

---

## Configure Control and Management Plane Protection

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

The Versa Operating System™ (VOS™) basic solution tier subscription has features that protect critical functions of the control and management planes against surges in traffic volume. Surge protection prevents unnecessary traffic from overwhelming the control and management plane processes, thus preventing this traffic from affecting the normal functioning of the system.

Control plane processes include ARP, multicast, BGP, DHCP, DNS, and OSPF. Management plane processes include FTP, NTP, SNMP, SSH, and TFTP. Typically, traffic that a VOS device receives over network interfaces, such as LAN and WAN interfaces, is categorized as either control and management plane traffic or as data plane traffic. Any traffic not handled by the control and management plane processes is considered to be data plane traffic and is handled by the VOS network and security functions.

The standard VOS zone protection and denial-of-service (DoS) features, which are part of the VOS firewall services, protect against surges in data plane traffic, such as DoS attacks, preventing the data traffic from passing to the end VOS devices.

This article primarily discusses how VOS devices process control plane traffic and how this processing impacts the security of the VOS device.

As a security-hardening measure, control plane services are not enabled on VOS devices by default. This means that, by default, all traffic categorized as control plane traffic is dropped immediately. You must explicitly enable any desired control plane services, such as a DHCP server or relay, BGP, or OSPF, so that VOS devices allow that particular type of control plane traffic. For the control plane services that you enable, you can configure them to protect against traffic surges. For example, a DoS attack can cause a spike in control plane utilization. While the VOS device can manage high CPU conditions using the self-protection features provided by the Linux kernel, the response of the device may slow down. So, to protect the VOS control plane services against DoS attacks, and for additional control and management plane protection, you can configure class of service (CoS) to prioritize traffic so that more important traffic is handled with a higher priority. For more information, see [Configuration Example for Control Plane and Management Plane Protection](#) below.

By default, VOS devices implement a deny-all approach, and only ports that are essential for a configured service are kept open. This strategy also applies to traffic inbound to the host. For example, UDP ports 67 and 68 are open only when you configure a DHCP service. For a LAN device on which you enable a DHCP server or configure DHCP relay, the two UDP ports are used to assign IP addresses to LAN users. For a WAN device, the ports are used by DHCP to

assign IP addresses. This traffic limiting also applies to other services. For example, if you configure DNS proxy, TCP, or UDP, port 53 is opened on the LAN side. You do not have to create a QoS deny policy on the VOS device to block unauthorized inbound host traffic, because the VOS device does not respond if a service is not configured.

To prevent traffic from overwhelming the control and management planes, and to fully protect VOS devices, you can use policers to limit the rate of inbound host traffic for the following protocols: BFD, BGP, DHCP, DNS, ICMP, NTP, OSPF, SSH, and VRRP. Choosing the policer rate for each protocol depends on multiple factors, including the network infrastructure and configuration, the number of users on a particular segment, VOS device hardware, and the services used. For example, for a small branch, the policer rate can include an observation period to check whether the threshold is crossed on the CoS policer. Periodic verifications can reveal whether the policer rate is too high to allow for normal operations, or whether the root cause of a traffic issue is a transient problem. Based on these results, you can change or optimize the policer rate. Note, however, that policers for control and management traffic are not widely deployed and so control and management plane protection mainly relies on the default built-in protections described above. For more information, see [Policing Ingress Traffic](#).

## Configure Control Plane and Management Plane Protection

To configure control plane and management plane rate-limiting protection:

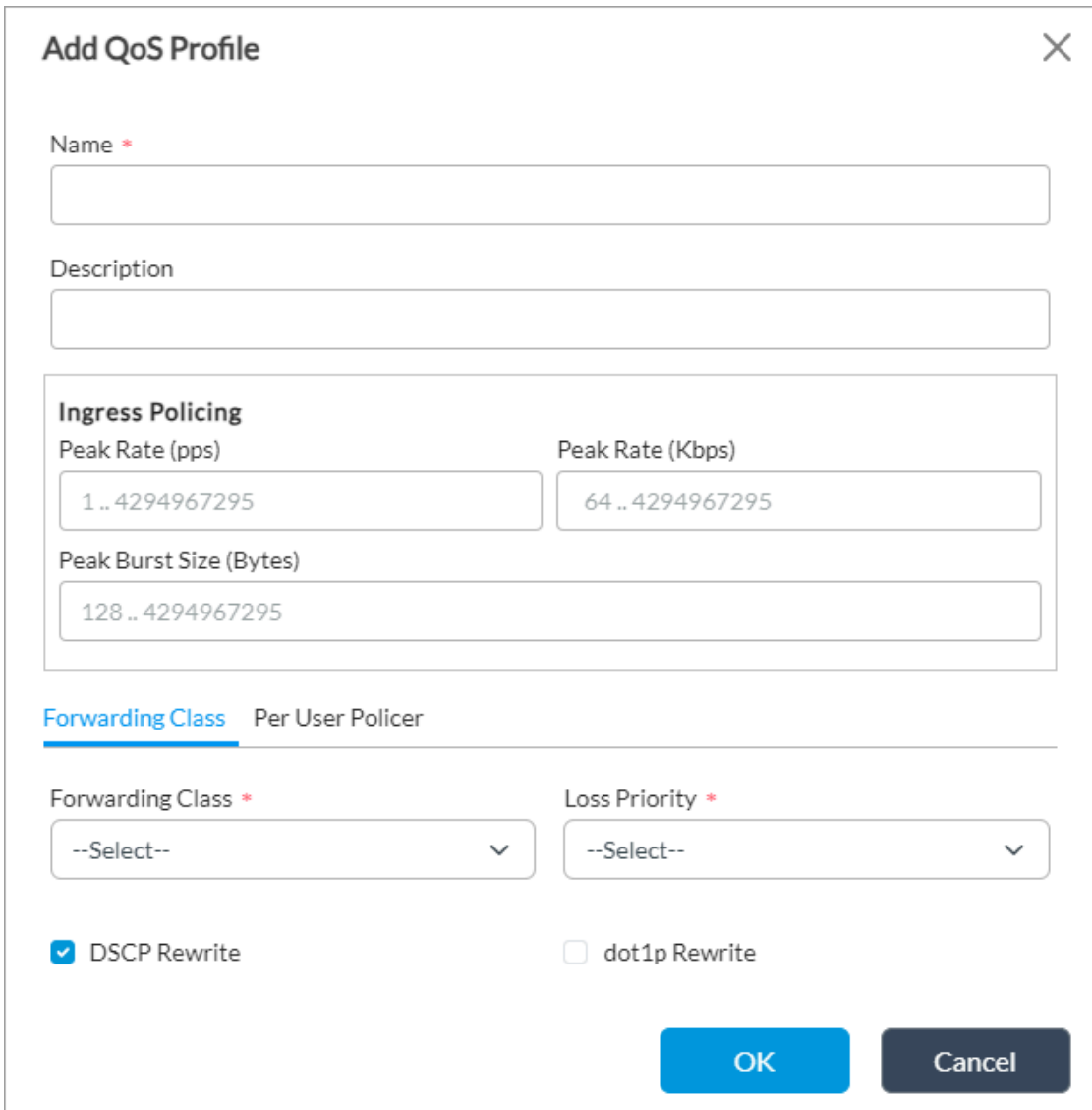
1. Configure a QoS profile to limit traffic:
  - a. In Director view:
    - i. Select the Configuration tab in the top menu bar.
    - ii. Select Devices > Devices in the horizontal menu bar.
    - iii. Select an organization in the left menu bar.
    - iv. Select a Controller node in the main pane. The view changes to Appliance view.
  - b. Select the Configuration tab in the top menu bar.
  - c. Select Networking > Class of Service > QoS Profiles in the left menu bar.

The screenshot shows the Versa Networks configuration interface. At the top, there are tabs for 'Director View', 'Appliance View' (selected), and 'Template View'. Below these are tabs for 'Monitor', 'Analytics', 'Configuration' (selected), and 'Administration'. The main header shows 'Appliance: SDWAN-Controller1' and 'Organization: Tenant12'. A message states 'You are currently in Appliance View'. The left sidebar has a menu with 'Networking', 'Services', and 'Objects & Connectors'. Under 'Networking', there are options like 'SaaS App Monitor', 'VRRP', 'Zones', 'DNS', 'LLDP', 'Zone Protection Profiles', 'Class of Service' (expanded), and 'RW Rules'. 'QoS Profiles' is highlighted under 'Class of Service'. The main pane shows a table with the following data:

	Name	Peak Rate (pps)	Peak Rate (Kbps)	Peak Burst Size (Byte)	Forwarding Class	Loss Priority	DSCP Rewrite	dot1p Rewrite
<input type="checkbox"/>	default_qos	700			Forwarding Class 13	low	Yes	No

At the bottom of the table, it says 'Rows per page: 25' and 'Showing 1 - 1 of 1'.

- d. Click the  Add icon to add a QoS profile. The Add QoS Profile window displays.



The 'Add QoS Profile' window is a modal dialog with a title bar and a close button (X) in the top right corner. It contains several input fields and checkboxes. The 'Name' field is required, indicated by a red asterisk. The 'Description' field is optional. The 'Ingress Policing' section contains three input fields: 'Peak Rate (pps)' with a range of '1 .. 4294967295', 'Peak Rate (Kbps)' with a range of '64 .. 4294967295', and 'Peak Burst Size (Bytes)' with a range of '128 .. 4294967295'. Below this, there are two tabs: 'Forwarding Class' (selected) and 'Per User Policer'. The 'Forwarding Class' tab contains two dropdown menus: 'Forwarding Class' and 'Loss Priority', both with a red asterisk and a '--Select--' placeholder. At the bottom, there are two checkboxes: 'DSCP Rewrite' (checked) and 'dot1p Rewrite' (unchecked). The window ends with 'OK' and 'Cancel' buttons.

**Add QoS Profile**

Name \*

Description

**Ingress Policing**

Peak Rate (pps) Peak Rate (Kbps)

1 .. 4294967295 64 .. 4294967295

Peak Burst Size (Bytes)

128 .. 4294967295

**Forwarding Class** Per User Policer

Forwarding Class \* Loss Priority \*

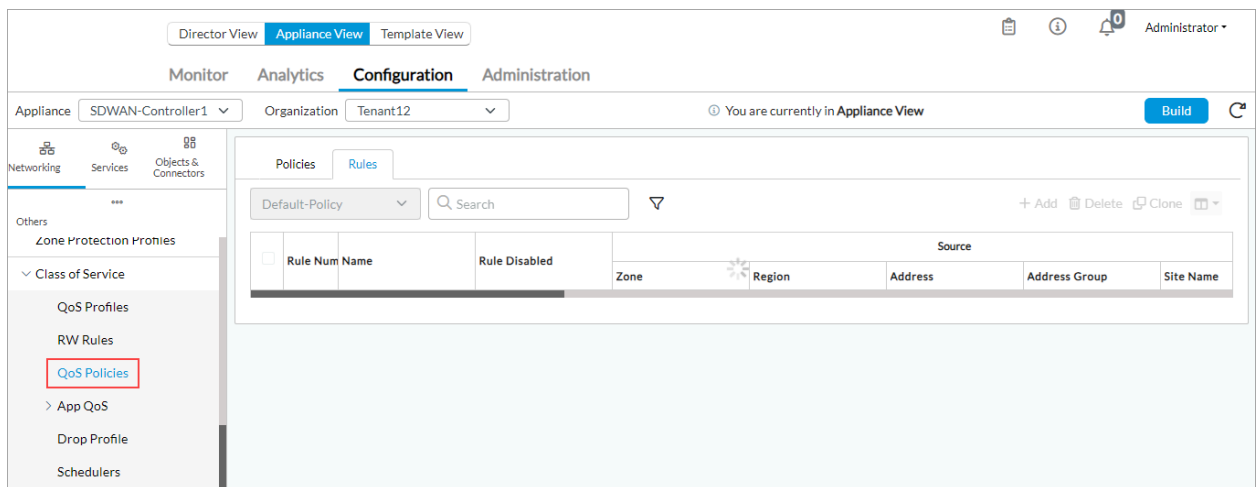
--Select-- --Select--


☒ DSCP Rewrite ☐ dot1p Rewrite

OK Cancel

- e. Enter a name for the QoS profile (here, Low-Bandwidth).
- f. Enter values for Peak Rate (Kbps) and Peak Burst Size (Bytes).
- g. For information about configuring the other fields, see [Configure QoS Profiles](#).
- h. Click OK.
2. Configure a QoS policy rule to associate with the QoS profile. You can also configure additional match criteria, as required. In this example, ICMP and destination IP address zone (host) are configured.
- a. In Director view:
- Select the Configuration tab in the top menu bar.
  - Select Devices > Devices in the horizontal menu bar.
  - Select an organization in the left menu bar.

- iv. Select a Controller node in the main pane. The view changes to Appliance view.
- b. Select the Configuration tab in the top menu bar.
- c. Select Networking > Class of Service > QoS Policies in the left menu bar.



- d. Select the Rules tab in the horizontal menu bar.
- e. Click the  Add icon to add a QoS policy rule. The Add Rule popup window displays.
- f. Select the General tab.

### Add QoS Rule

General
Source
Destination
Headers/Schedule
Layer2
Enforce

Name \*
ICMP-Policer

Session Timeout (secs)
1 .. 15999999

Description

Tags

☐ Disable Rule

OK

Cancel

- g. Add a name for the QoS rule (here, ICMP-Policer).
- h. Select the Destination tab.

Add QoS Rule

General
Source
Destination
Headers/Schedule
Layer2
Enforce

☐
Destination Zone

+ New Zone

+

Destination Zone Not Configured

☐
Destination Address

+ New Address

+ New Address Group

+

Destination Address Not Configured

☐
Destination Site Name

+

Destination Site Name Not Configured

☐
Custom Geo Circle

+

Custom Geo Circle Not Configured

☐
Region

+

Region Not Configured

☐
State

+

State Not Configured

☐
City


+

City Not Configured

☐ Destination Address Negate
☐ Destination Location Negate

OK

Cancel

- i. In the Destination Zone table, click the  Add icon, and select a host from the options to protect ICMP traffic to the host. You can also select IP addresses to protect from traffic. For more information, see [Configure Address Objects](#).
- j. Click + New Zone to add a zone. For more information, see [Configure Zones and Zone Protection Profiles](#).
- k. Select the Headers/Schedule tab.

Add QoS Rule

General

Source

Destination

Headers/Schedule

Layer2

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

TTL

Condition

Greater than or equal to

Value (Max 255)

1..255

Others

Schedules

--Select--

+ Schedule

Services

☐


Service List

+ New Service

Service List Not Configured

OK

Cancel

- I. In the Services table, click the  Add icon, and select ICMP from the predefined list. You can also select OSPF or BGP from the predefined list. To combine two service objects, such as ICMP and BGP in a QoS rule, select both the services from the predefined list. For example:

Add QoS Rule

General
Source
Destination
Headers/Schedule
Layer2
Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

+

TTL

Condition

Greater than or equal to

Value (Max 255)

1..255

Others

Schedules

--Select--

+ Schedule

Services

☐
Service List

+ New Service

+

Service List Not Configured

OK

Cancel

- m. Click + New Service to add a new service. For more information, see [Configure Service Objects](#).
- n. Click the Enforce tab to associate the rule with the QoS profile.

**Add QoS Rule** [X]

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

**Action Setting**  
☒ Allow ☐ Deny ☐ Bypass Service

Anchor Core Class  
 --Select--

**QoS Profile Setting**  
 QoS Profile  
 --Select--

**Permit Existing Flow**  
 Permit Existing Flow  
 --Select--

OK Cancel

- o. In the QoS Profile field, select the QoS profile that you configured in Step 1.
- p. For more information about configuring other fields, see [Configure QoS Policies](#).
- q. Click OK to configure a QoS rule for control plane and management plane protection.

You can also configure QoS policy rules for control and management plane protection using broadcast or multicast packet floods by setting traffic limits:

1. In the Add QoS Rule popup window, select the Layer 2 tab.
2. In the MAC Address Type field, select broadcast or multicast in the MAC Address Type field.

**Add QoS Rule** [X]

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

MAC Address Type  
 --Select--  
 --Select--  
 Broadcast  
 Multicast

IEEE 802.1p Values  
 [Text Field] +

Ether type Value ☐ None

OK Cancel

3. For more information about configuring the other fields, see [Configure QoS Policies](#).
4. Click OK.



---

## Monitor QoS Profiles and Policer Statistics

You monitor the policer statistics for QoS policies, checking the packets per second (pps) policer configured for ICMP traffic towards the host. For more information, see [Monitor Device Services](#).

To monitor QoS profiles:

1. Select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. Select a device name in the main pane. The view changes to Appliance view.
4. Select the Monitor tab in the top menu bar.
5. Select the organization or tenant in the left menu bar.
6. Select Networking > CoS, and click the QoS Policies tab.
7. Select a policy from the drop-down list. The QoS policy statistics displays information such as the number of dropped packets and bytes.

The screenshot displays the Versa Networks SD-WAN management interface. At the top, there are tabs for 'Director View', 'Appliance View' (selected), and 'Template View'. Below this is a navigation bar with 'Monitor', 'Analytics', 'Configuration', and 'Administration'. The 'Monitor' tab is active, and the 'Organization' is set to 'Tenant1'. A 'Build' button is visible on the right. The main content area shows 'Total Appliances: 7' and a list of appliances, with 'SDWAN-Branch1' selected. Below this, the device details for 'SDWAN-Branch1' are shown, including its location, management address, and system bridge address. A 'Reachable' status is indicated. The 'Networking' tab is selected, and the 'COS' sub-tab is active. Under 'COS', the 'QoS Policies' sub-tab is selected. A dropdown menu shows 'Default-Policy'. Below this, a table displays QoS statistics for 'policy1'. The table has columns for 'Rule Name', 'QoS Hit Count', 'QoS Drop Pac...', 'QoS Drop Byt...', 'QoS Forward ...', 'QoS Forward ...', 'QoS Session D...', 'QoS Drop Pac...', 'QoS Drop Byt...', 'QoS Drop Pac...', 'QoS Drop Byt...', and 'Dropped'. The values for 'policy1' are: 3276738, 0, 0, 3276738, 264984344, 0, 0, 0, 0, 0, 0, 0.

Rule Name	QoS Hit Count	QoS Drop Pac...	QoS Drop Byt...	QoS Forward ...	QoS Forward ...	QoS Session D...	QoS Drop Pac...	QoS Drop Byt...	QoS Drop Pac...	QoS Drop Byt...	Dropped
policy1	3276738	0	0	3276738	264984344	0	0	0	0	0	0

---

## Supported Software Information

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

---

## Additional Information

[Configure Address Objects](#)

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Common\\_Configuration/Configure\\_Contr...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Contr...)

Updated: Wed, 23 Oct 2024 08:27:45 GMT

Copyright © 2024, Versa Networks, Inc.

[Configure CoS](#)

[Configure Service Objects](#)

[Configure Zones and Zone Protection Profiles](#)

[Licensing Overview](#)

[Monitor Device Services](#)

[QoS in SD-WAN Design](#)