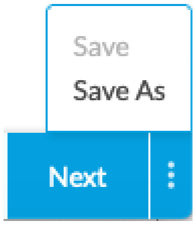
Configure Traffic-Steering Policies and Rules

For supported software information, click here.

To add traffic-steering policies and rules, you first create an application policy to classify incoming traffic based on match criteria, such as application, source IP address, destination IP address, and incoming zone. Then, you specify the action to take when traffic matches the configured criteria.

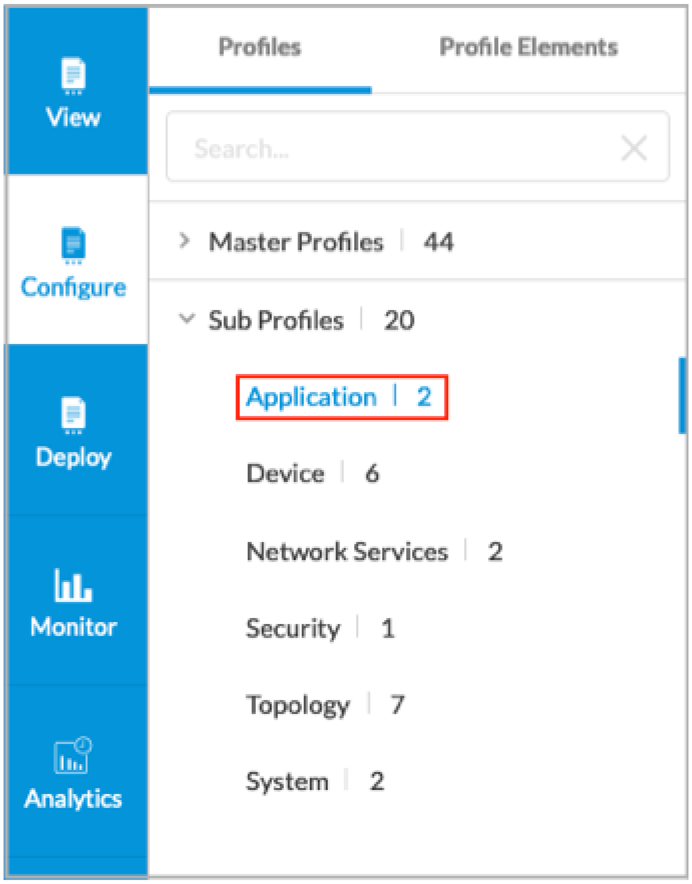
Traffic-steering policies and rules belong to the Application subprofile type. You can attach only one traffic-steering policy to an Application subprofile. You can add a traffic-steering policy to an existing Application subprofile, or you can add it when you create a new subprofile. You can add a traffic-steering policy as a profile element that can then be used in one or more Application subprofiles.

You can build reusable application policies by navigating to Policies > Application > Traffic Steering. You can also build policies and rules inline. These inline rules apply only to the policies currently being configured. You cannot reuse them in other subprofiles until you add them to the reusable Subprofiles folder by clicking the ellipsis to the right of Next and then selecting Save As:

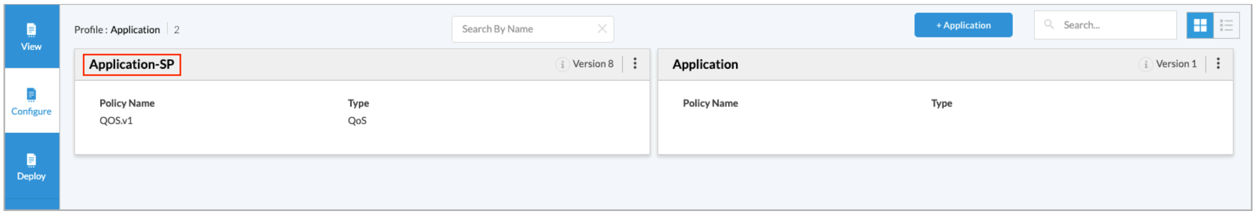


To add a traffic-steering policy to an existing Application subprofile:

1. Go to Configure > Profiles > Sub Profiles > Application.



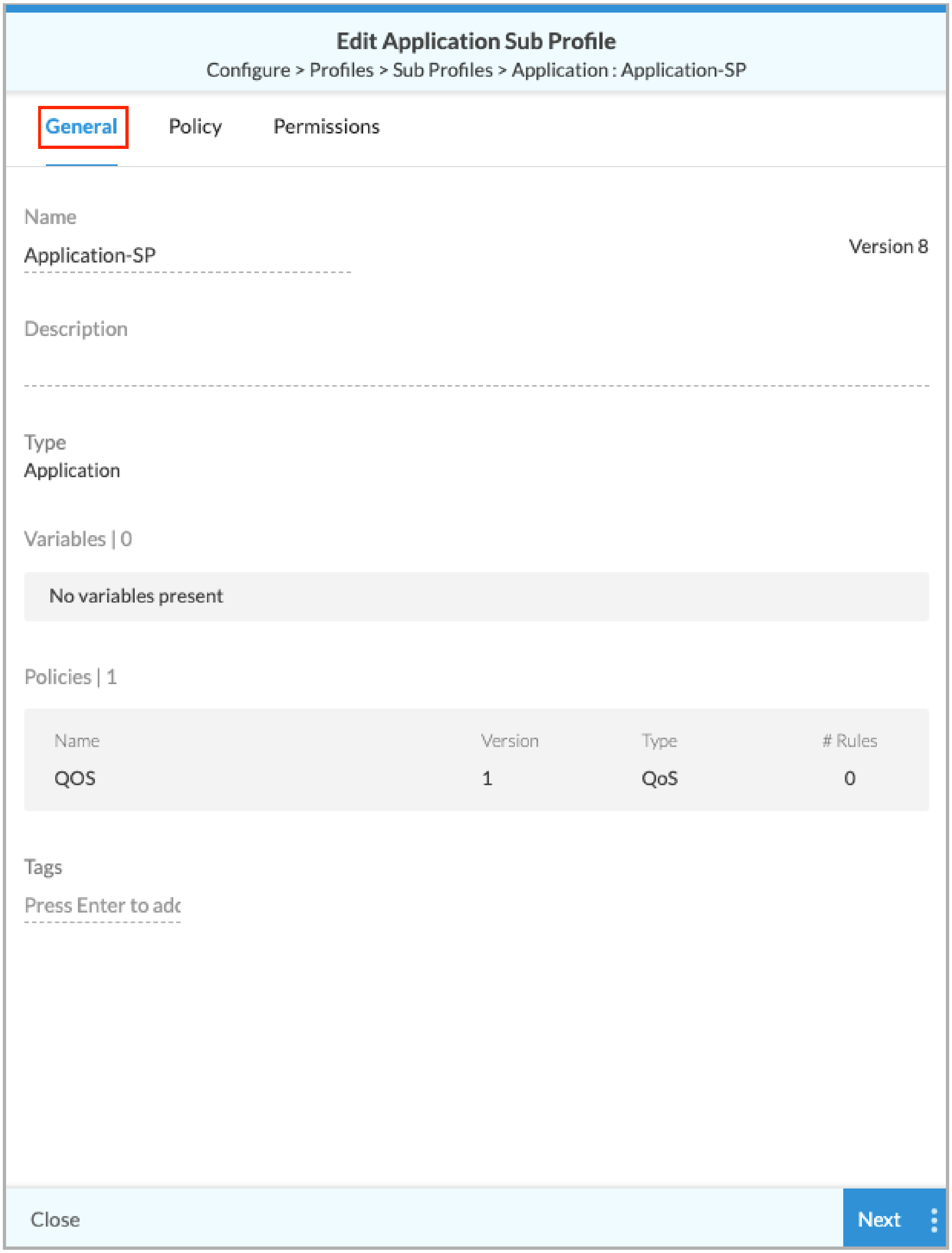
The screen displays the existing Application subprofiles.



Application-SP	Version 8
Policy Name	Type
QOS.v1	QoS

Application	Version 1
Policy Name	Type

2. To add a traffic steering policy, click an application subprofile (Application-SP in the example above), or click the ⋮ Elipsis icon, and then click the ✎ Edit icon in the popup menu. The Edit Application Sub Profile screen displays with the General tab selected by default.



Edit Application Sub Profile

Configure > Profiles > Sub Profiles > Application : Application-SP

Name: Application-SP

Version 8

Description

Type: Application

Variables | 0

No variables present

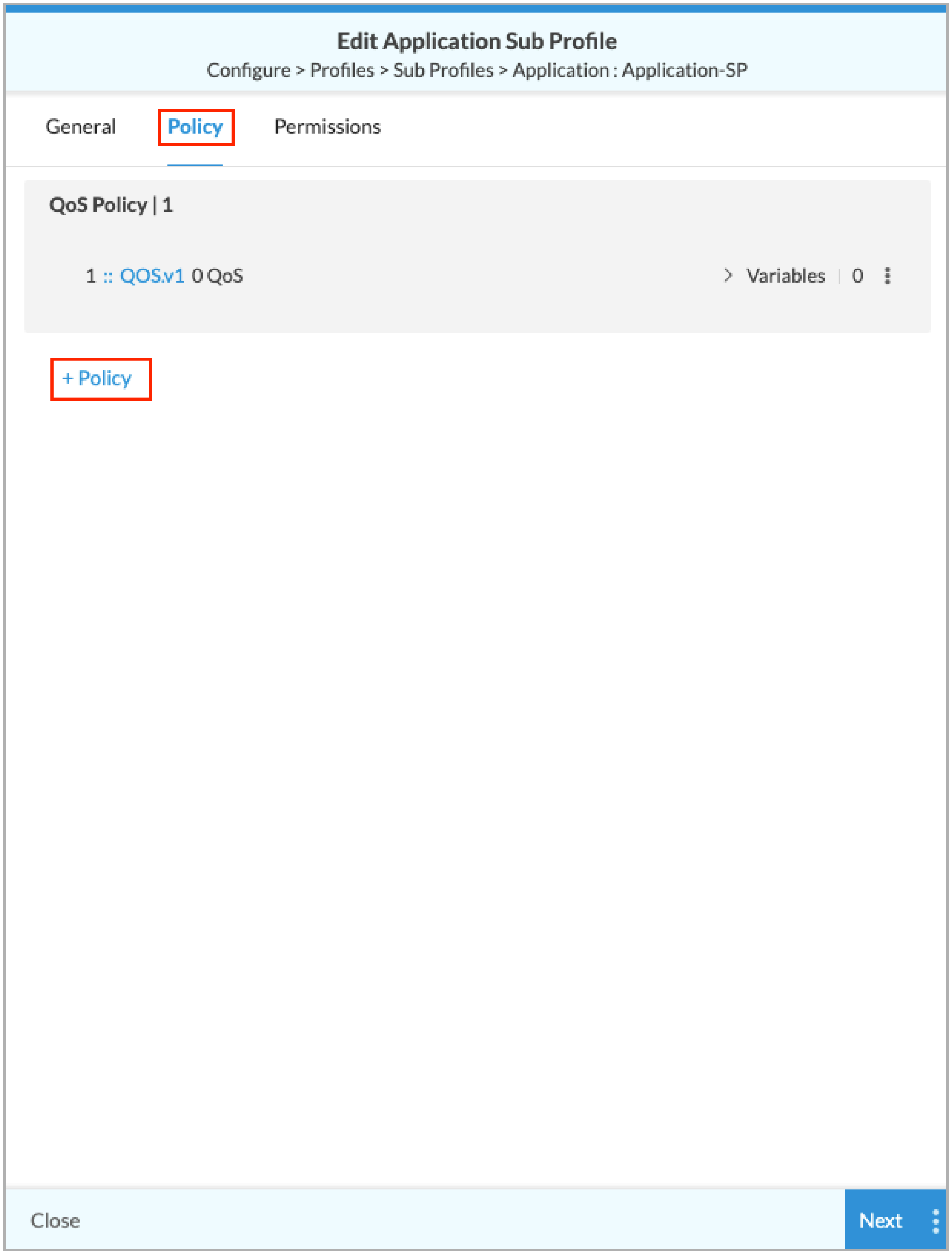
Policies | 1

Name	Version	Type	# Rules
QOS	1	QoS	0

Tags

Press Enter to adc

3. Select the Policy tab, and then click + Policy.



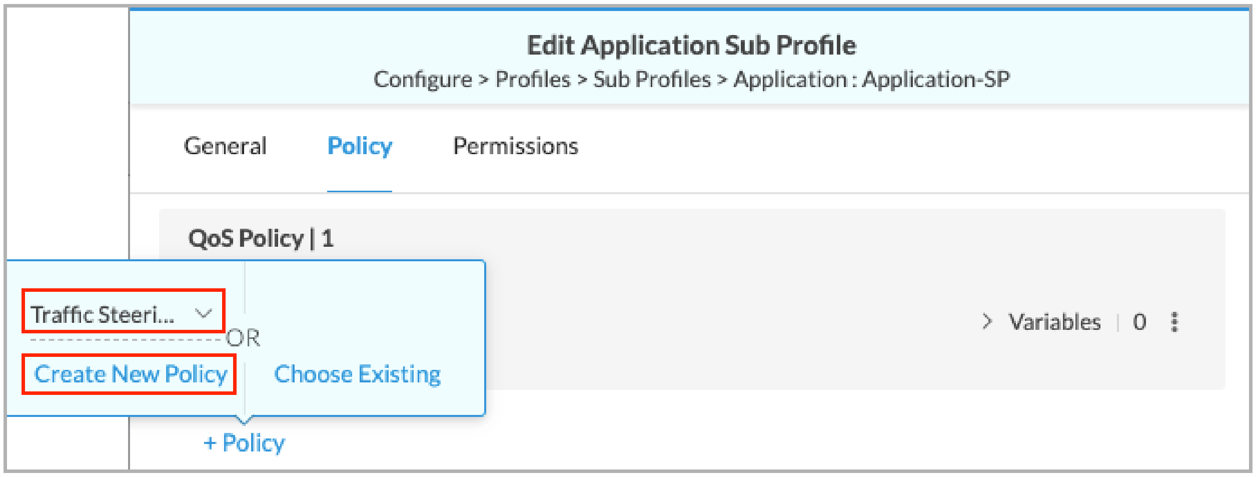
Edit Application Sub Profile

Configure > Profiles > Sub Profiles > Application : Application-SP

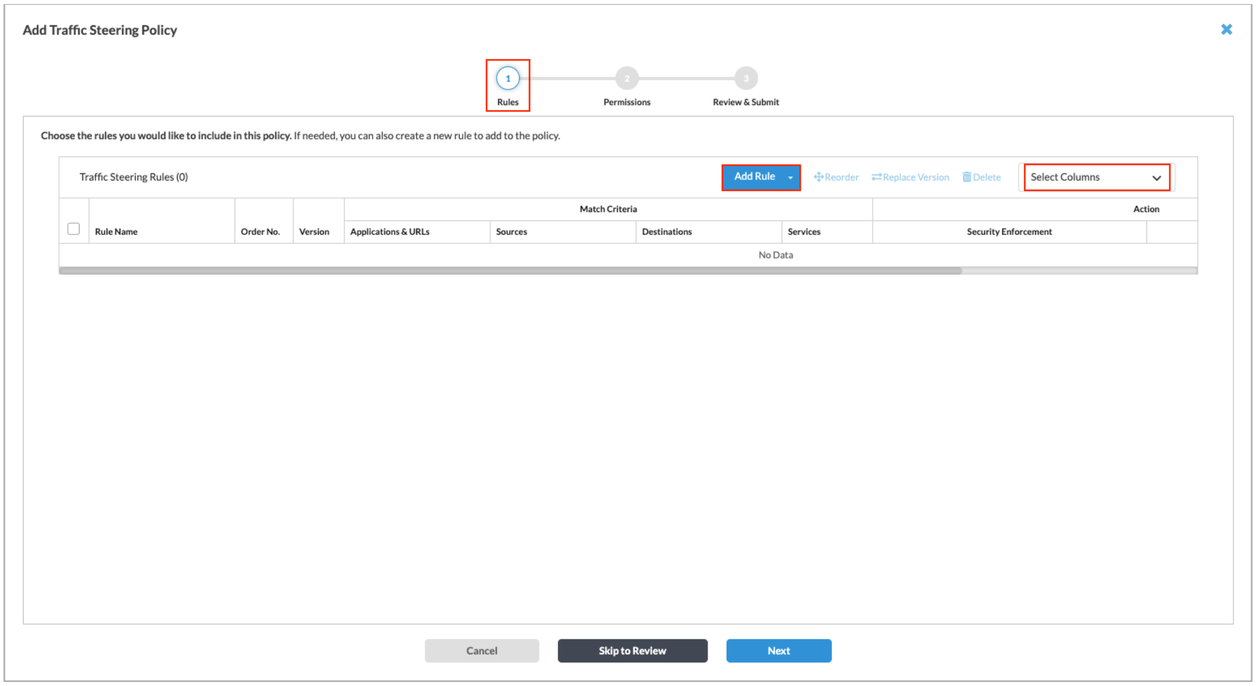
QoS Policy | 1

1 :: QOS.v1 0 QoS

4. In the popup menu, select Traffic Steering. To create a new policy, click Create New Policy. To use an existing policy, click Choose Existing and select a policy from the list.



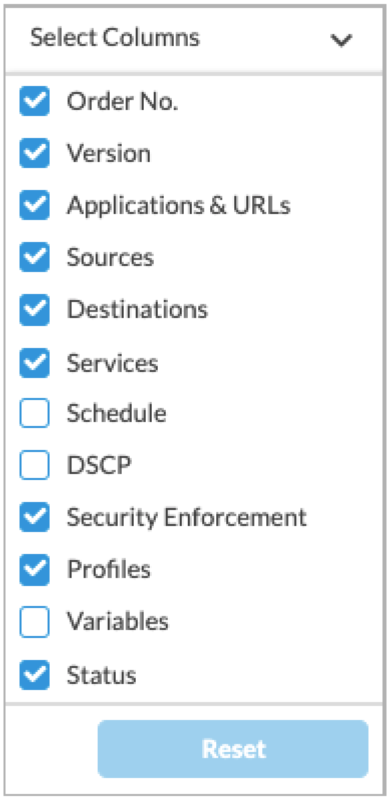
The Add Traffic Steering Policy screen displays with Step 1, Rules selected by Default.



Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy.

				Match Criteria				Action
□	Rule Name	Order No.	Version	Applications & URLs	Sources	Destinations	Services	Security Enforcement
					No Data			

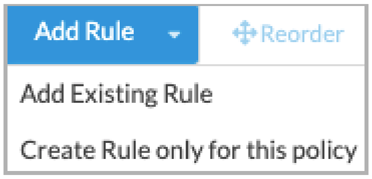
5. If desired, you can specify the columns to display, or you can accept the default selections and go to the next step. To change the settings, click the Select Columns down arrow and select the columns to be displayed. To restore the default column settings, click Reset.



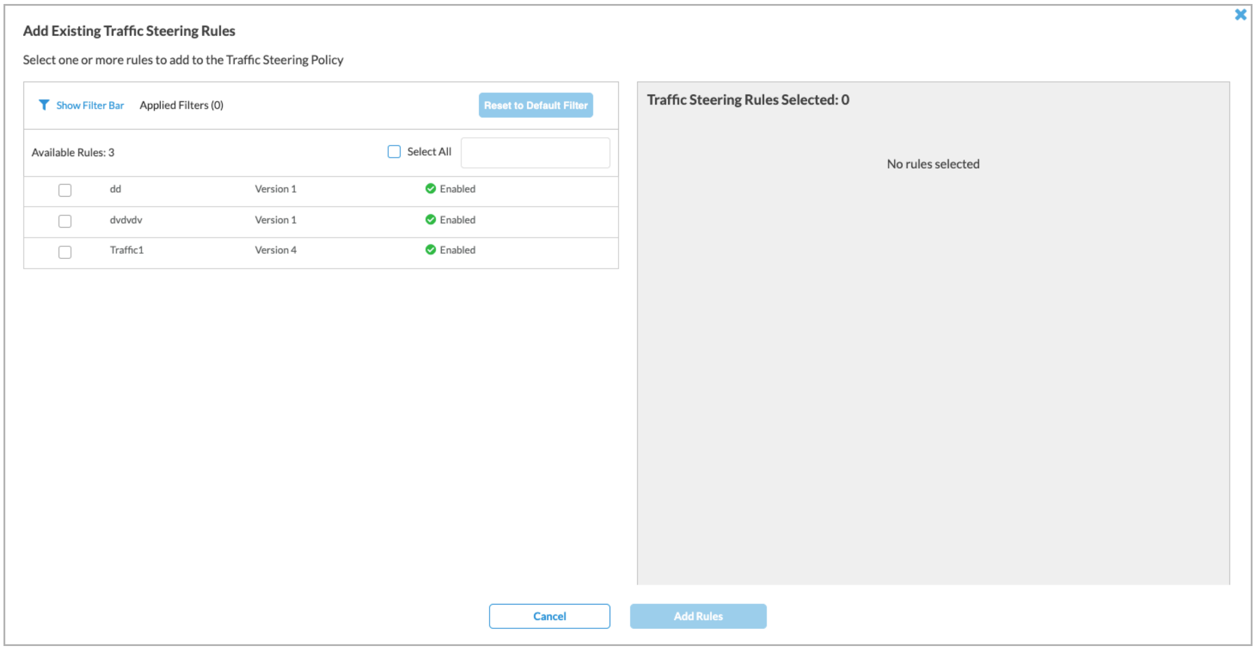
Select Columns

- ☑ Order No.
- ☑ Version
- ☑ Applications & URLs
- ☑ Sources
- ☑ Destinations
- ☑ Services
- ☐ Schedule
- ☐ DSCP
- ☑ Security Enforcement
- ☑ Profiles
- ☐ Variables
- ☑ Status

6. In the Add Traffic Steering Policy screen, click Add Rule. The following screen displays.



7. To create a new rule for the application policy, continue to Step 8. To add an existing rule:
   a. Click Add Existing Rule. The Add Existing Traffic Steering Rules screen displays the existing traffic steering rules.



Add Existing Traffic Steering Rules

Select one or more rules to add to the Traffic Steering Policy

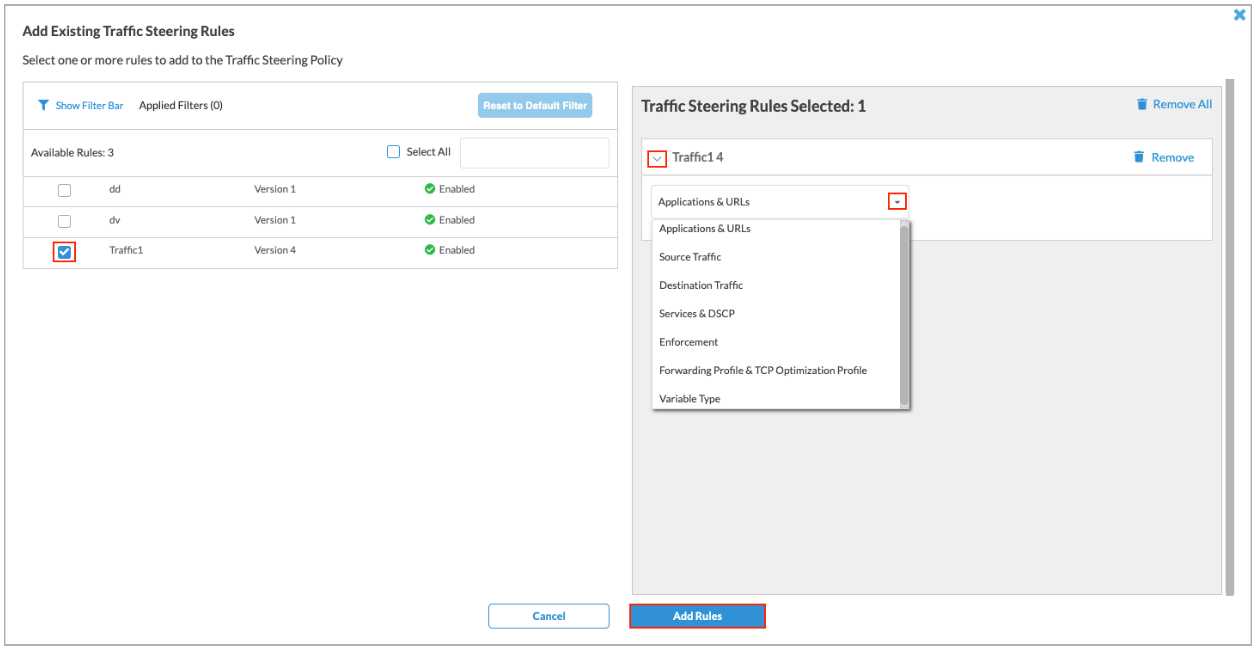
Available Rules: 3

□	dd	Version 1	✓ Enabled
□	dvdvdv	Version 1	✓ Enabled
□	Traffic1	Version 4	✓ Enabled

Traffic Steering Rules Selected: 0

No rules selected

b. Select one or more rules. The selected rules move to the Traffic Steering Rules Selected panel.



Add Existing Traffic Steering Rules

Select one or more rules to add to the Traffic Steering Policy

Available Rules: 3

□	dd	Version 1	✓ Enabled
□	dv	Version 1	✓ Enabled
☑	Traffic1	Version 4	✓ Enabled

Traffic Steering Rules Selected: 1

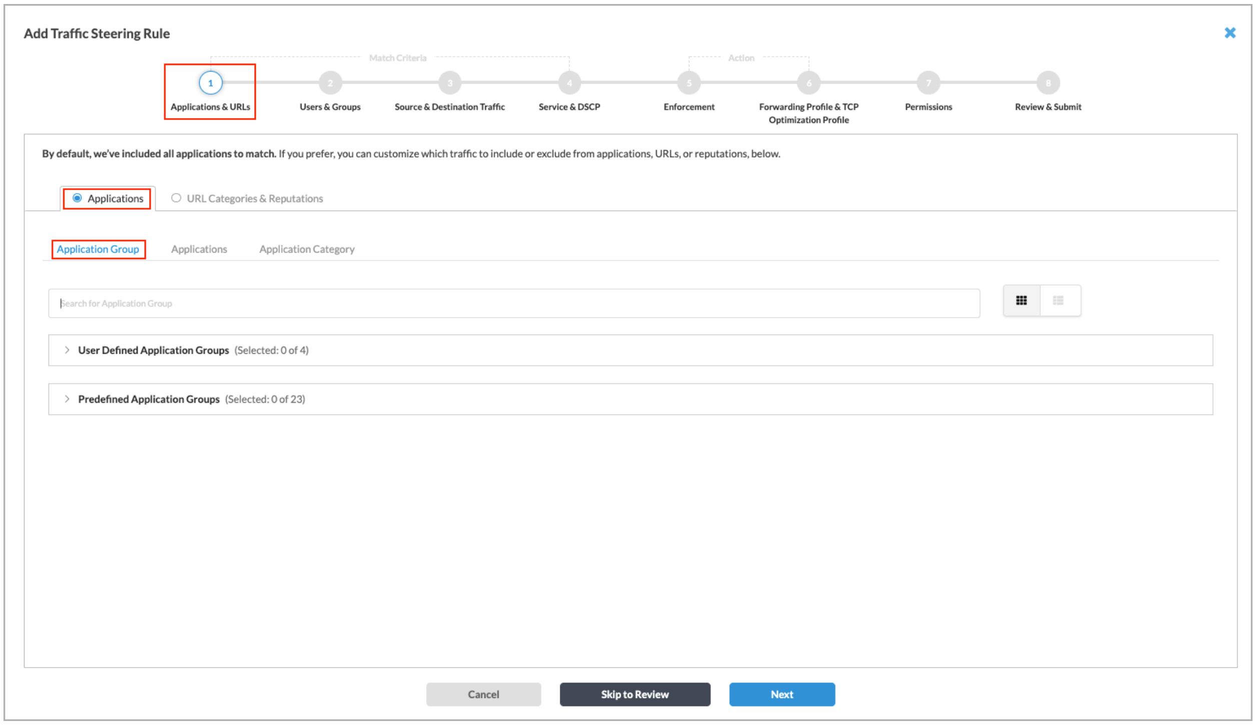
c. To view the configuration elements for a selected rule, click the down arrow next to the rule, and then select a category to display the configuration elements for that category. The categories are:

- Applications and URLs
- Destination Traffic
- Enforcement
- Forwarding Profile an TCP Optimization Profile
- Services and DSCP

        - Source Traffic
        - Variable Type

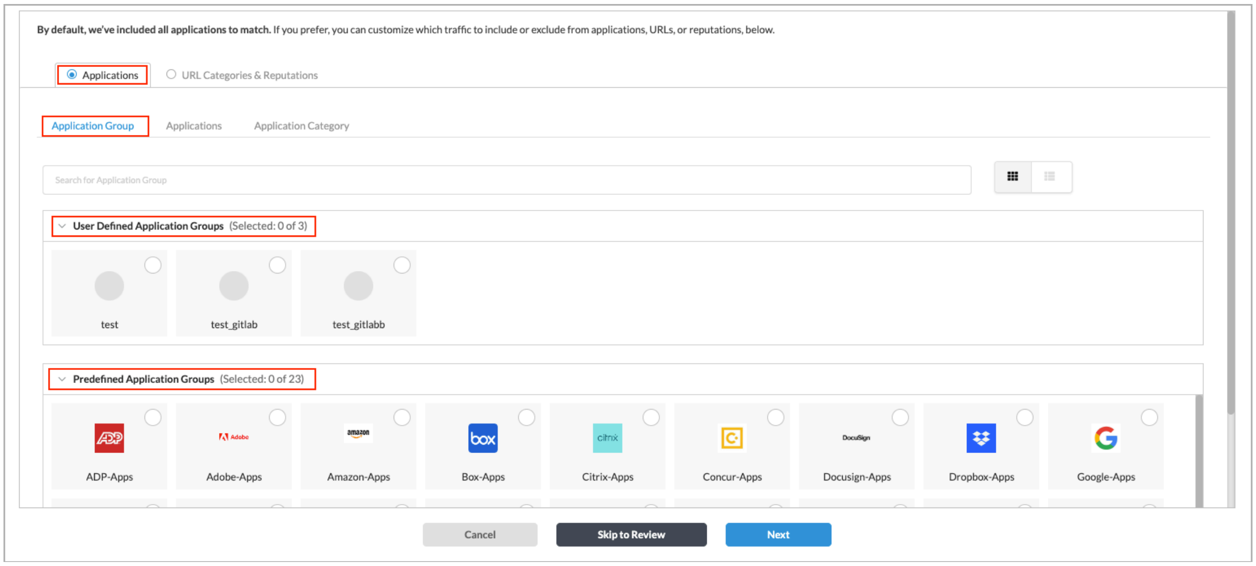
    d. Click Add Rules to add the traffic-steering rule to the application policy.

8. To create a new rule for the application policy, select Create Rule only for this Policy. The Add Traffic Steering Rule screen displays with Step 1, Applications & URLs, the Applications radio button, and the Application Group tab selected by default.


Add Traffic Steering Rule
Match Criteria
Action
1 Applications & URLs
2 Users & Groups
3 Source & Destination Traffic
4 Service & DSCP
5 Enforcement
6 Forwarding Profile & TCP Optimization Profile
7 Permissions
8 Review & Submit
● Applications
○ URL Categories & Reputations
Application Group
Applications
Application Category
Search for Application Group
User Defined Application Groups (Selected: 0 of 4)
Predefined Application Groups (Selected: 0 of 23)
Cancel
Skip to Review
Next

By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

9. From here, you can select specific applications, application groups, or application categories to include in the match criteria. All applications, URL categories, and reputation are included by default. You can use this screen to customize which applications, URL categories, and reputation to include in the match criteria.
    - To select application groups for the rule to match, on the Application Group tab, click the group category (User Defined Application Groups or Predefined Application Groups), and then select the application groups for the rule to match. You can also use the Search bar to find specific application groups.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

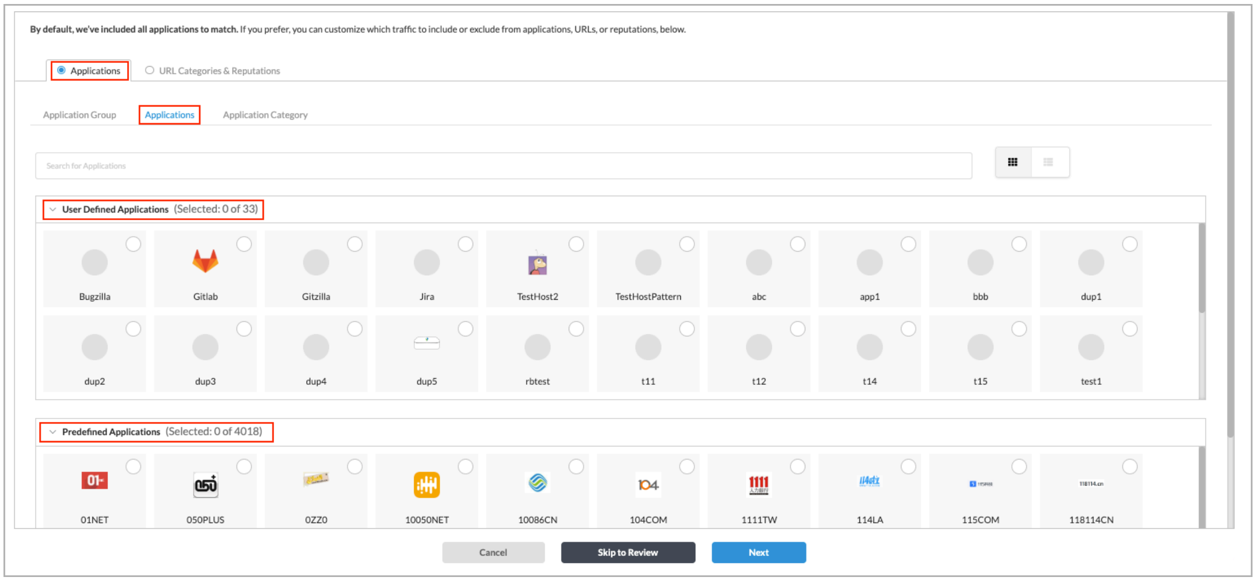
● Applications ○ URL Categories & Reputations

Search for Application Group

User Defined Application Groups (Selected: 0 of 3)

Predefined Application Groups (Selected: 0 of 23)

- To select applications for the rule to match, select the Applications > Applications tab, click the group category (User Defined Application Groups or Predefined Application Groups), and then select the applications. You can also use the Search bar to find specific applications.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

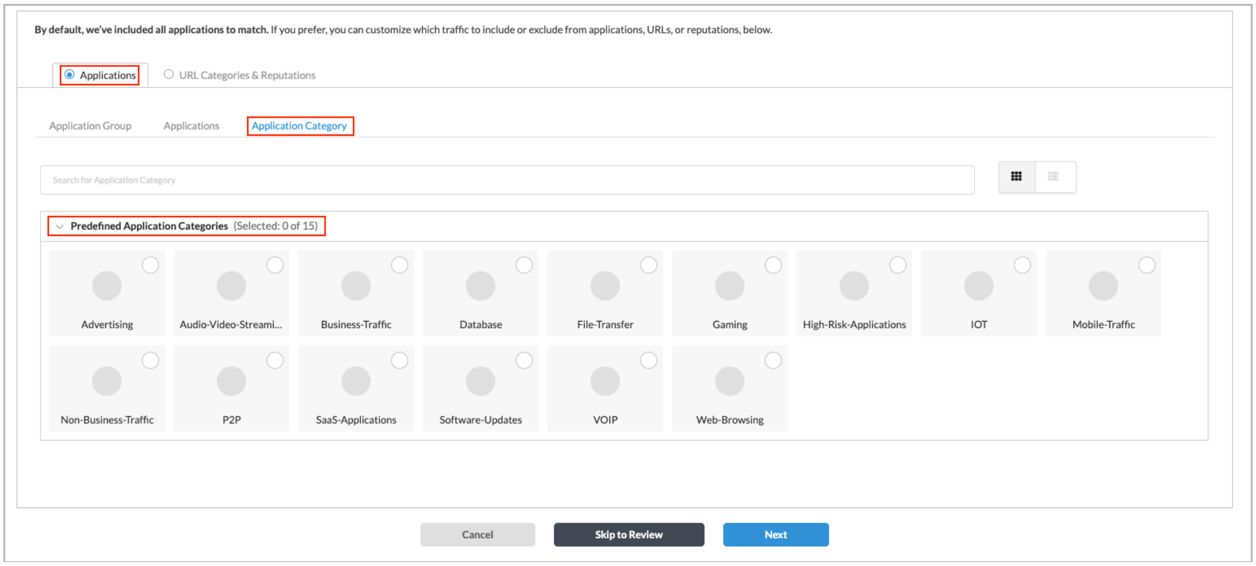
● Applications ○ URL Categories & Reputations

Search for Applications

User Defined Applications (Selected: 0 of 33)

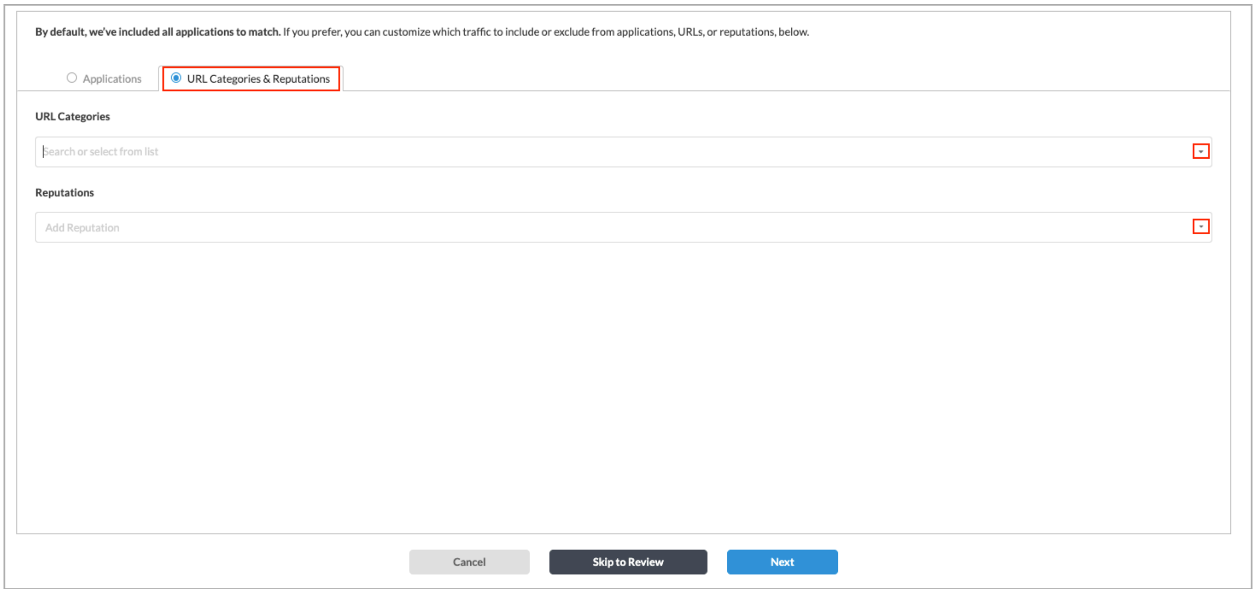
Predefined Applications (Selected: 0 of 4018)

- To select predefined application categories for the rule to match, select the Applications > Application Category tab, and then select one or more predefined application categories. You can also use the Search bar to find specific application categories.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

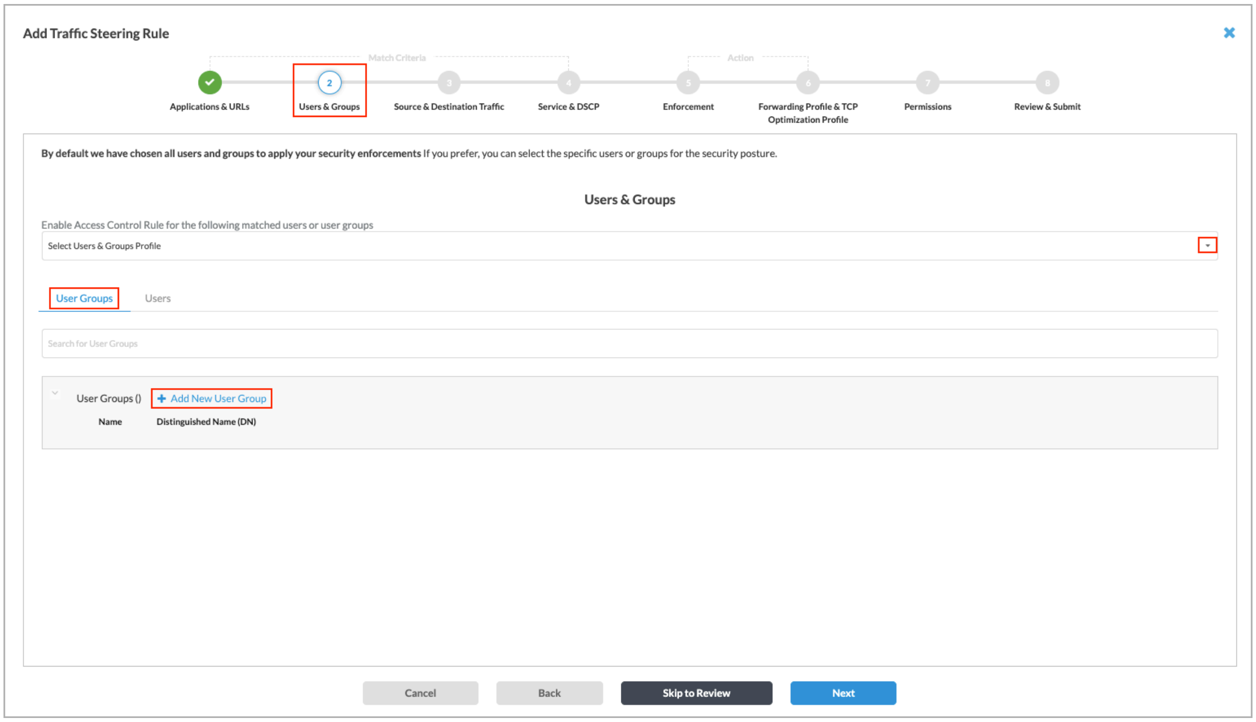
10. Select the URL Categories and Reputations tab. The following screen displays.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

11. In the URL Categories field, click the down arrow, and then select one or more URL categories for the rule to match.
12. In the Reputations field, click the down arrow, and then select one or more reputations to include in the rule:
    - High risk
    - Low risk
    - Moderate risk
    - Suspicious
    - Trustworthy
    - Undefined

13. Click Next or select Step 2, Users & Groups.



Add Traffic Steering Rule

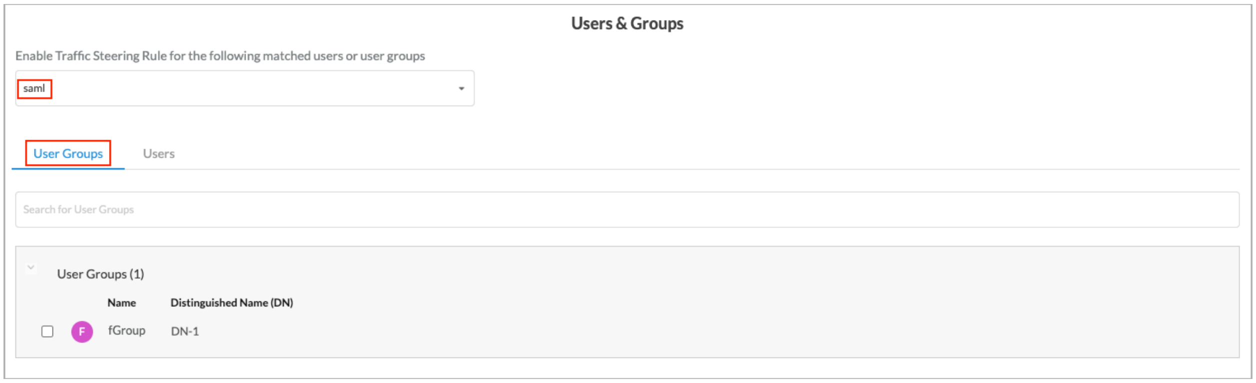
By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

Enable Access Control Rule for the following matched users or user groups: Select Users & Groups Profile

Name	Distinguished Name (DN)

14. To add an existing user group, click Select Users & Groups Profile and click the name of one or more user groups (fGroup in the figure below).

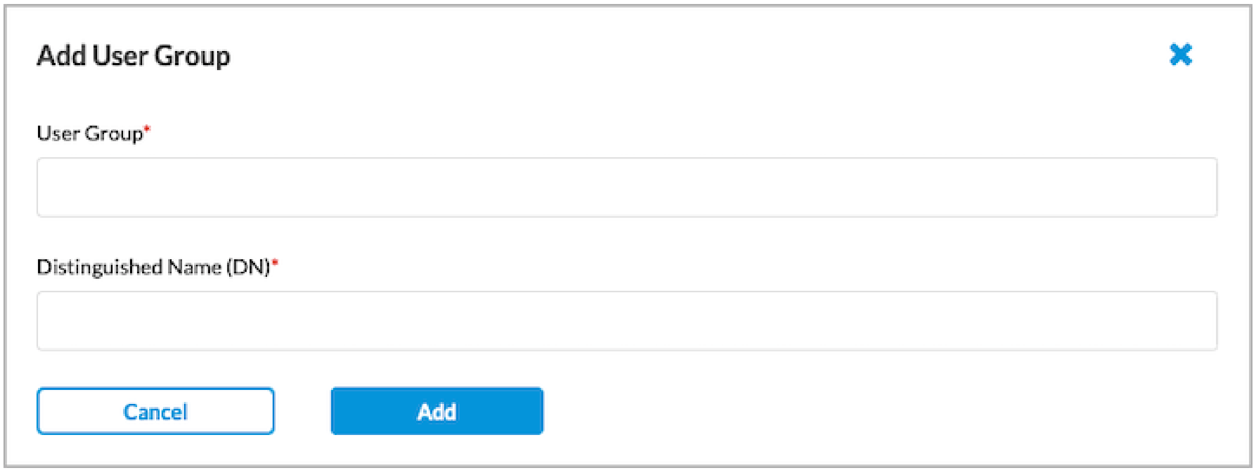


Users & Groups

Enable Traffic Steering Rule for the following matched users or user groups: saml

	Name	Distinguished Name (DN)
□ F	fGroup	DN-1

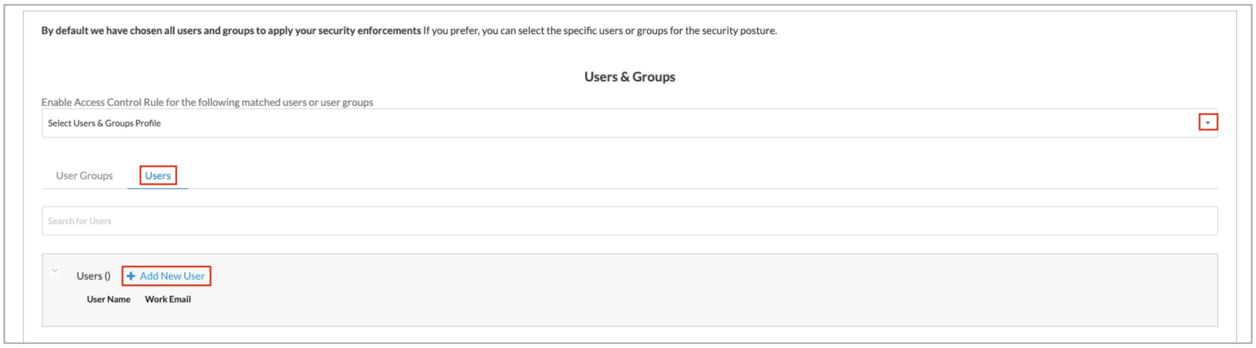
15. To add a new user group, click + Add New User Group. The following screen displays.



a. Enter a user group name and a distinguished name (DN).

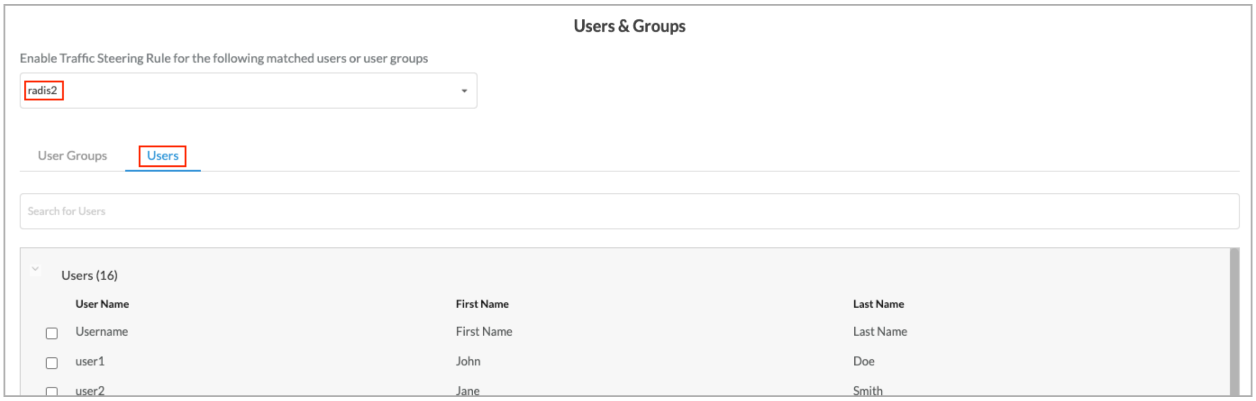
b. Click Add.

16. Select the Users tab.


By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

Users & Groups
Enable Access Control Rule for the following matched users or user groups
Select Users & Groups Profile
User Groups
Users
Search for Users
Users ()
+ Add New User
User Name
Work Email

17. To add existing users, click Select Users & Groups Profile and click the name of one or more users.

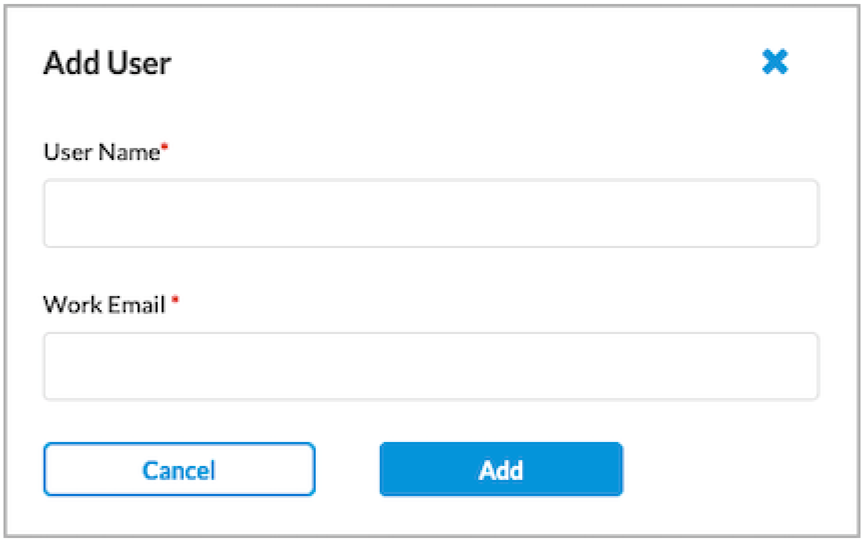

Users & Groups
Enable Traffic Steering Rule for the following matched users or user groups
User Groups
Users
Search for Users

Enable Traffic Steering Rule for the following matched users or user groups: radis2

Users (16)

	User Name	First Name	Last Name
□	Username	First Name	Last Name
□	user1	John	Doe
□	user2	Jane	Smith

18. To add a new user, click + Add New User. The following screen displays.



Add User

User Name*

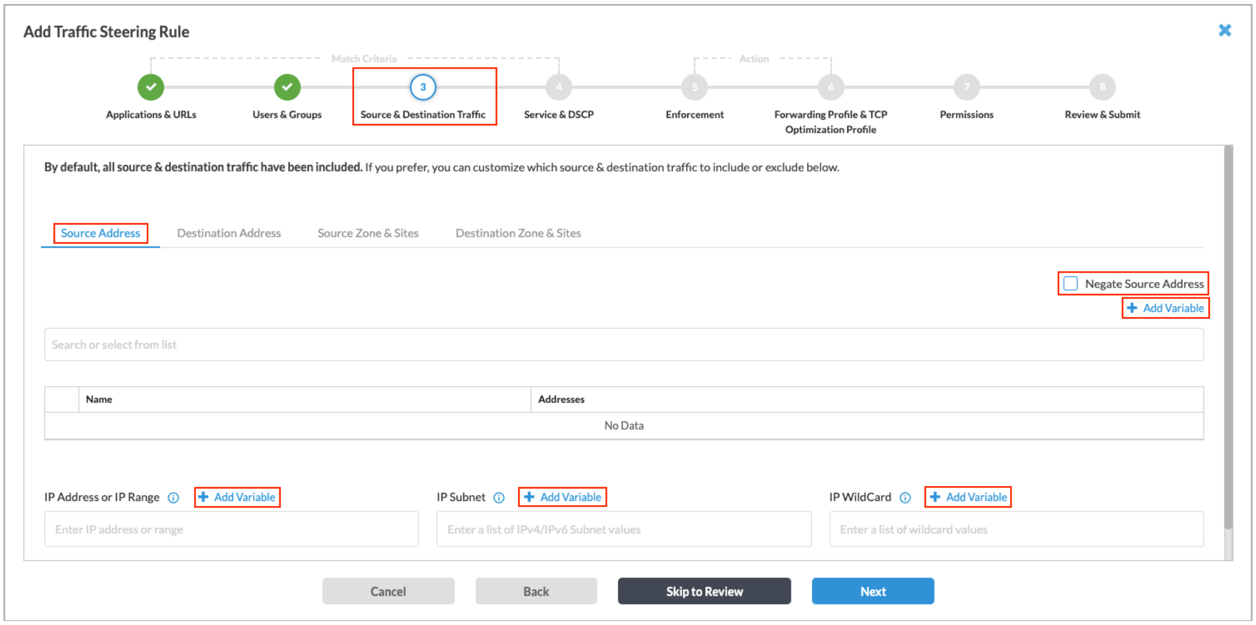
Work Email *

Cancel Add

a. Enter a user name and a work email address.

b. Click Add.

19. Click Next or select Step 3, Source & Destination Traffic. The following screen displays. All source and destination traffic is included in the match criteria by default. You can use this screen to customize the source and destination traffic to include in the match criteria.



Add Traffic Steering Rule

By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

□ Negate Source Address

+ Add Variable

Search or select from list

	Name	Addresses
	No Data	

IP Address or IP Range + Add Variable: Enter IP address or range

IP Subnet + Add Variable: Enter a list of IPv4/IPv6 Subnet values

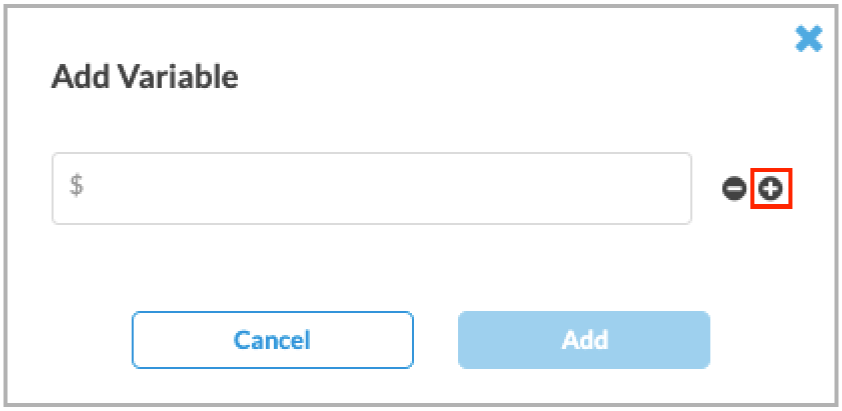
IP WildCard + Add Variable: Enter a list of wildcard values

20. To customize the source traffic, on the Source Address tab, use one of the following methods:

- To specify source addresses to include in the match criteria, continue to Step 21.
- To specify source addresses to exclude from the match criteria, select Negate Source Address to match all source addresses except the source addresses that you specify, and then continue to Step 21.

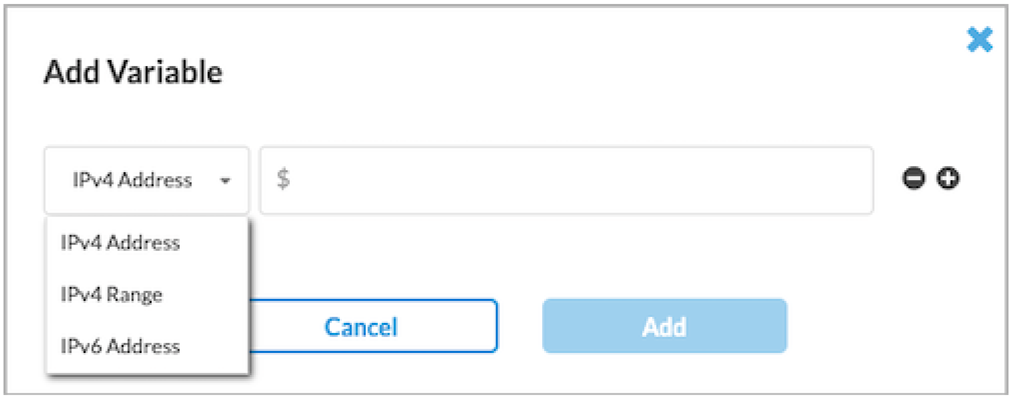
21. To specify a source address to include or exclude in the match criteria, you can select a source address from the list or use the search box to find a source address. To create a variable for the source address, click + Add

Variable to the right of the source address list. Enter a name for the variable, click the ⊕ Plus icon, then click Add. You can add multiple variables.

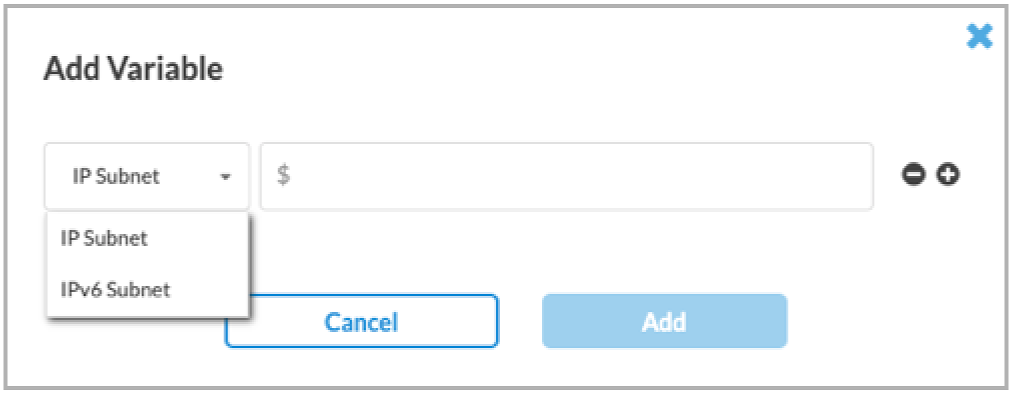


You can also enter values for the fields IP address or IP range, IPv4 or the IPv6 subnet, or the IP wildcard as part of the match criteria. To create variables for these values, click + Add Variable for that field.

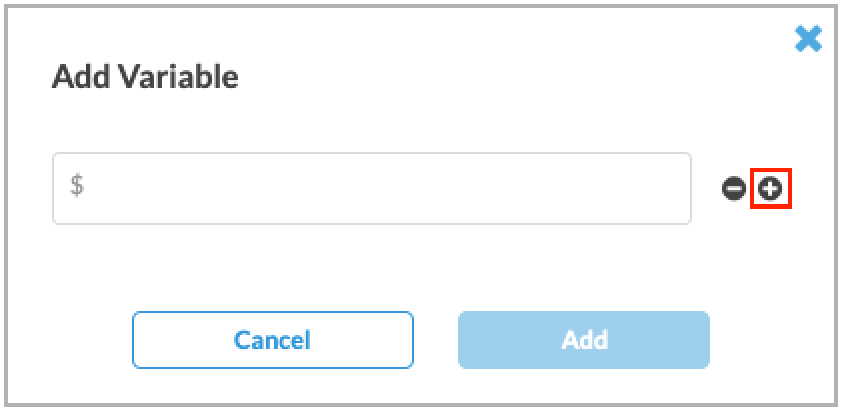
- To add a variable for the IP address or IP range, select IPv4 Address, IPv4 Range, or IPv6 Address from the drop-down list, click the ⊕ Plus icon, the click Add. You can add multiple variables.



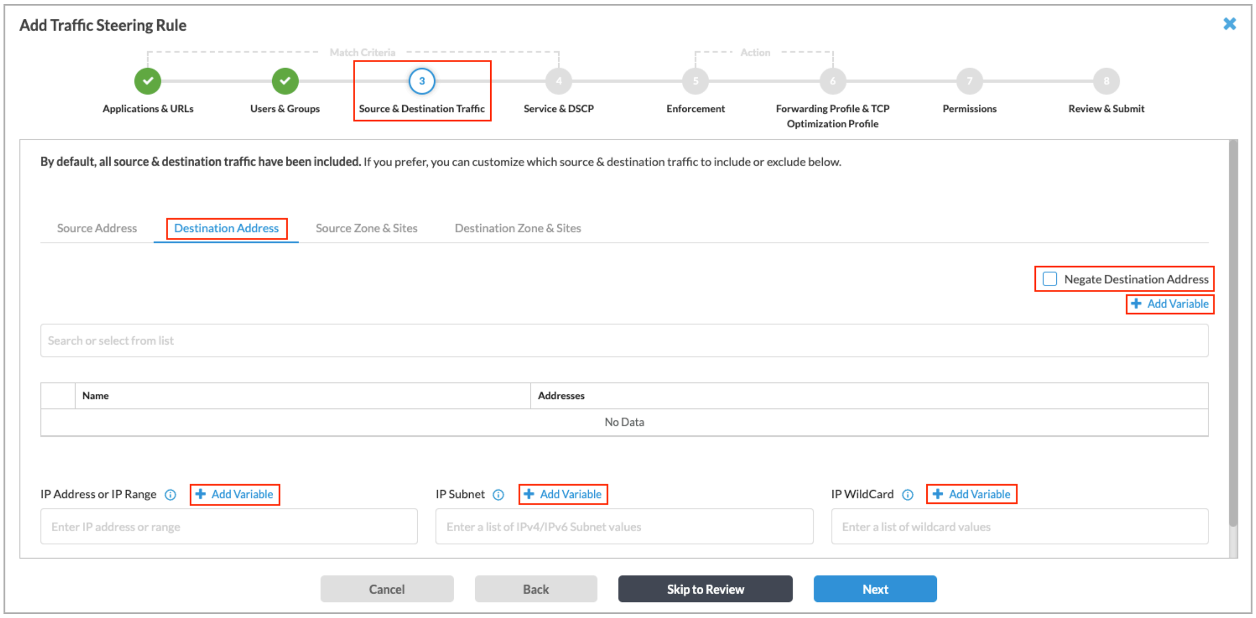
- To add a variable for the IP subnet, select IP Subnet or IPv6 Subnet from the drop-down list, click the ⊕ Plus icon, the click Add. You can add multiple variables.



- To add a variable for the IP wildcard, enter a name for the variable, click the ⊕ Plus icon, then click Add. You can add multiple variables.



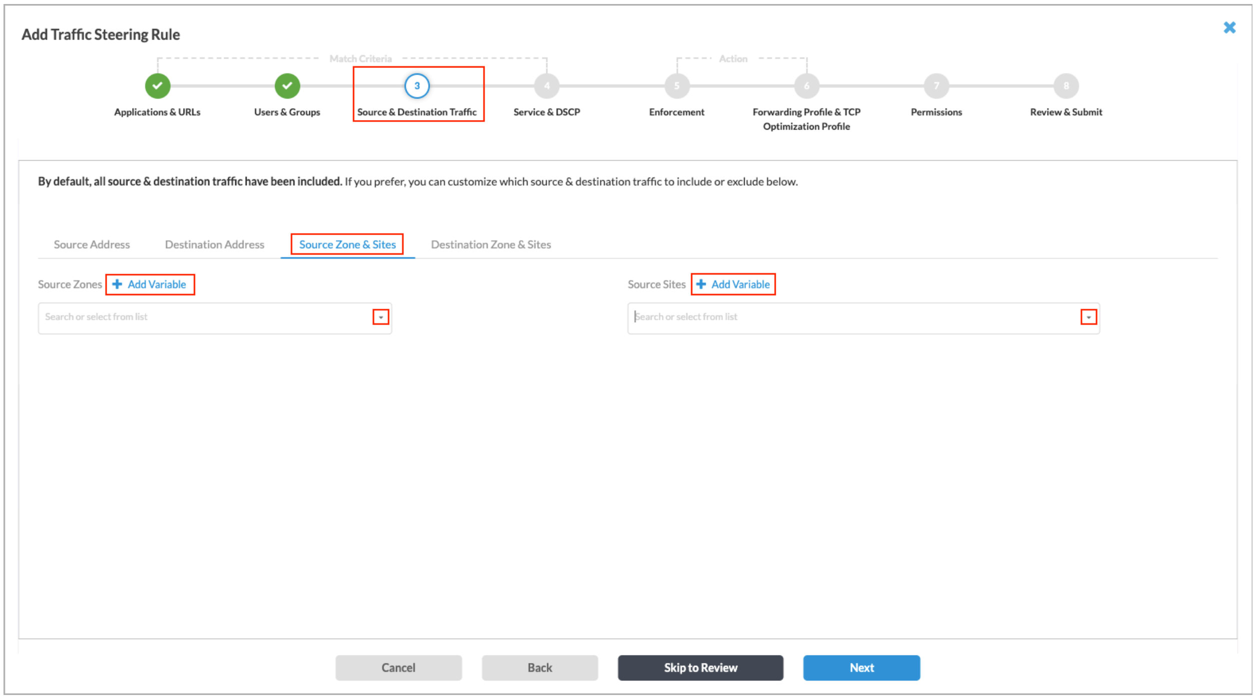
22. Click the Destination Address tab. The following screen displays.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Name	Addresses
No Data	

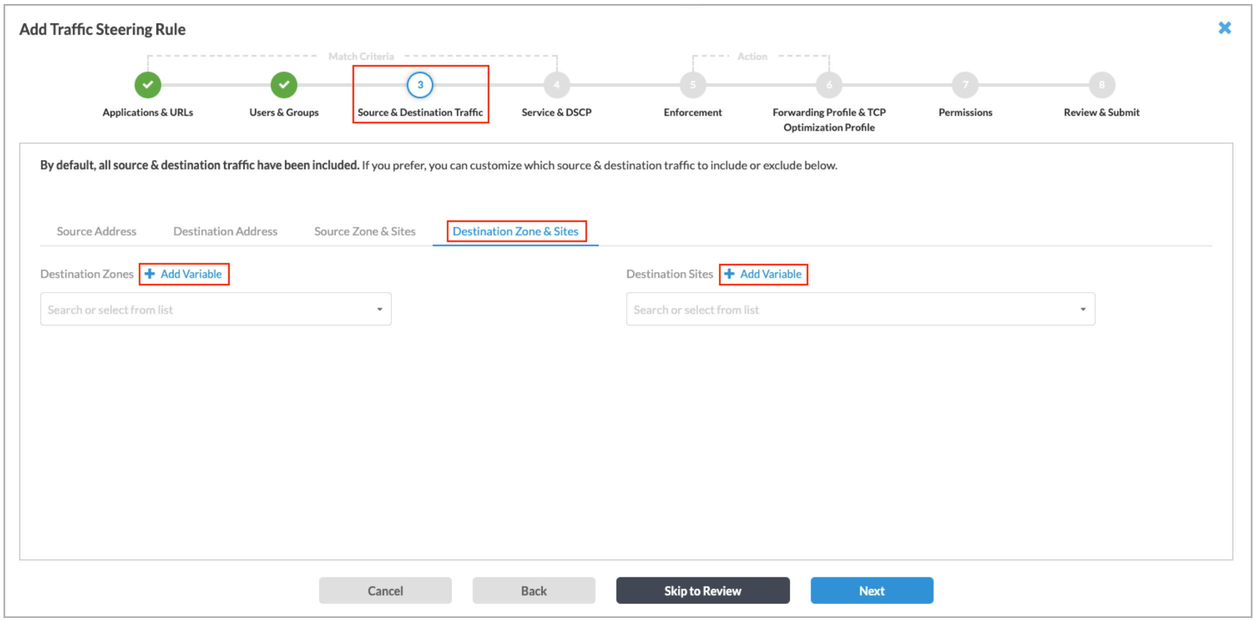
23. To customize the destination traffic, use one of the following methods:
    - To specify destination addresses to include in the match criteria, continue to Step 24 to select addresses.
    - To specify destination addresses to exclude from the match criteria, select Negate Source Address to match all destination addresses except the addresses that you specify, and then continue to Step 24 to select addresses.
24. To specify a destination address to include or exclude in the match criteria, you can select a destination address from the list or use the search box to find a destination address. To create a variable for the destination address, click + Add Variable to the right of the destination address list. You can also enter values for the fields IP address or IP range, IPv4 or the IPv6 subnet, or the IP wildcard as part of the match criteria. To create variables for these values, click + Add Variable for that field. For more information on adding variables, see step 21.
25. Select the Source Zone and Sites tab. The following screen displays. All source zones and source sites are included in the match criteria by default. To customize the source zones and source sites to be included in the match criteria, enter information for the following fields.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Field	Description
Source Zones	Click the down arrow, and then select one or more zones. To create a variable for the source zone, click ✚ Add Variable.
Source Sites	Click the down arrow, and then select one or more sites. To create a variable for the source zone, click ✚ Add Variable.

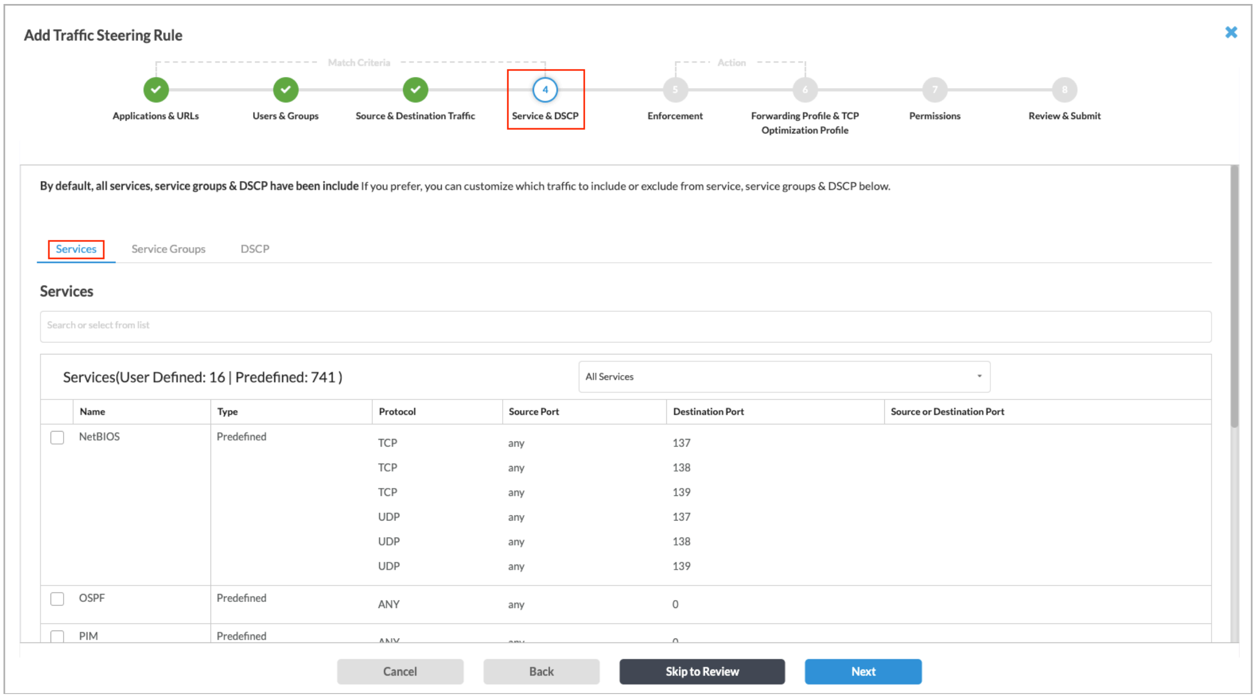
26. Select the Destination Zone and Sites tab. By default, all destination zones and destination sites are included in the match criteria. To customize the destination zones and destination sites to be included in the match criteria, enter information for the following fields.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Field	**Description**
Destination Zones	Click the down arrow, and then select one or more zones. To create a variable for the source zone, click ✚ Add Variable.
Destination Sites	Click the down arrow, and then select one or more sites. To create a variable for the source zone, click ✚ Add Variable.

27. Click Next or select Step 4, Service & DSCP. The following screen displays. All services, service groups, and DSCPs are included in the match criteria by default. You can use this screen to customize the services, service groups, and DSCPs to include in the match criteria.



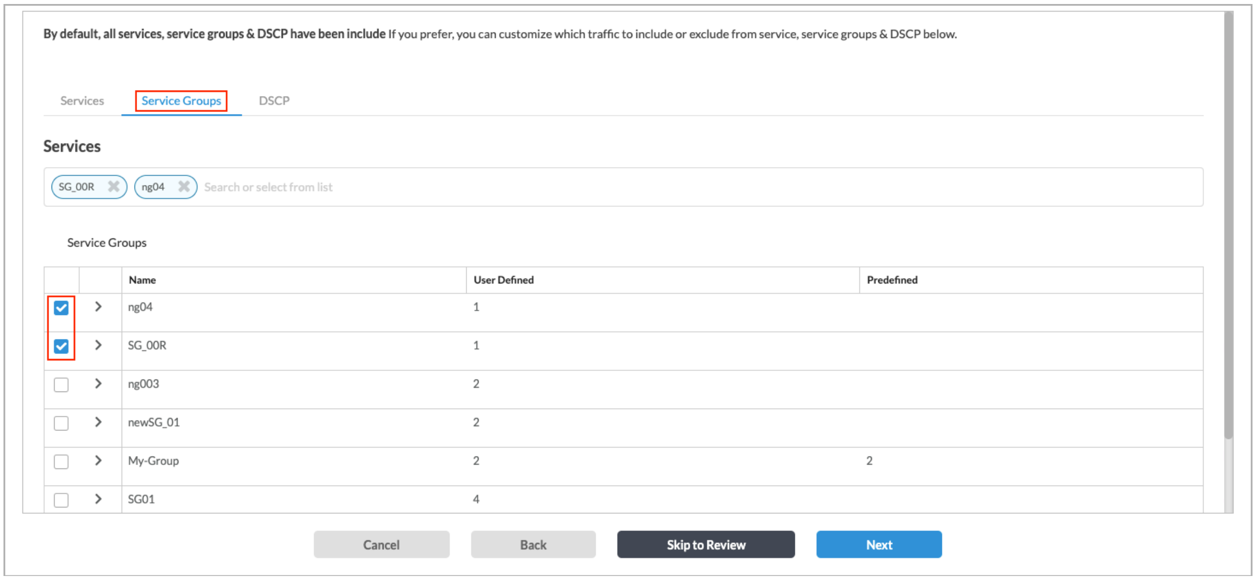
By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services

Services(User Defined: 16 | Predefined: 741)

	Name	Type	Protocol	Source Port	Destination Port	Source or Destination Port
□	NetBIOS	Predefined	TCP	any	137	
			TCP	any	138	
			TCP	any	139	
			UDP	any	137	
			UDP	any	138	
			UDP	any	139	
□	OSPF	Predefined	ANY	any	0	
□	PIM	Predefined	ANY	any	0	

28. To specify the services to include, do one or both of the following:
    - In the search box under Services, enter the service name.
    - Select one or more services from the list below the search box. You can select one of the following categories to filter the list:
        - All Services
        - Predefined
        - User Defined
29. Select the Service Groups tab, then select the service group to which you want to apply security access control rules. You can select User-Defined, Predefined, or both. Click the > Toggle Row Expand icon next to the service group name to view the details for each service group.



By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

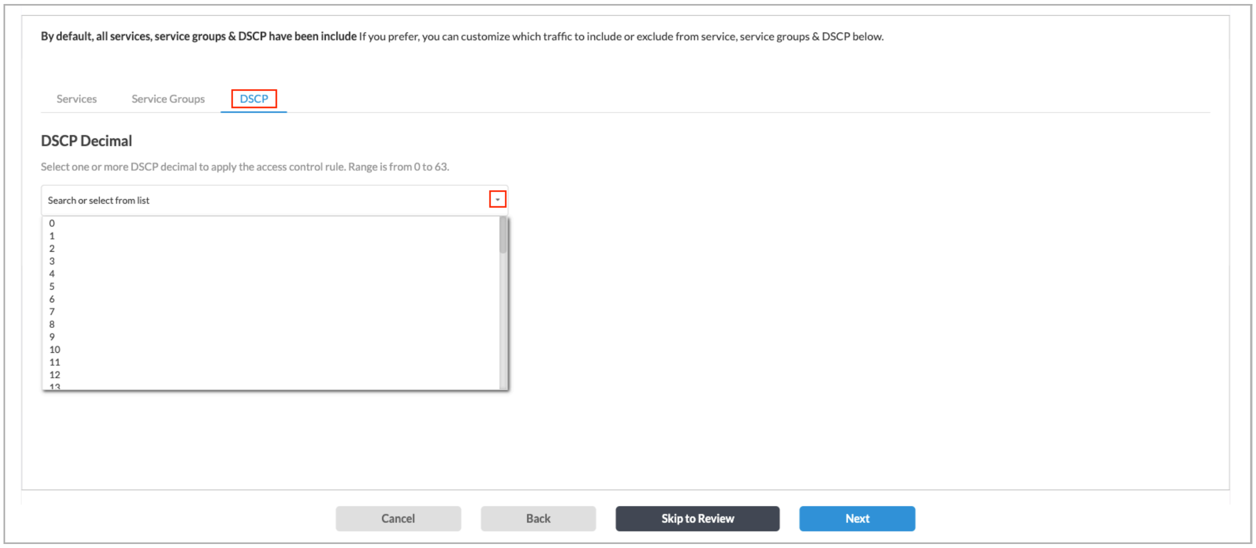
Services

SG_00R ✖ ng04 ✖ Search or select from list

Service Groups

		Name	User Defined	Predefined
☑	>	ng04	1	
☑	>	SG_00R	1	
□	>	ng003	2	
□	>	newSG_01	2	
□	>	My-Group	2	2
□	>	SG01	4	

30. Select one or more service groups to include in the match criteria. The service groups are added to the Services list.
31. Select the DSCP tab. All DSCP decimal values are included by default. You can specify which DSCP decimal values to include in the match criteria.



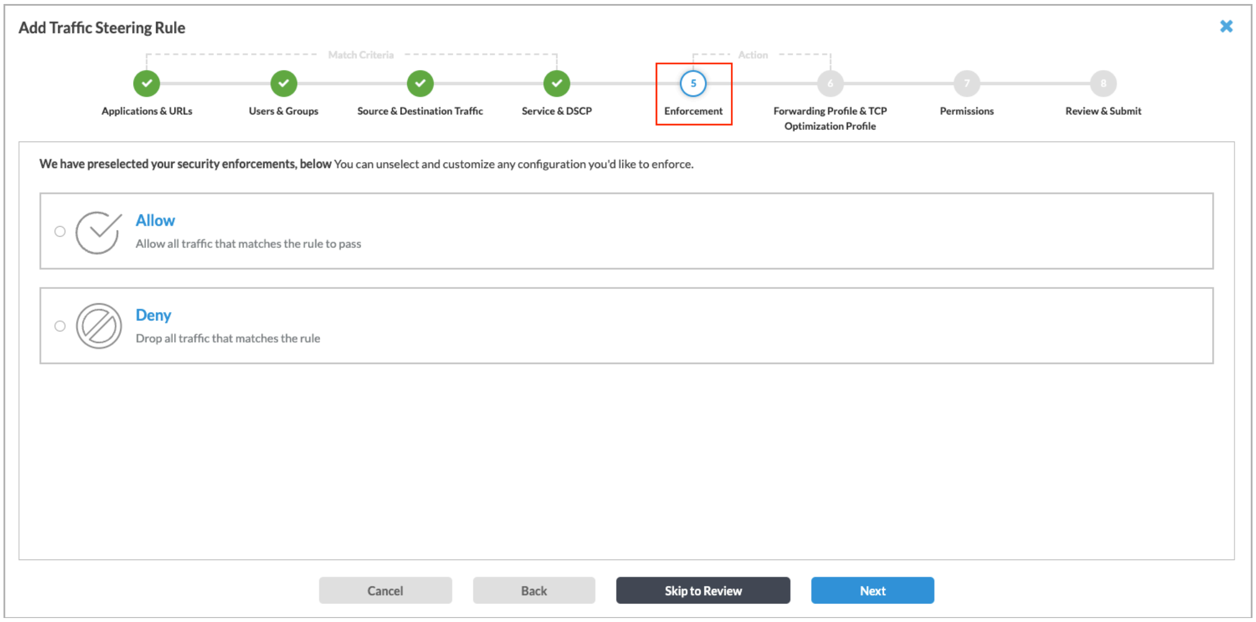
By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

DSCP Decimal

Select one or more DSCP decimal to apply the access control rule. Range is from 0 to 63.

Search or select from list

32. Select one or more DSCP decimal values from the drop-down list, or use search to locate one or more values.
33. Click Next to go to Step 5, Enforcement. Security enforcement rules define the actions to take on traffic that meets the previously defined match conditions, and defines the security enforcement actions to apply to matching traffic. The following screen shows the available security enforcement actions.



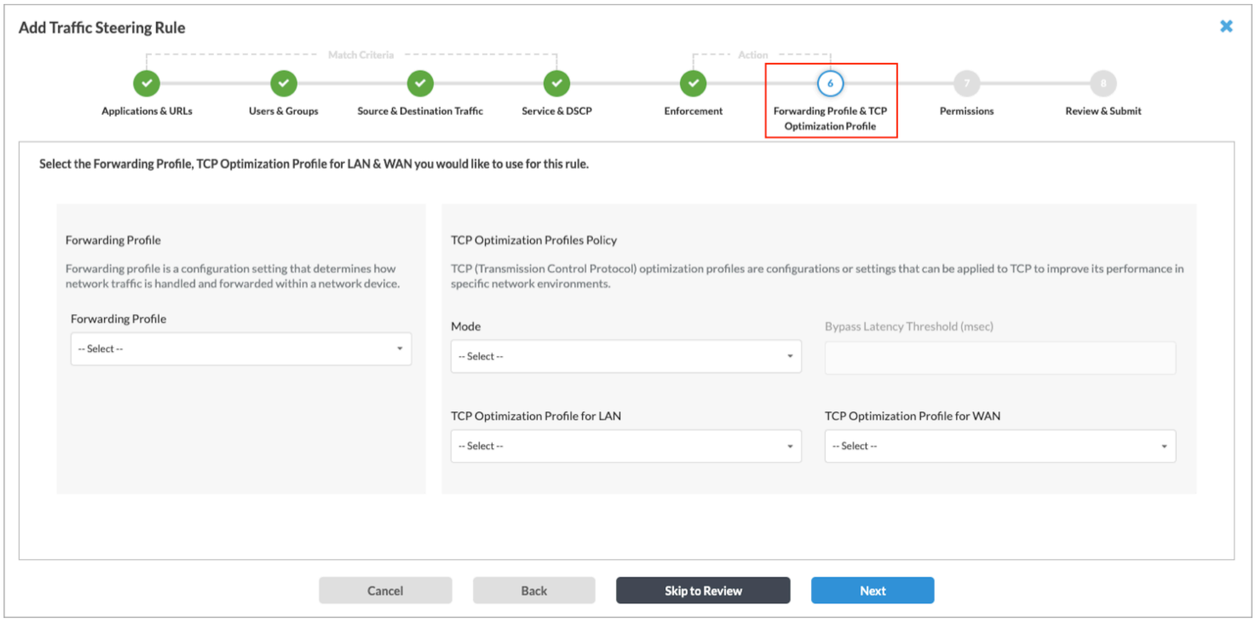
We have preselected your security enforcements, below You can unselect and customize any configuration you'd like to enforce.

○ Allow
Allow all traffic that matches the rule to pass

○ Deny
Drop all traffic that matches the rule

34. Click one of the following options to apply a security enforcement action:
    - Allow—Allow all traffic that matches the rule to pass unfiltered.
    - Deny—Drop all traffic that matches the rule.

35. Click Next to go to Step 6, Forwarding Profile & TCP Optimization Profile and enter the following information.



Select the Forwarding Profile, TCP Optimization Profile for LAN & WAN you would like to use for this rule.

Forwarding Profile

Forwarding profile is a configuration setting that determines how network traffic is handled and forwarded within a network device.

Forwarding Profile: -- Select --

TCP Optimization Profiles Policy

TCP (Transmission Control Protocol) optimization profiles are configurations or settings that can be applied to TCP to improve its performance in specific network environments.

Mode: -- Select --

Bypass Latency Threshold (msec)

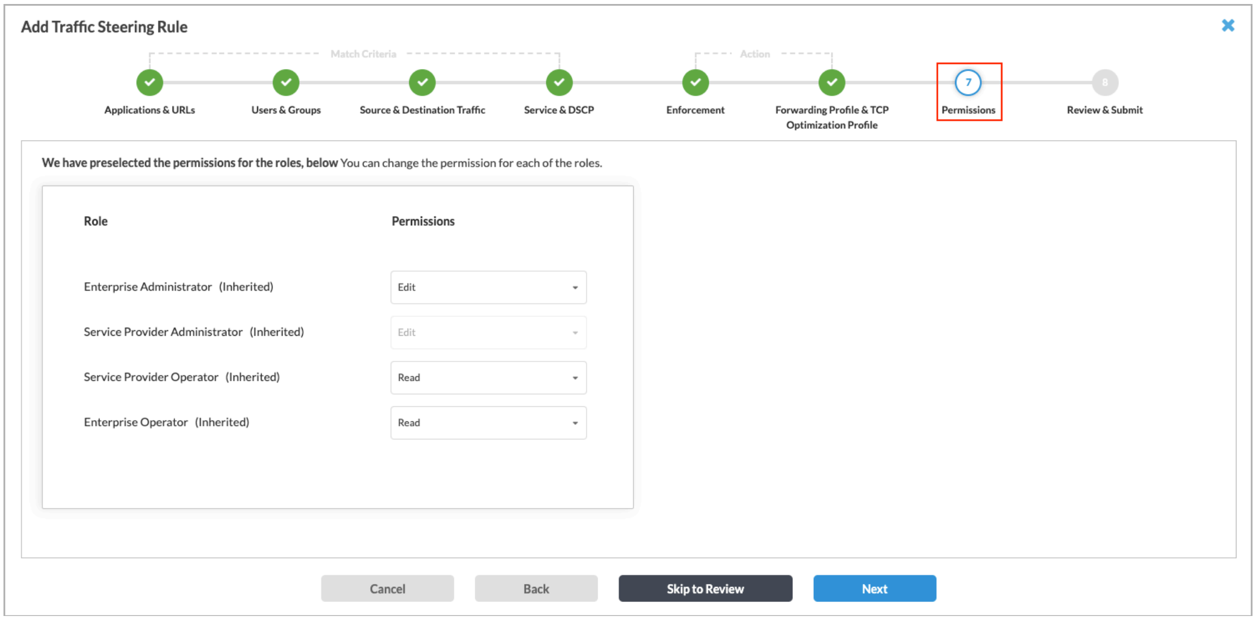
TCP Optimization Profile for LAN: -- Select --

TCP Optimization Profile for WAN: -- Select --

Field	Description
Forwarding Profile	Select a forwarding profile from the list. A forwarding

Field	Description
	profile is a configuration setting that determines how network traffic is handled and forwarded within a network device.
TCP Optimization Profiles Policy (Group of Fields)	TCP optimization profiles are configurations or settings that can be applied to TCP to improve its performance in specific network environments.
◦ Mode	Select a TCP optimization mode: ◦ Auto ◦ Bypass—Disable TCP optimizations. ◦ Forward proxy ◦ Proxy ◦ Reverse proxy ◦ Splice
◦ Bypass Latency Threshold	Enter how much latency must be measured before TCP optimizations begin. *Range*: 0 through 60000 milliseconds *Default*: 10 milliseconds
◦ TCP Optimization Profile for LAN	Select a LAN profile. For proxy mode, you must configure a TCP profile. If you do not select TCP profiles, a system default LAN profile is applied that uses the cubic congestion control algorithm and duplicate ACK loss detection.
◦ TCP Optimization Profile for WAN	Select a WAN profile. For proxy mode, you must configure a TCP profile. If you do not select TCP profiles, a system default WAN profile is applied that uses the BBR congestion control algorithm and RACK loss detection.

36. Click Next to go to Step 7, Permissions, and revise the permissions, if needed.

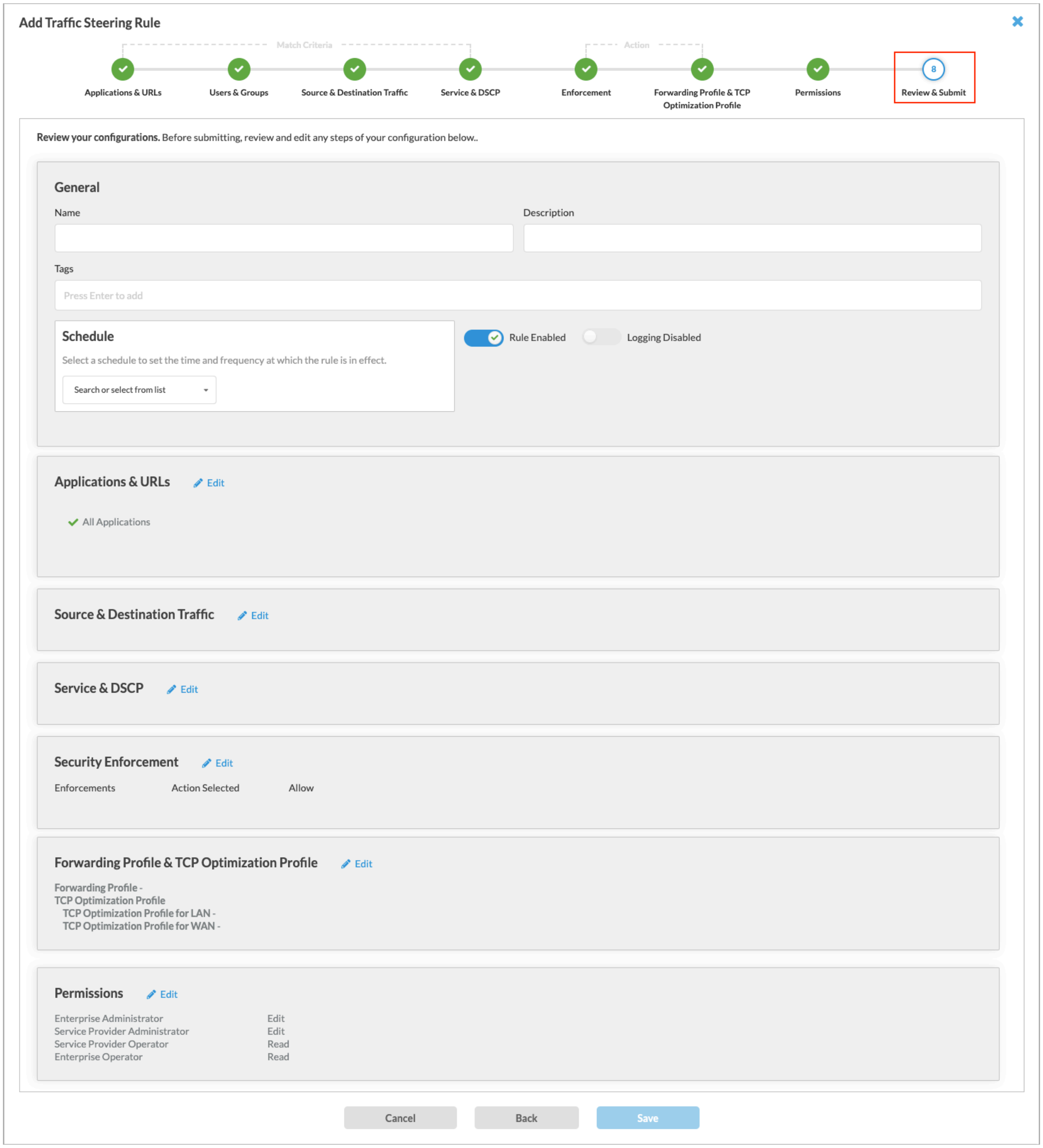


Add Traffic Steering Rule

We have preselected the permissions for the roles, below You can change the permission for each of the roles.

Role	Permissions
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

37. Click Next to go to Step 8, Review and Submit and enter the following information.



Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Name

Description

Tags

Press Enter to add

Schedule

Select a schedule to set the time and frequency at which the rule is in effect.

Search or select from list

Rule Enabled

Logging Disabled

Applications & URLs Edit

✓ All Applications

Source & Destination Traffic Edit

Service & DSCP Edit

Security Enforcement Edit

Enforcements Action Selected Allow

Forwarding Profile & TCP Optimization Profile Edit

Forwarding Profile -
TCP Optimization Profile
TCP Optimization Profile for LAN -
TCP Optimization Profile for WAN -

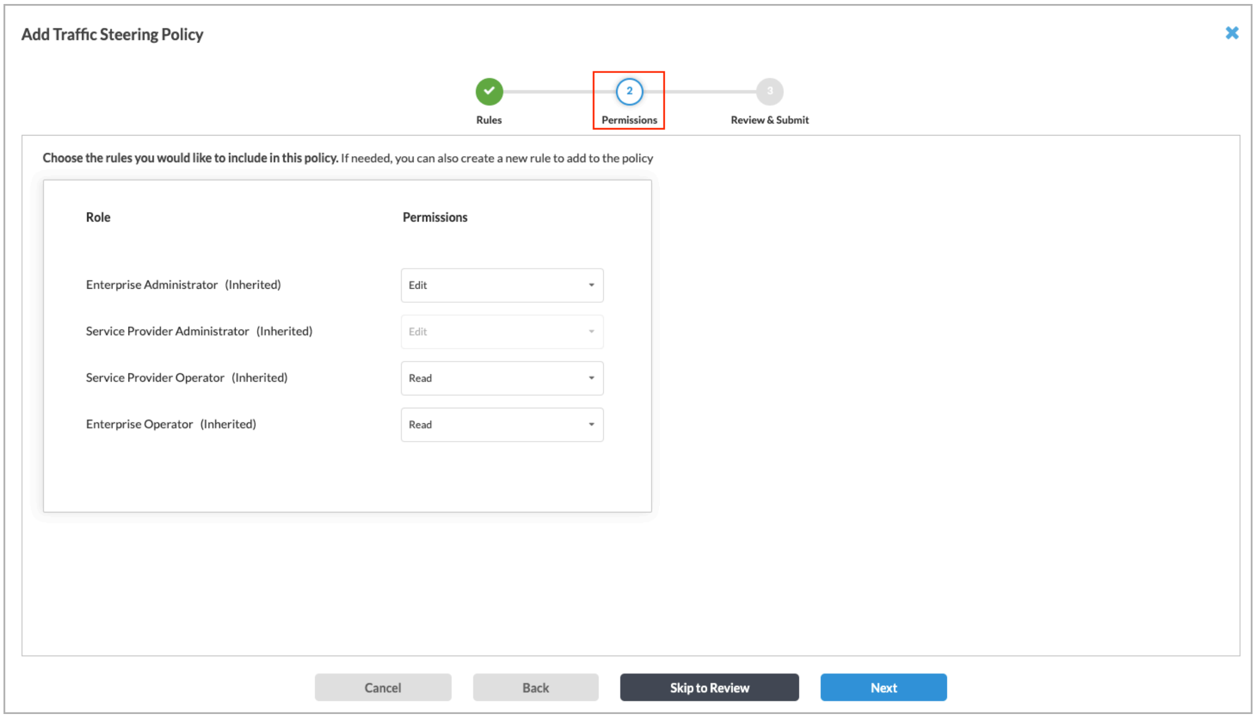
Permissions Edit

Enterprise Administrator	Edit
Service Provider Administrator	Edit
Service Provider Operator	Read
Enterprise Operator	Read

Field	Description
General (Group of Fields)	
◦ Name	Enter a name or the rule.

Field	Description
◦ Description	(Optional) Enter a description for the rule.
◦ Tags	(Optional) Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.
◦ Schedule	Select a schedule to set the time and frequency at which the rule is in effect.
◦ Enabled	Click to disable the rule once it is saved. By default, the rule is enabled.
◦ Logging Disabled	Click to the slider bar to enable logging for the rule. By default, logging is disabled.

38. Review the selected settings. Click the ✎ Edit icon to change a setting, as needed.
39. Click Save to save the rule.
40. In the Add Traffic Steering Policy screen, click Step 2, Permissions. The following screen displays.

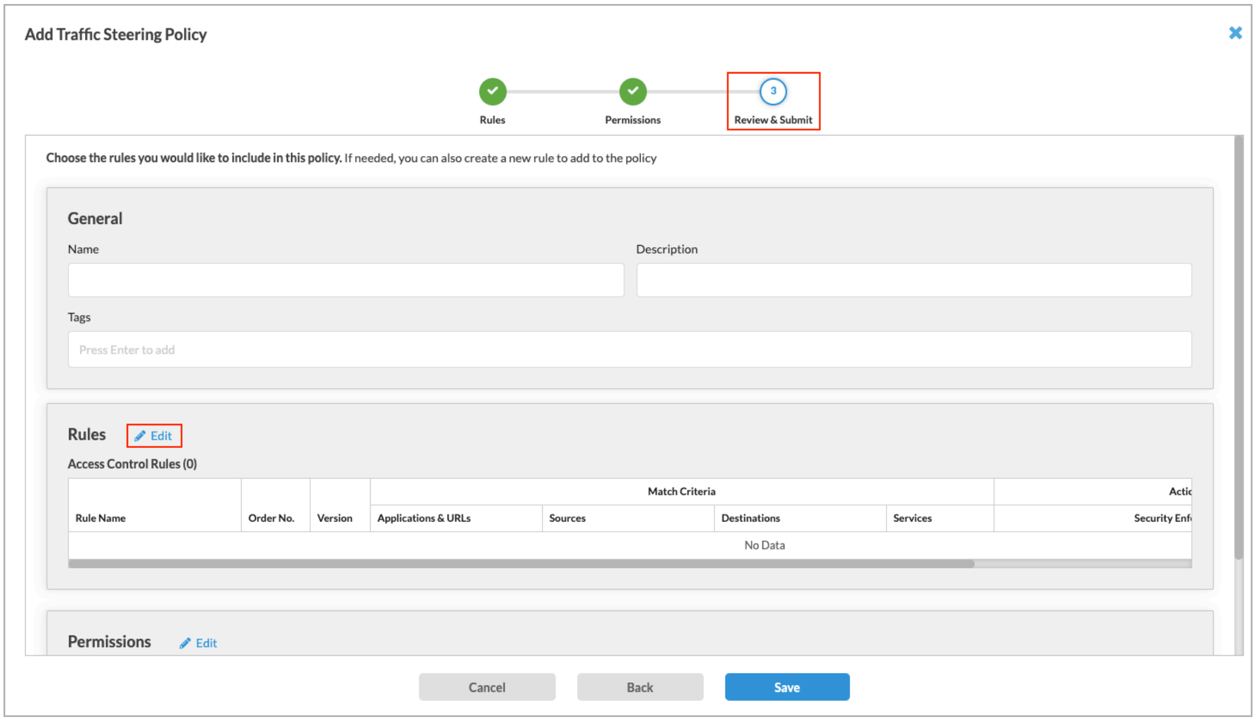


Add Traffic Steering Policy

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

Role	Permissions
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

41. To change the permissions for a role, select Edit, Hide, or Read in the Permissions column.
42. Click Next to go to the Step 3, Review and Submit.



Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

General

Name:

Description:

Tags: Press Enter to add

Rules ✎ Edit

Access Control Rules (0)

			Match Criteria				Actic
Rule Name	Order No.	Version	Applications & URLs	Sources	Destinations	Services	Security Enf
No Data							

Permissions ✎ Edit

43. In the General box, enter a name for the traffic steering policy, and optionally enter a text description for the policy and one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.

44. Review the settings you have selected. Click the ✎ Edit icon to change a setting, as needed.

45. Click Save to create the traffic steering policy.

Supported Software Information

Releases 10.2.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for the Negate Source Address and Negate Destination Address options when configuring a traffic-steering rule.

Additional Information

[Configure Profiles](#)
[Configure Security Access Control Policies and Rules](#)