Configuring Application-Aware Routing

This article provides general procedures for configuring application-aware routing.

Configuration Components

Application-aware routing consists of three components:

- Identify the applications of interest. To determine which applications are running on vEdge routers, you enable application visibility on these devices. Then you configure an application-aware routing policy on the vSmart controller, which defines the applications of interest and the data plane tunnel performance characteristics required to transmit an application's data traffic. These characteristics are called a service-level agreement (SLA). The controller automatically pushes the policy to the appropriate vEdge routers.

- Monitor and measure data plane tunnel performance is done automatically and continuously by the vEdge routers, by tracking BFD Hello packets. Application-aware routing periodically polls the performance statistics to calculate the packet latency, loss, and jitter information for each tunnel. The default polling interval is good for most network situations, but you can modify it to meet specific business needs.

- Map application traffic to a specific data plane tunnel is done on the vEdge routers, based on the SLA requirements defined in application-aware routing policy and based on the real-time performance of the vEdge routers' data plane tunnels. You can modify how often a vEdge router calculates each tunnel's SLA and determines a tunnel's SLA classification.

Regardless of whether you have configured an application-aware routing policy, each vEdge router automatically monitors traffic jitter, loss, and latency and other interface characteristics on their data plane tunnels. To display this information, use the `show app-route stats` command on the vEdge router. You can use these statistics to determine the baseline performance characteristics of the vEdge router's tunnels. You can also use them to create appropriate application-aware routing policies and to modify existing policies.

Configure Application-Aware Routing Policy

Application-aware routing policy affects only traffic that is flowing from the service side (the local/WAN side) to the tunnel (WAN) side of the vEdge router.

An application-aware routing policy matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications' data traffic. The primary purpose of application-aware routing policy is to optimize the path for data traffic being transmitted by vEdge routers.

An application-aware routing policy is a type of centralized data policy: you configure it on the vSmart controller, and the controller automatically pushes it to the affected vEdge routers. As with any policy, an application-aware routing 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 one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to use to transmit the packet. If a packet matches no parameters in any of the policy sequences, and if no default SLA class is configured, the packet is accepted and
forwarded with no consideration of SLA. Because application-aware routing policy accepts nonmatching traffic by default, it is considered to be a positive policy. Other types of policies in the Viptela software are negative policies, because by default they drop nonmatching traffic.

---

**General vManage Configuration Procedure**

To configure application-aware routing policy, 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 Applications or 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 application-aware routing policy to take effect, you must activate the policy.

### 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. Click Add Policy.

The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

### Create Applications or Groups of Interest

To create lists of applications or groups to use in centralized policy:

1. Start the policy configuration wizard as explained above.
2. Create new lists, as described in the following table:

<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Application | 1. In the left bar, click Application.  
2. Click New Application List. |
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. Click either the Application or Application Family 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 Add.</td>
</tr>
<tr>
<td></td>
<td><strong>Two application lists are preconfigured. You cannot edit or delete these lists.</strong></td>
</tr>
<tr>
<td></td>
<td>• Google Apps—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>• Microsoft Apps—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>Prefix</td>
<td>1. In the left bar, click Prefix.</td>
</tr>
<tr>
<td></td>
<td>2. Click New Prefix List.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. In the Add Prefix field, enter one or more data prefixes separated by commas.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add.</td>
</tr>
<tr>
<td>Site</td>
<td>1. In the left bar, click Site.</td>
</tr>
<tr>
<td></td>
<td>2. Click New Site List.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. In the Add Site field, enter one or more site IDs separated by commas.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add.</td>
</tr>
<tr>
<td>SLA Class</td>
<td>1. In the left bar, click SLA Class.</td>
</tr>
<tr>
<td></td>
<td>2. Click New SLA Class List.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>4. Define the SLA class parameters:</td>
</tr>
<tr>
<td>List Type</td>
<td>Procedure</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>1. In the Loss field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.</td>
</tr>
<tr>
<td></td>
<td>2. In the Latency field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>3. In the Jitter field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add.</td>
</tr>
<tr>
<td></td>
<td>4. Click Next to move to Configure Topology in the wizard. When you first open this screen, the Topology tab is selected by default.</td>
</tr>
</tbody>
</table>

**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.

**Configure the Network Topology**

To configure the network topology or a VPN membership to use in centralized policy:

1. If you are already in the policy configuration wizard, skip to Step 4. Otherwise, in vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.
3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.
4. Create a network topology, as described in the following table:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub and Spoke</td>
<td>Policy for a topology with one or more central hub sites and with spokes connected to a hub</td>
<td>1. In the Add Topology drop-down, select Hub and Spoke.</td>
</tr>
</tbody>
</table>

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/07Policy_Applications/01Application…
Created on: Fri, 01 Nov 2019 07:18:36 GMT
Generated by: Anonymous
<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Enter a name for the hub-and-spoke policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter a description for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. In the VPN List field, select the VPN list for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Double-click the My Hub-and-Spoke text string, and enter a name for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. In the right pane, add hub sites to the network topology:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add Hub Sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the Site List Field, select a site list for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Repeat Steps 7a, 7b, and 7c to add more hub sites to the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. In the right pane, add spoke sites to the network topology:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add Spoke Sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the Site List Field, select a site list for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Repeat Steps 8a, 8b, and 8c to add more spoke sites to the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Repeat Steps 5 through 8 to add more components to the hub-and-spoke policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Click Save Hub and Spoke Policy.</td>
</tr>
</tbody>
</table>

<p>| Mesh | Partial-mesh or full-mesh region | 1. In the Add Topology drop-down, select Mesh. |
|      |                                  | 2. Enter a name for the mesh region policy component. |</p>
<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>3. Enter a description for the mesh region policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. In the VPN List field, select the VPN list for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click New Mesh Region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. In the Mesh Region Name field, enter a name for the individual mesh region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. In the Site List field, select one or more sites to include in the mesh region.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Repeat Steps 5 through 7 to add more mesh regions to the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Click Save Mesh Region.</td>
</tr>
</tbody>
</table>

5. To use an existing topology:
   1. In the Add Topology drop-down, click Import Existing Topology. The Import Existing Topology popup displays.
   2. Select the type of topology.
   3. In the Policy drop-down, select the name of the topology.
   4. Click Import.

6. Click Next to move to Configure Traffic Rules in the wizard. When you first open this screen, the Application-Aware Routing tab is selected by default.

Configure Traffic Rules

To create the match and action rules to apply to traffic affected by the policy:

1. If you are already in the policy configuration wizard, skip this procedure. Otherwise, in vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.
3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.
4. Click Next. The Configure Traffic Rules screen opens, and in the Application-Aware Routing bar, the Application-Aware Routing tab is selected by default.

To configure traffic rules for application-aware routing policy:
1. In the Application-Aware Routing bar, select the Application-Aware Routing tab.

2. Click the Add Policy drop-down.

3. Select Create New, and in the left pane, click Sequence Type. A policy sequence containing the text string App Route is added in the left pane.

4. Double-click the App Route 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.

5. 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.

6. To select one or more Match conditions, click its box and set the values as described in the following 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>Applications/Application Family List</td>
<td>1. In the Match conditions, click Applications/Application Family List.</td>
</tr>
<tr>
<td></td>
<td>2. In the drop-down, select the application family.</td>
</tr>
<tr>
<td></td>
<td>3. To create an application list:</td>
</tr>
<tr>
<td></td>
<td>1. Click New Application List.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>3. Click the Application button to create a list of individual applications. Click the Application Family button to create a list of related applications.</td>
</tr>
<tr>
<td></td>
<td>4. In the Select Application drop-down, select the desired applications or application families.</td>
</tr>
<tr>
<td></td>
<td>5. Click Save.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>1. In the Match conditions, click Destination Data Prefix.</td>
</tr>
<tr>
<td></td>
<td>2. To match a list of destination prefixes, select the list from the drop-down.</td>
</tr>
<tr>
<td></td>
<td>3. To match an individual destination prefix, type the prefix in the Destination box.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>1. In the Match conditions, click Destination Port.</td>
</tr>
</tbody>
</table>
|                                             | 2. In the Destination 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
<table>
<thead>
<tr>
<th>Feature</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| DNS 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 (to enable 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. |
| PLP | 1. In the Match conditions, click PLP.  
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, type the prefix in the Source box. |
| 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 [-]). |

7. To select actions to take on matching data traffic, click the Actions box. The available policy actions are listed below.
8. Set the policy action as described in the following table:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Backup SLA Preferred Color | When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel interface is not available, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching. | 1. In the Action conditions, click Backup SLA Preferred Color.  
2. In the drop-down, select one or more colors.                                                                                       |
| 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.                                                   |
| Log                      | 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. | 1. In the Action conditions, click Log to enable logging.                                                                                                                                       |
| SLA Class List           | For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels. | 1. In the Action conditions, click SLA Class List.  
2. In the SLA Class drop-down, select one or more SLA classes.  
3. Optionally, in the Preferred Color drop-down, select the color of the data plane tunnel or tunnels to prefer. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.  
4. Click Strict to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA. |
9. Click Save Match and Actions.
10. Create additional sequence rules as desired. Drag and drop to re-arrange them.
11. Create additional sequence types as desired. Drag and drop to re-arrange them.
12. Click Save Application-Aware Routing Policy.

Click Next to move to Apply Policies to Sites and VPNs in the wizard.

Apply Policies to Sites and VPNs

In the last screen of the policy configuration wizard, you associate the policy blocks that you created on the previous three screens with VPNs and with sites in the overlay network.

To apply a policy block to sites and VPNs in the overlay network:

1. If you are already in the policy configuration wizard, skip to Step 6. Otherwise, in vManage NMS, select the Configure Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.
3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.
4. Click Next. The Configure Traffic Rules screen opens, and in the Application-Aware Routing bar, the Application-Aware Routing tab is selected by default.
5. Click Next. The Apply Policies to Sites and VPNs screen opens.
6. 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.
7. 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.
8. From the Topology bar, select the type of policy block. The table then lists policies that you have created for that type of policy block.
9. Click Add New Site List and VPN list. Select one or more site lists, and select one or more VPN lists. Click Add.
10. Click Preview to view the configured policy. The policy is displayed in CLI format.
11. Click Save Policy. The Configuration Policies screen opens, and the policies table includes the newly created policy.
Activate an Application-Aware Routing Policy

Activating an application-aware routing policy sends that policy to all connected vSmart controllers. To activate a 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. Select a policy.

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.

General CLI Configuration Procedure

Following are the high-level steps for configuring an application-aware routing policy:

1. Create a list of overlay network sites to which the application-aware routing policy is to be applied (in the apply-policy command):
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-site-list)# 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 SLA classes and traffic characteristics to apply to matching application data traffic:
   vSmart(config)# policy sla-class sla-class-name
   vSmart(config-sla-class)# jitter milliseconds
   vSmart(config-sla-class)# latency milliseconds
   vSmart(config-sla-class)# loss percentage

3. Create lists of applications, IP prefixes, and VPNs to use in identifying application traffic of interest (in the match section of the policy definition):
   vSmart(config)# policy lists
   vSmart(config-lists)# app-list list-name
   vSmart(config-app-list)# (app application-name | app-family family-name)

   vSmart(config-lists)# prefix-list list-name
   vSmart(config-prefix-list)# ip-prefix prefix/length

   vSmart(config-lists)# vpn-list list-name
   vSmart(config-vpn-list)# vpn vpn-id

4. If you are configuring a logging action, configure how often to log packets to syslog files:
   vEdge(config)# policy log-frequency number

5. Create an application-aware routing policy instance and associate it with a list of VPNs:
6. Within the policy, create one or more numbered sequence of match–action pairs, where the match parameters define the data traffic and applications of interest and the action parameters specify the SLA class to apply if a match occurs.

1. Create a sequence:
   ```
   vSmart(config-app-route-policy)# sequence number
   ```

2. Define match parameters for data packets:
   ```
   vSmart(config-sequence)# match parameters
   ```

3. Define the action to take if a match occurs:
   ```
   vSmart(config-sequence)# action sla-class sla-class-name [strict]
   vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color colors
   vSmart(config-sequence)# action backup-sla-preferred-color colors
   ```
   The first two action options direct matching data traffic to a tunnel interface that meets the SLA characteristics in the specified SLA class:
   • **sla-class sla-class-name**—When you specify an SLA class with no additional parameters, data traffic that matches the SLA is forwarded as long as one tunnel interface is available. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.
   • **sla-class sla-class-name preferred-color color**—To set a specific tunnel to use when data traffic matches an SLA class, include the preferred-color option, specifying the color of the preferred tunnel. If more than one tunnel matches the SLA, traffic is sent to the preferred tunnel. If a tunnel of the preferred color is not available, traffic is sent through any tunnel that matches the SLA class. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not.
   • **sla-class sla-class-name preferred-color colors**—To set multiple tunnels to use when data traffic matches an SLA class, include the preferred-color option, specifying two or more tunnel colors. Traffic is load-balanced across all tunnels. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not.
   When no tunnel matches the SLA, you can choose how to handle the data traffic:
   • **strict**—Drop the data traffic.
   • **backup-sla-preferred-color colors**—Direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available; if that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. As with the preferred-color option, the backup SLA preferred color is loose matching.
   In a single action configuration, you cannot include both the strict and backup-sla-preferred-color options.

4. Count the packets or bytes that match the policy:
   ```
   vSmart(config-sequence)# action count counter-name
   ```

5. Place a sampled set of packets that match the SLA class rull into syslog files:
   ```
   vSmart(config-sequence)# action log
   ```
6. The match–action pairs within a policy are evaluated in numerical order, based on the sequence number, starting with the lowest number. If a match occurs, the corresponding action is taken and policy evaluation stops.

7. If a packet does not match any of the conditions in one of the sequences, a default action is taken. For application-aware routing policy, the default action is to accept nonmatching traffic and forward it with no consideration of SLA. You can configure the default action so that SLA parameters are applied to nonmatching packets:
   vSmart(config-policy-name)# default-action sla-class sla-class-name

8. Apply the policy to a site list:
   vSmart(config)# apply-policy site-list list-name app-route-policy policy-name

---

Structural Components of Policy Configuration for Application-Aware Routing

Here are the structural components required to configure application-aware routing policy. Each one is explained in more detail in the sections below.

```
policy
    lists
        app-list list-name (app application-name | app-family application-family)
        prefix-list list-name
        site-list list-name
        site-id site-id
        vpn-list list-name
        vpn-id vpn-id
    log-frequency number
    sla-class sla-class-name
    jitter milliseconds
    latency milliseconds
    loss percentage
    app-route-policy policy-name
    vpn-list list-name
    sequence number
    match
    action
        backup-sla-preferred-color colors
        count counter-name
        log
        sla-class sla-class-name [strict] [preferred-color colors]
    default-action
        sla-class sla-class-name
    apply-policy site-list list-name
    app-route-policy policy-name
```

---

Lists

Application-aware routing policy uses the following types of lists to group related items. You configure these lists under the `policy lists` command hierarchy on vSmart controllers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications and application families</td>
<td>List of one or more applications or application families running on the subnets connected to the vEdge router. Each <code>app-list</code> can contain either applications or application families, but you cannot mix the two. To configure multiple applications or application families in a single list, include multiple <code>app</code> or <code>app-family</code> options, specifying one application or application family in each <code>app</code> or <code>app-family</code> option.</td>
<td>`app-list list-name (app application-name</td>
</tr>
<tr>
<td>List Type</td>
<td>Description</td>
<td>Command</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Data prefixes</td>
<td>List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple <code>ip-prefix</code> options, specifying one prefix in each option.</td>
<td><code>data-prefix-list list-name ip-prefix prefix/length</code></td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple <code>site-id</code> options, specifying one site number in each option. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td><code>site-list list-name site-id</code></td>
</tr>
<tr>
<td>VPNs</td>
<td>List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple <code>vpn</code> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <code>vpn-id 1</code>) or a range of VPN identifiers (such as <code>vpn-id 1-10</code>).</td>
<td><code>vpn-list list-name vpn vpn-id</code></td>
</tr>
</tbody>
</table>

In the vSmart controller configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these lists. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. (You can use ranges to specify data prefixes, site identifiers, and VPNs.) Here are two examples of lists that are configured with ranges and that contain overlapping values:

- `vpn-list list-1 vpn 1-10`  
  `vpn-list list-2 vpn 6-8`  
- `site-list list-1 site 1-10`  
  `site-list list-2 site 5-15`
When you configure data policies that contain lists with overlapping values, or when you apply data policies, you must ensure that the lists included in the policies, or included when applying the policies, do not contain overlapping values. To do this, you must manually audit your configurations. The Viptela configuration software performs no validation on the contents of lists, on the data policies themselves, or on how the policies are applied to ensure that there are no overlapping values.

If you configure or apply data policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Viptela software when it processes the configuration. This decision is not under user control, so the outcome is not predictable.

Logging Frequency

If you configure a logging action, by default, the vEdge router logs all data packet headers to a syslog file. To log only a sample of the data packet headers:

```
vEdge(config)# policy log-frequency number
```

`number` specifies how often to log packet headers. For example, if you configure `log-frequency 20`, every sixteenth packet is logged. While you can configure any integer value for the frequency, the software rounds the value down to the nearest power of 2.

SLA Classes

The action taken in application-aware routing is applied based on what is called an SLA (a service-level agreement). An SLA class is defined by the maximum jitter, maximum latency, maximum packet loss, or a combination of these values, for the vEdge router’s data plane tunnels. (Each tunnel is defined by a local TLOC–remote TLOC pair.) You configure SLA classes under the `policy sla-class` command hierarchy on vSmart controllers. You can configure a maximum of four SLA classes.

You can configure the following parameters in an SLA class:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum acceptable packet jitter on the data plane tunnel</td>
<td>jitter milliseconds</td>
<td>1 through 1000 milliseconds</td>
</tr>
<tr>
<td>Maximum acceptable packet latency on the data plane tunnel</td>
<td>latency milliseconds</td>
<td>1 through 1000 milliseconds</td>
</tr>
<tr>
<td>Maximum acceptable packet loss on the data plane tunnel</td>
<td>loss percentage</td>
<td>0 through 100 percent</td>
</tr>
</tbody>
</table>

VPN Lists

Each application-aware policy instance is associated with a VPN list. You configure VPN lists with the `policy app-route-policy vpn-list` command. The VPN list you specify must be one that you created with a `policy lists vpn-list` command.
Sequences

Within each VPN list, an application-aware policy contains 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. You configure sequences with the `policy app-aware-policy vpn-list sequence` command.

Each sequence in an application-aware policy can contain one **match** command and one **action** command.

Match Parameters

Application-aware routing policy can match IP prefixes and fields in the IP headers. You configure the match parameters with the **match** command under the `policy app-route-policy vpn-list sequence` command hierarchy on vSmart controllers.

You can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match all packets</td>
<td>Omit <strong>match</strong> command</td>
<td>—</td>
</tr>
<tr>
<td>Applications or application families</td>
<td><strong>app-list</strong> <code>list-name</code></td>
<td>Name of an <strong>app-list</strong> list</td>
</tr>
<tr>
<td>Group of destination prefixes</td>
<td><strong>destination-data-prefix-list</strong> <code>list-name</code></td>
<td>Name of a <strong>data-prefix-list</strong> list</td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td><strong>destination-ip</strong> <code>prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination <strong>port number</strong></td>
<td><strong>destination-port</strong> <code>number</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>DSCP value</td>
<td><strong>dscp</strong> <code>number</code></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td><strong>protocol</strong> <code>number</code></td>
<td>0 through 255</td>
</tr>
<tr>
<td>Packet loss priority (PLP)</td>
<td><strong>plp</strong></td>
<td>*(high</td>
</tr>
</tbody>
</table>
**Action Parameters**

When data traffic matches the match parameters, the specified action is applied to it. For application-aware routing policy, the action is to apply an SLA class. The SLA class defines the maximum packet latency or maximum packet loss, or both, that the application allows on the data plane tunnel used to transmit its data. The Viptela software examines the recently measured performance characteristics of the data plane tunnels and directs the data traffic to the WAN connection that meets the specified SLA.

The following actions can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching.</td>
<td>backup-sla-preferred-color colors</td>
<td>3G, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver</td>
</tr>
<tr>
<td>Count matching data packets.</td>
<td>action count</td>
<td>Name of a counter.</td>
</tr>
<tr>
<td>Description</td>
<td>Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Place a sampled set of packets that match the SLA class rule 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><code>counter-name</code></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>
<tr>
<td>SLA class to match. All matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.</td>
<td><code>action sla-class sla-class-name</code></td>
<td>SLA class name defined in <code>policy sla-class</code> command</td>
</tr>
<tr>
<td>Group of data plane tunnel colors to prefer when an SLA class match occurs. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.</td>
<td><code>action sla-class sla-class-name preferred-color colors</code></td>
<td>SLA class name defined in <code>policy sla-class</code> command and one of the supported tunnel colors.</td>
</tr>
<tr>
<td>Strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Note that for policy configured with this option, data traffic that matches the match conditions is dropped until the application-aware routing path is established.</td>
<td><code>action sla-class sla-class-name strict</code> <code>action sla-class sla-class-name preferred-color color strict</code> <code>action sla-class sla-class-name preferred-color</code></td>
<td>SLA class name defined in <code>policy sla-class</code> command</td>
</tr>
</tbody>
</table>
If more than one data plane tunnel satisfies an SLA class criteria, the vEdge router selects one of them by performing load-balancing across the equal paths.

### Default Action

A policy's default action defines how to handle packets that match none of the match conditions. For application-aware routing policy, if you do not configure a default action, all data packets are accepted and transmitted based on normal routing decisions, with no consideration of SLA.

To modify this behavior, include the `default-action sla-class sla-class-name` command in the policy, specifying the name of an SLA class you defined in the `policy sla-class` command.

When you apply an SLA class in a policy's default action, you cannot specify the `strict` option.

If no data plane tunnel satisfies the SLA class in the default action, the vEdge router selects one of the available tunnels by performing load-balancing across equal paths.

### Applying Application-Aware Routing Policy

For an application-aware route policy to take effect, you apply it to a list of sites in the overlay network:

```
 vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

When you apply the policy, you do not specify a direction (either inbound or outbound). Application-aware routing policy affects only the outbound traffic on the vEdge routers.

For all `app-route-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 `app-route-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:

- Centralized control policy (`control-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 `app-route-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 on the vSmart controller by issuing a `commit` command, the controller pushes the application-aware routing policy to the vEdge routers at the specified sites.

To view the policy configured on the vSmart controller, use the `show running-config` command on the controller.

To view the policy that the vSmart controller has pushed to the vEdge router, issue the `show policy from-vsmart` command on the router.

To display flow information for the application-aware applications running on the vEdge router, issue the `show app dpi flows` command on the router.

---

**How Application-Aware Routing Policy Is Applied in Combination with Other Data Policies**

If you configure a vEdge router with application-aware routing policy and with other policies, the policies are applied to data traffic sequentially.

On a vEdge router, you can configure the following types of data policy:

- **Centralized data policy.** You configure this policy on the vSmart controller, and the policy is passed to the vEdge router. You define the configuration with the `policy data-policy configuration` command, and you apply it with the `apply-policy site-list data-policy` or `apply-policy site-list vpn-membership` command.

- **Localized data policy.** Which is commonly called access lists. You configure access lists on the vEdge router with the `policy access-list` configuration command. You apply them, within a VPN, to an incoming interface with the `vpn interface access-list in` configuration command or to an outgoing interface with the `vpn interface access-list out` command.

- **Application-aware routing policy.** Application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the vEdge router. You configure application-aware routing policy on the vSmart controller with the `policy app-route-policy` configuration command, and you apply it with the `apply-policy site-list app-route-policy` command. When you commit the configuration, the policy is passed to the appropriate vEdge routers. Then, matching data traffic on the vEdge routers is processed in accordance with the configured SLA conditions. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

You can apply only one data policy and one application-aware routing policy to a single site in the overlay network. When you define and apply multiple site lists in a configuration, you must ensure that a single data policy or a single application-aware routing policy is not applied to more than one site. The CLI does not check for this circumstance, and the `validate` configuration command does not detect whether multiple policies of the same type are applied to a single site.

For data traffic flowing from the service side of the router to the WAN side of the router, policy evaluation of the traffic evaluation occurs in the following order:

1. Apply the input access list on the LAN interface. Any data traffic that is not dropped as a result of this access list is passed to the application-aware routing policy for evaluation.
2. Apply the application-aware routing policy. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

3. Apply the centralized data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

4. Apply the output access list on the WAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the WAN interface.

For data traffic coming from the WAN through the router and into the service-side LAN, the policy evaluation of the traffic occurs in the following order:

1. Apply the input access list on the WAN interface. Any data traffic that is not dropped as a result of the input access list is passed to the data policy for evaluation.

2. Apply the data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

3. Apply the output access list on the LAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the LAN interface, towards its destination at the local site.

As mentioned above, application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the vEdge router, so data traffic inbound from the WAN is processed only by access lists and data policy.

---

**Configure the Monitoring of Data Plane Tunnel Performance**

The Bidirectional Forwarding Detection (BFD) protocol runs over all data plane tunnels between vEdge routers, monitoring the liveness, and network and path characteristics of the tunnels. Application-aware routing uses the information gathered by BFD to determine the transmission performance of the tunnels. Performance is reported in terms of packet latency and packet loss on the tunnel.

BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The vEdge router records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket. If you configure an application-aware routing policy for the vEdge router, it is these statistics that the router uses to determine whether a data plane tunnel’s performance matches the requirements of the policy’s SLA.

The following parameters determine the size of the sliding window:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Configuration Command</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Hello packet interval</td>
<td>1 second</td>
<td><code>bfd color color hello-interval seconds</code></td>
<td>1 through 65535 seconds</td>
</tr>
</tbody>
</table>

---

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/07Policy_Applications/01Application...
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Configuration Command</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling interval for application-aware routing</td>
<td>10 minutes (600,000 milliseconds)</td>
<td>bfd app-route poll-interval milliseconds</td>
<td>1 through 4,294,967 (2^{32} – 1) milliseconds</td>
</tr>
<tr>
<td>Multiplier for application-aware routing</td>
<td>6</td>
<td>bfd app-route multiplier number</td>
<td>1 through 6</td>
</tr>
</tbody>
</table>

Let's use the default values for these parameters to explain how application-aware routing works:

- For each sliding window time period, application-aware routing sees 600 BFD Hello packets (BFD Hello interval x polling interval: 1 second x 600 seconds = 600 Hello packets). These packets provide measurements of packet loss and latency on the data plane tunnels.

- Application-aware routing retains the statistics for 1 hour (polling interval x multiplier: 10 minutes x 6 = 60 minutes).

- The statistics are placed in six separate buckets, indexed with the numbers 0 through 5. Bucket 0 contains the latest statistics, and bucket 5 the oldest. Every 10 minutes, the newest statistics are placed in bucket 0, the statistics in bucket 5 are discarded, and the remaining statistics move into the next bucket.

- Every 60 minutes (every hour), application-aware routing acts on the loss and latency statistics. It calculates the mean of the loss and latency of all the buckets in all the sliding windows and compares this value to the specified SLAs for the tunnel. If the calculated value satisfies the SLA, application-aware routing does nothing. If the value does not satisfy the SLA, application-aware routing calculates a new tunnel.

- Application-aware routing uses the values in all six buckets to calculate the mean loss and latency for a data tunnel. This is because the multiplier is 6. While application-aware always retains six buckets of data, the multiplier determines how many it actually uses to calculate the loss and latency. For example, if the multiplier is 3, buckets 0, 1, and 2 are used.

Because these default values take action only every hour, they work well for a stable network. To capture network failures more quickly so that application-aware routing can calculate new tunnels more often, adjust the values of these three parameters. For example, if you change just the polling interval to 1 minute (60,000 milliseconds), application-aware routing reviews the tunnel performance characteristics every minute, but it performs its loss and latency calculations based on only 60 Hello packets. It may take more than 1 minute for application-aware routing to reset the tunnel if it calculates that a new tunnel is needed.

To display statistics for each data plane tunnel, use the `show app-route stats` command:
To display the next-hop information for an IP packet that a vEdge router sends out a service side interface, use the `show policy service-path` command. To view the similar information for packets that the router sends out a WAN transport tunnel interface, use the `show policy tunnel-path` command.

---

**Enable Application Visibility on vEdge Routers**

You can enable application visibility directly on vEdge routers, without configuring application-aware routing policy so that you can monitor all the applications running in all VPNs in the LAN. To do this, configure application visibility on the router:

vEdge(config)# `policy app-visibility`

To monitor the applications, use the `show app dpi applications` and `show app dpi supported-applications` commands on the vEdge router.

---

**Additional Information**

- Application-Aware Routing
- Application-Aware Routing Policy Configuration Example
- Configuring Centralized Data Policy
Configuring Split DNS