Forwarding and QoS

Forwarding is the transmitting of data packets from one router to another.

Quality of Service (QoS) is synonymous with class of service (CoS). You can enable QoS with localized data policies, which control the flow of data traffic into and out of the interfaces of Cisco vEdge devices and Cisco IOS XE SD-WAN devices.

Cisco SD-WAN Forwarding and QoS Overview

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 router.

Once the control plane connections of the Cisco SD-WAN overlay network are up and running, data traffic flows automatically over the IPsec connections between the routers. Because data traffic never goes to or through the centralized vSmart controller, forwarding only occurs between the Cisco IOS XE SD-WAN devices as they send and receive data traffic.

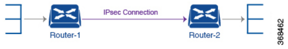
While the routing protocols running in the control plane provide a router the best route to reach the network that is on the service side of a remote router, there will be situations where it is beneficial to select more specific routes. Using forwarding, there are ways you can affect the flow of data 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 router.

To modify the default data packet forwarding flow, you create and apply a centralized data policy or a localized data policy. With a 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 a localized data policy, you can control the flow of data traffic into and out of the interfaces of a router, enabling features such as quality of service (QoS).

Traffic Behavior With and Without QoS

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

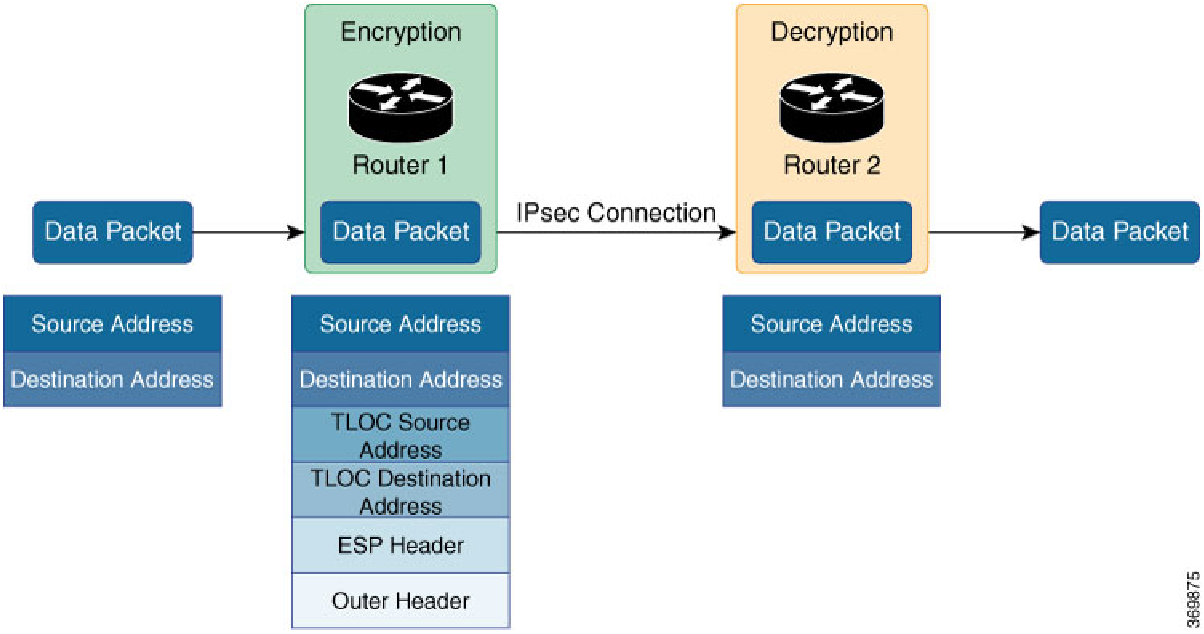


Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured:

- A data packet arriving from the local service-side network and destined for the remote service-side network comes to the router-1. The packet has a source IP address and a destination IP address.
- The router looks up the outbound SA in its VPN route table, and the packet is encrypted with SA and gets the local TLOC. (The 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 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 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 router looks up the destination IP address in its VPN route table to determine the interface to use to reach to the service-side destination.

The figure below details this process.

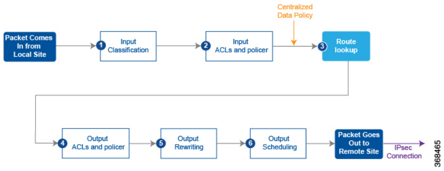
Figure 1: Data Packet Transmission without Policy



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 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 of the router, and the policies marked Output are applied on the outbound interface of the router, before the packets are transmitted out the IPSec tunnel.



The table below describes each of the above steps.

Step	Description	Command
1	Define class map to classify packets, by importance, into appropriate forwarding classes. Reference the class map in an access list.	**class-map**
2	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.	**policer**
3	The router checks the local route table to determine which interface the packet should use to reach its destination.	N/A

Step	Description	Command
4	Define policer and reference the policer in an access list. Apply the access list on an outbound interface.	**policer**
5	Define QoS map to define the priority of data packets. Apply the QoS map on the outbound interface.	**policy-map**
6	Define rewrite-rule to overwrite the DSCP field of the outer IP header. Apply the rewrite-rule on the outbound interface.	**rewrite-rule**

How QoS Works

The QoS feature on the Cisco IOS XE SD-WAN devices and Cisco vEdge devices 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 router.

To provision QoS, you must configure each 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 class of 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 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. 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 Cisco vEdge devices and Cisco IOS XE SD-WAN devices, 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. 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. When QoS is not configured for data traffic, queue 2 is the default queue.

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 Cisco IOS XE SD-WAN devices and Cisco vEdge devices 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.

Shaping Rate

You can configure shaping to control the maximum rate of traffic sent. You can configure the aggregate traffic rate on an interface to be less than the line rate so that the interface transmits less traffic than it is capable of transmitting. You can apply shaping to outbound interface traffic.

Limitations for Forwarding on Cisco IOS XE SD-WAN Devices

The following features are not supported on Cisco IOS XE SD-WAN devices

- Mirroring is not supported.
- Delaying buffer size is not supported.
- Specifying packet loss priority (PLP) is not supported.
- Policers cannot be applied on interfaces.
- Decreased priority dropping is not supported.

QoS vManage

Forwarding and QoS Configuration Examples

This section shows examples of how you can use access lists to configure quality of service (QoS), classifying data packets and prioritizing the transmission properties for different classes. Note that QoS is synonymous with class of service (CoS).

This example shows how to configure class of service (CoS) to classify data packets and control how traffic flows out of and into the interfaces on Cisco IOS XE SD-WAN devices on the interface queues. To configure a QoS policy:

1. Map each forwarding class to an output queue.
2. Configure the QoS scheduler for each forwarding class.
3. Define an access list to specify match conditions for packet transmission and apply it to a specific interface.

4. Apply the queue map and the rewrite rule to the egress interface.

The sections below show examples of each of these steps.

Map Each Forwarding Class to Output Queue

This example shows a data policy that classifies incoming traffic by mapping each forwarding class to an output queue.

```
policy
class-map
  class Queue0 queue 0
  class ef queue 0
  class Queue1 queue 1
  class Queue2 queue 2
  class be queue 2
  class Queue3 queue 3
  class af1 queue 3
  class Queue4 queue 4
  class af2 queue 4
  class Queue5 queue 5
  class af3 queue 5
!
```

Configure QoS Scheduler for Each Forwarding Class

This example illustrates how to configure the QoS scheduler for each queue to define the importance of data packets.

```
class-map match-any Queue0
match qos-group 0
!
class-map match-any Queue1
match qos-group 1
!
class-map match-any Queue2
match qos-group 2
!
class-map match-any Queue3
match qos-group 3
!
class-map match-any Queue4
match qos-group 4
!
class-map match-any Queue5
match qos-group 5
!

policy-map test
class Queue0
  priority percent 20
!
class Queue1
  random-detect
  bandwidth percent 20
!
class class-default
  bandwidth percent 20
!
class Queue3
```

```
  bandwidth percent 15
!
class Queue4
  random-detect
  bandwidth percent 15
!
class Queue5
  bandwidth percent 10
!
!
```

Create Access Lists to Classify Data Packets

Define Access Lists

Define an access list to specify match conditions for packet transmission.

```
policy
access-list acl1
  sequence 1
   match
    dscp 46 48
   !
   action accept
    class ef
   !
  !
  sequence 11
   match
    dscp 34
   !
   action accept
    class af3
   !
  !
  sequence 21
   match
    dscp 24
   !
   action accept
    class af2
   !
  !
  sequence 31
   match
    dscp 18
   !
   action accept
    class af1
   !
  !
  sequence 41
   match
    dscp 0 10
   !
   action accept
    class be
    log
   !
  !
  default-action accept
!
```

Apply Access Lists

Apply Access List to a Specific Interface

This example illustrates how to apply the previously access list defined on the input of a service interface. Here "access-list acl1" is applied on the input of interface Gi0/0/1.

```
sdwan
interface GigabitEthernet0/0/1
  access-list acl1 in
!
 !
!
```

Configure and Apply Rewrite Rule

Configure Rewrite Rule

This example shows how to configure the rewrite rule to overwrite the DSCP field of the outer IP header. Here the rewrite rule "transport" overwrites the DSCP value for forwarding classes based on the drop profile. Since all classes are configured with RED drop, they can have one of two profiles: high drop or low drop. The rewrite rule is applied only on the egress interface, so on the way out, packets classified as "af1" and a Packet Loss Priority (PLP) level of low are marked with a DSCP value of 3 in the IP header field, while "af1" packets with a PLP level of high are marked with 4. Similarly, "af2" packets with a PLP level of low are marked with a DSCP value of 5, while "af2" packets with a PLP level of high are marked with 6, and so on.

Apply the Queue Map and Rewrite Rule to the Egress Interface

```
policy
rewrite-rule transport
  class af1 low layer-2-cos 1
  class af2 low dscp 16 layer-2-cos 2
  class af3 low dscp 24 layer-2-cos 3
  class be low dscp 0
  class ef low dscp 46 layer-2-cos 5
!
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule transport
exit
```

Verify Configuration of QoS Policy Map

```
Device#show policy-map interface GigabitEthernet0/0/2
 GigabitEthernet0/0/2

  Service-policy output: shape_GigabitEthernet0/0/2

    Class-map: class-default (match-any)
      33823 packets, 6855717 bytes
  5 minute offered rate 31000 bps, drop rate 0000 bps
  Match: any
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 33823/6855717
  shape (average) cir 100000000, bc 400000, be 400000
  target shape rate 100000000

  Service-policy : test

    queue stats for all priority classes:
      Queueing
      queue limit 512 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 33802/6853827

    Class-map: Queue0 (match-any)
      33802 packets, 6853827 bytes
      5 minute offered rate 31000 bps, drop rate 0000 bps
      Match: qos-group 0
      Priority: 20% (20000 kbps), burst bytes 500000, b/w exceed drops: 0


    Class-map: Queue1 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 1
      Queueing
      queue limit 83 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
     (pkts output/bytes output) 0/0
      bandwidth 20% (20000 kbps)
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0 packets
        class       Transmitted         Random drop      Tail drop          Minimum
 Maximum     Mark
                pkts/bytes            pkts/bytes       pkts/bytes          thresh
thresh     prob

        0               0/0               0/0              0/0                   20
   41  1/10
        1               0/0               0/0              0/0                   22
   41  1/10
        2               0/0               0/0              0/0                   25
   41  1/10
        3               0/0               0/0              0/0                   27
   41  1/10
        4               0/0               0/0              0/0                   30
   41  1/10
        5               0/0               0/0              0/0                   32
   41  1/10
        6               0/0               0/0              0/0                   35
   41  1/10
        7               0/0               0/0              0/0                   37
   41  1/10

    Class-map: Queue3 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 15% (15000 kbps)

    Class-map: Queue4 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 4
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 15% (15000 kbps)
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0 packets
        class       Transmitted         Random drop      Tail drop          Minimum
 Maximum     Mark
                pkts/bytes            pkts/bytes       pkts/bytes           thresh
thresh     prob

        0               0/0               0/0              0/0                   16
   32  1/10
        1               0/0               0/0              0/0                   18
   32  1/10
        2               0/0               0/0              0/0                   20
   32  1/10
        3               0/0               0/0              0/0                   22
   32  1/10
        4               0/0               0/0              0/0                   24
   32  1/10
        5               0/0               0/0              0/0                   26
   32  1/10
        6               0/0               0/0              0/0                   28
   32  1/10
        7               0/0               0/0              0/0                   30
   32  1/10

    Class-map: Queue5 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 5
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 10% (10000 kbps)

    Class-map: class-default (match-any)
      21 packets, 1890 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 83 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 21/1890
      bandwidth 20% (20000 kbps)
```

Reference: Forwarding and QoS CLI Commands

Monitoring Commands

Use the following commands to monitor forwarding and QoS on a Cisco IOS XE SD-WAN device:

```
show sdwan policy access-list-associations
show sdwan policy access-list-counters
show sdwan policy access-list-names
show sdwan policy access-list-policers
show sdwan policy data-policy-filter
show sdwan policy rewrite-associations
show policy-map interface GigabitEthernet0/0/2
```