
Configure Service and Session Options



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

A Versa Operating System™ (VOS™) device is preconfigured with service options that define optimal operational and performance parameters for the device. In most cases you should never modify these parameters without explicit guidance from a Versa Networks technical team member. However, you can choose to modify the following:

- Maximum number of sessions allowed on a VOS device. This maximum is the total number of sessions for all tenants on the VOS device.
- Session-related parameters, such as the timeout values for a session and for particular protocols, and the TCP MSS adjustment.
- IPsec cipher key check, to comply with NIAP FCS_IPSEC_EXT.1.14 requirements (for Releases 22.1.1 and later).

Note: For options not discussed in this article, do not modify them without explicit guidance from a Versa Networks technical team member.

Change the Maximum Number of Allowed Sessions

For Releases 20.2.3 and later, the default maximum number of sessions that a VOS device supports is automatically adjusted down or up based on the total amount of system memory.

The following table shows the maximum number of sessions supported for different amounts of memory. It is recommended that you not increase the maximum number of sessions beyond the values shown in the table, because the VOS software is tuned to handle the maximum values.

Total Memory (RAM)	Maximum Number of Sessions
4 GB	32,000
8 GB	100,000
16 GB	500,000
32 GB	1,000,000
64 GB	2,500,000
96 GB	4,000,000

Total Memory (RAM)	Maximum Number of Sessions
> 96 GB	5,000,000

For an amount of RAM not listed in the table above, the default maximum number of sessions is 5,000,000.

Note that you should change the maximum number of sessions only during a service maintenance window, because as soon as you make the change, all services on the VOS device restart automatically.

For Release 20.2.3, Release 21.1.1, and Release 21.1.2 you cannot modify the default maximum number of sessions. If you need to change these values, contact Versa Networks Customer Support.

For Releases 20.2.4 and later, Releases 21.1.3 and later, and Releases 21.2.1 and later, you can modify the default maximum of sessions. However, before you change the values, it is recommended that you contact Versa Networks Customer Support.

It is recommended that you monitor the number of sessions and change the maximum number of sessions based on your peak production loads. For a VOS device to be operational, memory consumption should always be less than 90 percent. For VOS devices that have more than 32 GB RAM, you should also change the session limit at the tenant level. Otherwise, the maximum number of sessions is limited to 1 million per tenant regardless of the maximum limit set on the device. Note that when you change the session limit at the tenant, you do not need to restart services on the VOS device. To change the session limit for a tenant, see [Configure Organization Limits](#).

Because the earlier default value for the session limit was 1,000,000 (for releases prior to Release 21.2.1), if you configure a value of 1,000,000, you cannot distinguish between an explicitly configured value and the earlier system default. It is recommended that you configure a value slightly more or less than 1,000,000 to override the older default value of 1,000,000.

To change the maximum number of allowed sessions on a VOS device:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the left menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar.

Versa Networks

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Appliance: SDWAN-Branch1 You are currently in Appliance View **Build**

Networking Services **Objects & Connectors** Others

Search

> Organization

System

Configuration

Configuration

Core Profile

Speed Test

Domain Name Servers

Security Package Updates

> Time & Date

Storage Configurations

> Appliance User Manageme...

> Elasticity

> Service Nodes

Syslog Server

Alarms

Certificate Alarms Settings

VNF Manager

IP Address/Prefix : 192.168.75.2/32

Interface : tvi-0/41.0

Fix USB Port Affinity

Enable

Services

SFTP : WWW

SSH

Management

SSH

Maintenance Mode

Enable

ARP

Log Unknown Hostbound Packets Disabled

TCP Half Closed

TCP Secure Reset

Service Options

CGNAT Scale Factor : 8

Datapath RX-TX mode : poller

Driver Bulking : 16

Forwarding Queue : 16

Inter Thread Packet Rings Size : 0

Large Packet Buffer Cache : 256

Max Large Packet Buffer Size : 65535

Max Small Packet Buffer Size : 10000

Max Idle Sleep Time(micsec) : 10

Max Tenants : 32

Maximum Allowed Sessions : 1000000

Use Least Loaded Worker Thread

Least Loaded Worker Thread Mode : service-load

Traffic class Queue size : -

Nitrox Support

SDWAN Header Compression

Poller Count : -

QoS Frame Overhead Auto Adjust

QoS Frame Overhead Length : -

Continuous QoS Evaluation

Ignore SDWAN Peer Classification

Restart on Change

Run Mode : performance


Small Packet Buffer Cache : 32

Strip Input VLAN

Thread Bulking : 16

Token Bucket

Parameters

- In the Service Options pane, click the  Edit icon.
- In the Edit Service Options popup window, select the General tab.
- In the Maximum Allowed Session field, enter the number of sessions.

Edit Service Options



General QoS Path MTU Discovery IP Reassembly

Thread Bulking <input type="text" value="16"/>	Maximum Allowed Sessions <input type="text" value="1000000"/>	Driver Bulking <input type="text" value="16"/>	Poller Count <input type="text"/>
Number of RX Descriptors <input type="text" value="512"/>	Number of TX Descriptors <input type="text" value="512"/>	Worker Count <input type="text"/>	Inter Thread Packet Rings Size <input type="text" value="0"/>
Run Mode <div>Performance ▾</div>	Max Idle Sleep Time(micsec) <input type="text" value="10"/>	Min Idle Sleep Time(micsec) <input type="text" value="1000"/>	Datapath RX-TX mode <div>Poller ▾</div>
Forwarding Queue <div>16 ▾</div>	CGNAT Scale Factor <input type="text" value="8"/>	Max Tenants <input type="text" value="32"/>	Least Loaded Worker Thread Mode <div>Service Load ▾</div>
<input type="checkbox"/> Strip Input VLAN	<input type="checkbox"/> Minimal Core Support	<input type="checkbox"/> Nitrox Support	<input type="checkbox"/> VXLAN Entropy
<input checked="" type="checkbox"/> Token Bucket	<input type="checkbox"/> Restart on Change	<input type="checkbox"/> Tag Native VLAN	<input type="checkbox"/> Use Least Loaded Worker Thread
<input checked="" type="checkbox"/> TPM Support	<input checked="" type="checkbox"/> Crypto Accelerator Support	<input type="checkbox"/> IPsec Cipher Key Check	<input type="checkbox"/> SDWAN Header Compression
Host Huge Page Size <input type="text"/>	Total Huge Page Size <input type="text" value="0"/>	CPU Load Type <div>Service ▾</div>	<input type="checkbox"/> Ignore SDWANTE Path
			<div>OK Cancel</div>

- Click OK. Note that you should change the maximum number of sessions only during a service maintenance window, because as soon as you click OK, all services on the VOS device restart automatically.

Configure IPsec Cipher Key Check

For Releases 22.1.1 and later.

You can configure a VOS device to meet NIAP FCS_IPSEC_EXT.1.14 requirements by enabling the IPsec cipher key check option. Enabling IPsec cipher key check affects the VOS device only when FIPS mode is enabled on the device. For information about enabling FIPS mode, see [FIPS Compliance](#).

To view, enable, or disable IP cipher key check for a VOS device:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a VOS device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Others > System > Configuration > Configuration in the left menu bar. The following screen displays.

Versa Networks

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Appliance: SDWAN-Branch1 You are currently in Appliance View **Build**

Networking Services **Objects & Connectors** Others

Search

> Organization

System

Configuration

Configuration

Core Profile

Speed Test

Domain Name Servers

Security Package Updates

> Time & Date

Storage Configurations

> Appliance User Management

Elasticity

Service Nodes

Syslog Server

Alarms

Certificate Alarms Settings

VNF Manager

IP Address/Prefix : 192.168.75.2/32

Interface : tvi-0/41.0

Fix USB Port Affinity

Enable : ☐

Services

SFTP : ☐ WWW : ☒

SSH : ☒

Management

SSH : ☒

Maintenance Mode

Enable : ☐

ARP

Log Unknown Hostbound Packets Disabled : ☐

TCP Half Closed : 8

TCP Secure Reset : 120

Service Options

CGNAT Scale Factor : 8

Datapath RX-TX mode : poller

Driver Bulking : 16

Forwarding Queue : 16

Inter Thread Packet Rings Size : 0

Large Packet Buffer Cache : 256

Max Large Packet Buffer Size : 65535

Max Small Packet Buffer Size : 10000

Max Idle Sleep Time(micsec) : 10

Max Tenants : 32

Maximum Allowed Sessions : 1000000

Use Least Loaded Worker Thread : ☐

Least Loaded Worker Thread Mode : service-load

Traffic class Queue size : -

Nitrox Support : ☐

SDWAN Header Compression : ☐

Poller Count : -

QoS Frame Overhead Auto Adjust : ☐

QoS Frame Overhead Length : -

Continuous QoS Evaluation : ☐

Ignore SDWAN Peer Classification : ☐

Restart on Change : ☐

Run Mode : performance

Small Packet Buffer Cache : 32

Strip Input VLAN : ☐

Thread Bulking : 16

Token Bucket : ☒

Parameters


4. In the Service Options pane, scroll down to view the setting for IPsec Cipher Key Check. A checked box icon indicates that a feature is enabled, and an unchecked box icon indicates that a feature is disabled.

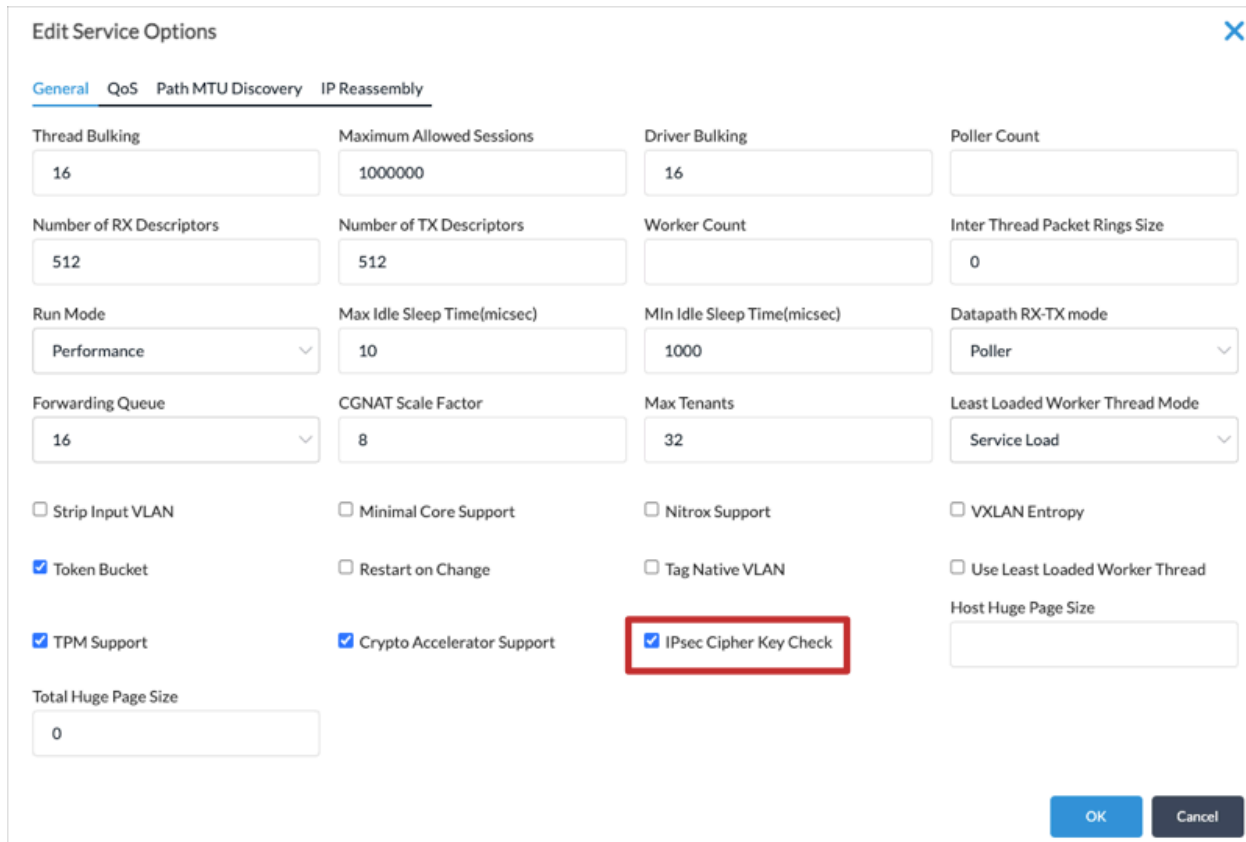
Service Options			
Maximum Allowed Sessions	: 1000000	Small Packet Buffer Cache	: 32
Use Least Loaded Worker Thread	: <input type="checkbox"/>	Strip Input VLAN	: <input type="checkbox"/>
Least Loaded Worker Thread Mode	: service-load	Thread Bulking	: 16
Minimal Core Support	: <input type="checkbox"/>	Token Bucket	: <input checked="" type="checkbox"/>
Min Idle Sleep Time(micsec)	: 1000	Worker Count	: -
Number of RX Descriptors	: 512	VXLAN Entropy	: <input type="checkbox"/>
Number of TX Descriptors	: 512	Crypto Accelerator Support	: <input checked="" type="checkbox"/>
Tag Native VLAN	: <input type="checkbox"/>	Host Huge Page Size	: -
TPM Support	: <input checked="" type="checkbox"/>	Total Huge Page Size	: 0
Max Life Time	: 15	Path MTU Discovery	: <input checked="" type="checkbox"/>
Low Buffer Threshold	: 60	Max Converged Range	: 10
High Buffer Threshold	: 80	Max Path RTT Time	: 2000
Core Class	: cc7	Min Probe Packet Size	: 1024
IPsec Cipher Key Check	: <input checked="" type="checkbox"/>	Path MTU Aging Time (seconds)	: 600

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Service...

Updated: Wed, 23 Oct 2024 08:24:00 GMT

Copyright © 2024, Versa Networks, Inc.

- To enable or disable the IPsec cipher key check option, click the  Edit icon. The Edit Service Options screen displays.



The screenshot shows the 'Edit Service Options' dialog box with the 'General' tab selected. The dialog contains various configuration fields and checkboxes. The 'IPsec Cipher Key Check' checkbox is highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom right.

Edit Service Options			
General QoS Path MTU Discovery IP Reassembly			
Thread Bulking 16	Maximum Allowed Sessions 1000000	Driver Bulking 16	Poller Count
Number of RX Descriptors 512	Number of TX Descriptors 512	Worker Count 	Inter Thread Packet Rings Size 0
Run Mode Performance	Max Idle Sleep Time(micsec) 10	Min Idle Sleep Time(micsec) 1000	Datapath RX-TX mode Poller
Forwarding Queue 16	CGNAT Scale Factor 8	Max Tenants 32	Least Loaded Worker Thread Mode Service Load
<input type="checkbox"/> Strip Input VLAN	<input type="checkbox"/> Minimal Core Support	<input type="checkbox"/> Nitrox Support	<input type="checkbox"/> VXLAN Entropy
<input checked="" type="checkbox"/> Token Bucket	<input type="checkbox"/> Restart on Change	<input type="checkbox"/> Tag Native VLAN	<input type="checkbox"/> Use Least Loaded Worker Thread
<input checked="" type="checkbox"/> TPM Support	<input checked="" type="checkbox"/> Crypto Accelerator Support	<input checked="" type="checkbox"/> IPsec Cipher Key Check	Host Huge Page Size
Total Huge Page Size 0			
OK Cancel			

- Click the IPsec Cipher Key Check box to change the setting.
- Click OK.

Configure Session Parameters

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Templates > Device Templates in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a template in the main pane. The view changes to Appliance view.
- Select Others > System > Configuration > Configuration in the left menu bar. The main pane displays various configuration-related panes.

Versa Networks

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Commit Template

Appliance SDWAN-Branch1 You are currently in Appliance View Build

Networking Services Objects & Connectors Others

Search

> Organization

> System

> Configuration

Configuration

Core Profile

Speed Test

Domain Name Servers

Security Package Updates

> Time & Date

Storage Configurations

> Appliance User Managemen...

> Elasticity

> Service Nodes

Syslog Server

Alarms

Certificate Alarms Settings

Identification Edit

Name : SDWAN-Branch1

Location : 1 Hacker Way, Menlo Park, CA, USA 94025

Subjugation Edit

Enabled : ☒

Allow CLI : ☐

VNF Manager Delete Edit

IP Address/Prefix : 192.168.75.2/32

Interface : tvi-0/41.0

Fix USB Port Affinity Edit

Enable : ☐

Services Edit

SFTP : ☐

WWW : ☒

Sessions Edit

: ☐ 240

Send ICMP Unreachable : TCP Wait : 20

: ☐ TCP MSS Adjustment : UDP Session : 30

: ☒ Interim Update Disabled : TCP Half Open : 8

: ☐ Log Unknown Hostbound Packets Disabled : TCP Half Closed : 120

: ☒ TCP Secure Reset

: ☐ TCP Send Reset

: ☐

Service Options Edit

CGNAT Scale Factor : 8

Datapath RX-TX mode : poller

Driver Bulking : 16

Forwarding Queue : 16

Inter Thread Packet Rings Size : 0

Traffic class Queue size : -


Nitrox Support : ☐

SDWAN Header Compression : ☐

Poller Count : -

QoS Frame Overhead Auto Adjust : ☐

QoS Frame Overhead Length : ☐

- In the Sessions pane, click the  Edit icon. In the Edit Sessions popup window, enter information for the following fields.

Edit Sessions



Timeout

Default

Hard Session

ICMP Session

TCP Session

TCP Wait

UDP Session

TCP Half Open

TCP Half Closed

Flags

☐ Allow Unsupported Protocol

☐ Check TCP SYN

☐ Reevaluate Reverse Flow

☐ Send ICMP Unreachable

☒ Session Reevaluate

☐ TCP Secure Reset

☐ TCP Send Reset

TCP MSS Adjustment

OK

Cancel

Field	Description
Timeout (Group of Fields)	Define session timeout values. All session timeout values except for Hard Session are the idle time period in seconds. The idle timer starts when the last packet in either direction was last seen.
◦ Default	This field is deprecated and is not used.
◦ Hard Session	Total duration of a session, after which the session times out. Note that this value is not an idle timeout but rather the lifetime of a session.
◦ ICMP Session	Idle timeout for ICMP sessions. <i>Default: 10 seconds</i>
◦ TCP Half Open	Timeout for a TCP sessions after it receives a SYN and before completion of the three-way handshake. <i>Default: 8 seconds</i>
◦ TCP Half Closed	Timeout for a TCP session after it receives the first FIN and before it receives the second FIN or a RST. <i>Default: 120 seconds</i>
◦ TCP Session	Idle timeout for TCP sessions. <i>Default: 240 seconds</i>
◦ TCP Wait	Session idle timeout after a TCP session has received a FIN or RST flag in either direction. <i>Default: 20 seconds</i>
◦ UDP Session	Idle timeout for UDP sessions. <i>Default: 30 seconds</i>
Flags (Group of Fields)	
◦ Allow Unsupported Protocol	Click to accept non-IP protocol packets. The VOS device performs an IP protocol validity check to

	determine the packet's protocol.
<ul style="list-style-type: none"> ◦ Check TCP SYN 	<p>Click to reject the first packet of a TCP session if, when the TCP session is being set up, the SYN flag is not set in the first packet. To accept the first packet, ensure that this option is not clicked.</p> <p>By default, the VOS device firewall rejects the first packet if the packet's SYN flag is not turned on. This security measure is taken is because normal TCP connections start with a three-way handshake, which means that if the first packet that the firewall sees is not the SYN packet, it is likely that the packet is not valid and the firewall discards it. In cases such as asymmetric routing, you might want to disable this feature.</p>
<ul style="list-style-type: none"> ◦ Reevaluate Reverse Flow 	Click to reevaluate the packet policy for first packet of a reverse flow if the forward flow action is set to Drop.
<ul style="list-style-type: none"> ◦ Send ICMP Unreachable 	Click to send ICMP unreachable messages to a source if a route lookup fails.
<ul style="list-style-type: none"> ◦ Session Reevaluate 	Click to reevaluate a session when the configuration or a route changes.
<ul style="list-style-type: none"> ◦ TCP Secure Reset 	Click to follow the secure criteria for accepting TCP reset (RST) packets.
<ul style="list-style-type: none"> ◦ TCP Send Reset 	Click to send a TCP RST packet to the source if the SYN flag in the first packet of a new TCP flow is not set.
TCP MSS Adjustment (Group of Fields)	Configure the largest packet, in bytes, that the VOS device can receive in a single TCP segment. The MSS does not include the TCP header (20 bytes) or the IP header (20 bytes).
<ul style="list-style-type: none"> ◦ Enable 	Click to allow the TCP MSS on an interface to be adjusted.
<ul style="list-style-type: none"> ◦ Interface Types 	<p>Select the interface on which to set TCP MSS adjustment value:</p> <ul style="list-style-type: none"> ◦ All—Set on all interfaces. ◦ Tunnel—Set only for the traffic that goes through

	the tunnel interface.
◦ MSS Value	Enter the TCP MSS value. <i>Range:</i> 512 to 8960 bytes
Interim Update (Group of Fields)	Configure interim update parameters.
◦ Disable	Click to disable interim updates.
◦ Interim Update Interval	Enter the time between updates. <i>Range:</i> 60 to 3600 seconds
Log Unknown Host-Bound Packets	(For Releases 22.1.3 and later.) Configure the logging of unknown packets that are destined for a VOS IP address.
◦ Disable	Click to disable the logging.
◦ Interval	Enter the logging time. <i>Default:</i> 60 seconds

4. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- For Release 21.2.1, the default maximum number of sessions that a VOS device supports is automatically adjusted down or up based on the total amount of system memory.
- Release 22.1.1 adds the IP cipher key check.
- Release 22.1.3 adds the log unknown host-bound packets session option.

Additional Information

[Configure Organization Limits](#)

[Configure Site-to-Site Tunnels](#)

[Versa Solution Scalability](#)