>
<td>policy zone-pair</td>
</tr>
</tbody>
</table>

To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:
### Table 217:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match portion of the firewall policy configuration.</td>
<td>Configuration ► Security ► Custom Options ► Lists ► Application</td>
<td>policy lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Custom Options ► Lists ► Zones</td>
<td>policy zone-based-policy</td>
</tr>
<tr>
<td>Numbered sequences of match–action pairs</td>
<td>Sequences establish the order in which the policy components are applied.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule</td>
<td>policy zone-based-policy</td>
</tr>
<tr>
<td>Application Match parameters</td>
<td>Conditions that packets must match to be considered for a security policy.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule ► Match ► Application/Application Family List</td>
<td>policy zone-based-policy</td>
</tr>
<tr>
<td>Actions</td>
<td>For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule ► Actions ► Inspect</td>
<td>policy zone-based-policy</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule ► Actions</td>
<td>policy zone-based-policy</td>
</tr>
<tr>
<td>Apply firewall policy to a zone pair</td>
<td>For a firewall policy to take effect, you include it in the definition of a zone pair.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Apply Policy</td>
<td>policy zone-pair</td>
</tr>
</tbody>
</table>

### General vManage Configuration Procedure

To configure firewall policies, use the vManage policy configuration wizard. The wizard is a UI policy builder that lets you configure policy components:

- Create Lists—Create lists that group together related items and that you call in the match condition of a firewall policy.
- Firewall Policy—Define the match and action conditions of the firewall policy.
Apply Configuration—Define zone pairs.

You must configure all these components to create a firewall policy. If you are modifying an existing firewall, you can skip a component by clicking the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

**Step 1: Create Lists**

To create lists:

1. In vManage NMS, select the Configure ► Security screen.
2. In the Title bar, click the Custom Options drop-down.
4. Select the list type to create. The following table describes the lists you can create for firewall policies.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Application | 1. In the left pane, click Application.  
2. Click New Application List.  
3. Enter a name for the list.  
4. Select individual applications or application families.  
5. Click Add. |
| Data Prefix | 1. In the left pane, click Data Prefix.  
2. Click New Data Prefix List.  
3. Enter a name for the list.  
4. Enter one or more IP prefixes.  
5. Click Add. |
| Zones | 1. In the left pane, click Zones.  
2. Click New Zone List.  
3. Enter a name for the zone list.  
4. In the Add VPN field, enter the number or numbers of the VPN in the zone. Separate numbers with commas.  
5. Click Add. |

1. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.
Step 2: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Security Policy.

The Add Security Policy configuration wizard opens, and various use-case scenarios display.

Step 3: Select a Use-Case Scenario

In Add Security Policy, select a policy based on use-case scenarios, or build your own custom policy.

1. Select a security policy use-case scenario. The following table describes the use-case scenarios.

- Compliance – Applies application firewall and intrusion prevention.
- Guest Access – Applies application firewall and URL filtering.
- Direct Cloud Access – Applies application firewall, URL filtering, and DNS Umbrella security.
- Direct Internet Access – Applies application firewall, intrusion prevention, URL filtering, and DNS Umbrella security.
- Custom – Build your own security policy by combining various security policy blocks.

1. Click Proceed to add a firewall policy in the wizard.

Step 4: Configure Firewall Policy

1. Click the Add Firewall Policy drop-down.
2. To create a new firewall policy:
   1. Select Create New.
   2. Enter a name and description for the policy.

1. To import an existing zone-based firewall policy:
   1. Select Copy from Existing. The Copy from Existing Firewall Policy dialog box appears.
   2. From the Policy drop-down, select the policy to copy.
   3. In the Policy Name field, accept the default name (policy_name_copy) or enter a new name.
   4. In the Policy Description field, enter a description.
   5. Click Copy.
   6. To modify the policy, click the More Actions icon to at the far right of the policy and select Edit. Go to Step 4.

Otherwise, click Next to move to the next security block in the configuration wizard.
In the left pane, click Sequence Rule to create a single sequence in the firewall policy. The Match tab is selected by default.

2. Click a match condition:
   - Source Data Prefix
   - Source Port
   - Destination Data Prefix
   - Destination Port
   - Protocol
   - Application/Application Family List

You can select and configure more than one match condition in a sequence.

1. Enter the values for the match condition.

Note: If you selected an Application or Application Family List, you must select at least one other match condition.

1. Click the Actions tab.

2. Enter the action or actions to take if the traffic matches.

Note: If a match condition contains an Application or Application Family List, the action must be Inspect. This inspect action is a Layer 4 action. The action for a specific application is block/deny.

1. Click Save Match and Actions to save match-action pair.

2. Repeat Steps 4 through 9 to add match–action pairs to the firewall policy.

3. To rearrange match–action pairs in the policy, drag them to the desired position.

4. To edit, copy, or delete a sequence rule, in the right pane, click the edit, copy, or delete icon to the right of the sequence rule.

5. If no packets match any of the policy sequence rules, the default action is to drop the packets. To change the default action:
   1. Click the Pencil icon.
   2. Change the default action to Inspect or Pass.
   3. Click Save Match and Actions.

Step 5: Apply Policy to a Zone Pair

1. At the top of the page, click Apply Zone-Pairs.

2. In the Source Zone field, select the zone that is the source of the data packets.

3. In the Destination Zone field, select the zone that is the destination of the data packets.

1. Click the plus (+) icon to add zone pairs.
2. Click Save.

3. At the bottom of the page, click Save Firewall Policy to save the policy.

4. To edit or delete a firewall policy, in the right pane, click the More Actions icon to the far right of the policy and select the desired option.

5. Click Next to configure the next security block in the wizard.
   - Intrusion Prevention
   - URL Filtering
   - DNS Security

You can select the same zone for both source and destination. However, if the packet's source and destination use the same physical interface (resulting in U-turn traffic), a firewall session is not created and traffic passes.

**Policy Summary**

1. Enter a name for the security policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores ( _ ). It cannot contain spaces or any other characters.

2. Enter a description for the security policy. This field is mandatory.

3. If you configured an application firewall policy, uncheck the “Bypass firewall policy and allow all Internet traffic to/from VPN 0” checkbox in the Additional Security Policy Settings area.

4. Click Save Policy to save the security policy.

**Apply a Security Policy to an XE SD-WAN Router**

1. In vManage NMS, select the Configuration ▶ Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the XE SD-WAN Router.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores ( _ ). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the security policy you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Related Topics

   Enterprise Firewall with Application Awareness, on page 498

Enterprise Firewall with Application Awareness

Cisco’s Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.
- Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Matching flows that are accepted can be processed in two different ways:

- Inspect—The packet’s header can be inspected to determine its source address and port.
- Pass—Allow the packet to pass to the destination zone without inspecting the packet’s header at all.

The following figure shows a simple scenario in which three VPNs are configured on a XE SD-WAN Router. One of the VPNs, VPN 3, has shared resources that you want to restrict access to. These resources could be printers or confidential customer data. For the remaining two VPNs in this scenario, only users in one of them, VPN 1, are allowed to access the resources in VPN 3, while users in VPN 2 are denied access to these resources. In this scenario, we want data traffic to flow from VPN 1 to VPN 3, but we do not want traffic to flow in the other direction, from VPN 3 to VPN 1.
Firewall policies perform stateful inspection of TCP, UDP, and ICMP flows between zones. They examine the source and destination IP addresses and ports in the packet headers, as well as the packet's protocol. Then, based on the configured zone-based policy, they allow traffic to pass between the zones or they drop the traffic.

The implementation of firewall policies varies slightly to that of localized security policy. Where you configure and apply localized security policy based only on VPNs, you configure and apply firewall policies to one or more VPNs that have been grouped into a zone. You activate localized security policy by applying it to individual interfaces on the XE SD-WAN Routers. When you activate firewall policies, they apply to the specific VPNs in the zones, without regard to any specific interfaces.

**Application Firewall**

The Application Firewall inspects and blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits:

- Application visibility and granular control
- Classification of 1400+ layer 7 applications
- Blocks traffic by application or application-family

You can create lists of individual applications or application families. A sequence that contains a specified application or application family list can be inspected. This inspect action is a Layer 4 action. Matching applications are blocked/denied.

vEdge Router provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall. Service NAT support is added for FTP ALG on the client and not on the FTP Server.

Firewall policies are a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows.

**Related Topics**

- Configuring Firewall Policies, on page 491

**Zone-based Firewall Configuration Examples**

This article provides an example of configuring a simple zone-based firewall.
Isolating Two VPNs

In this zone-based firewall configuration example, we have a scenario where a vEdge router is connected to three service-side networks:

- Guest network that provides point-of-sale (PoS) services
- Employee network
- Network that provides shared services, including shared printers and the customer database

We want users in the employee and guest networks to be able to access the shared services, but we do not want any traffic to be exchanged between the employee and guest networks. Similarly, we do not want any traffic that originates in the shared services network to enter into either the employee network or the guest network. The following figure illustrates this scenario:

In this figure:

- VPN 1 is the guest network used for PoS services.
- VPN 2 is the network used by the enterprise's employees.
- VPN 3 contains the shared services, including printers and customer databases.

The configuration consists of three sections:

- Define the zones.
- Define the zone-based firewall policy.
- Apply the zone-based firewall policy to a source zone and destination zone pair.

CLI Configuration

First, we define the zones for this scenario:

```
vEdge(config)# policy
vEdge(config-policy)# zone pos-zone vpn 1
vEdge(config-policy)# zone employee-zone vpn 2
vEdge(config-policy)# zone services-zone vpn 3
```

In this simple example, each zone corresponds to a single VPN. If you were to later add a second VPN for a discrete group of employees (let's say this is VPN 20) and you wanted this VPN to be subject to the same firewall policy, you could simply add this VPN to the employee zone:
Next, we configure the zone-based firewall policy. The policy matches all traffic that is destined for VPN 3, which is the services zone, and which has an IP prefix of 10.2.2.0/24. Because we want the policy to allow traffic to flow from VPN 1 and VPN 2 to VPN 3, but we do not want traffic to flow in the reverse direction, we set the action to pass.

We want to drop any traffic that does not match the zone-based firewall policy:

And here is the pairing between the employee zone and the services zone:

Here is a view of the entire policy:
virtualfirewall:

zone-pair services-pairing
source-zone pos-zone
destination-zone services-zone
zone-policy vpn-isolation-policy

zone-based-policy vpn-isolation-policy
sequence 10
match
destination-ip 10.2.2.0/24
action pass
default-action drop

vManage Configuration

To configure this zone-based firewall policy in vManage NMS:

2. Click Add Policy. The zone-based firewall configuration wizard opens.

Configure data prefix groups and zones in the Create Groups of Interest screen:

1. In the left pane, select Data Prefix.
2. In the right pane, click New Data Prefix List.
3. Enter a name for the list.
4. Enter the data prefix or prefixes to include in the list.
5. Click Add.

Configure zones in the Create Groups of Interest screen:

1. In the left pane, select Zones.
2. In the right pane, click New Zone List.
3. Enter a name for the list.
4. Enter the number of the zone or zones to include in the list. Separate numbers with a comma.
5. Click Add.

Click Next to move to Zone-Based Firewall in the zone-based firewall configuration wizard.

Configure zone-based firewall policies:

1. Click Add Configuration, and select Create New.
2. Enter a name and description for the policy.
3. In the left pane, click Add Sequence.
4. In the right pane, click Add Sequence Rule.
5. Select the desired match and action conditions.
6. Click Same Match and Actions.
7. In the left pane, click Default Action.
8. Select the desired default action.
9. Click Save Zone-Based Policy.

Click Next to move to the Apply Configuration in the zone-based firewall configuration wizard.
1. Enter a name and description for the zone-based firewall zone pair.
2. Click Add Zone Pair.
3. In the Source Zone drop-down, select the zone from which data traffic originates.
4. In the Destination Zone drop-down, select the zone to which data traffic is sent.
5. Click Add.
6. Click Save Policy. The Configuration ► Security screen is then displayed, and the zone-based firewalls table includes the newly created policy.

---

**Configuring Advanced Malware Protection**

The Cisco Advanced Malware Protection (AMP) integration equips routing and SD-WAN platforms to provide protection and visibility to cover all stages of the malware lifecycle:

- **Before:** Hardening the network border with firewall rules
- **During:** Blocking malware based on File Reputation and IPS Signatures

- **After:**
  - Using File Notifications to represent breaches that occurred;
  - Retrospectively detecting malware and providing automatic reporting;
  - During: Blocking malware based on File Reputation and IPS Signatures
  - Using advanced file analysis capabilities for detection and deeper insight into unknown files in a network

The Cisco Advanced Malware Protection is composed of three processes:

- **File Reputation:** The process of using a 256-bit Secure Hash Algorithm (SHA256) signature to compare the file against the Advanced Malware Protection (AMP) cloud server and access its threat intelligence information. The response can be Clean, Unknown, or Malicious. If the response is Unknown, and if File Analysis is configured, the file is automatically submitted for further analysis.

- **File Analysis:** The process of submitting an Unknown file to the Threat Grid (TG) cloud for detonation in a sandbox environment. During detonation, the sandbox captures artifacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change
the threat response to Clean or Malicious. Threat Grid’s findings are reported back to the AMP cloud, so that all AMP customers will be protected against newly discovered malware.

Note

File analysis requires a separate Threat Grid account. For information about purchasing a Threat Grid account, contact your Cisco representative.

• Retrospective: By maintaining information about files even after they are downloaded, we can report on files that were determined to be malicious after they were downloaded. The disposition of the files could change based on the new threat intelligence gained by the AMP cloud. This re-classification will generate automatic retrospective notifications.

Configuring an Advanced Malware Protection Policy

To configure an Advanced Malware Protection policy:

Step 1
In Cisco vManage NMS, select the Configuration > Security tab in the left side panel.

Step 2
Click Add Security Policy. The Add Security Policy wizard opens and various use-case scenarios display.

Step 3
In Add Security Policy, select Direct Internet Access and then click Proceed.

Step 4
In the Add Security Policy wizard, click Next as needed to select the Advanced Malware Protection tab.
Step 5  
In the **Advanced Malware Protection** tab, click the **Add Advanced Malware Protection Policy** drop-down.

Step 6  
Select **Create New**. The Add Advanced Malware Protection screen displays.

Step 7  
In the **Policy Name** field, enter a name for the malware policy. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8  
Make sure that the **Match All VPN** button is selected. Select **Match All VPN** if you want to apply the policy to all the VPNs, or select **Custom VPN Configuration** to input the specific VPNs.

Step 9  
From the **AMP Cloud Region** dropdown, select a global region.

Step 10  
From the **Alerts Log Level** dropdown, select a severity level (Critical, Warning, or Info).

**Note:** Because the Info severity level generates multiple notifications and can affect system performance, this level should be configured only for testing or debugging and not for real-time traffic.
Step 11  
Click **File Analysis** to enable Threat Grid (TG) file analysis.

**Note**  Before you can perform this step, configure a threat grid API key as described in Configuring Threat Grid API Key topic.

![Advanced Malware Protection - Policy Rule Configuration](image)

**Note**  File Analysis requires a separate Threat Grid license.

Step 12  
From the **TG Cloud Region** dropdown, select a global region.

**Note**  Configure the Threat Grid API Key by clicking on Manage API Key or as described in Configure Threat Grid API Key.

Step 13  
From the **File Types List** dropdown, select the file types that you want to be analyzed.

Step 14  
From the **Alerts Log Level** dropdown, select a severity level (Critical, Warning, or Info).

Step 15  
Click **Target VPNs** to select the target VPNs or all VPNs, and then click **Add VPN**.

Step 16  
Click **Save Changes**. The Policy Summary screen displays.

Step 17  
Click **Next**.

---

### Copying an existing Advanced Malware Protection Policy

To copy an existing Advanced Malware Protection policy into the security policy:

**Step 1**  
In the Advanced Malware Protection screen, click the **Add Advanced Malware Protection Policy** drop-down.

**Step 2**  
Select **Copy From Existing**.

**Step 3**  
In the **Copy from Existing Advanced Malware Protection** popup:

a)  In the **Policy** field, select a policy.

b)  In the **Policy Name** field, select a policy name.

c)  In the **Policy Description** field, enter a description of the Advanced Malware Protection policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
d) Click Copy. The copied policy is listed in the Security Policy Advanced Malware Protection table.

Step 4  Click Next.

---

**Applying an Advanced Malware Policy to a Device**

After you create or copy an advanced malware policy, apply the policy to the device as described in “Applying Intrusion Prevention Policy to a Device” in the “Intrusion Prevention Configuration on SD-WAN” article, which is available at https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Security/Cisco_SD-WAN_Security_Solution/Intrusion_Prevention_Configuration_on_SD-WAN.

---

**Configuring Threat Grid API Key**

To configure a Threat Grid API key from the Configuration screen:

**Step 1**  In Cisco vManage NMS, select the Configuration > Security tab in the left side panel.

**Step 2**  In the Security screen, click the Custom Options drop-down and select Threat Grid API Key.

**Step 3**  In the Manage Threat Grid API key pop-up box, take these actions:

a) Choose a region from the Region drop-down.

b) Enter a key in the Key field.

c) Click Add.

d) Click Save Changes.

---

**Rekeying the Device Threat Grid API Key**

To rekey the device Threat Grid API key from the Maintenance screen:

**Step 1**  In Cisco vManage NMS, select the Maintenance > Security tab in the left side panel.

**Step 2**  Select the Advanced Malware Protection tab.

**Step 3**  Select the device or devices that you want to rekey.

**Step 4**  Select Action > API Rekey.

---

**Monitoring Advanced Malware Protection**

You can monitor Advanced Malware Protection from the Device Dashboard by using the following steps.

**Step 1**  From the Monitor > Network screen, select a device.

**Step 2**  In the left panel, under Security Monitoring, select the Advanced Malware Protection tab.

This tab shows the following:
Monitoring from the Security Dashboard

You can monitor Advanced Malware Protection for the network from the Security Dashboard by using the following steps.

To do so, select Select Dashboard > Security.

- The Advanced Malware Protection area shows the following:
  - File Reputation – Number of malicious files.
  - File Analysis – Number of files uploaded to Threat Grid

Configuring Unified Threat Defense

This article provides procedures for configuring Unified Threat Defense (UTD) security mechanisms on IOS XE routers. You can configure the following UTD security mechanisms:

- Intrusion prevention and detection (IPS/IDS)
- Umbrella DNS security
- URL filtering

You provision zone-based firewall policies to define the data traffic that is subject to the UTD security mechanisms.

In vManage NMS, you configure UTD from the Configuration ➤ Security screen, using a policy configuration wizard.

**Configuration Components**

UTD security policy components consist of the following:

- Zone-based firewall— Allows you to filter data packets, to match allows data traffic and drop unwanted traffic. You must configure one or more zone-based firewalls for any type of security policy. Zone configuration consists of the following components:
  - Source zone— A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
  - Destination zone— A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
  - Zone pair— A container that associates a source zone with a destination zone and that applies a zone-based firewall policy to the traffic that flows between the two zones.
  - Zone-based firewall policy— A data policy, similar to a localized data policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Zone-based firewalls can match IP prefixes, IP ports, and the protocols TCP, UDP, and ICMP. Matching flows can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default.
  - Zone pair— A container that associates a source zone with a destination zone and that applies a zone-based firewall policy to the traffic that flows between the two zones.

- Intrusion prevention policy— Protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

- URL filtering policy— Allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on whitelists, blacklists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blacklist, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the whitelist, the traffic is allowed without further URL filtering inspection.

- DNS security policy— Directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella using DNS to stop threads over all ports and protocols and over direct-to-IP connections.
Configure Compliance Security

A compliance security policy implements both intrusion prevention and intrusion detection. Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

To configure intrusion prevention and detection, you use the Compliance policy option of the security policy configuration wizard.

Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Compliance Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

Step 2: Configure Application Firewall Policy

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:

   1. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
   2. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
   3. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:

   1. Click Add Sequence Rule.
   2. Click Match to add a match condition. You can match the following: - Application/Application Family List - Destination Data Prefix - Destination Port - Protocol - Source Data Prefix - Source Port
   3. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions: - Inspect: Inspect the packet's header to determine its source address
and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. - Log: Log the packet headers. - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

4. Click Save Match and Actions.

5. Add additional sequence rules as needed.

6. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Firewall popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

   • Intrusion prevention policy
   • Umbrella DNS policy
   • URL-filtering policy

**Step 3: Configure Intrusion Prevention and Detection**

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Click Create New. The Add Intrusion Prevention Policy screen displays.

3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Signature Set field, select the desired signature set:

   • Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
• Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

• Exploit-kit—Rules that are designed to detect exploit kit activity.

• Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.

• SQL Injection—Rules that are designed to detect SQL Injection attempts.

• Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.

• Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
  • App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
  • Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  • Exploit-kit—Rules that are designed to detect exploit kit activity.
  • Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  • SQL Injection—Rules that are designed to detect SQL Injection attempts.

1. In the Inspection Mode field, select the desired inspection mode:
   • Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
   • Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

1. In the Advanced ► Signature Whitelist field, select the desired signature list.

2. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.

3. Configure the VPNs to which to apply the intrusion prevention policy:
   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   3. Click Save Changes.

4. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.

5. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:
1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Intrusion Prevention Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

**Step 4: Configure Additional Policy Settings**

In the Policy Summary screen:
1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).
2. In the Security Policy Description field,
3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.
5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.
6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.
7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.
9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.
10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.
Step 5: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ▶ Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Configure Guest Access

A guest access security policy uses URL filtering policy, which allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on whitelists, blacklists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blacklist, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the whitelist, the traffic is allowed without further URL filtering inspection.

To configure URL filter, you use the Guest Access policy option of the security policy configuration wizard.

Step 1: Start the Security Policy Wizard

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ▶ Security screen.

2. Click Add Policy.
3. From the Add Security Policy popup, select Guest Access Policy.

4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

**Step 2: Configure Application Firewall Policy**

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Create New. The Add Firewall Policy screen displays.

3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.

4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

5. Create a zone pair or apply an existing zone pair to the firewall policy:
   1. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
   2. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
   3. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.

6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
   1. Click Add Sequence Rule.
   2. Click Match to add a match condition. You can match the following: - Application/Application Family List - Destination Data Prefix - Destination Port - Protocol - Source Data Prefix - Source Port
   3. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions: - Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. - Log: Log the packet headers. - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.
   4. Click Save Match and Actions.
   5. Add additional sequence rules as needed.
   6. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which they are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:
1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Firewall popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the Security Policy Firewall table.
4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:
   - Intrusion prevention policy
   - Umbrella DNS policy
   - URL-filtering policy

**Step 3: Configure URL Filtering**

To create a new URL-filtering policy:
1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.
2. Click Create New. The Add URL Filtering Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Web Categories field:
   1. In the Block drop-down, define the action to take if a URL matches a website category. Select Block (the default) to block access to the website category, or select Allow to allow access to the website category.
   2. In the Web Category field, select one or more webpage categories to block or accept. A category defines websites that contain a certain type of content. When you configure category-based or reputation-based URL filtering, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. To check a website's reputation, use the Webroot BrightCloud URL/IP Lookup tool.
5. In the Web Reputation field, select the reputation level of the website to block or accept. Each URL has a reputation score associated with it. The score ranges from 0 through 100 and is labeled as follows:
   - High Risk—Reputation score 0 through 20
   - Suspicious—Reputation score 0 through 40
   - Moderate Risk—Reputation score 0 through 60. This is the default reputation setting.
   - Low Risk—Reputation score 0 through 80.
• Trustworthy—Reputation score 0 through 100.

1. In the Advanced ► Whitelist URL List field, select a URL list to include in the URL filtering policy. A URL whitelist allows the specified URLs and blocks URLs not included in the list. For each URL filtering policy, you can configure only one whitelist URL list. To create a new list of URLs to whitelist:
   1. Click in the Advanced ► Whitelist URL List field.
   2. Click Add New Whitelist URL List.
   3. In the Whitelist URL List Name field, enter a name for the whitelist.
   4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as .*\cisco\com.
   5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.
   6. Click Save.

2. In the Advanced ► Blacklist URL List field, select one or more URL blacklists to include in the URL filtering policy. A URL blacklist blocks the specified URLs and allows URLs not included in the list. For each URL filtering policy, you can configure only one blacklist URL list. To create a new list of URLs to blacklist:
   1. Click in the Advanced ► Blacklist URL List field.
   2. Click Add New Blacklist URL List.
   3. In the Blacklist URL List Name field, enter a name for the blacklist.
   4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as .*\cisco\com.
   5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.
   6. Click Save.

3. In the Advanced ► Block Page Server section, configure how to handle blocked HTTP URLs. For blocked HTTPS websites, no blocking or redirection is performed. Instead, all traffic is dropped.
   1. To block and not display the content of a webpage, click Block Page Content. Then, type the message to display to the user indicated why the webpage is not displayed. This is the default method for handling blocked URLs. In the Default Content Header field, type the title of the message, which is displayed in bold letters. The default header is, "Access to the requested page has been denied." In the Content Body field, type the content of the blocked page message. The default message is, "Please contact your network administrator".
   2. To redirect to another URL, click Redirect URL. Then, enter the URL to which to redirect the user.

4. In the Advanced ► Alerts and Logs section, configure when to send alerts and syslog messages:
   1. Click Blacklist to send alerts when a blacklisted URL is blocked.
   2. Click Whitelist to send alerts when a whitelisted URL is allowed.
   3. Click Reputation/Category to send alerts when a URL is blocked because of its category or reputation.

5. Configure the VPNs to which to apply the URL filtering policy:
1. In the Target field, click Add Target VPNS.

2. Enter the VPN numbers to which to apply the URL filtering policy. To specify multiple VPNS, separate the numbers with commas.

3. Click Save Changes.

6. Click Save URL Filtering Policy. The URL filtering policy is then listed in the policy table.

7. Click Next. The Policy Summary screen displays.

To copy an existing URL filtering policy into the guest access policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing URL Filtering Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the URL Filtering table.


**Step 4: Configure Additional Policy Settings**

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).

2. In the Security Policy Description field,

3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.

5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.

6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.

7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ▶ Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.

9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.

10. Click Save Policy. The policy is listed in the table on the Configuration ▶ Policy screen.

**Step 5: Apply the Security Policy to an IOS XE Router**

1. In vManage NMS, select the Configuration ▶ Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

**Configure Direct Cloud Access**

A direct cloud access policy uses intrusion prevention and detection and Umbrella DNS security to control access from the local device to the cloud devices.
Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

DNS security policy directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella using DNS to stop threads over all ports and protocols and over direct-to-IP connections. To configure this, you use the Direct Cloud Access option of the security policy configuration wizard.

**Step 1: Start the Security Policy Wizard**

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ▶ Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Guest Access Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

**Step 2: Configure Application Firewall Policy**

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
   1. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
   2. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
   3. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
   1. Click Add Sequence Rule.
   2. Click Match to add a match condition. You can match the following: - Application/Application Family List - Destination Data Prefix - Destination Port - Protocol - Source Data Prefix - Source Port
   3. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions: - Inspect: Inspect the packet's header to determine its source address
and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. - Log: Log the packet headers. - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

4. Click Save Match and Actions.
5. Add additional sequence rules as needed.
6. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which that are defined in the policy.

7. Click Save Firewall Policy.
8. Click Next.

To copy an existing firewall policy into the compliance security policy:
1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing Firewall popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

- Intrusion prevention policy
- Umbrella DNS policy
- URL-filtering policy

Step 3: Configure Intrusion Prevention and Detection

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.
2. Click Create New. The Add Intrusion Prevention Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Signature Set field, select the desired signature set:

   • Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
• Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

• Exploit-kit—Rules that are designed to detect exploit kit activity.

• Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.

• SQL Injection—Rules that are designed to detect SQL Injection attempts.

• Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.

• Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
  • App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
  • Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
  • Exploit-kit—Rules that are designed to detect exploit kit activity.
  • Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
  • SQL Injection—Rules that are designed to detect SQL Injection attempts.

1. In the Inspection Mode field, select the desired inspection mode:
   • Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
   • Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

1. In the Advanced ► Signature Whitelist field, select the desired signature list.
2. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.
3. Configure the VPNs to which to apply the intrusion prevention policy:
   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   3. Click Save Changes.
4. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.
5. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:
1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Intrusion Prevention Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the Security Policy Firewall table.


**Step 4: Configure Umbrella DNS**

To create a new Umbrella DNS policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.


3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Umbrella Registration Status field:
   1. Click Manage Umbrella Registration.
   2. In the Manage Umbrella Registration pop-up, enter your Umbrella registration token.
   3. Click Save Changes.

5. By default, the DNS security policy applies to all VPNs, so the Match All VPN field is selected. To apply the DNS security policy to a custom set of VPNs:
   1. Select the Custom VPN Configuration field.
   2. In the Target field, click Add Target VPNs.
   3. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
   4. Click Save Changes.

6. In the Local Domain Bypass List field, select the web domain list that lists the websites domains that are allowed by bypass DNS lookups. To create a domain list:
   1. Click in the Local Domain Bypass List field and then click Add New Domain List.
   2. In the Domain List Name field, enter a name for the domain list.
   3. In the Domain field, enter one or more web domains. Examples of website domains are cisco.com and *.cisco.com. Separate lists with a comma. The first item in the list cannot start with an asterisk (*).
4. Click Save.

7. In the DNS Server IP field, select the IP address of the DNS server. By default, traffic using Umbrella as the DNS server. To use a different DNS server, select Custom DNS and enter the IP address of the DNS server.

1. In the Advanced ► DNSCrypt field, configure the encryption of DNS traffic. By default, encryption is enabled. To disable DNS traffic encryption, move the slider to the left.

2. Click Save DNS Security Policy. The intrusion prevention policy is then listed in the policy table.

3. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing DNS Security Policy popup:

   1. In the Policy field, select a policy.

   2. In the Policy Name field, select a policy name.

   3. Click Copy. The copied policy is listed in the Security Policy Firewall table.


**Step 5: Configure Additional Policy Settings**

In the Policy Summary screen:

1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).

2. In the Security Policy Description field,

3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.

5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.

6. By default, system logging (syslog) in enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.

7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.
8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.

9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.

10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.

Step 6: Apply the Security Policy to an IOS XE Router

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Configure Direct Internet Access
A direct internet access policy uses intrusion prevention and detection, URL filtering, and Umbrella DNS security to control access from the local device the internet.
Intrusion prevention policy protects against malicious attacks on data traffic by using signature sets and inspection mode. Intrusion detection passes all packets flowing between service-side and transport-side (WAN or internet) interfaces, and between VLANs, through an intrusion detection engine, generating alerts for traffic that is identified as malicious, and logging these alerts via syslog. Intrusion prevention blocks traffic that is identified as malicious.

URL filtering policy allows and disallows access to specific URLs and webpage categories. URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on whitelists, blacklists, categories, and reputations. For example, when a client sends a HTTP or HTTPS request, the router inspects the traffic. If, for example, the request matches the blacklist, either it is blocked by a blocked page response or it is redirected to a different URL. If, for example, the HTTP or HTTPS request matches the whitelist, the traffic is allowed without further URL filtering inspection.

DNS security policy directs traffic from your network to the cloud-based Cisco Umbrella secure internet gateway. Umbrella uses DNS to stop threads over all ports and protocols and over direct-to-IP connections. To configure this, you use the Direct Cloud Access option of the security policy configuration wizard.

**Step 1: Start the Security Policy Wizard**

To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select Guest Access Policy.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays.

**Step 2: Configure Application Firewall Policy**

To create a new application firewall policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.
2. Select Create New. The Add Firewall Policy screen displays.
3. In the Name field, enter a name for the firewall policy. The name can be up to 128 characters and can contain only alphanumeric characters.
4. In the Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
5. Create a zone pair or apply an existing zone pair to the firewall policy:
   1. Click Apply Zone Pairs. The Apply Zone Pairs popup displays.
   2. In Source Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
   3. In Destination Zone, select an existing zone. Or to create a new zone, click Create New Zone List. Then enter a name for the list and the VPNs in the zone, and click Save.
6. Create one or more security policy sequence rules to apply to the traffic that flows from the source zones to the destination zones:
1. Click Add Sequence Rule.

2. Click Match to add a match condition. You can match the following: - Application/Application Family List - Destination Data Prefix - Destination Port - Protocol - Source Data Prefix - Source Port

3. Click Actions to define the actions to take when a match occurs. By default, the packet is dropped. You can take these other actions: - Inspect: Inspect the packet's header to determine its source address and port. The address and port are used by the NAT device to allow traffic to be returned from the destination to the sender. - Log: Log the packet headers. - Pass: Allow the packet to pass to the destination zone without inspecting the packet's header at all. With this action, the NAT device blocks return traffic that is addressed to the sender.

4. Click Save Match and Actions.

5. Add additional sequence rules as needed.

6. Drag and drop the rules to arrange them in the desired sequence. Rules are applied to data packets in the order in which they are defined in the policy.

7. Click Save Firewall Policy.

8. Click Next.

To copy an existing firewall policy into the compliance security policy:

1. In the Firewall screen, click the Add Firewall Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Firewall popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.

4. Click Copy. The copied policy is listed in the Security Policy Firewall table.

4. Click Next. Depending on the security policy type you are configuring, one of the following screens displays:

   • Intrusion prevention policy
   • Umbrella DNS policy
   • URL-filtering policy

**Step 3: Configure Intrusion Prevention and Detection**

To create a new intrusion prevention and detection policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Click Create New. The Add Intrusion Prevention Policy screen displays.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Signature Set field, select the desired signature set:

   • Balanced (default)—Contains rules that are from the current year and the previous two years, are for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9 or greater, and are in one of the following categories:
     - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
     - Exploit-kit—Rules that are designed to detect exploit kit activity.
     - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
     - SQL Injection—Rules that are designed to detect SQL Injection attempts.

   • Connectivity—Contains rules from the current year and the previous two years for vulnerabilities with a CVSS score of 10.

   • Security—Contains rules that are from the current year and the previous three years, are for vulnerabilities with a CVSS score of 8 or greater, and are in one of the following categories:
     - App-detect—Rules that look for and control the traffic of certain applications that generate network activity.
     - Blacklist—Rules for URIs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.
     - Exploit-kit—Rules that are designed to detect exploit kit activity.
     - Malware-CNC—Rules for known malicious command and control activity for identified botnet traffic. These include call home, downloading of dropped files, and ex-filtration of data.
     - SQL Injection—Rules that are designed to detect SQL Injection attempts.

1. In the Inspection Mode field, select the desired inspection mode:

   • Detection—In intrusion detection mode, traffic is accepted or blocked based on the rules defined by the signature set that you choose.
   • Protection—In intrusion prevention mode, malicious traffic is automatically blocked, based on the intrusion prevention policy rules.

1. In the Advanced ► Signature Whitelist field, select the desired signature list.

2. In the Advanced ► Alerts Log Level field, select the desired log level for alerts. The level can be Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. The default is Error.

3. Configure the VPNs to which to apply the intrusion prevention policy:

   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.
3. Click Save Changes.

4. Click Save Intrusion Prevention Policy. The intrusion prevention policy is then listed in the policy table.

5. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:

1. In the Intrusion Prevention screen, click the Add Intrusion Prevention Policy drop-down.

2. Select Copy from Existing.

3. In the Copy from Existing Intrusion Prevention Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the Security Policy Firewall table.


**Step 4: Configure URL Filtering**

To create a new URL-filtering policy:

1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.

2. Click Create New. The Add URL Filtering Policy screen displays.

3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.

4. In the Web Categories field:
   1. In the Block drop-down, define the action to take if a URL matches a website category. Select Block (the default) to block access to the website category, or select Allow to allow access to the website category.
   2. In the Web Category field, select one or more webpage categories to block or accept. A category defines websites that contain a certain type of content. When you configure category-based or reputation-based URL filtering, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. To check a website's reputation, use the Webroot BrightCloud URL/IP Lookup tool.

5. In the Web Reputation field, select the reputation level of the website to block or accept. Each URL has a reputation score associated with it. The score ranges from 0 through 100 and is labeled as follows:

   • High Risk—Reputation score 0 through 20
   • Suspicious—Reputation score 0 through 40
   • Moderate Risk—Reputation score 0 through 60. This is the default reputation setting.
• Low Risk—Reputation score 0 through 80.
• Trustworthy—Reputation score 0 through 100.

1. In the Advanced ► Whitelist URL List field, select a URL list to include in the URL filtering policy. A URL whitelist allows the specified URLs and blocks URLs not included in the list. For each URL filtering policy, you can configure only one whitelist URL list. To create a new list of URLs to whitelist:
   1. Click in the Advanced ► Whitelist URL List field.
   2. Click Add New Whitelist URL List.
   3. In the Whitelist URL List Name field, enter a name for the whitelist.
   4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as .*/cisco\.*com.
   5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.
   6. Click Save.

2. In the Advanced ► Blacklist URL List field, select one or more URL blacklists to include in the URL filtering policy. A URL blacklist blocks the specified URLs and allows URLs not included in the list. For each URL filtering policy, you can configure only one blacklist URL list. To create a new list of URLs to blacklist:
   1. Click in the Advanced ► Blacklist URL List field.
   2. Click Add New Blacklist URL List.
   3. In the Blacklist URL List Name field, enter a name for the blacklist.
   4. In the Add Whitelist URL field, enter one or more URLs to whitelist. You can specify the full URL, or you can use regular expressions, such as .*/cisco\.*com.
   5. To import a list of URL into the whitelist, click the Upload arrow and then select the file to import.
   6. Click Save.

3. In the Advanced ► Block Page Server section, configure how to handle blocked HTTP URLs. For blocked HTTPS websites, no blocking or redirection is performed. Instead, all traffic is dropped.
   1. To block and not display the content of a webpage, click Block Page Content. Then, type the message to display to the user indicated why the webpage is not displayed. This is the default method for handling blocked URLs. In the Default Content Header field, type the title of the message, which is displayed in bold letters. The default header is, "Access to the requested page has been denied." In the Content Body field, type the content of the blocked page message. The default message is, "Please contact your network administrator".
   2. To redirect to another URL, click Redirect URL. Then, enter the URL to which to redirect the user.

4. In the Advanced ► Alerts and Logs section, configure when to send alerts and syslog messages:
   1. Click Blacklist to send alerts when a blacklisted URL is blocked.
   2. Click Whitelist to send alerts when a whitelisted URL is allowed.
   3. Click Reputation/Category to send alerts when a URL is blocked because of its category or reputation.
5. Configure the VPNs to which to apply the URL filtering policy:
   1. In the Target field, click Add Target VPNs.
   2. Enter the VPN numbers to which to apply the URL filtering policy. To specify multiple VPNs, separate the numbers with commas.
   3. Click Save Changes.

6. Click Save URL Filtering Policy. The URL filtering policy is then listed in the policy table.

7. Click Next. The Policy Summary screen displays.

To copy an existing URL filtering policy into the guest access policy:
1. In the URL Filtering screen, click the Add URL Filtering Policy drop-down.
2. Select Copy from Existing.
3. In the Copy from Existing URL Filtering Policy popup:
   1. In the Policy field, select a policy.
   2. In the Policy Name field, select a policy name.
   3. In the Policy Description field, enter a description of the firewall policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
   4. Click Copy. The copied policy is listed in the URL Filtering table.

**Step 5: Configure Umbrella DNS**

To create a new Umbrella DNS policy:
1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
3. In the Policy Name field, enter a name for the firewall policy. The name can be up to 32 characters and can contain only alphanumeric characters.
4. In the Umbrella Registration Status field:
   1. Click Manage Umbrella Registration.
   2. In the Manage Umbrella Registration pop-up, enter your Umbrella registration token.
   3. Click Save Changes.

5. By default, the DNS security policy applies to all VPNs, so the Match All VPN field is selected. To apply the DNS security policy to a custom set of VPNs:
   1. Select the Custom VPN Configuration field.
   2. In the Target field, click Add Target VPNs.
3. Enter the VPN numbers to which to apply the intrusion prevention policy. To specify multiple VPNs, separate the numbers with commas.

4. Click Save Changes.

6. In the Local Domain Bypass List field, select the web domain list that lists the websites domains that are allowed by bypass DNS lookups. To create a domain list:
   1. Click in the Local Domain Bypass List field and then click Add New Domain List.
   2. In the Domain List Name field, enter a name for the domain list.
   3. In the Domain field, enter one or more web domains. Examples of website domains are cisco.com and *.cisco.com. Separate lists with a comma. The first item in the list cannot start with an asterisk (*).
   4. Click Save.

7. In the DNS Server IP field, select the IP address of the DNS server. By default, traffic using Umbrella as the DNS server. To use a different DNS server, select Custom DNS and enter the IP address of the DNS server.
   1. In the Advanced ► DNSCrypt field, configure the encryption of DNS traffic. By default, encryption is enabled. To disable DNS traffic encryption, move the slider to the left.
   2. Click Save DNS Security Policy. The intrusion prevention policy is then listed in the policy table.
   3. Click Next. The Policy Summary screen displays.

To copy an existing intrusion prevention policy into the compliance security policy:
   1. In the Add Security Policy screen, click the Add DNS Security Policy drop-down.
   2. Select Copy from Existing.
   3. In the Copy from Existing DNS Security Policy popup:
      1. In the Policy field, select a policy.
      2. In the Policy Name field, select a policy name.
      3. Click Copy. The copied policy is listed in the Security Policy Firewall table.

**Step 6: Configure Additional Policy Settings**

In the Policy Summary screen:
   1. In the Security Policy Name field, enter the name of the security policy. The name can be up to 32 characters and can contain only alphanumeric characters, hyphens (-), and underscores (_).
   2. In the Security Policy Description field,
   3. In the Description field, enter a description of the security policy. The description can be up to 2048 characters and can contain only alphanumeric characters.
4. If you do not include VPN 0 in any of the zones that you configure in a zone-based firewall, by default, packets are able to reach destination zones that are accessible only over the public internet. To disallow this traffic, uncheck the Firewall ► Direct Internet Applications box.

5. To configure the number of TCP SYN packets that the router can receive while establishing a TCP connection to use for a zone-based firewall before the router shuts down the connection, move the Firewall ► TCP SYN Flood Limit slider to Enabled. Then enter a limit value from 1 through 2147483647 packets. The default limit is 2000 SYN packets.

6. By default, system logging (syslog) is enabled for intrusion detection. To disable syslog messages, move the Intrusion Prevention and/or URL Filtering ► Syslog slider to Disabled.

7. In the Intrusion Prevention and/or URL Filtering ► External Server field, configure an external syslog server. In the VPN field, specify the VPN through which the server can be reached. In the Server IP field, specify the IP address of the syslog server.

8. In the Intrusion Prevention and/or URL Filtering ► Failure Mode field, configure how the router handles traffic when the URL database update from the cloud fails. When you configure category-based or reputation-based URL filtering, as described above, a URL database is downloaded from the cloud. Incremental updates are automatically downloaded every 15 minutes. If connectivity to the cloud is lost for more than 24 hours, the database is invalidated. For the Failure Mode field, the default is Close, which drops all traffic destined for URL filtering when cloud connectivity is lost. To not drop traffic destined for URL filter, select Open.

9. To view the CLI commands that correspond to the compliance security policy configuration, click Preview.

10. Click Save Policy. The policy is listed in the table on the Configuration ► Policy screen.

**Step 7: Apply the Security Policy to an IOS XE Router**

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the zone-based firewall you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Configure a Custom UTD Security Policy
You can create a custom UTD security policy consisting of any of the standard UTD policy components. To start the security policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.
2. Click Add Policy.
3. From the Add Security Policy popup, select the Custom option.
4. Click Proceed.

The security policy configuration wizard opens, and the Firewall screen displays. Configure the desired security policy components.

This article describes how to configure zone-base firewalls.

Configuring Cloud OnRamp for IaaS
Cloud OnRamp for Infrastructure as a Service (IaaS) extends the fabric of the Cisco SD-WAN overlay network into public clouds by creating Cloud vEdges or Cisco Cloud Services Routers (CSRs), which provide the connectivity to cloud applications that customers host on these public clouds.

The connection between the overlay network and a public-cloud application is provided by two redundant cloud routers, which act together as a transit between the overlay network and the application. Using two routers to form the transit offers path resiliency to the public cloud. In addition, having redundant routers assists in brownout protection, to improve the availability of public-cloud applications. Together, the two routers can remediate link degradation that might occur during brownouts. You create these routers as part of the Cloud OnRamp workflow.

Cloud OnRamp for IaaS discovers any already existing public cloud instances in geographical cloud regions and allows you to select which of them to make available for the overlay network. In such a brownfield scenario, Cloud OnRamp for IaaS allows simple integration between legacy public-cloud connections and the Cisco overlay network.

You configure and manage Cloud OnRamp for IaaS through the vManage NMS server. A configuration wizard in the vManage NMS automates the bring-up of the transit to your public cloud account and automates the connections between public-cloud applications and the users of those applications at branches in the overlay network.

Cloud OnRamp for IaaS works in conjunction with Amazon Web Service (AWS) virtual private clouds (VPCs), and Azure virtual networks (VNets).
Supported Routers

Cloud OnRamp for IaaS is supported on Cisco Cloud vEdge and Cisco Cloud Services Routers (CSRs). In this article, supported routers are referred to collectively as cloud routers.

Cloud OnRamp Configuration Overview

To configure Cloud OnRamp for IaaS for AWS, you create AWS transit VPCs, each of which consists of a pair of edge routers. You then map the transit virtual private clouds (VPCs) to host VPCs that already exist in the AWS cloud.

• Transit VPCs provide the connection between the Cisco overlay network and the cloud-based applications running on host VPCs. Each transit VPC consists of two cloud routers that reside in their own VPC. Two routers are used to provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud routers, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.

• Host VPCs are virtual private clouds in which your cloud-based applications reside. When a transit VPC connects to an application or application provider, it is simply connecting to a host VPC.

Similarly, to configure Cloud OnRamp for IaaS for Azure, you create Azure transit VNets, each of which consists of a pair of edge routers. You then map the host VNets to transit VNets that already exist in the Azure cloud. All VNets reside in the same resource group.

• Transit VNets provide the connection between the overlay network and the cloud-based applications running on host VNet. Each transit VNet consists of two routers that reside in their own VNet. Two routers are used to provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud routers, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.

• Host VNets are virtual private clouds in which your cloud-based applications reside. When a transit VNet connects to an application or application provider, it is simply connecting to a host VNet.

In the Cloud OnRamp configuration process, you map one or more host VPCs or host VNets to a single transit VPC or transit VNet. In doing this, you are configuring the cloud-based applications that branch users are able to access.

The mapping process establishes IPsec and BGP connections between the transit VPC or transit VNet and each host VPC or host VNet. The IPsec tunnel that connects the transit and host VPC or VNet runs IKE to provide security for the connection. For AWS, the IPsec tunnel runs IKE Version 1. For Azure, the IPsec tunnel runs IKE version 2. The BGP connection that is established over the secure IPsec tunnel allows the transit and host VPC or VNet to exchange routes so that the transit VPC or VNet can direct traffic from the branch to the proper host VPC or VNet, and hence to the proper cloud-based application.

During the mapping process, the IPsec tunnels and BGP peering sessions are configured and established automatically. After you establish the mappings, you can view the IPsec and BGP configurations, in the VPN Interface IPsec and BGP feature configuration templates, respectively, and you can modify them as necessary.

vManage NMS Prerequisites

Before you can configure Cloud OnRamp for IaaS, you must properly provision the vManage NMS.
• Make sure that your vManage server has access to the internet and that it has a DNS server configured so that it can reach AWS. To configure a DNS server, in the vManage VPN feature configuration template, enter the IP address of a DNS server, and then reattach the configuration template to the vManage server.

• Ensure that two cloud routers that are to be used to bring up the Cloud OnRamp for IaaS have been added to the vManage NMS and have been attached to the appropriate configuration template. (These two routers are deployed in AWS in their own VPC, and together they form the transit VPC, which is the bridge between the overlay network and AWS cloud applications.) Ensure that the configuration for these two routers includes the following:
  • Hostname
  • IP address of vBond orchestrator
  • Site ID
  • Organization name
  • Tunnel interface configuration on the eth1 interface

• Ensure that the vManage NMS is synchronized to the current time. To check the current time, click the Help (?) icon in the top bar of any vManage screen. The Timestamp field shows the current time. If the time is not correct, configure the vManage server’s time to point to an NTP time server, such as the Google NTP server. To do this, in the vManage NTP feature configuration template, enter the hostname of an NTP server, and then reattach the configuration template to the vManage server. The Google NTP servers are time.google.com, time2.google.com, time3.google.com, and time4.google.com.

**AWS Prerequisites**

Before you can configure Cloud OnRamp for IaaS, you must properly provision AWS.

• Ensure that you have subscribed to the Viptela marketplace Amazon machine images (AMIs) and the Cisco CSR AMIs in your AWS account. See Subscribe to Viptela AMIs.

• Ensure that at least one user who has administrative privileges has the AWS API keys for your AWS account. For Cloud OnRamp for IaaS, these keys are used to authenticate the vManage server with AWS and to bring up the VPC and Elastic Compute Cloud (EC2) instances.

• Check the AWS limits associated with your account (in the Trusted Advisor section of AWS) to ensure that the following resources can be created in your account:
  • 1 VPC, which is required for creating the transit VPC
  • 6 Elastic IP addresses associated with the transit cloud routers
  • 1 AWS virtual transit (VGW) for each host VPC
  • 4 VPN connections for mapping each host VPC

vEdge Cloud Routers support C3 and C4 compute-intensive families.

**Subscribe to SD-WAN AMIs**

To use the Cloud OnRamp for IaaS and other SD-WAN services, you must subscribe to the Amazon Machine Image (AMI) for your router in AWS. When you subscribe, you can complete the following tasks:
• Launch a cloud router AMI instance
• Generate a key pair to use for the instance
• Use the key pair to subscribe to the cloud router instance.

You subscribe to the cloud router AMI only once, when you first create an AMI instance.

To create a new AMI subscription and generate a key pair:
1. In AWS, do a search to locate the cloud router AMI for your devices.
2. Select and launch an EC2 instance with the AMI instance. For more information, see Create Cisco IOS XE SD-WAN Cloud VM Instance on AWS.
3. To generate the key pair, in Step 12 of the section Set Up the Viptela Cloud VM Instance, select Create a new key pair.
4. Click Download Key Pair. The key pair is then downloaded to your local computer as a .pem file.
5. Click Launch Instance. A failure message is displayed, because you now need to upload the key pair to complete the subscription process.

To upload the key pair:
2. Click the Continue button.
3. Click Key Pair to spin up a cloud router instance. In the option to enter the key pair, upload the .pem file from your local computer. This is the file that you generated in Step 4, above.

Azure Prerequisites

Before you can configure Cloud OnRamp for IaaS, you must properly provision Azure.

• Ensure that you have accepted the terms and conditions for the Cisco Cloud vEdge Router in the Azure Marketplace. See Accept the Azure Terms of Service.

• Ensure that you create an App Registration in Azure and retrieve the credentials for your Azure account. For Cloud OnRamp for IaaS, these credentials are used to authenticate the vManage server with Azure and bring up the VNet and the Virtual Machine instances. See Create and Retrieve Azure Credentials.

• Check the Azure limits associated with your account (by going to your subscription in the portal and checking Usage + Quotas) to ensure that the following resources can be created in your account:
  • 1 VNet, which is required for creating the transit VNet
  • 1 Availability set, required for Virtual Machine distribution in the transit VNet
  • 6 Static Public IP addresses associated with the transit cloud routers
  • 1 Azure Virtual Network Transit and 2 Static Public IP Addresses for each host VNet
  • 4 VPN connections for mapping each host VNet

• F-series VMs (F4 and F8) are supported for the cloud routers.
Accept the Azure Terms of Service

To use the Cisco Cloud Router as part of the Cloud OnRamp workflow, you must accept marketplace terms for using a virtual machine (VM). You can do this in one of the following ways:

- Spin up the cloud router on the portal manually, and accept the terms as part of the final page of the bringup wizard.
- In the Azure APIs or Powershell/Cloud Shell, use the Set-AzureRmMarketplaceTerms command.

Create and Retrieve Azure Credentials

To create and retrieve Azure credentials, you must create an App Registration in Azure with Contributor privileges:

1. Launch the Microsoft Azure portal.
2. Create an application ID:
   1. In the left pane of the Azure portal, click Azure Active Directory.
   2. In the sub-menu, click App registrations.
   3. Click New application registration. The system displays the Create screen.
   4. In the Name field, enter a descriptive name such as CloudOnRampApp.
   5. In the Application Type field,
   6. In the Sign-on URL field, enter any valid sign-on URL; this URL is not used in Cloud OnRamp.
   7. Click Create. The system displays a summary screen with the Application ID.
3. Create a secret key for the Cloud OnRamp application:
   1. In the summary screen, click Settings in the upper-left corner.
   2. In the right pane, click Keys. The system displays the Keys > Passwords screen.
3. In the Passwords screen:
   1. In the Description column, enter a description for your secret key.
   2. In the Expires column, from the Duration drop-down, select the duration for your secret key.
   3. Click Save in the upper-left corner of the screen. The system displays the secret key in the Value column but then hides it permanently, so be sure to copy and save the password in a separate location.

4. In the left pane of the Azure portal, click Subscriptions to view the subscription ID. If you have multiple subscriptions, copy and save the subscription ID which you are planning to use for configuring the Cloud OnRamp application.

5. View the Tenant ID:
   1. In the left pane of the Azure portal, click Azure Active Directory.
   2. Click Properties. The system displays the directory ID which is equivalent to the tenant ID.

6. Assign Contributor privileges to the application:
   1. In the left pane of the Azure portal, click Subscriptions.
2. Click on the subscription you will be using for the Cloud OnRamp application.
3. In the subscription pane, navigate to Access Control (IAM).
4. Click Add. The system displays the Add Permissions screen.
5. From the Role drop-down menu, select Contributor.
6. From the Assign Access To drop-down, select the default value Azure AD user, group, or application.
7. From the Select drop-down, select the application you just created for Cloud OnRamp.
8. Click Save.

You can now log into the Cloud OnRamp application with the Azure credentials you just created and saved.

**Configure Cloud OnRamp for IaaS for AWS**

To configure Cloud OnRamp for IaaS for AWS, you configure cloud instances using a configuration wizard. Follow the steps below, which are illustrated by this video. (Note that the video has no sound.)

1. In vManage NMS, select the Configuration ► Cloud OnRamp screen.
2. Click Add New Cloud Instance.
3. In the Add Cloud Instance–Log In to a Cloud Server popup:
1. In the Cloud drop-down, select the cloud type to be AWS.

2. Click IAM Role or Key to log in to the cloud server. It is recommended that you use IAM Role.

3. If you select IAM Role:
   1. In the Role ARN field, enter the role ARN of the IAM role.
   2. In the External ID field, enter external ID created for the role ARN. It is recommended that the external ID include 10 to 20 characters in random order. To authenticate to the vManage NMS using an IAM role, vManage NMS must be hosted by Viptela on AWS and have the following attributes: • Trusts the AWS account, 200235630647, that hosts the vManage NMS. • Have all permissions for EC2 and VPC resources. • A default timeout of at least one hour. If vManage NMS is not hosted by Viptela on AWS, assign an IAM role with permissions to AssumeRole to the vManage server running the Cloud OnRamp process. Refer to the AWS documentation for details.

4. If you select Key:
   1. In the API Key field, enter your Amazon API key.
   2. In the Secret Key field, enter the password associated with the API key.

4. Click Login to log in to the cloud server. The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a region and discover hosts VPCs, add transit VPC, and map host VPCs to transit VPCs. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

5. Select a region and discover host VPCs:
   1. In the Choose Region drop-down, select a geographical region.
   2. Click Discover Host VPCs. A list of host VPCs discovered in that region is displayed.
   3. Select the desired VPCs.
   4. Click Next.

6. Add a transit VPC:
   1. In the Transit VPC Name field, type a name for the transit VPC. The name can be up to 128 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   2. Under Device Information, enter information about the transit VPC:
      1. In the Version drop-down, select the software version to run on the VPC transit.
      2. In the Size of Transit drop-down, select how much memory and how many CPUs to create on the VPC transit.
      3. In the Device 1 drop-down, select the serial number to use.
      4. In the Device 2 drop-down, select the serial number to use.
      5. Click Advanced if you wish to enter more specific configuration options:
1. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.

2. In the SSH PEM Key drop-down, select a PEM key pair to log in to an instance. Note that the key pairs are region-specific. Refer to the AWS documentation for instructions on creating key pairs.

3. Click Save and Finish to create the transit VPC. Or click Proceed to Mapping to continue with the wizard.

3. Click Next.

7. Map the host VPCs to transit VPCs:
   1. In the table of host VPCs, select the desired host VPCs.
   2. Click Map VPCs. The Map Host VPCs popup opens.
   3. In the Transit VPC drop-down, select the transit VPC to map to the host VPCs.
   4. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
   5. Click Map VPCs.
   6. Click Save and Complete.

In the VPN feature configuration template for VPN 0, when configuring the two cloud routers that form the transit VPC, ensure that the color you assign to the tunnel interface is a public color, not a private color. Public colors are 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, public-internet, red, and silver.

**Configure Cloud OnRamp for IaaS for Azure**

To configure Cloud OnRamp for IaaS for Azure, you configure cloud instances using a configuration wizard:

**Create a Cloud Instance**

1. In vManage NMS, select the Configuration ▶ Cloud onRamp screen.
2. Click Add New Cloud Instance:
3. In the Add Cloud Instance–Log In to a Cloud Server popup:
   1. In the Cloud drop-down, select the cloud type to be Azure.
   2. To give vManage programmatic access to your Azure Subscription, log in to the cloud server:
      1. In the Subscription ID field, enter the ID of the Azure subscription you want to use as part of the Cloud OnRamp workflow.
      2. In the Client ID field, enter the ID of an existing application or create a new application in Azure. To create a new application, go to your Azure Active Directory ► App Registrations ► New Application Registration.
      3. In the Tenant ID field, enter the ID of your Azure account. To find the tenant ID, go to your Azure Active Directory and click Properties.
      4. In the Secret Key field, enter the password associated with the client ID.
4. Click Log In. The cloud instance configuration wizard opens. This wizard consists of three screens that you use to select a location and discover host VNets, add transit VNet, and map host VNets to transit VNets. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. Steps not yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

5. Select a location and discover host VNets:
   1. In the Choose Location drop-down, select a geographical location.
   2. Click Discover Host VNets. A list of host VNets discovered in that location is displayed.
   3. Select the desired VNet.
   4. Click Next.
6. Add a transit VNet:
   1. In the Transit VNet Name field, type a name for the transit VNet. The name can be up to 32 characters and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   2. Under Device Information, enter information about the transit VNet:
      1. In the WAN Edge Version drop-down, select the Viptela software version to run on the VNet transit. The drop-down lists the published versions of the Viptela software in the Azure marketplace.
      2. In the Size of Transit VNet drop-down, select how much memory and how many CPUs to create on the VNet transit.
      3. In the Device 1 drop-down, select the serial number to use.
      4. In the Device 2 drop-down, select the serial number to use.
      5. Click Advanced if you wish to enter more specific configuration options.
      6. In the Transit VPC Subnet field, enter a custom CIDR that has a network mask in the range of 16 to 25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16.
   3. Click Next.

7. Map the host VNets to transit VNets:
   1. In the table of host VNets, select the desired host VNet.
   2. Click Map VNets. The Map Host VNets popup opens.
   3. In the Transit VNet drop-down, select the transit VNet to map to the host VNets.
   4. In the VPN drop-down, select the VPN in the overlay network in which to place the mapping.
   5. In the IPSec Tunnel CIDR section, enter two pairs of interface IP addresses for each cloud router to configure IPSec tunnels to reach the Azure virtual network transit. The IP addresses must be network addresses in the /30 subnet, be unique across the overlay network, and not be a part of the host VNet CIDR. If they are part of the host VNet CIDR, Azure will return an error while attempting to create VPN connections to the transit VNet.
   6. In the Azure Information section:
      1. In the BGP ASN field, enter the ASN that will be configured on the Azure Virtual Network Transit that is spun up within the host VNet. Use an ASN that is not part of an existing configuration on Azure. For acceptable ASN values, refer to Azure documentation.
      2. In the Host VNet Gateway Subnet field, enter a host VNet subnet in which the Virtual Network Gateway can reside. It is recommended you use a /28 subnet or higher. You must not provide a subnet that is already created in the VNet.
   7. Click Map VNets.
   8. Click Save and Complete.
In the VPN feature configuration template for VPN 0, when configuring the two cloud routers that form the transit VNet, ensure that the color you assign to the tunnel interface is a public color, not a private color. Public colors are 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, public-internet, red, and silver.

Troubleshoot Cloud OnRamp for IaaS
This section describes how to troubleshoot common problems with Cloud OnRamp for IaaS.

Two Edge Routers Not Available

Problem Statement
In vManage NMS, when you select the Configuration ► Cloud OnRamp screen and click Add New Cloud instance, you see an error message indicating that two edge routers are not available.

Resolve the Problem
The vManage NMS does not have two cloud routers that are running licensed SD-WAN software. Contact your operations team so that they can create the necessary cloud routers.

If the routers are present and the error message persists, the two cloud routers are not attached to configuration templates. Attach these templates in the vManage Configuration ► Templates ► Device screen. Select the router, and then select Attach Devices from the More Actions icon to the right of the row.

Required Permissions for API

Problem Statement
When you enter your API keys, you get an error message indicating that this user does not have the required permissions.

Resolve the Problem
Ensure that the vManage server can reach the internet and has a DNS server configured so that it can reach AWS or Azure. To configure a DNS server, in the vManage VPN feature configuration template, enter the IP address of a DNS server, and then reattach the configuration template to the vManage server.

For AWS, check the API keys belonging to your AWS account. If you think you have the wrong keys, generate another pair of keys.

For AWS, if you are entering the correct keys and the error message persists, the keys do not have the required permissions. Check the user permissions associated with the key. Give the user the necessary permissions to create and edit VPCs and EC2 instances.

If the error message persists, check the time of the vManage server to ensure that it is set to the current time. If it is not, configure the vManage server’s time to point to the Google NTP server. In the vManage NTP feature configuration template, enter a hostname of time.google.com, time2.google.com, time3.google.com, or time4.google.com. Then reattach the configuration template to the vManage server.

No Correct Software Versions Appear in the Drop-Down

Problem Statement
When you are trying to configure transit VPC parameters for the transit VPC, no cloud software versions are listed in the drop-down.

Resolve the Problem
Ensure that you have subscribed to the Viptela marketplace Amazon machine images (AMIs) and the Cisco CSR AMIs in your AWS account. See Subscribe to Viptela AMIs.

**No VPNs Appear in Drop-Down**

**Problem Statement**
When you select the host VPCs or VNets to map, no VPNs are listed in the drop-down.

**Resolve the Problem**
This problem occurs when the device configuration template attached to the cloud router includes no service-side VPNs. Service-side VPNs (VPNs other than VPN 0 and VPN 512) are required to configure the IPsec connection between the two cloud routers selected for the transit and host VPCs or VNets.
This problem can also occur if the two cloud routers selected for the transit VPC or VNet have no overlapping service-side VPNs. Because the two routers form an active–active pair, the same service-side VPNs must be configured on both of them.
To configure service-side VPNs, in the vManage VPN feature configuration template, configure at least one service-side VPN. Ensure that at least one of the service-side VPNs is the same on both routers. Then reattach the configuration template to the routers.

**Cloud OnRamp Task Fails**

**Problem Statement**
After you have completed mapping the host VPCs to the transit VPCs, or host VNets to transit VNets, the Cloud OnRamp tasks fails.

**Resolve the Problem**
Review the displayed task information that is displayed on the screen to determine why the task failed. If the errors are related to AWS or Azure resources, ensure that all required resources are in place.

**Cloud OnRamp Task Succeeds, But Routers Are Down**

**Problem Statement**
The Cloud OnRamp task was successful, but the cloud routers are still in the Down state.

**Resolve the Problem**
Check the configuration templates:

- Check that all portions of the cloud router configuration, including policies, are valid and correct. If any of the configurations are invalid, they are not applied to the router, so the router never comes up.
- Check that the configuration for the vBond orchestrator is correct. If the DNS name or IP address configured of the vBond orchestrator is wrong, the router is unable to reach it and hence is unable to join the overlay network.

After you have determined what the configuration issues are:

1. Delete the Cloud OnRamp components:
   1. Unmap the host VPNs and the transit VPCs or VNets.
   2. Delete the transit routers.
2. Edit the configuration templates and reattach them to the cloud routers.
3. Repeat the Cloud OnRamp configuration process.

**Desired Routes Not Exchanged**

**Problem Statement**
The Cloud OnRamp configuration workflow is successful, the cloud routers are up and running, but the desired routes are not getting exchanged.

**Resolve the Problem**
In vManage NMS, check the BGP configuration on the transit cloud routers. During the mapping process when you configure Cloud OnRamp for IaaS, BGP is configured to advertise the network 0.0.0.0/0. Make sure that the service-side VPN contains an IP route that points to 0.0.0.0/0. If necessary, add a static route in the VPN feature configuration template, and then reattach the configuration to the two cloud routers that you selected for the transit VPC or VNet.

On AWS, go to the host VPC and check its route table. In the route table, click the option “Enable route propagation” to ensure that the VPC receives the routes.

**End-to-End Ping Is Unsuccessful**

**Problem Statement**
Routing is working properly, but an end-to-end ping is not working.

**Resolve the Problem**
On AWS, check the security group rules of the host VPC. The security group rules must allow the source IP address range subnets of the on-premises or branch-side devices, to allow traffic from the branch to reach AWS.

---

**Configure DHCP**

When you configure a tunnel interface on a vEdge router, a number of services are enabled by default on that interface, including DHCP.

A vEdge router can act as a DHCP server for the service-side network to which it is connected, and it can also act as a DHCP helper, forwarding requests for IP addresses from devices in the service-side network to a DHCP server that is in a different subnet on the service side of the vEdge router.

**Enable DHCP on the WAN Interface**
On a vEdge router WAN interface—the interface configured as a tunnel interface in VPN 0, the transport VPN—DHCP is enabled by default. You can see this by using the details filter with the show running-config command. This command also shows that the DNS and ICMP services are enabled by default.

```
vml# show running-config vpn 0 interface ge0/2 tunnel-interface | details
vpn 0
interface ge0/2
  tunnel-interface
    encapsulation ipsec weight 1
    color lte
    control-connections
```
carrier  default
no allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service ospf
no allow-service sshd
no allow-service ntp
no allow-service stun
!
!
!

Enabling DHCP on the router's WAN interface allows the device that actually connects the router to the transport network (such as a DSL router) to dynamically assign a DHCP address to the vEdge router. The DHCP service in VPN 0 affects the transport-side network.

**Have a vEdge Router Be a DHCP Server**

One or more service-side interfaces on vEdge router can act as a DHCP server, assigning IP addresses to hosts in the service-side network. To do this, configure this function on the interface that connects the vEdge router to the local site's network. At a minimum, you must configure the pool of IP addresses available for assigning to hosts:

```
vEdge(config-vpn)# interface geslot/port dhcp-server address-pool ip-address/prefix
vEdge(config-dhcp-server)#
```

You can exclude IP addresses that fall within the range of the DHCP address pool:

```
vEdge(config-dhcp-server)# exclude ip-address
```

To specify multiple individual addresses, list them in a single exclude command, separated by a space (for example, exclude 1.1.1.1 2.2.2.2 3.3.3.3). To specify a range of addresses, separate them with a hyphen (for example, exclude 1.1.1.1-1.1.1.10).

You can also statically assign IP addresses to a host:

```
vEdge(config-dhcp-server)# static-lease mac-address ip ip-address
```

By default, the DHCP server on a single interface can assign 254 DHCP leases, and each lease is valid for 24 hours. The offer of an IP address is valid indefinitely, until that DHCP server runs out of addresses to offer. You can modify these values:

```
vEdge(config-dhcp-server)# max-leases number
vEdge(config-dhcp-server)# lease-time seconds
vEdge(config-dhcp-server)# offer-time minutes
```

These values can range from 0 through (2^32 – 1).

The Viptela software supports DHCP server options that allow you to configure the IP addresses of a default gateway, DNS server, and TFTP server in the service-side network and the network mask of the service-side network:

```
vEdge(config-dhcp-server)# options default-gateway ip-address
vEdge(config-dhcp-server)# options dns-servers ip-address
vEdge(config-dhcp-server)# options domain-name domain-name
vEdge(config-dhcp-server)# options interface-mtu mtu
vEdge(config-dhcp-server)# options tftp-servers ip-address
```
Have a vEdge Router Be a DHCP Helper

One or more service-side interfaces on a vEdge router can be a DHCP helper. With this configuration, the interface forwards any broadcast BOOTP DHCP requests that it receives from hosts on the service-side network to the DHCP server or servers specified by the configured IP helper address (or addresses) and returns the assigned IP address to the requestor.

When the DHCP server at the vEdge router's local site is on a different segment than the devices connected to the vEdge router or than the vEdge router itself. When configured as a DHCP helper, the vEdge interface forwards any broadcast BOOTP DHCP requests that it receives to the DHCP server specified by the configured IP helper address.

To configure an interface as a DHCP helper, configure the IP address of the DHCP server on the interface that connects to the local site's network:

```
vEdge(config-vpn)# interface geslot/port dhcp-helper ip-address
```

You can configure up to four IP addresses, and you must enter the addresses in a single dhcp-helper command.

In Releases 17.2.2 and later, you can configure up to eight IP addresses. You must enter all the addresses in a single dhcp-helper command.

---

Configuring Single Sign-On using Okta

Okta provides secure identity management software that lets you connect any person with any application on any device using Single Sign-On (SSO).

Perform the following steps for configuring SSO:

- Configure SSO on the vManage UI
- Configure SSO on the Okta website

To configure SSO on the vManage UI:

1. In vManage, click **Administration ▶ Settings ▶ Identify Provider Settings ▶ Edit**.
2. Click **Enabled**.
3. Navigate to **Click here to download the SAML metadata** and save the content in a file. This data will be used for configuring Okta.
4. In Metadata, you need the following information to configure Okta with vManager:

To configure SSO on the Okta website:

1. Log on to the Okta website.
2. Create a username using your email address. Make sure you are using the Classic UI view on Okta. If not, change your view to the Classic UI view by clicking on the **Settings** button in the upper right corner.
3. Navigate to **Add applications ▶ Add application**.
4. Select **SAML 2.0** and click **Create**.
5. Use a string for Application name.

6. (Optional) Upload a logo and then click Next.

7. At SAML Settings, add the SSO URL using the samlLoginResponse URL from the downloaded metadata from the vManage UI.

8. Copy the entityId string and paste it in the Service Provider ID field.

9. For Name ID format, select EmailAddress and then click Enter.

10. For Application username, select Okta username.

11. For Show Advanced Settings, enter the fields as indicated below.

Table 219:

<table>
<thead>
<tr>
<th>Component</th>
<th>Value</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Assertion Signature</td>
<td>Signed</td>
<td></td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>RSA-SHA256</td>
<td></td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>SHA256</td>
<td></td>
</tr>
<tr>
<td>Assertion Encryption</td>
<td>Encrypted</td>
<td></td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES256-CBC</td>
<td></td>
</tr>
<tr>
<td>Key Transport Algorithm</td>
<td>RSA-OAEP</td>
<td></td>
</tr>
<tr>
<td>Encryption Certificate</td>
<td></td>
<td>1. Copy the encryption certificate from the metadata you downloaded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Go to <a href="http://www.samltool.com">www.samltool.com</a> and click on X.509 CERTS, paste there. Click Format X.509 Certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Make sure to remove the last empty line and then save the output (X.509.cert with header) into a text file encryption.cer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Upload the file. The Firefox browser may not allow you to do the upload. You can use the Chrome browser, however. You should see the certificate information after uploading to Okta.</td>
</tr>
<tr>
<td>Enable Single Logout</td>
<td></td>
<td>Make sure this is checked.</td>
</tr>
<tr>
<td>Single Logout URL</td>
<td></td>
<td>Get from the metadata.</td>
</tr>
<tr>
<td>SP Issuer</td>
<td></td>
<td>Use the entityId from the metadata.</td>
</tr>
</tbody>
</table>
Component | Value | Configuration
--- | --- | ---
2. Save to a file, for example, `signing.cer` and upload.

Authentication context class | X.509 Certificate |  |
Honor Force Authentication | Yes |  |
SAML issuer ID string | SAML issuer ID string |  |
Attributes Statements (optional) | Name ▶ Username ▶ Name format (optional) ▶ Unspecified Value ▶ `user:login` |  |
Group Attribute Statements (optional) | Name ▶ Groups ▶ Name format (optional) ▶ Unspecified ▶ Filter ▶ "Regex" - ".\*" |  |

1. Click **Next**.
2. For **App type**, check **This is an internal app that we have created** (optional).
3. Click **Finish**. This brings you to the Okta application page.
4. Click on **View Setup Instructions**.
5. Copy the IDP metadata.
6. Navigate back to the vManage UI.
7. Click on **Identity Provider Settings**.
8. Paste the IDP metadata that you copied on to **Upload Identity Provider Metadata**, and then click **Save**.

To assign users to the application in Okta:
1. On the Okta application page, navigate to **Assignments ▶ People ▶ Assign**.
2. Select **Assign to people** from the drop-down menu.
3. Click on **Assign** next to the user(s) you selected and click **Done**.
4. To add a user, click on **Directory ▶ Add Person ▶ Save**.

Configuring SSO using OKTA
- Entity ID
- Signing certificate
License Management

Cisco vManage supports the Cisco Managed Subscription License Agreement (MSLA), which allows the use of smart licenses for devices that vManage manages.

For complete information about the MSLA and how to obtain it, contact your Cisco account representative.

Overview

Before you can use an MSLA with vManage, you must create a Cisco Smart Account and virtual accounts, obtain smart licenses, and associate licenses with virtual accounts. After you set up the MSLA, you can use the Cisco Smart Software Manager (CSSM) to manage your smart licenses. Your Cisco account representative can provide more information about the MSLA, CSSM, and related requirements.

After you set up the MSLA and the CSSM, you can use vManage to download licenses and assign licenses to devices. vManage reports license usage to the Cisco Billing Platform (SBP) automatically on a regular basis.

[For the requirement that license tags need to be defined in the CSSM, is there anything that a user needs to do on the vManage side or anything that should be add to this overview?]

Set up vManage for Smart Licenses

Before you can use vManage to assign smart licenses to devices, you must configure vManage with your Smart Account login credentials and enable license management. To do so, follow these steps:

1. Select Administration ► Settings to display the Settings page.
2. Take these actions to enter your Smart Account login credentials:
   1. Click Edit in the Smart Account Credentials row. This row displays near the bottom of the page.
   2. In the Username field, enter your Smart Account user name.
   3. In the Password field, enter your Smart Account password.
1. Take these actions to enable license management:
   1. Click Edit in the License Management row. This row displays at the bottom of the page.
   2. Select the Enable radio button.
To disable license management, select the Disable radio button. Disabling this feature when licenses are assigned to devices removes the license assignments and deletes the licensing information from vManage. [what specific information?].

1. Click the Save button.

**License Manager Page**

The License manager page provides information about smart licenses that are assigned in vManage, and lets you manage license assignments for devices.

To display the License Manager page, select Administration ► License Manager.

The following table describes the items on the License Manager page. On the Overview tab, the Select Devices button displays only if no licenses are assigned to devices. The other Overview Tab items that the table describes display only if at least one device has a license assigned.

*Table 220:*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Select Devices button</td>
<td>Click to display the Device tab, from which you can assign licenses to devices. This button displays only if no licenses are assigned to devices.</td>
</tr>
<tr>
<td>Refresh button</td>
<td>Click to update the information on the overview tab with current data.</td>
</tr>
<tr>
<td>Device Assignment Distribution area</td>
<td>Includes a donut graph that indicates how many devices in your deployment have licenses assigned to them (the purple segment of the graph) and how many devices do not have licenses assigned to them (the green segment of the graph). Hover your mouse pointer over a graph segment to see the number of devices in the corresponding category.</td>
</tr>
<tr>
<td>Top 5 Licenses area</td>
<td>Includes a donut graph that indicates up to the 5 most used license types (tags) in your deployment, and a list of these licenses. Hover your mouse pointer over a graph segment to see the number of devices the corresponding license types is assigned to.</td>
</tr>
<tr>
<td>Top 5 Subscriptions area</td>
<td>Includes a donut graph that indicates up to the 5 most used subscription IDs in your deployment, and a list of these subscription IDs. Hover your mouse pointer over a graph segment to see the number of devices the corresponding subscription ID is assigned to.</td>
</tr>
</tbody>
</table>
Includes a table that provides the following information for each license that is assigned to at least 1 device:

- **License**—Name of the license, received with the license
- **Subscription**—Subscription ID of the device
- **Bill To**—Code that indicates the billing region for the license, received with the license
- **# of Devices**—How many devices the license is assigned to
- **Last Assigned On**—Date and time that the license was last assigned to a device

You can click any column heading in the table to toggle the information that the table displays between ascending and descending alphanumeric order by that column. By default, the table displays information in descending order of the number of devices to which each license is assigned.

<table>
<thead>
<tr>
<th><strong>Devices Tab</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sync Licenses button</strong></td>
<td>Click to download your smart licenses from Cisco to vManage.</td>
</tr>
<tr>
<td><strong>Rows Selected display</strong></td>
<td>Indicates how many rows you have selected in the Device table on this tab. You select a row by clicking its corresponding check box.</td>
</tr>
<tr>
<td><strong>Assign Bill To/License button</strong></td>
<td>Becomes available when you select in the Device table 1 or more devices to which no bill-to code/subscription ID and license are assigned. Click to assign a bill-to code/subscription ID code and optionally a license to the selected devices. For detailed information, see Assign License Components to Devices section.</td>
</tr>
<tr>
<td><strong>Edit Bill To/License button</strong></td>
<td>Becomes available when you select in the Device table 1 or more devices to which the same bill-to code/subscription ID are assigned. Click to change the bill-to code/subscription ID or license that are assigned to the selected device or devices, or to add a license to devices that have only a bill-to code/subscription ID. For detailed information, see Edit License Components for Devices.</td>
</tr>
<tr>
<td><strong>Search field and Search Options drop-down menu</strong></td>
<td>In the search field, enter one or more alphanumeric strings to display in the Device table only rows that contain or match these strings. The strings are not case sensitive. Press the Enter key or the Spacebar after entering a string. To remove a string from this field, click the X that appears next to it. From the Search Options drop-down menu, select whether the rows that display in the table contain or exactly match each of the search strings that you enter, and select which table column or columns the search strings apply to.</td>
</tr>
<tr>
<td><strong>Refresh button</strong></td>
<td>Click to update the information in the Device table with current information.</td>
</tr>
</tbody>
</table>
Device table

<table>
<thead>
<tr>
<th>Device table</th>
<th>Provides the following information for each device in your deployment:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Check box—Click to select the corresponding device to be the target of an Assign Bill To/License or Edit Bill To/License operation. You can click the check box in the title row of the table to quickly check all boxes in the table.</td>
</tr>
<tr>
<td></td>
<td>• Hostname—Hostname of the device.</td>
</tr>
<tr>
<td></td>
<td>• Chassis Number/ID—Chassis number and identifier of the device.</td>
</tr>
<tr>
<td></td>
<td>• Device model—Model of the device.</td>
</tr>
<tr>
<td></td>
<td>• System IP—IP address of the device.</td>
</tr>
<tr>
<td></td>
<td>• License Status—One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Valid—A bill-to code/subscription ID and license are assigned to the device</td>
</tr>
<tr>
<td></td>
<td>• Invalid—The license [or bill-to code/subscription ID?] that is assigned to this device is not valid (for example, it might be expired)</td>
</tr>
<tr>
<td></td>
<td>• Subscription Needed—A bill-to code/subscription ID code and license have not been assigned to the device</td>
</tr>
<tr>
<td></td>
<td>• License Needed—A subscription code has been assigned to the device but a license has not been assigned to it</td>
</tr>
<tr>
<td></td>
<td>• [are there any other status strings that can appear?]</td>
</tr>
<tr>
<td></td>
<td>• Bill To—Bill-to code that is assigned to the device.</td>
</tr>
<tr>
<td></td>
<td>• Subscription—Subscription ID that is assigned to the device.</td>
</tr>
<tr>
<td></td>
<td>• License—Name of the license that is assigned to the device.</td>
</tr>
<tr>
<td></td>
<td>• Last Updated—Date and time that the license was last assigned to the device</td>
</tr>
<tr>
<td></td>
<td>• You can click any column heading in the table as needed to toggle the information in the table between ascending and descending alphanumeric order by that column.</td>
</tr>
</tbody>
</table>

**Assign License Components to Devices**

From the License Management page, you can assign a bill-to code and subscription ID in combination, and a license to devices.

The following guidelines apply to assigning these items:

• You can assign the same bill-to code/subscription ID and license to one or more devices at the same time.

• You can assign the same bill-to code/subscription ID to one or more devices at the same time, and then assign the same or different licenses to these devices later as described in Edit License Components for Devices.

• A bill-to code and subscription ID are always assigned in combination.

• A device cannot have a license without a bill-to code/subscription ID assigned to it.
To assign a bill-to-code/subscription ID and license to one or more devices, follow these steps:

1. Select Administration ▶ License Manager to display the License Manager page.
2. Click the Device tab.
3. (Optional) Click the Sync Licenses button to download to vManage current smart licenses from Cisco.
4. In the Device table, check the check box for each device to which you want to assign the same bill-to-code/subscription ID and optionally the same license.

You can use the Search Field and the Search Options drop-down menu to locate devices, as described in License Manager Page.

1. Click the Assign Bill To/License button.

The Assign Bill To/License dialog box displays.

1. In the Assign Bill To/License dialog box, take the following actions as needed.

In this dialog box, you can choose to assign a bill-to-code/subscription ID and license at the same time, or you can choose to assign only a bill-to-code/subscription ID and then assign licenses later.

You cannot assign only a license.

1. Click the Bill To/Subscription field, and choose the desired bill-to-code and subscription ID combination from the drop-down list.

Changing an entry in this field removes any entry that is in the License field.

If you want to remove a bill-to-code/subscription ID, select None from the drop-down list. Selecting None here automatically enters None in the License field.

1. Click the License field, and choose the desired license from the drop-down list.

If you want to remove a license, select None from the drop-down list.

1. Click the Save button.

1. Click Close in the confirmation dialog box that displays.

**Edit License Components for Devices**

From the License Management page, you can edit (change) the bill-to-code and subscription ID in combination, and license assignments for devices.

The following guidelines apply to editing these items:

- You can edit items for a device only if the device has a bill-to-code/subscription ID assigned. The device can also have a license assigned, but that assignment is not needed to be able to edit items. In this way, you can assign a license after a bill-to-code/subscription ID has been assigned.

- You can edit items for multiple devices that have different bill-to-code/subscription ID assignments, license assignments, or both. When you save the edits, the vManage applies the new assignments to all devices that you selected.

- A bill-to-code and subscription ID are always edited in combination.
A device cannot have a license without a bill-to-code/subscription ID assigned to it.

To edit a bill-to-code/subscription ID and license assignment for one or more devices, follow these steps:

1. Select Administration ► License Manager to display the License Manager page.
2. Click the Device tab.
3. (Optional) Click the Sync Licenses button to download to vManage current smart licenses from Cisco.
4. In the Device table, check the checkbox for each device for which you want to edit the bill-to-code/subscription ID assignment, license assignment, or both.

You can edit items for a device only if the device has a bill-to-code/subscription ID or a bill-to-code/subscription ID and license assigned to it.

You can use the Search Field and the Search Options drop-down menu to locate devices, as described in License Manager Page.

1. Click the Edit Bill To/License button.

1. If you see a dialog box that indicates how many devices you selected and what licenses they are assigned, click the Next button.

This dialog box appears if you select multiple devices that have different license assignments. [true?]

1. In the Edit Bill To/License dialog box, take the following actions as needed.

In this dialog box, you can change a bill-to-code/subscription ID and license at the same time, or you can change just one of these items.

1. Click the Bill To/Subscription field, and choose the desired bill-to-code and subscription ID combination from the drop-down list.

Changing an entry in this field removes any entry that is in the License field.

If you want to remove (unassign) a bill-to-code/subscription ID, select None from the drop-down list in the Bill To/Subcription field. Selecting None here automatically enters None in the License field.

If you want to remove (unassign) a license, select None from the drop-down list in the license field.

1. Click the License field, and choose the desired license from the drop-down list.

You cannot select a license if None is selected in the Bill To/Subscription field. If you want to remove a license, select None from the drop-down list.

1. Click the Save button.

1. Click Close in the confirmation dialog box that displays.

**Troubleshooting**

Symptom: A status of “Invalid” appears in the License Status field on the Device tab of the License Management page. Cause: After a valid license is assigned to a device, you click the Sync Licenses button to obtain current licenses from Cisco, and the license that is assigned to the device is no longer available from Cisco. Solution: [what should a user do in this case?]
[Are there other troubleshooting items to include?]

**Audit Log**

The vManage audit log tracks every sync, assign, edit, and unassign operation that you perform on the License Management page. To access the audit log, select Monitor ► Audit Log.

---

**IPsec for Cisco IOS XE Routers**

Use the VPN Interface IPsec feature template to configure IPsec tunnels on Cisco IOS XE service VPNs that are being used for Internet Key Exchange (IKE) sessions. You can configure IPsec on tunnels for VPN 1 through 65530, except for 512.

**Create and Name the Template**

1. From the vManage menu, select Configuration ► Templates.
2. Click Feature.
3. Click **Add Template**.
4. Select a Cisco IOS XE device from the list.
5. From the VPN section, click **VPN Interface IPsec**. The VPN Interface IPsec template displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining IPsec parameters.
1. In the **TemplateName** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

2. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

**Changing the Scope for a Parameter Value**

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (a blue check), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:
Table 221:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Device Specific]</td>
<td>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</td>
</tr>
<tr>
<td>![Global]</td>
<td>Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.</td>
</tr>
</tbody>
</table>

Once you have created and named the VPN Interface IPSec template, enter the following values for your IPSec template. Parameters marked with an asterisk are required.

**Basic Configuration**

To configure a basic IPSec tunnel interface select the Basic Configuration tab and configure the following parameters.

Table 222:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options/Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown*</td>
<td>Yes / No</td>
<td>Click No to enable the interface; click Yes to disable.</td>
</tr>
<tr>
<td>Interface Name*</td>
<td>ipsec number (1…255)</td>
<td>Enter the name of the IPSec interface. <em>Number can be from 1 through 255.</em></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Enter a description of the IPSec interface.</td>
</tr>
<tr>
<td>IPv4 Address*</td>
<td>ipv4-prefix/length</td>
<td>Enter the IPv4 address of the IPSec interface. The address must have a /30 subnet.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Options/Format</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source*</td>
<td></td>
<td>Set the source of the IPsec tunnel that is being used for IKE key exchange:</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>Click and enter the IPv4 address that is the source tunnel interface. This address must be configured in VPN 0.</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
<td>Click and enter the name of the physical interface that is the source of the IPsec tunnel. This interface must be configured in VPN 0.</td>
</tr>
<tr>
<td>Destination*</td>
<td></td>
<td>Set the destination of the IPsec tunnel that is being used for IKE key exchange.</td>
</tr>
<tr>
<td>IPsec Destination IP Address</td>
<td></td>
<td>Enter an IPv4 address that points to the destination.</td>
</tr>
</tbody>
</table>
| TCP MSS                     |                | Specify the maximum segment size (MSS) of TPC SYN packets passing through the router. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented.  
  Range: 552 to 1960 bytes  Default: None |
| IP MTU                      |                | Specify the maximum transmission unit (MTU) size of packets on the interface.  
  Range: 576 through 2000  Default: 1500 bytes |

To save the feature template, click Save.

**CLI Equivalent**

```plaintext
crypto
interface tunnel
  ifnum
    no shutdown
  vrf forwarding
    vrf_id
      ip address
        ip_address[mask]
  tunnel source
    wanif_ip
      tunnel mode {ipsec ipv4 | gre
        ipaddress}
  tunnel destination
    gateway_ip
      tunnel protection ipsec profile
        ipsec_profile_name
```
**Configure Dead-Peer Detection**

To configure Internet key exchange (IKE) dead-peer detection (DPD) to determine whether the connection to an IKE peer is functional and reachable, select the DPD tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **DPD Interval** | Specify the interval for IKE to send Hello packets on the connection.  
*Range:* 10 through 3600 seconds  
*Default:* Disabled |
| **DPD Retries** | Specify how many unacknowledged packets to accept before declaring an IKE peer to be dead and then tearing down the tunnel to the peer.  
*Range:* 2 through 60  
*Default:* 3 |

To save the feature template, click **Save**.

**CLI Equivalent**

```
crypto
ikev2
profile ikev2_profile_name
dpd
10-3600
2-60 (on-demand | periodic)
```  

**Configure IKE**

To configure IKE, select the IKE tab and configure the following parameters.

**Note:** When you create an IPsec tunnel on a Cisco IOS XE router, IKE Version 1 is enabled by default on the tunnel interface.

**IKE version 1**

To modify IKEv1 parameters, configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| **IKE Version** | 1 IKEv1  
2 IKEv2 | Enter 1 to select IKEv1.  
Default: IKEv1 |
| **IKE Mode** | Aggressive mode  
Main mode | Specify the IKE SA establishment mode.  
Default: Main mode |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 hour through 14 days Default: 14400 seconds (4 hours)</td>
</tr>
<tr>
<td>IKE Cipher Suite</td>
<td>AES128-CBC-SHA1</td>
<td>Specify the type of authentication and encryption to use during IKE key exchange.</td>
</tr>
<tr>
<td></td>
<td>AES256-CBC-SHA1</td>
<td>Default: AES256-CBC-SHA1</td>
</tr>
<tr>
<td>IKE Diffie-Hellman Group</td>
<td>1024-bit modulus</td>
<td>Specify the Diffie-Hellman group to use in IKE key exchange.</td>
</tr>
<tr>
<td></td>
<td>2048-bit modulus</td>
<td>Default: 4096-bit modulus</td>
</tr>
<tr>
<td></td>
<td>3072-bit modulus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4096-bit modulus</td>
<td></td>
</tr>
<tr>
<td>IKE Authentication</td>
<td>Configure IKE authentication.</td>
<td></td>
</tr>
<tr>
<td>Preshared Key</td>
<td>Enter the password to use with the preshared key.</td>
<td></td>
</tr>
<tr>
<td>IKE ID for Local End Point</td>
<td>If the remote IKE peer requires a local end point identifier, specify it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 64 characters</td>
<td>Default: Tunnel's source IP address</td>
</tr>
<tr>
<td>IKE ID for Remote End Point</td>
<td>If the remote IKE peer requires a remote end point identifier, specify it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Range: 1 through 64 characters</td>
<td>Default: Tunnel's destination IP address</td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

**CLI Equivalent**

```plaintext
crypto
isakmp
keepalive
  60-86400 2-60 {on-demand | periodic}
policy
  policy_num
  encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
  hash {sha384 | sha256 | sha}
  authentication pre-share
  group {2 | 14 | 16 | 19 | 20 | 21}
lifetime
  60-86400
```
IKE version 2

To configure the IPsec tunnel that carries IKEv2 traffic, select the IPsec tab and configure the following parameters:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Version</td>
<td>1 IKEv1</td>
<td>Enter 2 to select IKEv2.</td>
</tr>
<tr>
<td></td>
<td>2 IKEv2</td>
<td>Default: IKEv1</td>
</tr>
<tr>
<td>IKE Mode</td>
<td>Aggressive</td>
<td>Aggressive mode -- Negotiation is quicker, and the initiator and responder</td>
</tr>
<tr>
<td></td>
<td>Main</td>
<td>ID pass in the clear.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Main mode -- Establishes an IKE SA session before starting IPsec negotiations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Main</td>
</tr>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 hour through 14 daysDefault: 14400 seconds (4 hours)</td>
</tr>
</tbody>
</table>
## Parameter Name | Options | Description
--- | --- | ---
IKE Cipher Suite | AES128-CBC-SHA1, AES256-CBC-SHA1 | Specify the type of authentication and encryption to use during IKE key exchange. Default: AES256-CBC-SHA1

IKE Diffie-Hellman Group | 2 1024-bit modulus, 14 2048-bit modulus, 15 3072-bit modulus, 16 4096-bit modulus | Specify the Diffie-Hellman group to use in IKE key exchange. Default: 16 4096-bit modulus

IKE Authentication | Configure IKE authentication.

Preshared Key | Enter the password to use with the preshared key.

IKE ID for Local End Point | If the remote IKE peer requires a local end point identifier, specify it. Range: 1 through 64 characters. Default: Tunnel's source IP address

IKE ID for Remote End Point | If the remote IKE peer requires a remote end point identifier, specify it. Range: 1 through 64 characters. Default: Tunnel's destination IP address

To save the feature template, click **Save**.

**CLI Equivalent**

```bash
crypto
ikev2
proposal
proposal_name
    encryption 3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des
    integrity sha256 | sha384 | sha512
    group 2 | 14 | 15 | 16
    keyring idev2_keyring_name
    peer peer_name
    address tunnel_dest_ip [mask]
    pre-shared-key
    key_string
    profile idev2_profile_name
    match identity remote address
    ip_address
```
authentication (remote | local) pre-share
keyring local
ikev2_keyring_name
lifetime
120-86400

Configure IPsec Tunnel Parameters

To configure the IPsec tunnel that carries IKE traffic, select the IPsec tab and configure the following parameters:

Table 226:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec Rekey Interval</td>
<td>3600 - 1209600 seconds</td>
<td>Specify the interval for refreshing IKE keys.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 hour through 14 days Default: 3600 seconds</td>
<td></td>
</tr>
<tr>
<td>IKE Replay Window</td>
<td>64, 128, 256, 512, 1024, 2048, 4096, 8192 bytes</td>
<td>Specify the replay window size for the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>Default: 512</td>
<td></td>
</tr>
<tr>
<td>IPsec Cipher Suite</td>
<td>aes256-cbc-sha1, aes256-gcm, null-sha1</td>
<td>Specify the authentication and encryption to use on the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>Default: aes256-gcm</td>
<td></td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>2  1024-bit modulus</td>
<td>Specify the PFS settings to use on the IPsec tunnel.</td>
</tr>
<tr>
<td></td>
<td>14  2048-bit modulus</td>
<td>Select one of the following Diffie-Hellman prime modulus groups:</td>
</tr>
<tr>
<td></td>
<td>15  3072-bit modulus</td>
<td>1024-bit – group-2 2048-bit – group-14 3072-bit</td>
</tr>
<tr>
<td></td>
<td>16  4096-bit modulus</td>
<td>– group-15 4096-bit – group-16 none – disable PFS. Default: group-16</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

To save the feature template, click Save.

CLI Equivalent

```
crypto
ipsec
profile
ipsec_profile_name
set ikev2-profile
ikev2_profile_name
set security-association
lifetime {seconds 120-2592000 | kilobytes disable}
replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}}
set pfs group {2 | 14 | 15 | 16 | none}
set transform-set
```
Configuring IKE-Enabled IPsec Tunnels

To securely transfer traffic from the overlay network to a service network, you can configure IPsec tunnels that run the Internet Key Exchange (IKE) protocol. IKE-enabled IPsec tunnels provide authentication and encryption to ensure secure packet transport.

You create an IKE-enabled IPsec tunnel by configuring an IPsec interface. IPsec interfaces are logical interfaces, and you configure them just like any other physical interface. You configure IKE protocol parameters on the IPsec interface, and you can configure other interface properties.

The Viptela software supports IKE, Version 1, as defined in RFC 2409, Internet Key Exchange, and IKE, Version 2, as defined in RFC 7296, Internet Key Exchange Protocol, Version 2.

One use for IPsec tunnels is to allow vEdge Cloud router VM instances running on Amazon AWS to connect to the Amazon virtual private cloud (VPC). You must configure IKE Version 1 on these routers.

Configure an IPsec Tunnel

To configure an IPsec tunnel interface for secure transport traffic from a service network, you create a logical IPsec interface:

```
vEdge(config)# vpn
vEdge(config)# vpn-id interface ipsec number
vEdge(config)# interface ipsec number
vEdge(config)# ip address ipv4-prefix/length
vEdge(config)# (tunnel-source ip-address | tunnel-source-interface interface-name)
vEdge(config)# (tunnel-destination ipv4-address)
```

You can create the IPsec tunnel in the transport VPN (VPN 0) and in any service VPN (VPN 1 through 65530, except for 512).

The IPsec interface has a name in the format ipsec number, where number can be from 1 through 255.

Each IPsec interface must have an IPv4 address. This address must be a /30 prefix. All traffic in the VPN that is within this IPv4 prefix is directed to a physical interface in VPN 0 to be sent securely over an IPsec tunnel.

To configure the source of the IPsec tunnel on the local device, you can specify either the IP address of the physical interface (in the tunnel-source command) or the name of the physical interface (in the tunnel-source-interface command). Ensure that the physical interface is configured in VPN 0.

To configure the destination of the IPsec tunnel, specify the IP address of the remote device in the tunnel-destination command.

The combination of a source address (or source interface name) and a destination address defines a single IPsec tunnel. Only one IPsec tunnel can exist that uses a specific source address (or interface name) and destination address pair.
Configure an IPsec Static Route

To direct traffic from the service VPN to an IPsec tunnel in the transport VPN (VPN 0), you configure an IPsec-specific static route in a service VPN (a VPN other than VPN 0 or VPN 512):

```
vEdge(config)# vpn
  vpn-id
vEdge(config-vpn)# ip ipsec-route prefix/length
  vpn 0 interface
  ipsec
  number [ipsec
  number2]
```

The VPN ID is that of any service VPN (VPN 1 through 65530, except for 512).

`prefix/length` is the IP address or prefix, in decimal four-part-dotted notation, and prefix length of the IPsec-specific static route.

The interface is the IPsec tunnel interface in VPN 0. You can configure one or two IPsec tunnel interfaces. If you configure two, the first is the primary IPsec tunnel, and the second is the backup. With two interfaces, all packets are sent only to the primary tunnel. If that tunnel fails, all packets are then sent to the secondary tunnel. If the primary tunnel comes back up, all traffic is moved back to the primary IPsec tunnel.

Enable IKE Version 1

When you create an IPsec tunnel on a vEdge router, IKE Version 1 is enabled by default on the tunnel interface. The following properties are also enabled by default for IKEv1:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours
- SA establishment mode—Main

By default, IKEv1 uses IKE main mode to establish IKE SAs. In this mode, six negotiation packets are exchanged to establish the SA. To exchange only three negotiation packets, enable aggressive mode:

```
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# mode aggressive
```

By default, IKEv1 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# group
  number
```
By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```plaintext
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# cipher-suite
  suite
```

The authentication `suite` can be one of the following:

- **aes128-cbc-sha1**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
- **aes256-cbc-sha1**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.
- **aes256-cbc-sha2**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 1 hours (3600 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds). It is recommended that the rekeying interval be at least 1 hour.

```plaintext
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# rekey seconds
```

To force the generation of new keys for an IKE session, issue the `request ipsec ike-rekey` command.

```plaintext
vEdge(config)# vpn vpn-id interface ipsec number ike
```

For IKE, you can also configure preshared key (PSK) authentication:

```plaintext
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret
  password
```

`password` is the password to use with the preshared key. It can be an ASCII or a hexadecimal string from 1 through 127 characters long.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:
The identifier can be an IP address or any text string from 1 through 63 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

**Enable IKE Version 2**

When you configure an IPsec tunnel to use IKE Version 2, the following properties are also enabled by default for IKEv2:

- Authentication and encryption—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- Diffie-Hellman group number—16
- Rekeying time interval—4 hours

By default, IKEv2 uses Diffie-Hellman group 16 in the IKE key exchange. This group uses the 4096-bit more modular exponential (MODP) group during IKE key exchange. You can change the group number to 2 (for 1024-bit MODP), 14 (2048-bit MODP), or 15 (3072-bit MODP):

```
vEdge(config)# vpn
    vpn-id
    interface ipsec
    number
    ike
vEdge(config-ike)# group
    number
```

By default, IKE key exchange uses AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity. You can change the authentication:

```
vEdge(config)# vpn
    vpn-id
    interface ipsec
    number
    ike
vEdge(config-ike)# cipher-suite
    suite
```

The authentication *suite* can be one of the following:

- **aes128-cbc-sha1**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity
- **aes128-cbc-sha2**—AES-128 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity
• **aes256-cbc-sha1**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA1 keyed-hash message authentication code algorithm for integrity; this is the default.

• **aes256-cbc-sha2**—AES-256 advanced encryption standard CBC encryption with the HMAC-SHA256 keyed-hash message authentication code algorithm for integrity

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# rekey seconds
```

To force the generation of new keys for an IKE session, issue the `request ipsec ike-rekey` command.

For IKE, you can also configure preshared key (PSK) authentication:

```
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike
vEdge(config-ike)# authentication-type pre-shared-key pre-shared-secret
  password
```

`password` is the password to use with the preshared key. It can be an ASCII or a hexadecimal string, or it can be an AES-encrypted key.

If the remote IKE peer requires a local or remote ID, you can configure this identifier:

```
vEdge(config)# vpn
  vpn-id
  interface ipsec
  number
  ike authentication-type
vEdge(config-authentication-type)# local-id
  id
vEdge(config-authentication-type)# remote-id
  id
```

The identifier can be an IP address or any text string from 1 through 64 characters long. By default, the local ID is the tunnel's source IP address and the remote ID is the tunnel's destination IP address.

**Configure IPsec Tunnel Parameters**

By default, the following parameters are used on the IPsec tunnel that carries IKE traffic:

- Authentication and encryption—AES-256 algorithm in GCM (Galois/counter mode)
- Rekeying interval—4 hours
- Replay window—32 packets
You can change the encryption on the IPsec tunnel to the AES-256 cipher in CBC (cipher block chaining mode, with HMAC-SHA1-96 keyed-hash message authentication or to null, to not encrypt the IPsec tunnel used for IKE key exchange traffic:

```plaintext
vEdge(config-interface-ipsecnumber)# ipsec
tEdge(config-ipsec)# cipher-suite (aes256-cbc-shal | aes256-gcm | null-shal)
```

By default, IKE keys are refreshed every 4 hours (14,400 seconds). You can change the rekeying interval to a value from 30 seconds through 14 days (1209600 seconds):

```plaintext
vEdge(config-interface-ipsecnumber)# ipsec
tEdge(config-ipsec)# rekey seconds
```

To force the generation of new keys for an IPsec tunnel, issue the `request ipsec ipsec-rekey` command.

By default, perfect forward secrecy (PFS) is enabled on IPsec tunnels, to ensure that past sessions are not affected if future keys are compromised. PFS forces a new Diffie-Hellman key exchange, by default using the 4096-bit Diffie-Hellman prime module group. You can change the PFS setting:

```plaintext
vEdge(config-interface-ipsecnumber)# ipsec
tEdge(config-ipsec)# perfect-forward-secrecy pfs-setting
```

`pfs-setting` can be one of the following:

- **group-2** — Use the 1024-bit Diffie-Hellman prime modulus group.
- **group-14** — Use the 2048-bit Diffie-Hellman prime modulus group.
- **group-15** — Use the 3072-bit Diffie-Hellman prime modulus group.
- **group-16** — Use the 4096-bit Diffie-Hellman prime modulus group. This is the default.
- **none** — Disable PFS.

By default, the IPsec replay window on the IPsec tunnel is 512 bytes. You can set the replay window size to 64, 128, 256, 512, 1024, 2048, or 4096 packets:

```plaintext
vEdge(config-interface-ipsecnumber)# ipsec
tEdge(config-ipsec)# replay-window number
```

**Modify IKE Dead-Peer Detection**

IKE uses a dead-peer detection mechanism to determine whether the connection to an IKE peer is functional and reachable. To implement this mechanism, IKE sends a Hello packet to its peer, and the peer sends an acknowledgment in response. By default, IKE sends Hello packets every 10 seconds, and after three unacknowledged packets, IKE declares the neighbor to be dead and tears down the tunnel to the peer. Thereafter, IKE periodically sends a Hello packet to the peer, and re-establishes the tunnel when the peer comes back online.

You can change the liveness detection interval to a value from 0 through 65535 seconds, and you change the number of retries to a value from 0 through 255:

```plaintext
vEdge(config-interface-ipsecnumber)# dead-peer-detection
seconds
```
Configure Other Interface Properties

For IPsec tunnel interfaces, you can configure only the following additional interface properties:

```
vEdge(config-interface-ipsec)# mtu bytes
vEdge(config-interface-ipsec)# tcp-mss-adjust bytes
```

How to configure IKE-enabled IPsec tunnel interfaces on vEdge routers.

Intrusion Prevention Configuration on SD-WAN

You can configure Intrusion Prevention policy with a configuration wizard. The Intrusion Prevention configuration workflow contains the following components:

- Administration Settings
- Intrusion Prevention Configuration
- Apply IPS Policy to a device

In Cisco vManage NMS, select the Administration ► Settings tab in the left side panel to configure IPS Signature Update. Click on Edit to Enable/Disable and provide Username and Password details to save the Policy details as shown in the following screenshot.

How to configure Intrusion Prevention on SD-WAN routers.

Administration Settings

Intrusion Prevention Configuration

To configure Intrusion Prevention through Security, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ► Security tab in the left side panel.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios display.

3. In Add Security Policy, select a scenario that supports intrusion prevention (**Compliance**, **Direct Cloud Access**, **Direct Internet Access**, or **Custom**).

4. Click **Proceed** to add an Intrusion Prevention policy in the wizard.

5. In the **Add Security Policy** wizard, click **Next** to select the **Add Intrusion Prevention** tab to create a new Intrusion Prevention Policy.
6. Click the **Add Intrusion Prevention Policy** drop-down, select **Create New** to create a new Intrusion Prevention policy. The Intrusion Prevention - Policy Rule Configuration wizard appears.

7. Enter a policy name in the **Policy Name** field.

8. Choose a signature set that defines rules for evaluating traffic from the Signature Set drop-down. The following options are available. Connectivity provides the least restrictions and the highest performance. Security provide the most protections but can affect system performance.
   - Connectivity—Less restrictive/better performance (fewer rules)
   - Balanced—Designed to provide protection without a significant effect on system performance
   - Security—More protection/less performance

9. Choose mode of operation from the Inspection Mode drop-down. The following options are available:
   - Detection—Select this option for intrusion detection mode
• Protection—Select this option for intrusion protection mode

10. From the Advanced tab, choose one or more existing IPS signature whitelist lists or create new ones as needed from the Signature Whitelist drop-down.

To create a new signature list, click **New Signature List** at the bottom of the drop-down. In the IPS Signature List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the IPS Signature field, enter signatures in the format **Generator ID:Signature ID**, separated with commas. You also can use the Import button to add a whitelists from an accessible storage location. Click Save when you are finished.

You also can create or manage IPS Signature Whitelist lists by selecting the **Configuration ► Security** tab in the left side panel, choosing **Lists** from the Custom Options drop-down at the top right of the page, and then selecting **Signatures** in the left panel.

To remove an IPS Signature Whitelist from the Signature Whitelist field, click the “X” next to the list name in the field.

11. Choose an alert level for syslogs from the **Alert Log Level** drop-down. The options are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

12. Click on **Target VPNs** to add required number of VPNs in Add Target VPNs wizard.
13. Click **Save Changes** to add an Intrusion Prevention policy.

14. Click on **Policy Summary** tab to attach a policy to Security Master Policy Configuration.

15. Enter Security Policy Name and Security Policy Description in the respective fields.

16. In the Additional Policy Settings tab ► Intrusion Prevention and/or URL Filtering, choose the following options:
   - External Syslog Server VPN
   - Server IP
• Failure Mode – Open/Close

17. Click **Save Policy Changes** to configure Intrusion Security policy.

18. You can edit the existing Intrusion Prevention policy by clicking on **Custom Options** in the right-side panel of vManage ► Configuration ► Security wizard.

**Applying Intrusion Prevention Policy to a Device**

1. In vManage NMS, select the Configuration ► Templates screen.

2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.

3. From the **Device Model** drop-down, select one of the IOSXESD-WAN devices.

4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

5. From the **Security Policy** drop-down, select the name of the **Intrusion Policy** you configured in the above procedure.

6. Click **Create** to apply Intrusion policy to a device.

**Monitoring Intrusion Prevention Feature**

You can monitor the Intrusion Prevention System (IPS) signature violations by severity and by count using the following steps.
To monitor the Signatures of IPS Configuration on IOS XE SD-WAN device:

1. From the Monitor ► Network screen, select a device.

2. In the left panel, under Security Monitoring, select Intrusion Prevention tab. The Intrusion Prevention wizard displays.

3. Click By Severity or By Count to designate how you want to display intrusion prevention information.
How to configure Intrusion Prevention on SD-WAN routers.

**URL Filtering Configuration on vManage**

How to configure URL Filtering on a vManage

**URL Filtering Configuration on SD-WAN**

The URL Filtering feature enables the user to provide controlled access to Internet websites or Intranet sites by configuring URL-based policies and filters on the device. The URL Filtering feature is implemented using the Snort Intrusion Prevention engine.

You can configure URL Filtering with a Security configuration wizard.

**URL Filtering Configuration**

To configure URL Filtering through Security, use the vManage security configuration wizard:

1. In Cisco vManage, select the Configuration ▶ Security tab in the left side panel.
2. Click Add Security Policy. The Add Security Policy wizard appears and various use-case scenarios display.


4. Click Proceed to add an Intrusion Prevention policy in the wizard.

5. In the Add Security Policy wizard, select URL Filtering tab to create a new URL Filtering Policy.

7. Enter the policy name in Policy Name field.

8. Choose one of the following options from the Web Categories drop-down:
   - Block—Block websites that match the categories that you select
• Allow—Allow websites that match the categories that you select

9. Select one or more categories to block or allow from the Web Categories list.

10. Select the Web Reputation from the drop-down. The options are:
    • High Risk
    • Suspicious
    • Moderate Risk
    • Low Risk
    • Trustworthy

11. From the Advanced tab, choose one or more existing Whitelist URL lists or create new ones as needed from the Whitelist URL List drop-down.

Items on the whitelist are not subject to domain filtering. If the same item is configured under both the whitelist and the blacklist, the traffic is whitelisted.

To create a new URL list, click New Whitelist URL List at the bottom of the drop-down. In the Whitelist URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the Add Whitelist URL field, enter URLs to include in the list, separated with commas. You also can use the Import button to add whitelists from an accessible storage location. Click Save when you are finished.

1. From the Advanced tab, choose one or more existing Blacklist URL lists or create new ones as needed from the Blacklist URL List drop-down.

Items on the blacklist are subject to domain filtering. If the same item is configured under both the whitelist and the blacklist, the traffic is whitelisted.

To create a new URL list, click New Blacklist URL List at the bottom of the drop-down. In the Blacklist URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the Add Blacklist URL field, enter URLs to include in the list, separated with commas. You also can use the Import button to add blacklists from an accessible storage location. Click Save when you are finished.

You also can create or manage blacklist URL lists by selecting the Configuration ► Security tab in the left side panel, choosing Lists from the Custom Options drop-down at the top right of the page, and then selecting Blacklist URLs in the left panel.

To remove a URL list from the Blacklist URL List field, click the “X” next to the list name in the field.

1. In the Block Page Server pane, choose an option to designate what happens when a user visits a URL that is blocked. Choose Block Page Content to display a message that access to the page has been denied, or choose Redirect URL to display another page.
In the Alerts and Logs pane, select the alert type from the following options:

- **Blacklist**—Exports an alert as a Syslog message if a user tries to access a URL that is configure in the Blacklist URL List
- **Whitelist**—Exports an alert as a Syslog message if a user tries to access a URL that is configure in the Whitelist URL List
- **Reputation/Category**—Exports an alert as a Syslog message if a user tries to access a URL that has a reputation that is configured in the Web Reputation field or that matches a blocked or allowed web category

1. Click on Target VPNs to add required number of VPNs in Add Target VPNs wizard.
1. Click Save Changes to add target VPNs.
2. Click Save URL Filtering Policy to configure URL Filtering.
3. You can edit the existing URL Filtering policy by clicking on Custom Options in the right-side panel of vManage ► Configuration ► Security wizard.

Monitoring URL Filtering Feature

You can monitor the URL Filtering for a device by web categories using the following steps.
To monitor the URLs that are blocked or allowed on an IOS XE SD-WAN device:
1. From the Monitor ► Network screen, select a device.
2. In the left panel, under Security Monitoring, select URL Filtering tab. The URL Filtering wizard displays.
3. Click on Blocked tab, and the session count on a blocked URL appears as shown in the following screenshot.
4. Click on Allowed tab, the session count on allowed URLs appear as shown in the following screenshot.

How to configure URL Filtering on a vManage

Using Umbrella DNS Security

Umbrella Configuration on SD-WAN

How to configure Umbrella policy with a configuration wizard.

Umbrella Configuration on SD-WAN

The Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device.

You can configure Umbrella policy with a configuration wizard. The wizard is a UI policy builder that consists of the following components:
- Configure Umbrella API Token
- Define Domain list
- Configure Umbrella DNS
- Apply Umbrella DNS Security Policy to a Template
- Monitor Umbrella Feature

**Configure Umbrella API Token**

1. In Cisco vManage NMS, select the Configuration ► Security tab ► Custom Options on the right side to configure the Umbrella API Token as shown in the following screenshot.

   ![Cisco vManage Configuration Screen](image)

2. Enter token number in the **Umbrella Token** field.
3. Click **Save** to configure the Umbrella API Token.

### Defining Domain Lists

To define Domain-List, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ► Security tab ► Custom Options in the right side.

![Configuration ► Security tab](image1)

2. Click on **Lists** in the Custom Options drop-down. A Define Lists wizard appears.

![Define Lists wizard](image2)

3. Click on **New Domain List** to create a new domain list or select the domain name and click on pencil icon on the right side for the existing list.

![New Domain List](image3)

4. Enter the **Domain List Name**, **Domain** and click **Save** to create the list.

### Configure Umbrella DNS Policy

To configure umbrella through DNS Security, use the vManage security configuration wizard:

1. In Cisco vManage NMS, select the Configuration ► Security tab in the left side panel.

3. The Add Security Policy configuration wizard opens, and various use-case scenarios display.

4. In Add Security Policy, select **Direct Internet Access**.

5. Click **Proceed** to add a Umbrella DNS Security policy in the wizard.

6. In the Add Security Policy wizard, select DNS Security tab to create a new DNS Security policy.
7. Click the **Add DNS Security Policy** drop-down and select from the following options:
   - Copy from Existing - A Copy from Existing DNS Security Policy wizard appears. Select a **Policy** from the drop-down and enter **Policy Name** and copy the policy to a device.

8. If you are creating a new policy using **Create New**, a DNS Security - Policy Rule Configuration wizard appears.

9. Enter a policy name in the **Policy Name** field.

10. The Umbrella Registration Status displays the status about the API Token configuration.

11. Click on **Manage Umbrella Registration** to add a token.
12. Select **Match All VPN** option if you need to keep the same configuration for all the available VPNs and continue with step 13.

Or select **Custom VPN Configuration** if you need to add target VPNs to your policy. A Target VPNs wizard appears.

To add target VPNs, click **Target VPNs** in the Add DNS Security Policy wizard.

Click **Save Changes** to add the VPN.

13. Select the domain bypass from the **Local Domain Bypass List** drop-down as shown.
14. Configure the **DNS Server IP** from the following options:
   - Umbrella Default
   - Custom DNS

15. Click on the **Advanced** tab to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.

16. Click **Save DNS Security Policy** to configure DNS Security policy. The Configuration ► Security screen is then displayed, and the DNS Policy list table includes the newly created dns security policy.

---

**Applying DNS Umbrella Policy to a IOS XE Router**

1. In vManage NMS, select the Configuration ► Templates screen.
2. In the Device tab, from the Create Template drop-down, select From Feature Template.
3. From the Device Model drop-down, select one of the IOS XE devices.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
5. From the Security Policy drop-down, select the name of the Umbrella DNS Security Policy you configured in the above procedure.
6. Click Create to apply Umbrella policy to a device.

Monitoring Umbrella Feature

You can monitor the registered VPNs, DNSCrypt status, packet counts for required timestamps on a umbrella configured router using the following steps.
To monitor the status of Umbrella DNS Configuration on IOS XE device:

1. From the Monitor ► Network screen, select an IOS XE device.

2. In the left panel, under Security Monitoring, select Umbrella DNS Re-direct tab. The Umbrella DNS Re-direct wizard displays showing how many packets are redirected to configured DNS server.

3. Click on Local Domain Bypass to monitor the packet counts showing how many packets are bypassed to DNS server.

How to configure Umbrella policy with a configuration wizard.

**Umbrella Integration Using CLI**

The Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device. The security administrator configures policies on the Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). The
router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

**Restrictions for Umbrella Integration**

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.

- When the client is connected to a web proxy, the DNS query does not pass through the device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Umbrella portal.

- When the Umbrella Integration policy blocks a DNS query, the client is redirected to a Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Umbrella portal.

- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Umbrella cloud for further inspection.

- Only the IPv4 address of the host is conveyed in the EDNS option.

- A maximum of 64 local domains can be configured under bypass list, and the allowed domain name length is 100 characters.

**Prerequisites for Umbrella Integration**

Before you configure the Umbrella Integration feature, ensure that the following are met:

- The device has a security K9 license to enable Umbrella Integration.

- The device runs on the SD-WAN IOS XE 16.10 software image or later.

- SD-WAN Umbrella subscription license is available.

- The device is set as the default DNS server gateway and needs to ensure that the DNS traffic goes through the device.

**Cloud-based Security Service Using Umbrella Integration**

The SD-WAN Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through the device. When a host initiates the traffic and sends a DNS query, the Umbrella Connector in the device intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Umbrella Cloud applies different policies to the DNS query.

The Umbrella Integration cloud, based on the policies configured on the portal and the reputation of the DNS Fully Qualified Domain Name (FQDN) may take one of the following actions:

- If FQDN is found to be malicious or blocked by the customized Enterprise Security policy, then the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response. This is called a blacked list action at Umbrella Cloud.

- If FQDN is found to be non-malicious, then the IP address of the content provider is returned in the DNS response. This is called a whitelist action at Umbrella Cloud.

- If the FQDN is suspicious, then the intelligent proxy unicast IP addresses are returned in the DNS response. This is referred to as grey list action at Umbrella Cloud.
When the DNS response is received, the device forwards the response back to the host. The host will extract the IP address from the response and send the HTTP/HTTPS requests to this IP.

Note: The intelligent proxy option has to be enabled in the Umbrella dashboard for the Umbrella Resolver to return the intelligent proxy unicast IP addresses in the DNS response when an attempt is made to access the domains in the grey list.

Handling HTTP and HTTPS Traffic

With SD-WAN Umbrella Integration, HTTP and HTTPS client requests are handled in the following ways:

- If the Fully Qualified Domain Name (FQDN) in the DNS query is malicious (falls under blacklisted domains), Umbrella Cloud returns the IP address of the blocked landing page in the DNS response. When the HTTP client sends a request to this IP, Umbrella Cloud displays a page that informs the user that the requested page was blocked and the reason for blocking the page.

- If the FQDN in the DNS query is non-malicious (falls under whitelisted domains), Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the desired content.

- If the FQDN in the DNS query falls under grey-listed domains, Umbrella Resolver returns the unicast IP addresses of intelligent proxy in the DNS response. All HTTP traffic from the host to the grey domain gets proxied through the intelligent proxy and undergo URL filtering.

One potential limitation in using intelligent proxy unicast IP addresses is the probability of the datacenter going down when the client is trying to send the traffic to the intelligent proxy unicast IP address. This is a scenario where a client has completed DNS resolution for a domain which falls under grey-listed domain and client’s HTTP/(S) traffic is being sent to one of the obtained intelligent proxy unicast IP address. If that datacenter is down, then the client has no way of knowing it.

The Umbrella Connector does not act on the HTTP and HTTPS traffic. The connector does not redirect any web traffic or alter any HTTP/(S) packets.

Encrypting the DNS Packet
The DNS packet sent from the device to Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, device decrypts the packet and forwards it to the host. You can encrypt DNS packets only when the DNScrypt feature is enabled on the device.

The device uses the following Anycast recursive Umbrella Integration servers:

• 208.67.222.222
• 208.67.220.220
• 2620:119:53::53
• 2620:119:35::35

Figure 3: Umbrella Integration Topology

Benefits of Umbrella Integration

The Umbrella Integration provides security and policy enforcement at DNS level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). This helps the administrator to bypass the Umbrella Integration.

Configure the Umbrella Connector

Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a DigiCert root certificate which is auto installed on the router by default.

To configure Umbrella Connector:

• Get the API token from the Umbrella portal.
• Define VRFs and each VRF can has two options: DNS resolver and enabling local domain list.
  • Umbrella registration is done per VRF only if DNS resolver is configured as Umbrella.
  • Local domain bypass list is global and each VRF can enable or disable the local domain bypass list. If enabled, the DNS packet will be matched against the local domain list.
• Umbrella is a Direct Internet Access (DIA) feature, so NAT configuration is mandatory.

Sample configuration:

Device# config-transaction
Device(config)# parameter-map type umbrella global
Device(config-profile)#?
parameter-map commands:
  dnscrypt Enable DNSCrypt
  exit Exit from parameter-map
  local-domain Local domain processing
  no Negative or set default values of a command
  public-key DNSCrypt provider public key
  registration-vrf Cloud facing vrf
  resolver Anycast address
  token Config umbrella token
  udp-timeout Config timeout value for UDP sessions
  vrf Configure VRF

Per-VRF options are provided under VRF option:
Device(config)# parameter-map type umbrella global
Device(config-profile)#vrf 9
Device(config-profile-vrf)#?
vrf options:
  dns-resolver DNS resolver address
  exit Exit from vrf sub mode
  match-local-domain Match local-domain list(if configured)
  no Negate a command or set its defaults

parameter-map type regex dns_bypass
pattern www.cisco.com
pattern www.amazon.com
pattern .*

parameter-map type umbrella global
token 648BF6199C379DCCFFBA637FD1E22755001CE241
local-domain dns_bypass
dnscrypt
udp-timeout 5
vrf 9
dns-resolver 8.8.8.8
match-local-domain
vrf 19
dns-resolver 8.8.8.8
no match-local-domain
vrf 29
dns-resolver umbrella
match-local-domain
vrf 39
dns-resolver umbrella
no match-local-domain
!

The following table captures the per VRF DNS packet behavior:

<table>
<thead>
<tr>
<th>VRF</th>
<th>dns-resolver</th>
<th>Match-local-domain (dns_bypass)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>8.8.8.8</td>
<td>Yes</td>
</tr>
<tr>
<td>19</td>
<td>8.8.8.8</td>
<td>No</td>
</tr>
<tr>
<td>29</td>
<td>umbrella</td>
<td>Yes</td>
</tr>
<tr>
<td>39</td>
<td>umbrella</td>
<td>No</td>
</tr>
</tbody>
</table>
Note: The VRFs must be preconfigured. For example, the VRFs 9,19, 29, 39 are preconfigured in the above example.

Sample NAT config for DIA internet connectivity:

```
ip access-list extended dia-nat-acl
10 permit ip any any
ip nat inside source list dia-nat-acl interface <WAN-facing-Interface> overload
```

“ip nat outside” MUST be configured under <WAN-facing-Interface>

Configuring the Device as a Pass-through Server

You can identify the traffic to be bypassed using domain names. In the SD-WAN device, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the device matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# config-transaction
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.cisco.com
Device(config)# pattern www.amazon.com
Device(config)# pattern .*sales.abc.*
```

DNSCrypt, Resolver, and Public-key

When you configure the device using the `parameter-map type umbrella global` command, the following values are auto-populated:

- DNSCrypt
- Public-Key

Public-key

Public-key is used to download the DNSCrypt certificate from Umbrella Integration cloud. This value is preconfigured to

```
```

which is the public-key of Umbrella Integration Anycast servers. If there is a change in the public-key and if you modify this command, then you have to remove the modified command to restore the default value. If you modify the value, the DNSCrypt certificate download may fail.

DNSCrypt

DNSCrypt is an encryption protocol to authenticate communications between the device and the Umbrella Integration. When the `parameter-map type umbrella` is configured and enabled by default on all WAN interfaces. DNSCrypt gets triggered and a certificate is downloaded, validated, and parsed. A shared secret key is then negotiated, which is used to encrypt the DNS queries. For every hour this certificate is automatically downloaded and verified for an upgrade, a new shared secret key is negotiated to encrypt the DNS queries.

To disable DNSCrypt, use the `no dnscrypt` command and to re-enable DNSCrypt, use the `dnscrypt` command.

When the DNSCrypt is used, the DNS request packets size is more than 512 bytes. Ensure that these packets are allowed through the intermediary devices; otherwise, the response may not reach the intended recipients.

Sample umbrella dnscrypt notifications:

```
Device# show sdwan umbrella dnscrypt
  DNSCrypt: Enabled
```
Certificate Update Status:
  Last Successful Attempt: 08:46:32 IST May 21 2018
Certificate Details:
  Certificate Magic : DNSC
  Major Version : 0x0001
  Minor Version : 0x0000
  Query Magic : 0x714E7A696D657555
  Serial Number : 1517943461
  Start Time : 1517943461 (00:27:41 IST Feb 7 2018)
  End Time : 1549479461 (00:27:41 IST Feb 7 2019)
Server Public Key :
Client Secret Key Hash:
Client Public key :
  NM key Hash :
When disabled:
Device# show umbrella dnsencrypt
DNCrypt: Not enabled
Public-key: NONE

Sample configuration steps for dns-resolver and match-local-domain-to-bypass per vrf:
Router(config)# vrf definition 1
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commit
Commit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# ?
Possible completions:
  dnsencrypt
dns-resolver
  local-domain
  public-key
  registration-vrf
  resolver
token
  udp-timeout
vrf
Router(config-profile)# vrf 1
This line doesn't have a valid range expression
Possible completions:
  <name:string, min: 1 chars, max: 32 chars> 1
Router(config-profile)# vrf 1
Router(config-profile-vrf)# ?
Possible completions:
  dns-resolver
  match-local-domain-to-bypass
Router(config-profile-vrf)# dns-resolver umbrella
Router(config-profile-vrf)# match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router(config)# vrf definition 2
Router(config-vrf)# address-family ipv4
Router(config-ipv4)# exit-address-family
Router(config-vrf)# commit
Commit complete.
Router(config-vrf)# exit
Router(config)# parameter-map type umbrella global
Router(config-profile)# vrf 2
Router(config-profile-vrf)# dns-resolver 8.8.8.8
Router(config-profile-vrf)# no match-local-domain-to-bypass
Router(config-profile-vrf)# commit
Commit complete.
Router(config-profile-vrf)# end
Router#sh umbrella config

Umbrella Configuration
------------------------
Token: AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
OrganizationID: 1882034
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled

UDP Timeout: 5 seconds
Resolver address:
  1. 208.67.220.220
  2. 208.67.222.222
  3. 2620:119:53::53
  4. 2620:119:35::35
Registration VRF: default
VRF List:
1. VRF 1 (ID: 1)
   DNS-Resolver: umbrella
   Match local-domain-to-bypass: Yes
2. VRF 2 (ID: 3)
   DNS-Resolver: 8.8.8.8
   Match local-domain-to-bypass: No

Verifying the Umbrella Connector Configuration

Verify the Umbrella Connector configuration using the following commands:

Device# show umbrella config
Umbrella Configuration
------------------------
Token: 648BF6139C379DCCFFBA637FD1E22755001CE241
OrganizationID: 1892929
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt: Enabled

UDP Timeout: 5 seconds
Resolver address:
  1. 208.67.220.220
  2. 208.67.222.222
  3. 2620:119:53::53
  4. 2620:119:35::35
Registration VRF: default
VRF List:
1. VRF 9 (ID: 4)
   DNS-Resolver: 8.8.8.8
   Match local-domain: Yes
2. VRF 19 (ID: 1)
   DNS-Resolver: 8.8.8.8
   Match local-domain: No
3. VRF 29 (ID: 2)
   DNS-Resolver: umbrella
   Match local-domain: Yes
4. VRF 39 (ID: 3)
   DNS-Resolver: umbrella
   Match local-domain: No
The output of VRF will have name and ID. The ID here is VRF ID:
Device# show vrf detail | inc VRF Id
VRF 19 (VRF Id = 1); default RD <not set>; default VPNID <not set>
VRF 29 (VRF Id = 2); default RD <not set>; default VPNID <not set>
VRF 39 (VRF Id = 3); default RD <not set>; default VPNID <not set>
VRF 9 (VRF Id = 4); default RD <not set>; default VPNID <not set>

When DNSCrypt is disabled:
Device# show umbrella config
Umbrella Configuration

 Token: 648BF6139C379DCCFFBA637FD1E2275501CE241
 OrganizationID: 1892929
 Local Domain Regex parameter-map name: dns_bypass
 DNSCrypt: Not enabled
 Public-key: NONE
 UDP Timeout: 5 seconds
 Resolver address:
 1. 208.67.220.220
 2. 208.67.222.222
 3. 2620:119:53::53
 4. 2620:119:35::35
 Registration VRF: default
 VRF List:
 1. VRF 9 (ID: 4)
    DNS-Resolver: 8.8.8.8
    Match local-domain: Yes
 2. VRF 19 (ID: 1)
    DNS-Resolver: 8.8.8.8
    Match local-domain: No
 3. VRF 29 (ID: 2)
    DNS-Resolver: umbrella
    Match local-domain: Yes
 4. VRF 39 (ID: 3)
    DNS-Resolver: umbrella
    Match local-domain: No

Displaying Umbrella Registration Details

The following example displays the device registration information:

Device# show sdwan umbrella device-registration
Device registration details
VRF Tag Status Device-id
vpn29 200 SUCCESS 010a9b2b0d5cb21f
vpn39 200 SUCCESS 010a1a2e199989da19

The following example displays the device registration information in detail:
Device# show umbrella deviceid detailed
Device registration details
1.29
 Tag : vpn29
 Device-id : 010a9b2b0d5cb21f
 Description : Device Id recieved successfully
 WAN interface : None

2.39
 Tag : vpn39
 Device-id : 010a1a2e199989da19
 Description : Device Id recieved successfully
 WAN interface : None

Show Commands
Umbrella show commands at FP Layer

The `show platform software umbrella f0 config` command displays all the local domains configured for Open DNS in the FP Layer.

```
Device# show platform software umbrella f0 config
+++ Umbrella Config +++
Umbrella feature:
------------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
------------------
udp timeout: 5
OrgId :
------------------
orgid : 1892929
Resolver config:
RESOLVER IP's
------------------
208.67.220.220
208.67.222.222
2620:119:35::35
2620:119:53::53
Dnscrypt Info:
public key:
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
ProfileID DeviceID Mode Resolver Local-Domain Tag
------------------------------------------------------------------------------
 0 OUT False
 4 IN 8.8.8.8 True vpn9
 1 IN 8.8.8.8 False vpn19
 2 010a9b2b0d5cb21f IN 208.67.220.220 True vpn29
 3 010a1a2e1989da19 IN 208.67.220.220 False vpn39
```

The `show platform software umbrella f0 local-domain` displays the local domain list.

```
Device# show platform software umbrella f0 local-domain
01. www.cisco.com
02. www.amazon.com
03. .*sales.abc.*
```

Umbrella show commands at CPP Layer

The `show platform hardware qfp active feature umbrella client config` command displays the configuration in CPP layer.

```
+++ Umbrella Config +++
Umbrella feature:
------------------
Init: Enabled
Dnscrypt: Enabled
Timeout:
-------
udp timeout: 5
OrgId :
-------
orgid: 1892929
Resolver config:
------------------
RESOLVER IP's
------------------
208.67.220.220
```

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
208.67.222.222
2620:119:53::53
2620:119:35::35

Dnscrypt Info:
-----------------
public_key:
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461

Umbrella Interface Config:
--------------------------
11 GigabitEthernet4 :
    Mode : IN
    DeviceID : 010a9b2b0d5cb21f
    Tag : vpn29
10 GigabitEthernet3 :
    Mode : IN
    DeviceID : 0000000000000000
    Tag : vpn9
05 Null0 :
    Mode : OUT
06 VirtualPortGroup0 :
    Mode : OUT
07 VirtualPortGroup1 :
    Mode : OUT
08 GigabitEthernet1 :
    Mode : OUT
09 GigabitEthernet2 :
    Mode : OUT
12 GigabitEthernet5 :
    Mode : OUT

Umbrella Profile Deviceid Config:
---------------------------------
ProfileID: 0
    Mode : OUT
ProfileID: 1
    Mode : IN
    Resolver : 8.8.8.8
    Local-Domain: False
    DeviceID : 0000000000000000
    Tag : vpn19
ProfileID: 3
    Mode : IN
    Resolver : 208.67.220.220
    Local-Domain: False
    DeviceID : 010a1a2e1989da19
    Tag : vpn39
ProfileID: 4
    Mode : IN
    Resolver : 8.8.8.8
    Local-Domain: True
    DeviceID : 0000000000000000
    Tag : vpn9
ProfileID: 2
    Mode : IN
    Resolver : 208.67.220.220
    Local-Domain: True
    DeviceID : 010a9b2b0d5cb21f
    Tag : vpn29

Umbrella Profile ID CPP Hash:
-----------------------------
Umbrella Data-Plane show commands

The `show platform hardware qfp active feature umbrella datapath stats` command displays the umbrella statistics in data plane.

Device# show platform hardware qfp active feature umbrella datapath stats

Umbrella Connector Stats:

Parser statistics:
- parser unknown pkt: 0
- parser fmt error: 0
- parser count nonzero: 0
- parser pa error: 0
- parser non query: 0
- parser multiple name: 0
- parser dns name err: 0
- parser matched ip: 0
- parser opensdns redirect: 0
- local domain bypass: 0
- parser dns others: 0
- no device id on interface: 0
- drop erc dnscrypt: 0
- regex locked: 0
- regex not matched: 0
- parser malformed pkt: 0

Flow statistics:
- feature object allocs : 0
- feature object frees : 0
- flow create requests : 0
- flow create successful: 0
- flow create failed, CFT handle: 0
- flow create failed, getting FO: 0
- flow create failed, malloc FO : 0
- flow create failed, attach FO : 0
- flow create failed, match flow: 0
- flow create failed, set aging : 0
- flow lookup requests : 0
- flow lookup successful: 0
- flow lookup failed, CFT handle: 0
- flow lookup failed, getting FO: 0
- flow lookup failed, no match : 0
- flow detach requests : 0
- flow detach successful: 0
- flow detach failed, CFT handle: 0
- flow detach failed, getting FO: 0
- flow detach failed freeing FO : 0
- flow detach failed, no match : 0
The `show platform hardware qfp active feature umbrella datapath memory` command displays CFT information.

Device# show platform hardware qfp active feature umbrella datapath memory

---Umbrella Connector CFT Information---
CFT inst_id 0 feat id 0 fo id 0 chunk id 4

---Umbrella Connector Runtime Information---
umbrella init state 0x4
umbrella dsa client handler 0x2

The `show platform hardware qfp active feature umbrella datapath runtime` command displays internal information. For example, key index used for DNSCrypt.

Device# show platform hardware qfp active feature umbrella datapath runtime

udpflow_ageout: 5
ipv4_count: 2
ipv6_count: 2
ipv4_index: 0
ipv6_index: 0

Umbrella IPv4 Anycast Address
IP Anycast Address0: 208.67.220.220
IP Anycast Address1: 208.67.222.222

Umbrella IPv6 Anycast Address
IP Anycast Address0: 2620:119:53:0:0:0:0:53
IP Anycast Address1: 2620:119:35:0:0:0:0:35

=DNSCrypt=
key index: 0
-key[0]-
  sn: 1517943461
  ref cnt: 0
  magic: 71e4e7a696d647555
  Client Public Key:
-key[1]-
  sn: 0
Clear Command

The clear platform hardware qfp active feature umbrella datapath stats command clears the Umbrella connector statistics in datapath.

Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared

Troubleshooting Umbrella Integration

Troubleshoot issues that are related to enabling Umbrella Integration feature using these commands:

- debug umbrella device-registration
- debug umbrella config
- debug umbrella dnscrypt

Depending on the OS, run either of these two commands from the client device:

- The nslookup -type=txt debug.umbrella.com command from the command prompt of the Windows machine
- The nslookup -type=txt debug.umbrella.com command from the terminal window or shell of the Linux machine

nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
debug.opendns.com text = "server r6.mum1"
ddebug.opendns.com text = "device 010A826AAABB6C3D"
ddebug.opendns.com text = "organization id 1892929"
ddebug.opendns.com text = "remoteip 171.168.1.7"
ddebug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
ddebug.opendns.com text = "originid 119211936"
ddebug.opendns.com text = "orgid 1892929"
ddebug.opendns.com text = "orgflags 3"
ddebug.opendns.com text = "actype 0"
ddebug.opendns.com text = "bundle 365396"
ddebug.opendns.com text = "source 72.163.220.18:36914"
ddebug.opendns.com text = "dnscrypt enabled (71315677457306E)"

Close message

Learn more

Welcome to your new guide!

Click on "New" to build out your guide.

Tags recommended by the template: article:topic
Configuring Centralized Control Policy

Centralized control policy, which you configure on vSmart controllers, affects routing policy based on information in OMP routes and OMP TLOCs. This type of policy allows you to set actions for matching routes and TLOCs, including redirecting packets through network services, such as firewalls, a feature that is called service chaining.

In domains with multiple vSmart controllers, all the controllers must have the same centralized control policy configuration to ensure that routing within the overlay network remains stable and predictable.

This article provides procedures for configuring centralized control policy (including service chaining) from the CLI.

**Configuration Components**

A centralized control policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a route or TLOC matches the match conditions, the associated action or actions are taken and policy evaluation on that packets stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a route or TLOC matches no parameters in any of the sequences in the policy configure, it is, by default, rejected and discarded.

The following figure illustrates the configuration components for centralized control policy.

![Configuration Components Diagram](image)

To create a centralized control policy, you include the following components in the configuration on a vSmart controller:
Table 228: Configuring Centralized Control Policy

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the control policy configuration.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest  or  Configuration ► Policies ► Custom Options ► Centralized Policy ► Lists</td>
<td>policy lists</td>
</tr>
<tr>
<td>Centralized control policy instance</td>
<td>Container for centralized control policy.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy</td>
<td>policy control-policy</td>
</tr>
<tr>
<td>Network topology</td>
<td>Conditions that define the network topology</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest  or  Configuration ► Policies ► Custom Options ► Centralized Policy ► Lists</td>
<td>-</td>
</tr>
<tr>
<td>Numbered sequences of match-action pairs</td>
<td>Sequences that establish the order in which policy components are applied.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type  or  Configuration ► Policies ► Custom Options ► Centralized Policy ► Add Topology ► Custom Control ► Sequence Type</td>
<td>policy control-policy sequence</td>
</tr>
</tbody>
</table>

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match parameters</td>
<td>Conditions that the routes and TLOCs must match to be considered for a control policy.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule or Configuration ► Policies ► Custom Options ► Centralized Policy ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule</td>
<td>policy control-policy sequence match route—Match OMP route properties, including things such as the originating protocol and IP prefixes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
<td>policy control-policy sequence match tloc—Match transport location parameters, including things such as the domain ID and TLOC IP address.</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching routes and TLOCs, and how to process matching items.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule or Configuration ► Policies ► Custom Options ► Centralized Policy ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule</td>
<td>policy control-policy sequence action</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a route or TLOC matches none of the match parameters in any of the sequences. By default, nonmatching routes and TLOCs are rejected.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type ► Default Action or Configuration ► Policies ► Custom Options ► Centralized Policy ► Add Topology ► Custom Control ► Sequence Type ► Default Action</td>
<td>policy control-policy default-action</td>
</tr>
<tr>
<td>Application of centralized control policy</td>
<td>For a control policy to take effect, you apply it to one or more sites in the overlay network.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Apply Policies to Sites and VPNs</td>
<td>apply-policy site-list control-policy</td>
</tr>
</tbody>
</table>
**General vManage Configuration Procedure**

To configure centralized policies, use the vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- **Create Groups of Interest**—Create lists that group together related items and that you call in the match or action components of a policy.
- **Configure Topology**—Create the network structure to which the policy applies.
- **Configure Traffic Rules**—Create the match and action conditions of a policy.
- **Apply Policies to Sites and VPNs**—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For a centralized policy to take effect, you must activate the policy.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the **Configure > Policies** screen.
2. Select the **Centralized Policy** tab.
3. Click **Add Policy**.

The policy configuration wizard appears, and the **Create Applications or Groups of Interest** screen is displayed.

**Step 2: Configure Groups of Interest**

In **Create Groups of Interest**, create lists of groups to use in centralized policy:
1. Create new lists, as described in the following table:

**Table 229:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Color     | 1. In the left bar, click Color.  
           | 2. Click New Color List.  
           | 3. Enter a name for the list.  
           | 4. From the Select Color drop-down, select the desired colors.  
           | 5. Click Add. |
| Prefix    | 1. In the left bar, click Prefix.  
           | 2. Click New Prefix List.  
           | 3. Enter a name for the list.  
           | 4. In the Add Prefix field, enter one or more data prefixes separated by commas.  
           | 5. Click Add. |
**List Type** | **Procedure**
--- | ---
Site | 1. In the left bar, click Site.
2. Click New Site List.
3. Enter a name for the list.
4. In the Add Site field, enter one or more site IDs separated by commas.
5. Click Add.

TLOC | 1. In the left bar, click TLOC.
2. Click New TLOC List. The TLOC List popup displays.
3. Enter a name for the list.
4. In the TLOC IP field, enter the system IP address for the TLOC.
5. In the Color field, select the TLOC's color.
6. In the Encap field, select the encapsulation type.
7. In the Preference field, optionally select a preference to associate with the TLOC.
8. Click Add TLOC to add another TLOC to the list.
9. Click Save.

VPN | 1. In the left bar, click VPN.
2. Click New VPN List.
3. Enter a name for the list.
4. In the Add VPN field, enter one or more VPN IDs separated by commas.
5. Click Add.

2. Click Next to move to **Configure Topology and VPN Membership** in the wizard.

**Step 3: Configure Topology and VPN Membership**

When you first open the **Configure Topology and VPN Membership** screen, the **Topology** tab is selected by default:

To configure topology and VPN membership:

1. In the **Topology** tab, create a network topology, as described in the following table:
<table>
<thead>
<tr>
<th>Topology Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Custom Control (Route & TLOC) | Centralized route control policy (for matching OMP routes) | 1. In the Add Topology drop-down, select Custom Control (Route & TLOC).  
2. Enter a name for the control policy.  
3. Enter a description for the policy.  
4. In the left pane, click Add Sequence Type. The Add Control Policy popup displays.  
5. Select Route. A policy component containing the text string Route is added in the left pane.  
6. Double-click the Route text string, and enter a name for the policy component.  
7. In the right pane, click Add Sequence Rule. The Match/Actions box opens, and Match is selected by default.  
8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired. For an explanation of the match conditions, see the OMP Route Match Attributes section in the Configuring Centralized Control Policy article for your software release.  
9. Click Actions. The Reject radio button is selected by default. To configure actions to perform on accepted packets, click the Accept radio button. Then select the action or enter a value for the action. For an explanation of the actions, see the Action Parameters section in the Configuring Centralized Control Policy article for your software release.  
10. Click Save Match and Actions.  
11. Click Add Sequence Rules to configure more sequence rules, as desired. Drag and drop to re-order them.  
12. Click Add Sequence Type to configure more sequences, as desired. Drag and drop to re-order them.  
13. Click Save Control Policy. |
<table>
<thead>
<tr>
<th>Topology Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized TLOC control policy (for matching TLOC routes)</td>
<td>1. In the Add Topology drop-down, select Custom Control (Route &amp; TLOC).&lt;br&gt;2. Enter a name for the control policy.&lt;br&gt;3. Enter a description for the policy.&lt;br&gt;4. In the left pane, click Add Sequence Type. The Add Control Policy popup displays.&lt;br&gt;5. Select TLOC. A policy component containing the text string TLOC is added in the left pane.&lt;br&gt;6. Double-click the TLOC text string, and enter a name for the policy component.&lt;br&gt;7. In the right pane, click Add Sequence Rule. The Match/Actions box opens, and Match is selected by default.&lt;br&gt;8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired. For an explanation of the match conditions, see the OMP TLOC Match Attributes section in the Configuring Centralized Control Policy article for your software release.&lt;br&gt;9. Click Actions. The Reject radio button is selected by default. To configure actions to perform on accepted packets, click the Accept radio button. Then select the action or enter a value for the action. For an explanation of the actions, see the Action Parameters section in the Configuring Centralized Control Policy article for your software release.&lt;br&gt;10. Click Save Match and Actions.&lt;br&gt;11. Click Add Sequence Rules to configure more sequence rules, as desired. Drag and drop to re-order them.&lt;br&gt;12. Click Add Sequence Type to configure more sequences, as desired. Drag and drop to re-order them.&lt;br&gt;13. Click Save Control Policy.</td>
<td>1. To use an existing topology:&lt;br&gt;   1. In the Add Topology drop-down, click Import Existing Topology. The Import Existing Topology popup appears.&lt;br&gt;   2. Select the type of topology.&lt;br&gt;   3. In the Policy drop-down, choose the name of the topology.&lt;br&gt;   4. Click Import.&lt;br&gt; 2. Click Next to move to Configure Traffic Rules in the wizard.&lt;br&gt; 3. Click Next to move to Apply Policies to Sites and VPNs in the wizard.</td>
</tr>
</tbody>
</table>
Step 4: Apply Policies to Sites and VPNs

In Apply Policies to Sites and VPNs screen, apply a policy to a sites and VPNs:

1. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

3. From the Topology bar, choose the type of policy block. The table then lists policies that you have created for that type of policy block.

4. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:
   1. For a Topology policy block, click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Choose one or more site lists, and choose one or more VPN lists. Click Add.

   2. For an Application-Aware Routing policy block, click Add New Site List and VPN list. Choose one or more site lists, and choose one or more VPN lists. Click Add.

   3. For a Traffic Data policy block, click Add New Site List and VPN List. Choose the direction for applying the policy (From Tunnel, From Service, or All), choose one or more site lists, and choose one or more VPN lists. Click Add.

   4. For a cflowd policy block, click Add New Site List. Choose one or more site lists, Click Add.

5. Click Preview to view the configured policy. The policy appears in CLI format.

6. Click Save Policy. The Configuration > Policies screen appears, and the policies table includes the newly created policy.

Step 5: Activate a Centralized Policy

Activating a centralized policy sends that policy to all connected vSmart controllers. To activate a centralized policy:

1. In vManage NMS, select the Configure > Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Choose a policy.

3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup appears. It lists the IP addresses of the reachable vSmart controllers to which the policy must be applied.

4. Click Activate.

General CLI Configuration Procedure

To configure a centralized control policy using the CLI:

1. Create a list of overlay network sites to which the centralized control policy is to be applied (in the apply-policy command):
The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes, TLOCs, and VPNs, as needed:

```
vSmart(config)# policy lists
   vSmart(config-lists)# prefix-list
      list-name   vSmart(config-lists-list-name)# ip-prefix
         prefix/length
vSmart(config-lists)# tloc-list
      list-name   vSmart(config-lists-list-name)# tloc
         address
         color
         color
         encapsulation
            [preference
               value]
vSmart(config-lists)# vpn-list
      list-name   vSmart(config-lists-list-name)# vpn
         vpn-id
```

1. Create a control policy instance:

```
vSmart(config)# policy control-policy
   policy-name
vSmart(config-control-policy-policy-name)#
```

2. Create a series of match–action pair sequences:

```
vSmart(config-control-policy-policy-name)# sequence
   number
vSmart(config-sequence-number)#
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

3. Define match parameters for routes and for TLOCs:

```
vSmart(config-sequence-number)# match route
   route-parameter
vSmart(config-sequence-number)# match tloc
   tloc-parameter
```

4. Define actions to take when a match occurs:

```
vSmart(config-sequence-number)# action reject
vSmart(config-sequence-number)# action accept export-to
   vpn
      vpn-id  |  vpn-list
         list-name
vSmart(config-sequence-number)# action accept set
   omp-tag
      number
vSmart(config-sequence-number)# action accept set
   preference
      value
vSmart(config-sequence-number)# action accept set
   service
      service-name  (tloc
         ip-address  |  tloc-list
```

Cisco SD-WAN vManage Help, Cisco IOS XE Gibraltar 16.11.x, Cisco SD-WAN Release 19.1
list-name) [vpn
vpn-id]
vSmart(config-sequence-number)# action accept set tloc
ip-address
color
color [encap
encapsulation] vSmart(config-sequence-number)# action accept set tloc-action
action
vSmart(config-sequence-number)# action accept set tloc-list
list-name

5. Create additional numbered sequences of match–action pairs within the control policy, as needed.

6. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching routes to be accepted, configure the default action for the policy:

vSmart(config-policy-name)# default-action accept

7. Apply the policy to one or more sites in the Viptela overlay network:

vSmart(config)# apply-policy site-list
list-name
control-policy
policy-name (in | out)

8. If the action you are configuring is a service, configure the required services on the vEdge routers so that the vSmart controller knows how to reach the services:

vEdge(config)# vpn
vpn-id service service-name
address
ip-address

Specify the VPN is which the service is located and one to four IP addresses to reach the service device or devices. If multiple devices provide the same service, the vEdge router load-balances the traffic among them. Note that the vEdge router keeps track of the services, advertising them to the vSmart controller only if the address (or one of the addresses) can be resolved locally, that is, at the vEdge router's local site, and not learned through OMP. If a previously advertised service becomes unavailable, the vEdge router withdraws the service advertisement.

**Structural Components of Policy Configuration for Centralized Control Policy**

Following are the structural components required to configure centralized control policy. Each one is explained in more detail in the sections below.

policy lists color-list list-name color color prefix-list list-name
ip-prefix prefix site-list list-name site-id site-id tloc-list list-name
tloc address color color encap encapsulation [preference value] vpn-list list-name
vpn vpn-id
control-policy
policy-name number
sequence
match
match-parameters
action reject accept export-to vpn accept set parameter
default-action (accept | reject)apply-policy site-list list-name control-policy
policy-name (in | out)
Lists

Centralized control policy uses the following types of lists to group related items. In the CLI, you configure lists under the **policy lists** command hierarchy on vSmart controllers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colors</td>
<td>List of one or more TLOC colors. <em>color</em> can be 3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. To configure multiple colors in a single list, include multiple <em>color</em> options, specifying one color in each option.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest ► Color Options ► Centralized Policy ► Lists ► Color</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>color-list</strong> <code>list-name</code> <code>color</code> <code>color</code></td>
</tr>
<tr>
<td>Prefixes</td>
<td>List of one or more IP prefixes. Specify the IP prefixes as follows: • <em>prefix/length</em>—Exactly match a single prefix–length pair. • <code>0.0.0.0/0</code>—Match any prefix–length pair. • <code>0.0.0.0/0 le length</code>—Match any IP prefix whose length is less than or equal to <em>length</em>. For example, <code>ip-prefix 0.0.0.0/0 le 16</code> matches all IP prefixes with lengths from <code>/1</code> through <code>/16</code>. • <code>0.0.0.0/0 ge length</code>—Match any IP prefix whose length is greater than or equal to <em>length</em>. For example, <code>ip-prefix 0.0.0.0 ge 25</code> matches all IP prefixes with lengths from <code>/25</code> through <code>/32</code>. • <code>0.0.0.0/0 le length1 le length2</code>, or <code>0.0.0.0/0 le length2 ge length1</code>—Match any IP prefix whose length is greater than or equal to <em>length1</em> and less than or equal to <em>length2</em>. For example, <code>ip-prefix 0.0.0.0/0 ge 20 le 24</code> matches all <code>/20</code>, <code>/21</code>, <code>/22</code>, <code>/23</code>, and <code>/24</code> prefixes. Also, <code>ip-prefix 0.0.0.0/0 ge 20 ge 24</code> matches the same prefixes. If <em>length1</em> and <em>length2</em> are the same, a single IP prefix length is matched. For example, <code>ip-prefix 0.0.0.0/0 ge 24 le 24</code> matches only <code>/24</code> prefixes. To configure multiple prefixes in a single list, include multiple <em>ip-prefix</em> options, specifying one prefix in each option.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest ► Prefix Options ► Centralized Policy ► Lists ► Prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>prefix-list</strong> <code>list-name</code> <code>ip-prefix prefix/length</code></td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as <em>site-id 1</em>) or a range of site identifiers (such as <em>site-id 1-10</em>). To configure multiple sites in a single list, include multiple <em>site-id</em> options, specifying one site number in each option.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest ► Site Options ► Centralized Policy ► Lists ► Site</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>site-list</strong> <code>list-name</code> <code>site-id site-id</code></td>
</tr>
</tbody>
</table>
### List Type

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLOCs</td>
<td>List of one or more TLOCs in the overlay network. For each TLOC, specify its address, color, and encapsulation. address is the system IP address. color can be one of 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. encapsulation can be gre or ipsec. Optionally, set a preference value (from 0 to (2^{32} - 1)) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest ► TLOC v LOC-list list-name  tloc ip-address  color color  encaps (gre  ipsec) [preference number]</td>
</tr>
<tr>
<td>VPNS</td>
<td>List of one or more VPNS in the overlay network. For data policy, you can configure any VPNS except for VPN 0 and VPN 512. To configure multiple VPNS in a single list, include multiple vpn options, specifying one VPN number in each option. You can specify a single VPN identifier (such as vpn 1) or a range of VPN identifiers (such as vpn 1-10).</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Create Groups of Interest ► VPN v PN-list list-name  vpn vpn-id</td>
</tr>
</tbody>
</table>

### Sequences

A centralized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route or TLOC is analyzed by the match–action pairs in the policy.

In vManage NMS, you configure sequences from:

- Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Traffic Rules ► (Application-Aware Routing | Traffic Data | Cflowd) ► Sequence Type
- Configuration ► Policies ► Custom Options ► Centralized Policy ► Traffic Policy ► (Application-Aware Routing | Traffic Data | Cflowd) ► Sequence Type

In the CLI, you configure sequences with the `policy control-policy sequence` command.

Each sequence in a centralized control policy can contain one match condition (either for a route or for a TLOC) and one action condition.

### Match Parameters

Centralized control policy can match OMP route or TLOC route attributes.

In vManage NMS, you configure match parameters from:

- Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control (Route & TLOC) ► Sequence Type ► (Route | TLOC) ► Sequence Rule ► Match
In the CLI, you configure the OMP route attributes to match with the `policy control-policy sequence match route` command, and you configure the TLOC attributes to match with the `policy control-policy sequence match tloc` command.

Each sequence in a policy can contain one `match` section—either `match route` or `match tloc`.

**OMP Route Match Attributes**

For OMP routes (vRoutes), you can match these attributes:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual color.</td>
<td>Not available in vManage NMS color color</td>
<td>3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lite, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver</td>
</tr>
<tr>
<td>One or more colors.</td>
<td>Match Color List color-list list-name</td>
<td>Name of a color or a policy lists color-list list.</td>
</tr>
<tr>
<td>Tag value associated with the route or prefix in the routing database on the vEdge router.</td>
<td>Match OMP Tag omp-tag number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Protocol from which the route was learned.</td>
<td>Match Origin origin protocol</td>
<td>bgp-external, bgp-internal, connected, ospf-external1, ospf-external2, ospf-inter-area, ospf-intra-area, static</td>
</tr>
<tr>
<td>IP address from which the route was learned.</td>
<td>Match Originator originator ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>How preferred a prefix is. This is the preference value that the route or prefix has in the local site, that is, in the routing database on the vEdge router. A higher preference value is more preferred.</td>
<td>Match Preference preference number</td>
<td>0 through 255</td>
</tr>
<tr>
<td>One or more prefixes.</td>
<td>Match Prefix List prefix-list list-name</td>
<td>Name of a prefix list or a policy lists prefix-list list.</td>
</tr>
<tr>
<td>Individual site identifier.</td>
<td>Not available in vManage site-id site-id</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>One or more overlay network site identifiers.</td>
<td>Match Sitesite-list list-name</td>
<td>Name of a site or a policy lists site-list list.</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Individual TLOC address.</td>
<td>Match TLOC</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td><code>tloc ip-address</code></td>
<td></td>
</tr>
<tr>
<td>One or more TLOC addresses.</td>
<td>Match TLOC</td>
<td>Name of a TLOC or a policy lists tloc-list list.</td>
</tr>
<tr>
<td></td>
<td><code>tloc-list list-name</code></td>
<td></td>
</tr>
<tr>
<td>Individual VPN identifier.</td>
<td>Match VPN</td>
<td>0 through 65535</td>
</tr>
<tr>
<td></td>
<td><code>vpn vpn-id</code></td>
<td></td>
</tr>
<tr>
<td>One or more VPN identifiers.</td>
<td>Match VPN</td>
<td>Name of a VPN or a policy lists vpn-list list.</td>
</tr>
<tr>
<td></td>
<td><code>vpn-list list-name</code></td>
<td></td>
</tr>
</tbody>
</table>

### TLOC Route Match Attributes

For TLOC routes, you can match these attributes:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier for the control traffic.</td>
<td>Match Carrier</td>
<td>default, carrier1 through carrier8</td>
</tr>
<tr>
<td></td>
<td><code>carrier carrier-name</code></td>
<td></td>
</tr>
<tr>
<td>Individual color.</td>
<td>Not available in vManage NMS</td>
<td>3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver</td>
</tr>
<tr>
<td></td>
<td><code>color color</code></td>
<td></td>
</tr>
<tr>
<td>One or more colors.</td>
<td>Match Color List</td>
<td>See the colors above.</td>
</tr>
<tr>
<td></td>
<td><code>color-list list-name</code></td>
<td></td>
</tr>
<tr>
<td>Domain identifier associated with a TLOC.</td>
<td>Match Domain ID</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td><code>domain-id domain-id</code></td>
<td></td>
</tr>
<tr>
<td>Tag value associated with the TLOC route in the route table on the vEdge router.</td>
<td>Match OMP Tag</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td><code>omp-tag number</code></td>
<td></td>
</tr>
<tr>
<td>IP address from which the route was learned.</td>
<td>Match Originator</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td><code>originator ip-address</code></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>How preferred a TLOC route is. This is the preference value that the TLOC route has in the local site, that is, in the route table on the vEdge router. A higher preference value is more preferred.</td>
<td>Match Preference preference number</td>
<td>0 through 255</td>
</tr>
<tr>
<td>Individual site identifier.</td>
<td>Match Site site-id</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>One or more overlay network site identifiers.</td>
<td>Match Site site-list list-name</td>
<td>Name of a policy lists site-list list.</td>
</tr>
<tr>
<td>Individual TLOC address.</td>
<td>Match TLOC tloc address</td>
<td>IP address</td>
</tr>
<tr>
<td>One or more TLOC addresses.</td>
<td>Match TLOC tloc-list list-name</td>
<td>Name of a policy lists tloc-list list.</td>
</tr>
</tbody>
</table>

**Action Parameters**

For each match condition, you configure a corresponding action to take if the route or TLOC matches.

In vManage NMS, you configure match parameters from:

- Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control (Route & TLOC) ► Sequence Type ► (Route | TLOC) ► Sequence Rule ► Action
- Configuration ► Policies ► Custom Options ► Centralized Policy ► Topology ► Add Topology ► Custom Control (Route & TLOC) ► Sequence Type ► (Route | TLOC) ► Sequence Rule ► Action

In the CLI, you configure actions with the `policy control-policy action` command.

Each sequence in a centralized control policy can contain one action condition.

In the action, you first specify whether to accept or reject a matching route or TLOC:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept accept</td>
<td>—</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click Reject reject</td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a route or TLOC that is accepted, you can configure the following actions:
<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export the route the the specified VPN or list of VPNs (for a <strong>match route</strong> match condition only).</td>
<td>Click Accept, then action Export To **export-to (vpn vpn-id</td>
<td>vpn-list vpn-list)**</td>
</tr>
<tr>
<td>Change the tag string in the route, prefix, or TLOC.</td>
<td>Click Accept, then action OMP Tag <strong>set omp-tag number</strong></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Change the preference value in the route, prefix, or TLOC to the specified value. A higher preference value is more preferred.</td>
<td>Click Accept, then action Preference <strong>set preference number</strong></td>
<td>0 through 255</td>
</tr>
<tr>
<td>Specify a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the vEdge routers that are collocated with the service devices, using the <strong>vpn service</strong> configuration command.</td>
<td>Click Accept, then action Service **set service service-name (tloc ip-address</td>
<td>tloc-list list-name) [vpn vpn-id]**</td>
</tr>
<tr>
<td>Change the TLOC address, color, and encapsulation to the specified address and color.</td>
<td>Click Accept, then action TLOC <strong>set tloc ip-address color color [encap encapsulation]</strong></td>
<td>IP address, TLOC color, and encapsulation, Color can be one of <strong>3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver</strong>. Encapsulation can be either gre or ipsec.</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Direct matching routes or TLOCs using the mechanism specified by *action*, and enable end-to-end tracking of whether the ultimate destination is reachable. Setting a TLOC action is useful when traffic is first directed, via policy, to an intermediate destination, which then forwards the traffic to its ultimate destination. For example, for traffic from vEdge-A destined for vEdge-D, a policy might direct traffic from vEdge-A first to vEdge-B (the intermediate destination), and vEdge-B then sends it to the final destination, vEdge-D. Setting the TLOC action option enables the vSmart controller to perform end-to-end tracking of the path to the ultimate destination router. In our example, matching traffic goes from vEdge-A to vEdge-B and then, in a single hop, goes to vEdge-D. If the tunnel between vEdge-B and vEdge-D goes down, the vSmart controller relays this information to vEdge-A, and vEdge-A removes its route to vEdge-D from its local route table. End-to-end tracking works here only because traffic goes from vEdge-B to vEdge-D in a single hop, via a single tunnel. If the traffic from vEdge-A went first to vEdge-B, then to vEdge-C, and finally to vEdge-D, the vSmart controller is unable to perform end-to-end tracking and is thus unable to keep vEdge-A informed about whether full path between it and vEdge-D is up. | Click Accept, then action TLOC Action  
*set tloc-action action* | **ecmp**—Equally direct matching control traffic between the intermediate destination and the ultimate destination. In our example, traffic would be sent to vEdge-B (which would then send it to vEdge-D) and directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.  
**primary**—First direct matching traffic to the intermediate destination. If that router is not reachable, then direct it to the final destination. In our example, traffic would first be sent to vEdge-B. If this router is down, it is sent directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the final destination.  
**backup**—First direct matching traffic to the final destination. If that router is not reachable, then direct it to the intermediate destination. In our example, traffic would first be sent directly to vEdge-D. If the vEdge-A is not able to reach vEdge-D, traffic is sent to vEdge-B, which might have an operational path to reach vEdge-D. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination.  
**strict**—Direct matching traffic only to the intermediate destination. In our example, traffic is sent only to vEdge-B, regardless of whether it is reachable. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action action in a centralized control policy, strict is the default behavior. | Change the TLOC address and color to those in the specified TLOC list.  
Click Accept, then action TLOC  
*set tloc-list list-name* | Name of a **policy lists tloc-list** list. |
Default Action

If a route or TLOC being evaluated does not match any of the match conditions in a centralized control policy, a default action is applied to it. By default, the route or TLOC is rejected.

In vManage NMS, you modify the default action from Configuration ► Policies ► Centralized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control (Route and TLOC) ► Sequence Type ► (Route | TLOC) ► Sequence Rule ► Default Action.

In the CLI, you modify the default action with the control policy default-action accept command.

Applying Centralized Control Policy

For a centralized control policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in vManage NMS:

1. In vManage NMS, select the Configure ► Policies screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.
4. Click Activate.

To apply a centralized policy in the CLI:

```
vSmart(config)# apply-policy
site-list
list-name
control-policy
policy-name (in | out)
```

You apply centralized control policy directionally:

- **Inbound direction (in)** — The policy analyzes routes and TLOCs being received from the sites in the site list before placing the routes and TLOCs into the route table on the vSmart controller, so the specified policy actions affect the OMP routes stored in the route table.
- **Outbound direction (out)** — The policy analyzes routes and TLOCs in the vSmart controller's route table after they are exported from the route table.

For all control-policy policies that you apply with apply-policy commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different control-policy policies, the attempt to commit the configuration on the vSmart controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (app-route-policy)
- Centralized data policy (data-policy)
- Centralized data policy used for cflowd flow monitoring (data-policy hat includes a cflowd action and apply-policy that includes a cflowd-template command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for control-policy and data-policy policies can have overlapping site IDs. So for the
two example site lists above, site-list 1 site-id 1-100 and site-list 2 site-id 70-130, you could apply one to a control policy and the other to a data policy.

Centralized Control Policy Overview

In the Cisco SD-WAN network architecture, centralized control policy is handled by the vSmart controller, which effectively is the routing engine of the Cisco SD-WAN network. The vSmart controller is the centralized manager of network-wide routes, maintaining a master route table for these routes. The vSmart controller builds its route table based on the route information advertised by the vEdge routers in its domain, using these routes to discover the network topology and to determine the best paths to network destinations. The vSmart controller distributes route information from its route table to the vEdge routers in its domain, and the vEdge routers use these routes to forward data traffic through the network. The result of this architecture is that networking-wide routing decisions and routing policy are orchestrated by a central authority instead of being implemented hop by hop, by the devices in the network.

Centralized control policy allows you to influence the network routes advertised by the vSmart controllers. This type of policy, which is provisioned centrally on the vSmart controller, affects both the route information that the vSmart controller stores in its master route table and the route information that it distributes to the vEdge routers.

Centralized control policy is provisioned and applied only on the vSmart controller. The control policy configuration itself is never pushed to vEdge routers in the overlay network. What is pushed to the vEdge routers, via the Overlay Management Protocol (OMP), are the results of the control policy, which the vEdge routers then install in their local route tables and use for forwarding data traffic. This design means that the distribution of network-wide routes is always administered centrally, using policies designed by network administrators. These policies are always implemented by centralized vSmart controllers, which are responsible for orchestrating the routing decisions in the Cisco SD-WAN overlay network.

Within a network domain, the network topology map on all vSmart controllers must be synchronized. To support this, you must configure identical policies on all the vSmart controllers in the domain.

All centralized control plane traffic, including route information, is carried by OMP peering sessions that run within the secure, permanent DTLS connections between vEdge routers and the vSmart controllers in their domain. The end points of an OMP peering session are identified by the system IDs of the Cisco SD-WAN devices, and the peering sessions carry the site ID, which identifies the site in which the device is located. A DTLS connection and the OMP session running over it remain active as long as the two peers are operational.
Control policy can be applied both inbound, to the route advertisements that the vSmart controllers receives from vEdge routers, and outbound, to advertisements that it sends to them. Inbound policy controls which routes and route information are installed in the local routing database on the vSmart controller, and whether this information is installed as-is or is modified. Outbound control policy is applied after a route is retrieved from the routing database, but before vSmart controller advertises it, and affects whether the route information is advertised as-is or is modified.

**Route Types**

The vSmart controller learns the network topology from OMP routes, which are Cisco SD-WAN-specific routes carried by OMP. There are three types of OMP routes:

- **Cisco SD-WAN OMP routes**—These routes carry prefix information that the vEdge router learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well direct, connected, and static routes. OMP advertises OMP routes to the vSmart controller by means of an OMP route SAFI (Subsequent Address Family Identifier). These routes are commonly simply called OMP routes.

- **TLOC routes**—These routes carry properties associated with transport locations, which are the physical points at which the vEdge routers connect to the WAN or the transport network. Properties that identify a TLOC include the IP address of the WAN interface and a color that identifies a particular traffic flow. OMP advertises TLOC routes using a TLOC SAFI.

- **Service routes**—These routes identify network services, such as firewalls and IDPs, that are available on the local-site network to which the vEdge router is connection. OMP advertises these routes using a service SAFI.

A straightforward way to see the difference in these three types of routes is by using the various `show omp` operational commands when you are logged in to the CLI on a vSmart controller or a vEdge router. The `show omp routes` command displays information sorted by prefix, the `show omp services` command display route information sorted by service, and the `show omp tlocs` command sorts route information by TLOC.

**Default Behavior without Centralized Control Policy**

By default, no centralized control policy is provisioned on the vSmart controller. This results in the following route advertisement and redistribution behavior within a domain:

- All vEdge routers redistribute all the route-related prefixes that they learn from their site-local network to the vSmart controller. This route information is carried by OMP route advertisements that are sent over the DTLS connection between the vEdge router and the vSmart controller. If a domain contains multiple vSmart controllers, the vEdge routers send all OMP route advertisements to all the controllers.

- All vEdge routers send all TLOC routes to the vSmart controller or controllers in their domain, using OMP.

- All vEdge routers send all service routes to advertise any network services, such as firewalls and IDPs, that are available at the local site where the vEdge router is located. Again, these are carried by OMP.

- The vSmart controller accepts, as is, all the OMP, TLOC, and service routes that it receives from all the vEdge routers in its domain, storing the information in its route table. The vSmart controller tracks which OMP routes, TLOCs, and services belong to which VPNs. The vSmart controller uses all the routes to develop a topology map of the network and to determine routing paths for data traffic through the overlay network.
- The vSmart controller redistributes all information learned from the OMP, TLOC, and service routes in a particular VPN to all vEdge routers in the same VPN.

- The vEdge routers regularly send route updates to the vSmart controller.

- The vSmart controller recalculates routing paths, updates its route table, and advertises new and changed routing information to all the vEdge routers.

**Behavior Changes with Centralized Control Policy**

When you do not want to redistribute all route information to all vEdgeouters in a domain, or when you want to modify the route information that is stored in the vSmart controller's route table or that is advertised by the vSmart controller, you design and provision centralized control policy. To activate the control policy, you apply it to specific sites in the overlay network in either the inbound or the outbound direction. The direction is with respect to the vSmart controller. All provisioning of centralized control policy is done on the vSmart controller.

Applying a centralized control policy in the inbound direction filters or modifies the routes being advertised by the vEdge router before they are placed in the route table on the vSmart controller. As the first step in the process, routes are either accepted or rejected. Accepted routes are installed in the route table on the vSmart controller either as received or as modified by the control policy. Routes that are rejected by a control policy are silently discarded.

Applying a control policy in outbound direction filters or modifies the routes that the vSmart controller redistributes to the vEdge routers. As the first step of an outbound policy, routes are either accepted or rejected. For accepted routes, centralized control policy can modify the routes before they are distributed by the vSmart controller. Routes that are rejected by an outbound policy are not advertised.

**Examples of Modifying Traffic Flow with Centralized Control Policy**

This section provides some basic examples of how you can use centralized control policies to modify the flow of data traffic through the overlay network.
Create an Arbitrary Topology

When data traffic is exchanged between two vEdge routers, if you have provisioned no control policy, the two vEdge routers establish an IPsec tunnel between them and the data traffic flows directly from one router to the next. For a network with only two vEdge routers or with just a small number of vEdge routers, establishing connections between each pair of routers is generally not be an issue. However, such a solution does not scale. In a network with hundreds or even thousands of branches, establishing a full mesh of IPsec tunnels would tax the CPU resources of each vEdge router.

One way to minimize this overhead is to create a hub-and-spoke type of topology in which one of the vEdge routers acts as a hub site that receives the data traffic from all the spoke, or branch, routers and then redirects the traffic to the proper destination. This example shows one of the ways to create such a hub-and-spoke topology, which is to create a control policy that changes the address of the TLOC associated with the destination.

The figure here illustrates how such a policy might work. The topology has two branch locations, West and East. When no control policy is provisioned, these two vEdge routers exchange data traffic with each other directly by creating an IPsec tunnel between them (shown by the red line). Here, the route table on the West vEdge router contains a route to vEdge East with a destination TLOC of 2.1.1.1, color gold (which we write as the tuple \{2.1.1.1, gold\}), and vEdge East route table has a route to the West branch with a destination TLOC of \{1.1.1.1, gold\}.

To set up a hub-and-spoke--type topology here, we provision a control policy that causes the West and East vEdge routers to send all data packets destined for the other router to the vEdge hub router. (Remember that because control policy is always centralized, you provision it on the vSmart controller.) On the West vEdge router, the policy simply changes the destination TLOC from \{2.1.1.1, gold\} to \{10.1.1.1, gold\}, which is the TLOC of the vEdge hub router, and on the East router, the policy changes the destination TLOC from \{1.1.1.1, gold\} to the hub's TLOC, \{10.1.1.1, gold\}. If there were other branch sites on the west and east sides of the network that exchange data traffic, you could apply these same two control policies to have them redirect all their data traffic through the hub vEdge router.
**Set Up Traffic Engineering**

Control policy allows you to design and provision traffic engineering. In a simple case, suppose that you have two vEdge routers acting as hub devices. Here, you might want data traffic destined to a branch vEdge router to always transit through one of the hub vEdge routers. To engineer this traffic flow, you set the TLOC preference value to favor the desired hub vEdge router.

The figure on the left shows that Site ID 100 has two hub vEdge routers, one that serves the West side of the network and a second that serves the East side. We always want data traffic from the West vEdge branch router to be handled by the West vEdge hub, and similarly, we want data traffic from the East vEdge branch router to go through the east vEdge hub.

To engineer this traffic flow, you provision two control policies, one for Site ID 1, where the West vEdge branch router is located, and a second one for Site ID 2. The control policy for Site ID 1 changes the TLOC for traffic destined to the East vEdge router to \{10.1.1.1, gold\}, and the control policy for Site ID 2 changes the TLOC for traffic destined for Site ID 1 to \{20.1.1.1, gold\}. One additional effect of this traffic engineering policy is that it load-balances the traffic traveling through the two vEdge hub routers.

With such a traffic engineering policy, a route from the source router to the destination router is installed in the local route table, and traffic is sent to the destination regardless of whether the path between the source and destination vEdge routers is available. Enabling end-to-end tracking of the path to the ultimate destination allows the vSmart controller to monitor the path from the source to the destination, and to inform the source router when that path is not available. The source router can then modify or remove the path from its route table.
The figure to the right illustrates end-to-end path tracking. It shows that traffic from vEdge-A that is destined for vEdge-D first goes to an intermediate router, vEdge-B, perhaps because this intermediate router provides a service, such as a firewall. (You configure this traffic engineering with a centralized control policy that is applied to vEdge-A, at Site 1.) Then vEdge-B, which has a direct path to the ultimate destination, forwards the traffic to vEdge-D. So, in this example, the end-to-end path between vEdge-A and vEdge-D comprises two tunnels, one between vEdge-A and vEdge-B, and the second between vEdge-B and vEdge-D. The vSmart controller tracks this end-to-end path, and it notifies vEdge-A if the portion of the path between vEdge-B and vEdge-D becomes unavailable.

As part of end-to-end path tracking, you can specify how to forwarded traffic from the source to the ultimate destination via an intermediate router. (You do this by setting the TLOC action in the action portion of the control policy.) The default method is strict forwarding, where traffic is always sent from vEdge-A to vEdge-B, regardless of whether vEdge-B has a direct path to vEdge-D or whether the tunnel between vEdge-B and vEdge-D is up. More flexible methods forward some or all traffic directly from vEdge-A to vEdge-D. You can also set up a second intermediate router to provide a redundant path with the first intermediate router is unreachable and use an ECMP method to forward traffic between the two. The figure below adds vEdge-C as a redundant intermediate router.
Centralized Control Policy Configuration Examples

This article provides some straightforward examples of configuring centralized control policy to help you understand the configuration procedure and get an idea of how to use policy to influence traffic flow across the Cisco SD-WAN overlay network domain. You can find more complex examples in the Validated Examples articles.

Traffic Engineering

This example of traffic engineering forces all traffic to come to a vEdge router via a vEdge hub instead of directly.

One common way to design a domain in a Cisco SD-WAN overlay network is to route all traffic destined for branches through a vEdge hub router, which is typically located in a data center, rather than sending the traffic directly from one vEdge router to another. You can think of this as a hub-and-spoke design, where one vEdge router is acting as a hub and the vEdge routers are the spokes. With such a design, traffic between local branches travels over the IPsec connections that are established between the vEdge spoke routers and the vEdge hub routers when the vEdge routers booted up. Using established connections means that the vEdge routers do not need to expend time and CPU cycles to establish IPsec connections with each other. If you were to imagine that this were a large network with many vEdge routers, having a full mesh of connections between each pair of routers would require a large amount of CPU from the routers. Another attribute of this design is that, from an administrative point of view, it can be simpler to institute coordinated traffic flow policies on the vEdge hub routers, both because there are fewer of them in the overlay network and because they are located in a centralized data center.

One way to direct all vEdge spoke router traffic to a vEdge hub router is to create a policy that changes the TLOC associated with the routes in the local network. Let’s consider the topology in the figure here:
This topology has two vEdge routers in different branches:

- The West vEdge router in site ID 1. The TLOC for this router is defined by its IP address (1.1.1.1), a color (gold), and an encapsulation (here, IPsec). We write the full TLOC address as \{1.1.1.1, gold, ipsec\}. The color is simply a way to identify a flow of traffic and to separate it from other flows.

- The East vEdge router in site ID 2 has a TLOC address of \{2.1.1.1, gold, ipsec\}.

The West and East vEdge routers learn each other’s TLOC addresses from the OMP routes distributed to them by the vSmart controller. In this example, the East vEdge advertises the prefix 8.8.0.0/16 as being reachable at TLOC \{2.1.1.1, gold, ipsec\}. In the absence of any policy, the West vEdge router could route traffic destined for 8.8.0.0/16 to TLOC \{2.1.1.1, gold, ipsec\}, which means that the West vEdge router would be sending traffic directly to the East vEdge router.

However, our design requires that all traffic from West to East be routed through the vEdge hub router, whose TLOC address is \{100.1.1.1, gold, ipsec\}, before going to the East vEdge router. To effect this traffic flow, you define a policy that changes the route’s TLOC. So, for the prefix 8.8.0.0/16, you create a policy that changes the TLOC associated with the prefix 8.8.0.0/16 from \{2.1.1.1, gold, ipsec\}, which is the TLOC address of the East vEdge router, to \{10.1.1.1, gold, ipsec\}, which is the TLOC address of the vEdge hub router. The result is that the OMP route for the prefix 8.8.0.0/16 that the vSmart controller advertises to the West vEdge router contains the TLOC address of the vEdge hub router instead of the TLOC address of the East vEdge router. From a traffic flow point of view, the West vEdge router then sends all traffic destined for 8.8.0.0/16 to the vEdge hub router.

The vEdge Hub router also learns the TLOC addresses of the West and East vEdge routers from the OMP routes advertised by the vSmart controller. Because we want vEdge hub router to use these two TLOC addresses, no policy is required to control how the hub directs traffic to the other vEdge routers.

Here is a policy configuration on the vSmart controller that directs the West vEdge router (and any other vEdges in the network domain) to send traffic destined to prefix 8.8.0.0/16 to TLOC 10.1.1.1, gold, which is the vEdge hub router:
policy
lists
  prefix-list east-prefixes
  ip-prefix 8.8.0.0/16
  site-list west-sites
  site-id 1
control-policy change-tloc
  sequence 10
  match route
    prefix-list east-prefixes
    site-id 2
    action accept
      set tloc 10.1.1.1 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out

A rough English translation of this policy is:

Create a list named “east-prefixes” that contains the IP prefix “8.8.0.0/16”
Create a list named “west-sites” that contains the site-id “1”
Define a control policy named “change-tloc”
Create a policy sequence element that:
  Matches a prefix from list “east-prefixes”, that is, matches “8.8.0.0/16”
  AND matches a route from site-id “2”
If a match occurs:
  Accept the route
  AND change the route’s TLOC to “10.1.1.1” with a color of “gold” and an encapsulation of “ipsec”
Apply the control policy “change-tloc” to OMP routes sent by the vSmart controller to “west-sites”, that is, to site ID 1

This control policy is configured on the vSmart controller as an outbound policy, as indicated by the out option in the apply-policy site command. This option means the vSmart controller applies the TLOC change to the OMP route after it distributes the route from its route table. The OMP route for prefix 8.8.0.0/16 that the vSmart controller distributes to the West vEdge associates 8.8.0.0/16 with TLOC 10.1.1.1, gold. This is the OMP route that the West vEdge router installs in its route table. The end results are that when the West vEdge router sends traffic to 8.8.0.0/16, the traffic is directed to the vEdge hub; and the West vEdge router does not establish a DTLS tunnel directly with the East vEdge router.

If the West side of the network had many sites instead of just one and each site had its own vEdge router, it would be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the sites in the site-list west-sites list. This is the only change you need to make in the policy to have all the West side sites send traffic bound for the prefix 8.8.0.0/16 through the vEdge hub router. For example:

policy
lists
  prefix-list east-prefixes
  ip-prefix 8.8.0.0/16
  site-list west-sites
  site-id 1
  site-id 11
  site-id 12
  site-id 13
control-policy change-tloc
  sequence 10
  match route
    prefix-list east-prefixes
    site-id 2
    action accept
      set tloc 10.1.1.1 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out
Creating Arbitrary Topologies

To provide redundancy in the hub-and-spoke-style topology discussed in the previous example, you can add a second vEdge hub to create a dual-homed hub site. The following figure shows that site ID 10 now has two vEdge hubs. We still want all inter-branch traffic to be routed through a vEdge hub. However, because we now have dual-homed hubs, we want to share the data traffic between the two hub routers.

- vEdge hub West, with TLOC 10.1.1.1, gold. We want all data traffic from branches on the West side of the overlay network to pass through and be processed by this vEdge router.
- vEdge hub East, with TLOC 20.1.1.1, gold. Similarly, we all East side data traffic to pass through the East vEdge hub.

Here is a policy configuration on the vSmart controller that would send West side data traffic through vEdge hub West and East side traffic through vEdge hub East:

```plaintext
policy
  lists
    site-list west-sites
      site-id 1
    site-list east-sites
      site-id 2
    tloc-list west-hub-tlocs
      tloc-id 10.1.1.1 gold
    tloc-list east-hub-tlocs
      tloc-id 20.1.1.1 gold
  control-policy prefer-west-hub
    sequence 10
      match tloc
        tloc-list west-hub-tlocs
      action accept
      set preference 50
  control-policy prefer-east-hub
    sequence 10
      match tloc
        tloc-list east-hub-tlocs
      action accept
```

![Diagram showing vEdge hubs and site connections](image)
set preference 50
apply-policy
site west-sites control-policy prefer-west-hub out
site east-sites control-policy prefer-east-hub out

Here is an explanation of this policy configuration:

• Create the site lists that are required for the apply-policy configuration command:
  • site-list west-sites lists all the site IDs for all the vEdge routers in the West portion of the overlay network.
  • site-list east-sites lists the site IDs for the vEdge routers in the East portion of the network.

• Create the TLOC lists that are required for the match condition in the control policy:
  • west-hub-tlocs lists the TLOC for the West vEdge hub, which we want to service traffic from the West side vEdge routers.
  • east-hub-tlocs lists the TLOC for the East vEdge hub, to service traffic from the East vEdge routers.

• Define two control policies:
  • prefer-west-hub affects OMP routes destined to TLOC 10.1.1.1, gold, which is the TLOC address of the West vEdge hub router. This policy modifies the preference value in the OMP route to a value of 50, which is large enough that it is likely that no other OMP routes will have a larger preference. So setting a high preference value directs traffic destined for site 100 to the West hub router.
  • Similarly, prefer-east-hub sets the preference to 50 for OMP routes destined TLOC 20.1.1.1, gold, which is the TLOC address of the East vEdge hub router, thus directing traffic destined for site 100 site to the East vEdge hub router.

• Apply the control policies:
  • The first line in the apply-policy configuration has the vSmart controller apply the prefer-west-hub control policy to the sites listed in the west-sites list, which here is only site ID 1, so that the preference in their OMP routes destined to TLOC 10.1.1.1 is changed to 50 and traffic sent from the West vEdge routers to the hub site goes through the West vEdge hub router.
  • The vSmart controller applies the prefer-east-hub control policy to the OMP routes that it advertises to the vEdges in the east-sites list, which changes the preference to 50 for OMP routes destined to TLOC 20.1.1.1, so that traffic from the East vEdge routers goes to the East vEdge hub router.

Configuring Localized Control Policy

Localized control policy, which you configure on vEdge routers, lets you affect routing policy on the network at the local site where the vEdge router is located. This type of control policy is called route policy.

This article provides procedures for configuring localized control policy.

Configuration Components

A route policy consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match
conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configured, it is, by default, rejected and discarded.

The following figure illustrates the configuration components for localized control policy.

To create a localized control policy, you include the following components in the configuration on a vEdge router:

**Table 230:**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the control policy configuration.</td>
<td>Configuration ▶ Policies ▶ Localized Policy ▶ Add Policy ▶ Create Groups of Interest or Configuration ▶ Policies ▶ Custom Options ▶ Localized Policy ▶ Lists</td>
<td>policy lists</td>
</tr>
<tr>
<td>Localized control policy instance</td>
<td>Container for localized control policy.</td>
<td>Configuration ▶ Policies ▶ Localized Policy ▶ Add Policy</td>
<td>policy control-policy</td>
</tr>
<tr>
<td>Network topology</td>
<td>Conditions that define the network topology</td>
<td>Configuration ▶ Policies ▶ Localized Policy ▶ Add Policy ▶ Create Groups of Interest or Configuration ▶ Policies ▶ Custom Options ▶ Localized Policy ▶ Lists</td>
<td>—</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>vManage Configuration</td>
<td>CLI Configuration Command</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Numbered sequences of match–action pairs</td>
<td>Sequences that establish the order in which policy components are applied.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type or Configuration ► Policies ► Add Options ► Localized Policy ► Add Topology ► Custom Control ► Sequence Type</td>
<td>policy control-policy sequence</td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that the routes and TLOCs must match to be considered for a control policy.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule or Configuration ► Policies ► Custom Options ► Localized Policy ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule</td>
<td>policy control-policy sequence match route—Match OMP route properties, including things such as the originating protocol and IP prefixes. policy control-policy sequence match tloc—Match transport location parameters, including things such as the domain ID and TLOC IP address.</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching routes and TLOCs, and how to process matching items.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Topology and VPN Membership ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule or Configuration ► Policies ► Custom Options ► Localized Policy ► Add Topology ► Custom Control ► Sequence Type ► Sequence Rule</td>
<td>policy control-policy sequence action</td>
</tr>
</tbody>
</table>
### General vManage Configuration Procedure

To configure localized policies, use the vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure and modify the following localized policy components:

- Groups of interest, also called lists
- Forwarding classes to use for QoS
- Access control lists (ACLs)
- Route policies
- Policy settings

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

#### Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the **Configure > Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.

The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

#### Step 2: Configure Groups of Interest

In Create Groups of Interest, create lists of groups to use in localized policy:
1. Create new lists, as described in the following table:

**Table 231:**

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **AS Path** | 1. In the left bar, click AS Path.  
2. Click New AS Path List.  
3. Enter a name for the list.  
4. Enter the AS path, separating AS numbers with a comma.  
5. Click Add. |
| **Community** | 1. In the left bar, click Community.  
2. Click New Community List.  
3. Enter a name for the list.  
4. Enter the BGP community in the format `aarn` or as the string `internet`, `local-as`, `no-advertise`, or `no-export`, separating multiple items with a comma. For `aa` enter a 2-byte AS number, and for `nn` enter a 2-byte network number.  
5. Click Add. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Extended Community| 1. In the left bar, click Extended Community.  
2. Click New Extended Community List.  
3. Enter a name for the list.  
4. Enter the BGP extended community as rt *(aa:nn | ip-address)*, for a route target community, or soo *(aa:nn | ip-address)*, for a route origin community, separating multiple items with a comma. For *aa* enter a 2-byte AS number, and for *nn* enter a 2-byte network number.  
5. Click Add. |
| Mirror            | 1. In the left bar, click TLOC.  
2. Click New TLOC List. The TLOC List popup displays.  
3. Enter a name for the list.  
4. In the TLOC IP field, enter the system IP address for the TLOC.  
5. In the Color field, select the TLOC’s color.  
6. In the Encap field, select the encapsulation type.  
7. In the Preference field, optionally select a preference to associate with the TLOC.  
8. Click Add TLOC to add another TLOC to the list.  
9. Click Save. |
| Policer           | 1. In the left bar, click VPN.  
2. Click New VPN List.  
3. Enter a name for the list.  
4. In the Add VPN field, enter one or more VPN IDs separated by commas.  
5. Click Add. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Prefix    | 1. In the left bar, click Prefix.  
            2. Click New Prefix List.  
            3. Enter a name for the list.  
            4. Enter the IP prefix in one of the following formats:  
               • *prefix/length*—Exactly match a single prefix–length pair.  
               • *0.0.0.0/0*—Match any prefix–length pair.  
               • *0.0.0.0/0 le length*—Match any IP prefix whose length is less than or equal to *length*. For example, *ip-prefix 0.0.0.0/0 le 16* matches all IP prefixes with lengths from /1 through /16.  
               • *0.0.0.0/0 ge length*—Match any IP prefix whose length is greater than or equal to *length*. For example, *ip-prefix 0.0.0.0 ge 25* matches all IP prefixes with lengths from /25 through /32.  
               • *0.0.0.0/0 ge length1 le length2*, or *0.0.0.0 le length2 ge length1*—Match any IP prefix whose length is greater than or equal to *length1* and less than or equal to *length2*. For example, *ip-prefix 0.0.0.0/0 ge 20 le 24* matches all /20, /21, /22, /23, and /24 prefixes. Also, *ip-prefix 0.0.0.0/0 le 24 ge 20* matches the same prefixes. If *length1* and *length2* are the same, a single IP prefix length is matched. For example, *ip-prefix 0.0.0.0/0 ge 24 le 24* matches only /24 prefixes.  |
|           | 1. Click Add. |

1. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard.  
2. Click **Next** to move to Configure Access Control Lists in the wizard.  
3. Click **Next** to move to Configure Route Policies in the wizard.  

**Step 3: Configure Route Policies**  
In Configure Route Policies, configure the routing policies:  
To configure a route policy:  
1. In the **Add Route Policy** tab, select **Create New**.  
2. Enter a name and description for the route policy.  
3. In the left pane, click Add Sequence Type. A Route box is displayed in the left pane.  
4. Double-click the Route box, and type a name for the route policy.  
5. In the right pane, click Add Sequence Rule to create a single sequence in the policy. The Match tab is selected by default.  
6. Click a match condition.  
7. On the left, enter the values for the match condition.
8. On the right enter the action or actions to take if the policy matches.
9. Repeat Steps 6 through 8 to add match–action pairs to the route policy.
10. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.
11. To remove a match–action pair from the route policy, click the X in the upper right of the condition.
12. Click Save Match and Actions to save a sequence rule.
13. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.
14. To copy, delete, or rename an route policy sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
15. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
   1. Click Default Action in the left pane.
   2. Click the Pencil icon.
   3. Change the default action to Accept.
   4. Click Save Match and Actions.
16. Click Next to move to Policy Overview in the wizard.
17. Click Preview to view the full policy in CLI format.
18. Click Save Policy.

**Step 4: Apply a Route Policy in a Device Template**

1. In vManage NMS, select the Configuration ► Templates screen.
2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. To apply a route policy to BGP:
   1. Scroll to the Service VPN section.
   2. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   3. From Additional VPN Templates, select BGP.
   4. From the BGP drop-down, click Create Template or View Template.
   5. Select the Neighbor tab, click the plus sign (+), and click More.
   6. In Address Family, change the scope to Device Specific. Then, Click On to enable Address Family, Click On to enable Route Policy In, and specify the name of a route policy to apply to prefixes received from the neighbor, or click On to enable Route Policy Out, and specify the name of a route policy to apply to prefixes sent to the neighbor. This name is one that you configured with a `policy route-policy` command.
   7. Click Save to save the neighbor configuration, and then click Save to save the BGP configuration.

7. To apply a route policy to routes coming from all OSPF neighbors:
   1. Scroll to the Service VPN section.
   2. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   3. From Additional VPN Templates, select OSPF.
   4. Click Create Template or View Template.
   5. Select the Advanced tab.
   6. In Policy Name, specify the name of a route policy to apply to incoming routes. This name is one that you configured with a `policy route-policy` command.
   7. Click Save.

8. To apply a route policy before redistributing routes into OSPF:
   1. Scroll to the Service VPN section.
   2. In the Service VPN drop-down, type the service VPN number (a VPN number other than 0 or 512).
   3. From Additional VPN Templates, select OSPF.
   4. Click Create Template or View Template.
   5. Select the Redistribute tab, click the plus sign (+), and select the protocol from which to redistribute routes into OSPF.
   6. Specify the name of a route policy to apply to the routes being redistributed. This name is one that you configured with a `policy route-policy` command.
7. Click Save.

9. Click Save (for a new template) or Update (for an existing template).

**General CLI Configuration Procedure**

To configure a route policy using the CLI:

1. Create lists of prefixes, as needed:

   ```
   vEdge(config)# policy
   vEdge(config-policy)# lists
   vEdge(config-lists)# prefix-list
   list-name
   vEdge(config-lists-list-name)# ip-prefix prefix/length
   ```

2. Create lists of BGP AS paths, and community and extended community attributes, as needed:

   ```
   vEdge(config)# policy lists
   vEdge(config-lists)# as-path-list
   list-name
   vEdge(config-lists-list-name)# as-path
   path-list
   vEdge(config)# policy lists
   vEdge(config-lists)# community-list
   list-name
   vEdge(config-lists-list-name)# community [aa:nn | internet | local-as | no-advertise | no-export]
   vEdge(config-lists)# ext-community-list
   list-name
   vEdge(config-lists-list-name)# community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)]
   ```

3. Create a route policy instance:

   ```
   vEdge(config)# policy route-policy
   policy-name
   vEdge(config-route-policy-policy-name)#
   ```

4. Create a series of match–action pair sequences:

   ```
   vEdge(config-route-policy-policy-name)# sequence
   number
   vEdge(config-sequence-number)#
   ```

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for routes:

   ```
   vEdge(config-sequence-number)# match match-parameter
   ```

6. Define actions to take when a match occurs:

   ```
   vEdge(config-sequence-number)# action reject
   vEdge(config-sequence-number)# action accept set parameter
   ```

7. Create additional numbered sequences of match–action pairs within the router policy, as needed.

8. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching routes, configure the default action for the policy:

   ```
   vEdge(config-policy-name)# default-action accept
   ```

9. Apply the policy to a BGP address family, to all OSPF inbound routes, or when redistributing OSPF routes:

   ```
   vEdge(config)# vpn
   vpn-id
   ```
router bgp
  local-as-number
neighbor
  address

vEdge(config-neighbor)# address-family ipv4-unicast
vEdge(config-address-family-ipv4-unicast)# route-policy policy-name (in | out)
vEdge(config)# vpn
  vpn-id

router ospf
  vEdge(config-ospf)# route-policy
  policy-name
  in

vEdge(config)# vpn
  vpn-id

router ospf
  vEdge(config-ospf)# redistribute (bgp | connected | nat | ospf | static)
  route-policy
  policy-name

Structural Components of Policy Configuration for Localized Control Policy

Following are the structural components required to configure localized control policy. Each one is explained in more detail in the sections below.

- **policy lists**: as-path-list list-name as-path path-list community-list list-name
  - community [aa:nn | internet | local-as | no-advertise | no-export] ext-community-list
  - list-name community [rt (aa:nn | ip-address) | soo (aa:nn | ip-address)] prefix-list
- **route-policy**: policy-name
  - sequence number
  - match
  - action (accept | reject)
- **default-action**
  - vpn vpn-id router bgp local-as-number neighbor address
  - address-family ipv4-unicast route-policy
  - policy-name (in | out)
  - vpn vpn-id router ospf route-policy policy-name in redistribute
  - (bgp | connected | nat | ospf | static)

Lists

Route policy uses the following types of lists to group related items. You configure lists under the policy lists command hierarchy on vEdge routers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS paths</td>
<td>List of one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list in quotation marks (&quot; &quot;). To configure multiple AS paths in a single list, include multiple as-path options, specifying one AS path in each option.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► AS Path Custom Options ► Localized Policy ► Lists ► AS Path as-path-list list-name as-path path-list</td>
</tr>
<tr>
<td>List Type</td>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Communities</td>
<td>List of one or more BGP communities. In <code>community</code>, you can specify: • <code>autonumber</code>: Autonomous system number and network number. Each number is a 2-byte value with a range from 1 to 65535. • <code>internet</code>: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • <code>local-as</code>: Routes in this community are not advertised outside the local AS. • <code>no-advertise</code>: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • <code>no-export</code>: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple <code>community</code> options, specifying one community in each option.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Create Groups of Interest ➤ Community Configuration ➤ Policies ➤ Custom Options ➤ Localized Policy ➤ Lists ➤ Community `community-list list-name community [autonumber</td>
</tr>
<tr>
<td>Extended communities</td>
<td>List of one or more BGP extended communities. In <code>community</code>, you can specify: • `rt (autonumber</td>
<td>ip-address)<code>: Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • </code>soo (autonumber</td>
</tr>
</tbody>
</table>
List Type | Description | vManage Configuration/CLI Configuration Command
---|---|---
Prefixes | List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple `ip-prefix` options, specifying one prefix in each option. Specify the IP prefixes as follows: • `prefix/length`—Exactly match a single prefix–length pair. • `0.0.0.0/0`—Match any prefix–length pair. • `0.0.0.0/0 le length`—Match any IP prefix whose length is less than or equal to `length`. For example, `ip-prefix 0.0.0.0/0 le 16` matches all IP prefixes with lengths from /1 through /16. • `0.0.0.0/0 ge length`—Match any IP prefix whose length is greater than or equal to `length`. For example, `ip-prefix 0.0.0.0/0 ge 25` matches all IP prefixes with lengths from /25 through /32. • `0.0.0.0/0 ge length1 le length2`, or `0.0.0.0/0 le length2 ge length1`—Match any IP prefix whose length is greater than or equal to `length1` and less than or equal to `length2`. For example, `ip-prefix 0.0.0.0/0 ge 20 le 24` matches all /20, /21, /22, /23, and /24 prefixes. Also, `ip-prefix 0.0.0.0/0 le 24 ge 20` matches the same prefixes. If `length1` and `length2` are the same, a single IP prefix length is matched. For example, `ip-prefix 0.0.0.0/0 ge 24 le 24` matches only /24 prefixes. | Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Prefix

**Sequences**

A localized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route is analyzed by the match–action pairs in the policy.

In vManage NMS, you configure sequences from:

• Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Route Policy ► Sequence Type

• Configuration ► Policies ► Custom Options ► Localized Policy ► Route Policy ► Sequence Type

In the CLI, you configure sequences with the `route-policy sequence` command.

Each sequence in a localized control policy can contain one match condition and one action condition.

**Match Parameters**

In vManage NMS, you configure sequences from:

• Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Route Policy ► Sequence Type ► Sequence Rule ► Match

• Configuration ► Policies ► Custom Options ► Localized Policy ► Route Policy ► Sequence Type ► Sequence Rule ► Match

In the CLI, you configure sequences with the `route-policy sequence match` command.

For route policy routes, you can match these attributes:
### Table 233:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP prefix or prefixes from which the route was learned</td>
<td>Match Address</td>
<td>Name of an IP prefix list</td>
</tr>
<tr>
<td></td>
<td>address list-name</td>
<td></td>
</tr>
<tr>
<td>BGP AS paths</td>
<td>Match AS Path List</td>
<td>Name of an AS path list</td>
</tr>
<tr>
<td></td>
<td>as-path list-name</td>
<td></td>
</tr>
<tr>
<td>BGP communities</td>
<td>Match Community List</td>
<td>Name of a BGP community list</td>
</tr>
<tr>
<td></td>
<td>community list-name</td>
<td></td>
</tr>
<tr>
<td>BGP extended communities</td>
<td>Match Extended Community List</td>
<td>Name of a BGP extended community list</td>
</tr>
<tr>
<td></td>
<td>ext-community list-name</td>
<td></td>
</tr>
<tr>
<td>BGP local preference</td>
<td>Match BGP Local Preference</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>local-preference number</td>
<td></td>
</tr>
<tr>
<td>Route metric</td>
<td>Match Metric</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>metric number</td>
<td></td>
</tr>
<tr>
<td>Next hop</td>
<td>Match Next Hop</td>
<td>Name of an IP prefix list</td>
</tr>
<tr>
<td></td>
<td>next-hop list-name</td>
<td></td>
</tr>
<tr>
<td>OMP tag for OSPF</td>
<td>Match OMP Tag</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>omp-tag list-name</td>
<td></td>
</tr>
<tr>
<td>BGP origin code</td>
<td>Match Origin</td>
<td>egp (default), igp, incomplete</td>
</tr>
<tr>
<td></td>
<td>origin origin</td>
<td></td>
</tr>
<tr>
<td>OSPF tag value</td>
<td>Match OSPF Tag</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td></td>
<td>ospf-tag number</td>
<td></td>
</tr>
<tr>
<td>Peer address</td>
<td>Match Peer</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>peer address</td>
<td></td>
</tr>
</tbody>
</table>

**Action Parameters**

For each match condition, you configure a corresponding action to take if the packet matches.

In vManage NMS, you configure match parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Route Policy ► Sequence Type ► Sequence Rule ► Action

- Configuration ► Policies ► Custom Options ► Localized Policy ► Configure Route Policy ► Sequence Type ► Sequence Rule ► Action
In the CLI, you configure actions with the **policy control-policy action** command.

Each sequence in a localized control policy can contain one action condition. When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

**Table 234:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the <em>action</em> portion of the policy configuration.</td>
<td>Click Accept accept</td>
<td>—</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click Reject reject</td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a route that is accepted, the following actions can be configured:

**Table 235:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the AS number in which a BGP route aggregator is located and the IP address of the route aggregator.</td>
<td>Click Accept, then action Aggregator set aggregator as-number ip-address</td>
<td>1 through 65535</td>
</tr>
<tr>
<td>Set an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path.</td>
<td>Click Accept, then action AS Path set as-path (exclude</td>
<td>1 through 65535</td>
</tr>
<tr>
<td></td>
<td>prepend) as-number</td>
<td></td>
</tr>
<tr>
<td>Set the BGP atomic aggregate attribute.</td>
<td>Click Accept, then action Atomic Aggregate set atomic-aggregate</td>
<td>—</td>
</tr>
<tr>
<td>Set the BGP community value.</td>
<td>Click Accept, then action Community set community value</td>
<td>[aa:nn</td>
</tr>
<tr>
<td>Set the BGP local preference.</td>
<td>Click Accept, then action Local Preference set local-preference number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the metric value.</td>
<td>Click Accept, then action Metric set metric number</td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the metric type.</td>
<td>Click Accept, then action Metric Type set metric-type type</td>
<td>type1, type2</td>
</tr>
<tr>
<td>Set the next-hop address.</td>
<td>Click Accept, then action Next Hop set next-hop ip-address</td>
<td>IP address</td>
</tr>
</tbody>
</table>
### Configuring Localized Control Policy

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the OMP tag for OSPF to use.</td>
<td>Click Accept, then action OMP Tag &lt;br&gt;<code>set omp-tag number</code></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the BGP origin code.</td>
<td>Click Accept, then action Origin &lt;br&gt;<code>set origin origin</code></td>
<td>egp, igp (default), incomplete</td>
</tr>
<tr>
<td>Set the IP address from which the route was learned.</td>
<td>Click Accept, then action Originator &lt;br&gt;<code>set originator ip-address</code></td>
<td>IP address</td>
</tr>
<tr>
<td>Set the OSPF tag value.</td>
<td>Click Accept, then action OSPF Tag &lt;br&gt;<code>set ospf-tag number</code></td>
<td>0 through 4294967295</td>
</tr>
<tr>
<td>Set the BGP weight.</td>
<td>Click Accept, then action Weight &lt;br&gt;<code>set weight number</code></td>
<td>0 through 4294967295</td>
</tr>
</tbody>
</table>

To display the OMP and OSPF tag values associated with a route, use the `show ip routes detail` command.

### Default Action

If a route being evaluated does not match any of the match conditions in a localized control policy, a default action is applied to this route. By default, the route is rejected.

In vManage NMS, you modify the default action from Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Route Policy ► Sequence Type ► Sequence Rule ► Default Action.

In the CLI, you modify the default action with the `control policy default-action accept` command.

### Applying Route Policy for BGP

For a route policy to take effect for BGP, you must apply it to an address family. Currently, the Cisco SD-WAN software supports only the IPv4 address family.

To apply a BGP route policy in vManage NMS:

1. In vManage NMS, select the Configure ► Templates screen.
2. In the Device tab, click the Create Template drop-down and select From Feature Template.
3. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
6. In the Basic Information bar, click the Service VPN tab.
7. In the Service VPN field, select the VPN number.
8. In Additional VPN Templates, select BGP.
9. Select Create Template.
10. In the Basic Configuration bar, click IPv4 Unicast Address Family.
11. In the Address Family field, select ipv4-unicast.
12. In the Redistribute tab, click New Redistribute.
13. In the Route Policy field, enter the name of the route policy to apply to redistributed routes.
14. Click Add.
15. Click Save.

To apply a BGP route policy in the CLI:

```
vEdge(config)# vpn
vpn-id
router bgp
local-as-number
neighbor address
address-family ipv4-unicast route-policy
policy-name (in | out)
```

Applying the policy in the inbound direction (in) affects routes being received by BGP. Applying the policy in the outbound direction (out) affects routes being advertised by BGP.

Applying Route Policy for OSPF

For a route policy to take effect for OSPF, you can apply it to all inbound traffic.

To apply an OSPF route policy in vManage NMS:

1. In vManage NMS, select the Configure ► Templates screen.
2. In the Device tab, click the Create Template drop-down and select From Feature Template.
3. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
6. In the Basic Information bar, click the Service VPN tab.
7. In the Service VPN field, select the VPN number.
8. In Additional VPN Templates, select OSPF.
9. Select Create Template.
10. In the Basic Configuration bar, click Redistribute.

11. Click New Redistribute.

12. In the Route Policy field, enter the name of the route policy to apply to redistributed routes.

13. Click Add.

14. Click Save.

To apply an OSPF route policy in the CLI:

```
vEdge(config)# vpn
vpn-id
router ospf route-policy
policy-name
in
```

You can also apply the policy when redistributing routes into OSPF:

```
vEdge(config)# vpn
vpn-id
router ospf redistribute (bgp | connected | nat | omp | static) route-policy
policy-name
```

### Configuring Localized Data Policy for IPv4

This article provides procedures for configuring IPv4 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply QoS, mirroring, and policing to data packets. You can create access lists that act on unicast and multicast traffic.

In vManage NMS, you configure localized data policy from the Configuration ► Policies screen, using a policy configuration wizard. In the CLI, you configure these policies on the vEdge router.

#### Configuration Components

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for access lists.
To create an access list, you include the following components in the configuration for a vEdge router:

Table 236:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the data policy configuration.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest or</td>
<td>policy lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Policies ► Custom Options ► Localized Policy ► Lists</td>
<td></td>
</tr>
<tr>
<td>Logging frequency</td>
<td>If you configure a logging action, log only a sample of data packet headers instead of all of them.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Log Frequency</td>
<td>policy logging-frequency</td>
</tr>
<tr>
<td>QoS, mirroring, and policing parameters</td>
<td>Parameters and rules required to configure QoS, traffic mirroring, and traffic policing. For QoS, you can configure class maps, QoS maps, the QoS scheduler, and rewrite rules. For mirroring, you configure the addresses of the source of the packets to be mirrored and the mirroring site. (You can mirror only unicast traffic.) For policing, you define transmission parameters.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Forwarding Classes/QoS, Policy Overview or</td>
<td>policy class-map policy cloud-qos policy-cloud-qos-service-side policy qos-scheduler policy qos-map policy rewrite-rule policy mirror policy policer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Policies ► Custom Options ► Localized Policy ► Forwarding Class/QoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Policies ► Custom Options ► Localized Policy ► Create Groups of Interest</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>vManage Configuration</td>
<td>CLI Configuration Command</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Access list instance</td>
<td>Container for an access list.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Configure Access Control Lists or</td>
<td>policy access-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Access Control Lists</td>
<td></td>
</tr>
<tr>
<td>Numbered sequences of</td>
<td>Sequences that establish the order in which policy components are applied.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Configure Access Control Lists or</td>
<td>policy access-list sequence</td>
</tr>
<tr>
<td>match–action pairs</td>
<td></td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Access Control Lists</td>
<td></td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Configure Access Control Lists or</td>
<td>policy access-list sequence match</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Access Control Lists</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching packets, and how to process matching</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Configure Access Control Lists or</td>
<td>policy access-list sequence action</td>
</tr>
<tr>
<td></td>
<td>items.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Access Control Lists</td>
<td></td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the match parameters in any of</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Add Policy ➤ Configure Access Control Lists or</td>
<td>policy access-list default-action</td>
</tr>
<tr>
<td></td>
<td>the sequences. By default, nonmatching packets are dropped.</td>
<td>Configuration ➤ Policies ➤ Localized Policy ➤ Access Control Lists</td>
<td></td>
</tr>
</tbody>
</table>
### General vManage Configuration Procedure

To configure IPv4 localized policy, use the vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure IPv4 localized policy components:

- **Groups of Interest**, also called lists—Create data prefix lists and mirroring and policer parameters that group together related items and that you call in the match or action components of a policy.
- **Forwarding Classes**—Define forwarding classes and rewrite rules to use for QoS.
- **Access Control Lists**—Define the match and action conditions of ACLs.
- **Route Policies**—Define the match and action conditions of route policies.
- **Policy Settings**—Define additional policy settings, including Cloud QoS settings and the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

**Step 1: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ➤ Policies screen.
2. Select the Localized Policy tab.
3. Click Add Policy.

The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

**Step 2: Create Groups of Interest**

In the Create Groups of interest screen create lists to use in the localized data policy:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
</table>
| Application of access lists | For an access list to take effect, you apply it an interface. You can also apply policers directly to interfaces. | Configuration ► Templates ► Feature ► VPN Interface Bridge, VPN Interface Cellular, VPN Interface Ethernet, VPN Interface GRE, VPN Interface PPP, or VPN Interface PPP Ethernet | vpn interface access-list  
vpn interface policer |
1. Create new lists of groups, as described in the following table:

Table 237:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Data Prefix | 1. In the left bar, click Data Prefix.  
2. Click New Data Prefix List.  
3. Enter a name for the list.  
4. Enter one or more IP prefixes.  
5. Click Add. |
| Mirror | 1. In the left bar, click Mirror.  
2. Click New Mirror List. The Mirror List popup displays.  
3. Enter a name for the list.  
4. In the Remote Destination IP field, enter the IP address of the destination to which to mirror the packets.  
5. In the Source IP field, enter the IP address of the source of the packets to mirror.  
6. Click Save. |
**List Type** | **Procedure**
---|---
Policer | 1. In the left bar, click Policer.
2. Click New Policer List.
3. Enter a name for the list.
4. In the Burst field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.
5. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. Select Drop (the default) to set the packet loss priority (PLP) to low. Select Remark to set the PLP to high.
6. In the Rate field, enter the maximum traffic rate. It can be value from 0 through $2^{64} - 1$ bps.
7. Click Add.

1. Click Next to move to Configure Forwarding Classes/QoS in the wizard.

**Step 3: Configure Forwarding Classes for QoS**

When you first open the Forwarding Classes/QoS screen, the QoS tab is selected by default:

To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
   1. In the QoS tab, click the Add QoS drop-down.
   2. Select Create New.
   3. Enter a name and description for the QoS mapping.
   4. Click Add Queue. The Add Queue popup displays.
   5. Select the queue number from the Queue drop-down.
   6. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.
   7. Click Save.

2. To import an existing QoS mapping:
   1. In the QoS tab, click the Add QoS drop-down.
   2. Select Import Existing.
   3. Select a QoS mapping.
   4. Click Import.

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the More Actions icon to the right of the row, and select the desired action.

4. To configure policy rewrite rules for the QoS mapping:
1. In the QoS tab, click the Add Rewrite Policy drop-down.
2. Select Create New.
3. Enter a name and description for the rewrite rule.
5. Select a class from the Class drop-down.
6. Select the priority (Low or High) from the Priority drop-down.
7. Enter the DSCP value (0 through 63) in the DSCP field.
8. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field.
9. Click Save.

5. To import an existing rewrite rule:
   1. In the QoS tab, click the Add Rewrite Policy drop-down.
   2. Select Import Existing.
   3. Select a rewrite rule.
   4. Click Import.

6. Click Next to move to Configure Access Lists in the wizard.

**Step 4: Configure ACLs**
1. In the Configure Access Control Lists screen, configure ACLs.
2. To create a new IPv4 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv4 ACL Policy:
3. Enter a name and description for the ACL.
4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.
5. Double-click the Access Control List box, and type a name for the ACL.
6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.

15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.

16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
   1. Click Default Action in the left pane.
   2. Click the Pencil icon.
   3. Change the default action to Accept.
   4. Click Save Match and Actions.

17. Click Next to move to Configure Route Policy in the wizard.

18. Click Next to move to the Policy Overview screen.

**Step 5: Configure Policy Settings**

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.

2. To enable cflowd visibility so that a vEdge router can perform traffic flow monitoring on traffic coming to the router from the LAN, click Netflow.

3. To enable application visibility so that a vEdge router can monitor and track the applications running on the LAN, click Application.

4. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from transport-side interfaces, click Cloud QoS.

5. To enable QoS scheduling and shaping for traffic that a vEdge Cloud router receives from service-side interfaces, click Cloud QoS Service Side.

6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.

7. To configure how often packet flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

8. Click Preview to view the full policy in CLI format.

9. Click Save Policy.

**Step 6: Apply a Localized Data Policy in a Device Template**

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.

   2. From the Create Template drop-down, select From Feature Template.

   3. From the Device Model drop-down, select one of the vEdge devices.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.


3. If you are editing an existing device template:
1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
3. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

**General CLI Configuration Procedure**

Following are the high-level steps for configuring an access list using the CLI:

1. Create lists of IP prefixes, as needed:
   ```
   vEdge(config)# policy
   vEdge(config-policy)# lists data-prefix-list
   list-name
   vEdge(config-data-prefix-list)# ip-prefix
   prefix/length
   ```

2. If you configure a logging action, configure how often to log packets to the syslog files:
   ```
   vEdge(config)# policy log-frequency
   number
   ```

3. For QoS, map each forwarding class to an output queue, configure a QoS scheduler for each forwarding class, and group the QoS schedulers into a QoS map:
   ```
   vEdge(config)# policy class-map
   vEdge(config-class-map)# class
   class-name
   queue
   number
   vEdge(config)# policy qos-scheduler
   scheduler-name
   vEdge(config-qos-scheduler)# class
   class-name
   vEdge(config-qos-scheduler)# bandwidth-percent
   percentage
   vEdge(config-qos-scheduler)# buffer-percent
   percentage
   vEdge(config-qos-scheduler)# drops
   drop-type
   ```
4. For QoS, define rewrite rules to overwrite the DSCP field of a packet's outer IP header, if desired:

```bash
vEdge(config)# policy rewrite-rule
rule-name
class class-name
loss-priority
dscp dscp-value layer-2-cos number
```

*class-name* is one of the classes defined under a *qos-scheduler* command.

5. Define mirroring parameters (for unicast traffic only):

```bash
vEdge(config)# policy mirror
mirror-name
remote-dest ip-address
source ip-address
```

6. Define policing parameters:

```bash
vEdge(config)# policy policer
policer-name
rate bandwidth
burst bytes
exceed action
```

7. Create an access list instance:

```bash
vEdge(config)# policy access-list
list-name
```

8. Create a series of match–action pair sequences:

```bash
vEdge(config-access-list)# sequence number
vEdge(config-sequence)#
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

9. Define match parameters for packets:

```bash
vEdge(config-sequence-number)# match match-parameter
```

10. Define actions to take when a match occurs:

```bash
vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count
```
counter-name
vEdge(config-sequence)# action log
class-name
vEdge(config-sequence)# action accept class
mirror-name
vEdge(config-sequence)# action accept mirror
policer-name
vEdge(config-sequence)# action accept policer
dscp
vEdge(config-sequence)# action accept set dscp
ipv4-address
vEdge(config-sequence)# action accept set next-hop

11. Create additional numbered sequences of match–action pairs within the access list, as needed.

12. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:

vEdge(config-policy-name)# default-action accept

13. Apply the access list to an interface:

vEdge(config)# vpn
vpn-id
interface
interface-name
vEdge(config-interface)# access-list list-name (in | out)

Applying the access list in the inbound direction (in) affects packets being received on the interface. Applying it in the outbound direction (out) affects packets being transmitted on the interface. For QoS, apply a DSCP rewrite rule to the same egress interface:

vEdge(config)# vpn
vpn-id
interface
interface-name
rewrite-rule rule-name

14. You can apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

vEdge(config)# vpn
vpn-id
interface
interface-name
vEdge(config-interface)# policer policer-name (in | out)

Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists, shown as they appear in the CLI and when you click Preview in the vManage localized policy configuration wizard. Each component is explained in the sections below.

<table>
<thead>
<tr>
<th>Policy</th>
<th>List</th>
<th>Data-Prefix</th>
<th>Prefix Length</th>
<th>Class-Map</th>
<th>Class Map</th>
<th>Cloud-QoS</th>
<th>Cloud-QoS Service-Side</th>
<th>Implicit-Acl-Logging</th>
<th>Log-Frequency</th>
<th>Number</th>
<th>Qos-Scheduler</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy</td>
<td>lists</td>
<td>data-prefix-list</td>
<td>list-name</td>
<td>ip-prefix</td>
<td>prefix/length</td>
<td>class-map</td>
<td>class</td>
<td>class</td>
<td>map</td>
<td>map</td>
<td>cloud-qos</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Lists

Access lists use prefix lists to group related prefixes.

In vManage NMS, you configure prefix lists from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest
- Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Data Prefix

In the CLI, you configure lists under the policy lists command hierarchy on vEdge routers.

Table 238:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data prefixes</td>
<td>List of one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple ip-prefix options, specifying one prefix in each option.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Data Prefix ► New Data Prefix List Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Data Prefix ► New Data Prefix List data-prefix-list list-name ip-prefix prefix/length</td>
</tr>
</tbody>
</table>

Logging Parameters

If you configure a logging action in a data policy, by default, the vEdge router logs all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In vManage NMS, you configure how often to log packet headers from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Log Frequency field

In the CLI, you configure this as follows:

vEdge(config)# policy log-frequency number
number specifies how often to log packet headers. The default value is 1000. number can be an integer, and the software rounds the value down to the nearest power of 2. So for example, with the default value of 1000, the logging frequency is rounded down to 512, so every 512th packet is logged.

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an allow-service command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In vManage NMS, you configure this logging from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Implicit ACL Logging field

In the CLI, you do this as follows:

vEdge(config)# policy implicit-acl-logging

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the log-frequency command.

QoS Parameters

In vManage NMS, you configure QoS parameters on vEdge routers from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Class Map, or Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Class Map
- Configuration ► Policies ► Localized Policy ► Add Policy ► Configuring Forwarding Classes/QoS, or Configuration ► Policies ► Custom Options ► Localized Policy ► Configuring Forwarding Classes/QoS
- Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview, or Configuration ► Policies ► Custom Options ► Localized Policy ► Policy Overview

This section explains how to configure QoS parameters from the CLI.

To configure QoS parameters on a vEdge router, first define a classification. In vManage NMS:

vEdge(config)# policy class-map class

class-name

queue

type number

class-name is the name of the class. It can be a text string from 1 through 32 characters long.

For hardware vEdge routers, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing (LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted round-robin (WRR).

For Cloud vEdge routers, each interface has four queues, numbered from 0 through 3. Queue 0 is reserved for control traffic, and queues 1, 2, and 3 are available for data traffic. The scheduling method for all four queues is WRR. LLQ is not supported.

To configure QoS parameters on a vEdge Cloud router, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the vEdge Cloud router receives from transport-side interfaces:

vEdgeCloud(config)# policy cloud-qos
To enable QoS parameters for traffic that the vEdge Cloud router receives from service-side interfaces:

```
vEdgeCloud(config)# policy cloud-qos-service-side
```

Next, configure scheduling:

```
vEdge(config)# policy qos-scheduler
scheduler-name

VEdge(config-qos-scheduler)# class
percentage

VEdge(config-qos-scheduler)# buffer-percent

VEdge(config-qos-scheduler)# drops
(red-drop | tail-drop)

VEdge(config-qos-scheduler)# scheduling (llq | wrr)
```

scheduler-name is the name of the QoS scheduler. It can be a text string from 1 through 32 characters long.

class-name is the name of the forwarding class and can be a text string from 1 through 32 characters long. The common class names correspond to the per-hop behaviors AF (assured forwarding), BE (best effort), and EF (expedited forwarding).

The bandwidth percentage is the percentage of the interface's bandwidth to allocate to the forwarding class. The sum of the bandwidth on all forwarding classes on an interface should not exceed 100 percent.

The buffer percentage is the percentage of the interface's buffering capacity to allocate to the forwarding class. The sum of the buffering capacity of all forwarding classes on an interface should not exceed 100 percent.

Packets that exceed the bandwidth or buffer percentage are dropped either randomly, using random early detection (red-drop), or from the end of the queue (tail-drop). Low-latency queuing (LLQ) cannot use random early detection.

The algorithm to schedule interface queues can be either low-latency queuing (llq) or weighted round-robin (wrr).

Then, assign the scheduler to a QoS map:

```
vEdge(config-policy)# qos-map map-name
qos-scheduler

VEdge(config-qos-scheduler)# scheduling (llq | wrr)
```

map-name is the name of the QoS map, and scheduler-name is the name of the scheduler you configured above. Each name can be a text string from 1 through 32 characters long.

Finally, to configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header:

```
vEdge(config)# policy rewrite-rule
rule-name

class

class-name loss-priority

dscp
dscp-value

layer-2-cos
tag-number

rule-name is the name of the rewrite rule. It can be a text string from 1 through 32 characters long.

class-name is the name of a class you configured with the qos-scheduler class command. The packet loss priority (PLP) can be either high or low. To have a DSCP value overwrite the DSCP field of the packet's outer IP header, set a value from 0 through 63. To include an 802.1p marking in the packet, specify a number from 0 through 7.
Mirroring Parameters

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In vManage NMS, you configure mirroring parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Mirror ► New Mirror List
- Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Mirror ► New Mirror List

In the CLI, you configure mirroring parameters as follows:

```vEdge(config)# policy mirror
mirror-name
vEdge(config-mirror)# remote-dest ip-address
source
ip-address```

Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In vManage NMS, you configure policer parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Policer ► New Policer List
- Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Policer ► New Policer List

In the CLI, you configure policer parameters as follows:

```vEdge(config)# policy policer
policer-name
vEdge(config-policer)# rate bps
vEdge(config-policer)# burst bytes
vEdge(config-policer)# exceed action```

- `rate` is the maximum traffic rate. It can be a value from 0 through \(2^{64} - 1\) bits per second.
- `burst` is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes
- `exceed` is the action to take when the burst size or traffic rate is exceeded. `action` can be `drop` (the default) or `remark`. The `drop` action is equivalent to setting the packet loss priority (PLP) bit to low. The `remark` action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the `match plp` option.

Sequences

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In vManage NMS, you configure sequences from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Add Access Control List Policy ► Add ACL Sequence
In the CLI, you configure sequences with the `policy access-list sequence` command.

Each sequence in an access list can contain one match condition and one action condition.

**Match Parameters**

Access lists can match IP prefixes and fields in the IP headers.

In vManage NMS, you configure match parameters from:

```
• Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Add Access Control List Policy ► Add ACL Sequence ► Add Sequence Rule ► Match

• Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control List Policy ► Add Access Control List Policy ► Add ACL Sequence ► Add Sequence Rule ► Match
```

In the CLI, you configure the match parameters with the `policy access-list sequence match` command.

Each sequence in an access-list must contain one match condition.

For access lists, you can match these parameters:

**Table 239:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification map</td>
<td>Match Class</td>
<td>Name of a class defined with a <code>policy class-map</code> command.</td>
</tr>
<tr>
<td></td>
<td><code>class class-name</code></td>
<td></td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td>Match Destination Data Prefix</td>
<td>Name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td></td>
<td><code>destination-data-prefix-list list-name</code></td>
<td></td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td>Not available in vManage NMS</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td></td>
<td><code>destination-ip prefix/length</code></td>
<td></td>
</tr>
<tr>
<td>Destination port number</td>
<td>Match Destination Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td></td>
<td><code>destination-port number</code></td>
<td></td>
</tr>
<tr>
<td>DSCP value</td>
<td>Match DSCP</td>
<td>0 through 63</td>
</tr>
<tr>
<td></td>
<td><code>dscp number</code></td>
<td></td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td>Match Protocol</td>
<td>0 through 255</td>
</tr>
<tr>
<td></td>
<td><code>protocol number</code></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/ CLI Configuration Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Packet length</td>
<td>Match Packet Length</td>
<td>Length of the packet. <em>number</em> can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td>Match Source Data Prefix</td>
<td>Name of a <em>data-prefix-list</em> list.</td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>Match PLP</td>
<td>*(high</td>
</tr>
<tr>
<td>Individual source prefix</td>
<td>Match Source Data Prefix</td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source port number</td>
<td>Match Source Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>TCP flag</td>
<td>Match TCP</td>
<td><em>syn</em></td>
</tr>
</tbody>
</table>

**Action Parameters**

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In vManage NMS, you configure match parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Add Access Control List Policy ► Add ACL Sequence ► Add Sequence Rule ► Action

In the CLI, you configure the actions parameters with the *policy access-list sequence action* command.

Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:
**Table 240:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the access list.</td>
<td>Click Accept accept</td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td>Action Counter Click Accept, then action Counter count counter-name</td>
<td>Name of a counter. To display counter information, use the <code>show policy access-lists counters</code> command on the vEdge router.</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click Drop drop</td>
<td>—</td>
</tr>
<tr>
<td>Log the packet headers into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td>Action Log Click Accept, then action Log log</td>
<td>To display logging information, use the <code>show app log flow-all</code>, <code>show app log flows</code>, and <code>show log</code> commands on the vEdge router.</td>
</tr>
</tbody>
</table>

For a packet that is accepted, the following actions can be configured:

**Table 241:**

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify the packet.</td>
<td>Click Accept, then Class class class-name</td>
<td>Name of a QoS class defined with a <code>policy class-map</code> command.</td>
</tr>
<tr>
<td>Mirror the packet.</td>
<td>Click Accept, then Mirror List mirror mirror-name</td>
<td>Name of mirror defined with a <code>policy mirror</code> command.</td>
</tr>
<tr>
<td>Police the packet.</td>
<td>Click Accept, then Policer policer policer-name</td>
<td>Name of a policer defined with a <code>policy policer</code> command.</td>
</tr>
<tr>
<td>Packet's DSCP value.</td>
<td>Click Accept, then DSCP set dscp value</td>
<td>0 through 63.</td>
</tr>
<tr>
<td>Next-hop address.</td>
<td>Click Accept, then Next Hop set next-hop ipv4-address</td>
<td>IPv4 address.</td>
</tr>
</tbody>
</table>
Default Action

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped.

In vManage NMS, you modify the default action from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Default Action
- Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control List Policy ► Default Action

In the CLI, you modify this behavior with the `access-list default-action accept` command.

Apply Access Lists

For an access list to take effect, you must apply it to an interface.

In vManage NMS, you apply the access list in one of these interface feature configuration templates:

- Configuration ► Templates ► VPN Interface Bridge
- Configuration ► Templates ► VPN Interface Cellular
- Configuration ► Templates ► VPN Interface Ethernet
- Configuration ► Templates ► VPN Interface GRE
- Configuration ► Templates ► VPN Interface PPP
- Configuration ► Templates ► VPN Interface PPP Ethernet

In the CLI, you apply the access list as follows:

```
veEdge(config)# vpn
vpn-id
interface
  interface-name
veEdge(config-interface)# access-list
list-name (in | out)
```

Applying the policy in the inbound direction (in) affects prefixes being received on the interface. Applying it in the outbound direction (out) affects prefixes being transmitted on the interface.

For an access list that applies QoS classification, apply any DSCP rewrite rules to the same interface to which you apply the access list:

```
veEdge(config)# vpn
vpn-id
interface
  interface-name
veEdge(config-interface)# rewrite-rule
rule-name
```

Note that you can also apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

```
veEdge(config)# vpn
vpn-id
interface
```
Interaction between Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the `policy access-list` command are called explicit ACLs. You can apply explicit ACLs to any interface in any VPN on the router.

The router's tunnel interfaces in VPN 0 also have implicit ACLs, which are also referred to as services. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the `allow-service` command:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface
interface-name
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# allow-service
service-name
```

On vEdge routers, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (allow-service) or deny (no allow-service). Allowing a service in an implicit ACL is the same as specifying the accept action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the drop action in an explicit ACL.
- Whether, in an explicit ACL, the accept or deny action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

<table>
<thead>
<tr>
<th>Implicit ACL</th>
<th>Explicit ACL: Sequence</th>
<th>Explicit ACL: Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
<td>—</td>
<td>Deny (drop)</td>
</tr>
<tr>
<td>Allow (accept)</td>
<td>—</td>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
<td>—</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>—</td>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
</tr>
</tbody>
</table>
Configuring Localized Data Policy for IPv6

This article provides procedures for configuring IPv6 localized data policy. This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply mirroring and policing to data packets.

For IPv6, you can apply access lists only to interfaces in the transport VPN, VPN 0.

In vManage NMS, you configure localized data policy from the Configuration ▶ Policies screen, using a policy configuration wizard. In the CLI you configure these policies on the vEdge router.

Configuration Components

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for IPv6 access lists:

To create an IPv6 access list, you include the following components in the configuration on a vEdge router:

**Table 243:**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Frequency</td>
<td>If you configure a logging action, log only a sample of data packet headers instead of all of them.</td>
<td>Configuration ▶ Policies ▶ Localized Policy ▶ Add Policy ▶ Policy Overview ▶ Log Frequency</td>
<td>policy logging-frequency</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>vManage Configuration</td>
<td>CLI Configuration Command</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Mirroring and policing parameters</td>
<td>Parameters and rules required to configure traffic mirroring and policing. For mirroring, you configure the addresses of the source of the packets to be mirrored and the mirroring site. (You can mirror only unicast traffic.) For policing, you define transmission parameters.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest or Configuration ► Policies ► Custom Options ► Localized Policy ► Create Groups of Interest</td>
<td>policy mirror policy policer</td>
</tr>
<tr>
<td>Access list instance</td>
<td>Container for an access list.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists or Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control Lists</td>
<td>policy ipv6 access-list</td>
</tr>
<tr>
<td>Numbered sequences of match–action pairs</td>
<td>Sequences establish the order in which the policy components are applied.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists or Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control Lists</td>
<td>policy ipv6 access-list sequence</td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists or Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control Lists</td>
<td>policy ipv6 access-list sequence match</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching packets, and how to process matching items.</td>
<td>Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists or Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control Lists</td>
<td>policy ipv6 access-list sequence action</td>
</tr>
</tbody>
</table>
### CLI Configuration

**Component** | **Description** | **vManage Configuration** | **CLI Configuration Command**
---|---|---|---
Default action | Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped. | Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists or Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control Lists | policy ipv6 access-list default-action

**Application of access lists** | For an access list to take effect, you apply it an interface. | Configuration ► Templates ► Feature ► VPN Interface Bridge, VPN Interface Cellular, VPN Interface Ethernet, VPN Interface GRE, VPN Interface PPP, or VPN Interface PPP Ethernet | vpn 0 interface ipv6 access-list

### General vManage Configuration Procedure

To configure IPv6 localized data policy, use the vManage policy configuration wizard. The wizard is a UI policy builder that consists of five screens, and you use four of them to configure IPv6 localized policy components:

- Groups of Interest, also called lists—Create data prefix lists and mirroring and policer parameters that group together related items and that you call in the match or action components of a policy.

- Access Control Lists—Define the match and action conditions of ACLs.

- Route Policies—Define the match and action conditions of route policies.

- Policy Settings—Define additional policy settings, including the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

### Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Select the Localized Policy tab.
3. Click Add Policy. The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

### Step 2: Create Groups of Interest

In the Create Groups of interest screen create lists to use in the localized data policy:
1. Create new lists of groups, as described in the following table:
Table 244:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Mirror    | 1. In the left bar, click TLOC.  
2. Click New TLOC List. The TLOC List popup displays.  
3. Enter a name for the list.  
4. In the TLOC IP field, enter the system IP address for the TLOC.  
5. In the Color field, select the TLOC’s color.  
6. In the Encap field, select the encapsulation type.  
7. In the Preference field, optionally select a preference to associate with the TLOC.  
8. Click Add TLOC to add another TLOC to the list.  
9. Click Save. |
| Policier  | 1. In the left bar, click VPN.  
2. Click New VPN List.  
3. Enter a name for the list.  
4. In the Add VPN field, enter one or more VPN IDs separated by commas.  
5. Click Add. |

1. Click Next to move to Configure Forwarding Classes/QoS in the wizard. For IPv6 localized data policy, you cannot configure QoS.

2. Click Next to move to Configure Access Lists in the wizard.

**Step 3: Configure ACLs**

In the Configure Access Control Lists screen, configure ACLs:
1. In the Configure Access Control Lists screen, configure ACLs:
2. To create a new IPv6 ACL, click the Add Access Control List Policy drop-down. Then select Add IPv6 ACL Policy:
3. Enter a name and description for the ACL.
4. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.
5. Double-click the Access Control List box, and type a name for the ACL.
6. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. The Match tab is selected by default.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
13. Click Save Match and Actions to save a sequence rule.
14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename an ACL sequence rule, in the left pane, click More Options next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
   1. Click Default Action in the left pane.
   2. Click the Pencil icon.
   3. Change the default action to Accept.
   4. Click Save Match and Actions.
17. Click Next to move to Configure Route Policy in the wizard.
18. Click Next to move to the Policy Overview screen.

**Step 4: Configure Policy Settings**

In Policy Overview, configure policy settings:
1. Enter a name and description for the ACL.

2. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click Implicit ACL Logging.

3. To configure how often packet flows are logged, click Log Frequency. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

4. Click Preview to view the full policy in CLI format.

5. Click Save Policy.

**Step 5: Apply a Localized Data Policy in a Device Template**

1. On vManage NMS, select the Configuration ► Templates screen.
2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the vEdge devices.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.
   4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.
   5. From the Policy drop-down, select the name of the policy you configured in the above procedure.
   6. Click Create (for a new template) or Update (for an existing template).

**General CLI Configuration Procedure**

Following are the high-level steps for configuring an access list using the CLI:

1. Define mirroring parameters (for unicast traffic only):
   ```
   vEdge(config)# policy mirror
   mirror-name
   vEdge(config-mirror)# remote-dest
   ip-address
   source
   ip-address
   ```

2. Define policing parameters:
   ```
   vEdge(config)# policy policer
   policer-name
   vEdge(config-policer)# rate
   bandwidth
   vEdge(config-policer)# burst
   bytes
   vEdge(config-policer)# exceed
   action
   ```
3. Create an access list instance:
   ```
   vEdge(config)# policy ipv6 access-list
   list-name
   ```

4. Create a series of match–action pair sequences:
   ```
   vEdge(config-ipv6-access-list)# sequence
   vEdge(config-sequence)#
   ```
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for packets:
   ```
   vEdge(config-sequence-number)# match match-parameter
   ```

6. Define actions to take when a match occurs:
   ```
   vEdge(config-sequence)# action drop
   vEdge(config-sequence)# action count
   vEdge(config-sequence)# action log
   vEdge(config-sequence)# action accept class
   vEdge(config-sequence)# action accept mirror
   vEdge(config-sequence)# action accept policer
   ```

7. Create additional numbered sequences of match–action pairs within the access list, as needed.

8. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:
   ```
   vEdge(config-policy-name)# default-action accept
   ```

9. Apply the access list to an interface:
   ```
   vEdge(config)# vpn
   vpn-id
   interface
   interface-name
   vEdge(config-interface)# ipv6 access-list
   list-name (in | out)
   ```
   Applying the access list in the inbound direction (in) affects packets being received on the interface. Applying it in the outbound direction (out) affects packets being transmitted on the interface.

**Structural Components of Configuration for Access Lists**

Following are the structural components required to configure access lists. Each one is explained in more detail in the sections below:

```
policy
   implicit-acl-logging
```
### Logging Parameters

If you configure a logging action in a data policy, by default, the vEdge router logs all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In vManage NMS, you configure how often to log packet headers from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Log Frequency field

In the CLI, you configure this as follows:

```
vEdge(config)# policy log-frequency
```

`number` specifies how often to log packet headers. The default value is 1000. `number` can be an integer, and the software rounds the value down to the nearest power of 2. So for example, with the default value of 1000, the logging frequency is rounded down to 512, so every 512th packet is logged.

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an `allow-service` command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In vManage NMS, you configure this logging from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Policy Overview ► Implicit ACL Logging field
In the CLI, you do this as follows:

```plaintext
vEdge(config)# policy implicit-acl-logging
```

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the `log-frequency` command.

**Mirroring Parameters**

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In vManage NMS, you configure mirroring parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Mirror ► New Mirror List
- Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Mirror ► New Mirror List

In the CLI, you configure mirroring parameters as follows:

```plaintext
vEdge(config)# policy mirror
mirror-name
vEdge(config-mirror)# remote-dest
    ip-address
vEdge(config-mirror)# source
    ip-address
```

**Policer Parameters**

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In vManage NMS, you configure policer parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Create Groups of Interest ► Policer ► New Policer List
- Configuration ► Policies ► Custom Options ► Localized Policy ► Lists ► Policer ► New Policer List

In the CLI, you configure policer parameters as follows:

```plaintext
vEdge(config)# policy policer
policer-name
vEdge(config-policer)# rate
    bps
vEdge(config-policer)# burst
    bytes
vEdge(config-policer)# exceed
    action
```

`rate` is the maximum traffic rate. It can be a value from 0 through $2^{64} - 1$ bits per second.
burst is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes.

exceed is the action to take when the burst size or traffic rate is exceeded. action can be drop (the default) or remark. The drop action is equivalent to setting the packet loss priority (PLP) bit to low. The remark action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the match plp option.

Sequences
An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In vManage NMS, you configure sequences from:


In the CLI, you configure sequences with the `policy ipv6 access-list sequence` command.

Each sequence in an access list can contain one match condition and one action condition.

Match Parameters
Access lists can match IP prefixes and fields in the IP headers.

In vManage NMS, you configure match parameters from:


In the CLI, you configure the match parameters with the `policy ipv6 access-list sequence match` command.

Each sequence in an access-list must contain one match condition.

For access lists, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination port number</td>
<td>Match Destination Port number ( destination-port number )</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Next header protocol</td>
<td>Match Protocol number ( next-header number )</td>
<td>0 through 255, corresponding to an Internet Protocol number</td>
</tr>
</tbody>
</table>
### Table 246: Value or Range

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet length</td>
<td>Match Packet Length <code>packet-length number</code></td>
<td>Length of the packet. <code>number</code> can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>Match PLP <code>plp</code></td>
<td>(high</td>
</tr>
<tr>
<td>Source port number</td>
<td>Match Source Port <code>source-port address</code></td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
</tr>
<tr>
<td>TCP flag</td>
<td>Match TCP <code>tcp flag</code></td>
<td>syn</td>
</tr>
<tr>
<td>Traffic class</td>
<td>Match Class <code>traffic-class value</code></td>
<td>0 through 63</td>
</tr>
</tbody>
</table>

### Action Parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In vManage NMS, you configure match parameters from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Add Access Control List Policy ► Add ACL Sequence ► Add Sequence Rule ► Action

In the CLI, you configure the actions parameters with the `policy ipv6 access-list sequence action` command. Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

### Table 247:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the access list.</td>
<td>Click Accept accept</td>
<td>——</td>
</tr>
</tbody>
</table>
Count the accepted or dropped packets. | Action Counter | Name of a counter. To display counter information, use the `show ipv6 policy access-lists counters` command on the vEdge router.

Discard the packet. This is the default action. | Click Drop | —

Log the packet headers into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. | Action Log | To display logging information, use the `show app log flow-all` and `show app log flows` command on the vEdge router.

For a packet that is accepted, the following actions can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/ CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror the packet.</td>
<td>Click Accept, then Mirror List <code>mirror</code> <code>mirror-name</code></td>
<td>Name of mirror defined with a <code>policy mirror</code> command.</td>
</tr>
<tr>
<td>Police the packet.</td>
<td>Click Accept, then Policer <code>policer</code> <code>policer-name</code></td>
<td>Name of a policer defined with a <code>policy policer</code> command.</td>
</tr>
<tr>
<td>Set the packet's DSCP value.</td>
<td>Click Accept, then Class <code>set traffic-class</code> <code>value</code></td>
<td>0 through 63.</td>
</tr>
</tbody>
</table>

**Default Action**

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped.

In vManage NMS, you modify the default action from:

- Configuration ► Policies ► Localized Policy ► Add Policy ► Configure Access Control Lists ► Default Action
- Configuration ► Policies ► Custom Options ► Localized Policy ► Access Control List Policy ► Default Action

In the CLI, you modify this behavior with the `access-list ipv6 default-action accept` command.
Applying Access Lists

For an access list to take effect, you must apply it to a tunnel interface in VPN 0.

In vManage NMS, you apply the access list in one of these interface feature configuration templates:

- Configuration ► Templates ► VPN Interface Bridge
- Configuration ► Templates ► VPN Interface Cellular
- Configuration ► Templates ► VPN Interface Ethernet
- Configuration ► Templates ► VPN Interface GRE
- Configuration ► Templates ► VPN Interface PPP
- Configuration ► Templates ► VPN Interface PPP Ethernet

In the CLI, you apply the access list as follows:

```
vEdge(config)# vpn 0
  interface
    interface-name
vEdge(config-interface)# ipv6 access-list
    list-name {in | out}
```

Applying the policy in the inbound direction (in) affects prefixes being received on the interface. Applying it in the outbound direction (out) affects prefixes being transmitted on the interface.

Interaction between Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the `policy access-list` command are called explicit ACLs. You can apply explicit ACLs to any interface in any VPN on the router.

The router’s tunnel interfaces in VPN 0 also have implicit ACLs, which are also referred to as services. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the `allow-service` command:

```
vEdge(config)# vpn 0
vEdge(config-vpn)# interface
  interface-name
vEdge(config-interface)# tunnel-interface
vEdge(config-tunnel-interface)# allow-service
  service-name
vEdge(config-tunnel-interface)# no allow-service
  service-name
```

On vEdge routers, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (`allow-service allow-service`) or deny (`no allow-service service-name`). Allowing a service in an implicit ACL is the same as specifying the `accept` action in an
explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the **drop** action in an explicit ACL.

- Whether, in an explicit ACL, the **accept** or **deny** action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

**Table 248:**

<table>
<thead>
<tr>
<th>Implicit ACL</th>
<th>Explicit ACL: Sequence</th>
<th>Explicit ACL: Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
<td>—</td>
<td>Deny (drop)</td>
</tr>
<tr>
<td>Allow (accept)</td>
<td>—</td>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
<td>—</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>—</td>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
</tr>
</tbody>
</table>

**Configuring Centralized Data Policy**

This section provides general procedures for configuring centralized data policy on vSmart controllers. Centralized data policy can be used for different purposes, which are described in the sections that follow.

**Overview**

To base policy decisions on source and destination prefixes and on the headers in the IP data packets, you use centralized data policy, which you configure with the **policy data-policy** command. The vSmart controller pushes this type of data policy to the vEdge routers. In domains with multiple vSmart controllers, all the controllers must have the same centralized data policy configuration to ensure that traffic flow within the overlay network remains synchronized.

To base policy decisions on the application information in the packet payload, you use centralized data policy to perform deep packet inspection. You configure this by creating lists of applications with the **policy lists app-list** command and then calling these lists in a **policy data-policy** command. To specify the path that application traffic takes through the network, you can set the local TLOC or the remote TLOC, or both, to use to send the traffic over.

To configure the VPNSs that vEdge routers are allowed to receive routes from, you use centralized data policy, which you configure with the **policy vpn-membership** command. VPN membership policy affects which routes the vSmart controller sends to the vEdge router. The policy itself remains on the vSmart controller and is not pushed to the vEdge routers.
Configuring Centralized Data Policy Based on Prefixes and IP Headers

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is dropped and discarded by default.

Configuration Components

The following figure illustrates the configuration components for centralized data policy:

To create a centralized data policy to filter based on IP prefixes and IP packet headers, you include the following components in the configuration on a vSmart controller:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>policy data-policy vpn-list default-action</td>
</tr>
<tr>
<td></td>
<td>policy conditions.</td>
<td>(Traffic Data</td>
<td>Cflowd) &gt; Sequence Type &gt; Default Action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Traffic Policy &gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
<tr>
<td>Network topology</td>
<td>Conditions that define the network topology.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Topology and VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Membership &gt; Add Topology</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Topology</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>vManage Configuration</td>
<td>CLI Configuration Command</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
<tr>
<td>Centralized data policy instance</td>
<td>Container for centralized data policy that filters packets based on IP prefix and IP packet header fields.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy</td>
<td>policy data-policy</td>
</tr>
<tr>
<td>Application of centralized data policy</td>
<td>For a data policy to take effect, you apply it to one or more sites in the overlay network.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Apply Policies to Sites and VPNs</td>
<td>apply-policy site-list data-policy</td>
</tr>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the data policy configuration. For centralized data policy, you can group applications, IP prefixes, sites, TLOCs, and VPNs.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists</td>
<td>policy lists</td>
</tr>
<tr>
<td>Centralized data policy instance</td>
<td>Container for centralized data policy that filters packets based on IP prefix and IP packet header fields.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy</td>
<td>policy data-policy</td>
</tr>
<tr>
<td>VPN list</td>
<td>List of VPNs to which to apply the centralized data policy.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Topology and VPN Membership &gt; Add Topology &gt; &lt;topology_type&gt; or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Topology</td>
<td>policy data-policy vpn-list</td>
</tr>
<tr>
<td>Network topology</td>
<td>Conditions that define the network topology.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Topology and VPN Membership &gt; Add Topology or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Topology</td>
<td>—</td>
</tr>
</tbody>
</table>
### Configuring Centralized Data Policy Based on Prefixes and IP Headers

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbered sequences of match-action pairs</td>
<td>Sequences that establish the order in which the policy components are applied.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject (and drop) matching packets, and how to process matching packets.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the policy conditions.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Configure Traffic Rules &gt; (Application-Aware Routing</td>
<td>Traffic Data</td>
</tr>
</tbody>
</table>
General vManage Configuration Procedure

To configure centralized data policies, use the vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

- **Create Groups of Interest** — Create lists that group together related items and that you call in the match or action components of a policy.
- **Configure Topology** — Create the network structure to which the policy applies.
- **Configure Traffic Rules** — Create the match and action conditions of a policy.
- **Apply Policies to Sites and VPNs** — Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For a centralized data policy to take effect, you must activate the policy.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

**Step 1**  In vManage NMS, select the **Configure > Policies** screen.
**Step 2**  Select the Centralized Policy tab.
**Step 3**  Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen displays.

Step 1: Create Groups of Interest

You can create lists of groups to use in centralized policy.

---

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of centralized data</td>
<td>For a data policy to take effect, you apply it to one or more sites in the</td>
<td>Configuration ► Policies ► Centralized Policy ► Add Policy ► Apply Policies to Sites and</td>
<td>apply-policy site-list data-policy</td>
</tr>
<tr>
<td>policy</td>
<td>overlay network.</td>
<td>VPNs</td>
<td></td>
</tr>
</tbody>
</table>

---
Step 1: Create Groups of Interest

Create new lists, as described in the following table:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>1.  In the left bar, click <strong>Application</strong>.</td>
</tr>
<tr>
<td></td>
<td>2.  Click <strong>New Application List</strong>.</td>
</tr>
<tr>
<td></td>
<td>3.  Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4.  Click either the <strong>Application</strong> or <strong>Application Family</strong> button.</td>
</tr>
<tr>
<td></td>
<td>5.  From the Select drop-down, select the desired applications or application families.</td>
</tr>
<tr>
<td></td>
<td>6.  Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>Two application lists are preconfigured. You cannot edit or delete these lists.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Google Apps</strong>—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Microsoft Apps</strong>—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.</td>
</tr>
<tr>
<td>Data Prefix</td>
<td>1.  In the left bar, click <strong>Data Prefix</strong>.</td>
</tr>
<tr>
<td></td>
<td>2.  Click <strong>New Data Prefix List</strong>.</td>
</tr>
<tr>
<td></td>
<td>3.  Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4.  In the Add Data Prefix field, enter one or more data prefixes separated by commas.</td>
</tr>
<tr>
<td></td>
<td>5.  Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>List Type</td>
<td>Procedure</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| **Policer** | 1. In the left bar, click **Policer**.  
2. Click **New Policer List**.  
3. Enter a name for the list.  
4. Define the policing parameters:  
   1. In the Burst field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.  
   2. In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. It can be drop, which sets the packet loss priority (PLP) to low, or remark, which sets the PLP to high.  
   3. In the Rate field, enter the maximum traffic rate, a value from 0 through \(2^{64} - 1\) bits per second (bps).  
5. Click **Add**. |
| **Prefix** | 1. In the left bar, click **Prefix**.  
2. Click **New Prefix List**.  
3. Enter a name for the list.  
4. In the Add Prefix field, enter one or more data prefixes separated by commas.  
5. Click **Add**. |
| **Site** | 1. In the left bar, click **Site**.  
2. Click **New Site List**.  
3. Enter a name for the list.  
4. In the Add Site field, enter one or more site IDs separated by commas.  
5. Click **Add**. |
### List Type | Procedure
--- | ---
TLOC | 1. In the left bar, click TLOC.
2. Click New TLOC List. The TLOC List popup displays.
3. Enter a name for the list.
4. In the TLOC IP field, enter the system IP address for the TLOC.
5. In the Color field, select the TLOC's color.
6. In the Encap field, select the encapsulation type.
7. In the Preference field, optionally select a preference to associate with the TLOC.
8. Click Add TLOC to add another TLOC to the list.
9. Click Save.

**Note** The following IPv4/IPv6 data policy actions are not supported in this release: local-tloc, local-tloc-list, remote-tloc, remote-tloc-list.

VPN | 1. In the left bar, click VPN.
2. Click New VPN List.
3. Enter a name for the list.
4. In the Add VPN field, enter one or more VPN IDs separated by commas.
5. Click Add.

### Step 2: Configure the Network Topology

When you first open the Configure Topology and VPN Membership screen, the **Topology** tab is selected by default.

To configure the network topology and VPN membership:

**Hub and Spoke**

**Step 1** In the Add Topology drop-down, select **Hub and Spoke**.
**Step 2** Enter a name for the hub-and-spoke policy.
**Step 3** Enter a description for the policy.
**Step 4** In the VPN List field, select the VPN list for the policy.
**Step 5** In the left pane, click **Add Hub and Spoke**. A hub-and-spoke policy component containing the text string *My Hub-and-Spoke* is added in the left pane.
**Step 6** Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component.
**Step 7** In the right pane, add hub sites to the network topology:
a) Click **Add Hub Sites**.
b) In the **Site List Field**, select a site list for the policy component.
c) Click **Add**.
d) Repeat these steps to add more hub sites to the policy component.

**Step 8**
In the right pane, add spoke sites to the network topology:
a) Click **Add Spoke Sites**.
b) In the **Site List Field**, select a site list for the policy component.
c) Click **Add**.
d) Repeat these steps to add more spoke sites to the policy component.

**Step 9**
Repeat steps as needed to add more components to the hub-and-spoke policy.

**Step 10**
Click **Save Hub and Spoke Policy**.

---

**Mesh**

Policy for a topology with a partial-mesh or full-mesh region.

**Step 1**
In the Add Topology drop-down, select **Mesh**.

**Step 2**
Enter a name for the mesh region policy component.

**Step 3**
Enter a description for the mesh region policy component.

**Step 4**
In the **VPN List** field, select the VPN list for the policy.

**Step 5**
Click **New Mesh Region**.

**Step 6**
In the **Mesh Region Name** field, enter a name for the individual mesh region.

**Step 7**
In the **Site List** field, select one or more sites to include in the mesh region.

**Step 8**
Repeat these steps to add more mesh regions to the policy.

**Step 9**
Click **Save Mesh Region**.

---

**Custom Control (Route and TLOC)**

Policy for a topology with custom route and TLOC configuration.

**Step 1**
In the Add Topology drop-down, select **Custom Control (Route & TLOC)**.

**Step 2**
Enter a name for the custom control policy component.

**Step 3**
Enter a description of the custom control policy component.

**Step 4**
Click **Sequence Type**. The Add Control Policy popup displays.

**Step 5**
Click **Route** or **TLOC** to create a policy of that type.

**Step 6**
Click **Sequence Rule**.

---

**Custom Control (Route)**

Create a policy to apply on an OMP route. By default, the Match tab is selected, displaying match condition options.
Step 1  From the Add Custom Control Policy screen, click Route.
Step 2  Click Sequence Rule. Match and Actions options display.
Step 3  From the Match tab, select and configure match conditions for your route.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color List</td>
<td>Select a color list to match, or click New Color List to create a new list:</td>
</tr>
<tr>
<td></td>
<td>1. Enter a name for the Color list.</td>
</tr>
<tr>
<td></td>
<td>2. From the Select Color drop-down menu, select the color(s) you want included in your list.</td>
</tr>
<tr>
<td></td>
<td>3. Click Save.</td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Enter the OMP route tag, a number between 0-4294967295.</td>
</tr>
<tr>
<td>Origin</td>
<td>Select an origin for the route from the drop-down menu. Options include Aggregate, BGP External, BGP Internal, Connected, OSPF Inter-Area, OSPF Intra-Area, OSPF External 1, OSPF External 2, and Static.</td>
</tr>
<tr>
<td>Originator</td>
<td>Enter the IP address of the originator of this route.</td>
</tr>
<tr>
<td>Preference</td>
<td>Enter the preference number for the route, a number between 0-4294967295.</td>
</tr>
<tr>
<td>Site</td>
<td>Select a site list from the list of options., or create a new site list:</td>
</tr>
<tr>
<td></td>
<td>1. Enter a name for the Site list.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the Site numbers, following the example.</td>
</tr>
<tr>
<td></td>
<td>3. Click Save.</td>
</tr>
<tr>
<td>TLOC</td>
<td>Select a TLOC list to match, or create a new TLOC list:</td>
</tr>
<tr>
<td></td>
<td>1. Enter a name for the TLOC list.</td>
</tr>
<tr>
<td></td>
<td>2. In the TLOC IP field, enter the IP address for the TLOC.</td>
</tr>
<tr>
<td></td>
<td>3. In the Color drop-down menu, select the color you want to apply to the TLOC list.</td>
</tr>
<tr>
<td></td>
<td>4. From the Encap drop-down menu, select the encapsulation type for the TLOC list.</td>
</tr>
<tr>
<td></td>
<td>5. In the Preference field, enter the preference number for the route, a number between 0-4294967295.</td>
</tr>
<tr>
<td></td>
<td>6. Optionally, click Add TLOC and repeat steps 1-5 to open another TLOC list.</td>
</tr>
<tr>
<td></td>
<td>7. Click Save.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| VPN             | 1. From the Match Conditions ► VPN list field, select a VPN list, or click New VPN List to create a new one:  
2. Enter a name for the VPN List.  
3. In the VPN field, enter the VPN numbers, for example, 100 or 200 separated by commas, or 1000-2000 by range.  
4. Click Save. |
| Prefix List     | From the Match Conditions ► Prefix List field, select a Prefix list, or click New Prefix List to create a new one:  
1. From the Prefix List drop-down menu, select a prefix list, or create a new one.  
2. In the Add Prefix field, enter the IP prefixes, or click Import on the right to import prefixes.  
3. Click Save.  
**Note:** The Prefix List option is not available if you select protocol Both (IPv4 and IPv6). |

**Step 4**  
From the Actions tab, select IPv4, IPv6, or Both, to designate which protocol the actions should apply to. Not all of the following options are available for all protocols.

**Step 5**  
Click Accept or Reject for the IP traffic meeting the match conditions:
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Conditions</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Allow traffic from the selected protocol. Click the following menu buttons to open configuration fields:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export To</td>
<td>Select a VPN list, or create a new one.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Enter the OMP route tag, a number between 0-4294967295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preference</td>
<td>Enter the preference number for the route, a number between 0-4294967295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Enter the following information:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Select a service type. Options are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Prevention</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Service 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Service 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Service 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Service 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Service 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Enter the number of the Service VPN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC IP</td>
<td>Enter the IP address of the Service TLOC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Color</td>
<td>Select a Color type from the drop-down list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Select IPSEC or GRE as the encapsulation type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC List</td>
<td>Select a service TLOC list from the drop-down menu, or create a new one.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLOC Action</td>
<td>Select an action from the drop-down menu.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strict</td>
<td>Direct matching traffic only to the intermediate destination. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action action in a centralized control policy, strict is the default behavior.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary</td>
<td>First direct matching traffic to the intermediate destination. If that router is not reachable, then direct it to the final destination. With this action, if the intermediate destination is down, all traffic reaches the final destination.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>First direct matching traffic to the final destination. If that router is not reachable, then direct it to the intermediate destination. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Custom Control (TLOC)

Create a policy to apply to a TLOC. By default, the Match tab is selected, displaying match condition options.

**Step 1**
From the Add Custom Control Policy screen, click TLOC.

**Step 2**
Click Sequence Rule. Match and Actions options display.

**Step 3**
From the Match tab, select and configure match conditions for your route.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier</td>
<td>Select a carrier from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Color List</td>
<td>Select a color list from the drop-down list, or create a new one.</td>
<td></td>
</tr>
<tr>
<td>Domain ID</td>
<td>Enter a domain ID number, between 1-4294967295.</td>
<td></td>
</tr>
<tr>
<td>Group ID</td>
<td>Enter a Group ID number, between 1-4294967295.</td>
<td></td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Enter an OMP tag number, between 1-4294967295.</td>
<td></td>
</tr>
<tr>
<td>Originator</td>
<td>Enter the IP address of the originator of the TLOC.</td>
<td></td>
</tr>
<tr>
<td>Preference</td>
<td>Enter a preference number for the policy, between 1-4294967295.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Equal Cost Multi-path**
Equally direct matching control traffic between the intermediate destination and the ultimate destination. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.

**TLOC**
Enter the following information:

- **TLOC List**: Select a TLOC list, or create a new one.
- **TLOC IP**: Enter the IP address of the designated TLOC.
- **Color**: Select a color from the available options.

**Encapsulation**
Select IPSEC or GRE as the encapsulation type.

**Reject**
Reject traffic for the selected conditions.

1. Select a protocol from the **Protocol** dropdown: IPv4, IPv6, or Both.
2. Click **Accept** or **Reject** for the match conditions.
3. Optionally, repeat these steps with a different protocol.

Click **Save Match and Actions**.
### Match Condition

<table>
<thead>
<tr>
<th>Description</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site List</td>
<td>Select a site list from the drop-down list, create a new one, or enter a site ID in the Site ID field, between 1-4294967295.</td>
<td></td>
</tr>
</tbody>
</table>
| TLOC        | 1. Select a TLOC from the drop-down list, or create a new one.  
             | 2. Enter the following values: | |
| TLOC IP     | Enter the IP address of the TLOC. | |
| Color       | Select a color list from the available options. | |
| Encapsulation | Select IPSEC or GRE as the encapsulation type. | |

### Step 4
Click **Accept** or **Reject** to apply the following match conditions to an action.

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| Accept           | Allow traffic from the selected protocol. Click the following menu buttons to open configuration fields:  
|                  | OMP Tag | Enter an OMP tag number, between 1-4294967295. | |
|                  | Preference | Enter a preference number for the policy, between 1-4294967295. | |
| Reject           | Reject traffic for the selected conditions. | |

### Import Existing Topology

You can select an existing topology to use in your policy.

**Step 1**
In the Add Topology drop-down, select **Import Existing Topology** to open the matching popup.

**Step 2**
Under Policy Type, click the topology type you want to import:

- Hub and Spoke
- Mesh
- Custom

**Step 3**
Select a policy from the field list. vManage populates this field from the available topologies for the type you select.

**Step 4**
Click **Import**.

**Step 5**
Click **Save Control Policy** to save the Route policy.

### Create a VPN Membership Policy

You can create a VPN membership policy for the topology.

**Step 1**
In the Topology bar, click **VPN Membership**. Then:
Step 2: Configure Traffic Rules

When you first open the Traffic Rules screen, the Application-Aware Routing tab is selected by default. To configure traffic rules for deep packet inspection, see Configuring Deep Packet Inspection, on page 724.

To configure traffic rules for centralized data policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In the Application-Aware Routing bar, click the Traffic Data tab.</td>
</tr>
<tr>
<td>2</td>
<td>Click the Add Policy drop-down.</td>
</tr>
<tr>
<td>3</td>
<td>Click Create New. The Add Data Policy screen displays.</td>
</tr>
<tr>
<td>4</td>
<td>Enter a name and description for the data policy.</td>
</tr>
<tr>
<td>5</td>
<td>In the right pane, click Sequence Type. The Add Data Policy popup opens.</td>
</tr>
<tr>
<td>6</td>
<td>Select the type of data policy you want to create. Choices are: Application Firewall, QoS, Service Chaining, Traffic Engineering, and Custom.</td>
</tr>
<tr>
<td>7</td>
<td>A policy sequence containing the text string Application Firewall, QoS, Service Chaining, Traffic Engineering, or Custom is added in the left pane.</td>
</tr>
<tr>
<td>8</td>
<td>Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.</td>
</tr>
<tr>
<td>9</td>
<td>In the right pane, click Sequence Rule. The Match/Action box opens, and Match is selected by default. The available policy match conditions are listed below the box.</td>
</tr>
<tr>
<td>10</td>
<td>For QoS and Traffic Engineering data policies: From the Protocol drop-down list, select IPv4 to apply the policy only to IPv4 address families, IPv6 to apply the policy only to IPv6 address families, or Both to apply the policy IPv4 and IPv6 address families.</td>
</tr>
<tr>
<td>11</td>
<td>To select one or more Match conditions, click its box and set the values as described in the following table. Note that not all match conditions are available for all policy sequence types.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all packets)</td>
<td>Do not specify any match conditions.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Procedure</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Applications / Application Family List | 1. In the Match conditions, click **Applications/Application Family List**.  
2. In the drop-down, select the application family.  
3. To create an application list:  
   1. Click **New Application List**.  
   2. Enter a name for the list.  
   3. Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications.  
4. In the **Select Application** drop-down, select the desired applications or application families.  
5. Click **Save**. |
| Destination Data Prefix | 1. In the Match conditions, click **Destination Data Prefix**.  
2. To match a list of destination prefixes, select the list from the drop-down.  
3. To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field. |
| Destination Port | 1. In the Match conditions, click **Destination Port**.  
2. In the **Destination: Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). |
| DNS Application List | Add an application list to enable split DNS.  
1. In the Match conditions, click **DNS Application List**.  
2. In the drop-down, select the application family. |
| DNS | Add an application list to process split DNS.  
1. In the Match conditions, click **DNS**.  
2. In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications. |
| DSCP | 1. In the Match conditions, click **DSCP**.  
2. In the **DSCP** field, type the DSCP value, a number from 0 through 63. |
| Packet Length | 1. In the Match conditions, click **Packet Length**.  
2. In the Packet Length field, type the length, a value from 0 through 65535. |
**Step 3: Configure Traffic Rules**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **PLP**         | 1. In the Match conditions, click **PLP** to set the Packet Loss Priority.  
2. In the PLP drop-down, select **Low** or **High**. To set the PLP to high, apply a policer that includes the **exceed remark** option. |
| **Protocol**    | 1. In the Match conditions, click **Protocol**.  
2. In the Protocol field, type the Internet Protocol number, a number from 0 through 255. |
| **Source Data Prefix** | 1. In the Match conditions, click **Source Data Prefix**.  
2. To match a list of source prefixes, select the list from the drop-down.  
3. To match an individual source prefix, enter the prefix in the **Source** field. |
| **Source Port** | 1. In the Match conditions, click **Source Port**.  
2. In the Source field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). |
| **TCP**         | 1. In the Match conditions, click **TCP**.  
2. In the TCP field, **syn** is the only option available. |

**Step 12**
To select actions to take on matching data traffic, click the **Actions** box.

**Step 13**
To drop matching traffic, click **Drop**. The available policy actions are listed to the right of the button.

**Step 14**
To accept matching traffic, click **Accept**. The available policy actions are listed to the right of the button.

**Step 15**
Set the policy action as described in the following table. Note that not all actions are available for all match conditions.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **Counter**     | Count matching data packets. | 1. In the Action conditions, click **Counter**.  
2. In the **Counter Name** field, enter the name of the file in which to store packet counters. |
| **DSCP**        | Assign a DSCP value to matching data packets. | 1. In the Action conditions, click **DSCP**.  
2. In the **DSCP** field, type the DSCP value, a number from 0 through 63. |
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forwarding Class</strong></td>
<td>Assign a forwarding class to matching data packets.</td>
<td>1. In the Match conditions, click <strong>Forwarding Class</strong>. 2. In the <strong>Forwarding Class</strong> field, type the class value, which can be up to 32 characters long.</td>
</tr>
<tr>
<td><strong>Log</strong></td>
<td>Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td>1. In the Action conditions, click <strong>Log</strong> to enable logging.</td>
</tr>
<tr>
<td><strong>Policer</strong></td>
<td>Apply a policer to matching data packets.</td>
<td>1. In the Match conditions, click <strong>Policer</strong>. 2. In the Policer drop-down field, select the name of a policer.</td>
</tr>
</tbody>
</table>
| **Loss Correction** | Apply loss correction to matching data packets. Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data. FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels.  
- **FEC Adaptive** – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. Adaptive FEC starts to work at 2% packet loss; this value is hard-coded and is not configurable.  
- **FEC Always** – Corresponding packets are always subjected to FEC.  
- **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters. | 1. In the Match conditions, click **Loss Correction**. 2. In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**. |

Click **Save Match and Actions**.

**Step 16** Create additional sequence rules as desired. Drag and drop to re-arrange them.

**Step 17** Click **Save Data Policy**.

**Step 18** Click **Next** to move to Apply Policies to Sites and VPNs in the wizard.
Step 4: Apply Policies to Sites and VPNs

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs.

Step 1
In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

Step 2
In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

Step 3
From the Topology bar, select the tab that corresponds to the type of policy block—Topology, Application-Aware Routing, Traffic Data, or Cflowd. The table then lists policies that you have created for that type of policy block.

Step 4
Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:

a) For a Topology policy block, click Add New Site List and VPN List or Add New Site. Some topology blocks might have no Add buttons. Select one or more site lists, and select one or more VPN lists. Click Add.

b) For an Application-Aware Routing policy block, click Add New Site List and VPN List. Select one or more site lists, and select one or more VPN lists. Click Add.

c) For a Traffic Data policy block, click Add New Site List and VPN List. Select the direction for applying the policy (From Tunnel, From Service, or All), select one or more site lists, and select one or more VPN lists. Click Add.

d) For a Cflowd policy block, click Add New Site List. Select one or more site lists, Click Add.

Step 5
Click Preview to view the configured policy. The policy is displayed in CLI format.

Step 6
Click Save Policy. The Configuration > Policies screen appears, and the policies table includes the newly created policy.

Step 5: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected vSmart controllers. To activate a centralized policy:

Step 1
In vManage NMS, select the Configure ► Policies screen.

Step 2
Select a policy from the policy table.

Step 3
Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.

Step 4
Click Activate.

General CLI Configuration Procedure

Following are the high-level steps for configuring a VPN membership data policy:

1. Create a list of overlay network sites to which the VPN membership policy is to be applied (in the apply-policy command):

```
vSmart(config)# policy
vSmart (config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```
The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes and VPNs, as needed:

   vSmart(config)# policy lists
   vSmart(config-lists)# data-prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length

   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id

3. Create lists of TLOCs, as needed.

   vSmart(config)# policy
   vSmart(config-policy)# lists tloc-list list-name
   vSmart(config-lists-list-name)# tloc ip-address color color encapsulation
   | preference number

4. Define policing parameters, as needed:

   vSmart(config-policy)# policer policer-name
   vSmart(config-policer)# rate bandwidth
   vSmart(config-policer)# burst bytes
   vSmart(config-policer)# exceed action

5. Create a data policy instance and associate it with a list of VPNs:

   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name

6. Create a series of match–pair sequences:

   vSmart(config-vpn-list)# sequence number
   vSmart(config-sequence-number)#

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

7. Define match parameters for packets:

   vSmart(config-sequence-number)# match parameters

8. Define actions to take when a match occurs:

   vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log] [tcp-optimization]
   vSmart(config-sequence-number)# action accept nat [pool number] [use-vpn 0]
   vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
   vSmart(config-sequence-number)# action accept set parameters

9. Create additional numbered sequences of match–action pairs within the data policy, as needed.

10. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:

    vSmart(config-policy-name)# default-action accept

11. Apply the policy to one or more sites in the overlay network:

    vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
Structural Components of Policy Configuration for Centralized Data Policy

The following commands are the structural components required to configure VPN membership policy. Each one is explained in more detail in the sections that follow.

```
policy
  lists
    app-list list-name
    data-prefix-list list-name
    site-list list-name
    site-id site-id
    tloc-list list-name
    tloc ip-address color color encap encapsulation [preference value]
  vpn-list list-name
  vpn vpn-id
  policer policer-name
  burst bytes
  exceed action
  rate bandwidth

data-policy policy-name
  vpn-list list-name
  sequence number
  match
    app-list list-name
    destination-data-prefix-list list-name
    destination-ip prefix/length
    destination-port port-numbers
    dscp number
    dns-app-list list-name
    dns (request | response)
    packet-length number
    protocol number
    source-data-prefix-list list-name
    source-ip prefix/length
    source-port port-numbers
    tcp flag
  action
    cflowd (not available for deep packet inspection)
    count counter-name
    drop
    log
    redirect-dns (dns-ip-address | host)
    tcp-optimization
    accept
    nat [pool number] [use-vpn 0]
    set
      dscp number
      forwarding-class class
      local-tloc color color [encap encapsulation] [restrict]
      next-hop ip-address
      policer policer-name
      service service-name local [restrict] [vpn vpn-id]
      service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
      tloc ip-address color color [encap encapsulation]
      tloc-list list-name
  vpn vpn-id
  default-action
    (accept | drop)

apply-policy site-list list-name
  data-policy policy-name (all | from-service | from-tunnel)
```
## Lists

Centralized data policy for deep packet inspection uses the following types of lists to group related items. In the CLI, you configure lists under the **policy lists** command hierarchy on vSmart controllers.

- **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest**
- **Configuration > Policies > Custom Options > Lists.**

In the CLI, you configure lists under the **policy lists** command hierarchy on vSmart controllers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage / CLI Command</th>
</tr>
</thead>
</table>
| Applications and application families | List of one or more applications or application families running on the subnets connected to the vEdge router.  
  - *application-names* can be the names of one or more applications. The Viptela software supports about 2300 different applications. To list the supported applications, use the ? in the CLI.  
  - *application-families* can be one or more of the following: antivirus, application-service, audio_video, authentication, behavioral, compression, database, encrypted, erp, file-server, file-transfer, forum, game, instant-messaging, mail, microsoft-office, middleware, network-management, network-service, peer-to-peer, printer, routing, security-service, standard, telephony, terminal, thin-client, tunneling, wap, web, and webmail. | **Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Application**  
  or  
  **Configuration > Policies > Centralized Policy > Lists > Application**  
  **app-list list-name**  
  (**app applications | app-family application-families**) |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>vManage / CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes</td>
<td>List of one or more IP prefixes.</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Prefix or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Prefix &lt;br&gt; prefix-list list-name &lt;br&gt; ip-prefix prefix/length</td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as site-id 1) or a range of site identifiers (such as site-id 1-10).</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Site &lt;br&gt; Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site &lt;br&gt; list-name &lt;br&gt; site-id site-id</td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as site-id 1) or a range of site identifiers (such as site-id 1-10).</td>
<td>Configuration &gt; Policies &gt; Centralized Policy &gt; Add Policy &gt; Create Groups of Interest &gt; Site or Configuration &gt; Policies &gt; Custom Options &gt; Centralized Policy &gt; Lists &gt; Site &lt;br&gt; site-list list-name &lt;br&gt; site-id site-id</td>
</tr>
</tbody>
</table>
List Type | Description | vManage / CLI Command
---|---|---
TLOCs | List of one or more TLOCs in the overlay network. For each TLOC, specify its address, color, and encapsulation. **address** is the system IP address. **color** can be one of 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. **encapsulation** can be gre or ipsec. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an **action accept** condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion. | Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > TLOC or Configuration > Policies > Custom Options > Centralized Policy > Lists > Site tloc-list list-name tloc ip-address color color encap encapsulation [preference number]

VPNs | List of one or more VPNs in the overlay network. For data policy, you can configure any VPNs except for VPN 0 and VPN 512. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. You can specify a single VPN identifier (such as **vpn 1**) or a range of VPN identifiers (such as **vpn 1-10**). | Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > VPN or Configuration > Policies > Custom Options > Centralized Policy > Lists > VPN vpn-list list-name vpn vpn-id

VPN Lists

Each centralized data policy is associated with a VPN list. You configure VPN lists with the **policy data-policy vpn-list** command. The list you specify must be one that you created with a VPN Group of Interest or List in the vManage policy configuration wizard or with the **policy lists vpn-list** command.

For centralized data policy, you can include any VPNs except for VPN 0 and VPN 512. VPN 0 is reserved for control traffic, so never carries any data traffic, and VPN 512 is reserved for out-of-band network management, so also never carries any data traffic. Note that while the CLI allows you to include these two VPNs in a data policy configuration, the policy is not applied to these two VPNs.
Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In vManage NMS, you configure policer parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Create Groups of Interest > Policer
- Configuration > Policies > Custom Options > Centralized Policy > Lists > Policer

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

- **rate** is the maximum traffic rate. It can be a value from 0 through 264 – 1 bits per second.
- **burst** is the maximum traffic burst size. It can be a value from 15000 to 100000 bytes.
- **exceed** is the action to take when the burst size or traffic rate is exceeded. **action** can be **drop** (the default) or **remark**. The **drop** action is equivalent to setting the packet loss priority (PLP) bit to low. The **remark** action sets the PLP bit to high. In centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the **match plp** option.

Sequences

Each VPN list consists of sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy.

In vManage NMS, you configure sequences from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type
- Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type

In the CLI, you configure sequences with the **policy data-policy vpn-list sequence** command.

Each sequence can contain one match condition and one action condition.

Match Parameters

Centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

In vManage NMS, you configure match parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match
- Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Match

Each sequence in a policy can contain one match condition.
For data policy, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Command</th>
<th>Value or Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match all packets</td>
<td>Omit Match</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Omit <code>match</code> command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications or application families</td>
<td>Match Applications/Application Family List</td>
<td>Name of an application list or an <code>app-list</code> list</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>app-list list-name</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td>Match Destination Data Prefix</td>
<td>Name of a data prefix list or a <code>data-prefix-list</code> list</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>destination-data-prefix-list list-name</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td>Match Destination Port</td>
<td>IP prefix and prefix length</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>destination-ip prefix/length</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination port number</td>
<td>Match Destination Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>destination-port number</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable split DNS, to resolve and process DNS</td>
<td>Match DNS Application List</td>
<td>Name of an <code>app-list</code> list. This list specifies the applications whose DNS requests are processed.</td>
<td></td>
</tr>
<tr>
<td>requests and responses on an application-by-</td>
<td><code>dns-app-list list-name</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>application basis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the direction in which to process DNS</td>
<td>Match DNS</td>
<td>To process DNS requests sent by the applications (for outbound DNS queries), specify <code>dns request</code>. To process DNS responses returned from DNS servers to the applications, specify <code>dns response</code>.</td>
<td></td>
</tr>
<tr>
<td>packets</td>
<td>`dns (request</td>
<td>response)`</td>
<td></td>
</tr>
<tr>
<td>DSCP value</td>
<td>Match DSCP</td>
<td>0 through 63</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>dscp number</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet length</td>
<td>Match Packet Length</td>
<td>0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>packet-length number</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td>Match PLP</td>
<td>(high</td>
<td>low)By default, packets have a PLP value of low. To set the PLP value to high, apply a policer that includes the <code>exceed remark</code> option.</td>
</tr>
<tr>
<td></td>
<td><code>plp</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/CLI Configuration Parameter</td>
<td>Value or Range</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>Internet protocol number</td>
<td>Match Protocol</td>
<td>0 through 255</td>
<td></td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td>Match Source Data Prefix</td>
<td>Name of a data prefix or a data-prefix-list list</td>
<td></td>
</tr>
<tr>
<td>Individual source prefix</td>
<td>Match Source Data Prefix</td>
<td>IP prefix and prefix length</td>
<td></td>
</tr>
<tr>
<td>Source port number</td>
<td>Match Source Port</td>
<td>0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])</td>
<td></td>
</tr>
<tr>
<td>TCP flag</td>
<td>tcp flag</td>
<td>syn</td>
<td></td>
</tr>
</tbody>
</table>

### Action Parameters

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In vManage NMS, you configure match parameters from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action.**

In the CLI, you configure the action parameters with the `policy data-policy vpn-list sequence action` command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage Configuration/CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click Accept. accept</td>
<td>—</td>
</tr>
<tr>
<td>Enable cflowd traffic monitoring.</td>
<td>Click Accept, then action Cflowd cflowd</td>
<td>—</td>
</tr>
<tr>
<td>Description</td>
<td>vManage Configuration/CLI Configuration Parameter</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td>Action Counter&lt;br&gt;Click Accept, then action Counter count counter-name</td>
<td>Name of a counter. Use the <code>show policy access-lists counters</code> command on the vEdge router.</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click Drop drop</td>
<td>—</td>
</tr>
<tr>
<td>Log the packet. Packets are placed into the messages and vsyslog system logging (syslog) files.</td>
<td>Action Log&lt;br&gt;Click Accept, then action Log log</td>
<td>To view the packet logs, use the <code>show app log flows</code> and <code>show log</code> commands.</td>
</tr>
<tr>
<td>Redirect DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions.</td>
<td>Click Accept, then action Redirect DNS redirect-dns host redirect-dns ip-address</td>
<td>For an inbound policy, <code>redirect-dns host</code> allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server.</td>
</tr>
<tr>
<td>Fine-tune TCP to decrease round-trip latency and improve throughout for matching TCP traffic.</td>
<td>Click Accept, then action TCP Optimization tcp-optimization</td>
<td>—</td>
</tr>
</tbody>
</table>

Then, for a packet that is accepted, the following parameters can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>vManage / CLI Configuration Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable cflowd traffic monitoring.</td>
<td>Click Accept, then action Cflowd cflowd</td>
<td>—</td>
</tr>
<tr>
<td>Direct matching traffic to the NAT functionality so that it can be redirected directly to the Internet or other external destination.</td>
<td>Click Accept, then action NAT Pool or NAT VPN nat [pool number] [use-vpn 0]</td>
<td>—</td>
</tr>
<tr>
<td>DSCP value.</td>
<td>Click Accept, then action DSCP set dscp value</td>
<td>0 through 63</td>
</tr>
<tr>
<td>Forwarding class.</td>
<td>Click Accept, then action Forwarding Class set forwarding-class value</td>
<td>Name of forwarding class</td>
</tr>
<tr>
<td>Description</td>
<td>vManage / CLI Configuration Parameter</td>
<td>Value or Range</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Direct matching packets to a TLOC that mathces the color and encapsulation</td>
<td>Click Accept, then action Local TLOC set local-tloc color color [encap encapsulation]</td>
<td>color can be: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. By default, encapsulation is ipsec. It can also be gre.</td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct matching packets to one of the TLOC's in the list if the TLOC matches the color and encapsulation</td>
<td>Click Accept, then action Local TLOC set local-tloc-list color color encap encapsulation [restrict]</td>
<td></td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the restrict option.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the next hop to which the packet should be forwarded.</td>
<td>Click Accept, then action Next Hop set next-hop ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>Apply a policer.</td>
<td>Click Accept, then action Policer set policer policer-name</td>
<td>Name of policer configured with a policy policer command</td>
</tr>
<tr>
<td>Specify a service to redirect traffic to before delivering the traffic to its destination.</td>
<td>Click Accept, then action Service set service service-name [tloc ip-address]</td>
<td>Standard services: FW, IDS, IDP</td>
</tr>
<tr>
<td>The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.</td>
<td>[tloc-list list-name] [vpn vpn-id]</td>
<td>Custom services: netsvc1, netsvc2, netsvc3, netsvc4</td>
</tr>
<tr>
<td>The VPN identifier is where the service is located.</td>
<td></td>
<td>TLOC list is configured with a policy lists tloc-list list</td>
</tr>
<tr>
<td>Configure the services themselves on the vEdge routers that are collocated with the service devices, using the vpn service command.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation.</td>
<td>Click Accept, then action TLOC set tloc address color color [encap encapsulation]</td>
<td>TLOC address, color, and encapsulation</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct traffic to one of the remote TLOCs in the TLOC list if it matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.</td>
<td>Click Accept, then action TLOC set tloc-list list-name</td>
</tr>
<tr>
<td>Name of a policy list</td>
<td>Click Accept, then action VPN set vpn vpn-id</td>
</tr>
<tr>
<td>Name of a policy list</td>
<td>0 through 65530</td>
</tr>
</tbody>
</table>

### Default Action

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

In vManage NMS, you modify the default action from:

- **Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Default Action**
- **Configuration > Policies > Custom Options > Centralized Policy > Traffic Policy > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Default Action**

In the CLI, you modify the default action with the `policy data-policy vpn-list default-action accept` command.

### Applying Centralized Data Policy

For a centralized data policy to take effect, you apply it to a list of sites in the overlay network.

To apply a centralized policy in vManage NMS:

1. In vManage NMS, select the **Configure > Policies** screen.
2. Select a policy from the policy table.
3. Click the More Actions icon to the right of the row, and click **Activate**. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.
4. Click **Activate**.

To apply a centralized policy in the CLI:

```plaintext
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
```

By default, data policy applies to all data traffic passing through the vEdge router: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the **all** option. To have the data policy apply only to traffic coming from the service.
site and exiting from the local site through the tunnel interface, include the from-service option. To have the policy apply only to traffic entering from the tunnel interface and traveling to the service site, include the from-tunnel option. You can apply different data policies in each of the two traffic directions.

For all data-policy policies that you apply with apply-policy commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists site-list 1 site-id 1-100 and site-list 2 site-id 70-130. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different data-policy policies, the attempt to commit the configuration on the vSmart controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (app-route-policy)
- Centralized control policy (control-policy)
- Centralized data policy used for cflowd flow monitoring (data-policy that includes a cflowd action and apply-policy that includes a cflowd-template command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for control-policy and data-policy policies can have overlapping site IDs. So for the two example site lists above, site-list 1 site-id 1-100 and site-list 2 site-id 70-130, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration by issuing a commit command, the vSmart controller pushes the data policy to the vEdge routers located in the specified sites. To view the policy as configured on the vSmart controller, use the show running-config command on the vSmart controller:

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To view the policy that has been pushed to the vEdge router, use the show policy from-vsmart command on the vEdge router.

```
vEdge# show policy from-vsmart
```

### Configuring Deep Packet Inspection

You configure deep packet inspection using a standard centralized data policy. You define the applications of interest in a vManage policy list or with policy lists app-list CLI command, and you call these lists in the match portion of the data policy. You can control the path of the application traffic through the network by defining, in the action portion of the data policy, the local TLOC or the remote TLOC, or for strict control, you can define both.

### Centralized Data Policy Configuration Examples

This article provides some straightforward examples of configuring centralized data policy to influence traffic flow across the Cisco SD-WAN domain and to configure a vEdge router to be an Internet exit point.

#### General Centralized Data Policy Example

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a vSmart controller and that after you commit the configuration, the policy itself is pushed to the affected vEdge routers.
Here we configure a simple data policy on the vSmart controller vm9:

```
vm9# show running-config policy
policy
data-policy test-data-policy
    vpn-list test-vpn-list
        sequence 10
            match
                destination-ip 172.16.0.0/24
            !
                action drop
                    count test-counter
                !
                default-action drop
            !
        lists
            vpn-list test-vpn-list
                vpn 1
            !
            site-list test-site-list
                site-id 500
            !
    !

Then we apply this policy to the site list named test-site-list, which includes site 500:

```
vm9# show running-config apply-policy
apply-policy
    site-list test-site-list
    data-policy test-data-policy
    !
```

Immediately after we activate the configuration on the vSmart controller, it pushes the policy configuration to the vEdge routers in site 500. One of these routers is vm5, where we see that the policy has been received:

```
vm5# show omp data-policy
policy-from-vsmart
    data-policy test-data-policy
        vpn-list test-vpn-list
            sequence 10
                match
                    destination-ip 172.16.0.0/24
                !
                    action drop
                        count test-counter
                !
                    default-action drop
                !
            lists
                vpn-list test-vpn-list
                    vpn 1
                !
```
Control Access

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 1.1.1.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 2.2.2.2. This policy also specifies the next hop for the TCP traffic sent by 1.1.1.1, setting it to be TLOC 10.10.10.10, color gold. All other traffic is accepted as a result of the default-action statement.

```
policy
  lists
    site-list north
    site-id 100
    vpn-list vpn-north
    vpn 100
  !
  data-policy tcp-only
    vpn-list vpn-north
    sequence 10
    match
      source-ip 1.1.1.1/32
      destination-ip 2.2.2.2/32
      protocol tcp
    action accept
    set tloc 10.10.10.10 gold
  !
  default-action accept
  !
  apply-policy
    site north data-policy tcp-only
```

Restrict Traffic

This example illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 1.1.0.0/16. However, the policy accepts all other data traffic, including non-SMTP traffic from 1.1.0.0/16.

```
policy
  lists
    data-prefix-list north-ones
    ip-prefix 1.1.0.0/16
    port 25
    vpn-list all-vpns
    vpn 1
    vpn 2
    site-list north
    site-id 100
  !
  data-policy no-mail
    vpn-list all-vpns
    sequence 10
    match
      source-data-prefix-list north-ones
    action drop
  !
  default-action accept
  !
  apply-policy
    site north data-policy no-mail
```
Allow Traffic to Exit from a vEdge Router to the Internet

The following example allows data traffic destined for two prefixes on the Internet to exit directly from the local vEdge router to the Internet destination. Configure this policy on the vSmart controller.

```
policy
  lists
    vpn-list vpn-1
      vpn 1
    !
    site-list nat-sites
      site-id 100,200
    !
data-policy accept-nat
  vpn-list vpn-1
    sequence 100
      match
        source-ip 10.20.24.0/24
        destination-ip 10.0.12.12/32
      !
      action accept
      count nat
      nat use-vpn 0
    !
    sequence 101
      match
        source-ip 10.20.24.0/24
        destination-ip 10.1.15.13/32
      !
      action accept
      count nat_inet
      nat use-vpn 0
    !
    default-action accept
  !
apply-policy
  site-list nat-sites data-policy accept-nat
```

Using the destination port instead of a destination IP prefix allows greater flexibility for traffic exiting to the Internet. Here, traffic can go to all HTTP and HTTPS sites (ports 80 and 443, respectively). Configure this policy on a vSmart controller.

```
data-policy accept-nat
  vpn-list vpn-1
    sequence 100
      match
        source-ip 10.20.24.0/24
        destination-port 80
      !
      action accept
      count nat
      nat use-vpn 0
    !
    sequence 101
      match
        source-ip 10.20.24.0/24
        destination-port 443
      !
      action accept
      count nat_inet
```

Localized Control Policy

Control policy operates on the control plane traffic in the Cisco SD-WAN overlay network, influencing the determination of routing paths through the overlay network. Localized control policy is policy that is configured on a vEdge router (hence, it is local) and affects BGP and OSPF routing decisions on the site-local network that the vEdge router is part of.

In addition to participating in the overlay network, a vEdge router participates in the network at its local site, where it appears to the other network devices to be simply a regular router. As such, you can provision routing protocols, such as BGP and OSPF, on the vEdge router so that it can exchange route information with the local-site routers. To control and modify the routing behavior on the local network, you configure a type of control policy called route policy on the vEdge routers. Route policy applies only to routing performed at the local branch, and it affects only the route table entries in the local vEdge router's route table.

Localized Data Policy

Data policy operates on the data plane in the Cisco SD-WAN overlay network and affects how data traffic is sent among the vEdge routers in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on a vEdge router.

Localized data policy, so called because it is provisioned on the local vEdge router, is applied on a specific router interface and affects how a specific interface handles the data traffic that it is transmitting and receiving. Localized data policy is also referred to as access lists (ACLs). With access lists, you can provision class of service (CoS), classifying data packets and prioritizing the transmission properties for different classes. You can also provision packet mirroring and policing. For IPv4, you can also configure QoS actions.

You can apply IPv4 access lists in any VPN on the router, and you can create access lists that act on unicast and multicast traffic. You can apply IPv6 access lists only to tunnel interfaces in the transport VPN (VPN 0).

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local vEdge router. For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

Explicit and Implicit Access Lists

Access lists that you configure using localized data policy are called explicit ACLs. You can apply explicit ACLs in any VPN on the router.

Router tunnel interfaces also have implicit ACLs, which are also referred to as services. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On vEdge routers, the following services are enabled by default:
DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

**Perform QoS Actions**

With access lists, you can provision quality of service (QoS) which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. See Forwarding and QoS Overview.

**Mirror Data Packets**

Once packets are classified, you can configure access lists to send a copy of data packets seen on a vEdge router interface to a specified destination on another network device. The Cisco SD-WAN software supports 1:1 mirroring; that is, a copy of every packet is sent to the alternate destination.

### Localized Data Policy Configuration Examples

This article provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco SD-WAN domain. Localized data policy, also known as access lists, is configured directly on the local vEdge routers.

**QoS**

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces on a vEdge router and on the interface queues. For examples of how to configure a QoS policy, see Forwarding and QoS Configuration Examples.

**Mirroring Example**

This example illustrates how to configure a mirror instance to automatically send a copy of certain types of data packet to a specified destination for analysis. After you configure the mirror instance, include it in an access list. Here, "mirror-m1" is configured with the host at source address 10.20.23.16 and destination host at 10.2.2.11. The mirror instance is then included in the access list "acl2," which is configured so that data packets originating from the host at source address 10.20.24.17 and going to the destination host at 10.20.25.18 are mirrored to the destination host at 10.2.2.11 with the source address of the originating host as 10.20.23.16.

```
policy
  mirror m1
    remote-dest 10.2.2.11 source 10.20.23.16
  !
!
vm5# show running-config policy access-list acl2
policy
  access-list acl2
  sequence 1
    match
      source-ip 10.20.24.17/32
destination-ip 10.20.25.18/32
    !
    action accept
    mirror m1
    !
  !
default-action drop
```
Tools

- Operational Commands, on page 731
- Rediscover Network, on page 733
- SSH Terminal, on page 735

Operational Commands

Use the Operational Commands screen to run, on Viptela devices, a group of two or more operational commands as a single command.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Operational Commands.
  - Show Admin Tech List button—Click to display a list of all requests to generate admin-tech file.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
Admin Tech Command

Use the Admin Tech command to collect system status information for a device in a tar file, to aid in troubleshooting and diagnostics.

1. From the device table, select the device.
2. Click the More Actions icon to the right of the row and click Admin Tech.
3. In the Generate admin-tech File window, limit the contents of the Admin Tech tar file if desired:
   1. The Include Logs checkbox is selected by default. Deselect this checkbox to omit any log files from the compressed tar file. Log files are stored in the /var/log/directory on the local device.
2. Select the Include Cores checkbox to include any core files. Core files are stored in the /var/crash directory on the local device.

3. Select the Include Tech checkbox to include any files related to device processes (daemons) and operations. These files are stored in the /var/tech directory on the local device.

4. Click Generate. A tar file is created which contains the contents of various files on the local device. This file has a name similar to 20150709-032523-admin-tech.tar.gz, where the numeric fields are the date and time.

5. Send the admin-tech.tar.gz file to your Viptel customer support contact.

Interface Reset Command

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation, without having to modify the device's configuration.

1. From the device table, select the device.

2. Click the More Actions icon to the right of the row and click Interface Reset.

3. In the Interface Reset window, select the desired interface.

4. Click Reset.

Rediscover Network

Use the Rediscover Network screen to locate new devices in the overlay network and synchronize them with the vManage NMS.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Rediscover Network.
- Rows Selected—Displays the number of rows selected from the table.
  - Rediscover button—Click to rediscover the devices in the network.
- Device Groups drop-down—Lists all configured device groups in the network.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.
- Table of devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
Rediscover the Network

To locate new devices in the overlay network, click the Rediscover button located directly beneath the title bar. vManage NMS redisCOVERs every device and link and displays updated information about the network.

Synchronize Device Data

To synchronize the data on a specific device with the vManage NMS:

1. From the Device Groups drop-down list, select the device group to which the device belongs. The device table lists all the devices in the selected group.
2. Select the device.
3. Click the Rediscover button.
4. In the Rediscover Network window, click Rediscover to confirm re-synchronization of the device data.

**SSH Terminal**

Use the SSH Terminal screen to establish an SSH session to a Viptela device. From an SSH session, you can issue CLI commands on the Viptela device.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, SSH Terminal.
- **Left pane**—Includes:
  - **Device Groups drop-down**—Lists all configured device groups in the network.
  - **Search box**—Includes the Search Options drop-down, for a Contains or Match string.
  - **Sort by drop-down options.** You can sort the device list by reachability, hostname, system IP, site ID, or device model.
  - **List of all Viptela devices in the selected device group.**

- **Right pane**—Includes:
  - **An open SSH window.** The size of the window is based on the current browser size, and it does not readjust if you change the window size. A vertical scroll bar allows you to scroll up and down in the SSH window.
**Establish an SSH Session to a Device**

To establish an SSH session to a device:
1. From the left pane, select the device on which to collect statistics:
   1. Select the device group to which the device belongs.
   2. If needed, sort the device list by its status, hostname, system IP, site ID, or device type.
   3. Click on the device to select it.
2. Enter the username and password to log in to the device.

You can now issue CLI commands to monitor or configure the device.
vAnalytics

- Applications, on page 737
- Network Availability, on page 739
- Network Health, on page 740
- vAnalytics Dashboard, on page 742

Applications

Use the Applications screen to monitor application families and individual applications in your overlay network over time.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Applications.
  - Time Period—Click a predefined or custom time period for which to display data.
- Bandwidth—Displays bandwidth utilization for application families.
- Performance—Displays Viptela Quality of Experience (vQoE) values for application families. The vQoE value ranges from zero to ten, with zero being the worst performance and ten being the best. vQoE calculates this value based on latency, loss, and jitter, customizing the calculation for each application.
- Anomaly—Displays application families using more bandwidth than their baseline.
Display Bandwidth Utilization

To display bandwidth utilization for application families:

1. Click Bandwidth.
2. Click the Filter icon to select a specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.
4. Hover over an item in any chart to open a hover box with details about that item.
5. Select a view: By Summary, By Time, or By Sites:
   - By Summary displays a summary by application family. Click an application family to display applications in that family. Click an application to see that application's bandwidth utilization over time. Click a point on the timeline to see that application's bandwidth utilization by site. Click a site to see flows for that application at that site.
   - By Time displays a timeline of application family bandwidth utilization. Click an application family to display utilization for the applications in that family. Click an application to display utilization at each site running the application. Click a site to display flows for that application at that site.
   - By Sites displays bandwidth utilization on each vEdge router. Click a site to display a timeline of application family bandwidth utilization at that site. Click an application family to display utilization for applications in that family at that time. Click an application to display flows for that application at that site.

Display vQoE Values

To display vQoE values for each application family:

1. Click Performance.
2. Click the Filter icon to select a specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.
4. Hover over an application family in the chart to open a hover box with details for that application family.
5. Click an application family to display average latency, loss, jitter, and vQoE for each application in that family:
   1. Click an application to display that application's performance on each device in the tunnel.
   2. Click a device to display an hourly summary of that application on that device.

Display Deviations from Baseline Utilization

vAnalytics platform computes daily averages and standard deviations for application families at every site in a rolling window of seven days. An anomaly occurs if an application family's bandwidth utilization exceeds the average plus two times the standard deviation.

To display deviations from baseline values of bandwidth utilization for application families:

1. Click Anomaly.
2. Click the Filter icon to select a specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.
4. Hover over an application family in the chart to open a hover box with details for that application family.
5. Click a site to see a timeline of anomalies for that site.
6. Click an hour on the timeline to see anomalous behavior of individual applications in that hour.

**Network Availability**

Use the Network Availability screen to monitor downtime of nodes and circuits in your overlay network over time.

**Screen Elements**

- **Top bar**—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- **Title bar**—Includes the title of the screen, Network Availability.
  - **Time Period**—Click a predefined or custom time period for which to display data.
- **Selected View**—Displays downtime by sites or by time.
- **Summary**—Displays node and circuit downtime summaries.
Display Downtime by Site
To display vEdge router and circuit downtime for each site:
1. Select Aggregated Downtime by Sites.
2. Click the Filter icon to select specific application family to view.
3. Click the PDF icon to open a PDF version of the chart in a new tab.
4. Click a vEdge router or circuit to display details about that downtime event.

Display Downtime by Time
To display vEdge router and circuit downtime for a specified time period:
1. Select Aggregated Downtime by Time.
2. Select a length of time: Day, Week, Quarter, or Year.
3. Click the Filter icon to select specific device or circuit to view.
4. Click the PDF icon to open a PDF version of the chart in a new tab.
5. Click a vEdge router or circuit to display details about that downtime event.

Network Health
Use the Network Health screen to monitor the performance of circuits, tunnels, and carriers in your overlay network over time.

Screen Elements
- Top bar—On the left are the menu icon, for expanding and collapsing the vAnalytics menu, and the vAnalytics product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Network Health.
  - Tunnel—Displays latency, loss, and jitter by circuit.
  - Carrier—Displays application performance by carrier on a geographical map of your overlay network.
  - Time Period—Click a predefined or custom time period for which to display data.
Display Latency, Loss, and Jitter on Circuits
To display graphs for latency, loss, and jitter on each circuit in your overlay network:

1. Click Tunnel. Each line in the graphs indicates one circuit. The legend to the right indicates the color of each circuit.
2. Click the Filter icon to select specific circuits to view.
3. Click the PDF icon to open a PDF version of the graph in a new tab.
4. Hover over a point on a line to open a hover box with details for that point in time.
5. Click a point on a line to display average latency, loss, or jitter in that circuit at that point in time:
   1. Click a site to see latency, loss, or jitter for all tunnels at that site.
   2. Click a tunnel to see hourly latency, loss, or jitter for that tunnel.
   3. Click Overview to return to Network Health ► Tunnel.

6. To highlight specific circuits:
   1. Click a circuit in the legend to select it. To select more than one circuit, hold down the Shift key.
   2. Click the Highlight icon that appears. The selected circuits are highlighted on the map.
   3. To display all circuits again, click the Highlight icon.

Display Application Performance by Carrier
To display application performance by carrier on a geographical map of the overlay network:

1. Click Carrier. Circles on the map represent each carrier. The legend to the right indicates the color of each carrier.
2. Select Latency, Loss, or Jitter to change the data displayed.
3. Click the Filter icon to select specific carriers to view.
4. Click the PDF icon to open a PDF version of the map in a new tab.
5. Hover over a carrier's circle to display a hover box with details for that location.
6. Click a circle on the map to display that location's performance by loss, latency, or jitter:
   1. Click a point on the graph to see a graph of performance for each carrier at that location.
   2. Click a carrier to see performance for each vEdge router at that site.
   3. Click a vEdge router to see that device's performance over time.
   4. Click Overview to return to Network Health ► Carrier.

7. Hover over the map to display map functions:
   1. Click Search to search for a geographical location by name.
   2. Click the + (plus) or - (minus) zoom icons to zoom in or out.
   3. Click Home to return to the world-wide view.
4. Hover over the right arrow for other map functions, such as selecting a zoom area and panning.

8. To highlight specific carriers:
   1. Click a carrier in the legend to select it. To select more than one carrier, hold down the Shift key.
   2. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
   3. To display all carriers again, click the Highlight icon.

vAnalytics Dashboard

Use the vAnalytics dashboard screen to monitor the performance of the entire Viptela overlay network over time.

Top Bar

The top bar is located at the top of every vAnalytics screen and includes the following screen elements:

• Menu icon—Click the icon to expand or collapse the vAnalytics menu. The vAnalytics menu is closed by default.
• vAnalytics product name.
• Help—Links to product help and software version information about the vAnalytics platform.
• vAnalytics username—Username for the vAnalytics platform that you are logged into. Includes the sign-out button.
**Network Availability Pane**

The Network Availability pane displays network-wide availability for the last 24 hours by device and circuit. Each box displays uptime as a percentage and total downtime in minutes.

Click in the Device box to display downtime for each vEdge router in the overlay network. Click in the Circuit box to display downtime for each circuit in the overlay network.

- Click the Filter icon to select a specific vEdge router or circuit to view.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Click any bar to display the time period when that device or circuit was down.

**Applications Pane**

The Applications Pane displays application performance for the last 24 hours in three views: Least Performing Applications, Applications Consuming Most Bandwidth, and Anomalous Application Families.

**Least Performing Applications**

The Least Performing Applications box displays the applications in the network with the lowest performance. vAnalytics platform calculates application performance with the Viptela Quality of Experience (vQoE) value. This value ranges from zero to 10, with zero being the worst performance and 10 being the best. vQoE combines scores for latency, loss, and jitter, customizing the calculation for the needs of each application.

- Select vQoE, Latency, Loss, or Jitter to change the data displayed.
- Click the Sort icon to toggle between Least Performing Applications and Top Performing Applications.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a bar in the graph to open a hover box with details about that application.
- Click a bar in the graph to display that application's performance on each tunnel. Click a tunnel to display the application's hourly performance on that tunnel.

**Applications Consuming Most Bandwidth**

The Applications Consuming Most Bandwidth box displays applications consuming the most bandwidth in the network.

Each circle represents an application; the larger the circle, the greater is the bandwidth that it consumes. The legend to the right indicates the color of each application family. The graph displays the top ten applications using the most bandwidth, and an additional circle called Others. Click Others for details about any remaining applications.

- Click the PDF icon to open a PDF version of the graph in a new tab.
- Hover over a circle in the graph to open a hover box with details about that application.
- Click a circle in the graph to display that application's bandwidth consumption over time. Click a point on the graph to display sites using that application. Click a site to display flows for that site.
- To highlight specific application families:
  1. Click a family in the legend to select it. To select more than one family, hold down the Shift key.
2. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
3. To display all families again, click the Highlight icon.

**Anomalous Application Families**

The Anomalous Application Families box displays application families using more bandwidth than their baseline.

- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a bar in the graph to display a hover box with details about that application family.
- Click a bar in the graph to display that family's average octets by site. Click a bar in the graph to display that site's octets over time for that family. Click a bar in the timeline to display octets at that point in time for each application in the family.

**WAN Performance Pane**

The WAN Performance pane displays performance of carriers and tunnels for the last 24 hours by latency, loss, or jitter.

**Carrier Performance**

The Carrier Performance box displays application performance by carrier on a geographical map of the overlay network.

Circles on the map represent each carrier. The legend to the right indicates the color of each carrier.

- Select Latency, Loss, or Jitter to change the data displayed.
- Click the PDF icon to open a PDF version of the map in a new tab.
- Hover over a carrier's circle to display a hover box with details for that location.
- Click a circle on the map to display that location's performance for the last 24 hours in graphical format. Hover over a point on the graph for details about that point in time.
- Hover over the map to display map functions:
  - Click Search to search for a geographical location by name.
  - Click the + (plus) or – (minus) zoom icons to zoom in or out.
  - Click Home to return to the world-wide view.
  - Hover over the right arrow for other map functions, such as selecting a zoom area and panning.
- To highlight specific carriers:
  1. Click a carrier in the legend to select it. To select more than one carrier, hold down the Shift key.
  2. Click the Highlight icon that appears. The selected carriers are highlighted on the map.
  3. To display all carriers again, click the Highlight icon.
Tunnel Performance

The Tunnel Performance box displays the performance of tunnels for the last 24 hours by latency, loss, or jitter. The legend to the right indicates the color of each tunnel.

- Select Latency, Loss, or Jitter to change the data displayed.
- Click the PDF icon to open a PDF version of the chart in a new tab.
- Hover over a point on the graph to display a hover box with details about that point in time.
- To highlight specific tunnels:
  1. Click a tunnel in the legend to select it. To select more than one tunnel, hold down the Shift key.
  2. Click the Highlight icon that appears. The selected tunnels are highlighted on the graph.
  3. To display all tunnels again, click the Highlight icon.