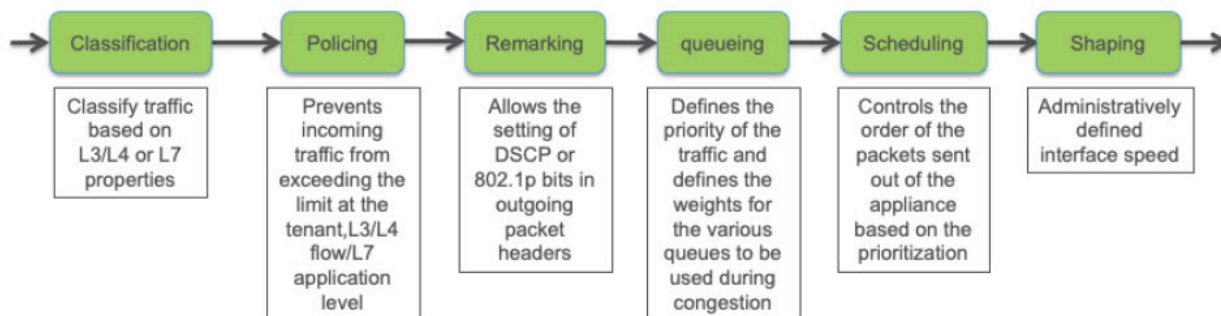


QoS

 For supported software information, click [here](#).

To handle periods of network congestion, you can configure quality of service (QoS), also known as class of service, or CoS, to ensure that the network prioritizes business critical traffic over less important traffic and treat this traffic with higher priority. You can also use QoS for other tasks, such as policing, shaping, and remarking the QoS bits in the IPv4/IPv6 and VLAN headers.

The following figure shows how a packet that is processed by QoS functions flows through a Versa Operating System™ (VOS™) edge device. Each green box is a stage in the VOS QoS processing. The figure illustrates the order in which the QoS stages are performed by the VOS software.



This article discusses some of the QoS functions and best practices for using them.

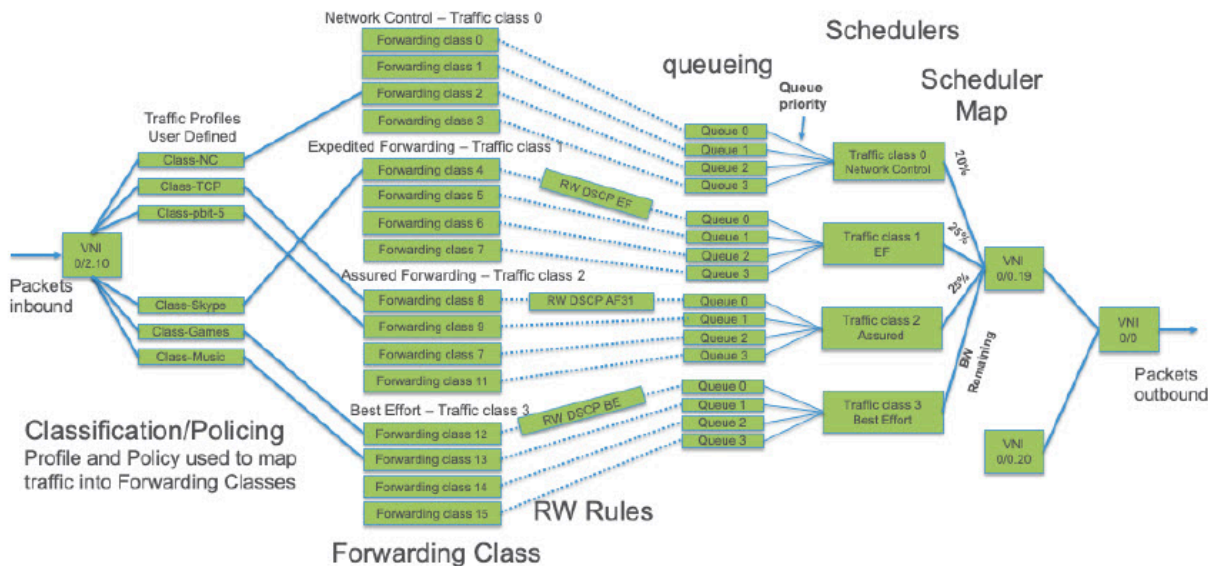
Classification

VOS edge devices support four traffic classes:

- Network control
- Expedited forwarding
- Assured forwarding
- Best effort

Each traffic class can use a maximum of four queues, and each queue can have a low or a high drop probability. The result is that 32 unique classification priorities are available.

If you use the default queue mapping, there are 16 forwarding classes that map to the forwarding queues, as illustrated in the following figure.

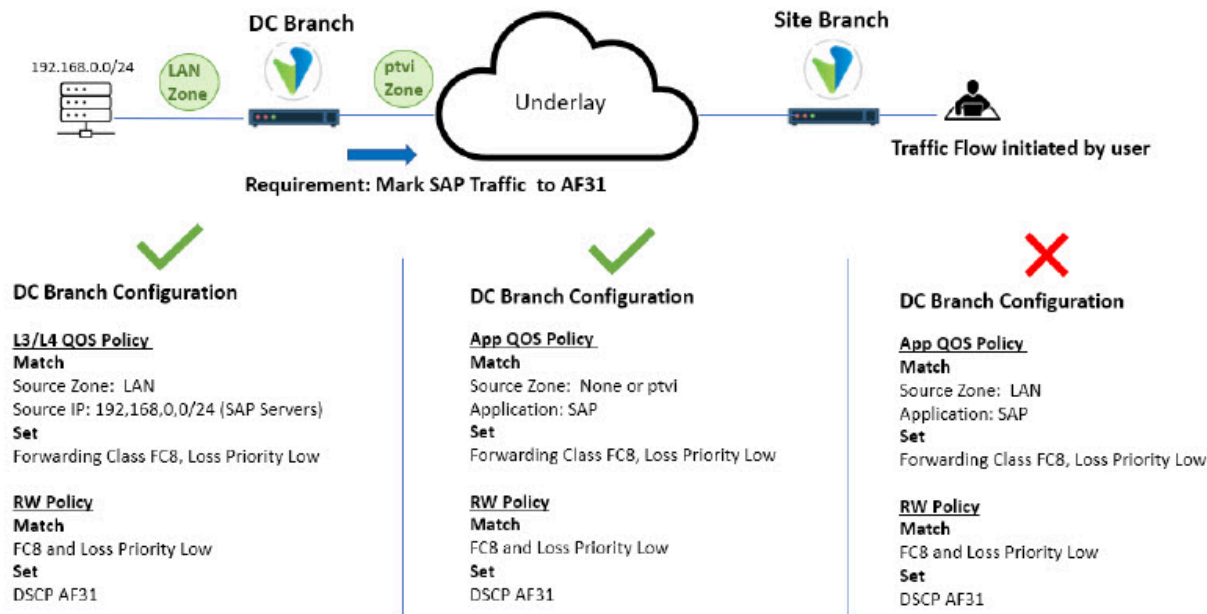


During the classification stage, ingress traffic is identified and associated with a forwarding class and loss priority. Classification can be done in two ways:

- Using QoS policies (Layer 3 and Layer 4 rules), which allow classification based on the following fields in the packet and packet header:
 - Destination port
 - Destination zone
 - DSCP
 - Ether-type
 - Ether-type-value
 - IEEE-802.1p
 - IP flags
 - Source IP address
 - Source port
 - Source zone
 - Time of day
 - TTL
- Using Application QoS (App QoS) policies (Layer 3 and Layer 7 rules), which allow classification based on the same fields as QoS policies classification as well as on applications and URL categories.

The following example illustrates how QoS classification works. Here, we have data center which hosts a SAP application that users access from remote locations, and we want to set the outgoing DSCP value of the SAP traffic on the data center MPLS WAN interface to AF31. The following figure illustrates the policies required to effect this scenario.

In addition to Layer 3/Layer 4 QoS policies and Layer 4 through Layer 7 App QoS policies, the configuration uses rewrite (RW) policies



On the VOS edge device in the data center, you apply an App QoS policy applies that matches the following conditions:

- Source zone—LAN
- Application—SAP

This App QoS policy references a QoS profile that places this traffic in the forwarding class FC8. Then, you apply a QoS propagation policy (that is, a rewrite policy) on the MPLS WAN network that remarks all FC8 traffic to a DSCP value of AF31.

This configuration works only if the traffic originates on a LAN connected to the data center VOS device. When the traffic originates from remote branch clients that are accessing the SAP application, the return traffic arrives from the DC LAN to the client. The traffic does not match the App QoS policy even though the source zone is set to LAN, because the App QoS policy classifies traffic based on a flow. Because the traffic originated at the remote branch, the first packet in the flow came from the PTVI zone (the PTVI zone is for traffic received over the SD-WAN overlay network), and so it does not match the App QoS policy whose source zone is set to LAN. Therefore, although the QoS rewrite policy is applied to traffic outgoing towards the MPLS network, the classification for the flow is performed when the packets arrive on this branch from the remote site.

The proper configuration is to have a match condition that either sets the source zone to PTVI or leaves the source zone empty, so that the SAP application matches regardless of whether it was initiated from a remote site or the local LAN.

The flow must be classified twice separately for both session directions: forward bidirectional flow and opposite bidirectional flow. For example:

- Forward-Initiated-App-QoS-Policy Match—Source LAN, destination PTVI will match the session for both session directions, forward and reverse: LAN-to-PTVI and PTVI-to-LAN.
- Reverse-Initiated-App-QoS-Policy Match—Source PTVI, Destination LAN will match the session for both session directions, forward and reverse: PTVI-to-LAN and LAN-to-PTVI.

If you must use a Layer 3/Layer 4 QoS policy in this use case, you need to match based on the IP address of the SAP application or on the source port, because a Layer 3/Layer 4 QoS policy does not support application-based matching. For a Layer 3/Layer 4 policy, the match is only in one direction, so you can specify the source LAN zone even if the traffic originates from a remote branch.

The flow must be classified twice separately for both flow directions: forward session direction and reverse session direction. For example:

- Forward-QoS-Policy Match—Source LAN, destination PTVI.
- Reverse-QoS-Policy Match—Source PTVI, destination LAN.

The following are best practices for QoS classification:

- Ensure that you use the correct match conditions, especially when you define source- or destination-based match conditions in an App QoS policy.
- When a traffic matches both a Layer 3 or Layer 4 QoS profile and an App QoS policy, the App QoS policy takes precedence.
- Verify the session details from the CLI to determine whether the session is attached to the expected QoS policy rule.

Policing Ingress Traffic

Policing allows you to rate-limit ingress traffic, providing a mechanism to prevent ingress traffic from overloading an egress port or the VOS device itself.

You can configure policing at the following levels. The policing configured at a lower level takes precedence over the policing configured at a higher level.

- Globally, at the tenant level, to enforce licensed bandwidth
- At the Layer 3/Layer 4 QoS policy level, for unidirectional policing on ingress traffic only
- At the Layer 7 App QoS policy level, for bidirectional policing on ingress and egress traffic

Policing uses the following parameters:

- Peak rate, which defines the maximum transmission rate, in pps or Kbps.
- Burst size, which defines the number of bytes that are allowed beyond the configured peak rate. You set the burst size to avoid retransmission during bursts of traffic.
- Loss priority to be used by congestion-avoidance algorithms.



The following are best practices for policing:

- The default maximum burst size for a policer is 15000 bytes.
- Use a policer rather than a shaper for real-time traffic especially for traffic that is sensitive to jitter, such as voice traffic.
- You can configure a policer at the tenant level to protect aggregated SD-WAN licensed bandwidth. For example, if two tenants are configured on VOS device that has a licensed bandwidth of 200 Mbps, you can configure a 100-Mbps policer for each organization to ensure fairness between them.
- A tenant-level policer applies only to inbound traffic arriving on the VOS device from a LAN or WAN interface. Hence, you can use a tenant-level policer to limit the download and upload bandwidth for a particular organization.

Use QoS Policy as an Access Control List

You can use QoS policies to emulate the function of an access control list (ACL) in a deployment in which no security services are configured and you want to deny traffic that matches a particular Layer 3 or Layer 4 rule. To do this, you create a QoS policy rule that has a match condition and a Deny action. Note that you can apply QoS policy to deny traffic only for through traffic or for external traffic destined for the VOS device. You cannot use QoS policy rules to control traffic generated by the VOS device itself.

To configure a policy rule to deny traffic:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. In the Networking  tab in the left menu bar, select Class of Service > QoS Policies.
4. Select the Rules tab in the horizontal menu bar to define the matching criteria to select the incoming packets to which to apply the QoS policy.
5. Click the  Add icon to add the rule.
6. To have the match condition be a source zone, select the Source/Destination tab and then select the source zone.

Add QoS Rule [X]

General **Source/Destination** Headers/Schedule Layer2 Enforce

☐ Source Zone [+ -]
☐ Intf-Internet-2-Zone
Source Zone Match
[+ New Zone](#)

☐ Destination Zone [+ -]

[+ New Zone](#)

☐ Source Address [+ -]

[+ New Address Group](#) [+ New Address](#)

☐ Destination Address [+ -]

[+ New Address Group](#) [+ New Address](#)

☐ Source Address Negate ☐ Destination Address Negate

[OK](#) [Cancel](#)

7. Select the Enforce tab to configure the Deny action.

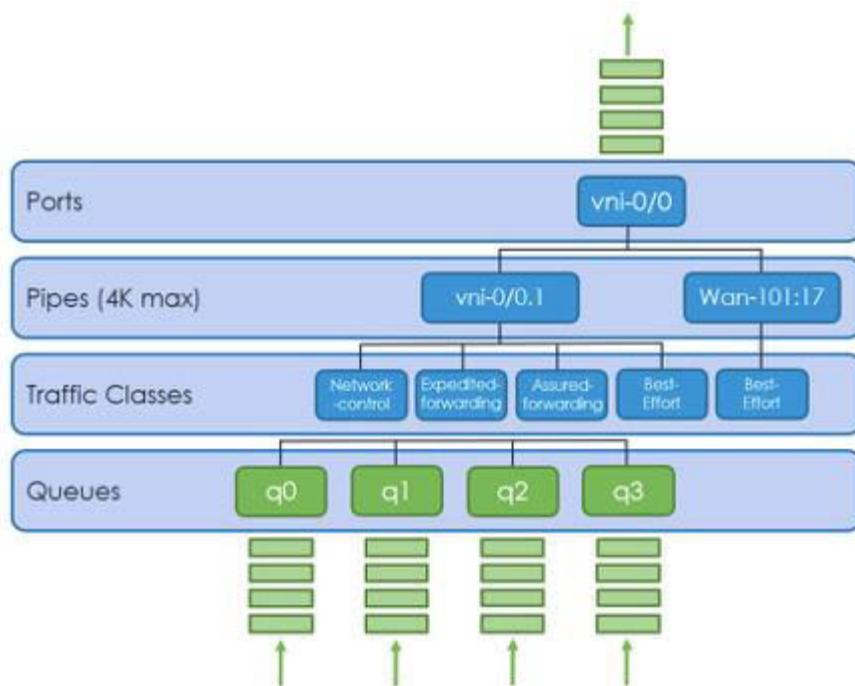
8. Click OK.

The following are best practices for using QoS Policy to emulate access lists:

- Create a QoS policy with a source zone that matches the VOS device interface you want to protect and associate the Deny action with the zone. You could use this configuration, for example, to prevent a WAN interface from being ping-able from the internet.
- Use this style of QoS policy as a stateless access list to block certain traffic.

Hierarchical Shaping

You can configure a hierarchical scheduler block on an egress interface to schedule and shape traffic. The following figures illustrates the arrangement of hierarchical shapers on VOS Edge devices.



You can use schedulers to perform shaping at the following levels:

- Port
- Pipe
- Traffic class

All ports have equal priority.

All pipes with a port have equal priority. A pipe represent seither a VLAN interface or a dynamically created IPsec path.

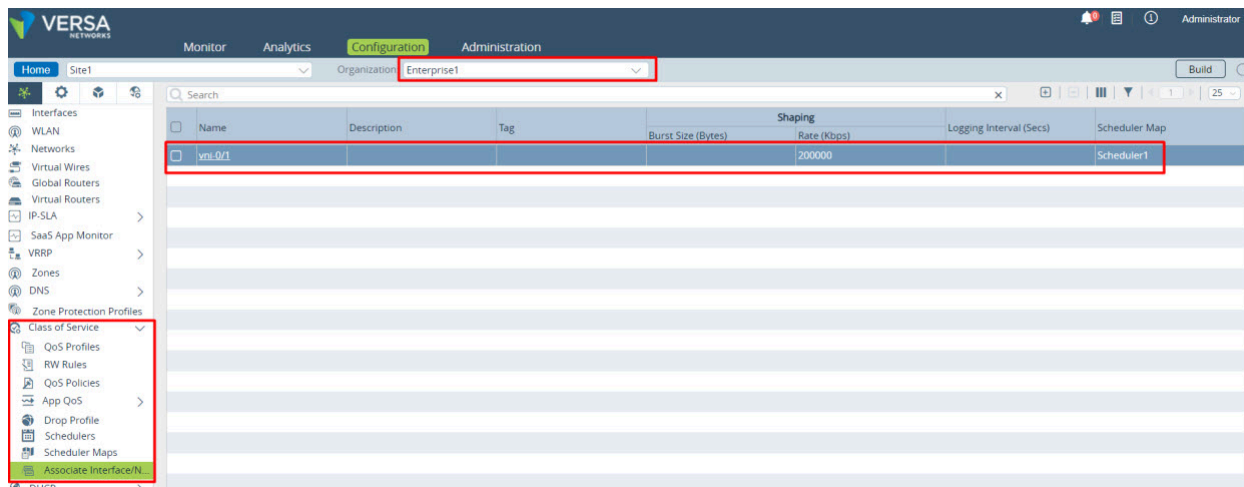
Traffic classes a pipe are handled in a strict priority order, which is, from highest to lowest, network control (tc0), expedited forwarding (tc1), assured forwarding (tc2), and best effort (tc3). Each traffic class has four queues that are scheduled using weighted round-robin (WRR).

The following are best practices for hierarchical shapers:


- To ensure that a higher priority traffic class does not starve the other traffic classes, thus ensuring both priority and fairness, apply a shaper at the port level. and configure a scheduler for each traffic class as a percentage of the port shaper rate or using an exact rate. For instance, an incorrectly configured network control traffic class can starve traffic classes 1, 2, and 3 if no transmit rate is configured and the network control traffic is using all available bandwidth on the port.
- For each scheduler, you can associate a unique drop profile for each loss priority as a congestion avoidance mechanism, that uses the. weighted random early detection (WRED) algorithm to keep track of queue depth and then, when the threshold is reached, starts randomly dropping packets.
- The shapers burst size is automatically set to the interface link speed divided 8000 bytes (burst size = interface link speed/8000 bytes) as per the Intel recommendation. If you configure a higher burst size, it may work but it may cause intermittent drops as a result of hardware limitations.

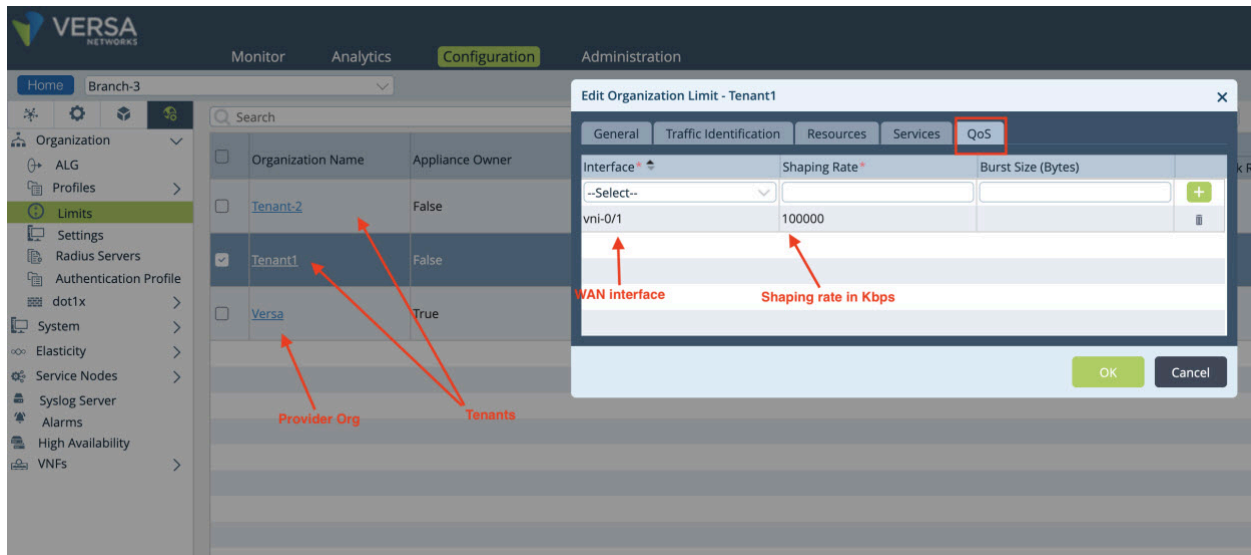
Per-Tenant Shapers

On VOS edge devices, you can configure traffic shapers for individual provider organizations to allocate the amount of WAN-facing bandwidth available on a per-tenant basis. The prerequisite for doing this is that you must have already configured CoS for the provider organization and already applied it to the WAN interface on which you want to configure a per-tenant shaper, as illustrated in the following screenshot.



Then configure the per-tenant traffic shaper for the tenant or tenants:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. Select Others  > Organization > Limits in the left menu bar.
4. Select the tenant in the main panel. The Edit Organization Limit popup window displays.
5. Select the QoS tab. In the Interface, select the WAN interface, and in the Shaping Rate field, enter the shaping rate, in Kbps.



6. Click OK.

The following is a best practice for per-tenant shapers:

- On a multitenant branch, configure the amount of bandwidth each tenant is entitled to use. For example, on a branch with two tenants that are allowed 100 Mbps of bandwidth, configure the shaping rate for each tenant to enforce fairness between tenants.

QoS Rewrite and Propagation

Rewrite (RW) rules allow you to rewrite the attributes of packets QoS attributes as they are leaving the VOS device so that you can convey the importance of the packet. Downstream nodes can use the QoS attributes to classify traffic and then take the appropriate scheduling action, or in case of congestion can give precedence to critical traffic. A rewrite rule rewrites QoS bits for an existing forwarding class.

With rewrite rules, you can rewrite the following fields:

- IEEE 802.1p bits in the VLAN header
- TOS bits in the IPv4 header
- Traffic class bits in the IPv6 header

The Versa Networks technology uses an overlay to transport packets from one branch to another. The packets are encapsulated in a VXLAN header and then transported to the remote branch. Hence, the packets have two headers, referred to as the inner header and the outer header. You can use two methods to change the QoS markings on the inner and outer headers:

- Use a rewrite policy to classify traffic and set the QoS bits.
- Use rewrite options to copy the inner header markings to the outer header, and vice versa.

Rewrite Policy

You can use a rewrite policy to remark packets and frames based on the classification done on ingress. The classification is done using a Layer 3/Layer 4 or App QoS policy that assigns the packets to a forwarding class and loss priority. The rewrite policy uses the forwarding class and loss priority information as match conditions to set a QoS value.

A typical use case is to rewrite the LAN traffic passing through a CPE device, whether the traffic is destined for another LAN port or for egress somewhere else on a remote branch. The DSCP of the traffic is modified and is carried, or propagated, with the traffic as it moves through the network.

There are three types of rewrite policies:

- DSCP rewrite policy
- DSCP6 rewrite policy
- 802.1p rewrite policy

Depending on where you apply the rewrite policy, it modifies the QoS bits of either the inner or outer header, but it does not propagate.

In a rewrite policy, the match condition is the forwarding class and the loss priority. You configure the forwarding class in the QoS profile, which is referenced in the Layer 3/Layer 4 or App QoS policy.

You enable the following options in the QoS profile depending on whether the type of rewrite policy:

- DSCP Rewrite
- Dot 1P Rewrite

If you do not select either the DSCP rewrite or Dot 1P rewrite option in the QoS profile, the rewrite policy does not take effect.

Add QoS Profile
✕

Name*

Description

Ingress Policing

Peak Rate (pps)
Peak Rate (Kbps)
Peak Burst Size (Bytes)

Forwarding Class

Forwarding Class*
Loss Priority*

☒ DSCP Rewrite
☒ Dot 1P Rewrite

OK

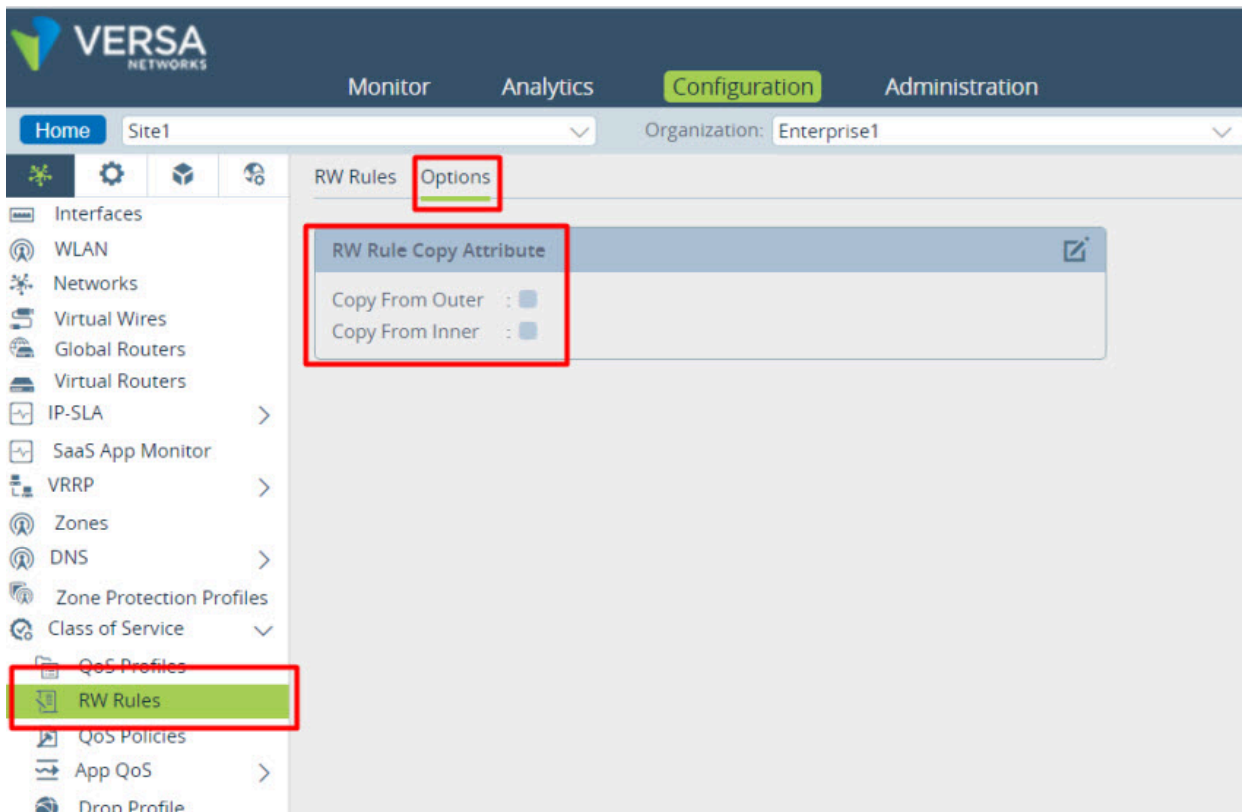
Cancel

One use case for this setting is when you have more than one QoS policy that classifies traffic to the same forwarding class. However, if you do not need to remark all the traffic with the rewrite policy, you can use this setting to help differentiate which traffic is forwarding class is evaluated by the rewrite policy.

A second use case is on a multitenant VOS device. on which the rewrite policy is applied on the WAN interfaces that are owned by the provider. If there are two customer tenants on the branch and each tenant uses the same forwarding class in their QoS policies, they can choose whether to set the DSCP Rewrite and Dot1P Rewrite option, depending on whether they want their traffic to be remarked..

Rewrite Options

The rewrite options set a flag to copy the markings between the inner and outer IP headers. This is a global setting, so it affects all the traffic passing through the VOS device. You cannot apply in on a per-interface or per-traffic class basis.



You can configure the following options:

- Copy From Outer—Copy the marking of the outer IP header to the inner IP header when a branch sends packets to a remote branch.
- Copy From Inner—Copy the marking of the inner IP header to the outer IP header when a branch receives packets from a remote branch.

The Copy From Outer setting remarks the inner IP header of traffic coming from a remote site. If the outgoing network applies a rewrite policy that also remarks the inner IP header of the same packet, the marking in the rewrite policy overwrites the marking made by the Copy From Outer option. For example, on a regular branch the outgoing network could be a LAN and, on the hub the outgoing network could be a WAN interface.

With the Copy From Outer setting, the VOS edge device trusts the markings from the underlay. You should trust outer markings on packets received on a private circuit such as MPLS, but you should not trust them on packets received not from the internet. Therefore, you should use this setting only on a branch that has only an MPLS WAN circuit.

The Copy From Inner settings works on a model whereby the VOS device trusts the markings from the LAN. Because this setting remarks the outer IP header of the traffic coming from the LAN site, if you apply a rewrite policy on the WAN network that also remarks the outer IP header of the same packet, the marking made by the Copy From Inner setting overrides the marking made by the rewrite policy.

QoS Propagation Policy on Hubs

On a hub, traffic that arrives encrypted from a remote site, is decrypted, and is encrypted again before it is sent it to another site. Because the packets are decrypted on the hub, the QoS propagation policy can remark both the inner and outer headers based on the classification made on the inner packet (that is, the actual application packet). The hub can also use the rewrite option flags like Copy From Outer and Copy From Inner.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Adaptive Shaping](#)

[Configure CoS](#)

[Configure Policy-Based Forwarding](#)

[Configure Schedule Objects](#)