

SonicOS 7.1

SD-WAN

Administration Guide

SONICWALL®

Contents

About SonicOS	4
Working with SonicOS	4
SonicOS Workflow	6
How to Use the SonicOS Administration Guides	7
Guide Conventions	8
About SD-WAN	9
Elements of SD-WAN	10
SD-WAN Groups	10
SLA Probes	10
SLA Class Objects	10
Path Selection Profiles	11
SD-WAN Rules	11
SD-WAN Groups	12
About SD-WAN Groups	12
Configuring SD-WAN Groups	13
Creating an SD-WAN Group	13
Editing an SD-WAN Group	14
Deleting an SD-WAN Group	14
Deleting Multiple SD-WAN Groups	15
SLA Probes	16
About SLA Probes	16
Configuring SLA Probes	17
Adding SD-WAN SLA Probes	18
Editing an SD-WAN SLA Probe	19
Deleting an SD-WAN SLA Probe	19
Deleting Multiple SD-WAN SLA Probes	21
SLA Class Objects	22
About SLA Class Objects	22
Configuring SD-WAN SLA Class Objects	23
Adding an SD-WAN SLA Class Object	24
Editing an SD-WAN SLA Class Object	25
Deleting an SD-WAN SLA Class Object	25
Deleting All Custom SLA Class Objects	25

Path Selection Profiles	26
About Path Selection Profiles	26
Configuring Path Selection Profiles	27
Adding Path Selection Profile	27
Editing a Path Selection Profile	28
Deleting a Path Selection Profile	29
Deleting Multiple Path Selection Profiles	29
SD-WAN Rules	30
About SD-WAN Rules	30
Configuring SD-WAN Rules	31
Adding SD-WAN Rules	32
Editing SD-WAN Rules	34
Deleting SD-WAN Rule	34
Deleting Multiple SD-WAN Rules	34
Monitoring SD-WAN	35
Viewing SD-WAN Rules Connections	36
SonicWall Support	38
About This Document	39

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on how to configure SD-WAN group, SLA Profiles, SLA Class Objects, Path Selection Profiles, and Rules on the SonicWall security appliances.

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

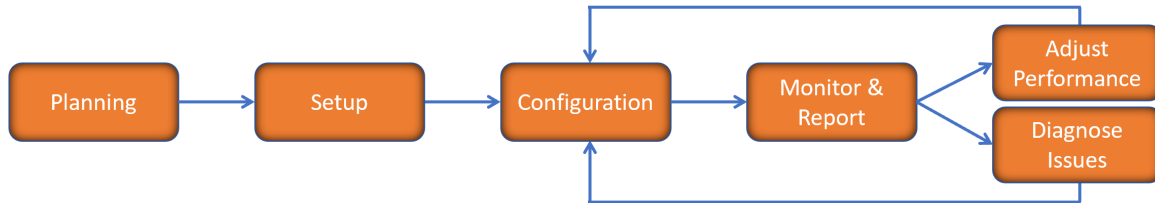
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS 7.1 API Reference Guide](#)

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

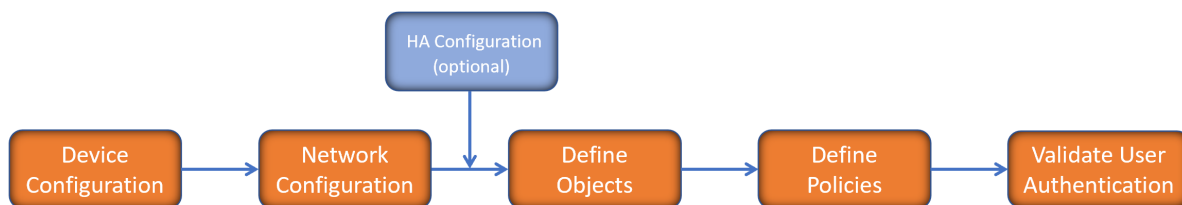


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

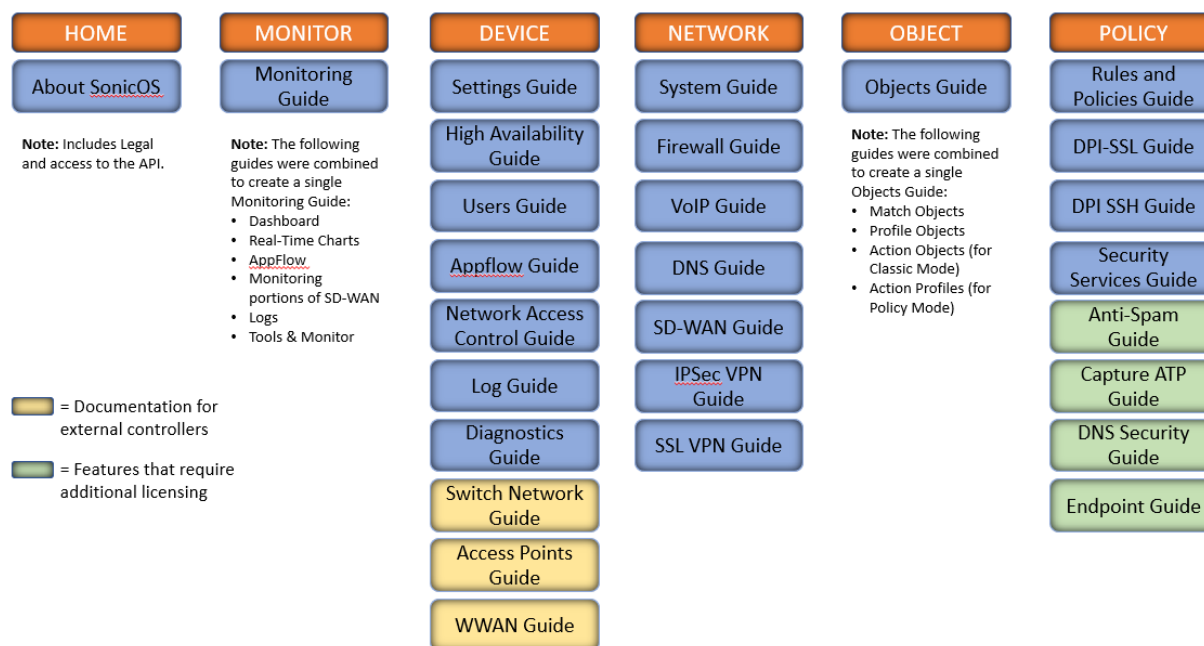


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the *SonicOS 7.1 Monitor Guide* and the *SonicOS 7.1 Objects Guide* which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 .
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

About SD-WAN

SD-WAN (Software-Defined Wide Area Network) provides software-based control over wide area network (WAN) connections. SonicOS SD-WAN offers these features:

- SD-WAN Interface Groups
 - WAN and VPN
 - Scalable from one to N interfaces
- Dynamic path selection based on:
 - Pre-defined Lowest Latency, jitter, or packet loss
 - User-defined thresholds based on any combination of 1 or more of latency, jitter, or packet loss criteria
- Application-aware routing
- Path SLA (Service-Level Agreement) Probes for metrics
- Connection-based traffic distribution
- Automatic connection failover over VPN
- Local or Centralized management via GMS or Network Security Manager.

SD-WAN is best used for specific traffic types and/or applications requiring dynamically chosen optimal destination interfaces depending on how the network paths are behaving. To operate well, each application has a certain requirement from the network path. For example, the network quality for VoIP to operate well requires the optimal latency be 100 ms or less while a latency of 150 ms or higher results in choppy calls. SD-WAN helps in such scenarios by first dynamically measuring the various network SLA metrics, such as latency, jitter and packet loss on multiple network paths. SD-WAN then compares these metrics with the SLA threshold for a particular traffic flow and determines the optimal network that meets the flow's network quality accordingly.

Elements of SD-WAN

Topics:

- [SD-WAN Groups](#)
- [SLA Probes](#)
- [SLA Class Objects](#)
- [Path Selection Profiles](#)
- [SD-WAN Rules](#)

SD-WAN Groups

SD-WAN Groups are logical groups of interfaces that can be used for load-balancing as well as dynamic path selection based on the performance criterion through each interface path. You can create your own custom groups.

Constraints for SD-WAN Groups

- Group need to have at-least one member interface
- Groups cannot have mix of WAN, Numbered Tunnel interface and Unnumbered Tunnel Interface
- Groups cannot share member interfaces with other groups.

Constraints for Member Interfaces

- Member interfaces can only be WAN, Numbered Tunnel Interface or Unnumbered Tunnel Interface
- Member interfaces cannot be Wire mode or L2 bridge interfaces
- Maximum member interfaces per group – 10.

. For more information, see section [SD-WAN Groups](#)

SLA Probes

SD-WAN SLA Probes are used to determine performance metrics such as latency, jitter, packet loss for a Network path. These are similar to Network Monitor Probes. SonicOS supports the ICMP and TCP probe types. A SD-WAN probe can be used by multiple Path Selection profiles. For more information, see section [SLA Probes](#).

SLA Class Objects

SD-WAN SLA Class Objects is used to configure the desired performance characteristics for the application/traffic categories. These objects are used in the Path Selection Profile to automate the selection of paths based on these metrics.

The default Performance Class Objects are:

- Lowest Jitter
- Lowest Latency
- Lowest Packet Loss

Custom class object can be configured with the thresholds that best meet the needs of your application/traffic categories with Performance Class Objects. For more information, see section [SLA Class Objects](#).

Path Selection Profiles

Path Selection Profiles (PSPs) are the settings that help to determine the network path that satisfies a specific network performance criteria, from a pool of available network paths. The dynamic path selection mechanism is implemented using the PSP settings when associated with Policy Based Routes (PBR). When more than one network path meets the criterion (as per the performance class in the PSP), then traffic is load balanced among the network paths. When associated with a policy-based routing policy, a path selection profile helps select the optimal path among the SD-WAN interfaces for the application/service. For more information, see section [Path Selection Profiles](#)

SD-WAN Rules

Dynamic Path selection for specific traffic flows uses Policy Based Routes. A SD-WAN Policy Based Route is used to configure the route policy for the specific source/destination service/App combination, with a corresponding Path Selection Profile that determines the outgoing path dynamically based on the Path Selection Profile. If there is more than one path qualified by the Path Selection Profile, the traffic is automatically load balanced among the qualified paths. If none of the paths are qualified by the path selection profile and the backup interface in the profile is not configured or is down, the route is disabled. For more information, see section [SD-WAN Rules](#).

SD-WAN Groups

Topics:

- [About SD-WAN Groups](#)
- [Configuring SD-WAN Groups](#)

About SD-WAN Groups

SD-WAN supports physical and Virtual WAN (VLAN) interface types as well as VPN Numbered and Un-Numbered Tunnel Interface instances, all choices provided while creating an SD-WAN group.

SD-WAN Groups are logical groups of interfaces that can be used for load-balancing as well as dynamic path selection based on the SLA criterion through each interface path.

The **SD-WAN Groups** page displays the custom pool of interfaces used for optimized and resilient traffic flow.

#	NAME	ZONE	IP ADDRESS	LINK STATUS	PRIORITY
1	tunnel1				
	U0	WAN	0.0.0.0	↓	1
	X1	WAN	10.203.28.159	↑	2

Name	Name of the SD-WAN group.
Zone	The zone of the interface member: <ul style="list-style-type: none"> • WAN • VPN
IP Address	IP address of physical, virtual (VLAN) interfaces or Numbered Tunnel Interfaces. Un-Numbered will be 0.0.0.0.
Link Status	Indicates whether the link is: <ul style="list-style-type: none"> • Link Up (green) • Link Down (red)

Configuring SD-WAN Groups

Topics:

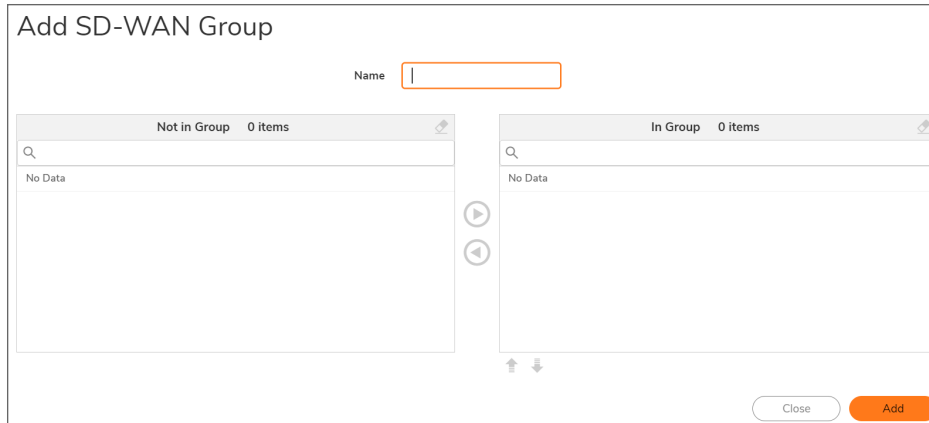
- [Creating an SD-WAN Group](#)
- [Editing an SD-WAN Group](#)
- [Deleting an SD-WAN Group](#)
- [Deleting Multiple SD-WAN Groups](#)

Creating an SD-WAN Group

You can create multiple SD-WAN Groups to meet your requirements.

To add an SD-WAN group:

1. Navigate to **Network | SDWAN > Groups**.
2. Click the **Add** icon.
The **Add SD-WAN Group** dialog displays.



3. Enter a descriptive name in the **Name** field.
4. Select one or more interfaces from the **Not in Group** list. Member interfaces available to select included Physical WAN, virtual (VLAN) WAN, numbered tunnel (VPN) interfaces and VPN policies for un-numbered tunnel interfaces.
 - ① | **IMPORTANT:** An interface cannot be a member of more than one SD-WAN group.
 - ① | **IMPORTANT:** The maximum number of interfaces that can be added in an SD-WAN group is 10.
5. Click the **Right Arrow** to move the selected interfaces to the **In Group** column.

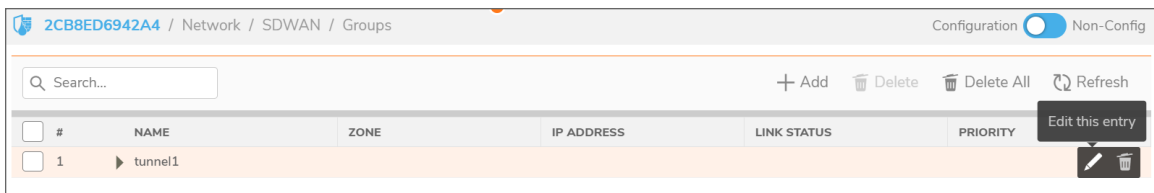
6. To change the priority of the selected group members:
 - a. Select the interface.
 - b. Click the **Up Arrow** or **Down Arrow**.

① **NOTE:** If user is using VPN tunnel interface for SD-WAN configuration, then in both the firewall the priority for the tunnel interface should be maintained same.
7. Repeat Step 6 for each interface to prioritize.
 1. Click **Add**.
If the group is created, a confirmation message is displayed.
 2. Click **Close**.

Editing an SD-WAN Group

To edit an SonicOS group:

1. Navigate to **Network | SDWAN > Groups**.
2. Hover over an SD-WAN group, click the **Edit** icon of the group to edit.



The **Edit this entry** is displayed.

3. Make required changes as described in [Creating an SD-WAN Group](#).
4. Click **Save**.

Deleting an SD-WAN Group

To delete an SD-WAN group:

1. Navigate to **Network | SDWAN > Groups**.
2. Hover over an SD-WAN group, click the **Delete** icon.
3. Click **Confirm**.
The message confirming the deletion of SD-WAN group is displayed.

Deleting Multiple SD-WAN Groups

To delete SD-WAN groups:

1. Navigate to **Network | SDWAN > Groups**.
2. Hover over an SD-WAN group, click the **Delete All** icon.
3. Click **Confirm**.
The message confirming the deletion of all SD-WAN group is displayed.

SLA Probes

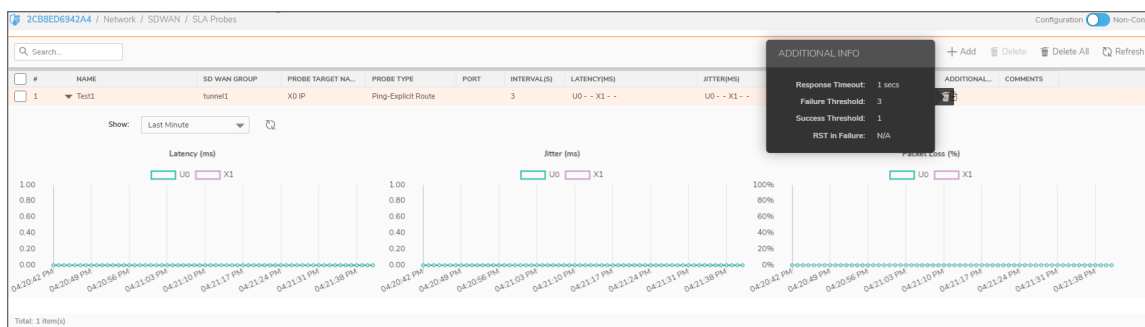
Topics:

- [About SLA Probes](#)
- [Configuring SLA Probes](#)

About SLA Probes

Network path performance metrics are determined using SD-WAN SLA probes, which are similar to Network Monitor Probes. SonicOS supports ICMP and TCP probe types. An SD-WAN SLA probe can be used by multiple Path Selection Profiles, for further information, see [About Path Selection Profiles](#).

The **Network | SD-WAN > SLA Probes** page shows the dynamic performance data (latency/jitter/packet loss) and probe status for each path (interface) in the SD-WAN group, in both tabular and graphic displays. The display can show data for the last minute (default), last day, last week, or last month.



#	Number of the probe. The Collapse/Expand icon toggles the display of the graphs.
NAME	Name of the SD-WAN SLA probe.
SD-WAN GROUP	Name of the SD-WAN group associated with the SD-WAN SLA probe.
PROBE TARGET NAME	Target address object of the SD-WAN SLA probe.
NAME	① NOTE: This field is empty for VPN based interfaces.

PROBE TYPE	Type of SLA probe: <ul style="list-style-type: none"> • Ping-Explicit Route • TCP-Explicit Route <p>① NOTE: When "TCP-Explicit Route" is selected, both Port field and "RST Response Counts As Miss" become available.</p>
PORT	Port for the SD-WAN SLA probe. The minimum/maximum values are 1 to 65535. <p>① NOTE: Ports are displayed only for TCP - Explicit Route probe types. A hyphen (-) displays for Ping - Explicit Route probe types.</p>
INTERVAL (S)	Time between SD-WAN SLA probes, in seconds.
LATENCY (MS)	Round trip delay for the probes sent through a particular path/interface to reach the probe target and acknowledge back, in milliseconds. This is also displayed as a graph below the probe's entry in the SLA Probe table.
JITTER (MS)	Variation in the latency measurements for the probes through a particular path/interface, in milliseconds. This is also displayed as a graph below the probe's entry in the SLA Probe table.
PACKET LOSS (%)	Percentage of probes that are missed of the probes sent through a particular path/interface. This is also displayed as a graph below the probe's entry in the SLA Probe table.
ADDITIONAL INFO	When you hover over the icon, you can view the data for the following: Response timeout, Success Threshold, Failure Threshold, & RST in Failure.
COMMENTS	Displays the comment entered when the SLA probe was configured.

Configuring SLA Probes

Topics:

- [Adding SD-WAN SLA Probes](#)
- [Editing an SD-WAN SLA Probe](#)
- [Deleting an SD-WAN SLA Probe](#)
- [Deleting Multiple SD-WAN SLA Probes](#)

Adding SD-WAN SLA Probes

① **IMPORTANT:** A SLA Probe is created automatically for an SD-WAN Group containing a VPN numbered tunnel interface/unnumbered tunnel interface. You do not need to create an additional SLA probe.

To add a SLA probe for non-VPN SD-WAN Groups:

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Click the **Add** icon.

The **Add SD-WAN SLA Probe** dialog is displayed.

Add SD-WAN SLA Probe

Name

SD-WAN Group

Probe Target

Probe Type

Port

Probe hosts every seconds

Reply time out seconds

Probe state is set to DOWN after missed intervals

Probe state is set to UP after successful intervals

RST Response Counts As Miss

Comment

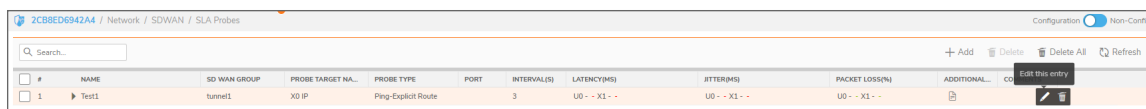
3. Enter a meaningful name in the **Name** field.
4. Select an SD-WAN group from **SD-WAN Group** drop-down menu.
5. Select an address object from **Probe Target**.
6. From **Probe Type**, select:
 - **Ping (ICMP) - Explicit Route** (default); go to Step 8.
 - **TCP - Explicit Route**; the **Port** field becomes available.

7. Enter the port number of the explicit route in the **Port** field.
8. Enter the interval between probes in the `Probe hosts every` field. The minimum is 1 second, the maximum is 3600 seconds, and the default is 3 seconds.
 - ① | **TIP:** The probe interval must be greater than the reply timeout.
9. Enter the maximum delay for a response in the `Reply time out ... seconds` field. The minimum is 1 second, the maximum is 60 seconds, and the default is 1 second.
10. Enter the maximum number of missed intervals before the SLA probe is set to the DOWN state in the `Probe state is set to DOWN after ... missed intervals` field. The minimum number is 1, the maximum is 100, and the default is 3.
11. Enter the maximum number of successful intervals before the SLA probe is set to the UP state in the `Probe state is set to UP after ... successful intervals` field. The minimum number is 1, the maximum is 100, and the default is 1.
12. If you selected TCP - Explicit Route for Probe Type, the RST Response Counts As Miss option becomes available. Select the option to count RST responses as missed intervals. This option is not selected by default.
13. Optionally, enter a comment in the `Comment` field.
14. Click **Add**.
A confirmation message is displayed.

Editing an SD-WAN SLA Probe

To edit an SD-WAN SLA probe:

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Hover over the SD-WAN SLA probe and click the **Edit** icon that appears.



#	NAME	SD WAN GROUP	PROBE TARGET NA...	PROBE TYPE	PORT	INTERVAL(S)	LATENCY(MS)	JITTER(MS)	PACKET LOSS(%)	ADDITIONAL...	CO...
1	Test1	tunnel1	XD IP	Ping-Explicit Route		3	U0 - - X1 - -	U0 - - X1 - -	U0 - - X1 - -		

3. The **Edit SD-WAN SLA Probe** dialog displays.
4. Make changes as described in [Adding SD-WAN SLA Probes](#).
5. Click **Save**.

Deleting an SD-WAN SLA Probe

To delete an SD-WAN SLA probe:

1. Navigate to **Network | SD-WAN > SLA Probes**.
2. Hover over the SD-WAN SLA probe and click the **Delete** icon that appears.

2C8B2E042A4 / Network / SD-WAN / SLA Probes Configuration Non-Config

Search

#	NAME	SD-WAN GROUP	PROBE TARGET NA...	PROBE TYPE	PORT	INTERVAL(S)	LATENCY(S)	JITTER(S)	PACKET LOSS(S)	ADDITIONAL...	CO
1	test1	testnet	80 IP	Pre-Eq/IC Route		3	10 - X1 -	10 - X1 -	10 - X1 -		

+ Add Delete Delete All Refresh

A confirmation message is displayed.

3. Click **Confirm**.

Deleting Multiple SD-WAN SLA Probes

To delete multiple SD-WAN SLA probes:

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Click **Delete All** icon at the top of the SD-WAN SLA Probe table.



A confirmation message is displayed.

3. Click **Confirm**.

SLA Class Objects

Topics:

- [About SLA Class Objects](#)
- [Adding an SD-WAN SLA Class Object](#)

About SLA Class Objects

A SLA Class specifies the SLA criterion for selecting the optimal path. It could be the:

- Best latency/jitter/packet loss among the existing paths.
- SLA Class Object that defines the metric thresholds for any combination of latency, jitter and packet loss.

You use SD-WAN SLA Class Objects to configure the desired SLA characteristics for the application/traffic categories. These objects are used in the Path Selection Profile to automate the selection of paths based on these metrics.

These are the default SLA Class Objects:

- **Lowest Jitter**
- **Lowest Latency**
- **Lowest Packet Loss**

ⓘ | NOTE: These default SLA Class Objects cannot be edited or deleted.

You can configure custom SLA thresholds that best meet the needs of your application/traffic categories with custom SLA Class Objects. You can include or exclude the Latency, Jitter, or Packet Loss attributes in your custom object, although you cannot exclude all three attributes in the same object. When excluded, the value of that attribute is not used as a criterion or threshold when determining whether a particular path is qualified or not. For example, if you want to evaluate a particular path only on the Latency attribute but you don't care about the other attributes, you can include Latency and exclude Jitter and Packet Loss in your custom object.

#	NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	COMMENT
1	Lowest Latency	LOWEST	-	-	Auto-added Perf Class Obj
2	Lowest Jitter	-	LOWEST	-	Auto-added Perf Class Obj
3	Lowest Packet Loss	-	-	LOWEST	Auto-added Perf Class Obj

NAME	Name of the SLA Class Object
LATENCY (MS)	Threshold time for the round trip delay for the probes sent through a particular path/interface to reach the probe target and acknowledge back, in milliseconds. For the Lowest Latency SLA Class Object, the time is always LOWEST ; for the other default SLA Class Objects, a hyphen (–) displays.
JITTER (MS)	Threshold variation in the latency measurements for the probes through a particular path/interface, in milliseconds. For the Lowest Jitter SLA Class Object, the time is always LOWEST ; for the other default SLA Class Objects, a hyphen (–) displays.
LOSS (%)	Threshold percentage of probes that are missed of the probes sent through a particular path/interface. For the Lowest Packet Loss SLA Class Object, the percentage is always LOWEST ; for the other default SLA Class Objects, a hyphen (–) displays.
COMMENT	Displays the comment entered when the SLA Class Object was configured.

Configuring SD-WAN SLA Class Objects

Topics:

- [Adding an SD-WAN SLA Class Object](#)
- [Editing an SD-WAN SLA Class Object](#)
- [Deleting an SD-WAN SLA Class Object](#)
- [Deleting All Custom SLA Class Objects](#)

Adding an SD-WAN SLA Class Object

To add a SLA Class Object:

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Click the **Add** icon.
The **Add SLA Class** Object dialog appears.

The screenshot shows a dialog box titled "Add SLA Class Object". It contains the following fields and controls:

- Name**: A text input field with a vertical cursor.
- Include Latency**: A toggle switch that is currently turned on.
- Latency (ms)**: A text input field containing the value "0".
- Include Jitter**: A toggle switch that is currently turned on.
- Jitter (ms)**: A text input field containing the value "0".
- Include Loss**: A toggle switch that is currently turned on.
- Loss (%)**: A text input field containing the value "0".
- Comment**: A text input field.
- Buttons**: "Cancel" and "OK" buttons at the bottom right.

3. Enter a meaningful name in the `Name` field.
4. Enable **Include Latency** to include the SLA class latency attribute for this object to exclude the latency attribute. This option is selected by default.
5. If **Include Latency** is enabled, enter the acceptable latency, in milliseconds, in the `Latency (ms)` field. The minimum is 0 milliseconds, the maximum is 1000 milliseconds, and the default is 0 milliseconds.
6. Enable **Include Jitter** to include the SLA class jitter attribute for this object to exclude the jitter attribute. This option is selected by default.
7. If **Include Jitter** is enabled, enter the acceptable jitter, in milliseconds, in the `Jitter (ms)` field. The minimum is 0 milliseconds, the maximum is 1000 milliseconds, and the default is 0 milliseconds.
8. Enable **Include Loss** to include the SLA class packet loss attribute for this object to exclude the packet loss attribute. This option is selected by default.
9. If **Include Loss** is enabled, enter the acceptable percentage of packet loss in the `Loss (%)` field. The minimum is 0, the maximum is 100, and the default is 0.

NOTE:

1. You cannot exclude all three attributes (Latency, Jitter, Packet Loss) in the same object.
2. You can view the SLA Probe section to see what you are getting on each link to determine practical thresholds.

10. Optionally, enter a comment in the `Comment` field.
11. Click **OK**.

Editing an SD-WAN SLA Class Object

To edit an SD-WAN SLA class object:

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Hover over a SLA class object, click the **Edit** icon. The **Edit SLA Class Object** dialog appears, make required changes as described in [Adding an SD-WAN SLA Class Object](#).
3. Click **OK**.

Deleting an SD-WAN SLA Class Object

To delete an SD-WAN SLA Class Object:

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Hover over an object and click the **Delete** icon.

#	NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	COMMENT
1	Lowest Latency	LOWEST	-	-	Auto-added Perf Class Obj
2	Lowest Jitter	-	LOWEST	-	Auto-added Perf Class Obj
3	Lowest Packet Loss	-	-	LOWEST	Auto-added Perf Class Obj
4	FFR	3,000	3,000	3,000	

3. Click **Confirm** in the confirmation prompt that is displayed.

Deleting All Custom SLA Class Objects

To delete multiple SD-WAN SLA Class Objects:

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. To delete all the Custom SLA Class Objects, click **Delete All** icon at the top of the SLA Class Object table. A confirmation message is displayed.
3. Click **Confirm**.

Path Selection Profiles

Topics:

- [About Path Selection Profiles](#)
- [Configuring Path Selection Profiles](#)

About Path Selection Profiles

Path Selection Profiles (PSPs) determine the network paths or interfaces that satisfy a specific network SLA criteria from a pool (SD-WAN Group) of available network paths/interfaces.

The dynamic path selection mechanism is implemented using the PSP settings when associated with Policy-based Routes (PBR). When more than one network path meets the criterion (as per the SLA class in the PSP), then traffic is load balanced among the qualified network paths/interfaces. When associated with a policy-based routing policy or SD-WAN Rule, a Path Selection Profile helps select the optimal path among the SD-WAN interfaces for the application/service.

#	NAME	SD WAN GROUP	INTERFACE STATUS	SLA PROBE	SLA CLASS OBJECT	BACKUP INTERFACE	PROBE DEFAULT UP
1	test	lan1	U0 - Qualified X1 - Qualified	test	TEST	None	✓

Name	Name of the Path Selection Profile.
SD-WAN Group	SD-WAN interface group to which the profile applies.
Interface Status	Status of the members of the SD-WAN interface group: <ul style="list-style-type: none"> • Qualified (green) • Not Qualified (red)
SLA Probe	SLA Probe used by the Path Selection Profile.

SLA Class Object	<p>SLA Class Object used by the Path Selection Profile:</p> <ul style="list-style-type: none"> • Lowest Latency • Lowest Jitter • Lowest Packet Loss • Custom SLA Class Object
Backup Interface	<p>Indicates the interface chosen when none of the SD-WAN group interfaces meet the performance criteria. If a backup interface was not chosen, None displays.</p>
Probe Default UP	<p>Indicates whether the default state of the SLA probe is:</p> <ul style="list-style-type: none"> • UP (Checkmark icon) • DOWN (Crossmark icon)

Configuring Path Selection Profiles

Topics:

- [Adding Path Selection Profile](#)
- [Editing a Path Selection Profile](#)
- [Deleting a Path Selection Profile](#)
- [Deleting Multiple Path Selection Profiles](#)

Adding Path Selection Profile

To add a Path Selection Profile:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Click the **Add** icon above the table.
The **Add SD-WAN Path Selection Profile** dialog is displayed.

Add SD-WAN Path Selection Profile

Name

SD-WAN Group

Performance Probe

Performance Class

Backup Interface

Performance Probe default state is UP

Reset connections if path does not meet the performance criteria

3. Add a meaningful name in the `Name` field.
4. From **SD-WAN Group**, select the SD-WAN interface group to which the profile applies.
You have an option to create a new SD-WAN group from this dialog and then select the newly created group.
5. From **SLA Probe**, select the probe to use in the profile.
A probe, if added for the SD wan group you selected, is displayed by default. Otherwise, select the appropriate probe.
6. From **SLA Class**, select the SLA Class Object for the dynamic selection of the optimal network path:
 - **Lowest Latency**
 - **Lowest Jitter**
 - **Lowest Packet Loss**
 - Custom SLA Class ObjectYou have an option to create a New SLA Class Object from the drop-down menu.
7. From Backup Interface, select the most optimum interface to use when all the SD-WAN Group interfaces fail to meet the SLA criteria specified in **SLA Class**:
 - **None** (default)
 - Individual interface
 - VPN Tunnel Interface (if any)

NOTE: If user selecting backup interface as VPN Tunnel interface, then in both the Firewall and Tunnel interface should be same in Backup Interface.
8. To specify whether the default state of the SLA probe should be treated as DOWN, disable **SLA Probe default state is UP**. This option is enabled by default and is treated as UP.
9. For path selection profiles with Non-VPN SD-WAN groups, if existing connections on the path should be reset when the path does not meet the performance criteria any more, select **Reset conditions if path does not meet the performance criteria**. This option is disabled by default.
10. Click **Save**.
A confirmation message is displayed.

Editing a Path Selection Profile

To edit a Path Selection Profile:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Hover over a path selection profile, click the **Edit** icon. The **Edit SD-WAN Path Selection Profile** dialog is displayed.
3. Make changes as described in [Adding Path Selection Profile](#).
4. Click **Save**.

Deleting a Path Selection Profile

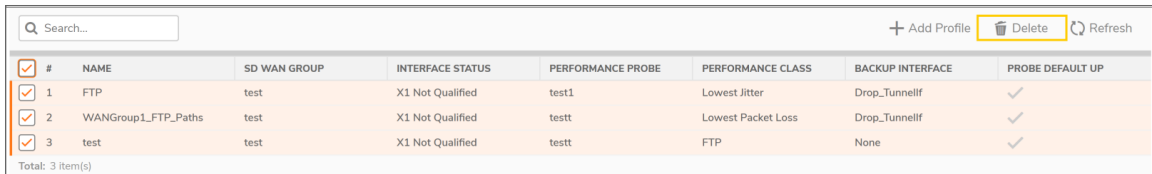
To delete an SD-WAN Path Selection Profile:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Hover over a path selection profile, click the **Delete** icon.
3. Click **OK** to confirm deletion.

Deleting Multiple Path Selection Profiles

To delete multiple Path Selection Profiles:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Select the profiles that you want to delete or click the **Delete All** icon above the Path Selection Profiles table to delete all the profiles.



The screenshot shows a table with the following columns: #, NAME, SD WAN GROUP, INTERFACE STATUS, PERFORMANCE PROBE, PERFORMANCE CLASS, BACKUP INTERFACE, and PROBE DEFAULT UP. Three rows are selected, and the 'Delete' button in the top right is highlighted with a yellow box.

#	NAME	SD WAN GROUP	INTERFACE STATUS	PERFORMANCE PROBE	PERFORMANCE CLASS	BACKUP INTERFACE	PROBE DEFAULT UP	
<input checked="" type="checkbox"/>	1	FTP	test	X1 Not Qualified	test1	Lowest Jitter	Drop_Tunnelf	✓
<input checked="" type="checkbox"/>	2	WANGroup1_FTP_Paths	test	X1 Not Qualified	testt	Lowest Packet Loss	Drop_Tunnelf	✓
<input checked="" type="checkbox"/>	3	test	test	X1 Not Qualified	testt	FTP	None	✓

Total: 3 item(s)

3. Click **OK** to confirm deletion.

SD-WAN Rules

Topics:

- [About SD-WAN Rules](#)
- [Configuring SD-WAN Rules](#)

About SD-WAN Rules

SD-WAN Rules bring Path Selection Profiles and routing criteria together to provide dynamic path selection. SD-WAN Rules combine a Path Selection Profile with either a Source and/or Destination and/or Service Object/Group or a specific Match Object of type "Application List" or "Application Category List" which determines the outgoing path dynamically based on the Path Selection Profile's parameters. If there is more than one path qualified by the Path Selection Profile, the traffic is automatically load balanced among the qualified paths. If none of the paths are qualified by the Path Selection Profile and the backup interface in the profile is not configured or is down, the rule is disabled.

TIP: SD-WAN Rules can also be configured or viewed from the **Policy | Rules and Policies > Routing Rules** page. The **Network | SDWAN > Rules** page, however, only shows the SD-WAN Rules and only allows configuration of SD-WAN-type rules.

#	IP VER.	NAME	SOURCE	DESTINATION	SERVICE	APP	TOS / MASK	PATH PROFILE	INTERFACE	METRIC	PRIORITY	COMMENT
1	IPv6	test	WAN Subnets	Firewalled Subnets	N/A	-appname= AlienBl Jumpshare+00unblo	Any	test	tun1	25	1	

NAME	Name of the SD-WAN Rules.
IP VERSION	The IP version is shown by an icon showing whether the rule is for IPv4 and/or IPv6.
SOURCE	Source address object for the SD-WAN Rule.
DESTINATION	Destination address object for the SD-WAN Rule.
SERVICE	Service object for the for the SD-WAN Rule. If App was selected instead of Service for the type of rule, N/A appears.

APP	Application match object for the for the SD-WAN Rule. If Service was selected instead of App for the type of rule, N/A appears ① NOTE: "Application List" or "Application Category List" Match Objects used here are created at Object Match Objects > Match Objects .
TOS/Mask	Hexadecimal TOS and TOS Mask. If these options were not configured, you will see this field as blank.
PATH PROFILE	Path Selection Profile for the SD-WAN Rule.
INTERFACE	SD-WAN interface group associated with the SD-WAN Rule.
METRIC	Metric used for the SD-WAN Rule.
PRIORITY	Priority of the rule in Routing Rules route table.
COMMENT	When you hover over the comment icon, the comment entered when the SD-WAN Rule was configured is displayed.

Configuring SD-WAN Rules

Topics:

- [Adding SD-WAN Rules](#)
- [Editing SD-WAN Rules](#)
- [Deleting SD-WAN Rule](#)
- [Deleting Multiple SD-WAN Rules](#)

Adding SD-WAN Rules

To add an SD-WAN rule:

1. Navigate to **Network | SDWAN > Rules**.
2. Click the **Add SDWAN Rule** icon. The **Add SDWAN Rule** dialog is displayed.

The screenshot shows the 'Add SDWAN Rule' dialog box. It has two tabs: 'General' and 'Advanced'. The 'General' tab is active. Under the heading 'RULE SETTINGS', there are several fields and options:

- Name:** A text input field.
- Source:** A dropdown menu with 'Any' selected.
- Destination:** A dropdown menu with 'Any' selected.
- Service:** Two radio buttons, 'Service' (selected) and 'App'.
- Service Object:** A dropdown menu with 'Any' selected.
- Path Profile:** A dropdown menu with 'Select a Path Selectio...' selected.
- Interface:** A dropdown menu with 'Select an Interface' selected.
- Metric:** A text input field.
- Comment:** A text input field.
- Disable rule when the interface is disconnected:** A toggle switch that is turned on.
- Permit Acceleration:** A toggle switch that is turned off.

At the bottom right of the dialog are two buttons: 'Cancel' and 'Add'.

① | **NOTE:** The Interface and Disable rule when the interface is disconnected settings options are dimmed and cannot be edited. The Interface option is populated with the SD-WAN group name associated with the Path Selection Profile (PSP) you select.

3. Enter a meaningful name in the **Name** field.
4. From **Source**, select the source address object for the static route or select **Create new Address object** to dynamically create a new address object. The default is **Any**.
5. From **Destination**, select the destination address object or select **Create new Address object** to dynamically create a new address object. The default is **Any**.
6. Choose the type of rule:
 - **Service** (default)
 - **App**
 - ① | **IMPORTANT:** Application Control Licensing is required for application-based rule.
7. If you selected **Service**, select a **Service Object** from the drop-down. For a generic static rule that allows all traffic types, simply select **Any** (the default).
8. If you selected **App**, select an App Match Object from **App Object** drop-down.
 - ① | **NOTE:** "Application List" or "Application Category List" Match Objects used here are created at **Object | Match Objects > Match Objects**.

Add SDWAN Rule

General

Advanced

RULE SETTINGS

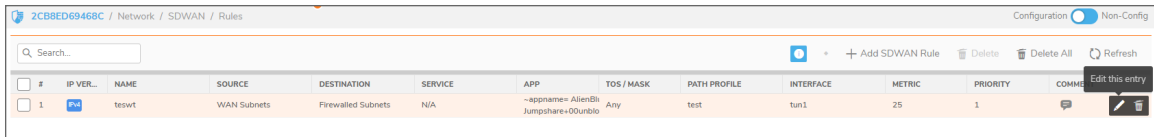
Name	<input type="text"/>	App Object	<input type="text" value="Select App Object"/> <small>Select App Object</small>
Source	<input type="text" value="Any"/>	Path Profile	<input type="text" value="Select a Path Selectio..."/>
Destination	<input type="text" value="Any"/>	Interface	<input type="text" value="Select an Interface"/>
Service	<input type="radio"/>	Metric	<input type="text"/>
App	<input checked="" type="radio"/>	Comment	<input type="text"/>
		Disable rule when the interface is disconnected	<input checked="" type="checkbox"/>
		Permit Acceleration	<input type="checkbox"/>

9. From **Path Profile**, select a Path Selection Profile.
10. Enter the `Metric` (weighted cost) for the route. The minimum is 1, and the maximum is 254.
 ⓘ | **TIP:** Lower metrics are considered better and take precedence over higher metrics (costs).
11. Optionally, enter a `Comment` for the route policy. This field allows you to enter a descriptive comment for the new static route policy.
12. To permit acceleration on the route policy, enable **Permit Acceleration**.
13. Click **Advanced**.
14. Optionally enter a TOS value in the `TOS (Hex)` field. The maximum value is FF. If the TOS and TOS Mask fields are not configured, a value of 0 is used.
15. Enter the same value in the `TOS Mask (Hex)` field.
16. To manually specify an administration distance:
 - a. Deselect **Auto**. This option is selected by default.
 The `Admin Distance` field becomes available.
 - b. Enter the administration distance in the `Admin Distance` field.
17. Click **Add**.

Editing SD-WAN Rules

To edit a SDWAN rule:

1. Navigate to **Network | SDWAN > Rules**.
2. Hover over a rule and click the **Edit** icon.



3. The **Update SDWAN Rule** dialog is displayed.
4. Make changes as described in [Adding SD-WAN Rules](#).
5. Click **Update**.

Deleting SD-WAN Rule

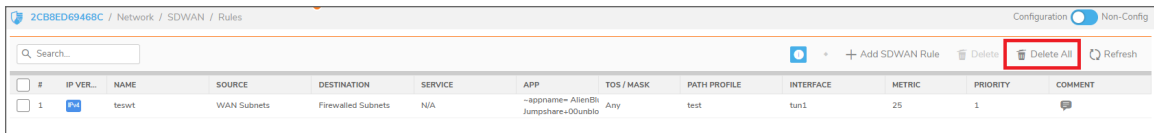
To delete a rule:

1. Navigate to **Network | SDWAN > Rules**.
2. Hover over a rule and click the **Delete** icon.
3. Click **Confirm**.

Deleting Multiple SD-WAN Rules

To delete multiple SD-WAN Rules:

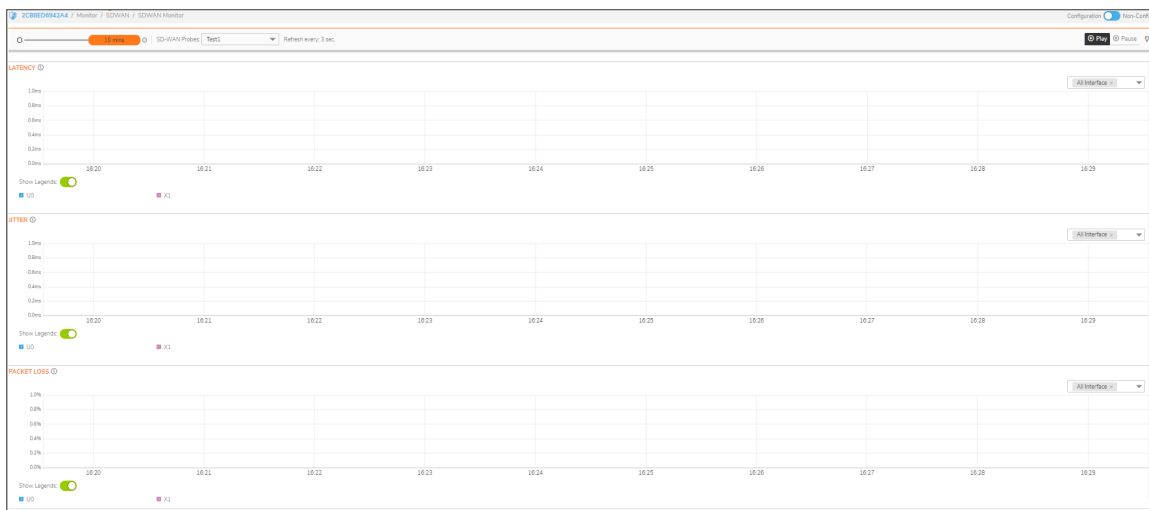
1. Navigate to **Network | SDWAN > Rules**.
2. Select the Path Selection Profiles to delete or click **Delete All** icon above the **SD-WAN Rules** table.



3. Click **Confirm**.

Monitoring SD-WAN

NOTE: A chart may be empty or blank if there are no recent data entries received within the viewing range.



To monitor SD-WAN SLA:

1. Navigate to **Monitor | SD-WAN > SDWAN Monitor**.
2. From **SD-WAN Probes** drop-down box, select the SLA probe you would like to use to monitor.
3. Indicate the Refresh rate, in seconds, in the `Refresh Every` field.
4. Select a View Range:
 - **60 seconds** (default)
 - **2 minutes**
 - **5 minutes**
 - **10 minutes**
5. Choose an interface to track or select **All Interfaces** from the drop-down menu on the right side.

Viewing SD-WAN Rules Connections

You can view the connections that have been associated with SD-WAN Rules on the **Monitor | SDWAN > SD-WAN Connections** page.

- To view the activities associated with IPv4 SD-WAN Rules, click **IPv4** tab.
- To view the activities associated with IPv6 SD-WAN Rules, click **IPv6** tab.

SD-WAN CONNECTION DETAILS

SRC MAC	MAC address of the appliance that is the source of the connection.
SRC VENDOR	Name of the vendor of the appliance that is the source of the connection.
SRC IP	IP address of the appliance that is the source of the connection.
SRC PORT	Port on the appliance that is the source of the connection.
DST MAC	MAC address of the appliance that is the destination of the connection.
DST VENDOR	Name of the vendor of the appliance that is the destination of the connection.
DST IP	IP address of the appliance that is the destination of the connection.
DST PORT	Port on the appliance that is the destination of the connection.
PROTOCOL	Protocol used for the connection.
SRC IFACE	Interface on the appliance that is the source of the connection.
DST IFACE	Interface on the appliance that is the destination of the connection.
SRC ROUTE	Source route of the connection.
DST ROUTE	Destination route of the connection.
FLOW TYPE	Type of data flow control, such as FTP Control.
IPS CATEGORY	Internet Provider Security (IPS) category. If this information is not available or relevant, the column displays N/A.
ABR APP ID	App-Based Routing Application ID.
ABR CATEGORY ID	App-Based Routing Category ID.
EXPIRY (SEC)	Number of seconds until the connection expires.
TX BYTES	Number of bytes transmitted on the connection.
RX BYTES	Number of bytes received on the connection.
TX PKTS	Number of packets transmitted on the connection.

Rx PKTS	Number of packets received on the connection.
Flush	Displays the Flush icon. Clicking the icon flushes the connection.
Total	Total number of entries on the page. This is displayed at the bottom of the page.

You can perform the following actions on the SD-WAN Connections page:

- To search a log, enter a keyword related to an activity in the `Search` bar
- To filter the logs, click **Filter** icon, select the appropriate filter options, and then click **APPLY FILTERS**.
- To clear the filters applied, click **Clear Filter** icon
- To export the logs in CSV or TEXT files, click **Export** icon and select the required format
- To refresh the page, click **Refresh** icon

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

SonicOS SD-WAN Administration Guide

Updated - December 2023

Software Version - 7.1

232-005874-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035