
Configure Service Objects

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

In the Versa Operating System™ (VOS™) software, security policies can reference service objects, which define match criteria based on protocol name and number, and on source and destination port number. The Versa Security Research team provides default predefined services and object definitions, and periodically provides security packages (SPacks) to update the default services and objects.

You can also create custom service objects. One reason to do this might be if a well-known service runs on a non-standard port or if the predefined services are missing a desired port and protocol combination. Another reason might be to limit the number of ports that an application can use. For example, you could limit FTP to use only port 21 instead of using both ports 20 and 21.

The custom service objects that you define for a tenant can be used only by that tenant, and they are not visible or available to any other tenants.

View Predefined Services

The Versa Security Research team defines predefined services and object definitions, which are essentially factory defaults. Versa periodically updates these predefined services and object definitions in security packages (SPacks). You can use the security package to update the predefined objects at any time, without any operational impact to the Director node or to VOS devices.

To provide feedback about the predefined objects, including input about adding or modifying them, send email to support@versa-networks.com.

To view the predefined services 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. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > Services to view the list of predefined service objects.

The screenshot shows the Versa Networks configuration interface. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. The left sidebar shows a menu with 'Endpoint Protection', 'File Filtering Profile', 'IP Filtering Profile', 'IP Reputations', 'Operating System', 'Proxy Apps', 'Regions', 'SASE Applications', 'SASE Client', 'Services' (selected), 'States', 'URL Categories', 'URL Filters', and 'URL Profiles'. The main panel displays a table of service objects with the following columns: Name, Protocol, Protocol Value, Source Port, and Destination Port. The table contains 12 rows of data.

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
echo	tcp	6	any	7
echo	udp	17	any	7
discard	tcp	6	any	9
discard	udp	17	any	9

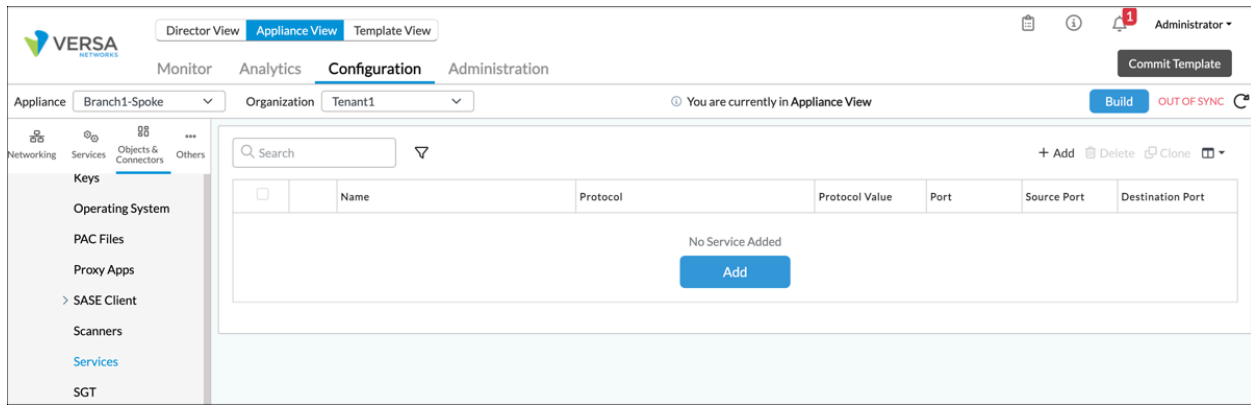
4. Click the Column Filter icon to restrict the columns to display in the table.
5. Click the Filter icon to filter the display by the protocol name, protocol value, source port, and destination port.

Configure Custom Service Objects

You can create custom service objects, for example, if a well-known service runs on a non-standard port or if the predefined services are missing the desired port and protocol combination.

To create a custom service object:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. 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.



4. Click + Add in the main pane to add a custom service. In the Add Service window, enter information for the following fields.

×

Add Service

Name *

Description

Tags

☒ Protocol

☐ Protocol Value

Protocol *

TCP

Protocol Value

0..255

☐ Port Range

☒ Source/Destination Port

☐ ICMP

Port ⓘ

Source Port

ICMP Type

Use /- for values/ranges

Destination Port

ICMP Code

Use /- for values/ranges

OK

Cancel

Field	Description
Name	Enter a name for the custom service object.
Description	Enter a text description for the custom service object.
Tags	Enter a text string to describe the custom service object.
Protocol	<p>Click to define a custom service object by protocol name. Then, in the Protocol field, select the protocol:</p> <ul style="list-style-type: none"> ◦ AH ◦ ESP ◦ ICMP ◦ ICMPv6 (for Releases 22.1.1 and later.) ◦ TCP ◦ TCP or UDP ◦ UDP
Protocol Value	Click to define a custom service object by protocol number. Then, in the Protocol Value field, enter the number of the protocol.
Port Range	Click to configure a port range for the custom service object. Then, in the Port field, enter the port number range. You can enter a single port number (for example, 20000), multiple comma-separated port numbers (for example, 20000,22000,5600), or a hyphen-separated range of port numbers (for example, 20000-22000).
Source/Destination Port	Click to associate the custom service object with a single source or destination port, or with a combination of source and destination ports. Then, in the Source Port and Destination Port fields, enter the port numbers. You can enter a single port number (for example, 20000), multiple comma-separated port numbers (for example, 20000,22000,5600), or a hyphen-separated range of port numbers (for example, 20000-22000).
ICMP	(For Releases 22.1.1 and later.) If you select the

	<p>ICMP or ICMPv6 protocol, click to define a custom service object by ICMP values:</p> <ul style="list-style-type: none"> ◦ ICMP Code—Enter the ICMP code. You can enter an individual value, a comma-separated list of values, or a range of values. ◦ 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).
--	--

5. Click OK.

Apply a Service Object to an Access Policy

You can apply a service object to a security access policy to define a security policy. To define and configure a security access policy, see [Configure Security Access Policy Rules](#).

To apply a service object to an access policy:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and then select the Rules tab.

The screenshot shows the Versa Networks Director web interface. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The 'Configuration' tab is selected. The left sidebar shows a tree view with 'Next Gen Firewall' expanded, and 'Policies' selected. The main panel displays a table of rules under the 'Rules' tab.

Rule Num	Name	Rule Disabled	Alias Name	Enforce	Services	Applications	URL
1	Allow-To-Analytics	False		Allow	Custom: Analytics-Servi...		
2	Allow-From-CPE-Ports	False		Allow	Custom: CPE-Ports, SN...		
3	Allow-ICMP	False		Allow	Predefined: ICMP		
4	Deny-to-ControlNetZo...	False		Deny			
5	Allow-All	False		Allow			

Rows per page: 25 Showing 1 - 5 of 5

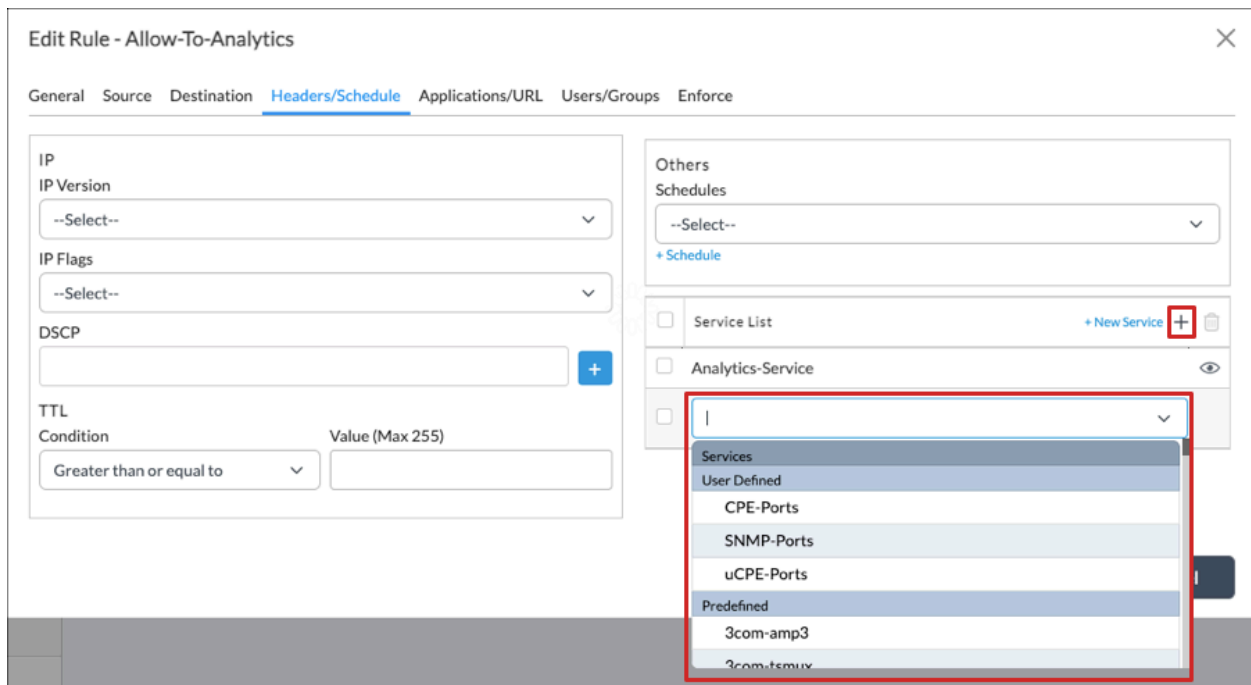
4. Click a security access policy rule name in the main pane. The Edit Rule popup window displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Servic...

Updated: Wed, 23 Oct 2024 08:17:45 GMT

Copyright © 2024, Versa Networks, Inc.

5. Select the Headers/Schedule tab.



6. In the Service List table, select the + Add icon, and then select a service object.
7. Click OK.

Configuration Example

The following example shows how to deny HTTP traffic based on a service object and associated access policy rule and how to monitor the effects of the rule.

To configure the service object:

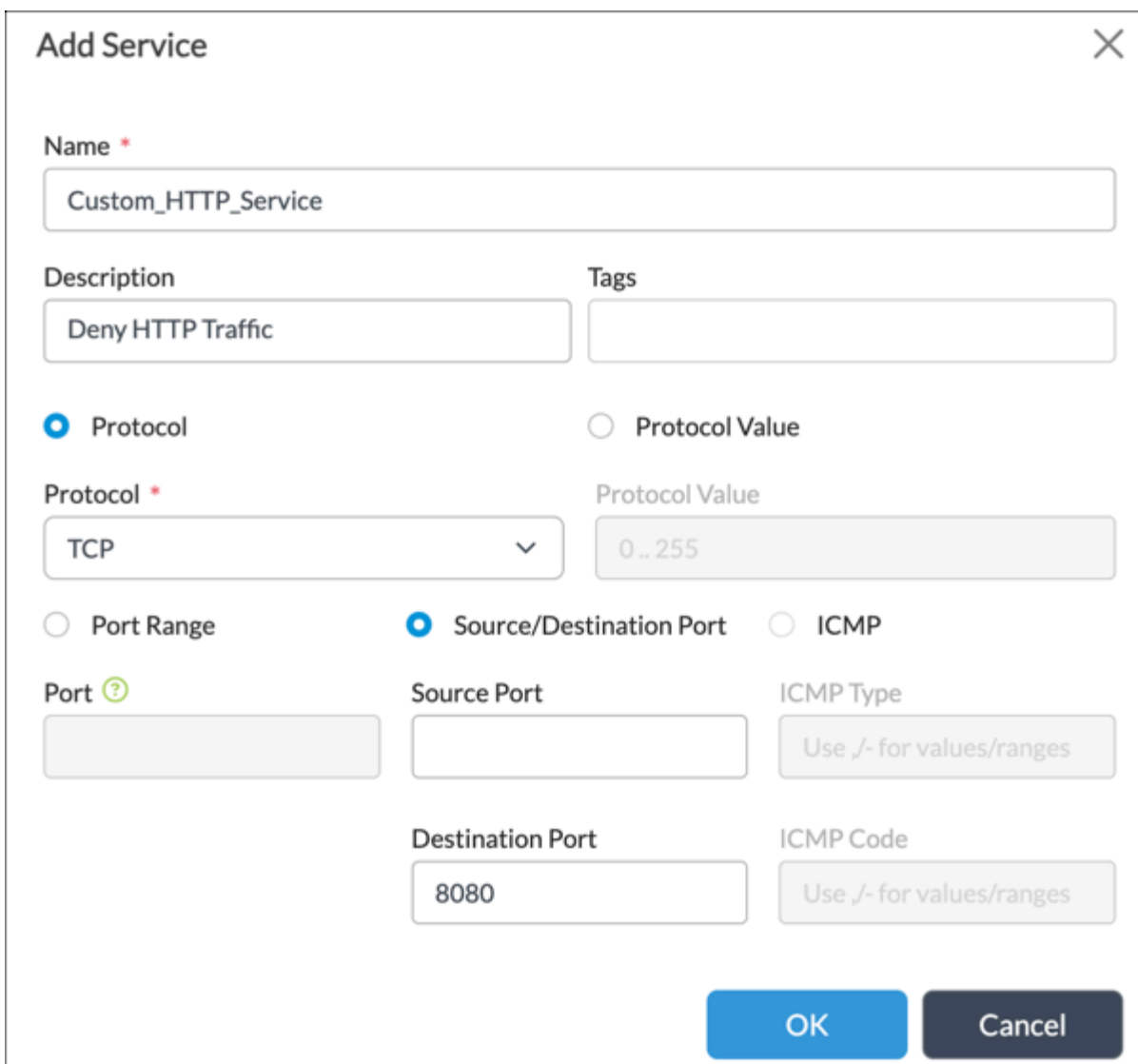
1. In Director view:
 1. Select the Administration tab in the top menu bar.
 2. Select Appliances in the left menu bar.
 3. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Services in the left menu bar.
4. Select + Add.
5. In the Add Service popup window, add a service object.
 - a. Enter a name for the service object. In the example here, the name is Custom_HTTP_Service.
 - b. Click the Protocol field, and select TCP as the protocol.
 - c. Click the Source/Destination field, and enter a value for Destination Port. In the example, the port is 8080.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Servic...

Updated: Wed, 23 Oct 2024 08:17:45 GMT

Copyright © 2024, Versa Networks, Inc.

- d. Click OK.

The image shows a 'Add Service' dialog box with a close button (X) in the top right corner. It contains several input fields and radio buttons. The 'Name' field is labeled 'Name *' and contains the text 'Custom_HTTP_Service'. Below it are 'Description' and 'Tags' fields; 'Description' contains 'Deny HTTP Traffic'. There are two radio buttons: 'Protocol' (selected) and 'Protocol Value'. Below 'Protocol' is a dropdown menu showing 'TCP'. Below 'Protocol Value' is a text field containing '0..255'. There are three more radio buttons: 'Port Range', 'Source/Destination Port' (selected), and 'ICMP'. Below 'Port Range' is a disabled 'Port' field with a question mark icon. Below 'Source/Destination Port' are 'Source Port' and 'Destination Port' fields; 'Destination Port' contains '8080'. Below 'ICMP' are 'ICMP Type' and 'ICMP Code' fields, both with placeholder text 'Use /- for values/ranges'. At the bottom right are 'OK' and 'Cancel' buttons.

Add Service

Name *
Custom_HTTP_Service

Description
Deny HTTP Traffic

Tags

☒ Protocol ☐ Protocol Value

Protocol *
TCP

Protocol Value
0..255

☐ Port Range ☒ Source/Destination Port ☐ ICMP

Port ?
[disabled]

Source Port
[empty]

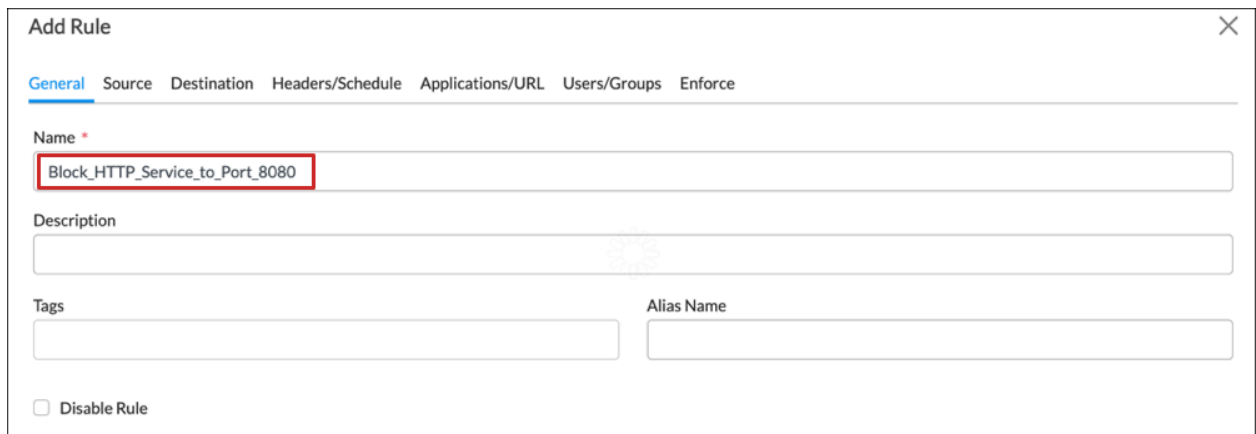
Destination Port
8080

ICMP Type
Use /- for values/ranges

ICMP Code
Use /- for values/ranges

OK Cancel

6. Click OK.
7. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and select the Rules tab.
8. Click + Add. The Add Rule popup window displays.
9. Create an access policy rule that includes the scheduled object.
- a. Select the General tab, and then enter the name of the access policy rule, here, Block_HTTP_Service_to_Port_8080.



Add Rule [X]

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

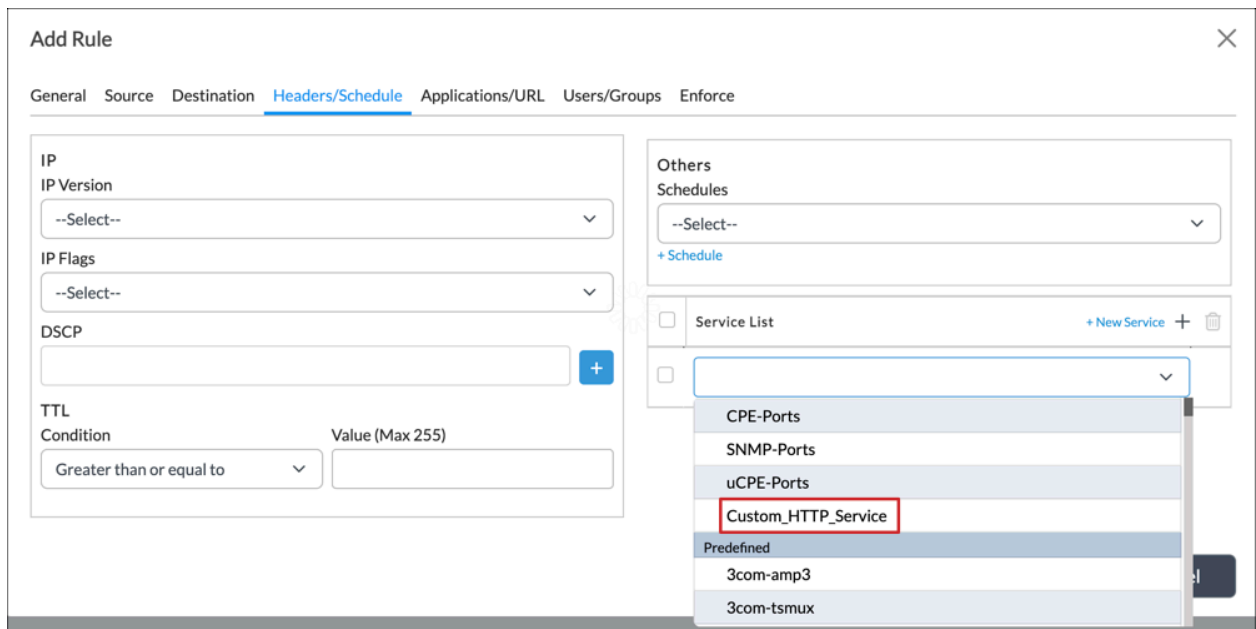
Name *
Block_HTTP_Service_to_Port_8080

Description

Tags Alias Name

☐ Disable Rule

- b. Select the Headers/Schedule tab, and then select the service you created in Step 5, here, Custom_HTTP_Service.



Add Rule [X]

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

IP
IP Version: --Select--
IP Flags: --Select--
DSCP: [] +
TTL
Condition: Greater than or equal to Value (Max 255): []

Others
Schedules: --Select--
+ Schedule

Service List: + New Service + [X]
CPE-Ports
SNMP-Ports
uCPE-Ports
Custom_HTTP_Service
Predefined
3com-amp3
3com-tsmux

- c. Select the Enforce tab, and then select Deny under Action.

d. Click OK to creates a rule that denies HTTP traffic to port 8080.

To see how the service object associated with a policy affects the traffic flow, you monitor the policy:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. 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 Organization field
4. Select the Services tab in the horizontal menu bar.
5. Select NGFW > Policies. The NGFW policy statistics display, and the Rule Name column displays statistics about the access policy rule that you created.

Monitor
Analytics
Configuration
Administration
Commit Template

Organization
Provider
You are currently in Appliance View
Build

Controller1
2550 Great America Way Suite 350 Santa Clara ca United States 95054
Mgmt. Address: 10.40.233.210
System Bridge Address: 0A:28:E9:D2:01:00
Reachable | SYNC: IN_SYNC Up since: Mon Mar 27 14:24:45 2023

Summary
Services
Networking
System
Tools
Configuration
Shell
Config Status
Upgrade
Subscription

ADC
NGFW
Secure Access
SDLAN
Sessions
APM
Policies
Security Packages
Sessions
SSL Cloud
URL Filtering
User Identification
Vulnerability
Vulnerability Signature
Web Proxy
Zone Protection

Default-Policy
Search
Clear

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
Allow-To-Analytics	0	0	0	0	0	0	-	-
Allow-From-CPE-Ports	665	91471	12266197	211034	16999249	665	Mon Mar 27 15:43:51 2023	Tue Jun 27 11:58:59 2023
Allow-ICMP	0	0	0	0	0	0	-	-
Deny-to-ControlNetZone	0	0	0	0	0	0	-	-
Allow-All	11201769	251985028	22810888299	135731494	35561073431	11201700	Mon Mar 27 14:25:39 2023	Wed Jun 28 17:09:10 2023
Block_HTTP_Service_to_Por...	0	0	0	0	0	0	-	-

Supported Software Information

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

- Release 22.1.1 adds support for ICMPv6. You can specify the ICMP type and code for ICMPv4 and ICMPv6 custom service objects.

Additional Information

- [Configure Stateful Firewall](#)
- [Monitor Device Services](#)
- [Use Security Packages](#)