Configure NGFW

For supported software information, click here.

The Versa Operating System^{TM} (VOS^{TM}) next-generation firewall (NGFW) is a robust security module that has the intelligence to distinguish different types of traffic. NGFW provides network protection beyond the protection based on ports, protocols, and IP addresses. In addition to traditional firewall capabilities, NGFW includes filtering functions such as an application firewall, an intrusion prevention system (IPS), TLS/SSL encrypted traffic inspection, website filtering, and QoS and bandwidth management.

To configure NGFW, you create an access policy profile (also called an ACL) and rules (also called ACL rules) for that access policy profile. NGFW policy includes all the match criteria of a stateful firewall policy in addition to Layer 7 match criteria, such as application and URL category, and assigns an action on them based on the match condition. The application for a session is automatically determined based on various identification methods such as applying signatures, heuristics, and statistical identification.

You create an NGFW security profile in which you define the access policy and access policy rules (ACL rules) that include criteria to allow or reject the traffic. You define access policy rules using VOS objects. An object is a method for grouping related security parameters. The VOS software provides predefined objects, which you can modify, and you can create the following custom objects:

- Application—An application object lets you define family, subfamily, risk, productivity, tags, and application timeout attributes per tenant.
- Application filter—You create application filters to select applications based on the application attributes. For example, you can filter applications based on the assigned tag, such as SD-WAN, security, or general.
- Application group—You create group applications based on attributes such as application family, subfamily, risk level, productivity level, and tags, and then you can apply the profile to the group instead of to each application.
- Services—You define a service based on its protocol and ports. For example, you can create a service for ICMP.
- URL category—You create URL categories to control access to websites based on their category. For example, you can create a category for news URLs.
- URL reputation—You create URL reputation objects to control access to websites based on their reputation score.

This article discusses how to view and modify predefined objects, create custom objects, and create access profiles using predefined and custom objects.

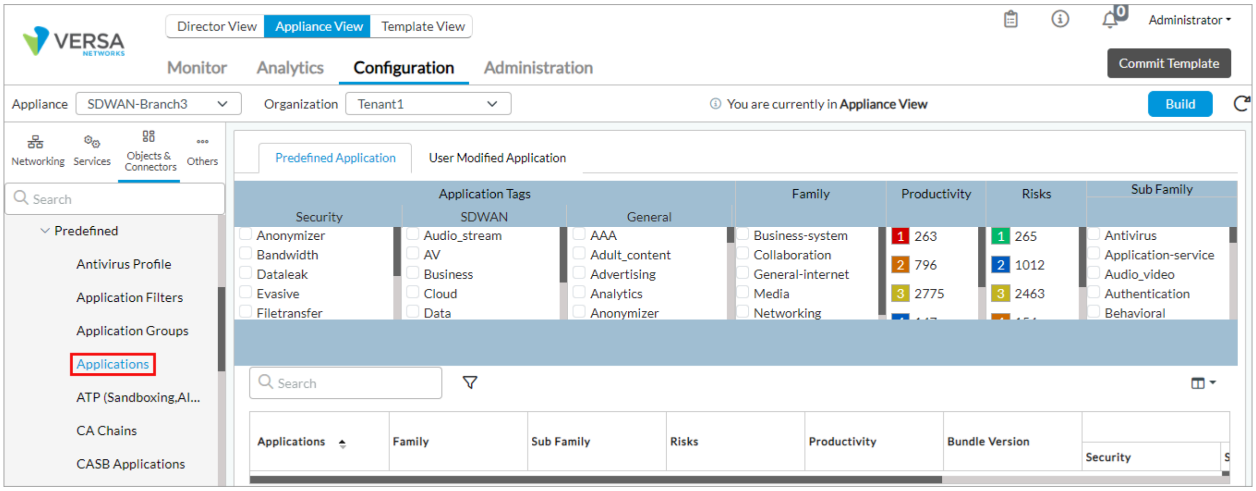
Note that the VOS software does not support decryption of the QUIC protocol. For the VOS security software modules to work, you must block QUIC traffic.

View Predefined Objects

The VOS software provides predefined objects, which are containers for grouping related security parameters.

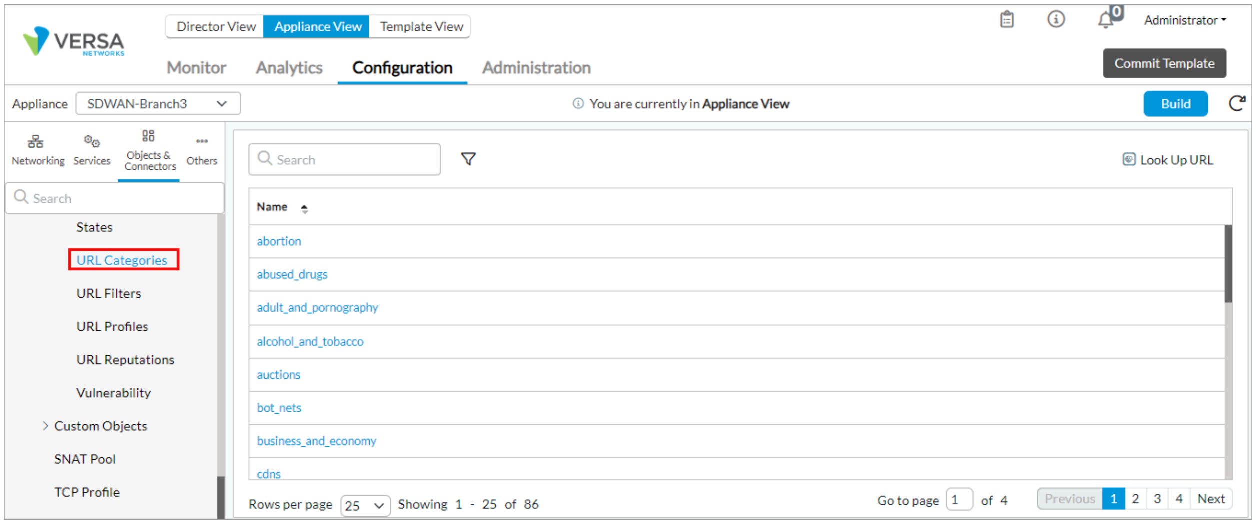
To view predefined objects:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template from the dashboard. The view changes to Appliance view.
2. Select Configuration > Objects & Connectors > Objects > Predefined > Applications in the left menu bar.



Appliance: SDWAN-Branch3 | Organization: Tenant1 | You are currently in Appliance View

3. To view predefined URL categories, select Predefined > URL Categories in the left menu bar.

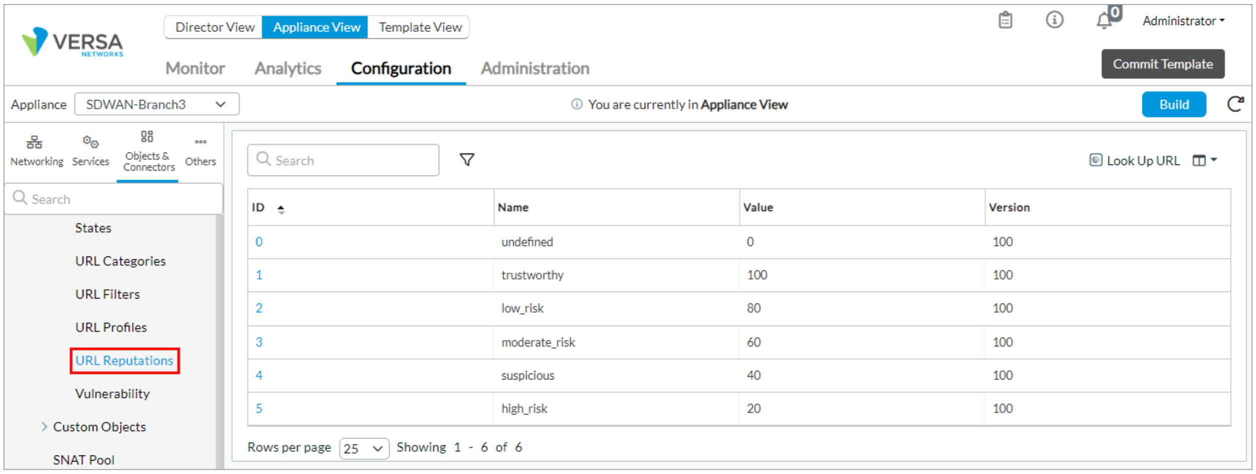


Appliance: SDWAN-Branch3 | You are currently in Appliance View

Name
abortion
abused_drugs
adult_and_pornography
alcohol_and_tobacco
auctions
bot_nets
business_and_economy
cdns

Rows per page 25 Showing 1 - 25 of 86 Go to page 1 of 4

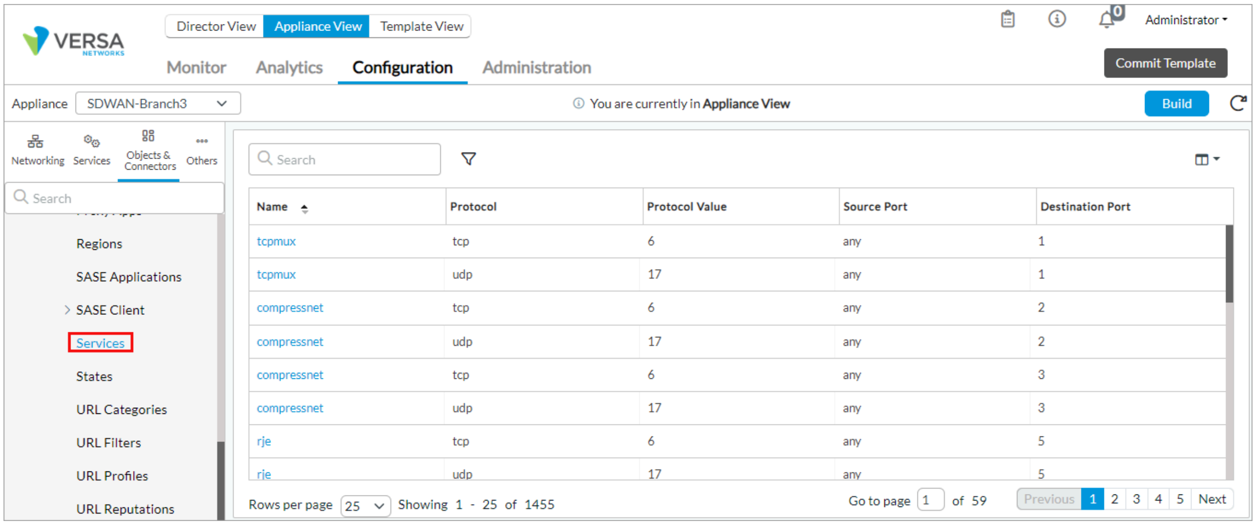
4. To view predefined URL reputation, select Predefined > URL Reputations in the left menu bar.



ID	Name	Value	Version
0	undefined	0	100
1	trustworthy	100	100
2	low_risk	80	100
3	moderate_risk	60	100
4	suspicious	40	100
5	high_risk	20	100

Rows per page 25 Showing 1 - 6 of 6

5. To view predefined services, select Predefined > Services in the left menu bar.



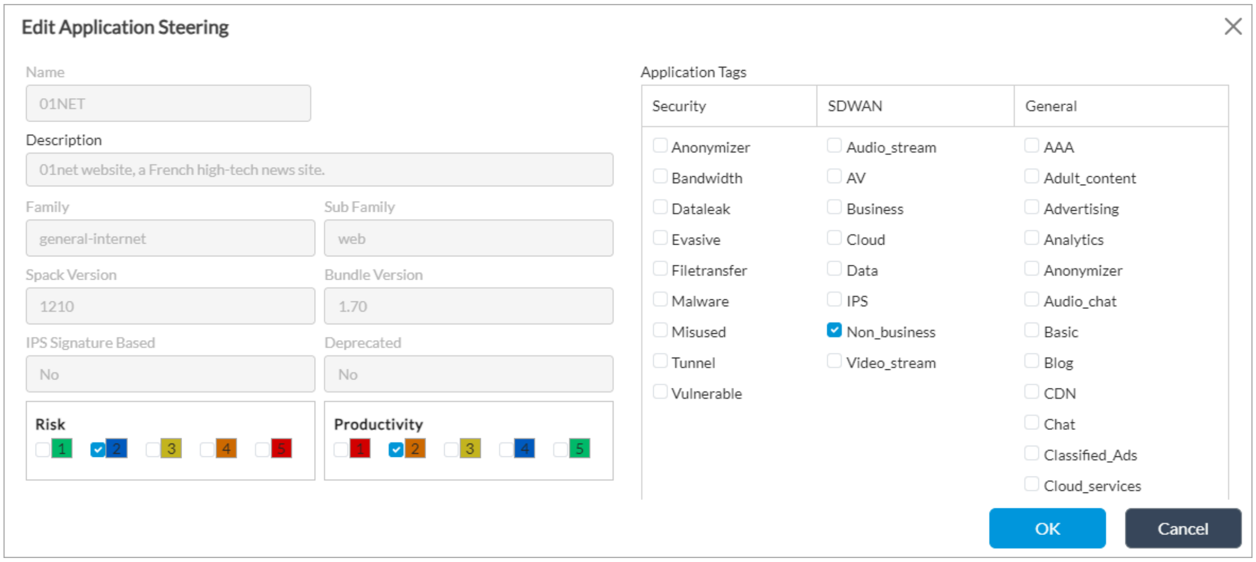
Name	Protocol	Protocol Value	Source Port	Destination Port
tcpmux	tcp	6	any	1
tcpmux	udp	17	any	1
compressnet	tcp	6	any	2
compressnet	udp	17	any	2
compressnet	tcp	6	any	3
compressnet	udp	17	any	3
rje	tcp	6	any	5
rje	udp	17	any	5

Rows per page 25 Showing 1 - 25 of 1455 Go to page 1 of 59 Previous 1 2 3 4 5 Next

Modify a Predefined Object

To change the attributes of an application for each tenant:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > Applications in the left menu bar.
4. In the Applications column, click the application name whose attributes you want to change. In the Edit Application Steering popup window, select the desired attributes, such as risk, productivity, timeout, and the application tags.



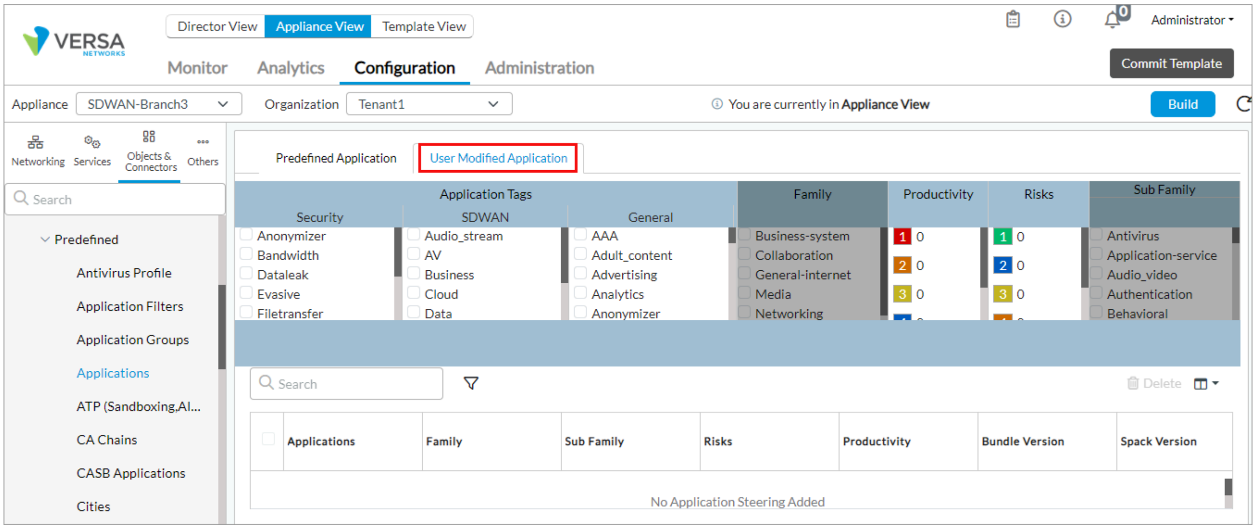
Edit Application Steering

Name	01NET
Description	01net website, a French high-tech news site.
Family	general-internet
Sub Family	web
Spack Version	1210
Bundle Version	1.70
IPS Signature Based	No
Deprecated	No
Risk	□ 1 ☑ 2 □ 3 □ 4 □ 5
Productivity	□ 1 ☑ 2 □ 3 □ 4 □ 5

Application Tags

Security	SDWAN	General
□ Anonymizer	□ Audio_stream	□ AAA
□ Bandwidth	□ AV	□ Adult_content
□ Dataleak	□ Business	□ Advertising
□ Evasive	□ Cloud	□ Analytics
□ Filetransfer	□ Data	□ Anonymizer
□ Malware	□ IPS	□ Audio_chat
□ Misused	☑ Non_business	□ Basic
□ Tunnel	□ Video_stream	□ Blog
□ Vulnerable		□ CDN
		□ Chat
		□ Classified_Ads
		□ Cloud_services

5. Click OK.
6. Click Yes to confirm that you want to save the changes.
7. Select the User-Modified Application tab in the horizontal menu bar to display the modified application object.



Appliance: SDWAN-Branch3 Organization: Tenant1

You are currently in **Appliance View**

Application Tags: Security	Application Tags: SDWAN	Application Tags: General	Family	Productivity	Risks	Sub Family
□ Anonymizer	□ Audio_stream	□ AAA	□ Business-system	1 0	1 0	□ Antivirus
□ Bandwidth	□ AV	□ Adult_content	□ Collaboration	2 0	2 0	□ Application-service
□ Dataleak	□ Business	□ Advertising	□ General-internet	3 0	3 0	□ Audio_video
□ Evasive	□ Cloud	□ Analytics	□ Media			□ Authentication
□ Filetransfer	□ Data	□ Anonymizer	□ Networking			□ Behavioral

□ Applications	Family	Sub Family	Risks	Productivity	Bundle Version	Spack Version

No Application Steering Added

Create Custom Application Objects

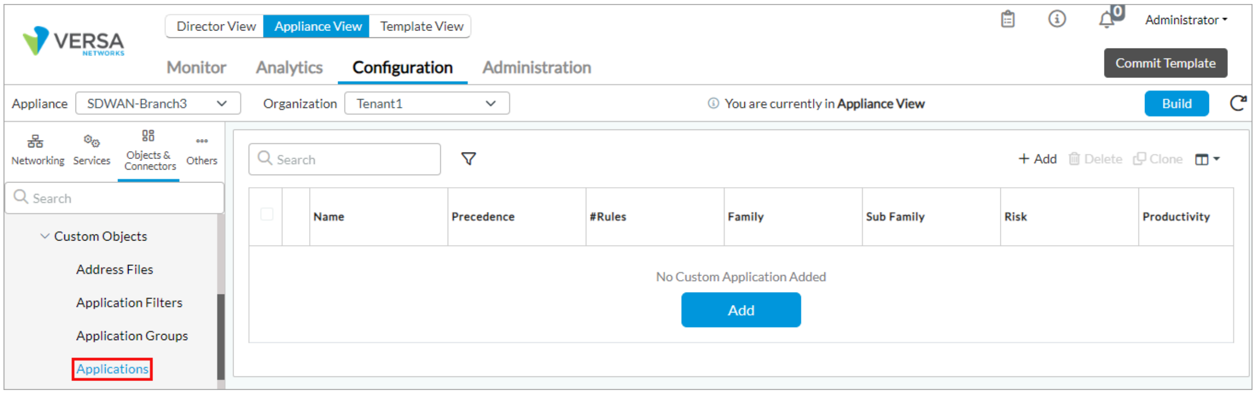
The following sections describe how to configure custom application objects, which are containers for grouping related security parameters.

Configure an Application Object

1. In Director view:

    a. Select the Configuration tab in the top menu bar.
    b. Select Templates in the horizontal menu bar.
    c. Select an organization in the left navigation bar.
    d. Select a template in the dashboard. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Applications in the left menu bar. The following screen displays:



Appliance: SDWAN-Branch3

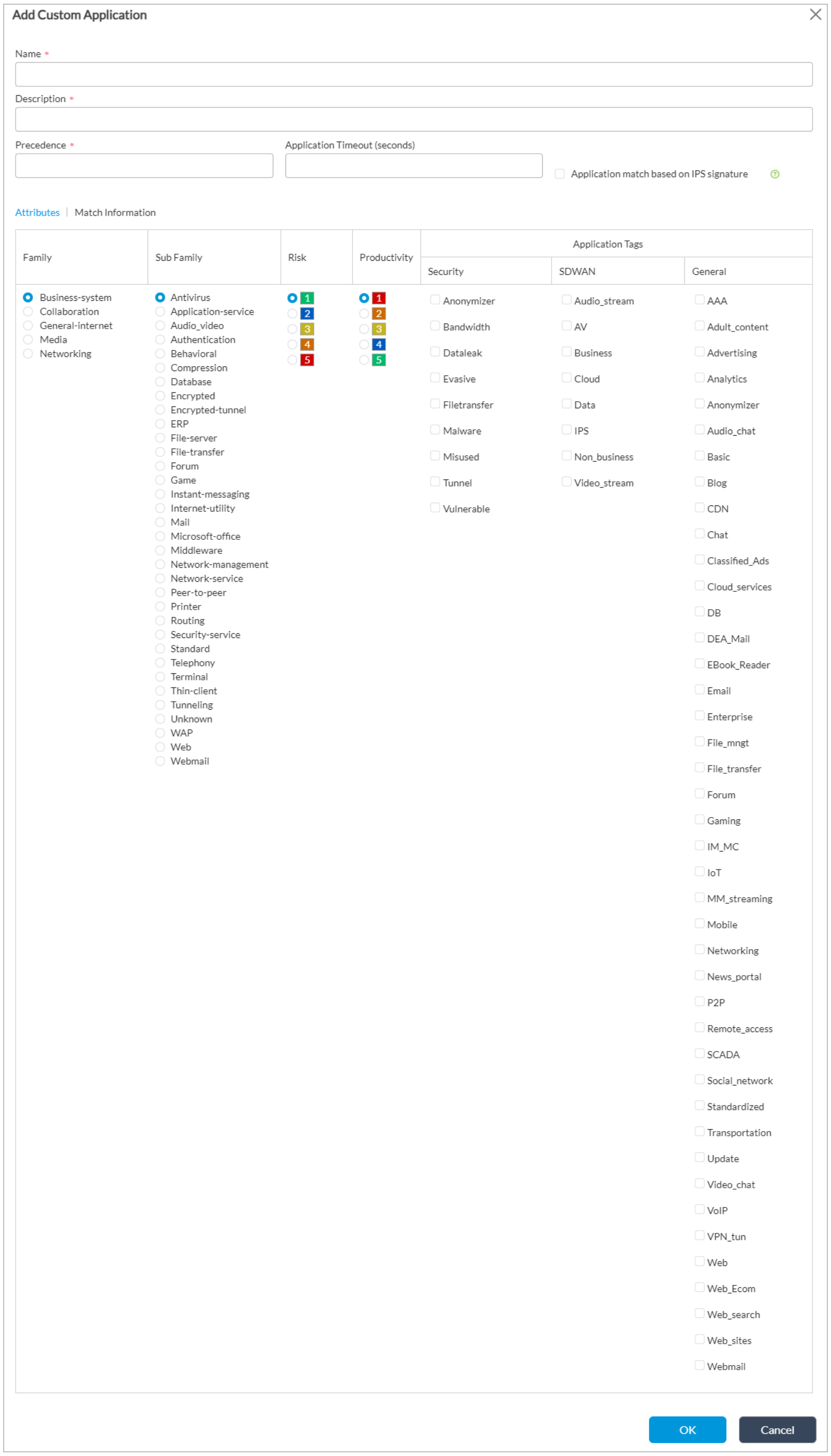
Organization: Tenant1

You are currently in Appliance View

	Name	Precedence	#Rules	Family	Sub Family	Risk	Productivity

No Custom Application Added

4. Click the + Add icon. In the Add Application Steering popup window, enter information for the following fields.



Add Custom Application

Name *

Description *

Precedence *

Application Timeout (seconds)

□ Application match based on IPS signature

Attributes | Match Information

Family

- ● Business-system
- ○ Collaboration
- ○ General-internet
- ○ Media
- ○ Networking

Sub Family

- ● Antivirus
- ○ Application-service
- ○ Audio_video
- ○ Authentication
- ○ Behavioral
- ○ Compression
- ○ Database
- ○ Encrypted
- ○ Encrypted-tunnel
- ○ ERP
- ○ File-server
- ○ File-transfer
- ○ Forum
- ○ Game
- ○ Instant-messaging
- ○ Internet-utility
- ○ Mail
- ○ Microsoft-office
- ○ Middleware
- ○ Network-management
- ○ Network-service
- ○ Peer-to-peer
- ○ Printer
- ○ Routing
- ○ Security-service
- ○ Standard
- ○ Telephony
- ○ Terminal
- ○ Thin-client
- ○ Tunneling
- ○ Unknown
- ○ WAP
- ○ Web
- ○ Webmail

Risk

- ● 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Productivity

- ● 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Application Tags

Security

- □ Anonymizer
- □ Bandwidth
- □ Dataleak
- □ Evasive
- □ Filetransfer
- □ Malware
- □ Misused
- □ Tunnel
- □ Vulnerable

SDWAN

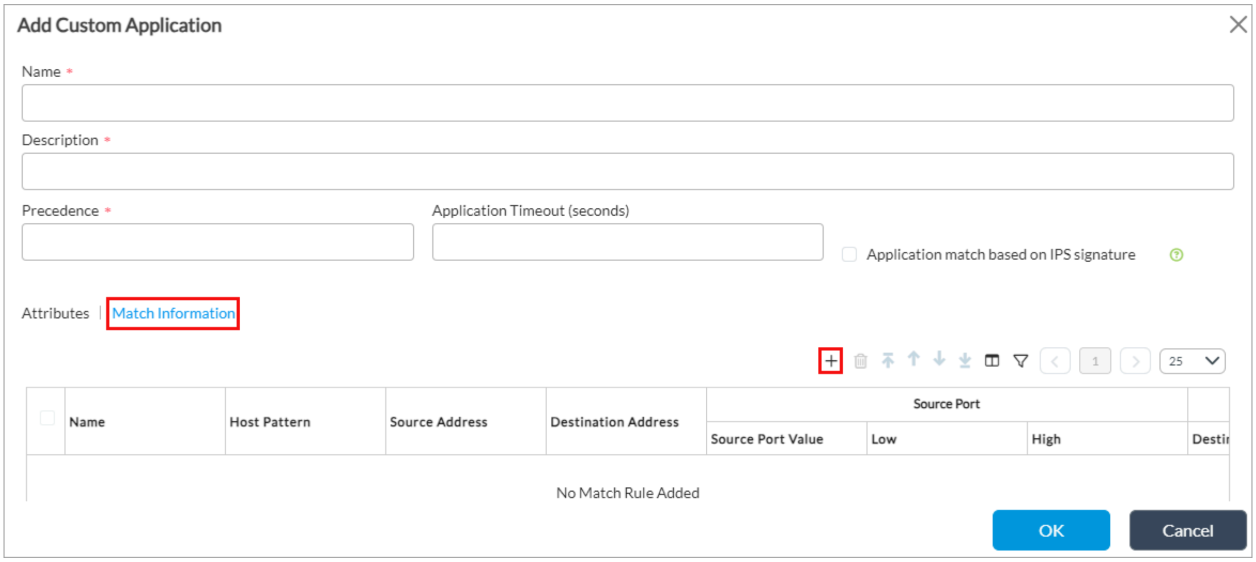
- □ Audio_stream
- □ AV
- □ Business
- □ Cloud
- □ Data
- □ IPS
- □ Non_business
- □ Video_stream

General

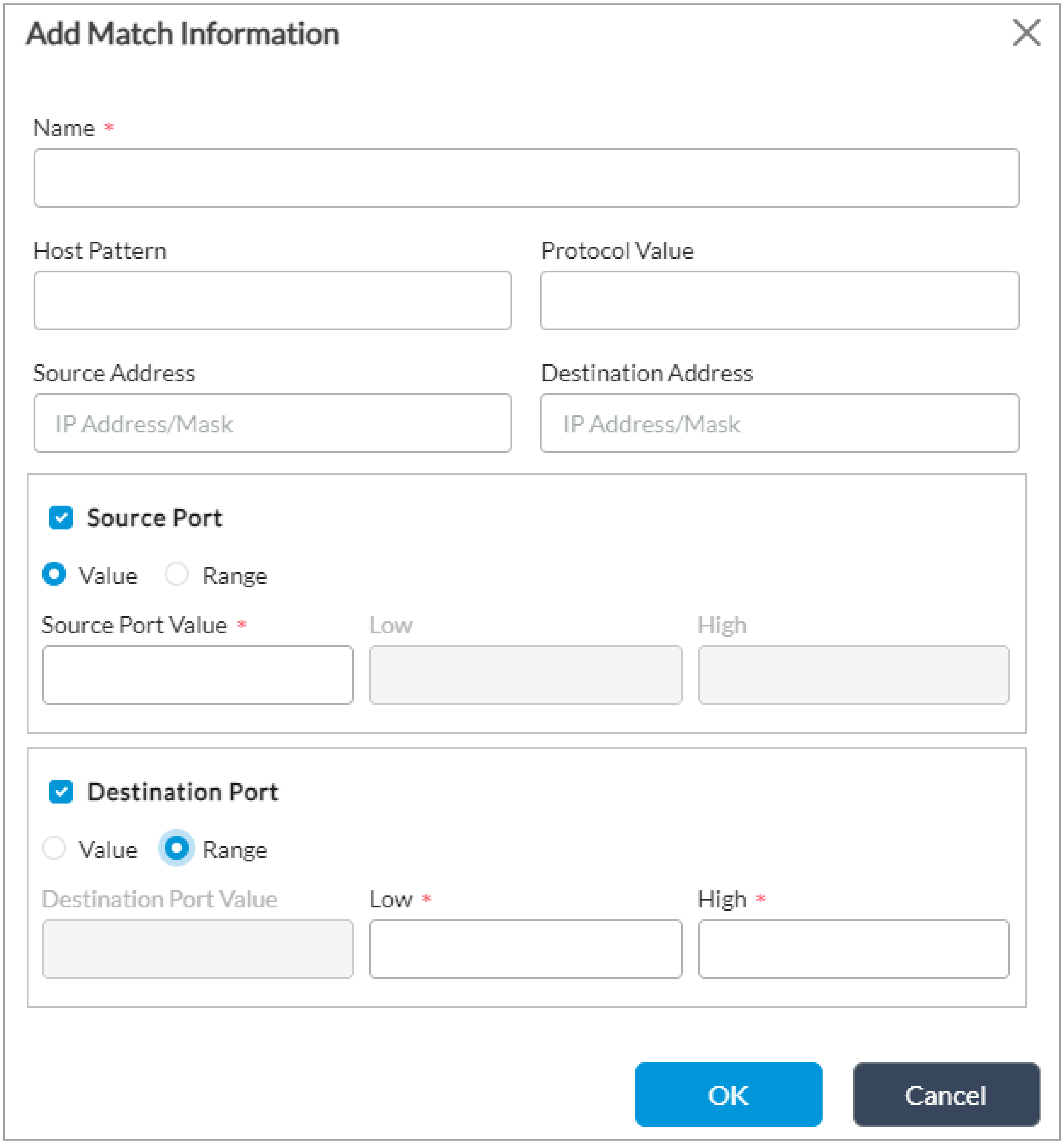
- □ AAA
- □ Adult_content
- □ Advertising
- □ Analytics
- □ Anonymizer
- □ Audio_chat
- □ Basic
- □ Blog
- □ CDN
- □ Chat
- □ Classified_Ads
- □ Cloud_services
- □ DB
- □ DEA_Mail
- □ EBook_Reader
- □ Email
- □ Enterprise
- □ File_mngt
- □ File_transfer
- □ Forum
- □ Gaming
- □ IM_MC
- □ IoT
- □ MM_streaming
- □ Mobile
- □ Networking
- □ News_portal
- □ P2P
- □ Remote_access
- □ SCADA
- □ Social_network
- □ Standardized
- □ Transportation
- □ Update
- □ Video_chat
- □ VoIP
- □ VPN_tun
- □ Web
- □ Web_Ecom
- □ Web_search
- □ Web_sites
- □ Webmail

Field	Description
Name	Name of the application.
Precedence	Priority of the application.
Application Timeout	Application timeout, in seconds. *Range*: 1 through 86400 seconds
Application Match IPS	Select to match the IPS signature.
Attributes	Select the family, subfamily, risk, productivity, and application tag.

5. Select the Match Information tab.



6. Click the + Add icon to add a match condition. In the Add Match Information popup window, enter information for the following fields.



Add Match Information

Name *

Host Pattern

Protocol Value

Source Address: IP Address/Mask

Destination Address: IP Address/Mask

☑ Source Port

● Value ○ Range

Source Port Value * | Low | High

☑ Destination Port

○ Value ● Range

Destination Port Value | Low * | High *

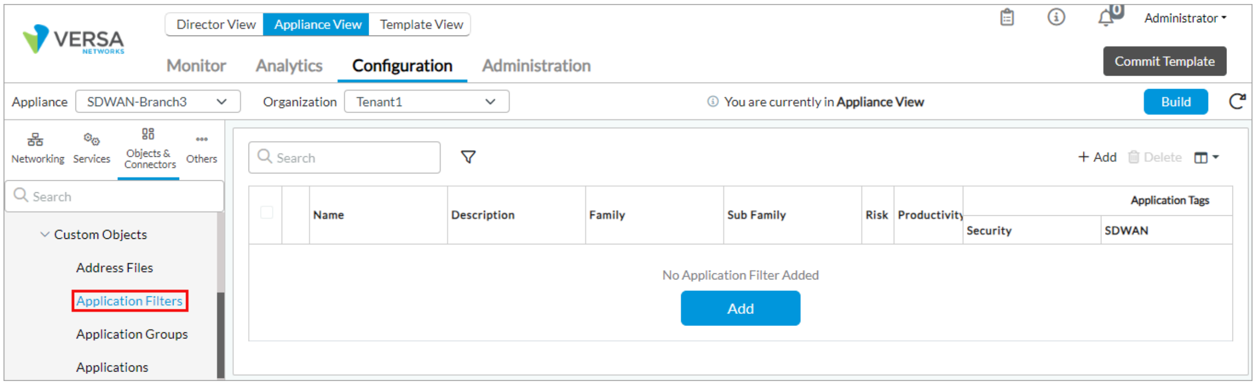
Field	Description
Name	Enter a name for the rule.
Host Pattern	Enter the host pattern to match for the HTTP header and TLS Server Name Indication (SNI).
Protocol Value	Enter the protocol name or number to match.

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

7. Click OK.

Configure Application Filters

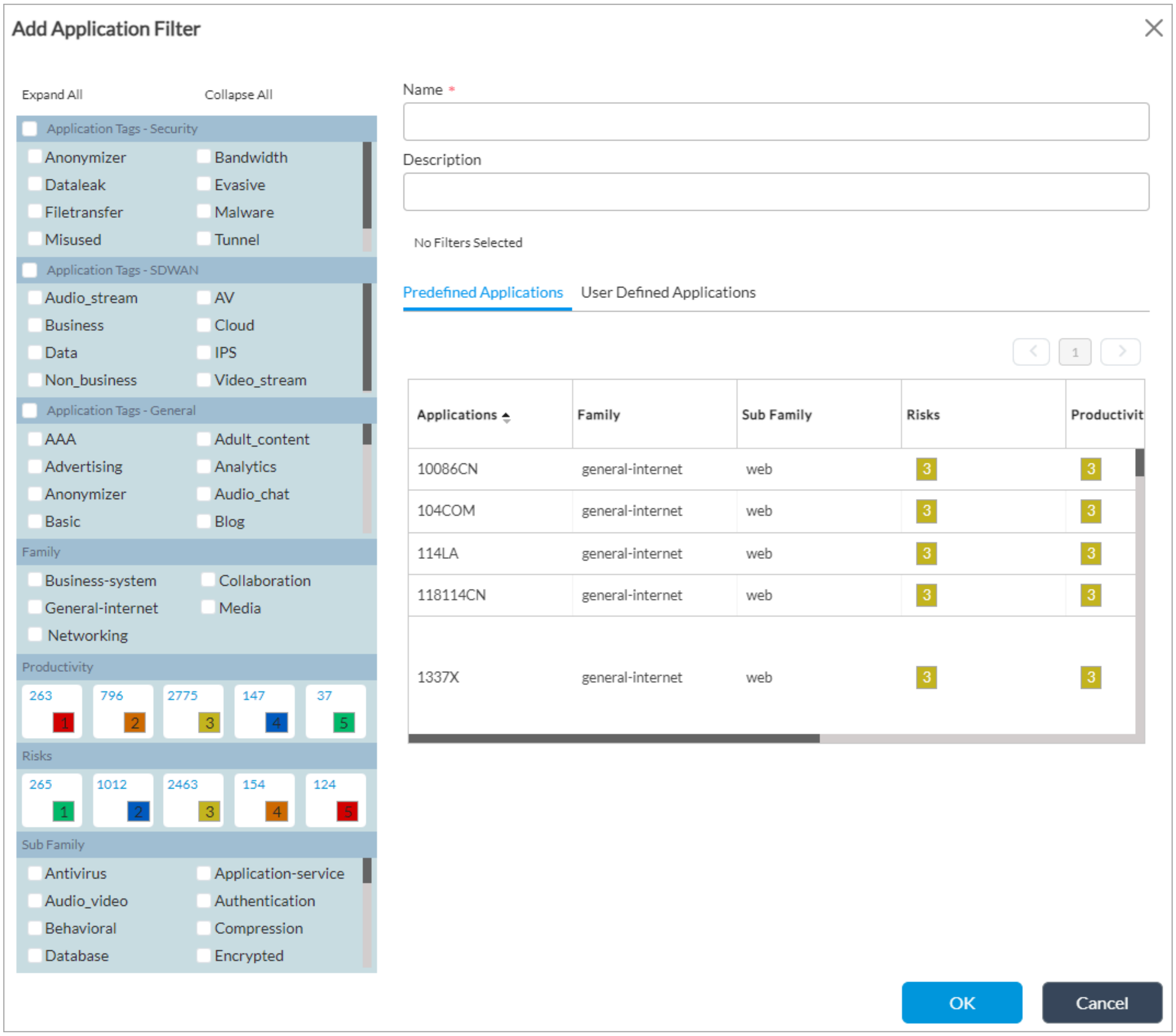
1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates in the horizontal menu bar.
    c. Select an organization in the left navigation bar.
    d. Select a template in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Application Filters in the left menu bar.



	Name	Description	Family	Sub Family	Risk	Productivity	Application Tags	
							Security	SDWAN

No Application Filter Added

4. Click the + Add icon. The Add Application Filter window displays.

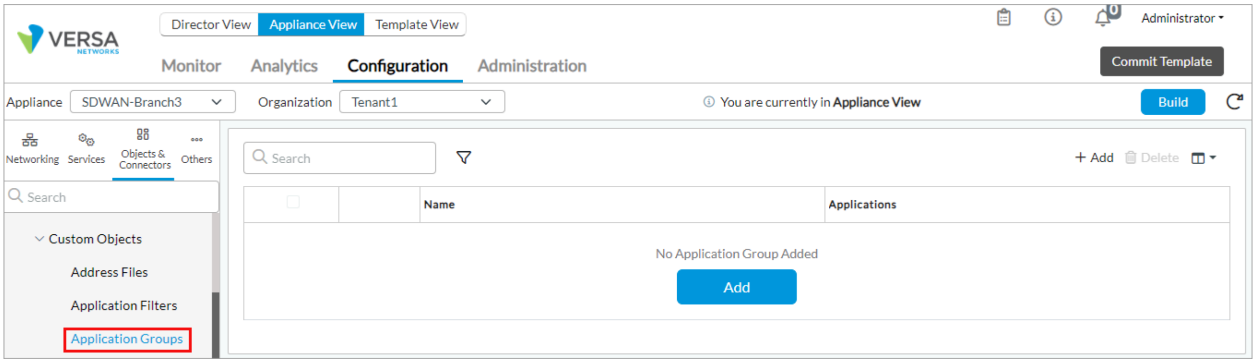


Applications ▲	Family	Sub Family	Risks	Productivit
10086CN	general-internet	web	3	3
104COM	general-internet	web	3	3
114LA	general-internet	web	3	3
118114CN	general-internet	web	3	3
1337X	general-internet	web	3	3

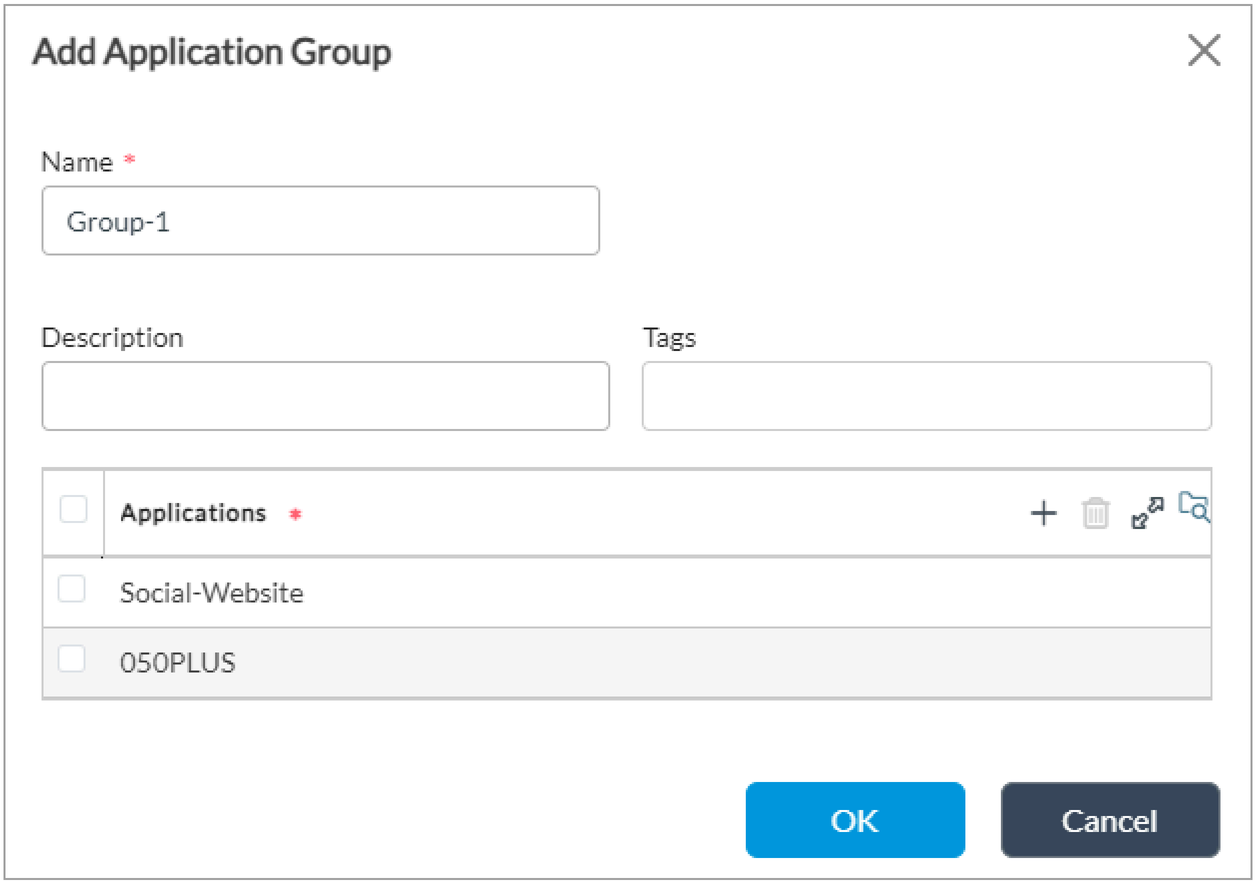
5. In the left panel, select the required application attributes to create a filter.
6. Click OK.

Configure an Application Group Object

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates in the horizontal menu bar.
    c. Select an organization in the left navigation bar.
    d. Select a template in the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Application Groups in the left menu bar.



4. Click the + Add icon. In the Add Application Group popup window, enter information for the following fields.



Field	Description
Name	Enter a name for the application group object.
Description	Enter a text description for the application group object.
Tags	Enter a keyword or phrase that you can use to filter the application group object.

5. Click OK.

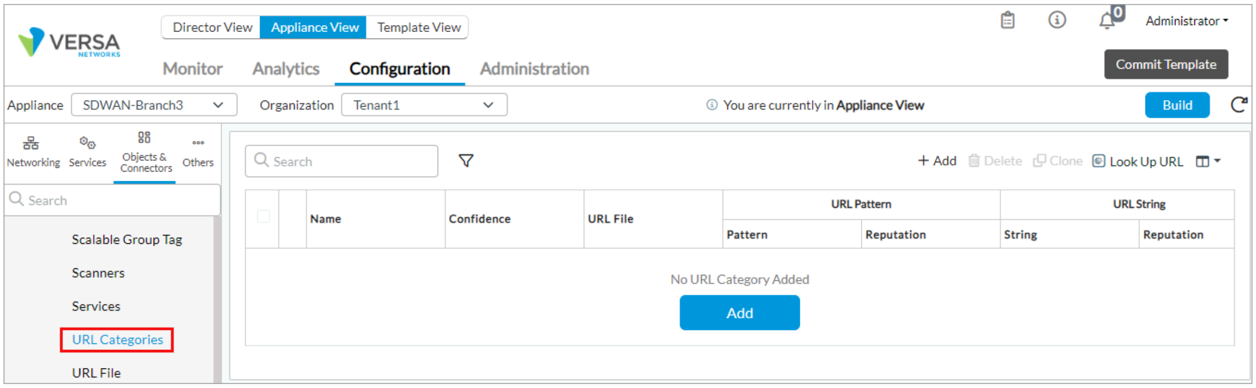
Configure URL Objects

To configure URL categories:

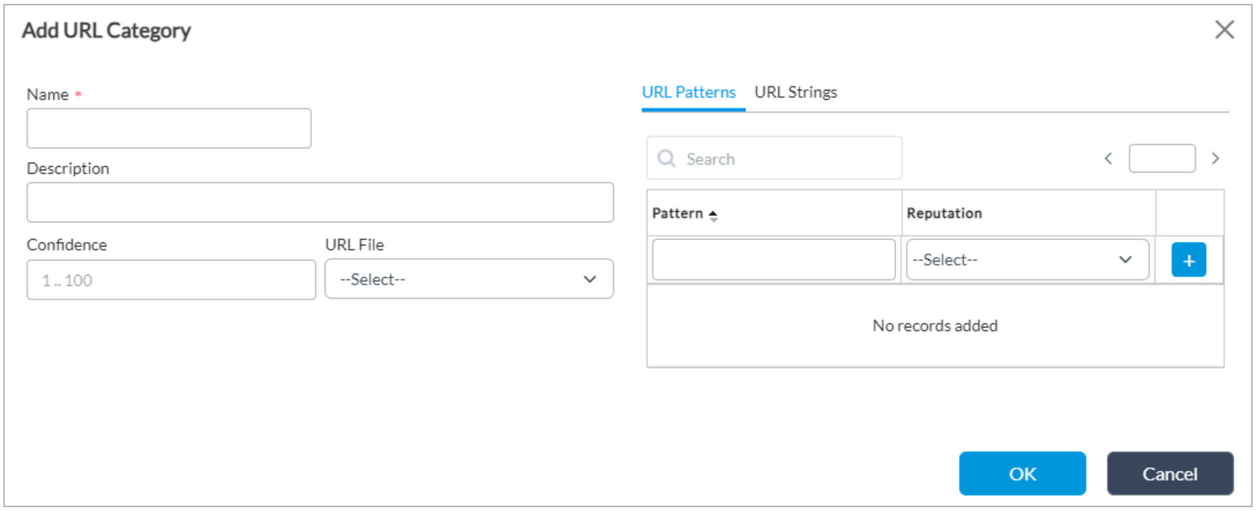
1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates in the horizontal menu bar.
    c. Select an organization in the left navigation bar.

   d. Select a template from the dashboard. The view changes to Appliance view.

2. Select Configuration > Objects & Connectors > Objects > Custom Objects > URL Category in the left menu bar.



3. Click the + Add icon. In the Add URL Category popup window, enter information for the following fields.



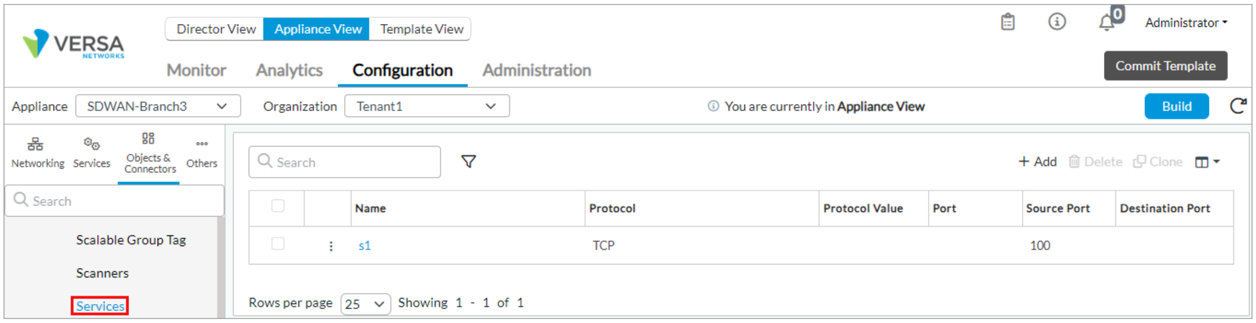
Field	Description
Name	Enter a name for the URL category object.
Description	Enter a description for the URL category object.
Tags	Enter a keyword or phrase that you can use to filter the URL category object name.
Confidence	Enter a level of confidence.
URL File	Select a file that contains a list of URLs.
URL Patterns (Tab)	

Field	Description
◦ Pattern	Enter a regex pattern to match the URLs. If you include a backslash (\) in the regex pattern, you must escape it by preceding it with a backslash.
◦ Reputation	Select a reputation to assign to the URLs.
URL Strings (Tab)	
◦ String	Enter a URL string to match.
◦ Reputation	Select a reputation to assign to the URLs.

4. Click OK.

Configure Services

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template from the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Services in the left menu bar.



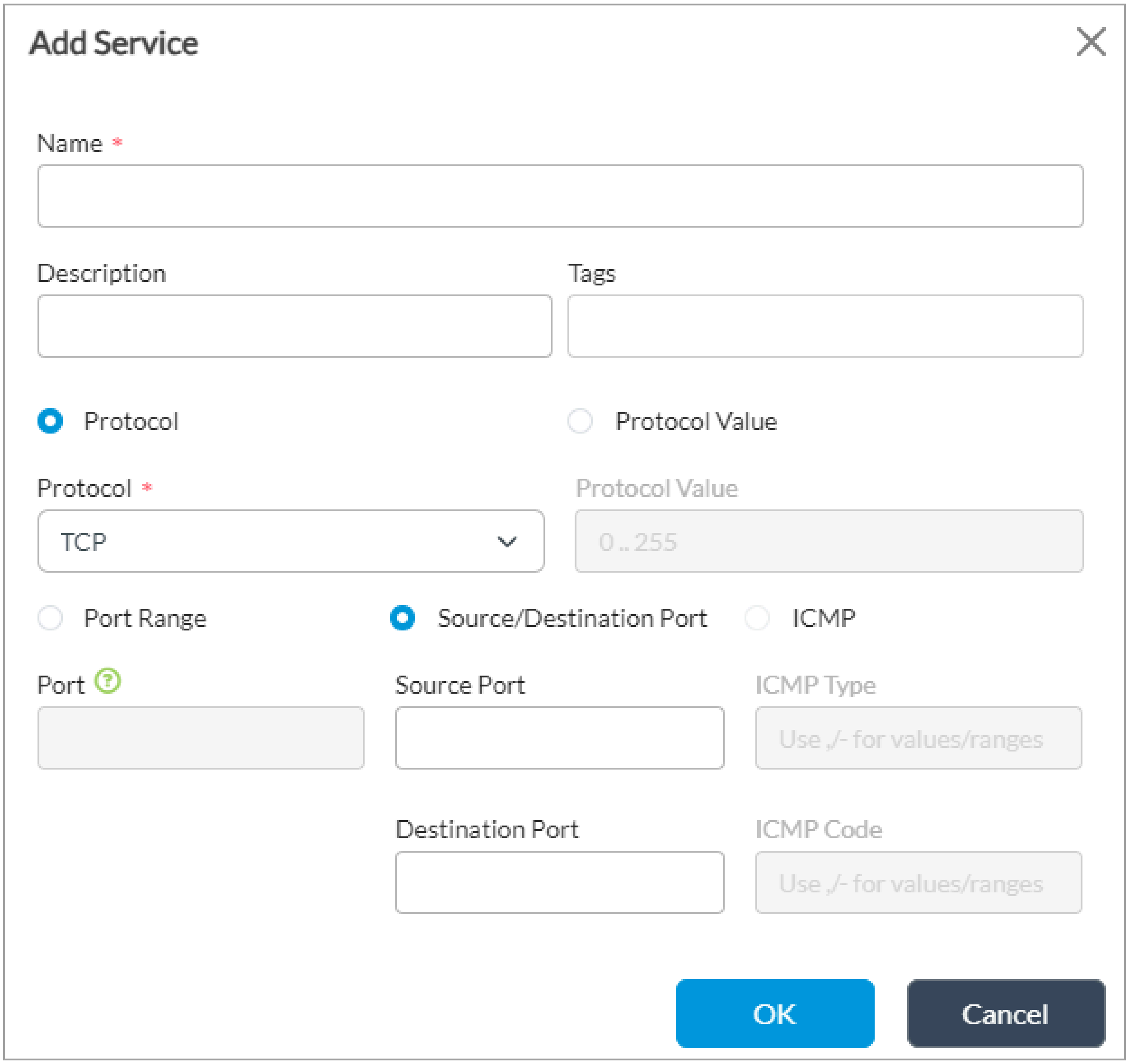
Appliance: SDWAN-Branch3 Organization: Tenant1

You are currently in Appliance View

Name	Protocol	Protocol Value	Port	Source Port	Destination Port
s1	TCP			100	

Rows per page 25 Showing 1 - 1 of 1

4. Click the + Add icon. In the Add Service popup window, enter information for the following fields.



● Protocol ○ Protocol Value

Protocol * TCP

○ Port Range ● Source/Destination Port ○ ICMP

Field	Description
Name	Enter a name for the service object.
Description	Enter a description for the service object.
Tags	Enter a keyword or phrase that you can use to filter the service object.
Protocol or Protocol Value	Select to configure the service by protocol name or protocol number.
Protocol	For a protocol name, select the protocol for the service.

Field	Description
Protocol Value	For a protocol number, enter the protocol number for the service.
Port or Source/Destination	Select to use the same port number for the source and destination or to use different port numbers.
Port	For a port, enter the port number for the source and destination.
Source Port	For a source/destination, enter the source port number.
Destination Port	For a source/destination, enter the destination port number.

5. Click OK.

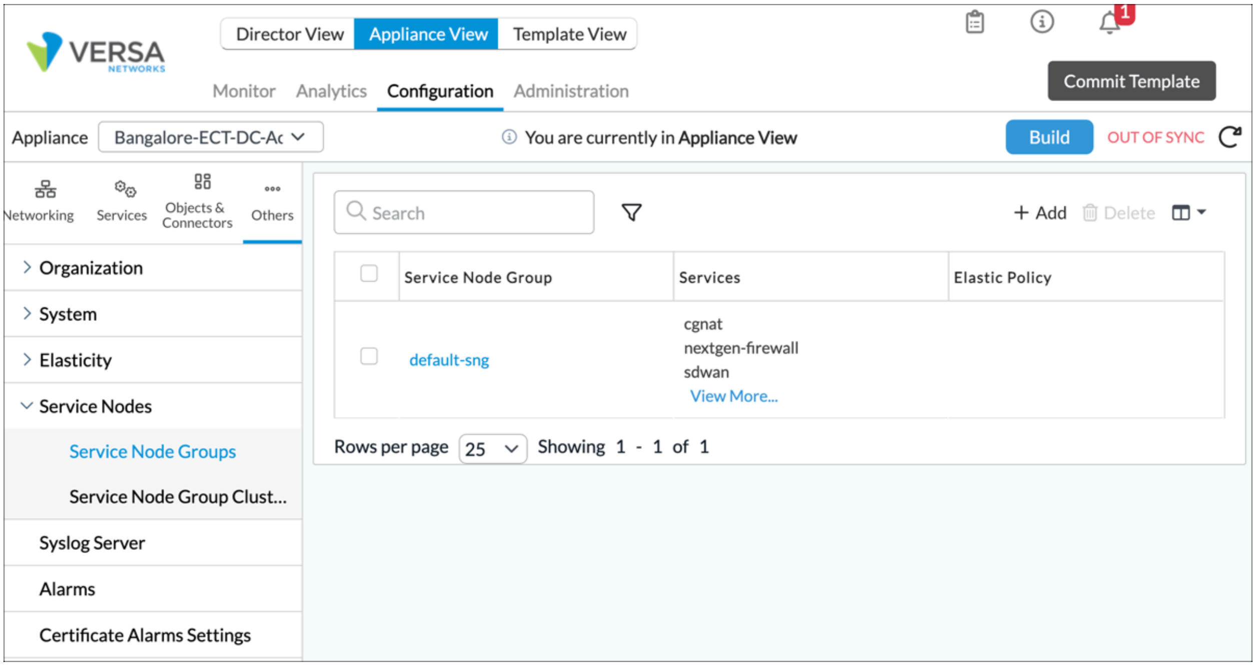
Enable NGFW

Before you configure NGFW services, you must enable NGFW on the VOS device. To do this, you enable NGFW globally in the service node group used by the organizations on the VOS device. Then you can enable NGFW for individual organizations, which you do by adding NGFW services to the organization limits for the provider or tenant organization.

For information about configuring service node groups, see Configure Service Node Groups. For information about configuring organization limits, see Configure Organization Limits.

To enable NGFW globally for a VOS device:

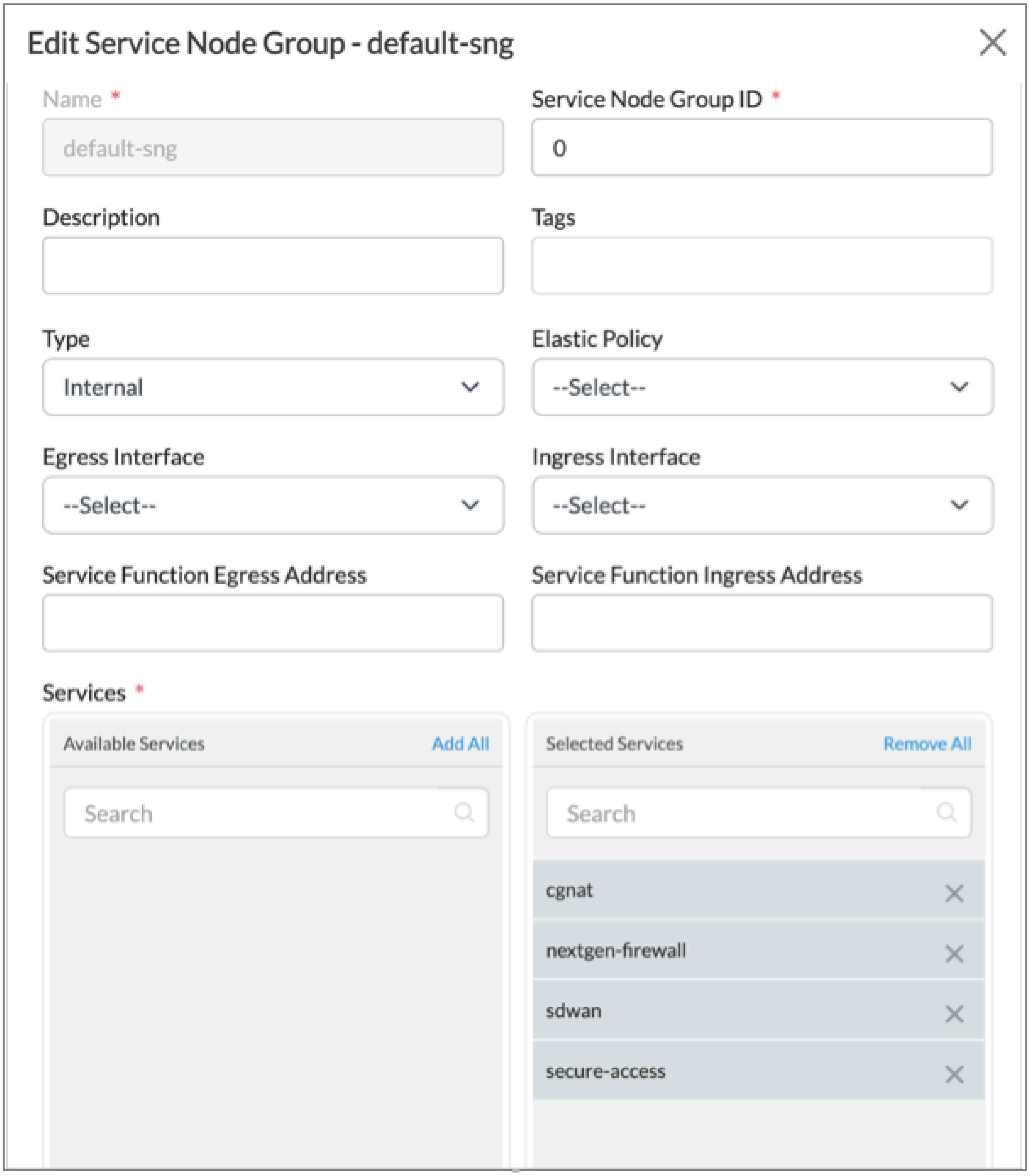
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. In the main pane, click the name of the VOS device. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Service Nodes > Service Node Groups in the left menu bar. The main pane displays the service node groups that are already configured.



□	Service Node Group	Services	Elastic Policy
□	default-sng	cgnat nextgen-firewall sdwan View More...	

Rows per page 25 Showing 1 - 1 of 1

4. Click the name of the service node group. The Edit Service Node Group popup window displays.



Edit Service Node Group - default-sng

Name * : default-sng

Service Node Group ID * : 0

Description:

Tags:

Type: Internal

Elastic Policy: --Select--

Egress Interface: --Select--

Ingress Interface: --Select--

Service Function Egress Address:

Service Function Ingress Address:

Services *

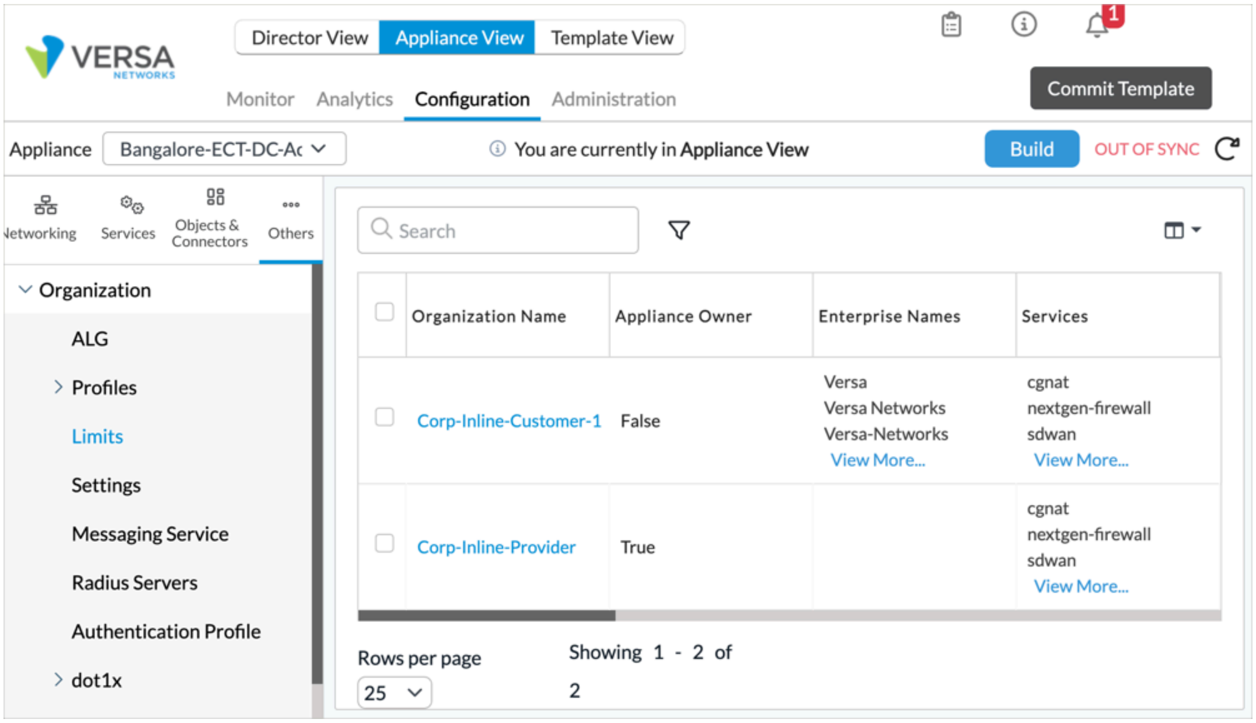
Available Services

Selected Services: cgnat, nextgen-firewall, sdwan, secure-access

5. In the Selected Services table, ensure that the nextgen-firewall service is listed. If it is not listed, click nextgen-firewall in the Available Services table to move it to the Selected Services table.
6. Click OK.
7. Refresh the browser window.

To enable NGFW for an organization on a VOS device:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. In the main pane, click the name of the VOS device. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations that are already configured.



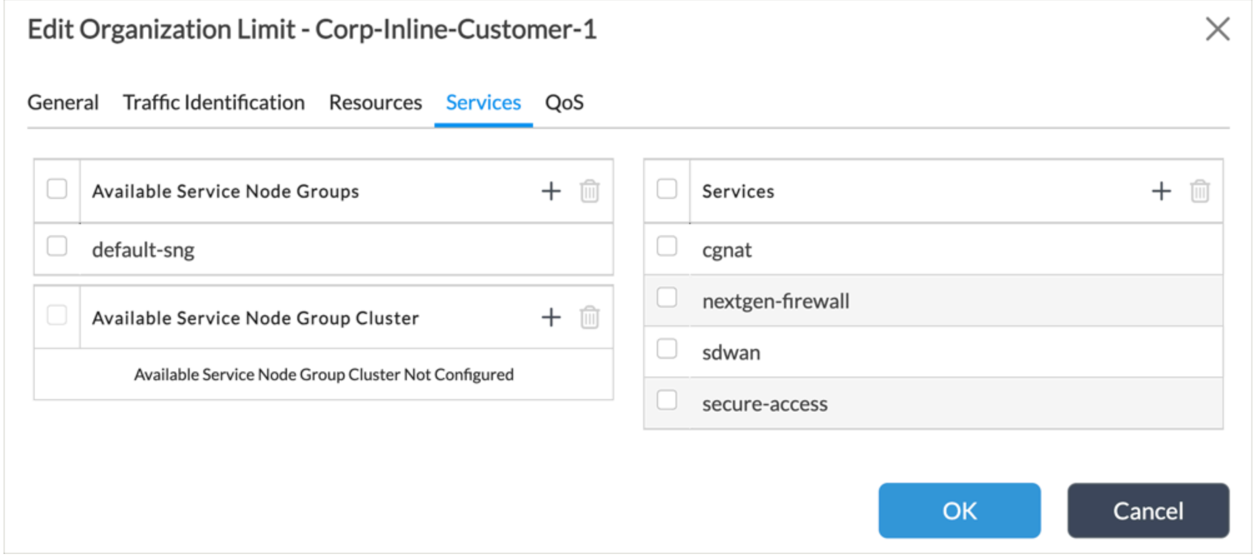
Appliance: Bangalore-ECT-DC-Ac

You are currently in Appliance View

	Organization Name	Appliance Owner	Enterprise Names	Services
□	Corp-Inline-Customer-1	False	Versa Versa Networks Versa-Networks View More...	cgnat nextgen-firewall sdwan View More...
□	Corp-Inline-Provider	True		cgnat nextgen-firewall sdwan View More...

Showing 1 - 2 of 2

4. Click the name of the organization. The Edit Organization Limit popup window displays.
5. Select the Services tab.



□	Available Service Node Groups
□	default-sng

□	Available Service Node Group Cluster
	Available Service Node Group Cluster Not Configured

□	Services
□	cgnat
□	nextgen-firewall
□	sdwan
□	secure-access

6. In the Services table, ensure that the nextgen-firewall service is listed in the Services table. If it is not listed, click the + Add icon and then select nextgen-firewall.
7. Click OK.
8. Refresh the browser window.

Configure a Security Access Policy

After you have configured custom objects, you can configure security access policies to filter traffic based on the predefined and custom objects. A security access policy consists of an ordered set of one or more policy rules. Each policy rule consists of a set of match criteria and enforcement actions. NGFW security access policy rules can match traffic based on Layer 3, Layer 4, and Layer 7 information, as well as on time of day. In an NGFW security access policy, you define:

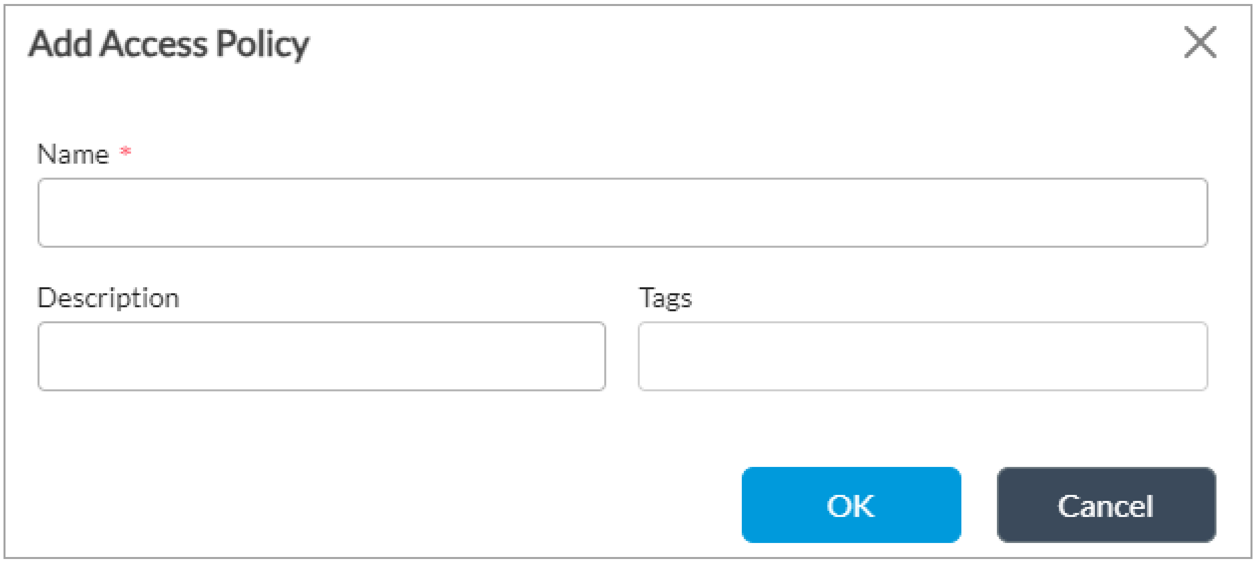
- Actionable options, such as :
  - Accept
  - Deny
  - Reject
  - Generate logs
  - Packet capture
  - Logging profile based on start, end, both, or never
  - Apply security profiles, such as IP filtering, URL filtering, antivirus, vulnerability, IP reputation, and domain name system (DNS) filtering
- Traffic-filtering criteria, such as:
  - Source zone
  - Destination zone

- Source address
  - Destination address
  - IP headers
- TCP and UDP services, such as:
  - Applications, application groups, and application filters
  - URL categories
- Schedule objects based on time of day

Configure Access Policies (ACLs)

You configure an access policy to define match criteria. To configure an access policy:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template from the dashboard. The view changes to Appliance view.
2. Or, in Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select the device from the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Services > Next Gen Firewall > Security > Policies in the left menu bar. Note: If Next Gen Firewall does not display in the Services menu, then enable it using the procedure in Enable NGFW.
5. Click the + Add icon to define a policy. In the Add Access Policy popup window, enter information for the following fields.

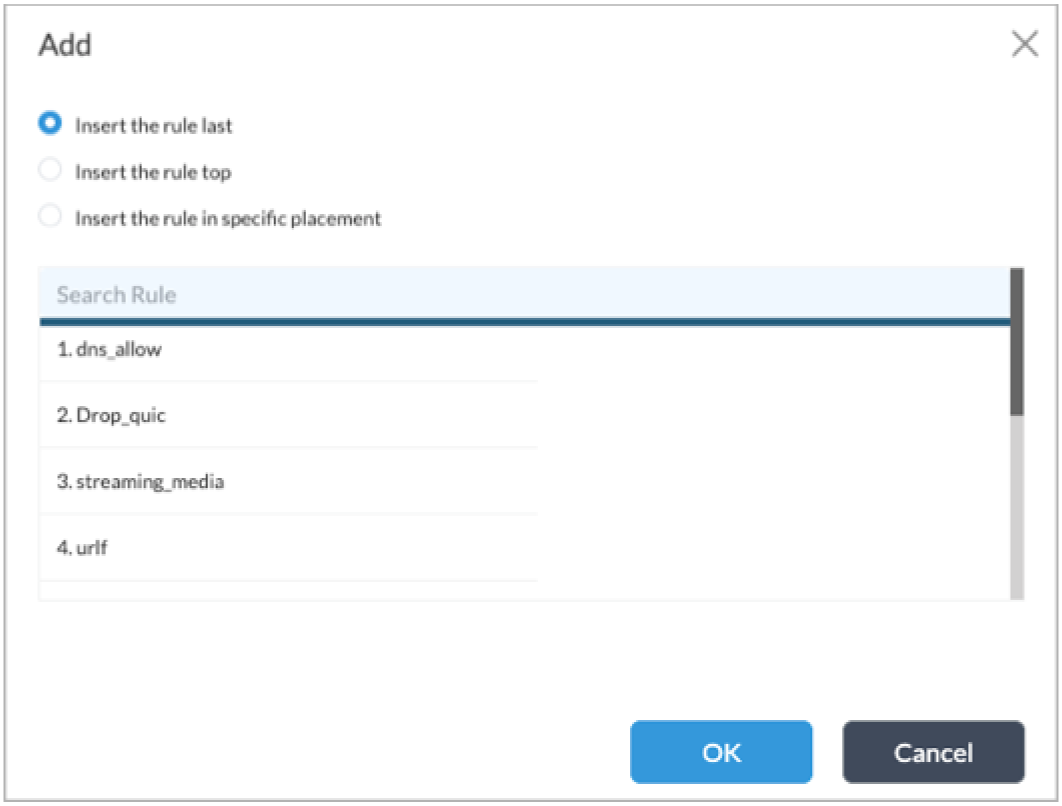


Field	Description
Name	Enter a name for the access policy.
Description	Enter a description for the access policy.

6. Click OK.

Configure Access Policy Rules (ACL Rules)

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates in the horizontal menu bar.
    c. Select an organization in the left navigation bar.
    d. Select a template in the main pane. The view changes to Appliance view.
2. Or, in Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliance in the left menu bar.
    c. Select the device in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Services > Next Gen Firewall > Security > Policies in the left menu bar, and select the Rules tab.
5. Click the + Add icon to define rules for the policy. The Add Rule popup window displays.
6. (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 end of the existing rules, the top of the existing rules, or in a specific location in the list of existing rules. You can use the Search Rule field to search for a specific rule in the list.



Add

● Insert the rule last

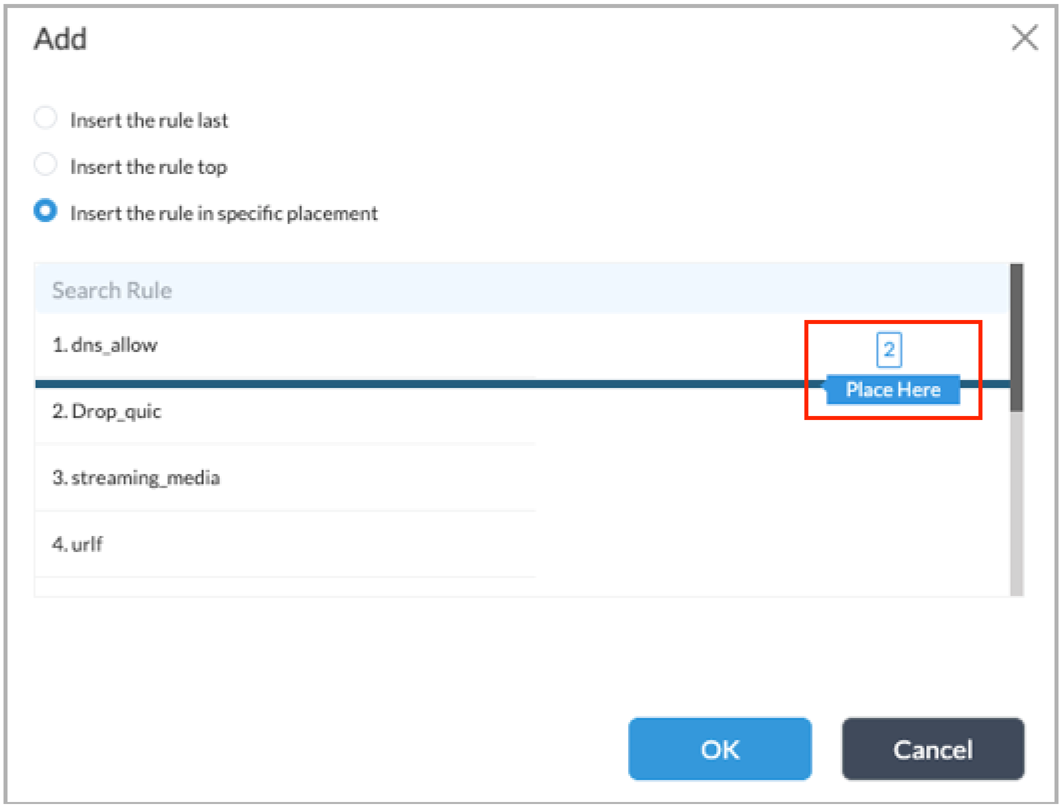
○ Insert the rule top

○ Insert the rule in specific placement

Search Rule

1. dns_allow
2. Drop_quic
3. streaming_media
4. urlf

b. If you select Insert the Rule in Specific Placement, you can drag the rule name to the desired location in the list, as shown below.



Add

○ Insert the rule last

○ Insert the rule top

● Insert the rule in specific placement

Search Rule

1. dns_allow

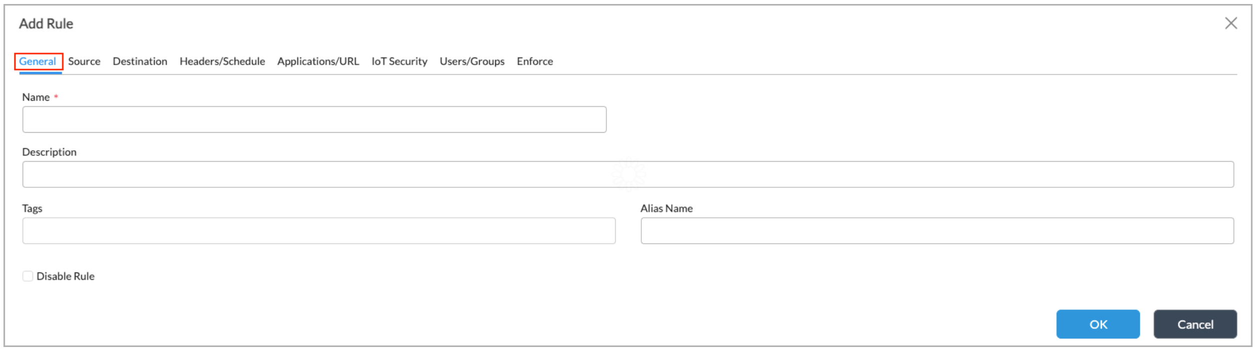
2. Drop_quic

3. streaming_media

4. urlf

c. Click OK. The Add Rule popup window displays.

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



Add Rule

General | Source | Destination | Headers/Schedule | Applications/URL | IoT Security | Users/Groups | Enforce

Name *

Description

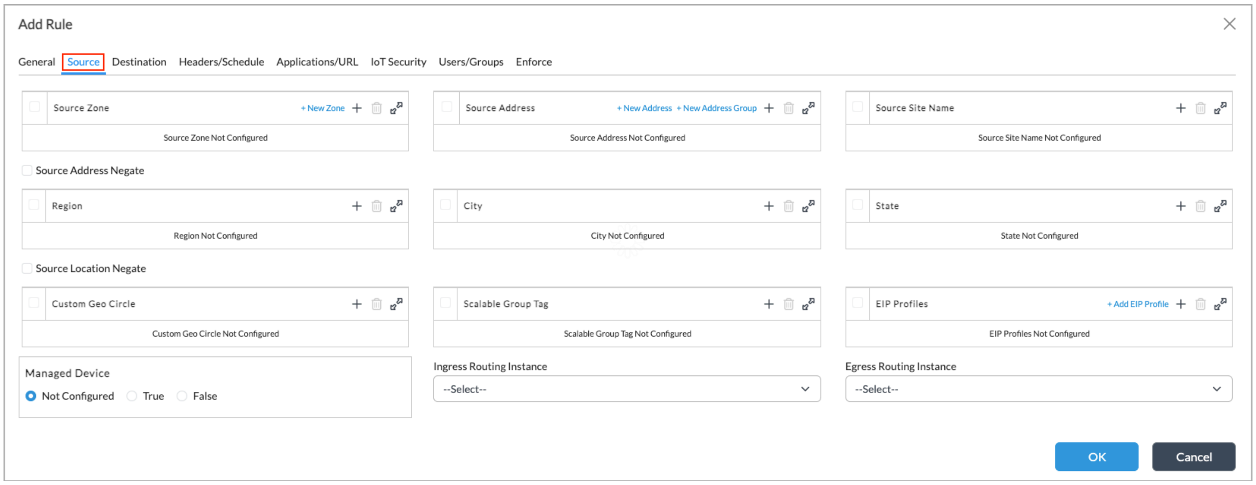
Tags

Alias Name

□ Disable Rule

Field	Description
Name	Enter a name for the access policy rule.
Description	Enter a brief description of the access policy rule.
Tags	Enter a keyword or phrase that you can use to filter the rule name. Tags are useful when you have many policies and want to view those that are tagged with a particular keyword.
Alias Name	(For Releases 21.2.1 and later.) Enter an alias name for the rule, if desired, up to a maximum of 63 characters (non-unique).
Rule Number	(For Releases 21.1 and earlier.) Enter a number which acts as an identifier for the rule. If you upgrade from Release 21.1 or earlier to Release 21.2.1 or later, the security access policy rule automatically sets the Alias Name value to the value configured previously for the Rule Number.
Disabled	(For Releases 21.1 and earlier.) Click to not activate the access policy rule after you configure it

8. Select the Source tab, and enter information for the following fields. (Note that for Releases 21.1 and earlier, the Source and Destination rule fields are on a single tab.)



Source Zone: Source Zone Not Configured

Source Address: Source Address Not Configured

Source Site Name: Source Site Name Not Configured

□ Source Address Negate

Region: Region Not Configured

City: City Not Configured

State: State Not Configured

□ Source Location Negate

Custom Geo Circle: Custom Geo Circle Not Configured

Scalable Group Tag: Scalable Group Tag Not Configured

EIP Profiles: EIP Profiles Not Configured

Managed Device: ● Not Configured ○ True ○ False

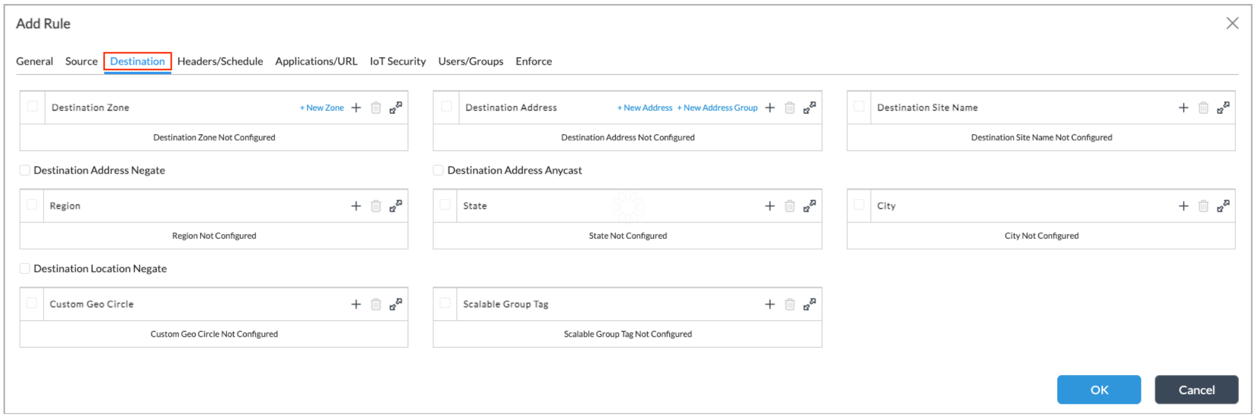
Ingress Routing Instance: --Select--

Egress Routing Instance: --Select--

Field	Description
Source Zone	Select the source zone to apply the rule to traffic coming from any interface in the specified zone. Click the ⊞ Add icon to add more source zones.
Source Address	Select and enter one or more source addresses to which to apply the DoS protection policy rule. Click the ⊞ Add icon to add more source addresses. (For Releases 20.2.2 and later.) For IPv4 addresses, you can enter a wildcard mask. 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 (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. You can configure overlapping wildcard addresses. A single session can match a maximum of 16 wildcard addresses. For more information, see [Configure Address Objects](https://docs.versa-networks.com). When you include multiple addresses in a rule, you cannot combine addresses of type FQDN, dynamic address and wildcard mask with regular IP address prefixes or ranges to create an address set to match as source or destination.
Source Site Name	Click the + Add icon and select the source site name to apply the rule to traffic coming from any interface in the specified zone. You can add multiple source site names.
Source Address Negate	Click to have the rule select any addresses except the

	configured addresses.
Region	Click the + Add icon to select a region.
City	Click the + Add icon to select a city.
State	Click the + Add icon to select a state.
Source Location Negate	Click to have the rule select any location except the configured locations.
Custom Geo Circle	Click the + Add icon to select a custom geographic circle, which consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. For more information, see Configure Geolocation Objects.
Scalable Group Tag	Click the + Add icon to select a scalable group tag.
EIP Profiles	Click the + Add icon and select an EIP profile. You can add multiple EIP profiles.
Managed Device	Select the management status of the source device. The options are: ◦ Not Configured ◦ True ◦ False
Ingress Routing Instance	Select the routing instance to use for incoming traffic.
Egress Routing Instance	Select the routing instance to use for outgoing traffic.

9. Select the Destination tab, and enter information for the following fields. (Note that for Releases 21.1 and earlier, the Source and Destination rule fields are on a single tab.)



Destination Zone

Destination Zone Not Configured

Destination Address

Destination Address Not Configured

Destination Site Name

Destination Site Name Not Configured

□ Destination Address Negate

□ Destination Address Anycast

Region

Region Not Configured

State

State Not Configured

City

City Not Configured

□ Destination Location Negate

Custom Geo Circle

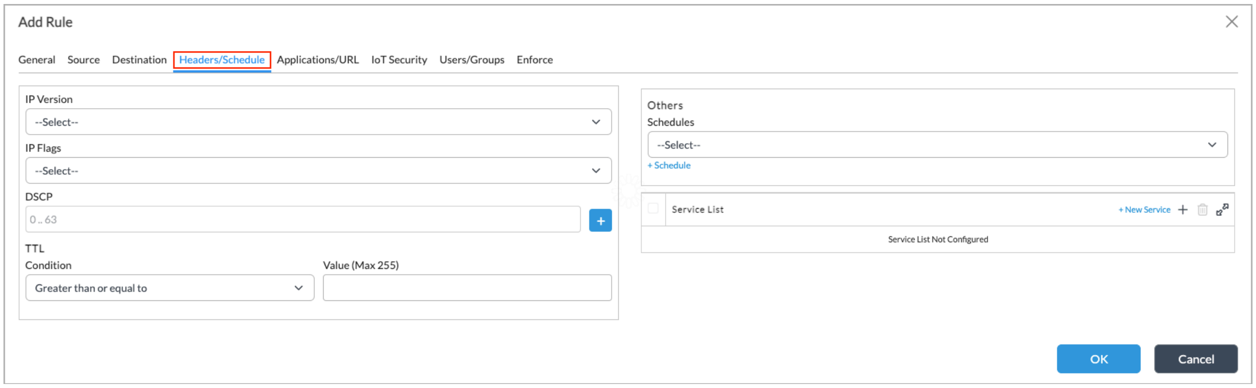
Custom Geo Circle Not Configured

Scalable Group Tag

Scalable Group Tag Not Configured

Field	Description
Destination Zone	Click the + Add icon and select the destination zone to apply the policy to traffic coming from all interfaces into a given zone. You can add multiple destination zones.
Destination Address	Click the + Add icon and select a destination addresses to which to apply the protection policy rule. You can add multiple destination addresses.
Destination Site Name	Click the + Add icon and select the destination site name to apply the policy to traffic coming from all interfaces into a given zone. You can add multiple destination site names.
Destination Address Negate	Click to have the rule select any addresses except the configured addresses.
Destination Address Anycast	Click to bypass geographic-location destination matches for anycast IP addresses.
Region	Click the + Add icon to select a region.
State	Click the + Add icon to select a city.
City	Click the + Add icon to select a state.
Destination Location Negate	Click to have the rule select any location except the configured locations.
Custom Geo Circle	Click the + Add icon to select a custom geographic circle, which consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. For more information, see Configure Geolocation Objects.
Scalable Group Tag	Click the + Add icon to select a scalable group tag.

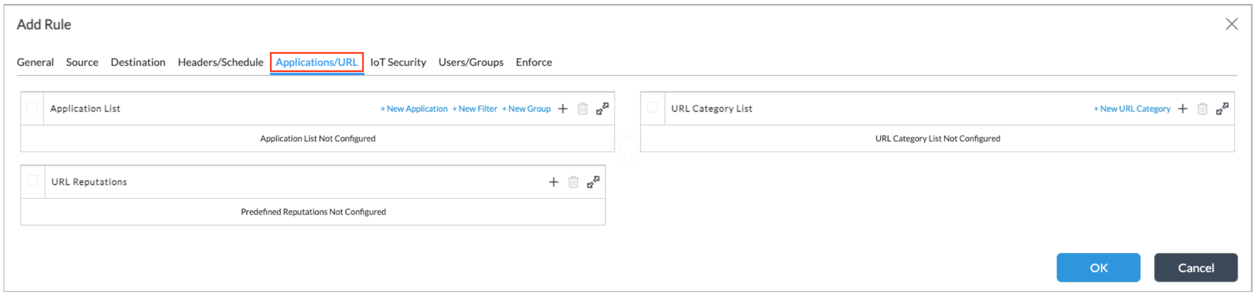
10. Select the Header/Schedule tab, and enter information for the following fields.


Add Rule
General
Source
Destination
Headers/Schedule
Applications/URL
IoT Security
Users/Groups
Enforce
IP Version
--Select--
IP Flags
--Select--
DSCP
0 .. 63
+
TTL
Condition
Greater than or equal to
Value (Max 255)
Others
Schedules
--Select--
+ Schedule
Service List
+ New Service
Service List Not Configured
OK
Cancel

Field	Description
IP Version	Select the IP version to which the security access rule applies, either IPv4 or IPv6..
IP Flags	Select an IP flag: ◦ Don’t Fragment ◦ More Fragment
DSCP	Enter a differentiated service code point (DSCP) value to classify how the IP packet is queued for forwarding, then click the + Add icon. You can enter multiple DSCP values. *Range*: 0 through 63 *Default*: None
TTL (Group of Fields)	
◦ Condition	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: ◦ 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
◦ Value	Enter the value for the TTL. *Range*: 1 through 255 *Default*: None
Others (Group of Fields)	

◦ Schedules	Select a schedule to set the time and frequency at which the rule is in effect. To create a new schedule, see Configure Schedule Objects.
Services	
◦ Service List	Click the + Add icon to select one or more services to apply the security access rule to the configured services.

11. Select the Applications/URL tab, and enter information for the following fields.



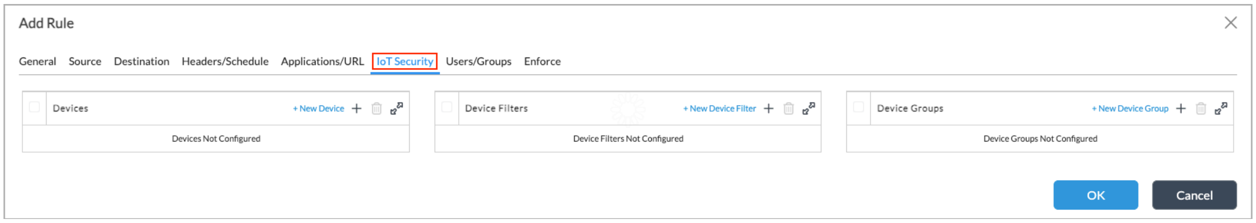
Application List Not Configured

URL Category List Not Configured

Predefined Reputations Not Configured

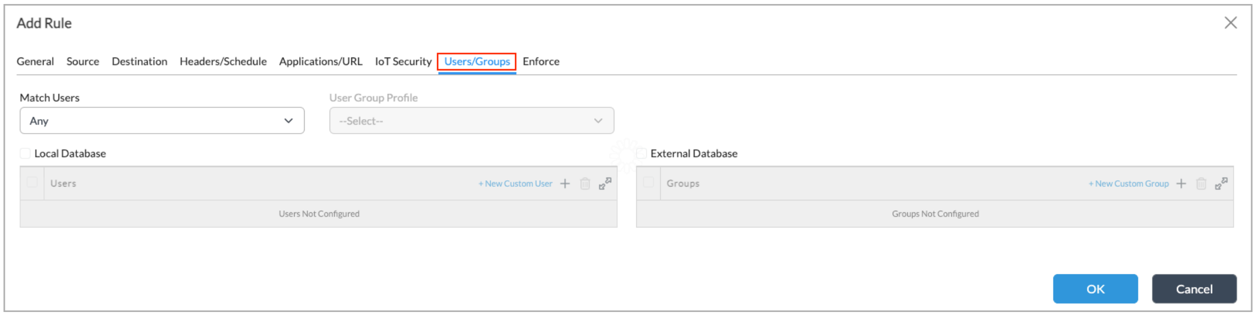
Field	Description
Application List	Click the + Add icon to select one or more predefined or custom application signatures and apply the security access rule to the application. To create an application, click + New Application. To create an application filter, click + New Filter. To create an application group, click + New Group.
URL Category List	Click the + Add icon to select one or more predefined or custom URL categories and apply the security access rule to the URL. To define a new category, click + New URL Category.
URL Reputations	(For Releases 21.2.1 and later.) Click the + Add icon to select one or more predefined reputations and apply the security access rule to the URL. For information about the predefined URL reputations, see View a Predefined URL Reputation.

12. (For Releases 22.1.3 and later.) Select the IoT Security tab and enter information for the following fields. For more information, see Configure IoT Security.



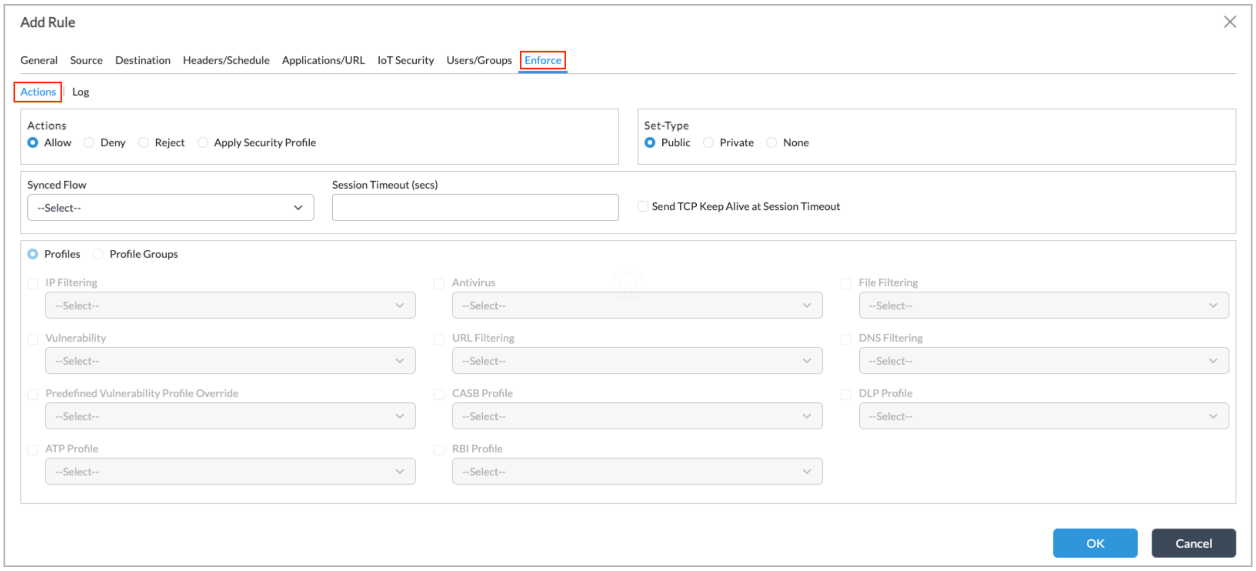
Field	Description
Devices	Click the + Add icon and select an IoT security device. Click + New Device to configure a new user-defined device.
Device Filters	Click the + Add icon and select an IoT security filter. Click + New Filter to configure a new user-defined device filter.
Device Groups	Click the + Add icon and select an IoT security device group. Click + New Device Group to configure a new user-defined device group.

13. Select the Users/Groups tab, and enter information for the following fields.



Field	Description
Match Users	Select a user to bind with the security policy: ◦ Any ◦ Known ◦ Unknown ◦ Selected Users Groups
User Group Profile	(Enabled only when you choose Selected Users Groups in the Match Users field.) Select the user group profile to match a group of users.
Local Database	(Enabled only when you select a user group profile in the User Group Profile field.) Click the + Add icon and select the local database for the selected user group.
External Database	Enabled only when you select a user group profile in the User Group Profile field.) Click the + Add icon and select the external database for the selected user group.

14. Select the Enforce tab, then click the Actions subtab and and enter information for the following fields. For log collection recommendations, see [Versa Analytics Scaling Recommendations](https://docs.versa-networks.com).


Add Rule

Actions: ● Allow ○ Deny ○ Reject ○ Apply Security Profile

Set-Type: ● Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout

● Profiles ○ Profile Groups

□ IP Filtering: --Select--

□ Antivirus: --Select--

□ File Filtering: --Select--

□ Vulnerability: --Select--

□ URL Filtering: --Select--

□ DNS Filtering: --Select--

□ Predefined Vulnerability Profile Override: --Select--

□ CASB Profile: --Select--

□ DLP Profile: --Select--

□ ATP Profile: --Select--

□ RBI Profile: --Select--

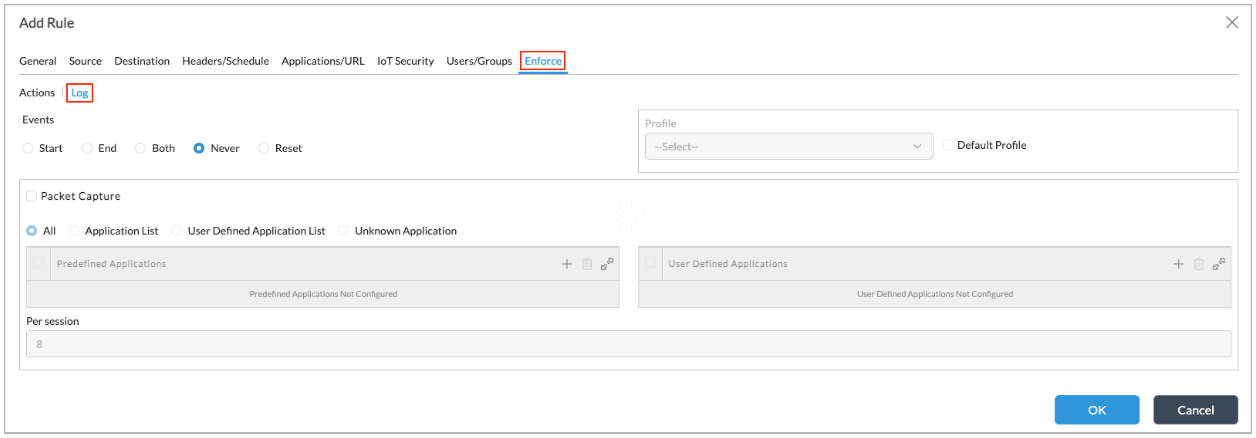
Field	Description
Actions	Select the action to take on matching traffic: ◦ Allow—Allow sessions that match the rule to pass. ◦ Apply Security Profile—Apply a security profile based on IP filtering, IP reputation, URL filtering, antivirus, vulnerability, and, for Releases 20.2 and later, DNS filtering. Traffic is allowed, if it is not blocked by any of the selected security profiles. ◦ Deny—Drop the sessions that match the rule. ◦ Reject—Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message.
Set Type	Select a type. The options are: ◦ Public ◦ Private ◦ None
Synced Flow	Select the action to take for a synced flow of session after an HA switchover: ◦ Allow—Allow the session to continue after the switchover, with a bare minimal subset of service modules that can handle the synced session. ◦ Deny—Drop all packets belonging to the matching synced sessions. ◦ Reject—Send a TCP reset (RST) or, for UDP, an ICMP unreachable message to the sender and tear down the matching synced sessions.
Session Timeout	Enter the timeout period, in seconds, after which to clear idle sessions. *Range*: 1 to 15999999 seconds *Default*: None

Send TCP Keepalive at Session Timeout	Click to send a TCP keepalive probe when the session times out.
Profiles (Group of Fields)	When you select the Apply Security Profile action, select the security access policy to enforce as the action.
◦ IP Filtering	Click, and then select a predefined IP-based filtering profile: ◦ Block Bad Traffic ◦ Block Bots ◦ Block DoS ◦ Block Scanners ◦ Block Spam ◦ Block Windows Exploits ◦ Versa Recommended Profile ◦ Web Protection
◦ Antivirus	Click, and then select a predefined antivirus profile: ◦ Scan Email traffic ◦ Scan Web and Email traffic ◦ Scan Web traffic
◦ File Filtering	Click, and then select a predefined or a user-defined file-filtering profile.
◦ Vulnerability	Click, and then select a predefined traffic vulnerability: ◦ All Anomaly Rule ◦ All Attack Rules Caution: Do not select All Attack Rules if the device has only 8 GB of RAM, because enforcing this rule might use most of the device's memory, leaving very little for sessions and other operations. ◦ Client Protection ◦ Database Profile ◦ ICS Profile ◦ IoT Profile ◦ Lateral Movement Detection

	◦ Linux OS Profile ◦ MAC OS Profile ◦ Malware Profile ◦ Server Protection ◦ Versa Branch Profile ◦ Versa-Recommended Profile ◦ Windows OS Profile ◦ User-Defined Profiles
◦ URL Filtering	Click, and then select a predefined URL-filtering profile: ◦ Allow All ◦ Block All ◦ Block All Adult ◦ Block All Adult and Ads ◦ Block All Adult, Games, and Ads ◦ Block All Communication ◦ Block All Mail ◦ Block Mail and Communication ◦ Corporate
◦ Predefined Vulnerability Profile Override	Click, and then select an override for the predefined vulnerability profile. Note: Versa Networks provides predefined vulnerability profiles in security package (SPack) updates. All tenants can use the predefined vulnerability profiles.
◦ DNS Filtering	(For Releases 20.2 and later.) Click, and then select a predefined or a user-defined DNS-filtering profile. The following option is available: ◦ Versa Recommended
◦ Predefined Vulnerability Profile Override	Not currently supported.
◦ CASB Profile	Select a user-defined profile.

◦ DLP Profile	Select a user-defined profile.
◦ ATP Profile	Select a user-defined profile.
◦ RBI Profile	Select a profile.
◦ Profile Groups	(For Releases 20.2.1 and later.) Click, and then select a user-defined or predefined profile group: ◦ Versa Recommended AV IPS ◦ Versa recommended AV IPS

15. Click the Logs subtab, then enter the following information.



Events

○ Start ○ End ○ Both ● Never ○ Reset

Profile: --Select-- □ Default Profile

□ Packet Capture

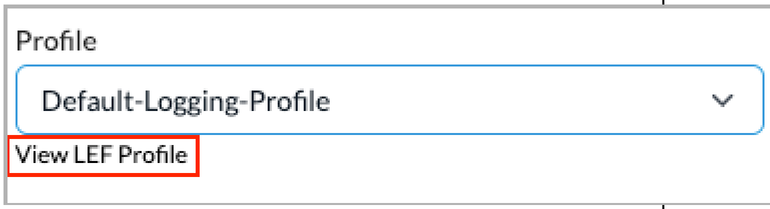
● All ○ Application List ○ User Defined Application List ○ Unknown Application

Predefined Applications Not Configured

User Defined Applications Not Configured

Per session: 8

Field	Description
Events	Select an option to log the data: ◦ Start—Log data at the start of each session. ◦ End—Log data at the end of each session. ◦ Both—Log data at the start and end of each session. ◦ Never—Never log data. ◦ Reset—Reset the logging option.
Profile	Select the log export functionality (LEF) profile to associate with the policy or click Default Profile to use the default LEF profile instead. Logs are sent to the active collector of the LEF profile. For information

Field	Description
	about configuring a LEF profile and assigning a default LEF profile, see Configure Log Export Functionality. For information about associating a LEF profile with a feaure or service, see Apply Log Export Functionality. Once selected, you can click View LEF Profile to see the details of the profile.  Profile Default-Logging-Profile View LEF Profile
Packet Capture (Group of Fields)	Click Packet Capture, and then select the application type to which to apply the security profile ◦ All ◦ Application List ◦ User-Defined Application List ◦ Unknown Application For each category, select one of the following options: ◦ Predefined Applications—Click to select a predefined application. User Defined Applications—Click to select a custom-defined application. ◦ Packet capture information is automatically sent to Analytics nodes, where you can view and download it. For more information, see View Analytics Dashboards and Log Screens.
◦ Per Session	Enter the number of sessions allowed per log. *Range*: 1 through 20 *Default*: 8

16. Click OK.

Configure Log Export for NGFW

You can configure logging control for NGFW to export statistics about NGFW security parameters to an Analytics node. You can export a summary of all statistics, which is the default, or you can export session statistics.

Summary statistics logs include statistics about the following:

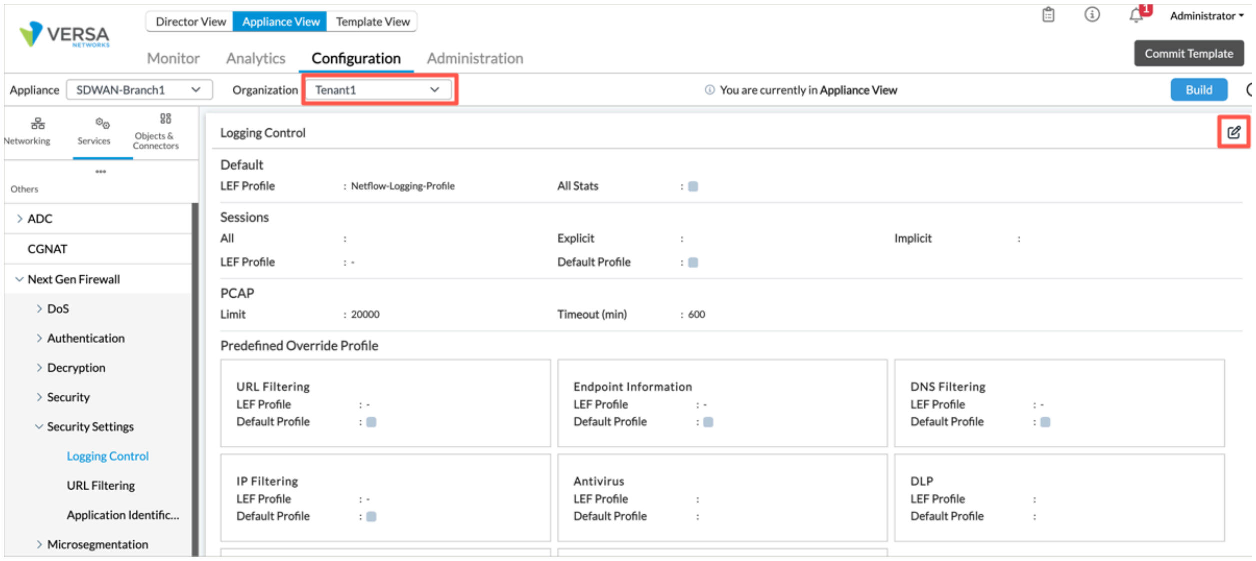
- Applications categorized based on risk, productivity, family, and subfamily
- Destination IP addresses
- Device identification
- Firewall rules
- Forwarding classes
- Source IP addresses
- URL categories
- URL reputation
- Zones

Sessions statistics include firewall access logs for all sessions. To reduce the number of logs from a device, it is recommended that you do not enable all session logs.

You can also set the packet capture (PCAP) limit and timeout for logs. If you enable PCAP logging in an NGFW security rule, these PCAP settings are used by default. For more information, see Configure a Security Access Policy, above.

To configure the type of NGFW security logs to export:

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 a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security Settings > Logging Control in the left menu bar, and then select an organization from the drop-down menu in the horizontal menu bar.



Appliance: SDWAN-Branch1
Organization: Tenant1

Logging Control

Default
LEF Profile : Netflow-Logging-Profile
All Stats :

Sessions
All :
Explicit :
Implicit :
LEF Profile : -
Default Profile :

PCAP
Limit : 20000
Timeout (min) : 600

Predefined Override Profile

URL Filtering
LEF Profile : -
Default Profile :

Endpoint Information
LEF Profile : -
Default Profile :

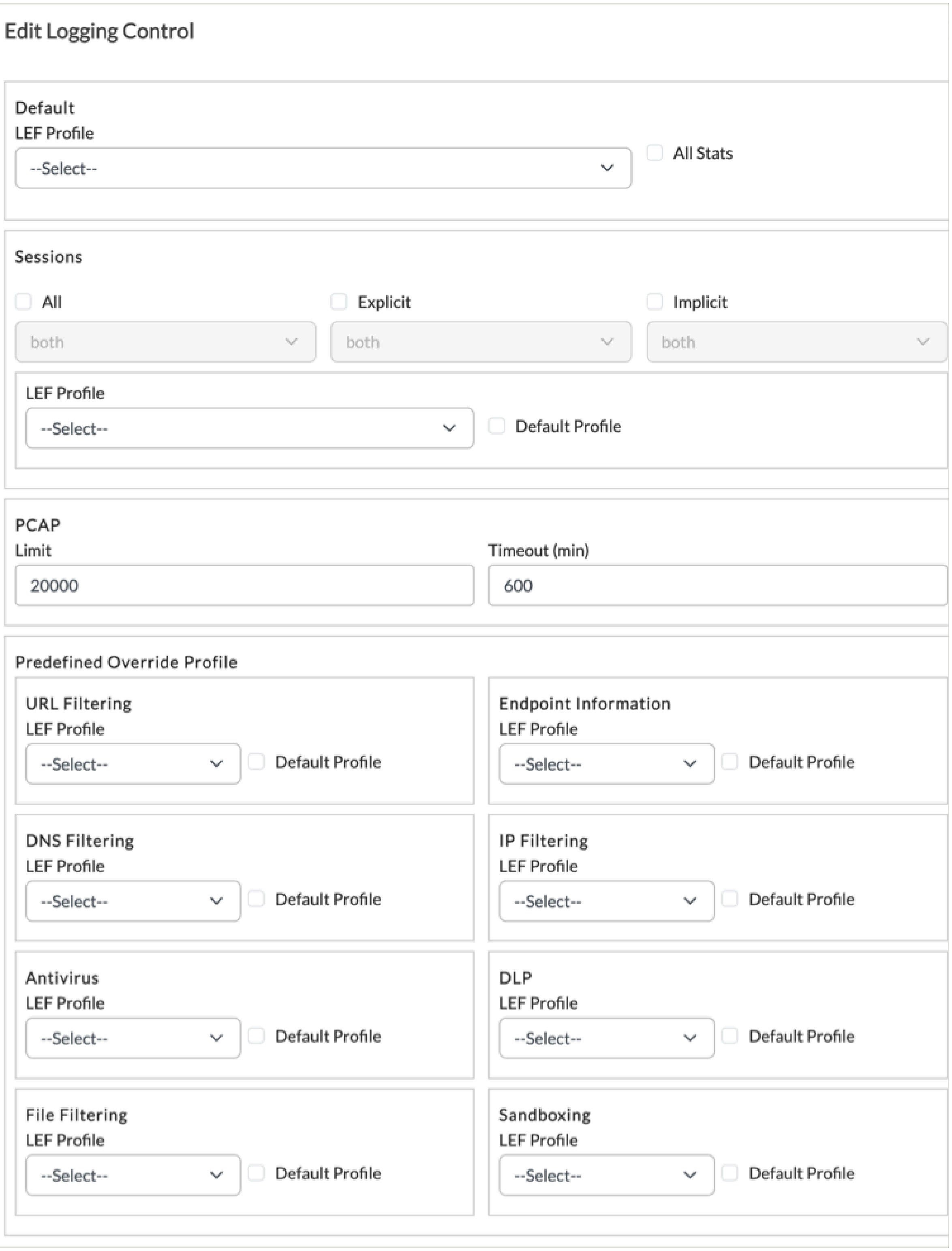
DNS Filtering
LEF Profile : -
Default Profile :

IP Filtering
LEF Profile : -
Default Profile :

Antivirus
LEF Profile :
Default Profile :

DLP
LEF Profile :
Default Profile :

4. Click the Edit icon. In the Edit Logging Control popup window, enter information for the following fields.



Edit Logging Control

Default

LEF Profile: --Select-- □ All Stats

Sessions

□ All: both
□ Explicit: both
□ Implicit: both

LEF Profile: --Select-- □ Default Profile

PCAP

Limit: 20000
Timeout (min): 600

Predefined Override Profile

URL Filtering
LEF Profile: --Select-- □ Default Profile

Endpoint Information
LEF Profile: --Select-- □ Default Profile

DNS Filtering
LEF Profile: --Select-- □ Default Profile

IP Filtering
LEF Profile: --Select-- □ Default Profile

Antivirus
LEF Profile: --Select-- □ Default Profile

DLP
LEF Profile: --Select-- □ Default Profile

File Filtering
LEF Profile: --Select-- □ Default Profile

Sandboxing
LEF Profile: --Select-- □ Default Profile

Field	Description
Default (Group of Fields)	(For Releases 22.1.1 and later.) Select a LEF profile to use for NGFW logs.
◦ LEF Profile	Select a LEF profile. NGFW logs are sent to the active LEF collector configured in the LEF profile.
◦ All Stats	Click to enable the export of all NGFW statistics. These statistics display as aggregate statistics on the Analytics Security dashboard.
Sessions (Group of Fields)	Select the logs to export.
◦ All	Click to log all traffic flows, and then select when to export the logs: ◦ Start—Export the logs at the beginning of the traffic flow. ◦ End—Export the logs at the end of the traffic flow. ◦ Both—Export the logs at the beginning and end of the traffic flow. Selecting this option disables the Explicit and Implicit options.
◦ Explicit	Click to enable logging when the traffic matches a rule, and then select when to export the logs: ◦ Start—Export the logs at the beginning of the traffic flow. ◦ End—Export the logs at the end of the traffic flow. ◦ Both—Export the logs at the beginning and end of the traffic flow.
◦ Implicit	Click to enable logging even when the traffic matches no rule, and then select when to export the logs: ◦ Start—Export the logs at the beginning of the traffic flow. ◦ End—Export the logs at the end of the traffic flow. ◦ Both—Export the logs at the beginning and end of the traffic flow.

◦ LEF Profile	(For Releases 22.1.1 and later.) Select a LEF profile to use to export security session logs to the active LEF collector for the profile.
◦ Default Profile	(For Releases 22.1.1 and later.) Click to export security session logs to the active LEF collector for the default LEF profile.
PCAP (Group of Fields)	Configure packet capture parameters.
◦ Limit	Enter the number of packets to capture across the sessions. *Range*: 1000 through 50000 *Default*: 20000
◦ Timeout	Enter the time, in seconds, after which packet capture resumes. *Range*: 300 through 6000 seconds *Default*: 600 seconds
Predefined Override (Group of Fields)	(For Releases 22.1.1 and later.) Select LEF profiles to use with predefined vulnerability profile overrides.
◦ URL Filtering	Select a LEF profile to use to export URL-filtering logs when predefined override rules apply to the logs.
◦ Endpoint Information	Select a LEF profile to use to export endpoint information profile (EIP) logs when predefined override rules apply to the logs.
◦ DNS Filtering	Select a LEF profile to use to export DNS-filtering logs when predefined override rules apply to the logs.
◦ IP Filtering	Select a LEF profile to use to export IP-filtering logs when predefined override rules apply to the logs.
◦ Antivirus	Select a LEF profile to use to export antivirus logs when predefined override rules apply to the logs.
◦ DLP	Select a LEF profile to use to export data loss prevention (DLP) logs when predefined override rules apply to the logs.

◦ File Filtering	Select a LEF profile to use to export file-filtering logs when predefined override rules apply to the logs.
◦ Sandboxing	Select a LEF profile to use to export sandboxing logs when predefined override rules apply to the logs.
LEF Profile	(For Releases 21.2 and earlier.) Select a LEF profile. NGFW logs are sent to the active collector of the LEF profile. For information about configuring a LEF profile and assigning a default LEF profile, see Configure Log Export Functionality. For information about associating a LEF profile with a feature or service, see Apply Log Export Functionality.
All Stats	(For Releases 21.2 and earlier.) Click to enable the export of all NGFW statistics. These statistics display as aggregate statistics on the Analytics Security dashboard. Logs are sent to the active collector of the LEF profile selected in the LEF profile field. For information about forwarding NGFW logs, see Apply Log Export Functionality.

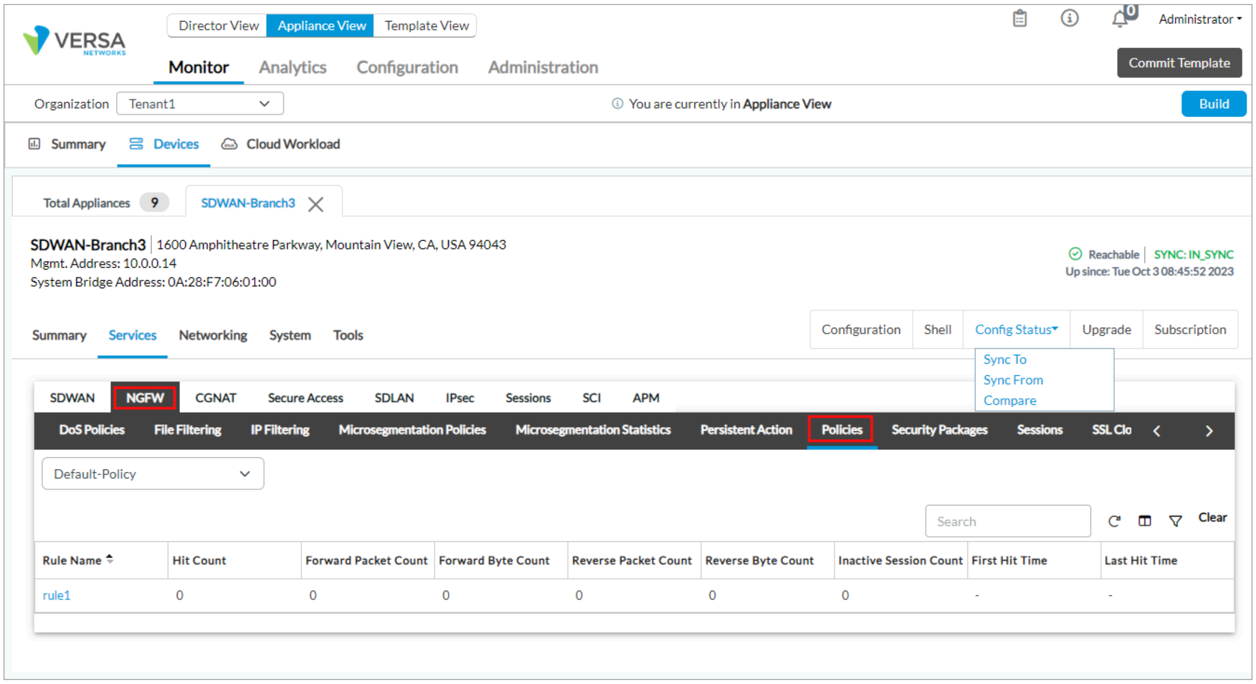
5. Click OK.

Monitor NGFW Policies

NGFW policy includes all the match criteria of a stateful firewall policy as well as Layer 7 match criteria such as application and URL category. You monitor NGFW policies to view the traffic flow details when a policy is used.

To monitor NGFW policies:

1. Select the Administration tab in the top menu bar.
    a. Select Appliances in the left menu bar.
    b. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a provider organization in the left menu bar.
4. Select the Services tab in the horizontal menu bar.
5. Select NGFW > Policies.



SDWAN-Branch3 | 1600 Amphitheatre Parkway, Mountain View, CA, USA 94043
Mgmt. Address: 10.0.0.14
System Bridge Address: 0A:28:F7:06:01:00

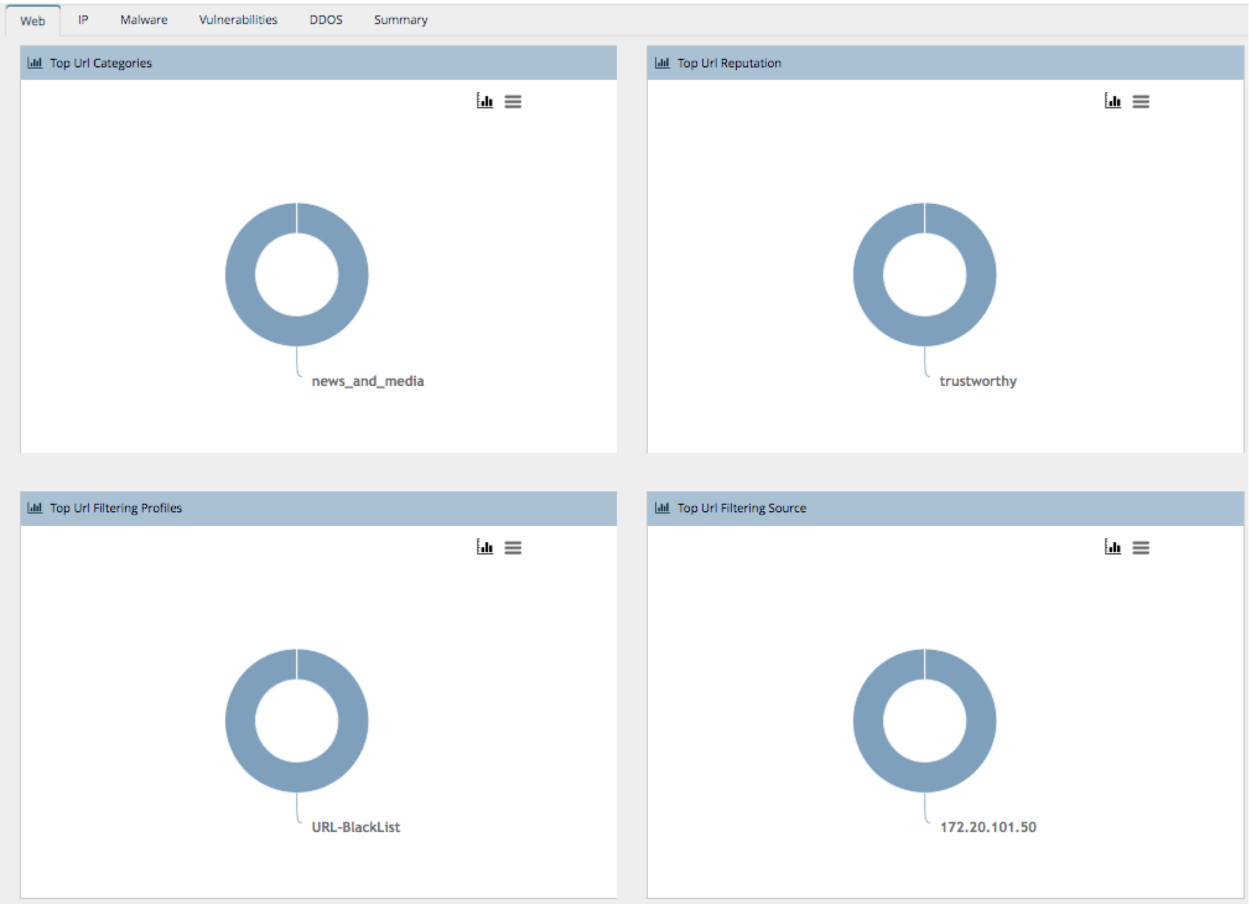
Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
rule1	0	0	0	0	0	0	-	-

6. Select the policy to monitor. Note that the File Filtering tab is available only for Releases 20.2 and later. For more information, see Services > NGFW in the Monitor Device Services article.

Monitor Threats

To view threat monitoring reports generated by NGFW:

1. In Director view, select the Analytics tab in the top menu bar.
2. Select Home > Security > Threats in the left menu bar to view the dashboard.
3. Select the Web tab to view reports for URL filtering and URL Filtering profiles. The dashboard displays the following panes:
   - Top URL Categories
   - Top URL Reputation
   - Top URL Filtering Profiles
   - Top URL Filtering Source



For more information about NGFW threat monitoring, see Threat Monitoring in the Security Dashboards article.

Supported Software Information

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

- Releases 20.2.1 and later support profile groups.
- Releases 21.2.1 and later support configuring rule order and URL reputations in secure access policies.
- Releases 22.1.1 and later support streaming of NGFW security session logs to a non-default LEF profile. You can select a LEF profile for predefined overrides.
- Releases 22.1.4 and later support configuring destination address matches for Anycast IP addresses.

Additional Information

Apply Log Export Functionality
Configure Address Objects
Configure DoS Protection

Configure File Filtering
Configure Layer 7 Objects
Configure Log Export Functionality
Configure Schedule Objects
Configure Security Profile Groups
Configure Stateful Firewall
Configure URL Filtering
Configure User and Group Policy
Monitor Device Services
Security Dashboards
Versa Analytics Scaling Recommendations
View Analytics Dashboards and Log Screens