
Configure SD-WAN Policy

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

Normally, packets are routed based on entries in the routing table. To change how packets are routed, you configure SD-WAN policy. You can configure SD-WAN policy for Layer 2 traffic (for Releases 21.2.1 and later) and for Layer 3 traffic (for Releases 20.2 and later).

A policy consists of the following components:

- Policy name, which identifies the policy.
- Policy rules, which define the conditions for matching packets. A policy can have one or more rules, and the rules are evaluated in order until a match occurs. A rule can match traffic based on any combination of Layer 3 criteria (such as IP addresses and header fields, zones, and DSCP values), Layer 4 criteria (such as Layer 4 protocol and ports), and Layer 7 criteria. A rule can match individual applications and groups of applications. For Layer 2 SD-WAN policy, rules can also match Layer 2 criteria, such as MAC address and VLAN ID. For groups of application, a rule can match based on tags or attributes associated with the application (for example, FTP, SFTP and TFTP are tagged as file transfer applications). In a rule, you can define time schedules to taking the policy action.
- Enforcement criteria, which define the action to take on packets that match the rules and whether to log and monitor matching packets.

Each policy is specific to an organization (that is, a tenant). This means that each tenant on a multitenant branch device can control their path selection behavior independently.

To allow an SD-WAN policy to correctly process all traffic in an application flow, it uses application detection, which is always running on the VOS device, to inspect the first packet in a flow and to identify the Layer 7 application sending the flow.


To configure a policy, you do the following:

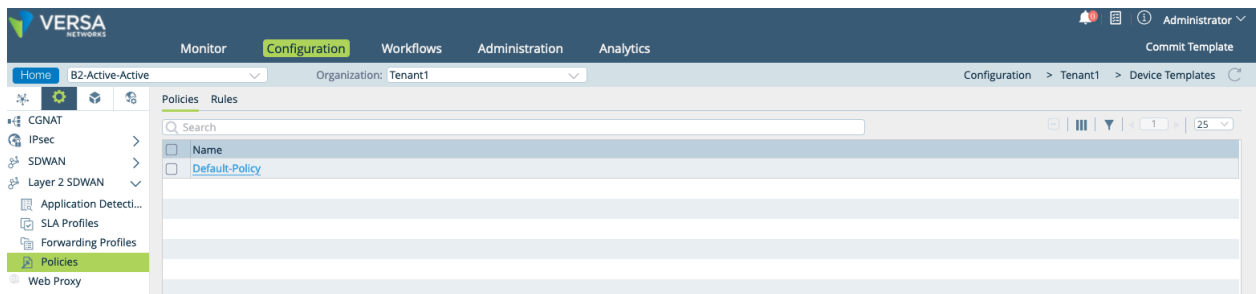
- Define a policy name
- Configure policy rules
- Configure application detection parameters


Configure Policy Names

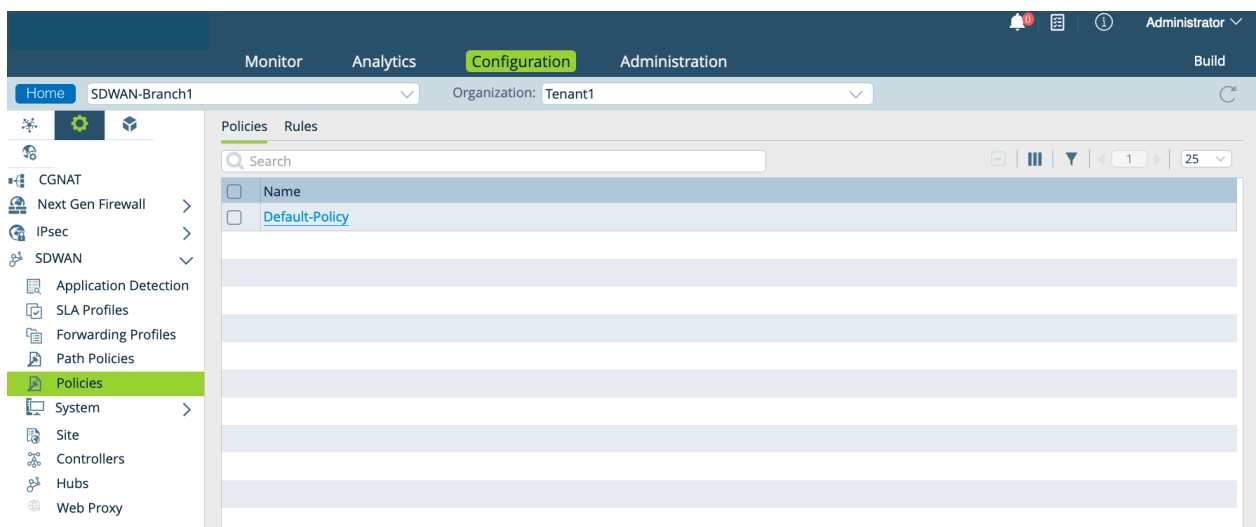
To configure a policy, you first name the policy. Currently, each template can have only one access policy, and this policy is called Default-Policy. If desired, you can add a description for the policy, but you cannot rename it.

To add a description to a policy name:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization from the left menu bar.
 - d. Select a post-staging template in the main pane. The view changes to Appliance view.
 - e. Or, to add a policy name description for a device's policy, select Devices > Devices in Step 1b and then select a device in the main pane.
2. Select the Configuration tab in the top menu bar.
3. For a Layer 2 SD-WAN policy:
 - a. Select Services  > Layer 2 SD-WAN > Policies in the left menu bar.
 - b. Select the Policies tab in the horizontal menu bar. The main pane displays a list of configured policies.



4. For a Layer 3 SD-WAN policy:
 - a. Select Services  > SD-WAN > Policies in the left menu bar.
 - b. Select the Policies tab in the horizontal menu bar. The main pane displays a list of configured policies.



5. Click the name of the policy. In the Edit Policies popup window, enter a description for the policy.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:09:58 GMT

Copyright © 2024, Versa Networks, Inc.

6. Click OK.

Configure Policy Rules for Layer 2 SD-WAN Policy

For Releases 21.2.1 and later.


In policy rules, you configure the conditions for matching packets of interest, and you also configure the forwarding and logging actions to take on the packets that match the conditions. To configure policy rules, you select an organization (that is, a tenant), and then you select one of the tenant's post-staging templates. Then you perform the following steps, which are described in the procedure below:

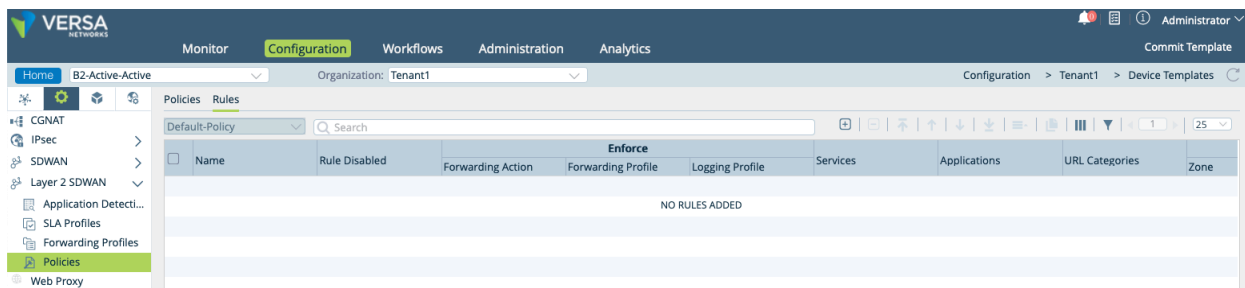
- Add a new rule (Steps 1 through 5).
- Configure a rule name (Step 6).
- Configure match conditions:
 - Configure source address, source MAC address, source zone, and source site match criteria (Steps 7 through 14).
 - Configure destination address, destination MAC address, destination zone, and destination site match criteria (Steps 15 through 20).
 - Configure match criteria based on the contents of the IP packet header and VLAN ID, and set a time at which to apply the policy (Step 21).
 - Configure application and SaaS application match criteria (Steps 22 through 31).
 - Configure match criteria for URL categories (Steps 32 through 34).
 - Define the users and user groups to which the rule applies (Step 35).
 - Select the forwarding classes and loss priorities to match (Step 36).
- Select the actions to take on matching packets, including applying a forwarding and a logging profile (Step 37).


When you configure the match conditions for a policy rule, you configure each group of related rules on a single tab on the Add Rules popup window. All rule values that you configure on the same tab, and within the same pane on a tab, are processed as a logical OR function, and rule values that you configure on different tabs are processed as a logical AND function. For example, if you include multiple addresses in the source address field, any one of the addresses can fulfill the match criteria for that field. If you include multiple source addresses and if you also configure a source zone (on the

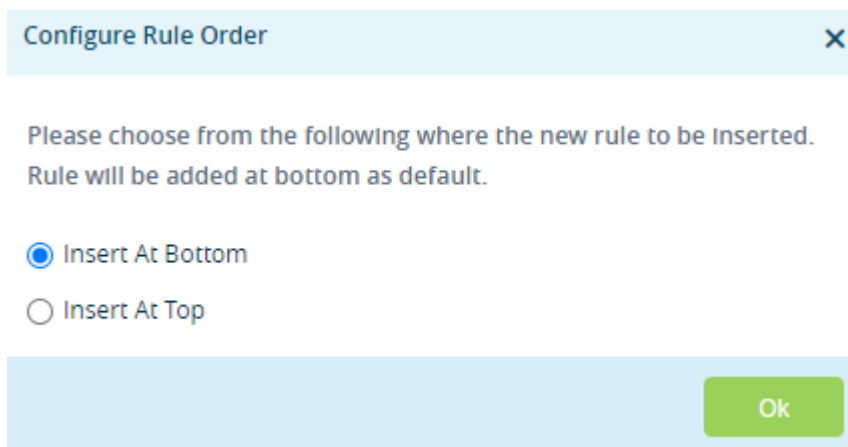
same tab, but in different panes), the traffic must match one of the source addresses AND one of the source zone parameters.

To configure a policy rule:

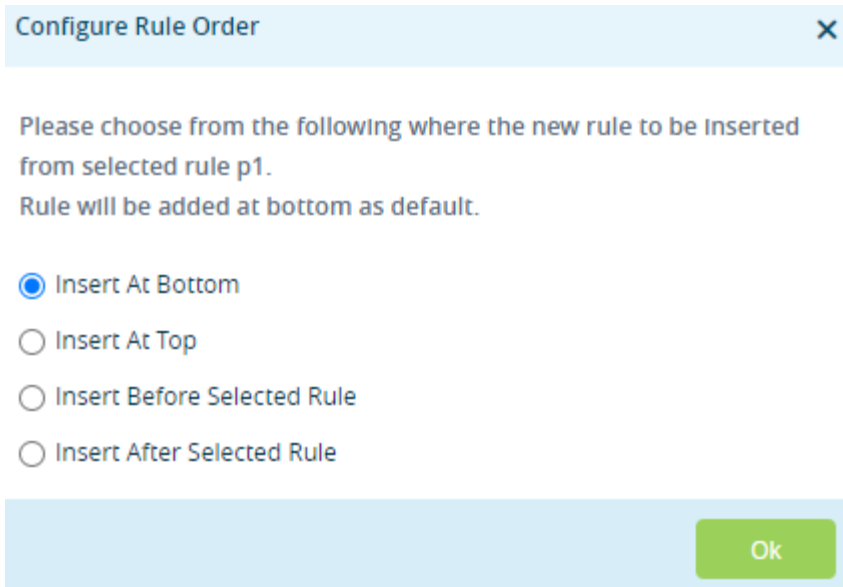
1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation bar.
 - d. Select a post-staging template in the main panel. The view changes to Appliance view.
 - e. Or, to configure a policy rule for a device's policy, select Devices > Devices in Step 1b and then select a device in the main pane.
2. Select the Configuration tab in the top menu bar.
3. Select Services  > Layer 2 SD-WAN > Policies in the left menu bar. In the main pane, the Rules tab in the horizontal menu bar is selected, and the table displays a list of configured rules. To display more of the rule components, scroll the main pane horizontally.



4. Click the  Add icon to add a rule. The Add Rules window displays.
5. If you have already added one or more rules, the Configure Rule Order popup window displays.
 - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

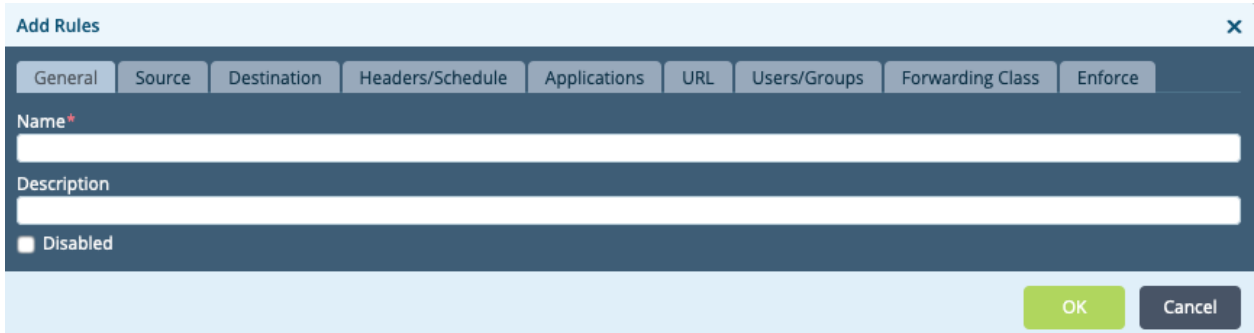


- b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:



The image shows a 'Configure Rule Order' popup window. It has a title bar with a close button (X). The main text says: 'Please choose from the following where the new rule to be inserted from selected rule p1. Rule will be added at bottom as default.' There are four radio button options: 'Insert At Bottom' (which is selected), 'Insert At Top', 'Insert Before Selected Rule', and 'Insert After Selected Rule'. At the bottom right, there is a green 'Ok' button.

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Rules popup window displays.



The image shows an 'Add Rules' popup window. It has a title bar with a close button (X). Below the title bar is a tabbed interface with tabs: 'General', 'Source', 'Destination', 'Headers/Schedule', 'Applications', 'URL', 'Users/Groups', 'Forwarding Class', and 'Enforce'. The 'General' tab is selected. Under the 'General' tab, there are two text input fields: 'Name*' and 'Description'. Below these fields is a checkbox labeled 'Disabled'. At the bottom right, there are two buttons: a green 'OK' button and a grey 'Cancel' button.

6. Select the General tab, and enter a name for the rule and a text description for the rule. Click Disabled to disable the rule after it is created.
7. Select the Source tab to configure match criteria based on source addresses, source MAC addresses, source zone, source site names. These match criteria match traffic coming from ptvi (overlay) interfaces from the configured remote sites or zones.

Add Rules [X]

General | **Source** | Destination | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | Enforce

☐ **Source Address** [+ -]

☐ **Source Mac Address** [+ -]

☐ **Source Zone** [+ -]


☐ **Source Site Name** [+ -]

+ New Address Group + New Address

+ New Zone

☐ **Source Address Negate**

OK Cancel

8. Click the  Add icon in the Source Address pane, and then select the source address, source address group, or source address region of incoming traffic to match. For zones that you have configured for interfaces and networks, select the source zone to apply the rule to traffic coming from any interfaces or networks in the zone. Note that you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see [Configure Zones and Zone Protection Profiles](#).
9. Click + New Address to add a source address. In the Add Address popup window, enter information for the following fields.

Add Address

Name*

Description

Tags

Type*

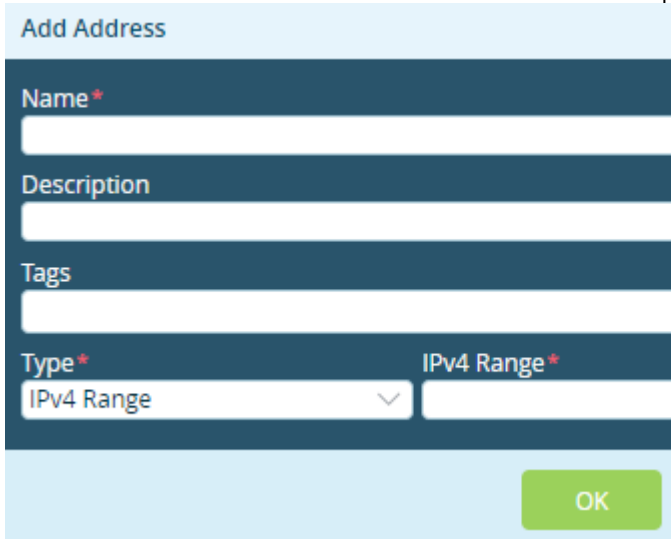
IPv4

IPv4 Address/Prefix*

OK

Cancel

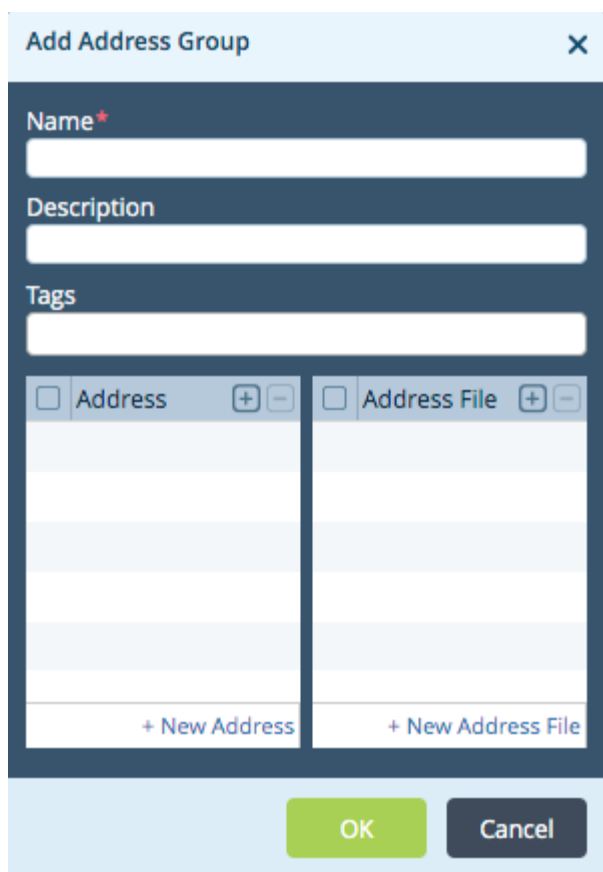
Field	Description
Name (Required)	Enter a name for the source address.
Description	Enter a text description for the source address.
Tags	Enter a keyword or phrase that allows you to filter the source address. This is useful when you have many addresses and want to view those that are tagged with a particular keyword.
Type and Address/Prefix (Required)	Select the type of IP address to match and the value to match. The name of the Address/Prefix field changes depending on the value you select in the Type field.
<ul style="list-style-type: none"> IPv4 (type); IPv4 Address/Prefix (match) 	Evaluate the address match using an IP address within the IPv4 prefix specified in the IPv4 Address/Prefix field. This is the default.
<ul style="list-style-type: none"> IPv4 Wildcard Mask (type); IPv4 Wildcard Mask (match) 	<div data-bbox="852 917 1624 1457" data-label="Form"> <p>Add Address</p> <p>Name *</p> <input type="text"/> <p>Description</p> <input type="text"/> <p>Tags</p> <input type="text"/> <p>Type * IPv4 Wildcard Mask *</p> <p>IPv4 Wildcard Mask <input type="text"/></p> <p>OK Cancel</p> </div> <p>(For Releases 20.2.2 and later.) Enter a wildcard mask for an IPv4 address. The bits in the mask can be on (1) or off (0). Only the bits that are enabled in the mask are used to determine whether an IPv4 address matches. When a bit in a wildcard mask is on, that bit must match. When a bit in a wildcard mask is off, it is considered as a "don't care" bit and is disregarded for purposes of address matching. For</p>

	<p>example, the IPv4 address and mask 192.168.3.100/255.255.3.255 matches any IPv4 address 192.168.x.100, where, for x, the first 6 bits can be on (1) or off (0) and the last two bits must be on (11). Note that in a wildcard mask, at least one bit must be on.</p> <p>You can configure overlapping wildcard addresses.</p> <p>A single session can match a maximum of 16 wildcard addresses.</p> <p>You can configure wildcard address objects individually or as part of address groups.</p> <p>You cannot combine an address prefix (or range) match with wildcard addresses to match a source or destination address.</p>
<ul style="list-style-type: none"> ◦ IPv4 Range (type); IPv4 Range (range) 	 <p>Evaluate the address match using an IP address within the IPv4 address range specified in the IPv4 Range field.</p>

<ul style="list-style-type: none">◦ IPv6 Address/Prefix (type); IPv6 Address/Prefix (range)	<div data-bbox="857 210 1624 745"><h3>Add Address</h3><p>Name*</p><input type="text"/><p>Description</p><input type="text"/><p>Tags</p><input type="text"/><p>Type* IPv6 Address/Prefix*</p><div><div>IPv6 Address/Prefix</div><div>▼</div></div><input type="text"/><p>OK Cancel</p></div> <p>Evaluate the address match using any of the IP addresses within the IPv6 address range specified in the IPv6 Address/Prefix field.</p>
<ul style="list-style-type: none">◦ FQDN (type); FQDN (match)	<div data-bbox="857 989 1624 1524"><h3>Add Address</h3><p>Name*</p><input type="text"/><p>Description</p><input type="text"/><p>Tags</p><input type="text"/><p>Type* FQDN*</p><div><div>FQDN</div><div>▼</div></div><input type="text"/><p>OK Cancel</p></div> <p>Evaluate the address match using an IP address returned in a DNS query that resolves the fully qualified domain name (FQDN) into an IP address. The FQDN cannot contain any wildcard characters.</p>

<ul style="list-style-type: none">◦ Dynamic Address (type); no range	<div data-bbox="857 205 1624 747"><div>Add Address</div><div><div>Name*</div><div></div></div><div><div>Description</div><div></div></div><div><div>Tags</div><div></div></div><div><div>Type*</div><div>Dynamic Address</div><div>Match*</div><div></div></div><div><div>OK</div><div>Cancel</div></div></div> <p>(For Releases 22.1.3 and later.) Use a dynamic address object, which is a container for an IP address list that can change dynamically. Using dynamic addresses in a policy allows you to perform a configuration before the IP addresses are known, thus avoiding the need to update the configuration each time IP addresses are added or deleted. You typically configure dynamic address objects for hosts whose IP addresses may change later, for example, if you are performing a live migration of virtual machines (VMs) using the vSphere vMotion technology to migrate a VM from one cluster to another, which changes the IP address of the VM.</p> <p>To configure a dynamic address object, issue the set orgs org-services tenant name objects addresses address object name dynamic-address CLI command.</p> <p>To update the list of IP addresses associated with a dynamic address object without updating the configuration, issue the request orgs org-services tenant name objects dynamic-address add name tenant name address private-internet-IP address CLI command.</p>
OK	Click OK.



- Click + New Address Group to add an address group. In the Add Address Group popup window, enter information for the following fields.





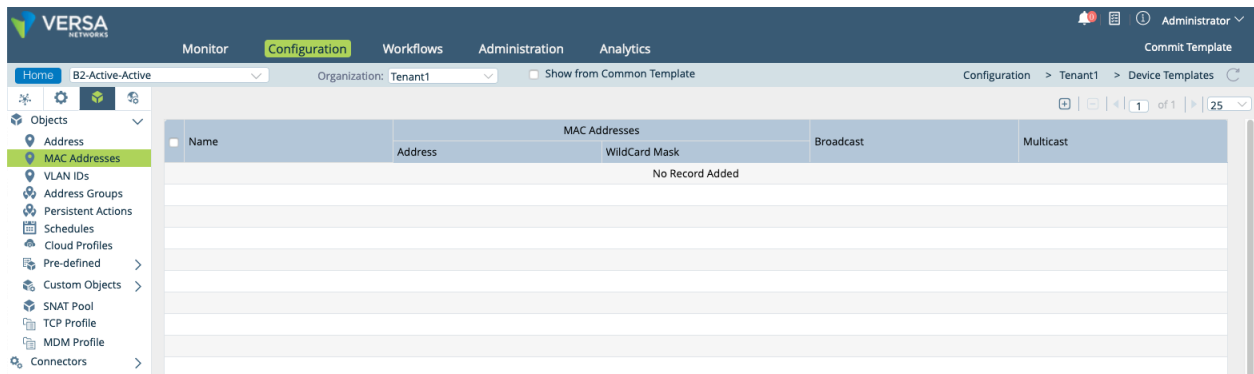
The image shows a 'Add Address Group' popup window. It has a title bar with the text 'Add Address Group' and a close button (X). The form contains the following fields:

- Name***: A text input field with a red asterisk indicating it is required.
- Description**: A text input field.
- Tags**: A text input field.
- Address**: A list box with a header row containing a checkbox and the text 'Address'. Below the header are five empty rows. At the bottom right of the list is a '+ New Address' link.
- Address File**: A list box with a header row containing a checkbox and the text 'Address File'. Below the header are five empty rows. At the bottom right of the list is a '+ New Address File' link.

At the bottom of the popup are two buttons: 'OK' (green) and 'Cancel' (dark blue).

Field	Description
Name (Required)	Enter a name for the address group.
Description	Enter a text description for the address group.
Tags	Enter a keyword or phrase that allows you to filter the address group. This is useful when you have many address groups and want to view those that are tagged with a particular keyword.
Address	Click the  Add icon to select an address to add to the group.
+ New Address	Click to add a new address to the group. In the Add Address popup window, enter a name, description, and tags for the address, select the IP address type (IPv4 or IPv6), and enter the IP address prefix.
Address File	Click the  Add icon to select an address file. The address file contains IP addresses to add to the group.
+ New Address File	Click to upload a file containing IP addresses to the VOS device. In the Upload Address Files to Appliance popup, select the filename in the Filename field. The Appliance field displays the name of the VOS device, which is the name of the tenant's device.
OK	Click OK.

11. Click Source Address Negate below the Source Address pane to block traffic to the selected source addresses instead of accepting it.
12. Click the  Add icon in the Source MAC Address pane, and then select the source MAC address. If no source MAC address is configured, create the source MAC address as follows:
 - a. In Appliance view, select Configuration from the top menu bar.
 - b. In the left menu bar, select Objects & Connectors  > Objects > MAC Addresses. The MAC Addresses dashboard displays.



- c. Click the  Add icon. In the Create MAC Address screen, enter the following information.

Create MAC Address

Name*

Customer1_mac_address

MAC Addresses

Addresses*	Description	
<div> <div></div> <div></div> </div>		+
00:23:11:11:22:11		

MAC Type

Broadcast



Wildcard Mask

Masks*	Description	
<div> <div></div> <div></div> </div>		+
06:56:8a:ab:4f:02/ff:ff:00...		



OK

Cancel

Field	Description
Name (Required)	Enter a name for the MAC address,
MAC Addresses (Group of Fields)	
<ul style="list-style-type: none"> Addresses (Required) 	Enter a MAC address.
<ul style="list-style-type: none"> Description 	Enter a description for the MAC address.

Field	Description
<ul style="list-style-type: none">  Add icon 	Click to add the MAC address.
MAC Type	Select a MAC type: <ul style="list-style-type: none"> Broadcast Multicast
Wildcard Mask (Group of Fields)	
<ul style="list-style-type: none"> Masks (Required) 	Enter a wildcard mask. For example, the wildcard mask in the screenshot above is 06:56:8a:ab:4f:02/ff:ff:00:ff:00:00.
<ul style="list-style-type: none"> Description 	Enter a description for the wildcard mask.
<ul style="list-style-type: none">  Add icon 	Click to add the MAC address.

d. Click OK.

13. In the Source Zone pane, click the  Add icon, and then select the source zone of the traffic. A zone is a set of interfaces.
14. In Source Site Name pane, click the  Add icon and select the source sites to match.
15. Select the Destination tab to configure match criteria based on destination addresses, destination MAC addresses, destination zone, and destination site names.

Add Rules

General | Source | **Destination** | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | Enforce

☐ Destination Address + -

☐ Destination Mac Address + -

☐ Destination Zone + -




☐ Destination Site Name + -

+ New Address Group + New Address

+ New Zone

☐ Destination Address Negate

OK Cancel

16. Click the  Add icon in the Destination Address pane, and then select a destination address, destination address group, or destination address region of traffic that you want to match. You can add new addresses or address groups to the Destination Address pane, and you can negate destination addresses, in the same way as was done in the Source Address pane, as described above.
17. Click the  Add icon in the Destination Mac Address pane, and then select the destination MAC address. If no destination MAC address is configured, create the destination MAC address in the same way that you created the source MAC address in Step 12.
18. Click the  Add icon in the Destination Zone pane, and then select the destination zone of the traffic. A zone is a set of interfaces.
19. Click + New Zone to add a zone. In the Add Zone popup window, enter information for the following fields. For zones that you have configured for interfaces and networks, select the destination zone to apply the rule to traffic going to any interfaces or networks in the zone. Note that you cannot configure destination zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see [Configure Zones and Zone Protection Profiles](#).

Add Zone

Name*

Interface-network

Description

Tags

Zone Protection Profile

--Select--

Log Profile

--Select--

+ Create Zone Protection Profile

+ Create Log Profile

☒ Interface and Networks

☐ Routing Instance

☐ Organization

☐ Interfaces


☐ Routing Instances


☐ Networks

☐ Organizations

OK

Cancel

Field	Description
Name	Enter a name for the zone.
Description	Enter a text description for the zone.
Tags	Enter a keyword or phrase that allows you to filter the zone. This is useful when you have many zones and want to view those that are tagged with a particular keyword.
Zone Protection Profile	Select a zone protection profile.
+ Create Zone Protection Profile	Click to create a zone protection profile.
Log Profile	Select a log profile.
+ Create Log Profile	Click to create a log profile.
Interface and Network	Click to specify the interfaces and networks that are in the zone. In the Interfaces and Networks panes, select the interfaces and network that are in the zone. Click the  Add icon to add interfaces or networks.
OK	Click OK.

20. In Destination Site Name pane, select the destination site to match. Click the  Add icon to add destination sites.
21. Select the Headers/Schedule tab to configure match criteria based on the contents of the IP packet header and to set a time at which to apply the policy. Enter information for the following fields.

Add Rules

General

Source

Destination

Headers/Schedule

Applications

URL

Users/Groups

Forwarding Class

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

+

TTL

Condition

Greater than or equal to

Value

Others

Schedules

--Select--

+ Schedule

Services

☐ Service List

+ -

+ New Service


VLAN IDs

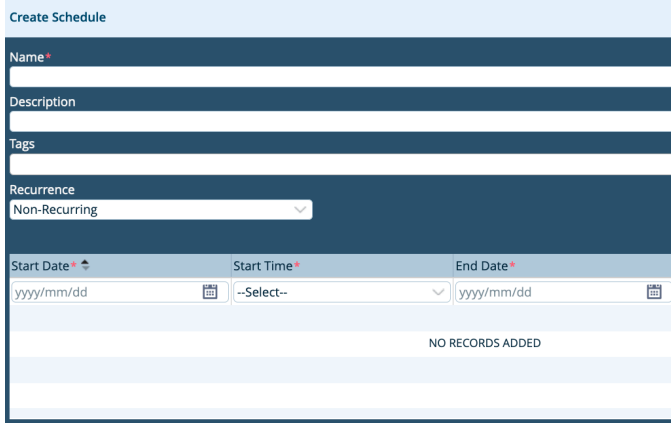


☐ VLAN ID List

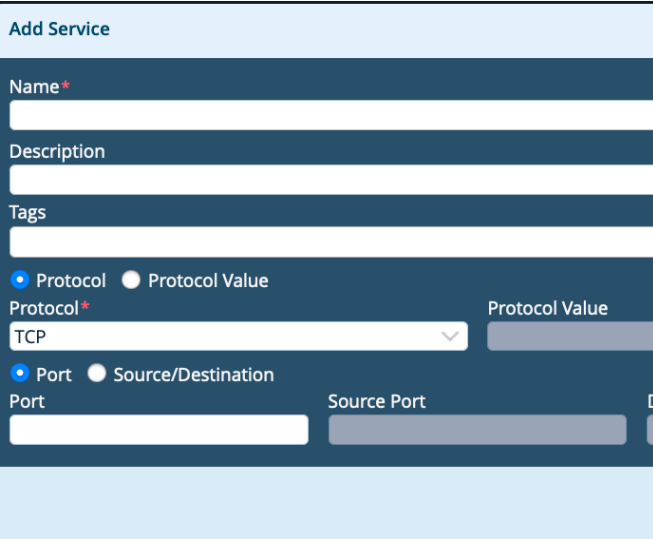

+ -


OK

Cancel

Field	Description
IP (Group of Fields)	
<ul style="list-style-type: none"> IP Version 	<p>Select the IP version:</p> <ul style="list-style-type: none"> IPv4 IPv6
<ul style="list-style-type: none"> IP Flags 	<p>Select whether routers can fragment data packets:</p> <ul style="list-style-type: none"> Don't Fragment More Fragments
<ul style="list-style-type: none"> DSCP 	<p>Click the  Add icon to add a differentiated services code point (DSCP) value.</p> <p><i>Range:</i> 0 to 63</p> <p><i>Default:</i> None</p>
TTL (Group of Fields)	
<ul style="list-style-type: none"> Condition 	<p>Select the TTL condition to use for the match. The TTL is the number of hops that a packet can travel before it is discarded. It indicates the lifespan of a packet. The condition can be one of the following boolean values:</p> <ul style="list-style-type: none"> Equal to—TTL value must be equal to the specified value to trigger the security access rule Greater than or equal to—TTL value must be greater than or equal to the specified value to trigger the security access rule Less than or equal to—TTL value must be less than or equal to the specified value to trigger the security access rule
<ul style="list-style-type: none"> Value 	<p>Enter the value for the TTL.</p> <p><i>Range:</i> 1 to 255</p> <p><i>Default:</i> None</p>
Others (Group of Fields)	

<ul style="list-style-type: none"> ◦ Schedules 	<p>Select a schedule to set the time during which the rule is in effect and now often the schedule recurs.</p>
<ul style="list-style-type: none"> ◦ + Schedule 	<p>Click to create a schedule. In the Create Schedule popup window, enter information for the following fields.</p>  <ul style="list-style-type: none"> ◦ Name (Required)—Enter a name for the schedule. ◦ Description—Enter a description for the schedule. ◦ Tags—Enter a keyword or phrase that allows you to filter the schedule name. ◦ Recurrence—Select Non-Recurring (for a one-time schedule), Daily, or Weekly. ◦ State Date, Start Time, End Date, and End Time (Required)—Enter or select the starting and ending date and time for the schedule. Then click the  Add icon. <p>Then, click OK.</p>
Services (Group of Fields)	
<ul style="list-style-type: none"> ◦ Service List 	<p>Select the services to allow or block. Click the  Add icon to select a service. The list includes predefined and custom services. A service is defined based on the destination address and port.</p>

<ul style="list-style-type: none"> + New Service 	<p>Click to create a service. In the Add Service popup window, enter information for the following fields.</p>  <ul style="list-style-type: none"> Name (Required)—Enter a name for the service. Description—Enter a description for the service. Tags—Enter a keyword or phrase that allows you to filter the service name. Protocol (Required)—Click the Protocol button and select a protocol name in the Protocol field. Protocol Value (Required)—Click the Protocol Value button and enter a protocol value in the second Protocol Value field. <i>Range:</i> 0 to 255 <i>Default:</i> None Port—Click the Port button and the ports to use in the Port field, which can be a range of ports or individual ports. <i>Range:</i> 24000 to 24500 <i>Individual ports:</i> 25000, 25001, or 25002 <i>Default:</i> None Source/Destination—Click the Source/Destination button and enter a port number in the Source Port and Destination Port fields. <p>Then, click OK.</p>
<p>VLAN IDs (Group of Fields)</p>	
<ul style="list-style-type: none"> VLAN ID List 	<p>Click the  Add icon to add VLAN IDs to the list. If no VLAN IDs are configured, create the VLAN IDs as follows:</p>

1. In Appliance view, select Configuration from the top menu bar.
2. In the left menu bar, select Object & Connectors  > VLAN ID.
3. Click the Add icon. In the Create VLAN ID screen, enter the following information.

Create VLAN ID

Name*

Description

VLAN ID*

Field	Description
Name (Required)	Enter a name for the VLAN ID.
Description	Enter a description of the VLAN ID.
VLAN ID (Required)	Enter the VLAN ID. <i>Range: 1 to 4094</i> <i>Default: None</i>

4. Click OK.

22. Select the Applications tab to configure matching criteria for applications and SaaS application groups.

Add Rules [X]

General | Source | Destination | Headers/Schedule | **Applications** | URL | Users/Groups | Forwarding Class | Enforce

Applications



Application List	[+]	[-]

+ New Group + New Filter + New Application

Saas Application Groups

Saas Application Group List	[+]	[-]

OK Cancel

23. In the Applications table, click the  Add icon and then select an application list from the predefined and custom applications. For more information about predefined and custom applications, see [Configure NGFW](#).
24. To add an application group, click + New Group. In the New Group popup window, enter a name for the group, a description, and tags.
25. Click the  Add icon and select applications to add to the group. You can click the Browse icon to display the available applications in the Application Browser window.

New Group

Name *

Description

Tags

☐ Applications

+

-

OK

Cancel

26. Click OK.
27. To add an application filter, click + New Filter. In the Add Application Filter popup window, enter a name for the filter, select the desired filters, and click OK.

Add Application Filter

Family

☐ Business-system
☐ Collaboration
☐ General-internet

Sub Family

☐ Antivirus
☐ Application service
☐ Audio_video

Risks

223

1

817

2

1205

3

121

4

167

5

Productivity

225

1

586

2

1582

3

101

4

39

5

Application Tags - Security

☐ Anonymizer
☐ Bandwidth
☐ Dataleak

Application Tags - SDWAN

☐ Audio_stream
☐ Business
☐ Cloud

Application Tags - General

☐ Networking
☐ News_portal
☐ P2p

Name *

Non-Business

Description

Non_business X

Applications

	Family	Sub Family	Risks	Productivity	Security	SDWAN	General
01NET	general-inter...	web	2	2		Non_business	Web
050PLUS	media	audio_video	4	2	Dataleak	Audio_stream Non_business	Im_mc Voip
0ZZ0	general-inter...	web	4	2	Filetransfer	Cloud Data Non_business	File_mngt Web
10050NET	general-inter...	web	3	1		Non_business	Web Web_sites
10086CN	general-inter...	web	3	3		Non_business	Web
104COM	general-inter...	web	3	3		Non_business	Web
1111TW	general-inter...	web	3	1		Non_business	Web
114LA	general-inter...	web	3	3		Non_business	Web

OK

Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:09:58 GMT

Copyright © 2024, Versa Networks, Inc.

28. To add an application, click + New Application. In the New Application popup window, enter information for the following fields.

New Application

Name*

Description*

Precedence*

Application Timeout (sec)

Application match IPS

Attributes

Match Information

Family	Sub-Family	Risk	Productivity	Application Tags		
				Security	SDWAN	General
<input checked="" type="radio"/> Business-sys...	<input checked="" type="radio"/> Antivirus	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> 1	<input type="checkbox"/> Anonymizer	<input type="checkbox"/> Audio_stream	<input type="checkbox"/> Aaa
<input type="radio"/> Collaboration	<input type="radio"/> Application-s...	<input type="radio"/> 2	<input type="radio"/> 2	<input type="checkbox"/> Bandwidth	<input type="checkbox"/> Av	<input type="checkbox"/> Adult_content
<input type="radio"/> General-inte...	<input type="radio"/> Audio_video	<input type="radio"/> 3	<input type="radio"/> 3	<input type="checkbox"/> Dataleak	<input type="checkbox"/> Business	<input type="checkbox"/> Advertising
<input type="radio"/> Media	<input type="radio"/> Authenticati...	<input type="radio"/> 4	<input type="radio"/> 4	<input type="checkbox"/> Evasive	<input type="checkbox"/> Cloud	<input type="checkbox"/> Analytics
<input type="radio"/> Networking	<input type="radio"/> Behavioral	<input type="radio"/> 5	<input type="radio"/> 5	<input type="checkbox"/> Filetransfer	<input type="checkbox"/> Data	<input type="checkbox"/> Anonymizer
	<input type="radio"/> Compression			<input type="checkbox"/> Malware	<input type="checkbox"/> Ips	<input type="checkbox"/> Audio_chat
	<input type="radio"/> Database			<input type="checkbox"/> Misused	<input type="checkbox"/> Non_business	<input type="checkbox"/> Basic
	<input type="radio"/> Encrypted			<input type="checkbox"/> Tunnel	<input type="checkbox"/> Video_stream	<input type="checkbox"/> Blog
	<input type="radio"/> Encrypted-tu...			<input type="checkbox"/> Vulnerable		<input type="checkbox"/> Cdn
						<input type="checkbox"/> Chat

OK

Cancel

Field	Description
Name (Required)	Enter a name for the application.
Description (Required)	Enter a description for the application.
Precedence (Required)	Enter a value for the priority of the application. <i>Range:</i> 0 to 65535 <i>Default:</i> None
Application Timeout	Enter how long to wait before timing out the application, in seconds. <i>Range:</i> 1 through 15999999 seconds <i>Default:</i> None
App Match IPs	Click to match the IP address of the application.

29. In the Attributes tab, enter information for the following fields.

Field	Description
Family	Select the family to which the application belongs.
Subfamily	Select the subfamily to which the application belongs.
Risk	Select the risk level to assign to the application. A value of 1 indicates the lowest risk level, and a value of 5 indicates the highest.
Productivity	Select a productivity level to assign to the application.
Application Tags	Select one or more security, Layer 2 SD-WAN, and general tags to associate with the application.

30. Select the Match Information tab. In the Add Match Information popup window, enter information for the following fields.

Add Match Information
✕

Name*

Host Pattern

Protocol Value

Source Address

Destination Address

☐ Source Port

☒ Value
☐ Range

Source Port Value
Low
High

☐ Destination Port

☒ Value
☐ Range

Destination Port Value
Low
High

OK

Cancel


Field	Description
Name	Enter a name for the application match.
Host Pattern	Enter the host pattern to match.
Protocol Value	Enter the application's protocol name or number. <i>Range:</i> 0 to 255 <i>Default:</i> None
Source Address	Enter the IP address and mask of the source application.
Destination Address	Enter the IP address and mask of the destination application.
Source Port (Group of Fields)	Click to match the source ports of the application.

Field	Description
◦ Value	Click to match a single source port of the application.
◦ Source Port Value	Enter the source port number. <i>Range:</i> 0 to 65535 <i>Default:</i> None
◦ Range	Click to match a range of source ports of the application.
◦ Low	For a range of source ports, enter the lowest port number. <i>Range:</i> 0 to 65535 <i>Default:</i> None
◦ High	For a range of source ports, enter the highest port number. <i>Range:</i> 0 to 65535 <i>Default:</i> None
Destination Port (Group of Fields)	Click to match destination ports of the application.
◦ Value	Click to match a single destination port of the application.
◦ Destination Port Value	Enter the destination port number. <i>Range:</i> 0 to 65535 <i>Default:</i> None
◦ Range	Click to match a range of destination ports of the application.
◦ Low	For a range of destination ports, enter the lowest port

Field	Description
	<p>number.</p> <p><i>Range:</i> 0 to 65535</p> <p><i>Default:</i> None</p>
<ul style="list-style-type: none"> High 	<p>For a range of destination ports, enter the highest port number.</p> <p><i>Range:</i> 0 to 65535</p> <p><i>Default:</i> None</p>

31. Click OK.
32. Select the URL tab to configure match criteria for URL categories. Note that for URL matching to work, you must enable the URL category cache. For more information, see [Configure Application and URL Category Detection Parameters](#), below.

The screenshot shows the 'Add Rules' window with the 'URL' tab selected. Under 'URL Categories', there is a list containing 'URL Category List'. A '+ New URL Category' button is located at the bottom right of the list area. The window has 'OK' and 'Cancel' buttons at the bottom right.

33. In URL Category List, click the  Add icon and select a URL category.
34. To add a URL category, click + New URL Category. In the New URL Category popup window, enter information for the following fields. For more information, see [Configure URL Filtering](#).

New URL Category

X

Name*

Description

Tags

Confidence

URL File

--Select--

URL Patterns

URL Strings

Q Search



< 1 >

Pattern	Reputation	
	--Select--	+
NO RECORDS ADDED		

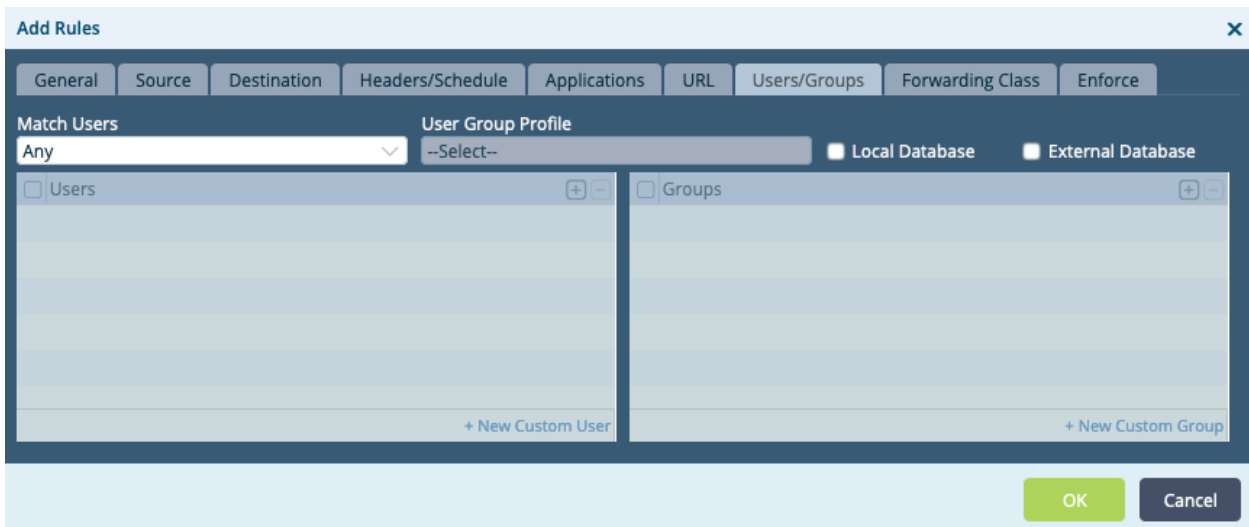
OK

Cancel

Field	Description
Name (Required)	Enter a name for the URL category.
Description	Enter a description for the URL category.
Tags	Enter a keyword or phrase that allows you to filter the URL category. This is useful when you have many categories and want to view categories that are tagged with a particular keyword.
Confidence	<p>Enter a confidence value for the URL category. The confidence value is used to break a tie when multiple URL categories match a single URL. If a URL matches multiple categories, the one with the higher confidence value takes precedence.</p> <p><i>Range:</i> 1 through 100</p> <p><i>Default:</i> None</p>
URL File	Select a file that contains URL patterns or strings.
URL Patterns (Tab)	
<ul style="list-style-type: none"> Pattern 	<p>Enter a URL pattern to match a group of URLs. The pattern can include regex patterns. For example, you can enter <code>www.versa-networks.com</code> or <code>*.versa-networks</code>. If you include a backslash (\) in the regex pattern, you must escape it by preceding it with a backslash.</p>
<ul style="list-style-type: none"> Reputation 	<p>Select a reputation to assign to the URL pattern. The following are the predefined URL reputation types, listed in order from lowest to highest risk:</p> <ul style="list-style-type: none"> Trustworthy Low Risk Moderate Risk Suspicious High

<ul style="list-style-type: none"> ◦  Add icon 	Click to add the URL pattern to the URL category.
URL Strings (Tab)	
<ul style="list-style-type: none"> ◦ String 	Enter a URL string to match a single URL.
<ul style="list-style-type: none"> ◦ Reputation 	<p>Select a reputation to assign to the URL string. The following are the predefined URL reputation types, listed in order from lowest to highest risk:</p> <ul style="list-style-type: none"> ◦ Trustworthy ◦ Low Risk ◦ Moderate Risk ◦ Suspicious ◦ High
<ul style="list-style-type: none"> ◦  Add icon 	Click to add the URL string to the URL category.

35. Select the Users/Groups tab to define the users and user groups to which the rule applies. Enter information for the following fields.



Add Rules [X]



General Source Destination Headers/Schedule Applications URL **Users/Groups** Forwarding Class Enforce

Match Users: Any [v] User Group Profile: --Select-- [v] ☐ Local Database ☐ External Database

☐ Users [+ -] ☐ Groups [+ -]

+ New Custom User + New Custom Group

OK Cancel

Field	Description
Match Users	<p>Select the users to match:</p> <ul style="list-style-type: none"> Any—If you select to match any users, you cannot configure any other fields on this tab. Known—If you select to match known users, you cannot configure any other fields on this tab. Unknown—If you select to match unknown users, you cannot configure any other fields on this tab. Selected—If you choose this option, you can configure the other fields on this tab.
User Group Profile	If you chose Selected in the Match Users field, select a user group profile to match users in a group.
Local Database	If you chose Selected in the Match Users field, click to create a local database to match users and user groups. Select these users and user groups in the Users and Groups tables.
External Database	If you chose Selected in the Match Users field, click to use an external database to match users and user groups. Select these users in the Users table.
Users	If you chose Selected in the Match Users field, click the  Add icon and select a user. Select + New Custom User to add a user.
Groups	If you chose Selected in the Match Users field, click the  Add icon and select a user group. Select + New Custom Group to add a user group.

36. Select the Forwarding Class tab to choose the forwarding classes and loss priorities to match. Enter information for the following fields.
- Note that in some situations, such as App QoS policy, a forwarding class may not be assigned to a session until the second packet in the session or sometimes until the eighth packet in the session. For this reason, it is recommended that you do not configure a match based on the forwarding class for sessions that consist only of a few packets. Also, do not configure anything on the Forwarding Class tab if you are also configuring DIA or next-hop selection rules in the SD-WAN forwarding profile.

Add Rules

General
Source
Destination
Headers/Schedule
Applications
URL
Users/Groups
Forwarding Class
Enforce

Forwarding Class

Select options

Loss Priority

--Select--

OK
Cancel

Field	Description
Forwarding Class	<p>Select the forwarding class to match:</p> <ul style="list-style-type: none"> Forwarding Class 0 (network control) Forwarding Class 1 Forwarding Class 2 Forwarding Class 3 Forwarding Class 4 (expedited forwarding) Forwarding Class 5 Forwarding Class 6 Forwarding Class 7 Forwarding Class 8 (assured forwarding) Forwarding Class 9 Forwarding Class 10 Forwarding Class 11 Forwarding Class 12 (best effort) Forwarding Class 13 Forwarding Class 14 Forwarding Class 15
Loss Priority	<p>Select the loss priority to assign to the forwarding class:</p> <ul style="list-style-type: none"> High—Traffic has a greater likelihood of being dropped. Low—Traffic has a lesser likelihood of being dropped.

37. Select the Enforce tab to select the actions to take on matching packets, including applying a forwarding and a logging profile. Enter information for the following fields.

Add Rules

General

Source

Destination

Headers/Schedule

Applications

URL

Users/Groups

Forwarding Class

Enforce

Forwarding

Action*
Allow Flow

Forwarding Profile
FP1

View Forwarding Profile

Logging

LEF Profile
--Select--

Event
Never

Rate Limit
10

Default Profile

OK

Cancel

Field	Description
Forwarding (Group of Fields)	
<ul style="list-style-type: none"> Action 	Select the action to take on matching traffic: <ul style="list-style-type: none"> Allow Flow Deny Flow
<ul style="list-style-type: none"> Forwarding Profile 	Select the forwarding profile to apply to matching traffic.
<ul style="list-style-type: none"> View Forwarding Profile 	Click to view the selected forwarding profile.
Logging (Group of Fields)	Log changes in the forwarding action.
<ul style="list-style-type: none"> LEF Profile 	Select a LEF profile. Logs are sent to the active collector of the LEF profile. For information about configuring a LEF profile, see Configure Log Export Functionality . For information about associating a LEF profile with a feature or service, see Apply Log Export Functionality .
<ul style="list-style-type: none"> Default Profile 	Click to use the default LEF profile instead of the profile from the LEF profile field. For information about configuring a default LEF profile, see Configure Log Export Functionality .
<ul style="list-style-type: none"> Event 	Select the events to log: <ul style="list-style-type: none"> All SLA Violated—Generate a log when the session moves to or from an SLA-violated circuit. Priority Change—Generate a log when the session moves between circuits of different priorities. Never—Never log changes. <p><i>Default:</i> Never</p>
<ul style="list-style-type: none"> Rate Limit 	Enter the number of logs to generate per second. You should configure a rate limit when changes happen constantly, to buffer all changes logged during the specified interval and send them together in a single message. <p><i>Range:</i> 10 to 200</p> <p><i>Default:</i> 10</p>

38. Click OK.


Configure Policy Rules for Layer 3 SD-WAN Policy

In policy rules, you configure the conditions for matching packets of interest, and you also configure the forwarding, logging, and monitoring actions to take on the packets that match the conditions. To configure policy rules, you select an organization (that is, a tenant), and then you select one of the tenant's post-staging templates. Then you perform the following steps, which are described in the procedure below:

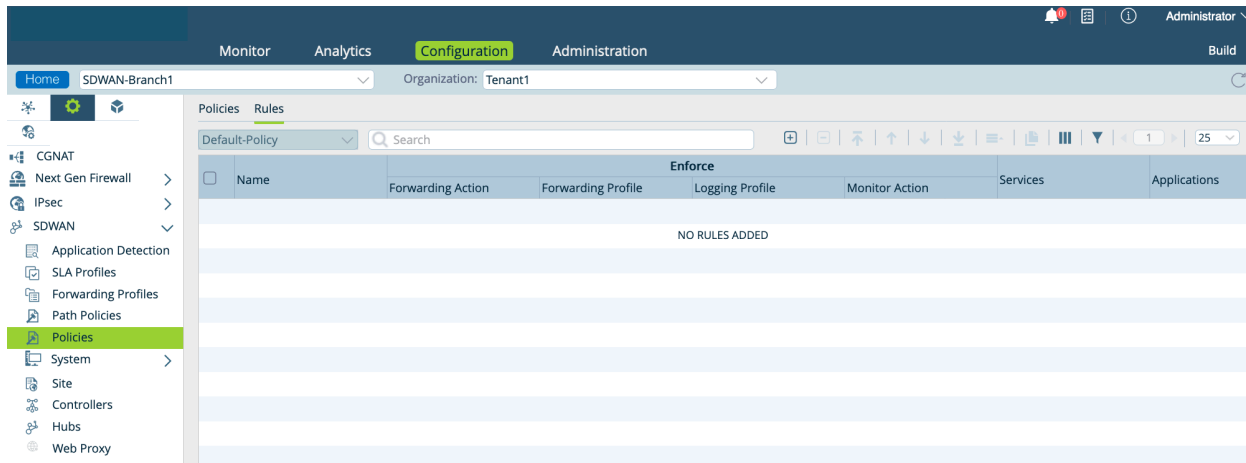
- Add a new rule (Steps 1 through 5).
- Configure a rule name (Step 6).
- Configure match conditions:
 - Configure address, site, and zone match criteria (Steps 7 through 18).
 - Configure match criteria based on the contents of the IP packet header and to set a time at which to apply the policy (Step 19).
 - Configure application and SaaS application match criteria (Steps 20 through 27).
 - Configure match criteria for URL categories (Steps 28 through 30).
 - Define the users and user groups to which the rule applies (Step 31).
 - Select the forwarding classes and loss priorities to match (Step 32).
- Select the actions to take on matching packets, including applying a forwarding and a logging profile and defining monitor parameters (Step 33).


When you configure the match conditions for a policy rule, you configure each group of related rules on a single tab on the Add Rules popup window. All rule values that you configure on the same tab, and within the same pane on a tab, are processed as a logical OR function, and rule values that you configure on different tabs are processed as a logical AND function. For example, if you include multiple addresses in the source address field, any one of the addresses can fulfill the match criteria for that field. If you include multiple source addresses and if you also configure a source zone (on the same tab, but in different panes), the traffic must match one of the source addresses AND one of the source zone parameters.

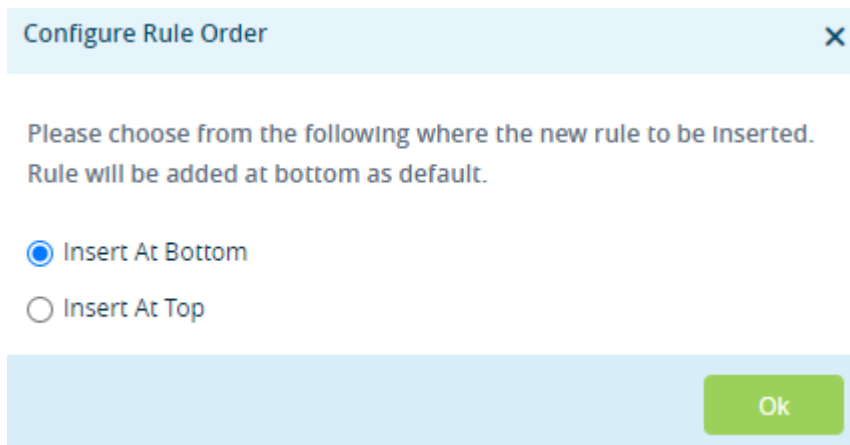
To configure a policy rule:


1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation bar.
 - d. Select a post-staging template in the main panel. The view changes to Appliance view.
 - e. Or, to configure a policy rule for a device's policy, select Devices > Devices in Step 1b and then select a device in the main pane.
2. Select the Configuration tab in the top menu bar.
3. Select Services  > SD-WAN > Policies in the left menu bar. In the main pane, the Rules tab in the horizontal

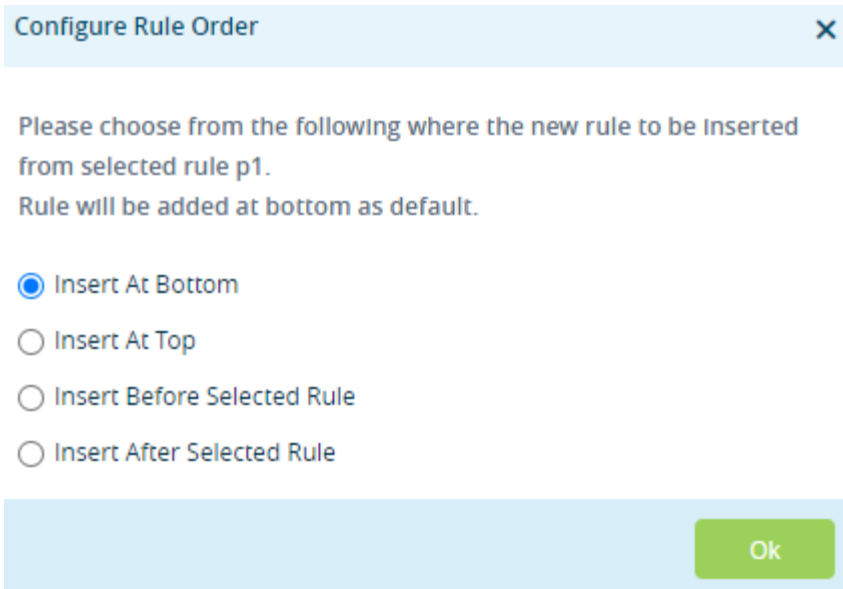
menu bar is selected, and the table displays a list of configured rules. To display more of the rule components, scroll the main pane horizontally.



4. Click the  Add icon to add a rule. The Add Rules window displays.
5. (For Releases 21.2.1 and later.) If you already added one or more rules, the Configure Rule Order popup window displays.
 - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.



- b. If you select a rule and then click the  Add icon, the Configure Rule Order popup window displays the following options:



Configure Rule Order [X]

Please choose from the following where the new rule to be inserted from selected rule p1.
Rule will be added at bottom as default.

☒ Insert At Bottom

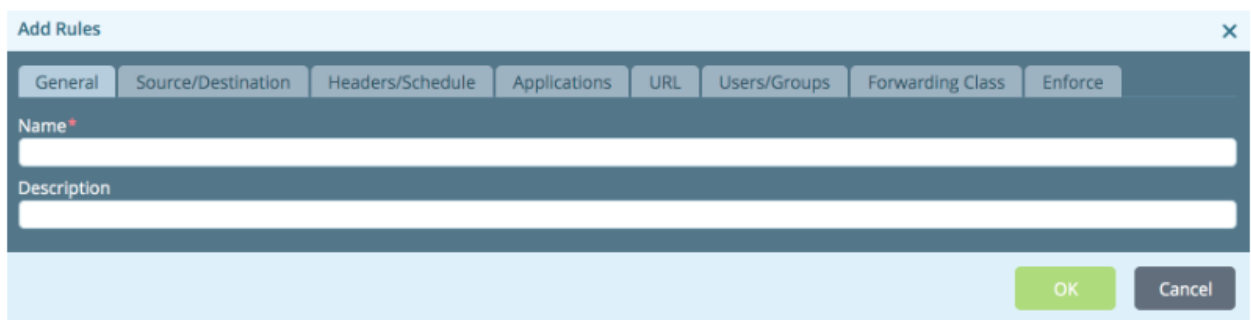
☐ Insert At Top

☐ Insert Before Selected Rule

☐ Insert After Selected Rule

[Ok]

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Rule popup window displays.



Add Rules [X]

General Source/Destination Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

Name *

Description

[Ok] [Cancel]

6. Select the General tab, and enter a name for the rule and a text description for the rule.
7. Select the Source/Destination tab to configure match criteria based on source and destination addresses, source and destination site names, and source and destination zones. These match criteria match traffic coming from ptvi (overlay) interfaces from the configured remote sites or zones.

Add Rules

General | **Source/Destination** | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | Enforce

☐ Source Zone

☐ Destination Zone

☐ Source Site Name

☐ Destination Site Name

☐ Source Address


☐ Destination Address

☐ Source Address Negate

☐ Destination Address Negate

Routing Instance: --Select--

OK Cancel

8. Click the  Add icon in the Source Zone pane, For zones that you have configured for interfaces and networks, select the source zone to apply the rule to traffic coming from any interfaces or networks in the zone. Note that you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see [Configure Zones and Zone Protection Profiles](#).
9. Click + New Zone to add a zone. In the Add Zone popup window, enter information for the following fields.

Add Zone

Name*

Interface-network

Description

Tags

Zone Protection Profile

--Select--

Log Profile

--Select--

+ Create Zone Protection Profile

+ Create Log Profile

☒ Interface and Networks

☐ Routing Instance

☐ Organization

☐ Interfaces


☐ Routing Instances





☐ Networks

☐ Organizations

OK

Cancel

Field	Description
Name	Enter a name for the zone.
Description	Enter a text description for the zone.
Tags	Enter a keyword or phrase that allows you to filter the zone. This is useful when you have many zones and want to view those that are tagged with a particular keyword.
Zone Protection Profile	Select a zone protection profile.
+ Create Zone Protection Profile	Click to create a zone protection profile.
Log Profile	Select a log profile.
+ Create Log Profile	Click to create a log profile.
Interface and Network	Click to specify the interfaces and networks that are in the zone. In the Interfaces and Networks panes, select the interfaces and network that are in the zone. Click the  Add icon to add interfaces or networks.
OK	Click OK.

10. Click the  Add icon in the Destination one pane. For zones that you have configured for interfaces and networks, select the destination zone to apply the rule to traffic going to any interfaces or networks in the zone. Note that you cannot configure destination zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see [Configure Zones and Zone Protection Profiles](#). Click + New Zone to add a zone, as described in Step 9.
11. In Source Site Name pane, select the source sites to match. Click the  Add icon to add source sites.
12. In Destination Name Site pane, select the destination site to match. Click the  Add icon to add destination sites.
13. Click the  Add icon in the Source Address pane, and from the drop-down list select the source address, source address group, or source address region of incoming traffic to match.
14. Click + New Address to add a source address. In the Add Address popup window, enter information for the following fields.

Add Address

Name*

Description

Tags

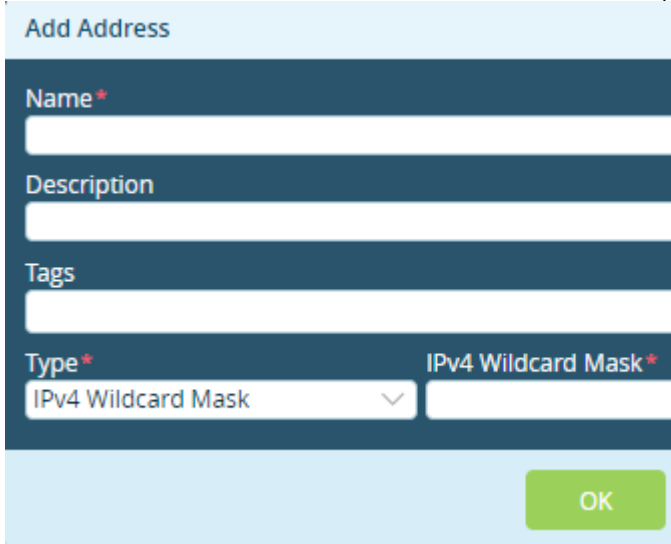
Type*

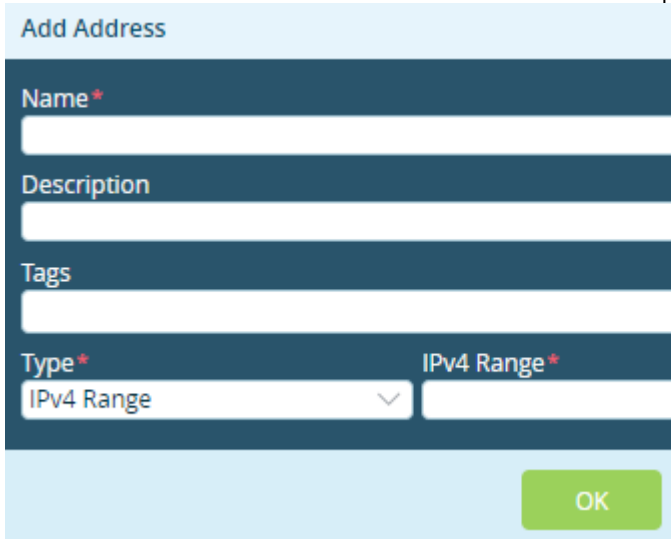
IPv4

IPv4 Address/Prefix*

OK

Cancel

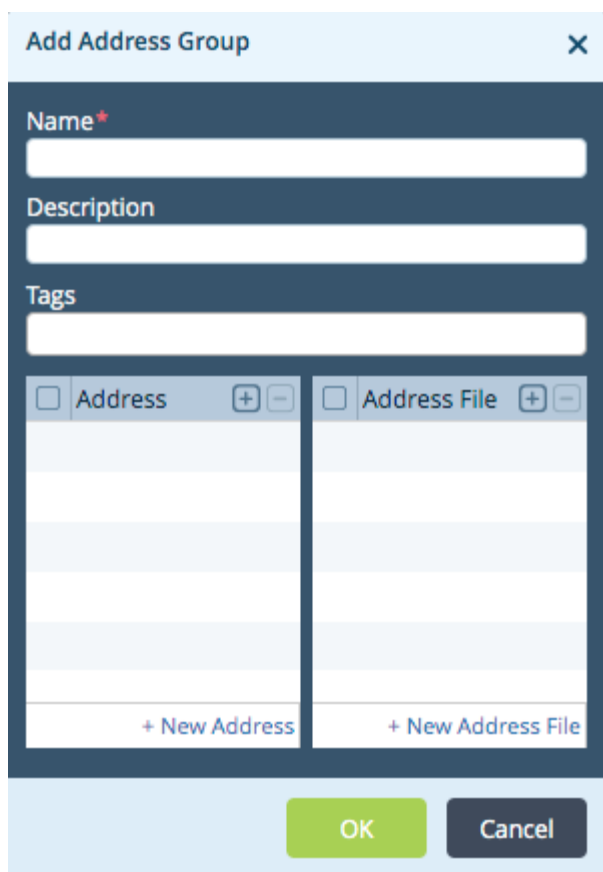
Field	Description
Name	Enter a name for the source address.
Description	Enter a text description for the source address.
Tags	Enter a keyword or phrase that allows you to filter the source address. This is useful when you have many addresses and want to view those that are tagged with a particular keyword.
Type and Address/Prefix (Required)	Select the type of IP address to match and the value to match. The name of the Address/Prefix field changes depending on the value you select in the Type field.
<ul style="list-style-type: none"> IPv4 (type); IPv4 Address/Prefix (match) 	Evaluate the address match using an IP address within the IPv4 prefix specified in the IPv4 Address/Prefix field. This is the default.
<ul style="list-style-type: none"> IPv4 Wildcard Mask (type); IPv4 Wildcard Mask (match) 	 <p>(For Releases 20.2.2 and later.) Enter a wildcard mask for an IPv4 address. The bits in the mask can be on (1) or off (0). Only the bits that are enabled in the mask are used to determine whether an IPv4 address matches. When a bit in a wildcard mask is on, that bit must match. When a bit in a wildcard mask is off, it is considered as a "don't care" bit and is disregarded for purposes of address matching. For</p>

	<p>example, the IPv4 address and mask 192.168.3.100/255.255.3.255 matches any IPv4 address 192.168.x.100, where, for x, the first 6 bits can be on (1) or off (0) and the last two bits must be on (11). Note that in a wildcard mask, at least one bit must be on.</p> <p>You can configure overlapping wildcard addresses.</p> <p>A single session can match a maximum of 16 wildcard addresses.</p> <p>You can configure wildcard address objects individually or as part of address groups.</p> <p>You cannot combine an address prefix (or range) match with wildcard addresses to match a source or destination address.</p>
<ul style="list-style-type: none"> ◦ IPv4 Range (type); IPv4 Range (range) 	 <p>Evaluate the address match using an IP address within the IPv4 address range specified in the IPv4 Range field.</p>

<ul style="list-style-type: none">◦ IPv6 Address/Prefix (type); IPv6 Address/Prefix (range)	<div data-bbox="857 210 1624 745"><div>Add Address</div><div><div>Name*</div><div></div></div><div><div>Description</div><div></div></div><div><div>Tags</div><div></div></div><div><div>Type*</div><div>IPv6 Address/Prefix</div></div><div><div>IPv6 Address/Prefix*</div><div></div></div><div><div>OK</div><div>Cancel</div></div></div> <p>Evaluate the address match using any of the IP addresses within the IPv6 address range specified in the IPv6 Address/Prefix field.</p>
<ul style="list-style-type: none">◦ FQDN (type); FQDN (match)	<div data-bbox="857 989 1624 1524"><div>Add Address</div><div><div>Name*</div><div></div></div><div><div>Description</div><div></div></div><div><div>Tags</div><div></div></div><div><div>Type*</div><div>FQDN</div></div><div><div>FQDN*</div><div></div></div><div><div>OK</div><div>Cancel</div></div></div> <p>Evaluate the address match using an IP address returned in a DNS query that resolves the fully qualified domain name (FQDN) into an IP address. The FQDN cannot contain any wildcard characters.</p>

<ul style="list-style-type: none">◦ Dynamic Address (type); no range	<div data-bbox="857 205 1624 747"><div>Add Address</div><div><div>Name*</div><div></div></div><div><div>Description</div><div></div></div><div><div>Tags</div><div></div></div><div><div>Type*</div><div>Dynamic Address</div><div>Match*</div><div></div></div><div><div>OK</div><div>Cancel</div></div></div> <p>(For Releases 22.1.3 and later.) Use a dynamic address object, which is a container for an IP address list that can change dynamically. Using dynamic addresses in a policy allows you to perform a configuration before the IP addresses are known, thus avoiding the need to update the configuration each time IP addresses are added or deleted. You typically configure dynamic address objects for hosts whose IP addresses may change later, for example, if you are performing a live migration of virtual machines (VMs) using the vSphere vMotion technology to migrate a VM from one cluster to another, which changes the IP address of the VM.</p> <p>To configure a dynamic address object, issue the set orgs org-services tenant name objects addresses address object name dynamic-address CLI command.</p> <p>To update the list of IP addresses associated with a dynamic address object without updating the configuration, issue the request orgs org-services tenant name objects dynamic-address add name tenant name address private-internet-IP address CLI command.</p>
OK	Click OK.



- Click + New Address Group to add an address group. In the Add Address Group popup window, enter information for the following fields.




The image shows a 'Add Address Group' popup window. It has a title bar with the text 'Add Address Group' and a close button (X). The form contains the following fields:

- Name***: A text input field with a red asterisk indicating it is required.
- Description**: A text input field.
- Tags**: A text input field.
- Address**: A list box with a header row containing a checkbox and the text 'Address'. Below the header are five empty rows. At the bottom right of the list is a '+ New Address' link.
- Address File**: A list box with a header row containing a checkbox and the text 'Address File'. Below the header are five empty rows. At the bottom right of the list is a '+ New Address File' link.

At the bottom of the window are two buttons: 'OK' (green) and 'Cancel' (dark blue).

Field	Description
Name	Enter a name for the address group.
Description	Enter a text description for the address group.
Tags	Enter a keyword or phrase that allows you to filter the address group. This is useful when you have many address groups and want to view those that are tagged with a particular keyword.
Address	Click the  Add icon to select an address from the drop-down list to add to the group.
+ New Address	Click to add a new address to the group. In the Add Address popup window, enter a name, description, and tags for the address, select the IP address type (IPv4 or IPv6), and enter the IP address prefix.
Address File	Click the  Add icon to select an address file from the drop-down list. The address file contains IP addresses to add to the group.
+ New Address File	Click to upload a file containing IP addresses to the Versa Operating System™ (VOS™) device. In the Upload Address Files to Appliance popup enter, select the filename in the Filename field. The Appliance field displays the name of the VOS device, which is the name of the tenant's device.
OK	Click OK.

16. Click Source Address Negate below the Source Address pane to block traffic to the selected source addresses instead of accepting it.
17. Select a Routing Instance from the drop-down menu.
18. Click the  Add icon in the Destination Address pane, and from the drop-down list, select a destination address, destination address group, or destination address region of traffic that you want to match. You add new addresses or address groups to the Destination Address pane, and you can negate destination addresses, in the same way as for the Source Address pane, as described in Steps 14 through 16.
19. Select the Headers/Schedule tab to configure match criteria based on the contents of the IP packet header and to set a time at which to apply the policy. Enter information for the following fields.

Add Rules

General

Source/Destination

Headers/Schedule

Applications

URL

Users/Groups

Forwarding Class

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

+

TTL

Condition

Greater than or equal to

Value

Others

Schedules

--Select--

+ Schedule

Services


☐ Service List



+ -

+ New Service

OK

Cancel

Field	Description
IP (Group of Fields)	
<ul style="list-style-type: none"> IP Version 	<p>Select the IP version:</p> <ul style="list-style-type: none"> IPv4 IPv6
<ul style="list-style-type: none"> IP Flags 	<p>Select whether routers can fragment data packets:</p> <ul style="list-style-type: none"> Don't Fragment More Fragments
<ul style="list-style-type: none"> DSCP 	<p>Click the  Add icon to a differentiated services code point (DSCP) value.</p>
TTL (Group of Fields)	
<ul style="list-style-type: none"> Condition 	<p>Select the TTL condition to use for the match. The TTL is the number of hops that a packet can travel before it is discarded and indicates the lifespan of a packet. The condition can be one of the following boolean values:</p> <ul style="list-style-type: none"> Equal to—TTL value must be equal to the specified value to trigger the security access rule Greater than or equal to—TTL value must be greater than or equal to the specified value to trigger the security access rule Less than or equal to—TTL value must be less than or equal to the specified value to trigger the security access rule
<ul style="list-style-type: none"> Value 	<p>Enter the value for the TTL.</p>
Others (Group of Fields)	
<ul style="list-style-type: none"> Schedules 	<p>Select a schedule to set the time and frequency at which the rule is in effect.</p>
<ul style="list-style-type: none"> + Schedule 	<p>Click to create a schedule. In the Create Schedule popup window, enter information for the following fields.</p>

	 <ul style="list-style-type: none"> ◦ Name—Enter a name for the schedule. ◦ Description—Enter a description for the schedule. ◦ Tags—Enter a keyword or phrase that allows you to filter the schedule name. ◦ Recurrence—Select Non-Recurring (for a one-time schedule), Daily, or Weekly. ◦ State Date, Start Time, End Date, and End Time—Enter or select the starting and ending date and time for the schedule. Then click the . <p>Then, click OK.</p>
Services (Group of Fields)	
<ul style="list-style-type: none"> ◦ Service List 	<p>Select the services to allow or block. Click the  Add icon to select a service from the drop-down list. The list includes predefined and user-defined services. A service is defined based on the destination address and port.</p>
<ul style="list-style-type: none"> ◦ + New Service 	<p>Click to create a service. In the Add Service popup window, enter information for the following fields.</p>

- Name—Enter a name for the service.
- Description—Enter a description for the service.
- Tags—Enter a keyword or phrase that allows you to filter the service name.
- Protocol—Click and enter a protocol name in the second Protocol field.
- Protocol Value—Click and enter a protocol number in the second Protocol Value field.
- Port—Click and in the second Port field, enter a source or destination port number.
- Source/Destination—Click and enter a port number in the Source Port and Destination Port fields.

Then, click OK.

20. Select the Applications tab to configure matching criteria for applications and SaaS application groups.

Add Rules [X]

General | Source/Destination | Headers/Schedule | **Applications** | URL | Users/Groups | Forwarding Class | Enforce

Applications


Application List	[+]

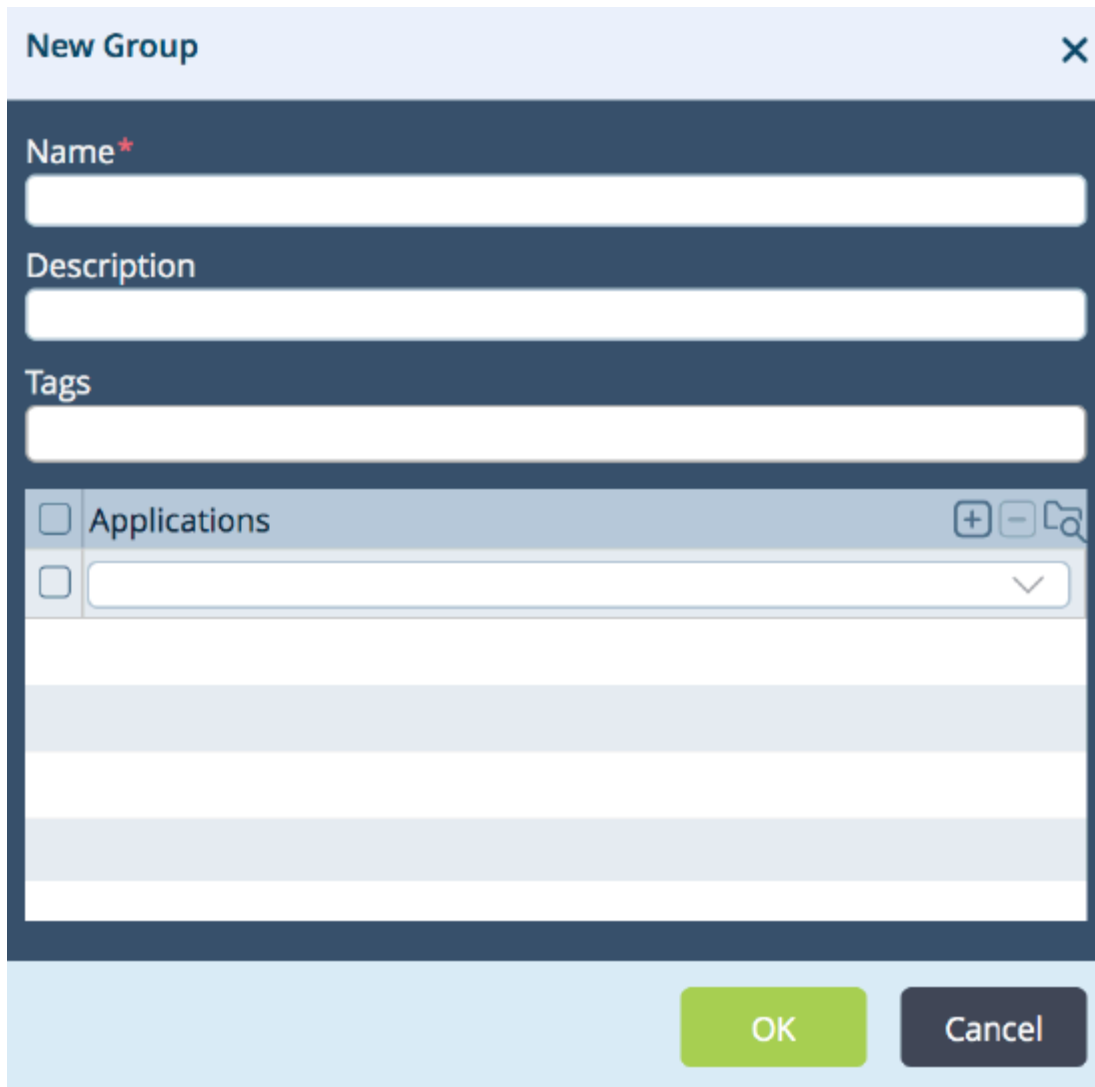
+ New Group + New Filter + New Application

Saas Application Groups

Saas Application Group List	[+]

OK Cancel

21. In the Applications table, click the  Add icon and select an application list from the drop-down list, which includes predefined and user-defined applications. For more information about predefined and user-defined applications, see [Configure NGFW](#).
22. To add an application group, click + New Group. In the New Group popup window, enter a name for the group, a description, and tags, and select or add applications to the group. Click OK.

A dialog box titled "New Group" with a close button (X) in the top right corner. It contains three text input fields labeled "Name*", "Description", and "Tags". Below these fields is a section titled "Applications" which includes a list of application filters. The first filter is "Applications" with a checkbox, and there are icons for adding (+), removing (-), and searching (magnifying glass). Below this is a search bar with a dropdown arrow. The bottom of the dialog box has two buttons: "OK" (green) and "Cancel" (dark blue).

New Group ✕

Name*

Description

Tags

☐ Applications + - 🔍

☐ ▼

OK **Cancel**

23. To add an application filter, Click + New Filter. In the Add Application Filter popup window, enter a name for the filter, select the desired filters, and click OK.

Family

☐ Business-system
 ☐ Collaboration
 ☐ General-Internet

Sub Family

☐ Antivirus
 ☐ Application service
 ☐ Audio_video

Risks

223 1 817 2 1205 3 121 4 167 5

Productivity

225 1 586 2 1582 3 101 4 39 5

Application Tags - Security

☐ Anonymizer
 ☐ Bandwidth
 ☐ Dataleak

Application Tags - SDWAN

☐ Audio_stream
 ☐ Business
 ☐ Cloud

Application Tags - General

☐ News_portal
 ☐ P2p

Name*

Non-Business

Description

Non_business X

Applications	Family	Sub Family	Risks	Productivity	Security	SDWAN	General
01NET	general-inter...	web	2	2		Non_business	Web
050PLUS	media	audio_video	4	2	Dataleak	Audio_stream Non_business	Im_mc Voip
0ZZ0	general-inter...	web	4	2	Filetransfer	Cloud Data Non_business	File_mngt Web
10050NET	general-inter...	web	3	1		Non_business	Web Web_sites
10086CN	general-inter...	web	3	3		Non_business	Web
104COM	general-inter...	web	3	3		Non_business	Web
1111TW	general-inter...	web	3	1		Non_business	Web
114LA	general-inter...	web	3	3		Non_business	Web

OK Cancel

24. To add an application, click + New Application. In the New Application popup window, enter information for the following fields.

New Application

Name*

Description*

Precedence*

Application Timeout (sec)

☐ Application match IPS

Attributes

Match Information

Family	Sub-Family	Risk	Productivity	Application Tags		
				Security	SDWAN	General
<input checked="" type="radio"/> Business-syst...	<input checked="" type="radio"/> Antivirus	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> 1	<input type="checkbox"/> Anonymizer <input type="checkbox"/> Bandwidth <input type="checkbox"/> Dataleak <input type="checkbox"/> Evasive <input type="checkbox"/> Filetransfer <input type="checkbox"/> Malware <input type="checkbox"/> Misused	<input type="checkbox"/> Audio_stream <input type="checkbox"/> Av <input type="checkbox"/> Business <input type="checkbox"/> Cloud <input type="checkbox"/> Data <input type="checkbox"/> Ips <input type="checkbox"/> Non_business	<input type="checkbox"/> Aaa <input type="checkbox"/> Adult_content <input type="checkbox"/> Advertising <input type="checkbox"/> Analytics <input type="checkbox"/> Anonymizer <input type="checkbox"/> Audio_chat <input type="checkbox"/> Basic <input type="checkbox"/> Blog
<input type="radio"/> Collaboration	<input type="radio"/> Application-se...	<input type="radio"/> 2	<input type="radio"/> 2			
<input type="radio"/> General-inter...	<input type="radio"/> Audio_video	<input type="radio"/> 3	<input type="radio"/> 3			
<input type="radio"/> Media	<input type="radio"/> Authentication	<input type="radio"/> 4	<input type="radio"/> 4			
<input type="radio"/> Networking	<input type="radio"/> Behavioral	<input type="radio"/> 5	<input type="radio"/> 5			
	<input type="radio"/> Compression					
	<input type="radio"/> Database					
	<input type="radio"/> Encrypted					

OK Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:09:58 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
Name	Enter a name for the application.
Description	Enter a description for the application.
Precedence	Enter a value for the priority of the application.
Application Timeout	Enter how long to wait before timing out the application, in seconds. <i>Range:</i> 1 through 86400 seconds
App Match IPs	Click to match the IP address of the application.

25. In the Attributes tab, enter information for the following fields.

Field	Description
Family	Select the family to which the application belongs.
Subfamily	Select the subfamily to which the application belongs.
Risk	Select the risk level to assign to the application. A value of 1 indicates the lowest risk level, and a value of 5 indicates the highest.
Productivity	Select a productivity level to assign to the application.
Application Tags	Select one or more security, SD-WAN and general tags to associate with the application.

26. Select the Match Information tab. In the Add Match Information popup window, enter information for the following fields.

Add Match Information
×

Name*

Host Pattern

Protocol Value

Source Address

Destination Address

☐ Source Port

☒ Value
☐ Range

Source Port Value
Low
High

☐ Destination Port

☒ Value
☐ Range

Destination Port Value
Low
High

OK


Cancel

Field	Description
Name	Enter a name for the application match.
Host Pattern	Enter the host pattern to match.
Protocol Value	Enter the application's protocol name or number.
Source Address	Enter the source address of the application.
Destination Address	Enter the destination address of the application.
Source Port (Group of Fields)	Click to match the source ports of the application.
◦ Value or Range	Click to match a single source port of the application.
◦ Range	Click to match a range of source ports of the application.
◦ Source Port Value	Enter the source port number.

Field	Description
◦ Low	For a range of source ports, enter the lowest port number.
◦ High	For a range of source ports, enter the highest port number.
Destination Port (Group of Fields)	Click to match destination ports of the application.
◦ Value	Click to match a single destination port of the application.
◦ Range	Click to match a range of destination ports of the application.
◦ Destination Port Value	Enter the destination port number.
◦ Low	For a range of destination ports, enter the lowest port number.
◦ High	For a range of destination ports, enter the highest port number.

27. Click OK.
28. Select the URL tab to configure match criteria for URL categories. Note that for URL matching to work, you must enable the URL category cache. For more information, see [Configure Application and URL Category Detection Parameters](#), below.

The screenshot shows the 'Add Rules' dialog box with the 'URL' tab selected. Under 'URL Categories', there is a 'URL Category List' with a '+ New URL Category' button at the bottom right. The dialog has tabs for General, Source/Destination, Headers/Schedule, Applications, URL, Users/Groups, Forwarding Class, and Enforce. The URL tab is selected.

29. In URL Category List, click the  Add icon and select a URL category from the drop-down list.
30. To add a URL category, click + New URL Category. In the New URL Category popup window, enter information for the following fields. For more information, see [Configure URL Filtering](#).

New URL Category

Name*

Description

Tags

Confidence

URL File

URL Patterns

URL Strings


Search


1

Pattern	Reputation	
	--Select--	+
NO RECORDS ADDED		

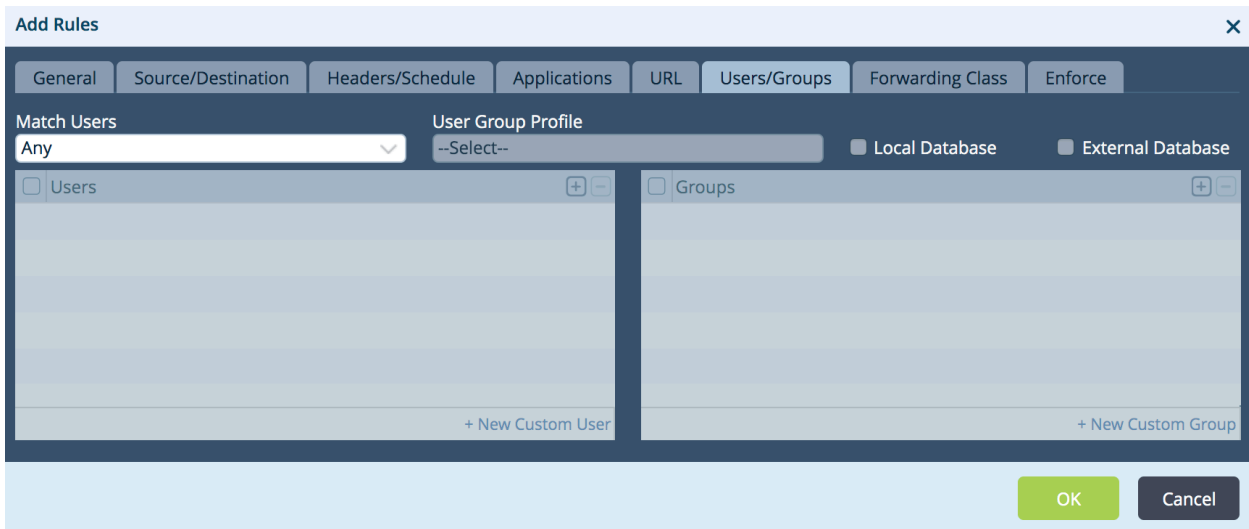
OK

Cancel

Field	Description
Name	Enter a name for the URL category.
Description	Enter a description for the URL category.
Tags	Enter a keyword or phrase that allows you to filter the URL category. This is useful when you have many categories and want to view categories that are tagged with a particular keyword.
Confidence	<p>Enter a confidence value for the URL category. The confidence value is used to break a tie when multiple URL categories match a single URL. If a URL matches multiple categories, the one with the higher confidence value takes precedence.</p> <p><i>Range:</i> 1 through 100</p>
URL File	Select a file that contains URL patterns or strings.
URL Patterns (Tab)	
<ul style="list-style-type: none"> Pattern 	Enter a URL pattern to match a group of URLs. The pattern can include regex patterns. For example, you can enter <code>www.versa-networks.com</code> or <code>*.versa-networks</code> . If you include a backslash (<code>\</code>) in the regex pattern, you must escape it by preceding it with a backslash.
<ul style="list-style-type: none"> Reputation 	<p>Select a reputation to assign to the URL pattern. The following are the predefined URL reputation types, listed in order from lowest to highest risk:</p> <ul style="list-style-type: none"> Trustworthy Low Risk Moderate Risk Suspicious High
<ul style="list-style-type: none">  Add icon 	Click to add the URL pattern to the URL category.

URL Strings (Tab)	
◦ String	Enter a URL string to match a single URL.
◦ Reputation	<p>Select a reputation to assign to the URL string. The following are the predefined URL reputation types, listed in order from lowest to highest risk:</p> <ul style="list-style-type: none"> ◦ Trustworthy ◦ Low Risk ◦ Moderate Risk ◦ Suspicious ◦ High
◦  Add icon	Click to add the URL string to the URL category.

31. Select the Users/Groups tab to define the users and user groups to which the rule applies. Enter information for the following fields.



Add Rules [X]



General Source/Destination Headers/Schedule Applications URL **Users/Groups** Forwarding Class Enforce

Match Users: Any [v] User Group Profile: --Select-- [v] ☐ Local Database ☐ External Database

☐ Users [+ -] ☐ Groups [+ -]

+ New Custom User + New Custom Group

OK Cancel

Field	Description
Match Users	<p>Select the users to match:</p> <ul style="list-style-type: none"> Any—If you select to match any users, you cannot configure any other fields on this tab. Known—If you select to match known users, you cannot configure any other fields on this tab. Selected—If you select to match selected users, you can configure the other fields on this tab. Unknown—If you select to match unknown users, you cannot configure any other fields on this tab.
User Group Profile	If you match selected users, select a user group profile to match users in a group.
Local Database	If you match selected users, click to create a local database to match users and user groups. Select these users and user groups in the Users and Groups fields.
External Database	If you match selected users, click to use an external database to match users and user groups. Select these users in the Users and Groups fields.
Users	If you match selected users, click the  Add icon and select a user from the drop-down list. Select + New Custom User to add a user.
Groups	If you match selected users, click the  Add icon and select a user group from the drop-down list. Select + New Custom Group to add a user group.

32. Select the Forwarding Class tab to choose the forwarding classes and loss priorities to match. Enter information for the following fields.
- Note that in some situations, such as App QoS policy, a forwarding class may not be assigned to a session until the second packet in the session or sometimes until the eighth packet in the session. For this reason, it is recommended that you do not configure a match based on the forwarding class for sessions that consist only of a few packets. Also, do not configure anything on the Forwarding Class tab if you are also configuring DIA or next-hop selection rules in the SD-WAN forwarding profile.

Add Rules

General
Source/Destination
Headers/Schedule
Applications
URL
Users/Groups
Forwarding Class
Enforce

Forwarding Class

Select options

Loss Priority

--Select--

OK
Cancel

Field	Description
Forwarding Class	<p>Select the forwarding class to match:</p> <ul style="list-style-type: none"> Forwarding Class 0 (network control) Forwarding Class 1 Forwarding Class 2 Forwarding Class 3 Forwarding Class 4 (expedited forwarding) Forwarding Class 5 Forwarding Class 6 Forwarding Class 7 Forwarding Class 8 (assured forwarding) Forwarding Class 9 Forwarding Class 10 Forwarding Class 11 Forwarding Class 12 (best effort) Forwarding Class 13 Forwarding Class 14 Forwarding Class 15
Loss Priority	<p>Select the loss priority to assign to the forwarding class:</p> <ul style="list-style-type: none"> High—Traffic has a greater likelihood of being dropped. Low—Traffic has a lesser likelihood of being dropped.

33. Select the Enforce tab to select the actions to take on matching packets, including applying a forwarding and a logging profile and defining monitor parameters. Enter information for the following fields.

Add Rules

General
Source/Destination
Headers/Schedule
Applications
URL
Users/Groups
Forwarding Class
Enforce

Forwarding

Action *

Allow Flow

Forwarding Profile

--Select--

Nextthop IP address

IP Address

Routing Instance

--Select--

☐ Enable Symmetric Forwarding of Return Traffic

☐ Enable Symmetric L2 Forwarding of Return Traffic

Monitor

Address

IP Address

Routing Instance

--Select--

Action

--Select--

Interval(sec)

3

Threshold(Events)

5

Logging

LEF Profile

--Select--

☐ Default Profile

Event

Never

Rate Limit

10

TCP Optimization

Bypass Latency Threshold (msec)

Mode

--Select--

Lan Profile

--Select--

Wan Profile

--Select--

OK
Cancel

Field	Description
Forwarding (Group of Fields)	
<ul style="list-style-type: none"> Action 	<p>Select the action to take on matching traffic:</p> <ul style="list-style-type: none"> Allow Flow Deny Flow
<ul style="list-style-type: none"> Forwarding Profile 	<p>Select the forwarding profile to apply to matching traffic.</p>
<ul style="list-style-type: none"> Next-Hop IP Address 	<p>Enter the IP address of the next hop to which to forward the flow. Using a next hop statically assigns the next hop instead of using dynamic routing.</p>
<ul style="list-style-type: none"> Routing Instance 	<p>Select the routing instance to reach the next hop.</p>
<ul style="list-style-type: none"> Enable Symmetric Forwarding of Return Traffic 	<p>Click to enable symmetric forwarding of return traffic. With this option, after a route lookup is performed, the reverse traffic flow transits through the same interface on which the flow was received. To effect symmetric forwarding, the VOS software records the (tunnel) interface on which the forward-direction traffic for the session arrives and places the reverse-direction traffic on that same tunnel interface. You do not need to install any static routes to make this happen. You can configure an SD-WAN or a policy-based forwarding (PBF) policy rule to subject the reverse direction traffic to a stateful Layer 3 return.</p> <p>You should use this option to enforce symmetric traffic return only over a non-SD-WAN VPN tunnel (for example, a paired TVI tunnel, GRE tunnel, or IPsec tunnel). You should not use this option to enforce symmetric traffic return over SD-WAN VPN tunnels, that is, to send traffic back to the same branch, over the same SD-WAN path on which the forward direction traffic arrived. Instead, you should use the symmetric forwarding option in the SD-WAN forwarding profile.</p> <p>The following are a few examples of when symmetric forwarding of return traffic might be useful:</p>

	<ul style="list-style-type: none"> ◦ You want to do application-based DIA. You do this by creating the appropriate PBF or SD-WAN rule in the LAN VR to send forward-direction traffic for the application session (say S1) over a paired TVI/split tunnel into the transport VR. Here, a second session, S2, is created and traffic is source-NATed before it is transmitted on the WAN interface. One way for the reverse-direction traffic of session S2 to get back to the LAN VR is to use routing (VOS Workflows set up BGP between the LAN and transport VR, or you can use static routes). This works fine except if you have multiple LAN VRs with overlapping address spaces. In this case, you can create a second PBF rule to match the traffic coming into the transport VR over the WAN side of the split tunnel (for example, "match source zone w-st-lan-internet") and statefully send reverse-direction traffic for S2 back over the tunnel without requiring a route. ◦ You want to selectively divert some internet-bound traffic to a cloud security device, such as a Zscaler, over an IPsec or a GRE tunnel. You may place this tunnel in a different routing instance (such as a Zscaler VR) and send traffic to it over a split tunnel to that routing instance, from where it can reach the Zscaler VR over the IPsec or GRE tunnel. Again, the reverse-direction traffic (traffic coming back from the Zscaler VR) either needs a route to get to the LAN or you can configure a PBF rule that includes the enforce symmetric forwarding option.
<ul style="list-style-type: none"> ◦ Enable Symmetric Layer 2 Forwarding of Return Traffic 	<p>Click to enable symmetric Layer 2 forwarding of return traffic. With this option, no route lookup is performed, and the reverse traffic flow transits through the same interface on which the flow was received and is sent to the same MAC address from which the traffic was received. You can configure an SD-WAN or a PBF policy rule to subject the reverse direction traffic to a stateful Layer 2 return.</p> <p>Click to enable stateful layer 2 forwarding of reverse-direction traffic to the same MAC address from which the forward-direction traffic is received. This is an advanced configuration for SD-WAN or PBF policy rules and is applicable to a very specific use case; you</p>

	<p>must not enable it in any other use case. Specifically, you enable it when forward-direction traffic is sourced from a Layer 2 adjacent service function, such as a WAN optimization device, that spoofs the client IP address. Normally, for such traffic, the reverse-direction traffic must also be diverted back to the same function. However, regular routing-based forwarding prevents this from happening: the traffic is forwarded wherever the route lookup points to. To enable route-less forwarding of reverse-direction traffic to the same function, you create an SD-WAN or PBF rule that matches the forward-direction traffic and for which you select the Enable Symmetric Layer 2 Forwarding of Return Traffic option.</p>
Logging (Group of Fields)	Log changes in the forwarding action.
<ul style="list-style-type: none"> LEF Profile 	<p>Select a LEF profile. Logs are sent to the active collector of the LEF profile. For information about configuring a LEF profile, see Configure Log Export Functionality. For information about associating a LEF profile with a feature or service, see Apply Log Export Functionality.</p>
<ul style="list-style-type: none"> Default Profile 	<p>Click to use the default LEF profile instead of the LEF profile from the previous field. For information about configuring a default LEF profile, see Configure Log Export Functionality.</p>
<ul style="list-style-type: none"> Event 	<p>Select the events to log:</p> <ul style="list-style-type: none"> All SLA Violated—Generate a log when the session moves to or from an SLA-violated circuit. Never—Never log changes. This is the default. Priority Change—Generate a log when the session moves between circuits of different priorities. <p><i>Default:</i> Never</p>
<ul style="list-style-type: none"> Rate Limit 	<p>Enter the number of logs to generate per second. You should configure a rate limit when changes happen constantly, to buffer all changes logged during the specified interval and send them together in a single message.</p>

Monitor (Group of Fields)	Enter Monitor information when you specify a next-hop IP address in the forwarding Action. In the fields in this section, specify the parameters to monitor and the actions to take if the monitoring fails.
◦ Address	Enter the IP address to monitor using ICMP probes.
◦ Action	<p>Select the monitoring action to take:</p> <ul style="list-style-type: none"> ◦ Failover—Route traffic and do not implement the SD-WAN traffic policy. A route lookup is performed to determine the Layer 3 destination IP address. ◦ Next-Rule—Evaluate the other rules until a match is found. If no match is found, route the traffic. ◦ Wait-Recover—Drop traffic until the next hop recovers.
◦ Threshold (Events)	Enter the number of successive ICMP ping failures after which the next hop is considered down.
◦ Routing Instance	Select the routing instance to use or the VRF in which you want to run the monitor.
◦ Interval	Enter how often to send ICMP probes, in seconds.
TCP Optimization (Group of Fields)	
◦ Bypass Latency Threshold	<p>Enter how much latency must be measured before TCP optimizations begin.</p> <p><i>Range:</i> 0 through 60000 milliseconds</p> <p><i>Default:</i> 10 milliseconds</p>
◦ Mode	<p>Select a TCP optimization mode:</p> <ul style="list-style-type: none"> ◦ Auto ◦ Bypass—Disable TCP optimizations. ◦ Forward proxy ◦ Proxy ◦ Reverse proxy ◦ Splice

<ul style="list-style-type: none"> ◦ LAN Profile 	<p>Select a LAN profile.</p> <p>If you select proxy mode, you must configure a TCP profile.</p> <p>If you do not select a TCP profile, a system default LAN profile is applied that uses the cubic congestion control algorithm and duplicate ACK loss detection.</p>
<ul style="list-style-type: none"> ◦ WAN Profile 	<p>Select a WAN profile.</p> <p>If you select proxy mode, you must configure a TCP profile.</p> <p>If you do not select a TCP profile, a system default WAN profile is applied that uses the BBR congestion control algorithm and RACK loss detection.</p>

34. Click OK.

Configure Application and URL Category Detection Parameters

For Layer 3 SD-WAN policy, application and URL-category detection allow an SD-WAN traffic-steering policy to correctly process all traffic in a flow. These two detection systems are always running on a VOS device.

Application and URL-category detection inspect the Layer 7 (application) payload. However, most applications other than basic ones such as ICMP and DNS are identified only after a few packets for the session have been received. Because SD-WAN policies are often used to override route table-based routing and divert the traffic to a different path, the application must be identified correctly on the first packet instead of after a few packets so that the SD-WAN policy is applied to all packets in the flow. The rapid identification is made possible by having application and URL category caches, which are used to identify the application in the first packet, instead of waiting for the application identification engine to do so.

By default, application caching is enabled.


To configure application and URL detection parameters:

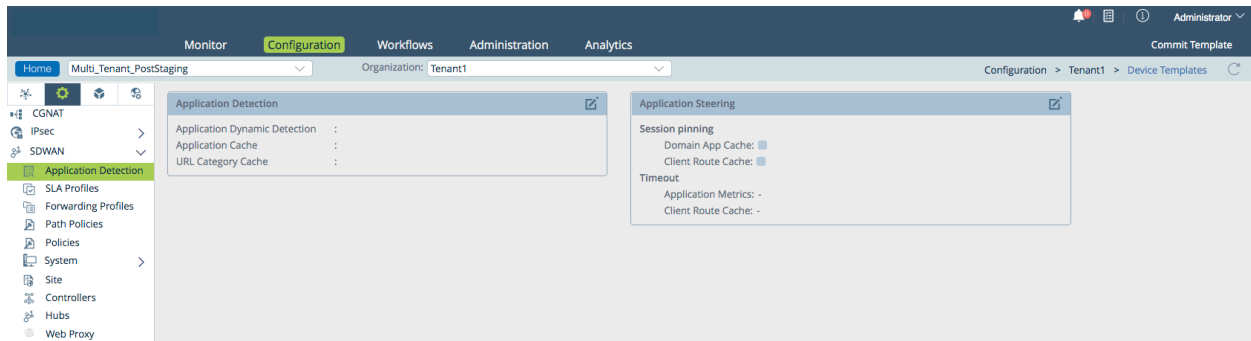
1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.


https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

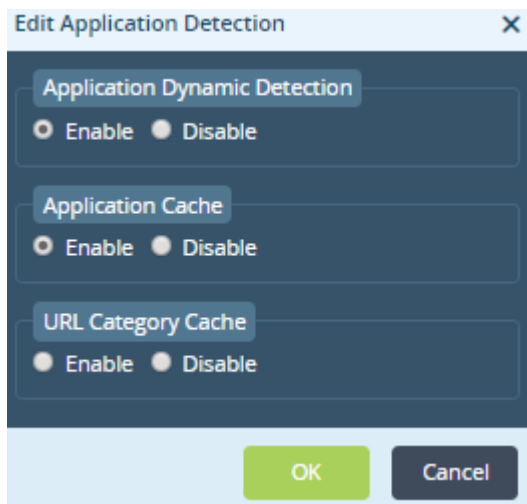
Updated: Wed, 23 Oct 2024 08:09:58 GMT

Copyright © 2024, Versa Networks, Inc.


2. Select the Configuration tab in the top menu bar.
3. Select Services  > SD-WAN > Application Detection in the left menu bar. The main pane displays the Application Detection and Application Steering panes.

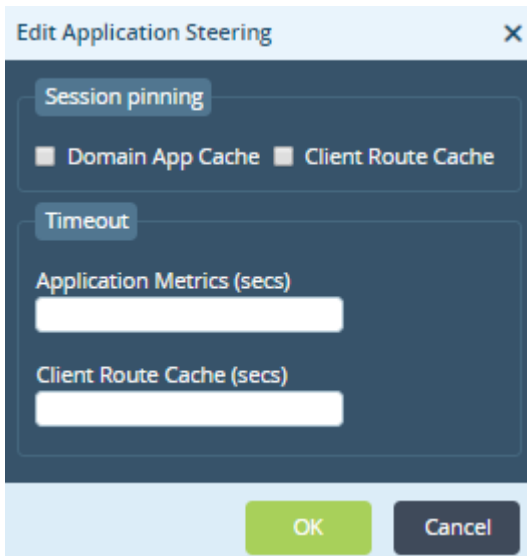


4. Click the  Edit icon in the Application Detection pane. In the Edit Application Detection popup window, enter information for the following fields.



Field	Description
Application Dynamic Detection	Click Enable to dynamically re-evaluate SD-WAN traffic-steering rules when an application or URL category is detected in a traffic flow even if the packet being inspected is not the first packet in the flow. <i>Default:</i> Enabled
Application Cache	Click Enable to cache applications associated with server IP address and port numbers. <i>Default:</i> Enabled
URL Category Cache	Click Enable to cache URL categories associated with HTTP and HTTPS server IP addresses and port numbers. <i>Default:</i> Disabled

- Click OK.
- Click the  Edit icon in the Application Steering pane. In the Edit Application Steering popup window, enter information for the following fields.



Edit Application Steering [X]

Session pinning

☐ Domain App Cache ☐ Client Route Cache

Timeout

Application Metrics (secs)

Client Route Cache (secs)

OK Cancel

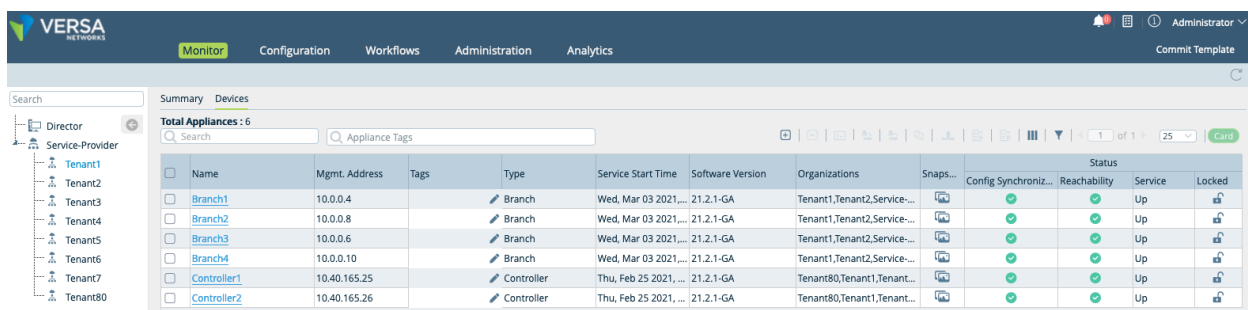
Field	Description
Session Pinning (Group of Fields)	Configure path affinity.
<ul style="list-style-type: none"> Domain Application Cache 	Click to pin subsequent sessions of an SaaS application transaction to the path used by the DNS query.
<ul style="list-style-type: none"> Client Route Cache 	Click to pin all consecutive sessions of a SaaS application transaction between a specific client and server to the same path.
Timeout (Group of Fields)	Configure the timeout period for session pinning.
<ul style="list-style-type: none"> Application Metrics 	<p>Enter the maximum time, in seconds, that a link with the worst metric has to wait before trying again.</p> <p><i>Default: 300 seconds</i></p>
<ul style="list-style-type: none"> Client Route Cache 	<p>Enter the maximum time, in seconds, that sessions between a host and client remain pinned to the same link.</p> <p><i>Default: 30 seconds</i></p>

7. Click OK.

Verify the SD-WAN Policy Configuration

To verify the SD-WAN policy configuration:

1. In Director view, select the Monitor tab in the top menu bar.
2. Select the organization in the left navigation panel.
3. Select the Devices tab in the horizontal menu bar.



4. Select a device in the main pane. The view changes to Appliance view.

5. To view the Layer 2 SD-WAN policy configuration:
 - a. In the Services tab, select SD-LAN.
 - b. Select the Policies tab.

Rule Name	Hit Count	Tx Pkts Tunnel	Tx Bytes Tunnel	Rx Pkts Tunnel	Rx Bytes Tunnel
Rule1	0	0	0	0	0

- c. Click the policy name to view the policy configuration.

```

{
  - sdwan:rule: {
    name: "Rule1",
    rule-disable: false,
    - match: {
      - source: {
        - zone: {
          - zone-list: [
            "L2-zone1"
          ]
        },
        - user: {
          - local-database: {
            status: "disabled"
          },
          - external-database: {
            status: "disabled"
          },
          user-type: "any"
        }
      },
      - vlan-id: {
        - vlan-id-list: [
          "vlan-1001"
        ]
      }
    },
    - set: {
  
```

6. To view the Layer 3 SD-WAN policy configuration:
 - a. In the Services tab, select SD-WAN.
 - b. Select the Policies tab.
 - c. Click the policy name to view the policy configuration.

Supported Software Information

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

- Release 21.2.1 adds support for configuring Layer 2 SD-WAN policy and for configuring rule order and matching based on the destination zone.
- Release 22.1.3 adds support for configuring a dynamic source address object.

Additional Information

[Apply Log Export Functionality](#)

[Configure Address Objects](#)

[Configure CoS](#)

[Configure Layer 2 Services](#)

[Configure Log Export Functionality](#)

[Configure MOS Score Monitoring](#)

[Configure NGFW](#)

[Configure Policy-Based Forwarding](#)

[Configure SD-WAN Traffic Steering](#)

[Configure SLA Profiles for SD-WAN Traffic Steering](#)

[Configure URL Filtering](#)

[Configure User and Group Policy](#)