Forwarding and QoS Overview

Forwarding is the transmitting of data packets from one vEdge router to another. Once the control plane connections of the Viptela overlay network are up and running, data traffic flows automatically over the IPsec connections between vEdge routers. Because data traffic never goes to or through the centralized vSmart controller, forwarding only occurs between the vEdge routers as they send and receive data traffic.

While the routing protocols running in the control plane provide a vEdge router the best route to reach the network that is on the service side of a remote vEdge router, there will be situations where it is beneficial to select more specific routes. Using forwarding, there are ways you can affect the flow of data traffic. Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote vEdge router.

To modify the default data packet forwarding flow, you create and apply centralized data policy or localized data policy. With centralized data policy, you can manage the paths along which traffic is routed through the network, and you can permit or block traffic based on the address, port, and DSCP fields in the packet’s IP header. With localized data policy, you can control the flow of data traffic into and out of a vEdge router’s interfaces, enabling features such as quality of service (QoS) and mirroring. Note that QoS is synonymous with class of service (CoS).

Default Behavior without Data Policy

When no centralized data policy is configured on the vSmart controller, all data traffic is transmitted from the local service-side network to the local vEdge router, and then to the remote vEdge router and the remote service-side network, with no alterations in its path. When no access lists are configured on the local vEdge router to implement QoS or mirroring, the data traffic is transmitted to its destination with no alterations to its flow properties.

Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured:

• A data packet arriving from the local service-side network and destined for the remote service-side network comes to the vEdge-1 router. The packet has a source IP address and a destination IP address.

• The vEdge router looks up the outbound SA in its VPN route table, and the packet is encrypted with SA and gets the local TLOC. (The vEdge router previously received its SA from the vSmart controller. There is one SA per TLOC. More specifically, each TLOC has two SAs, an outbound SA for encryption and an inbound SA for decryption.)

• ESP adds an IPsec tunnel header to the packet.

• An outer header is added to the packet. At this point, the packet header has these contents: TLOC source address, TLOC destination address, ESP header, destination IP address, and source IP address.
• The vEdge router checks the local route table to determine which interface the packet should use to reach its destination.

• The data packet is sent out on the specified interface, onto the network, to its destination. At this point, the packet is being transported within an IPsec connection.

• When the packet is received by the vEdge router on the remote service-side network, the TLOC source address and TLOC destination address header fields are removed, and the inbound SA is used to decrypt the packet.

• The remote vEdge router looks up the destination IP address in its route table to determine the interface to use to reach to the service-side destination.

The figure below details this process.

---

Behavior Changes with QoS Data Policy

When you want to modify the default packet forwarding flow, you design and provision QoS policy. To activate the policy, you apply it to specific interfaces in the overlay network in either the inbound or the outbound direction. The direction is with respect to the vEdge routers in the network. You can have policies for packets coming in on an interface or for packets going out of an interface.

The figure below illustrates the QoS policies that you can apply to a data packet as it is transmitted from one branch to another. The policies marked Input are applied on the inbound interface to the vEdge router, and the policies marked Output are applied on the outbound interface to the vEdge router, before the packets are transmitted out the IPSec tunnel.
The table below describes each of the above steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Define class map to classify packets, by importance, into appropriate forwarding classes. Reference the class map in an access list.</td>
<td>class-map</td>
</tr>
<tr>
<td>2</td>
<td>Define policer to specify the rate at which traffic is sent on the interface. Reference the policer in an access list. Apply the access list on an inbound interface.</td>
<td>policer</td>
</tr>
<tr>
<td>3</td>
<td>vEdge router checks the local route table to determine which interface the packet should use to reach its destination.</td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td>Define policer and reference the policer in an access list. Apply the access list on an outbound interface.</td>
<td>policer</td>
</tr>
<tr>
<td>5</td>
<td>Define QoS map to define the priority of data packets. Apply the QoS map on the outbound interface.</td>
<td>qos-map</td>
</tr>
<tr>
<td>6</td>
<td>Define rewrite-rule to overwrite the DSCP field of the outer IP header. Apply the rewrite-rule on the outbound interface.</td>
<td>rewrite-rule</td>
</tr>
</tbody>
</table>

Understanding How QoS Works

The QoS feature on the vEdge routers works by examining packets entering at the edge of the network. With localized data policy, also called access lists, you can provision QoS to classify incoming data packets into multiple forwarding
classes based on importance, spread the classes across different interface queues, and schedule the transmission rate level for each queue. Access lists can be applied either in the outbound direction on the interface (as the data packet travels from the local service-side network into the IPsec tunnel toward the remote service-side network) or in the inbound direction (as data packets are exiting from the IPsec tunnel and being received by the local vEdge router.

To provision QoS, you must configure each vEdge router in the network. Generally, each router on the local service-side network examines the QoS settings of the packets that enter it, determines which packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

**Classify Data Packets**

You can classify incoming traffic by associating each packet with a forwarding class. Forwarding classes group data packets for transmission to their destination. Based on the forwarding class, you assign packets to output queues. The vEdge routers service the output queues according to the associated forwarding, scheduling, and rewriting policies you configure.

**Schedule Data Packets**

You can configure a QoS map for each output queue to specify the bandwidth, delay buffer size, and packet loss priority (PLP) of output queues. This enables you to determine how to prioritize data packets for transmission to the destination. Depending on the priority of the traffic, you can assign packets higher or lower bandwidth, buffer levels, and drop profiles. Based on the conditions defined in the QoS map, packets are forwarded to the next hop.

On hardware vEdge routers and Cloud vEdge virtualized routers, each interface has eight queues, which are numbered 0 to 7. Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ. All control traffic is transmitted. Queues 1 to 7 are available for data traffic, and the default scheduling for these seven queues is weighted round-robin (WRR). For these queues, you can define the weighting according to the needs of your network.

**Rewrite Data Packets**

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network. Rewrite rules allow you to map traffic to code points when the traffic exits the system. Rewrite rules use the forwarding class information and packet loss priority (PLP) used internally by the vEdge routers to establish the DSCP value on outbound packets. You can then configure algorithms such as RED/WRED to set the probability that packets will be dropped based on their DSCP value.

**Police Data Packets**

You can configure policers to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels. Traffic that conforms to the policer rate is transmitted, and traffic that exceeds the policer rate is sent with a decreased priority or is dropped.

You can apply a policer to inbound or outbound interface traffic. Policers applied to inbound interface traffic allow you to conserve resources by dropping traffic that does not need to be routed through the network. Policers applied to
outbound interface traffic control the amount of bandwidth used.

Additional Information

Centralized Data Policy
Centralized Data Policy Configuration Examples
Forwarding and QoS Configuration Examples