

---

## Configure Policy-Based Forwarding

 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 policy to enable policy-based forwarding (PBF).

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 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.

When a policy that contains multiple rules is evaluated, the rules are evaluated in the order in which they are listed in the policy. When a rule matches, the action in that rule is applied to the traffic, and no further rules in the policy are evaluated.

To correctly process all traffic in an application flow, the PBF policy 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 PBF policy, you do the following:

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

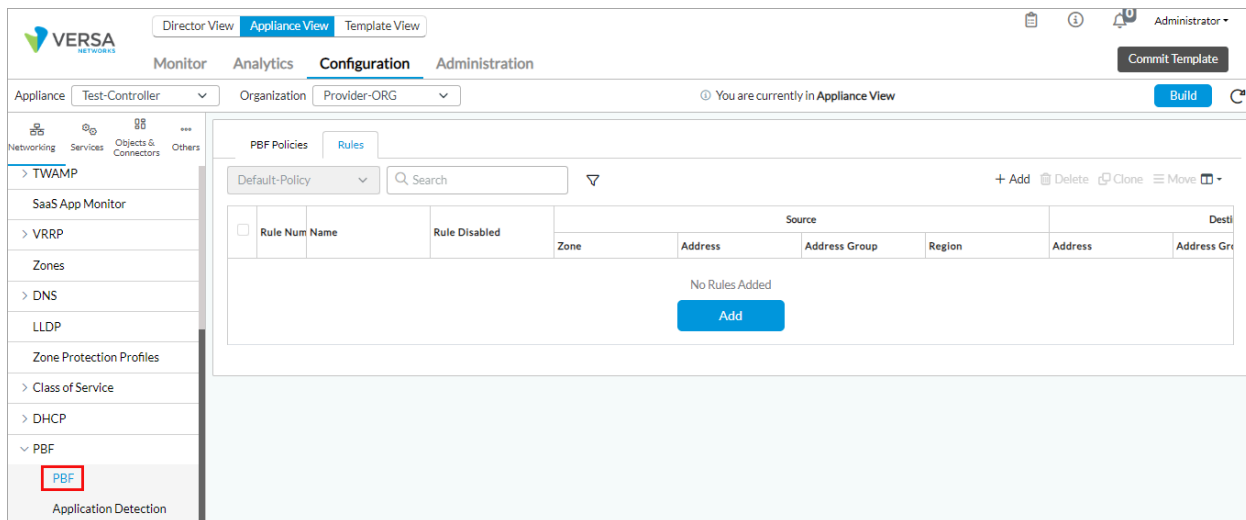
---

## Define a Policy Name

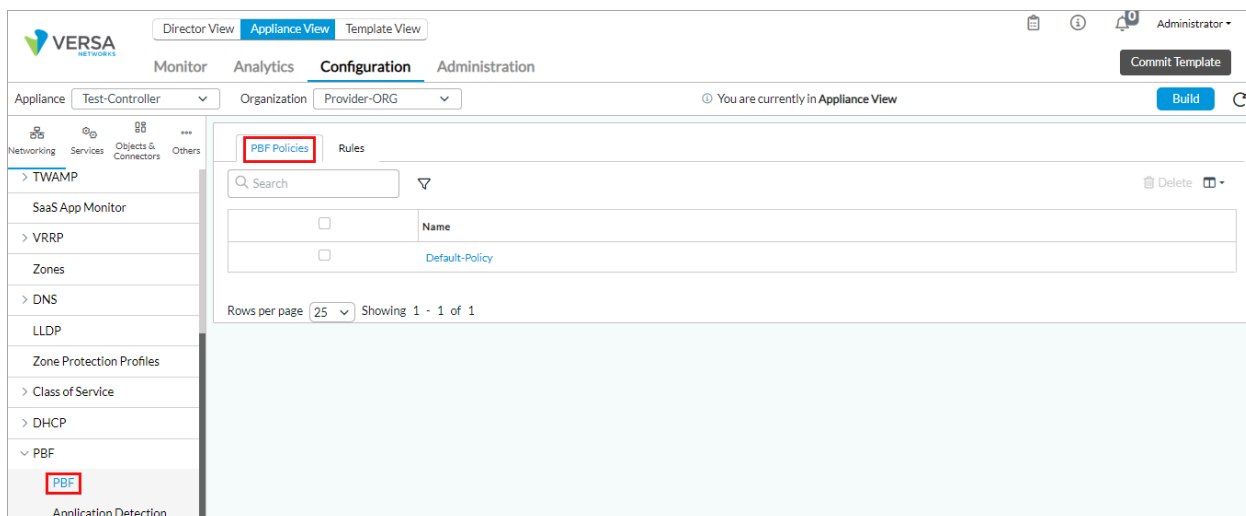
To configure a policy, you first name the policy. Currently, each template can have only one PBF policy, and this policy is called Default-Policy. If desired, you can add a description for the policy, but you cannot rename it.

To add a description to the policy name:

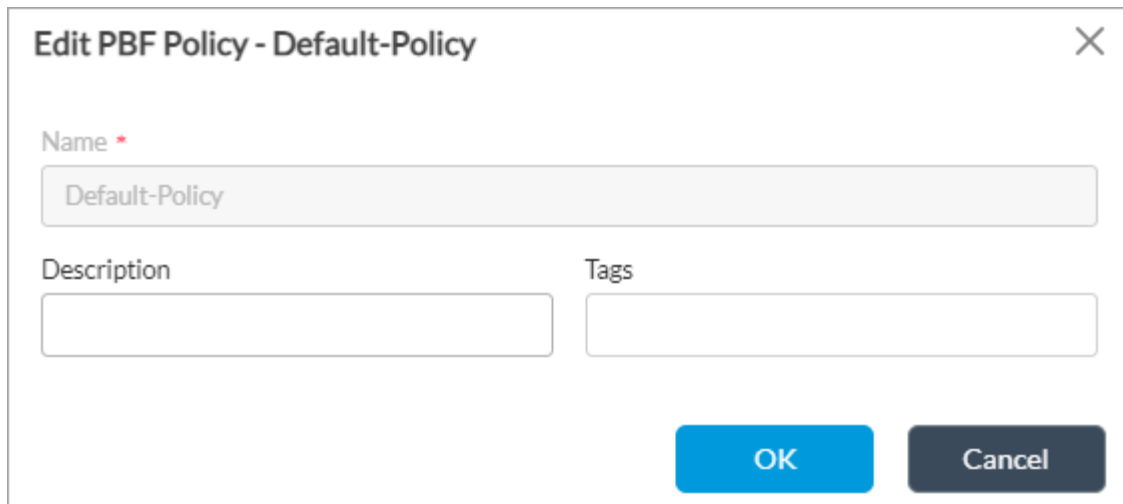
1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization from the left menu bar.
  - d. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > PBF > PBF in the left menu bar. The main pane displays a table of configure policy-based forwarding rules.



4. Select the PBF Policies tab in the horizontal menu bar.



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



7. Click OK.

---

## Configure Policy Rules

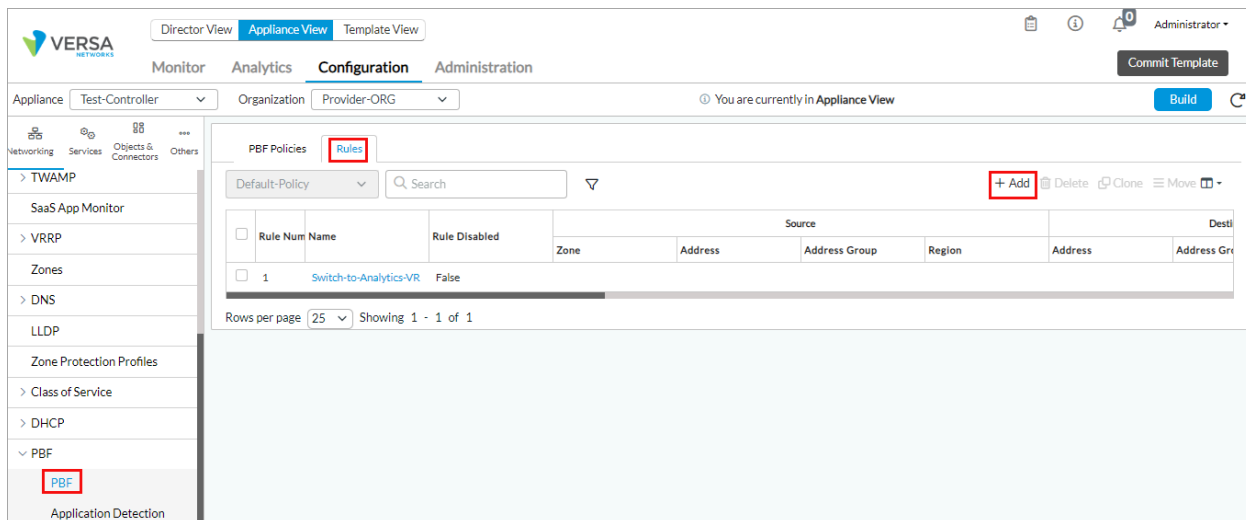
In policy rules, you configure the conditions for matching packets of interest, and you also configure the forwarding, logging, and monitoring actions to take on the packets that match the conditions. To configure policy rules, you select an organization (that is, a tenant), and then you perform the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

- Navigate to the rules configuration screen (Steps 1 through 3).
- Reorder existing rules (Step 4)
- Configure a rule name (Steps 5 and 6).
- Configure match conditions:
  - Configure address, site, and zone match criteria (Steps 7 through 14).
  - Configure match criteria based on the contents of the IP packet header and to set a time at which to apply the policy (Step 15).
  - Configure match criteria for URL categories (Steps 16 through 21).
  - Define the users and user groups to which the rule applies (Step 22).
- Select the actions to take on matching packets, including applying a forwarding and a logging profile and defining monitor parameters (Step 23).

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 Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left navigation bar.
  - d. Select a device in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > PBF > PBF 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.



4. Click + Add.
5. (For Releases 22.1.1 and later.) If you have already added a rule, the Add popup window displays.
  - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rule.

Add

☒ Insert the rule last

☐ Insert the rule top

Search Rule

1. Switch-to-Analytics-VR

End of records

OK

Cancel

- b. If there are two or more rules, you can drag the line with the Place Here text to insert the rule where required.

**Add**

☐ Insert the rule last  
☐ Insert the rule top  
☒ Insert the rule in specific placement

Search Rule

1. Switch-to-Analytics-VR

2. PBF-1

End of records

Place Here

OK Cancel

- c. Click OK. The Add Rules popup window displays.
6. (For Releases 21.2.1 and later.) 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.

**Configure Rule Order**

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

☒ Insert At Bottom  
☐ Insert At Top

Ok

- 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

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

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

Name \*

Description
Tags

☐ Disable Rule

OK
Cancel

7. In the General tab, enter information for the following fields.

Field	Description
Name	Enter a name for the policy rule.
Description	Enter a text description for the policy.
Tags	Enter a keyword or phrase that allows you to filter the rule name. This is useful when you have many rules and want to view those that are tagged with a particular keyword.
Disable Rule	Click to disable the rule. You can disable a rule to skip it from evaluating traffic and to use other rules in the policy in the configuration order.

8. Select the Source tab to configure matching criteria based on source addresses and source zone.

**Add Rules** [Close]

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

☐ **Source Zone** + New Zone + [trash] [refresh]  
Source Zone Not Configured

☐ **Source Address** + New Address + New Address Group + [trash] [refresh]  
Source Address Not Configured

☐ **Custom Geo Circle** + [trash] [refresh]  
Custom Geo Circle Not Configured

☐ **Region** + [trash] [refresh]  
Region Not Configured

☐ **EIP Profile** + [trash] [refresh]  
EIP Profiles Not Configured

☐ **State** + [trash] [refresh]  
State Not Configured

☐ **City** + [trash] [refresh]  
City Not Configured

Routing Instance  
--Select--

☐ Source Address Negate
☐ Source Location Negate

**OK** **Cancel**

9. 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](#).
10. Click + New Zone to add a zone. In the Add Zone popup window, enter information for the following fields.



Add Zone

×

Name \*

Description

Tags

Zone Protection Profile

--Select--

+ Create Zone Protection Profile

Log Profile

--Select--

+ Create Log Profile

Organization

Routing Instance

Interface and Networks

Organization

--Select--

Routing Instance

--Select--

Networks

Networks Not Configured

Interfaces

Interfaces Not Configured

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. For more information, see <a href="#">Configure Zones and Zone Protection Profiles</a> .
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.
Routing Instance	Click to specify the routing instances that are in the zone. In the Routing Instance pane, select the routing instances. Click the + Add icon to add routing instances.
Organization	Click to specify the organizations (tenants) that are in the zone. In the Organization pane, select the organizations. Click the + Add icon to add organizations.
OK	Click OK.

11. 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.
12. 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

Add a tag

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"> <li>IPv4 (type); IPv4 Address/Prefix (match)</li> </ul>	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"> <li>IPv4 Wildcard Mask (type); IPv4 Wildcard Mask (match)</li> </ul>	<div data-bbox="857 919 1624 1346"> <p><b>Add Address</b></p> <p>Name *</p> <input type="text"/> <p>Description <input type="text"/></p> <p>Tags <input type="text" value="Add a tag"/></p> <p>Type *</p> <div> <div>IPv4 Wildcard Mask</div> <div>▼</div> </div> <p>IPv4 Wildcard Mask *</p> <input type="text"/> <p>OK</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 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</p>



<ul style="list-style-type: none"> <li>◦ IPv6 Address/Prefix (type); IPv6 Address/Prefix (range)</li> </ul>	<div data-bbox="857 210 1624 636"> <h3>Add Address</h3> <p>Name *</p> <input type="text"/> <p>Description <span>Tags</span></p> <input type="text"/> <input type="text" value="Add a tag"/> <p>Type * <span>IPv6 Address/Prefix *</span></p> <div> <span>IPv6 Address/Prefix</span> <span>▼</span> <input type="text"/> </div> <p>OK</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"> <li>◦ FQDN (type); FQDN (match)</li> </ul>	<div data-bbox="857 879 1624 1306"> <h3>Add Address</h3> <p>Name *</p> <input type="text"/> <p>Description <span>Tags</span></p> <input type="text"/> <input type="text" value="Add a tag"/> <p>Type * <span>FQDN *</span></p> <div> <span>FQDN</span> <span>▼</span> <input type="text"/> </div> <p>OK</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"> <li>◦ Dynamic Address (type); no range</li> </ul>	<div data-bbox="857 210 1624 634"> <p><b>Add Address</b></p> <p>Name *</p> <input type="text"/> </div> <div data-bbox="873 373 1315 441"> <p>Description</p> <input type="text"/> </div> <div data-bbox="1338 373 1624 441"> <p>Tags</p> <input type="text" value="Add a tag"/> </div> <div data-bbox="873 470 1315 537"> <p>Type *</p> <div>Dynamic Address ▼</div> </div> <div data-bbox="1539 588 1624 630"> <p>OK</p> </div>
--	--

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

Add Address Groups

✕

Name \*

Description

Tags

Add Tag

Type

Static

▼

Address ↕

Select Option

▼

+

No Records to Display

+ Address

Address File ↕

Select Option

▼

+

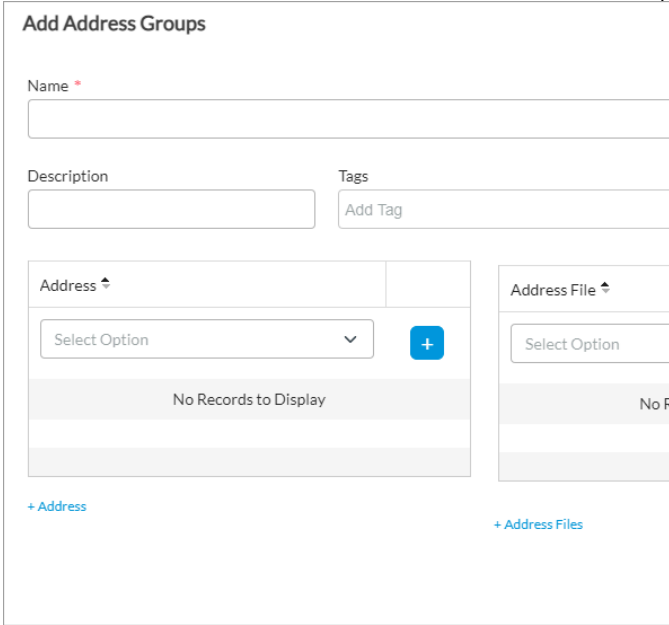

No Records to Display


+ Address Files

OK

Cancel



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.
Type	<p>(For Releases 22.1.1 and later.) Select the address type for the group:</p> <ul style="list-style-type: none"> <li>Static (default)</li> <li>Dynamic</li> </ul> <p>If you select Static, the following fields display in the lower part of the screen:</p>  <p> <ul style="list-style-type: none"> <li>Address—Click the  icon to select IP addresses to add to the address group object. Click +New Address to add a new address object. For more information, see <a href="#">Configure Address Objects</a>, above.</li> </ul> </p>

- Address File—Click the  icon to select an address file. For more information about uploading address files, see [Upload Address Files](#), above.

Select Dynamic to add dynamic IP addresses address for cloud resources. The following screen displays:

**Add Address Groups**

Name <sup>\*</sup>

Description Tags Type

Add Tag Dyn

**Match Terms (OR)**

<input type="checkbox"/>	Name	Tags (AND)	Action
No Record Added			

OK

(For Releases 22.1.1 and later.) Click + Add in the Match Terms (OR) section to add matching terms. The Add Match Terms (OR) screen displays.

**Add Match Terms (OR)**

Name <sup>\*</sup>

Match-Term-1

Tags (AND)

Add Tag

OK

- Match Term—Enter a name for the match term.

	<p>The term Match Term displays by default followed by the serial number of the match term, which you can edit. For example, the first match term name display as Match-Term-1.</p> <ul style="list-style-type: none"> <li>Tags (AND)—If cloud workload protection (CWP) is enabled for the CMS connector, this field displays the tags for the cloud service provider associated with CMS connector. You can select the necessary tag. If cloud resource tags are not displayed, you can enter custom tags. For more information, see <a href="#">Add a CMS Connector in Install on Google Cloud Platform</a>.</li> </ul>
--	--

15. Click OK.
16. Click + Add next to Custom Geo Circle, Region, State, and City to select geolocation objects.
17. Click + Add next to EIP Profile to select one or more user-defined or predefined EIP profiles, and then click the + Add icon to associate EIP with the rule. With EIPs, you collect information about the security status of the endpoint devices connecting to your networks, such as whether they have the latest security patches and antivirus definitions installed. For more information, see [Configure Endpoint Information Profiles](#).
18. Click Source Address Negate below the Source Address pane to block traffic to the selected source addresses instead of accepting it. The negation action provides a way to fine-tune which specific source addresses to block. A rule with a negation action is like any other rule. If a session matches the rule, the block action is applied to the traffic, and no further rules in the policy are evaluated.  
In a situation where you want to omit one source IP address out of an entire subnet so that it is not routed by PBF, you can do this without creating a negation rule. Instead, you create two sequential policy rules. In the first rule, you match the address that you do not want the policy to apply to and set the action to Allow, and in the second rule, you match the entire subnet. The result is that a session with this IP address matches the first rule and no action is taken on it, and it is forwarded using normal route lookup. In the second rule, you match the entire subnet. Suppose the source address you want to omit from PBF routing is 1.2.3.4. The first rule would match and allow this source address, and then policy evaluation would stop. Other source addresses in the subnet do not match the first rule, and so they are evaluated by the second rule, which applies PBF actions.
19. Select Destination tab and enter information in the same way as for the Source Address pane, as described in Steps 9 through 18.

Add Rules

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

☐
Destination Zone
+ New Zone
+

Destination Zone Not Configured

☐
Destination Address
+ New Address
+ New Address Group
+

Destination Address Not Configured

☐
Custom Geo Circle
+

Custom Geo Circle Not Configured

☐
Region
+

Region Not Configured

☐
State
+

State Not Configured

☐
City
+

City Not Configured

☐ Destination Address Negate
☐ Destination Location Negate

OK
Cancel

20. Select the Headers/Schedule tab to configure the matching 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

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

TTL

Condition

--Select--

Value (Max 255)

1 .. 255

Services


Service List

+ New Service

Service List Not Configured

OK

Cancel

Field	Description
IP (Group of Fields)	
<ul style="list-style-type: none"> <li>IP Version</li> </ul>	<p>Select the IP version:</p> <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> </ul>
<ul style="list-style-type: none"> <li>IP Flags</li> </ul>	<p>Select whether routers can fragment data packets:</p> <ul style="list-style-type: none"> <li>Don't Fragment</li> <li>More Fragments</li> </ul>
<ul style="list-style-type: none"> <li>DSCP</li> </ul>	<p>Click the  Add icon to add a differentiated services code point (DSCP) value.</p>
TTL (Group of Fields)	
<ul style="list-style-type: none"> <li>Condition</li> </ul>	<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"> <li>Equal to—TTL value must be equal to the specified value to trigger the security access rule</li> <li>Greater than or equal to—TTL value must be greater than or equal to the specified value to trigger the security access rule</li> <li>Less than or equal to—TTL value must be less than or equal to the specified value to trigger the security access rule</li> </ul>
<ul style="list-style-type: none"> <li>Value</li> </ul>	<p>Enter the value for the TTL.</p>
Others (Group of Fields)	
<ul style="list-style-type: none"> <li>Schedules</li> </ul>	<p>Select a schedule to set the time and frequency at which the rule is in effect.</p>
Services (Group of Fields)	
<ul style="list-style-type: none"> <li>Service List</li> </ul>	<p>Select the services to allow or block. Click the + Add icon to select a service. The list includes predefined and user-defined services. A service is defined based</p>

	on the destination address and port.
<ul style="list-style-type: none"> <li>+ New Service</li> </ul>	<p>Click to create a service. In the Add Service popup window, enter information for the following fields.</p> <div data-bbox="857 340 1624 1087"> <p><b>Add Service</b></p> <p>Name *</p> <p>Description Tags</p> <p><input type="radio"/> Protocol <input type="radio"/> Protocol Value</p> <p>Protocol * Protocol Value</p> <p>TCP 0..255</p> <p><input type="radio"/> Port Range <input checked="" type="radio"/> Source/Destination Port <input type="radio"/> ICMP</p> <p>Port <input type="text"/> Source Port Destination Port ICMP Type ICMP Code</p> <p>Use /- for values/ranges</p> <p>OK Cancel</p> </div> <ul style="list-style-type: none"> <li>Name—Enter a name for the service.</li> <li>Description—Enter a description for the service.</li> <li>Tags—Enter a keyword or phrase that allows you to filter the service name.</li> <li>Protocol—Click and enter a protocol name in the second Protocol field.</li> <li>Protocol Value—Click and enter a protocol number in the second Protocol Value field.</li> <li>Port—Click and in the second Port field, enter a source or destination port number.</li> <li>Source/Destination—Click and enter a port number in the Source Port and Destination Port fields.</li> <li>(For Releases 22.1.1 and later.) If you select the ICMP or ICMPv6 protocol, click to define a custom service object by ICMP values:             <ul style="list-style-type: none"> <li>ICMP Code—Enter the ICMP code. You can</li> </ul> </li> </ul>

	<p>enter an individual value, a comma-separated list of values, or a range of values.</p> <ul style="list-style-type: none"> <li>▪ ICMP Type—Enter the ICMP type. You can enter an individual value, a comma-separated list of values, or a value range of values (for example, 9-12).</li> </ul> <p>Then, click OK.</p>
--	--

21. Select the Applications/URL tab to select traffic based on the source applications.

The screenshot shows the 'Add Rules' dialog box with the 'Applications/URL' tab selected. The dialog has a title bar with a close button (X). Below the title bar are tabs: General, Source, Destination, Headers/Schedule, Applications/URL (selected), Users/Groups, and Enforce. The main content area is divided into two sections: 'Applications' and 'URL Categories'. Each section has a checkbox, a label, and a row of action buttons. In the 'Applications' section, the checkbox is unchecked, the label is 'Application List', and the buttons are '+ New Application', '+ New Group', '+', and a trash icon. Below this is a message 'Application List Not Configured'. In the 'URL Categories' section, the checkbox is unchecked, the label is 'URL Category List', and the buttons are '+ Add URL Category', '+', and a trash icon. Below this is a message 'URL Category List Not Configured'. At the bottom right are 'OK' and 'Cancel' buttons.

22. In the Applications table, click the + Add icon and select an application list. The list includes predefined and user-defined applications. For more information about predefined and user-defined applications, see [Configure NGFW](#).
23. Click + New Group to add an application 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.



New Group

Name \*

Description

Tags

Applications \*

+

Applications Not Configured

OK

Cancel

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

New Application

Name \*

Description \*

Precedence \*

Application Timeout (seconds)

☐ Application match based on IPS signature

Attributes | Match Information

Family	Sub Family	Risk	Productivity	Application Tags		
				Security	SDWAN	General
<input checked="" type="radio"/> Business-system <input type="radio"/> Collaboration <input type="radio"/> General-internet <input type="radio"/> Media <input type="radio"/> Networking	<input checked="" type="radio"/> Antivirus <input type="radio"/> Application-service <input type="radio"/> Audio_video <input type="radio"/> Authentication <input type="radio"/> Behavioral <input type="radio"/> Compression <input type="radio"/> Database <input type="radio"/> Encrypted <input type="radio"/> Encrypted-tunnel <input type="radio"/> ERP <input type="radio"/> File-server <input type="radio"/> File-transfer <input type="radio"/> Forum <input type="radio"/> Game <input type="radio"/> Instant-messaging <input type="radio"/> Internet-utility <input type="radio"/> Mail <input type="radio"/> Microsoft-office <input type="radio"/> Middleware <input type="radio"/> Network-management <input type="radio"/> Network-service <input type="radio"/> Peer-to-peer <input type="radio"/> Printer <input type="radio"/> Routing <input type="radio"/> Security-service <input type="radio"/> Standard <input type="radio"/> Telephony <input type="radio"/> Terminal <input type="radio"/> Thin-client <input type="radio"/> Tunneling <input type="radio"/> Unknown <input type="radio"/> VAP <input type="radio"/> Web <input type="radio"/> Webmail	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5	<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"/> Tunnel <input type="checkbox"/> Vulnerable	<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"/> Video_stream	<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="checkbox"/> CDN <input type="checkbox"/> Chat <input type="checkbox"/> Classified_Ads <input type="checkbox"/> Cloud_services <input type="checkbox"/> DB <input type="checkbox"/> DEA_Mail <input type="checkbox"/> EBook_Reader <input type="checkbox"/> Email <input type="checkbox"/> Enterprise <input type="checkbox"/> File_mngt <input type="checkbox"/> File_transfer <input type="checkbox"/> Forum <input type="checkbox"/> Gaming <input type="checkbox"/> IM_MC <input type="checkbox"/> IoT <input type="checkbox"/> MM_streaming <input type="checkbox"/> Mobile <input type="checkbox"/> Networking <input type="checkbox"/> News_portal <input type="checkbox"/> P2P <input type="checkbox"/> Remote_access <input type="checkbox"/> SCADA <input type="checkbox"/> Social_network <input type="checkbox"/> Standardized <input type="checkbox"/> Transportation <input type="checkbox"/> Update <input type="checkbox"/> Video_chat <input type="checkbox"/> VoIP <input type="checkbox"/> VPN_tun <input type="checkbox"/> Web <input type="checkbox"/> Web_Ecom <input type="checkbox"/> Web_search <input type="checkbox"/> Web_sites <input type="checkbox"/> Webmail

OK

Cancel

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: 1 through 86400 seconds</i>
Application Match Based on IPS Signature	Click to match the IP address of the application.

25. In the URL Categories table, click the + Add icon and select a URL category.
26. Click + New URL Category to add a URL category. In the Add URL Category popup window, enter information for the following fields. For more information, see [Configure URL Filtering](#).

Add URL Category

Name \*

Description

Confidence

1 .. 100

URL File

--Select--

URL Patterns

URL Strings

Q Search

<


>


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"> <li>Pattern</li> </ul>	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> .
<ul style="list-style-type: none"> <li>Reputation</li> </ul>	<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"> <li>Trustworthy</li> <li>Low Risk</li> <li>Moderate Risk</li> <li>Suspicious</li> <li>High</li> </ul>
<ul style="list-style-type: none"> <li> Add icon</li> </ul>	Click to add the URL pattern to the URL category.
URL Strings (Tab)	
<ul style="list-style-type: none"> <li>String</li> </ul>	Enter a URL string to match a single URL.

<ul style="list-style-type: none"> <li>◦ Reputation</li> </ul>	<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"> <li>◦ Trustworthy</li> <li>◦ Low Risk</li> <li>◦ Moderate Risk</li> <li>◦ Suspicious</li> <li>◦ High</li> </ul>
<ul style="list-style-type: none"> <li>◦  Add icon</li> </ul>	<p>Click to add the URL string to the URL category.</p>

27. 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

General

Source

Destination

Headers/Schedule

Applications/URL

Users/Groups

Enforce

Match Users

Selected

User Group Profile

--Select--

☐ Local Database

☐ External Database

☐

Users

+ New Custom User

+

Users Not Configured

☐

Groups

Groups N

OK

Cancel

Field	Description
Match Users	<p>Select the users to match:</p> <ul style="list-style-type: none"> <li>◦ Any—If you select to match any users, you cannot configure any other fields on this tab.</li> <li>◦ Known—If you select to match known users, you cannot configure any other fields on this tab.</li> <li>◦ Selected—If you select to match selected users, you can configure the other fields on this tab.</li> <li>◦ Unknown—If you select to match unknown users, you cannot configure any other fields on this tab.</li> </ul>
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. Select + New Custom User to add a user.
Groups	If you match selected users, click the + Add icon and select a user group. Select + New Custom Group to add a user group.

28. 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

Enforce

Forwarding

Action

--Select--

Nexthop IP Address

Routing Instance

--Select--

☐ Enable Symmetric Forwarding of Return Traffic

☐ Enable Symmetric L2 Forwarding of Return Traffic

Monitor

Address

Routing Instance

--Select--

Action

wait-recover

Interval(seconds)

3

Threshold(Events)

5

OK

Cancel

Field	Description
Forwarding (Group of Fields)	
<ul style="list-style-type: none"> <li>Action</li> </ul>	<p>Select the action to take on matching traffic:</p> <ul style="list-style-type: none"> <li>Allow Flow</li> <li>Deny Flow</li> </ul>
<ul style="list-style-type: none"> <li>Next-Hop IP Address</li> </ul>	<p>Enter the IP address of the next hop to which to forward the flow. Specifying a next hop statically assigns the next hop instead of using dynamic routing. When you configure a next hop, you do not need to also configure a routing instance.</p>
<ul style="list-style-type: none"> <li>Routing Instance</li> </ul>	<p>Select the routing instance to reach the next hop.</p>
<ul style="list-style-type: none"> <li>Enable Symmetric Forwarding of Return Traffic</li> </ul>	<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"> <li>◦ 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.</li> <li>◦ 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.</li> </ul>
<ul style="list-style-type: none"> <li>◦ Enable Symmetric Layer 2 Forwarding of Return Traffic</li> </ul>	<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>
Monitor (Group of Fields)	<p>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.</p>
◦ Address	<p>Enter the IP address to monitor by sending ping messages.</p>
◦ Routing Instance	<p>Select the routing instance to reach the monitored address.</p>
◦ Action	<p>Select the monitoring action to take if there is no response to the ping messages after a given number of times</p> <ul style="list-style-type: none"> <li>◦ Failover—Route traffic and do not implement the PBF traffic policy. A route lookup is performed to determine the Layer 3 destination IP address.</li> <li>◦ Next-Rule—Evaluate the other rules until a match is found. If no match is found, route the traffic.</li> <li>◦ Wait-Recover—Drop traffic until the next hop recovers.</li> </ul>
◦ Interval	<p>Enter how often to send ping messages to monitor the flow of the data packets.</p> <p><i>Range:</i> 1 through 60 seconds</p>

	<i>Default: 3 seconds</i>
--	---------------------------

29. Click OK.

---

## Configure Application Detection

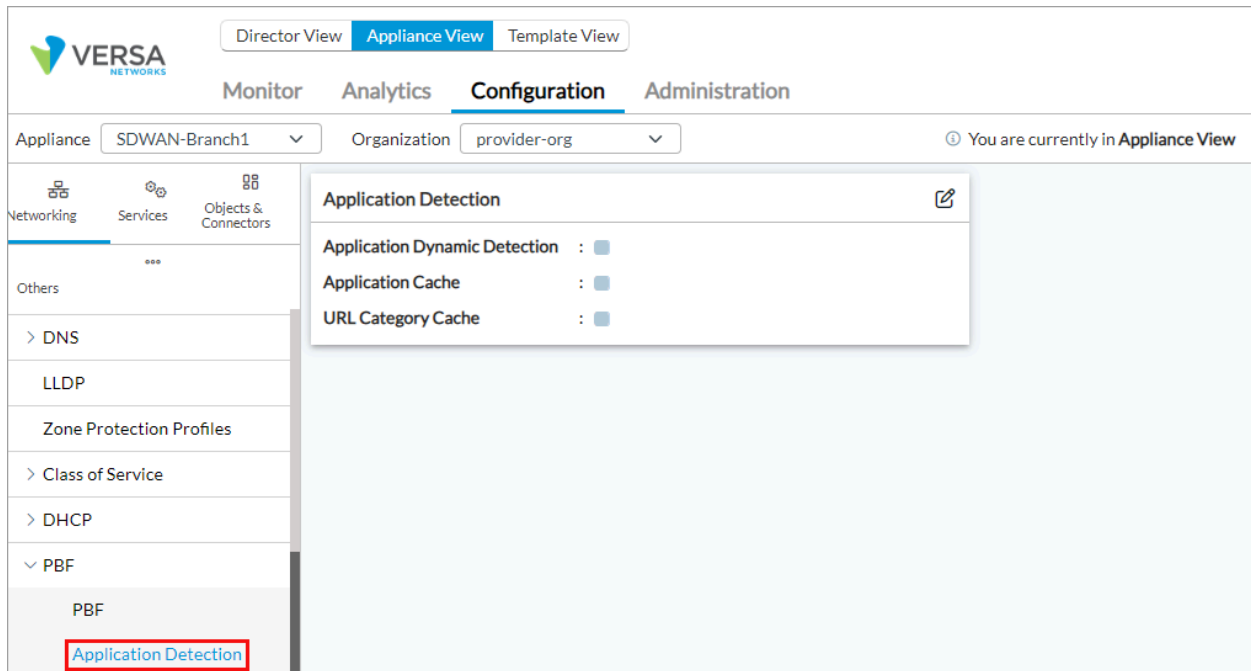
Application detection allows a PBF policy to correctly process all traffic in a flow. Application detection is always running on a VOS device.

Application detection inspects 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 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 policy is applied to all packets in the flow. The rapid identification is made possible by having an application cache, which is used to identify the application in the first packet, instead of waiting for the application identification engine to do so.

By default, dynamic application detection and application caching are enabled.

To configure application detection parameters:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Policy-Based Forwarding > Application Detection in the left menu bar. The main pane displays the Application Detection pane.



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

### Edit Application Detection

**Application Dynamic Detection**  
☐ Enable ☐ Disable

**Application Cache**  
☐ Enable ☐ Disable

**URL Category Cache**  
☐ Enable ☐ Disable

OK

Cancel

Field	Description
Application Dynamic Detection	Click Enable to dynamically re-evaluate PBF policy 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

5. Click OK.

---

## Supported Software Information

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

- Release 21.2.1 adds support for configuring rule order for policy rules.
- Use of dynamic address object available through Versa Networks cloud-hosted SASE services only.

---

## Additional Information

[Configure Address Objects](#)

[Configure SD-WAN Policy](#)

[Configure URL Filtering](#)

[Configure User and Group Policy](#)

[Configure Zones and Zone Protection Profiles](#)