Configure Microsegmentation

For supported software information, click here.

Microsegmentation is a network security strategy that allows you to divide a network into smaller, isolated segments, called microsegments. You create each microsegment around a specific set of resources or services, and you define access controls and configure security policies that are specific for the resources and services in the microsegment. Traditional network security models primarily rely on securing the network perimeter, using methods such as firewalls to protect the entire network. With microsegmentation, you can divide the network into smaller segments and then apply security controls at a more granular level, thus providing an additional layer of security. You can create security zones in your network and apply security policies to each microsegment to provide enhanced security by restricting lateral movement within the network.

With Versa Operating System^{TM} (VOS^{TM}) microsegmentation, you can place user client devices and clientless (headless) IoT devices into microsegments.

To create a microsegment, you define a policy whose match criteria place a user or device into the microsegment. Then you apply policies to restrict or allow traffic among microsegments.

In VOS microsegmentation policy rules, you can configure match criteria based on information collected by Versa SASE client-based devices and by clientless devices. For end user client devices that use the Versa SASE client, such as laptops, you can configure endpoint information profiles (EIPs), which periodically provide device (endpoint) information to registered SASE gateways. You can then configure microsegmentation access policy rules that match the EIP data provided by the SASE client, which allows the VOS devices to identify user devices and place them into the proper microsegment. Because the SASE client sends periodic updates, the SASE gateways regularly evaluate client devices. For example, if a microsegmentation policy determines that a device's antivirus software is not up to date, thus making the device vulnerable to attack, it can place the device into a quarantined microsegment to ensure that the device cannot communicate with other users or devices in the network. Then, if the device's antivirus software is upgraded, after the SASE client conveys this information to the first-hop SASE gateway, the microsegmentation policy can move the device into a non-quarantined microsegment.

For headless IoT devices that do not run the Versa SASE client, such as sensors and printers, you use VOS device fingerprinting to identify the device based on its model, vendor, and other associated attributes. You can then configure microsegmentation access policy rules that match the fingerprinting data, which allows the VOS devices to identify user devices and place them into the proper microsegment.

This article describes how to configure microsegmentation policy and rules, associate microsegments with NPU and

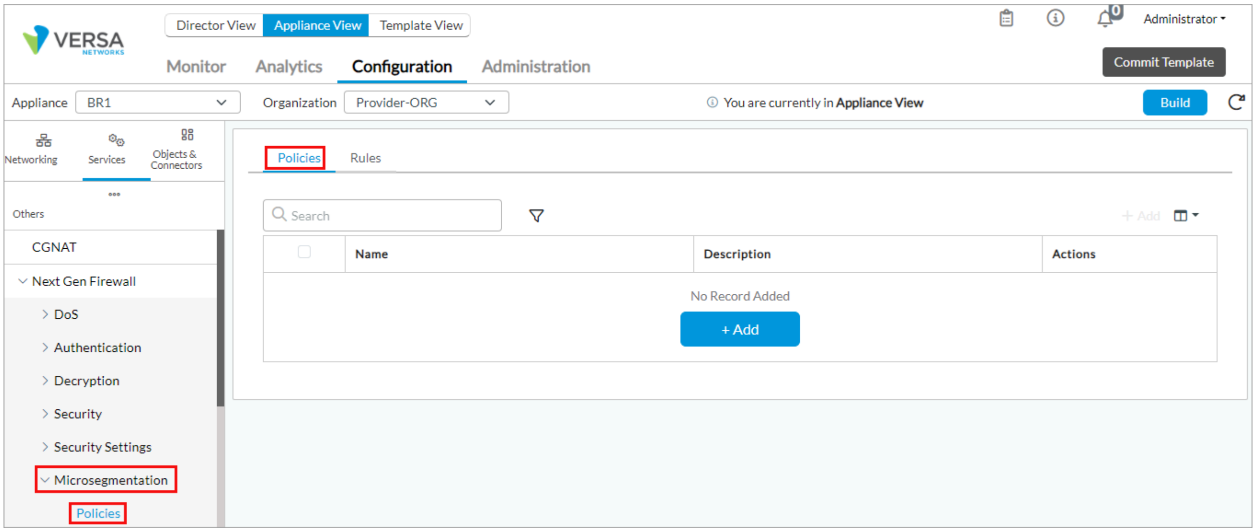
NGFW policies, and monitor microsegmentation policies and statistics.

Configure Microsegmentation Policies

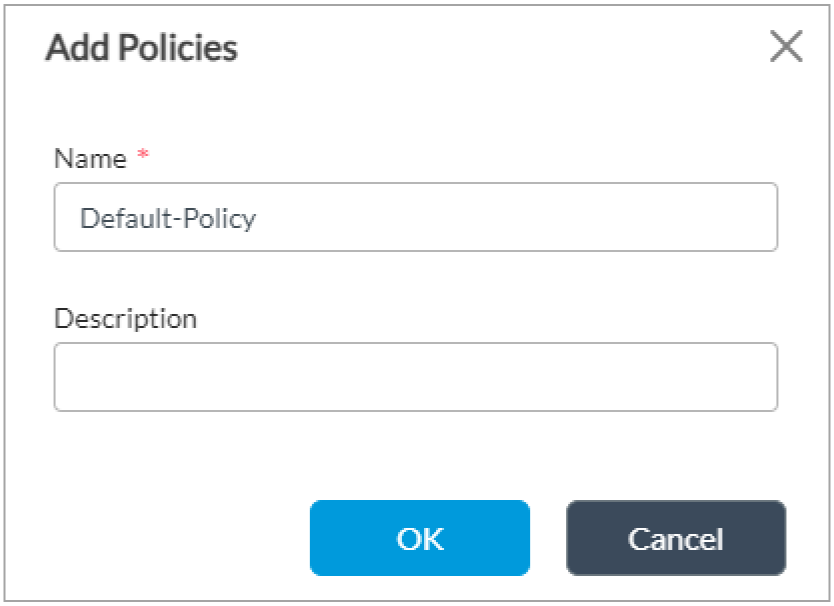
To create a microsegmentation policy, first you create a policy, and then you create rules to place devices and users in microsegments.

Configure a Microsegmentation Policy

1. 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.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Microsegmentation > Policies in the left menu bar. For more information about enabling NGFW, see Enable NGFW in Configure NGFW.



4. In the Policies tab click + Add. In the Add Policies popup window, enter information for the following fields.



Add Policies

Name *

Default-Policy

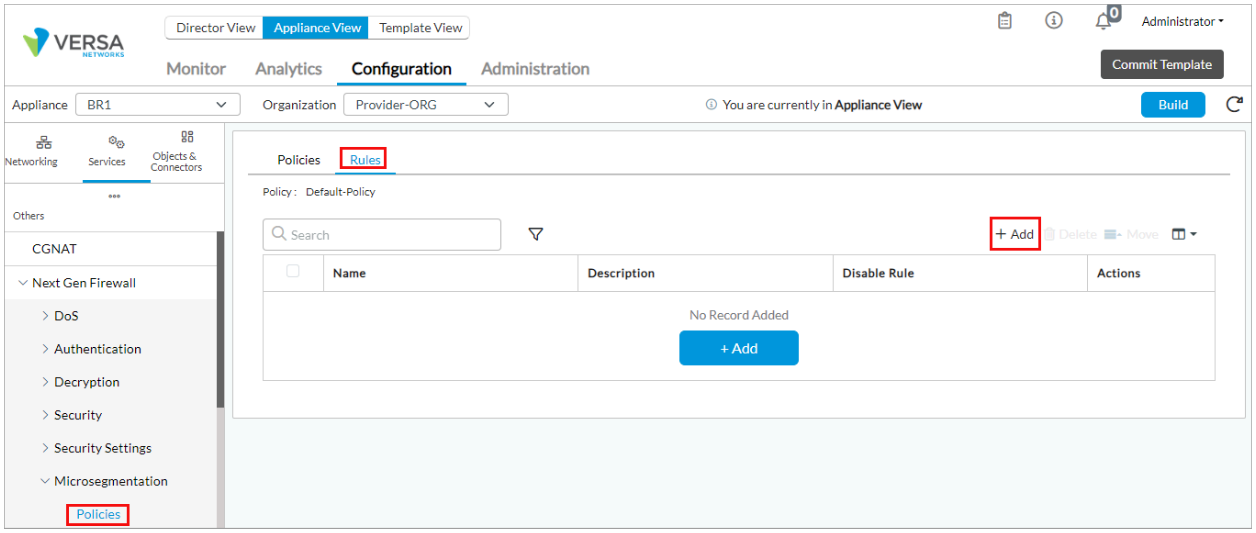
Description

Field	Description
Name (Required)	Enter a name for the microsegmentation policy. The name, Default-Policy, displays by default, which you can edit.
Description	Enter a text description for the microsegmentation policy.

5. Click OK.

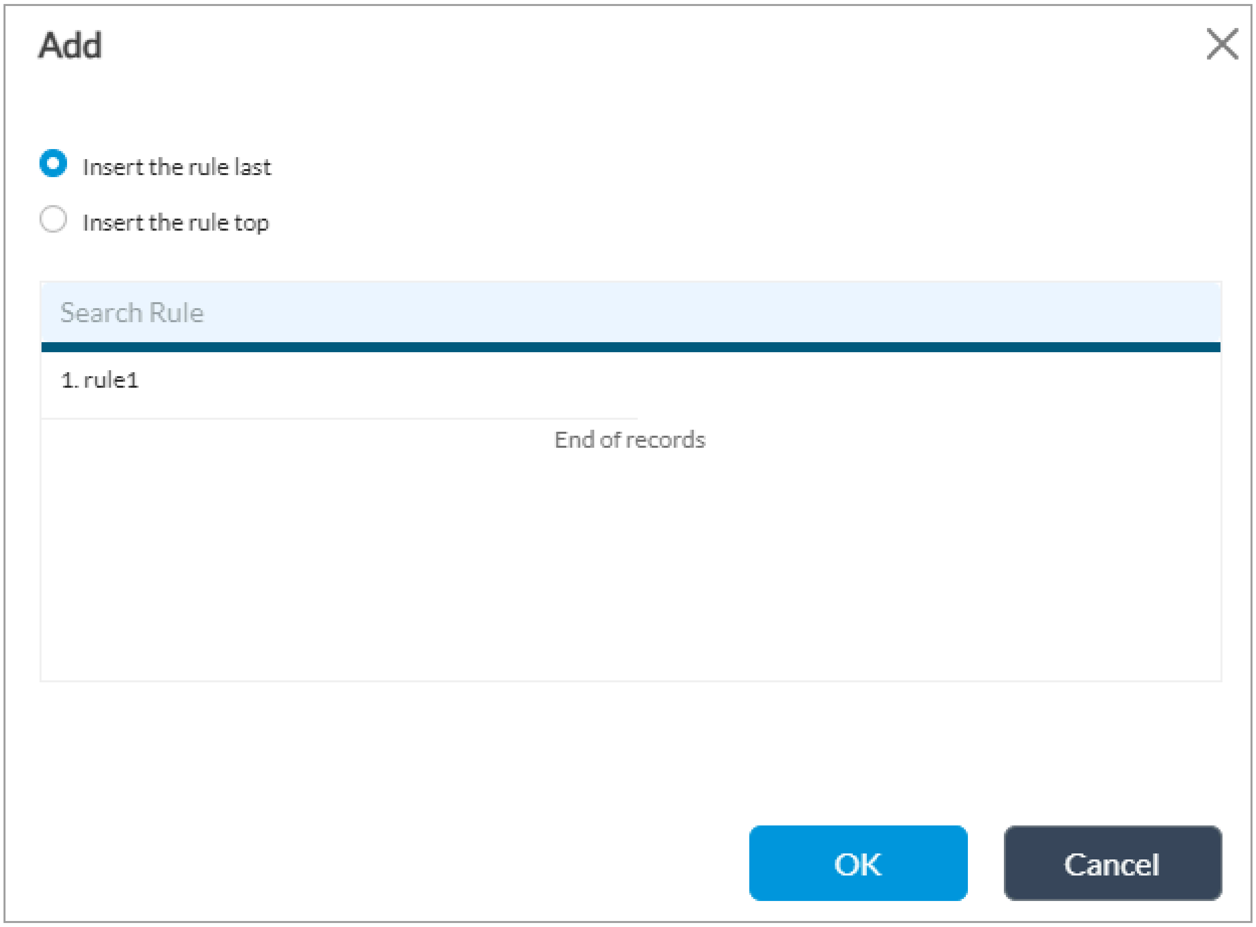
Configure Microsegmentation Rules

1. 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.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Microsegmentation > Policies in the left menu bar.

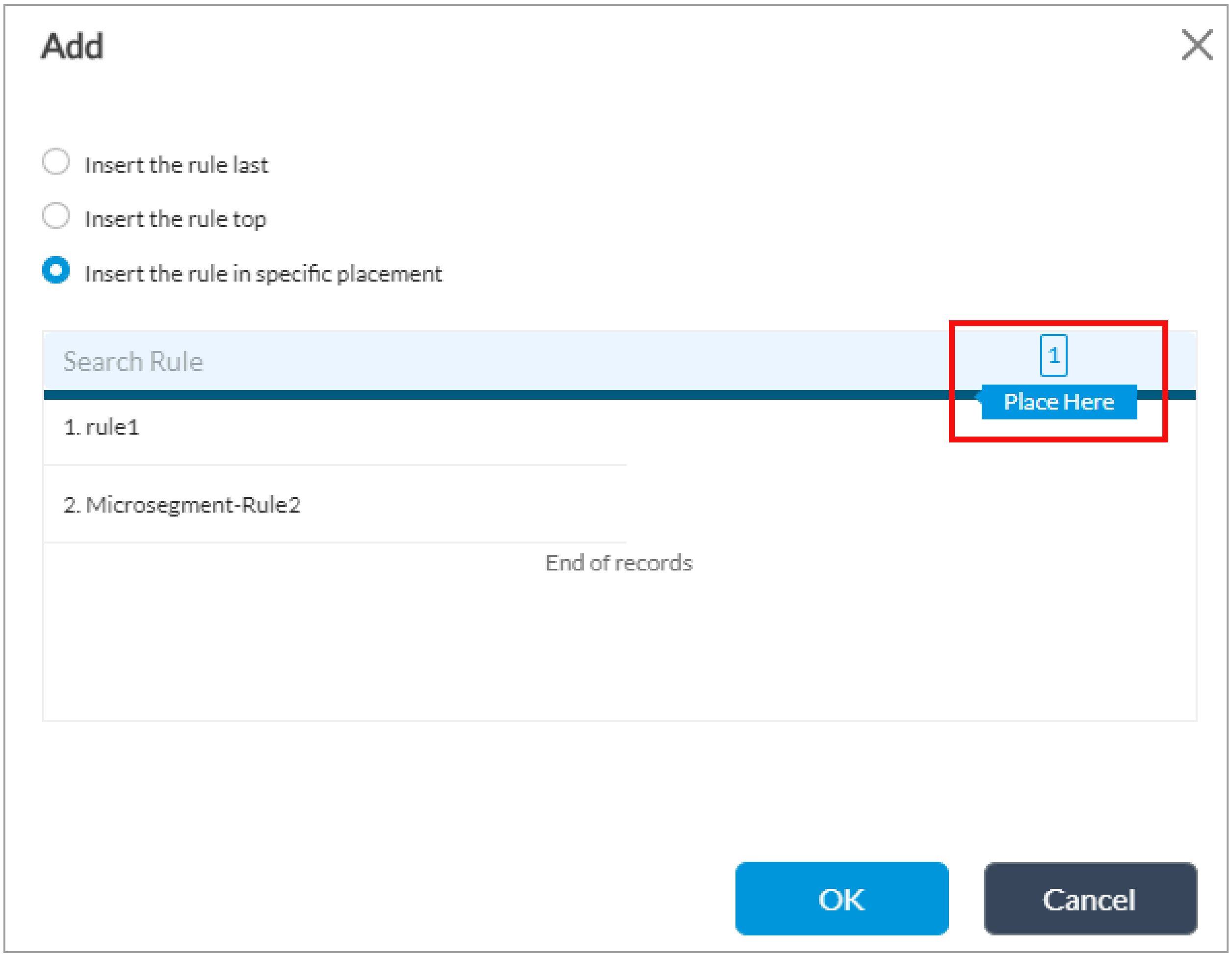


	Name	Description	Disable Rule	Actions

4. Select the Rules tab, and then click + Add.
5. If you have already added a rule, the Add popup window displays.
   a. Select where you want to insert the policy rule, either at the beginning or end of the existing rule.



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



Add

○ Insert the rule last

○ Insert the rule top

● Insert the rule in specific placement

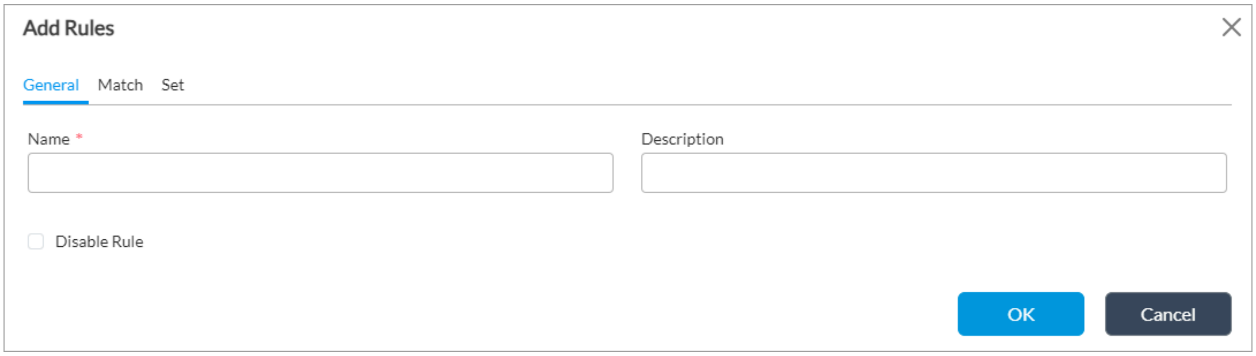
Search Rule

1. rule1
2. Microsegment-Rule2

End of records

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

6. Select the General tab, and then enter Information for the following fields.



Add Rules

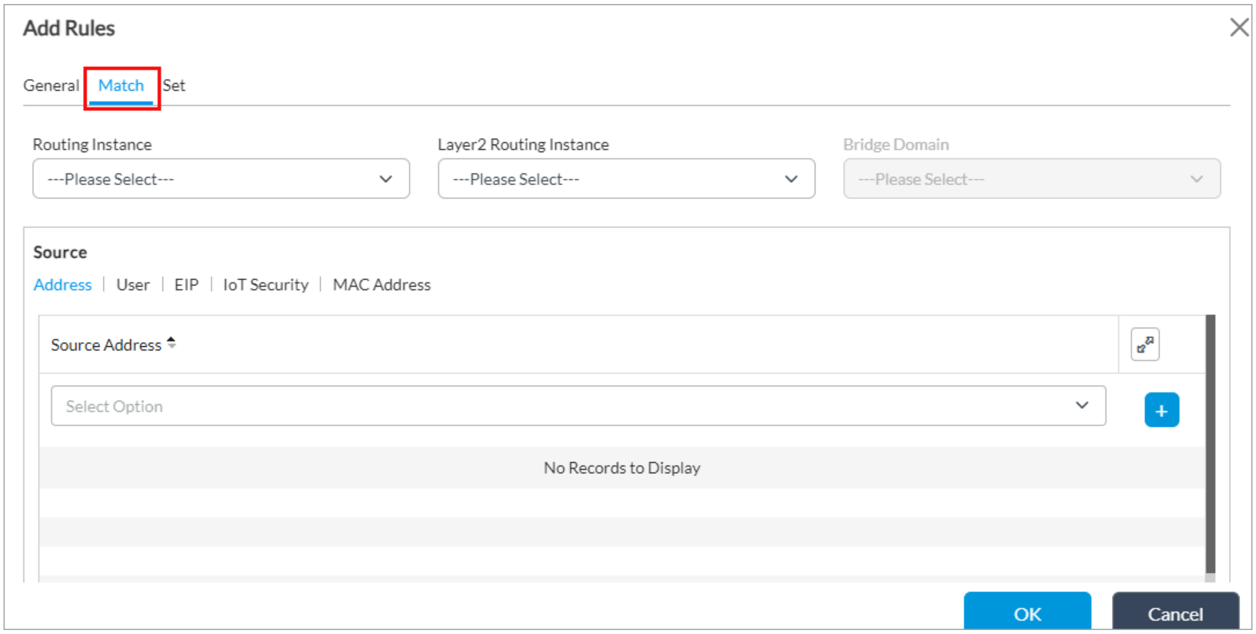
Name *

Description

□ Disable Rule

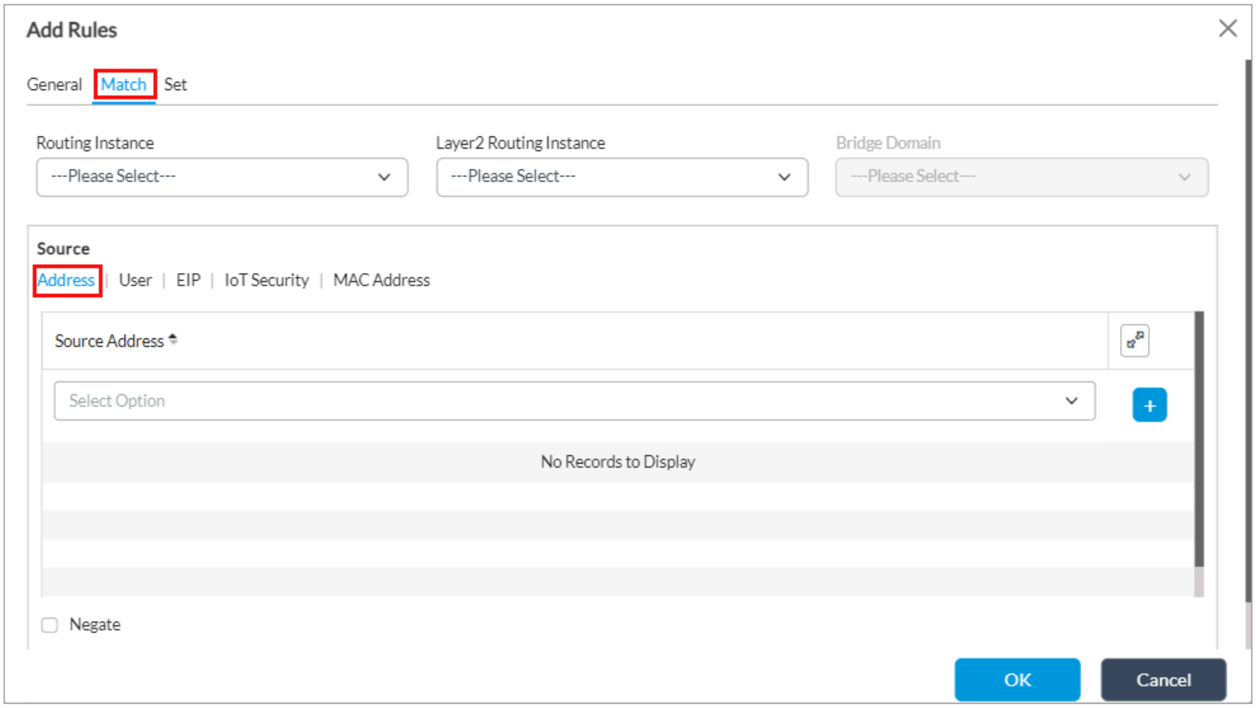
Field	Description
Name (Required)	Enter a name for the microsegmentation rule.
Description	Enter a text description for the microsegmentation rule.
Disable Rule	Click to disable the rule. You can disable a rule to skip it from evaluating traffic and to use other rules in the policy in the configuration order.

7. Select the Match tab, and then enter information for the following fields.



Field	Description
Routing Instance	Select a routing instance on which to match incoming traffic. You can select a router instance or a Layer 2 routing instance, but not both.
Layer 2 Routing Instance	Select a Layer 2 routing instance of type Virtual Switch. This matches the incoming traffic on the bridge domain you select in the Bridge Domain field. Because a bridge domain is Layer 2, you must configure a virtual switch instead of a virtual router. You can select a router instance or a Layer 2 routing instance, but not both.
Bridge Domain	If you select Layer 2 Routing Instance, select a bridge domain for Layer 2 routing instance.

8. In the Source field, select the Address tab, and then enter information for the following fields.



Add Rules

Routing Instance: ---Please Select---

Layer2 Routing Instance: ---Please Select---

Bridge Domain: ---Please Select---

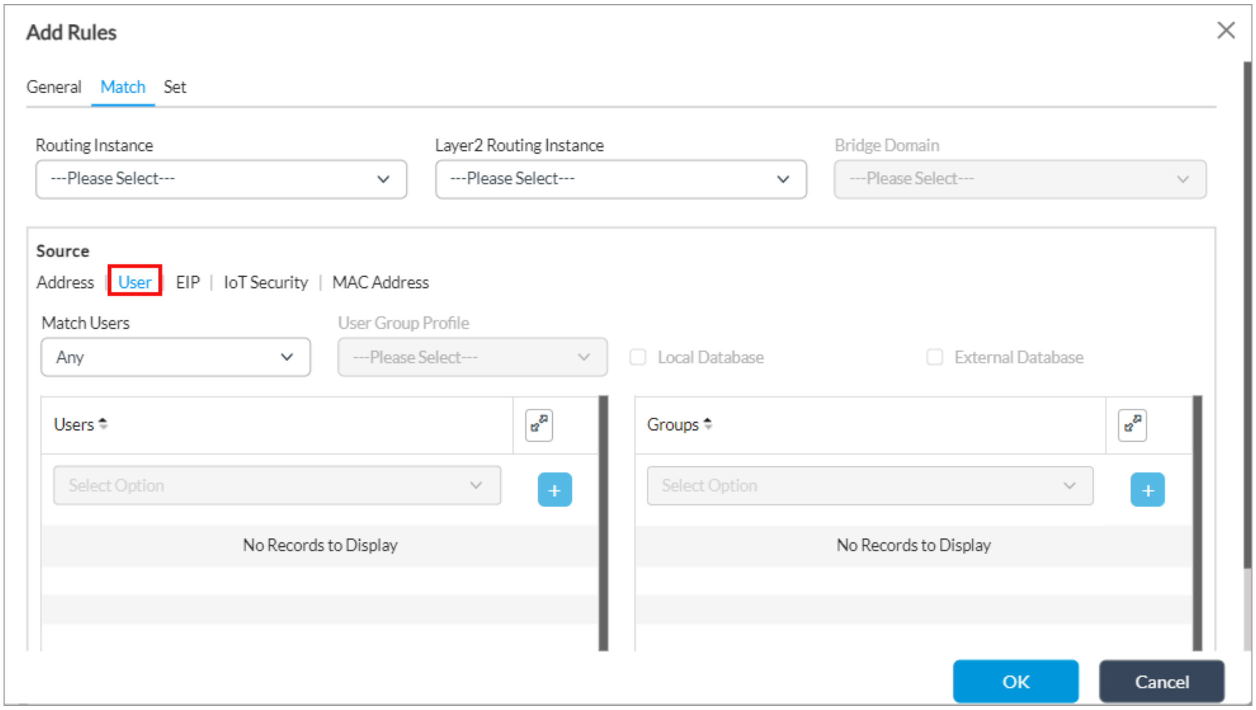
Source

No Records to Display

□ Negate

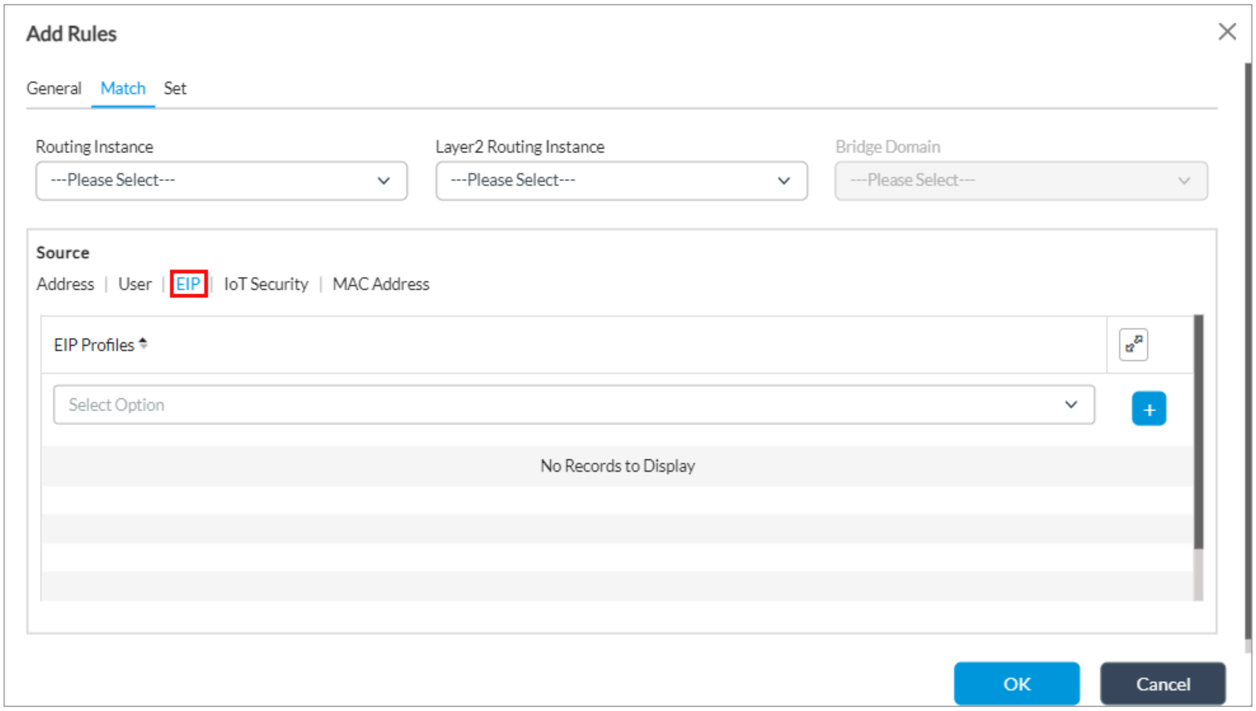
Field	Description
Source Address	Select the one or more source addresses or source address groups of incoming traffic to match, and then click the + Add icon.
Negate	Click to block traffic to the selected source addresses or groups instead of accepting it.

9. Select the User tab, and then enter information for the following fields.



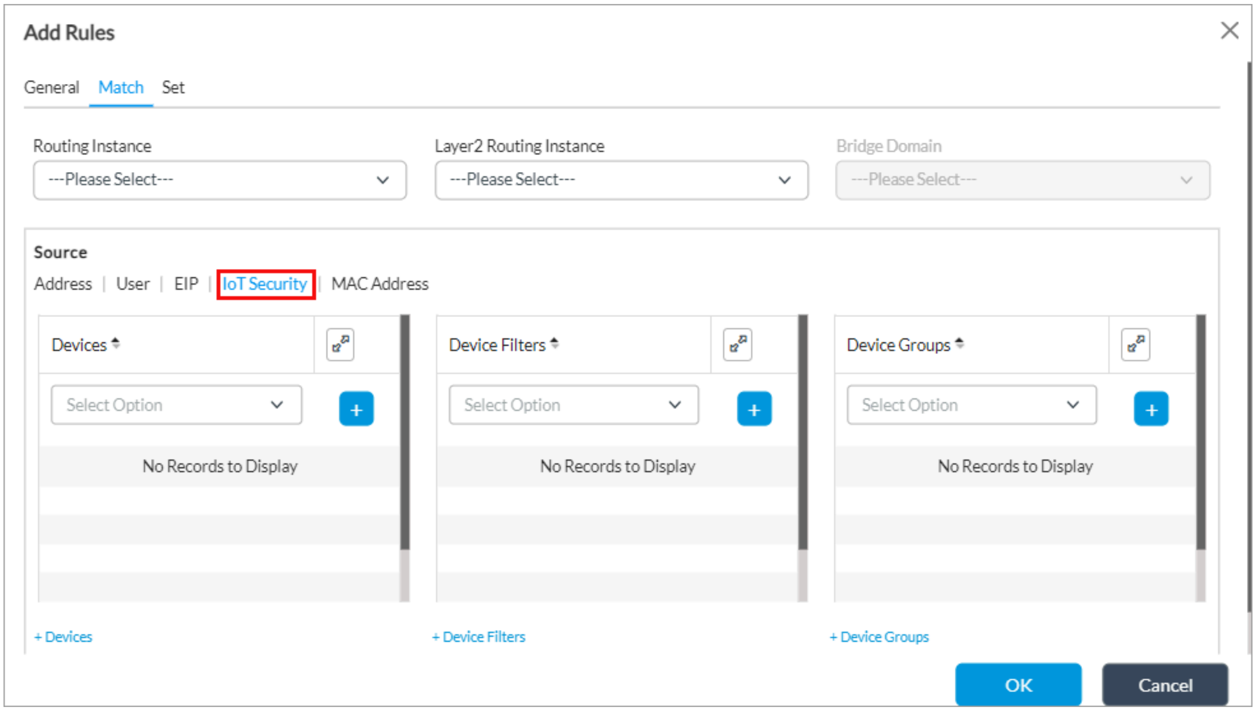
Field	Description
Match Users	Select the users to match. You can select only one option. ◦ Any—Match any users. ◦ Known—Match known users. ◦ Selected—Match selected users. ◦ Unknown—Match unknown users.
User Group Profile	If you match selected users, select a user group profile to match the users in the group.
Local Database	If you match selected users, click to create a local database to match users and user groups. Select these users and user groups in the Users and Groups fields. For more information, see Configure a Local Database.
External Database	If you match selected users, click to use an external database to match users and user groups. Select these users in the Users and Groups fields. For more information, see Configure User and Group Policy.
Users	If you match selected users, select a user and then click the + Add icon to add the user.
Groups	If you match selected users, select a user group and then click the + Add icon to add the group.

10. Select the EIP Profiles tab to associate endpoint information profiles (EIPs) with the rule.



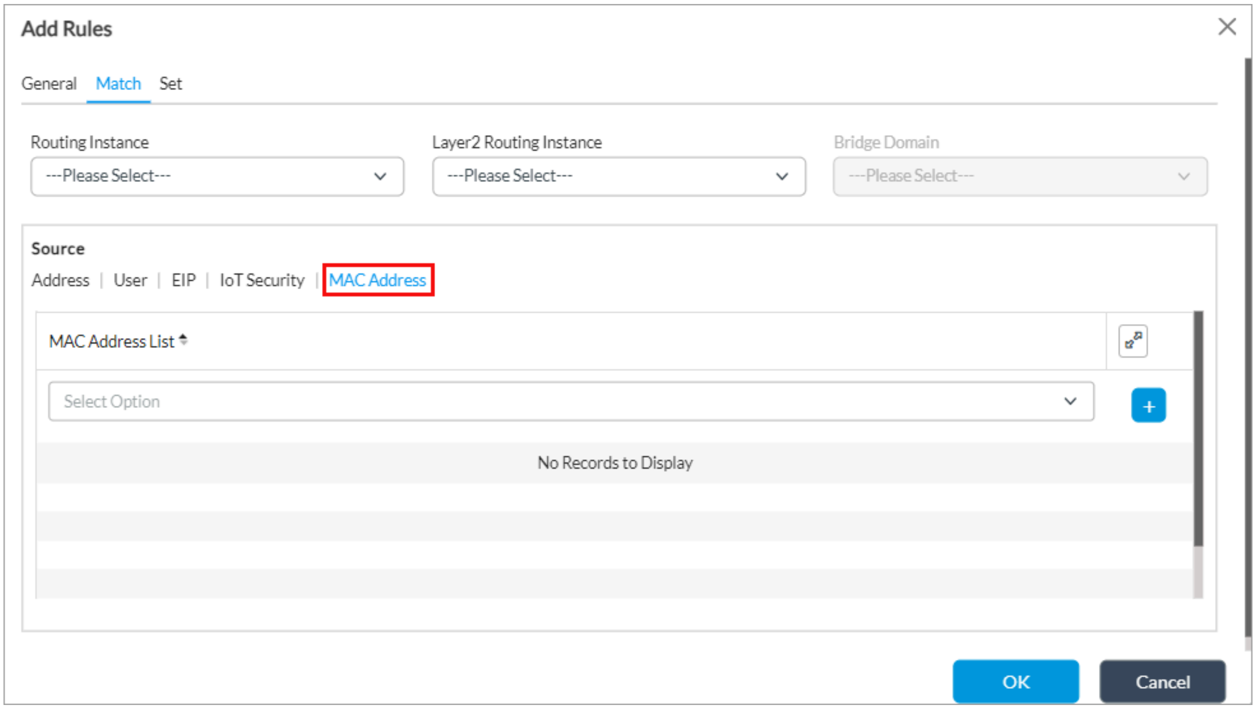
11. In the EIP Profiles table, select one or more user-defined or predefined EIP profiles, and then click the + Add icon to associate EIP with the rule. With EIPs, you collect information about the security status of the endpoint devices connecting to your networks, such as whether they have the latest security patches and antivirus definitions installed. For more information, see [Configure Endpoint Information Profiles](#).

12. Select the IoT Security tab, and then enter information for the following fields.

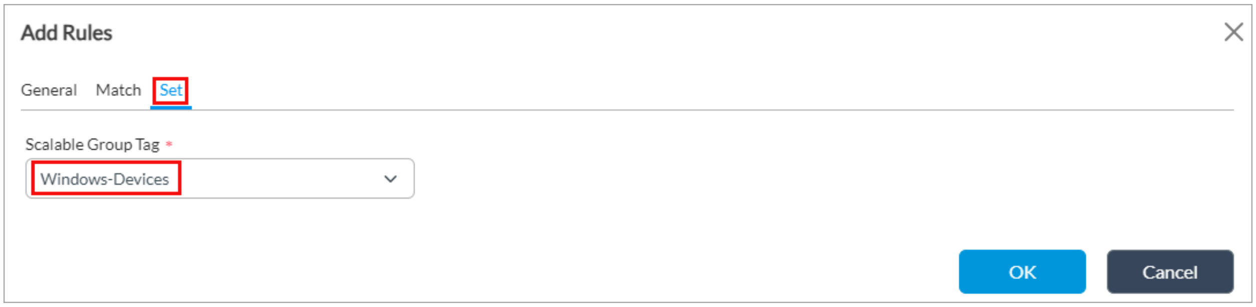


Field	**Description**
Devices	Select user-defined or discovered devices to associate with the rule, and then click the + Add icon to add the device. Click + Devices to add an IoT security device. When you enable IoT security, VOS starts to discover and identify devices that enter your network traffic. For more information, see Configure IoT Security.
Device Filters	Select user-defined or predefined device filters to associate with the rule, and then click the + Add icon to add a device filter. Click + Device Filters to add an IoT security device filter. For more information, see Configure IoT Security.
Device Groups	Select a IoT device group to associate with the rule, and then click the + Add icon to add a device group. Click + Device Groups to add an IoT security device group. For more information, see Configure IoT Security.

13. Select the MAC Address tab to configure match criteria based on source MAC addresses.



14. In the MAC Address List table, select a MAC address, and the click the + Add icon.
15. Click OK.
16. Select the Set tab to select scalable group tags (SGTs) to classify and tag network traffic, and then define security policies to take actions on this traffic.



Scalable Group Tag * Windows-Devices

17. In the Scalable Group Tag field, select an SGT. Clients that match the filter criteria are placed in this microsegment for this rule.
18. Click OK.

Associate Microsegments with NGFW and NPU Policies

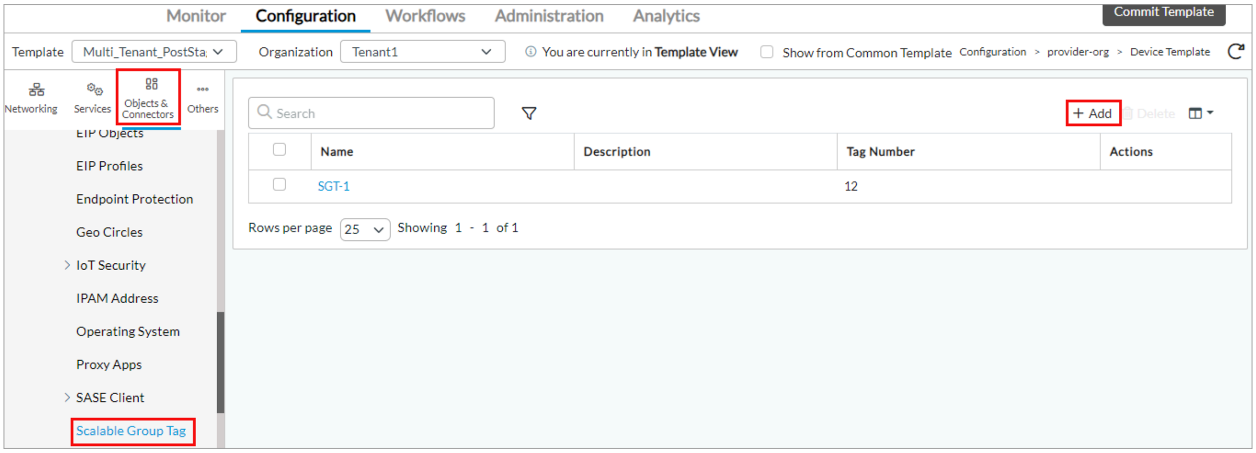
You add match parameters in NPU and NGFW policy rules to match microsegments.

One method to associate a microsegment with an NPU or NGFW rule is to associate the SGT ID used in a microsegmentation rule with an NPU or NGFW rule. For this type of configuration, you do the following:

- Create an SGT object.
- Associate the SGT object with a microsegmentation rule.
- Associate the SGT object with an NPU ACL policy rule or an NGFW security policy rule.

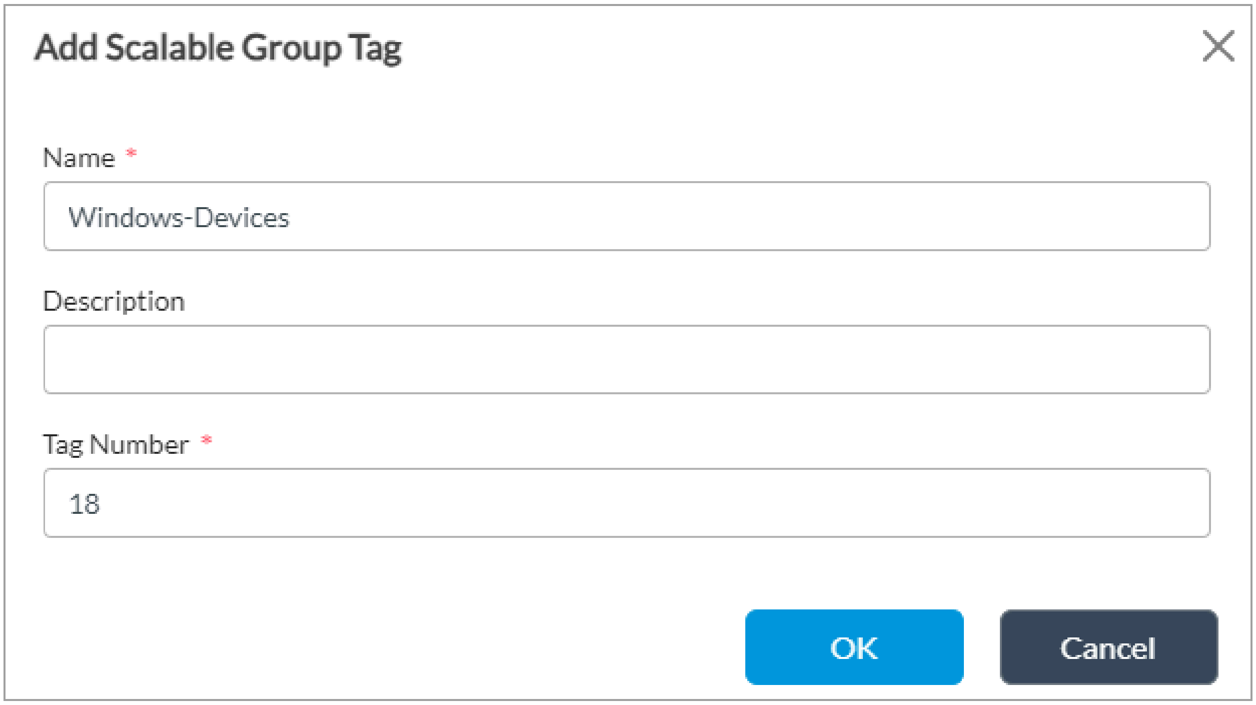
Create an SGT Object

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Templates > Device Templates in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Scalable Group Tag in the left menu bar.



Name	Description	Tag Number	Actions
SGT-1		12	

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


Add Scalable Group Tag

Name *

Windows-Devices

Description

Tag Number *

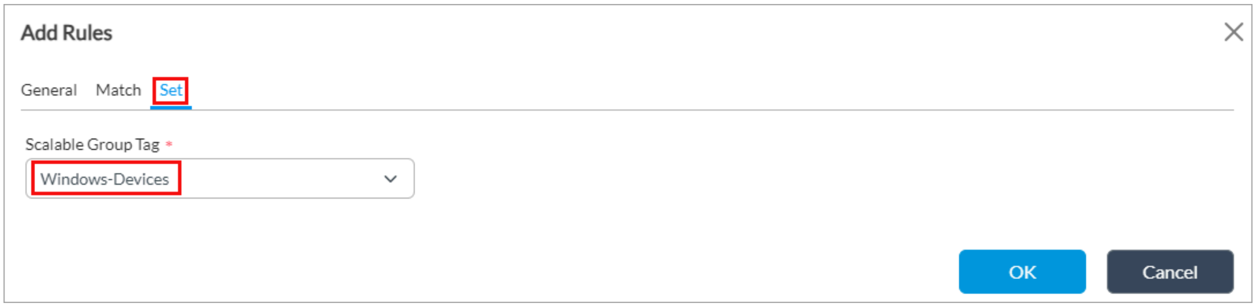
18

Field	Description
Name (Required)	Enter a name for the SGT (here, Windows-Devices).
Description	Enter a text description for the SGT.
Tag Number (Required)	Enter a tag number. *Range*: 0 to 4094

5. Click OK.

Associate the SGT with a Microsegmentation Rule

1. 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.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Microsegmentation > Policies in the left menu bar.
4. Select the Rules tab and click + Add.
5. In the Add Rules popup window, select the Set tab.



Scalable Group Tag * Windows-Devices

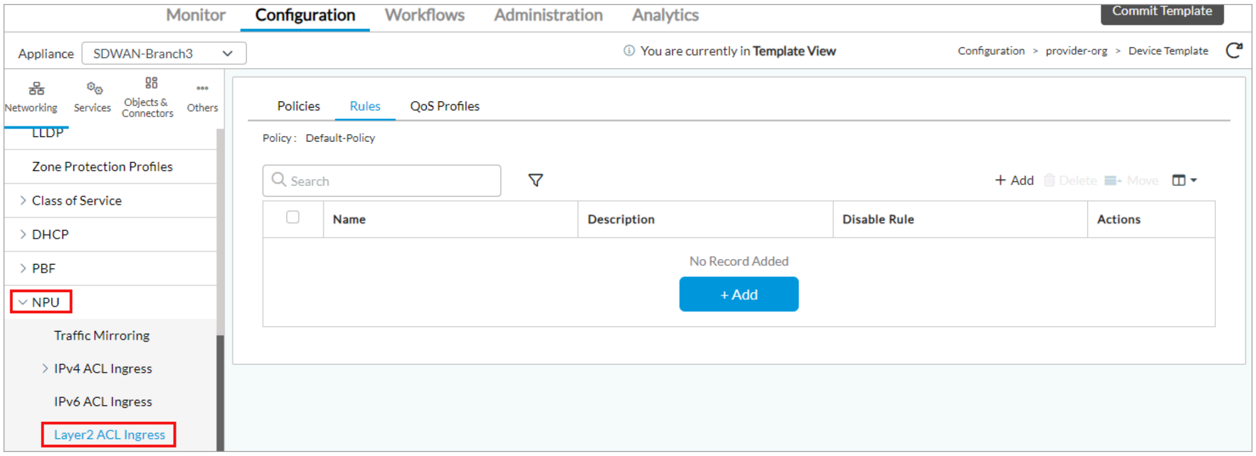
6. In the Scalable Group Tag field, select the SGT (here, Windows-Devices) that you configured in [Create an SGT Object](), above.
7. For information about configuring other parameters, see [Configure Microsegmentation Rules](), above.

Associate the SGT with an NPU ACL Policy Rule

In this example, we associate the SGT with a Layer 2 ingress ACL rule. You can associate SGT with Layer 2 IPv4 and IPv6, Layer 3 IPv4 (single wide and double wide), and Layer 3 IPv6 ACL rules. For more information, see [Configure NPU Policy-Based Forwarding]().

To configure a Layer 2 ingress ACL policy:

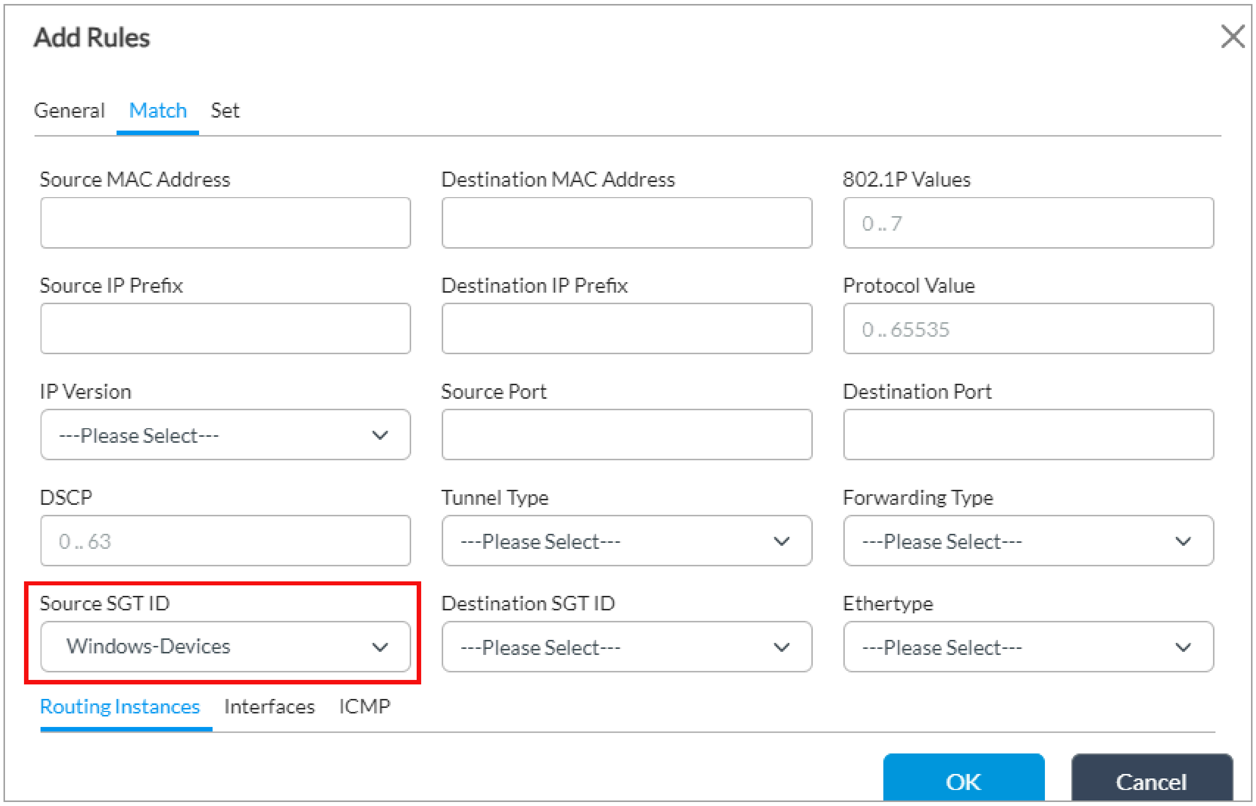
1. In Director View:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Click the name of an appliance. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > NPU > Layer 2 ACL Ingress in the left menu bar.



Policy : Default-Policy

☐	Name	Description	Disable Rule	Actions

4. Select the Policies tab, and then click the + Add icon or the + Add button. The Add Rules popup window displays.
5. Select the Match tab.

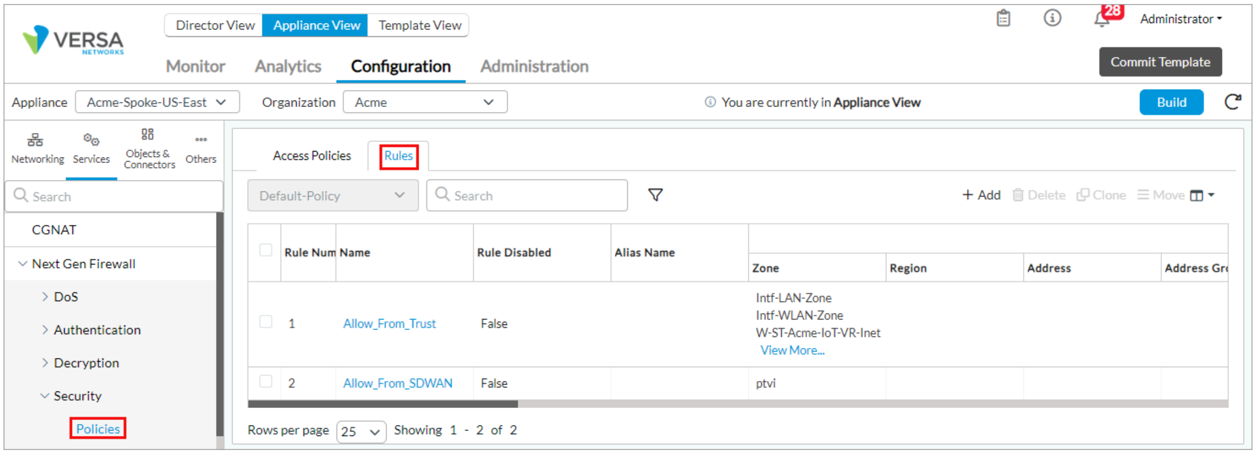


Source SGT ID: Windows-Devices

6. In the Source SGT ID or Destination SGT ID field, select the SGT (here, Windows-Devices) that you configured in Create an SGT Object, above.
7. For information about configuring other parameters, see Configure Layer 2 Ingress ACLs.
8. Click OK.

Associate the SGT with an NGFW Security Policy Rule

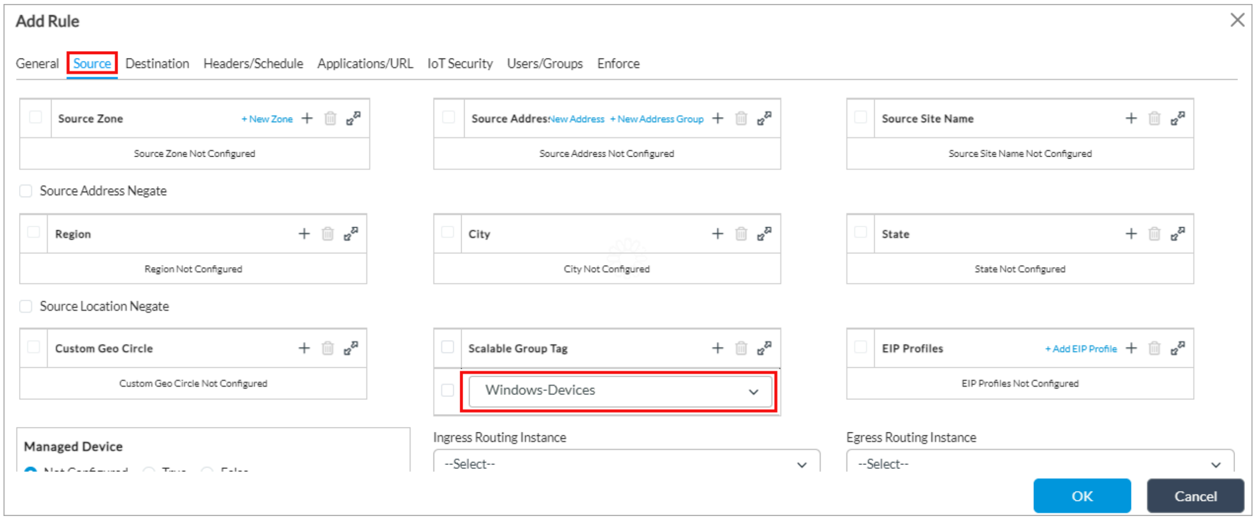
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and then select the Rules tab.



	Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Gr
□	1	Allow_From_Trust	False		Intf-LAN-Zone Intf-WLAN-Zone W-ST-Acme-IoT-VR-Inet View More...			
□	2	Allow_From_SDWAN	False		ptvi			

Rows per page 25 Showing 1 - 2 of 2

4. Click + Add to define rules for the policy. The Add Rule popup window displays.
5. Select the Source 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: Windows-Devices

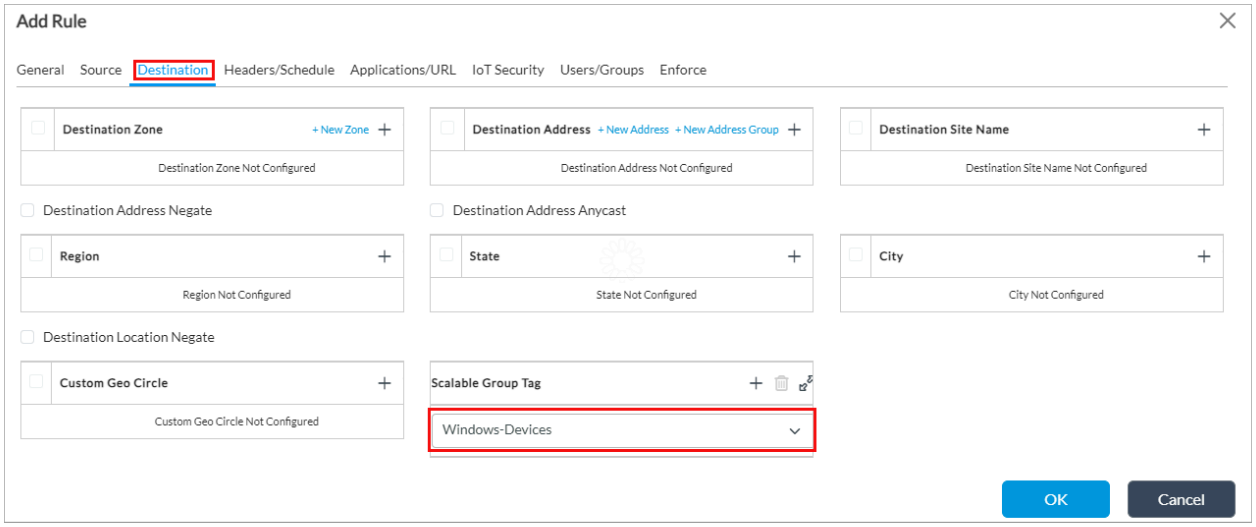
EIP Profiles: EIP Profiles Not Configured

Managed Device: ● Not Configured ○ True ○ False

Ingress Routing Instance: --Select--

Egress Routing Instance: --Select--

6. In the Scalable Group Tab field, select the SGT (here, Windows-Devices) that you configured in Create an SGT Object, above.
7. For information about configuring other parameters, see Configure Access Policy Rules (ACL Rules) in Configure NGFW.
8. To associate the SGT with the destination traffic, select the Destination tab.



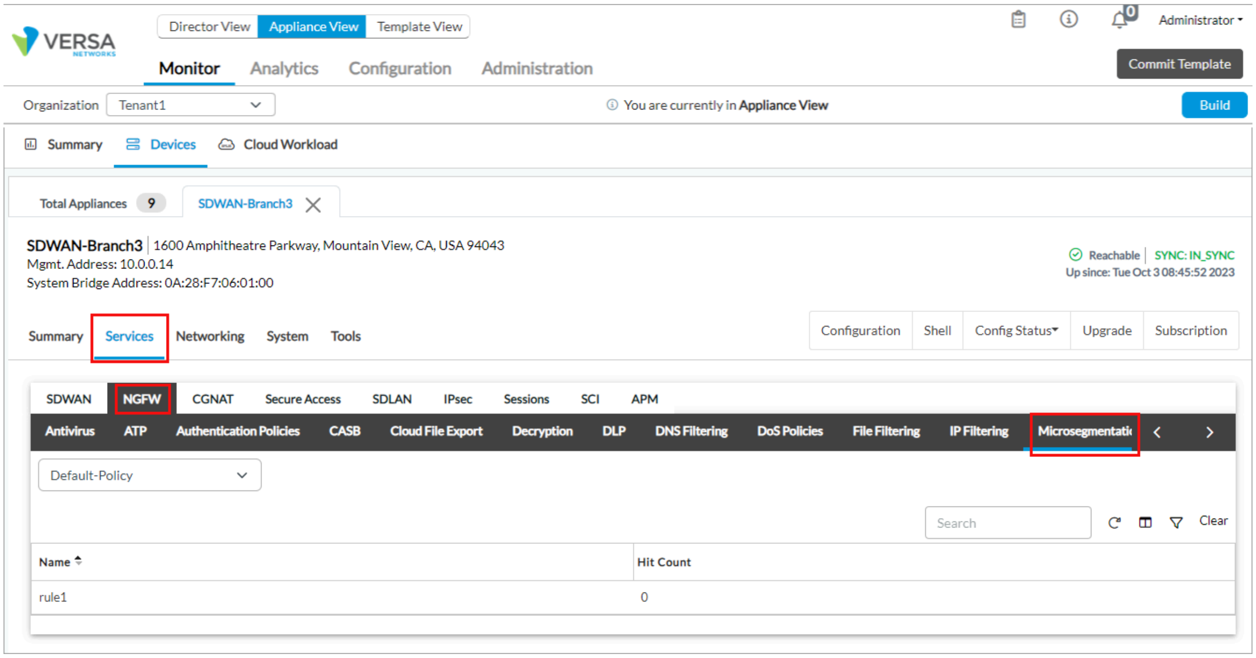
Scalable Group Tag: Windows-Devices

9. In the Scalable Group Tag field, select the SGT (here, Windows-Devices) that you configured in Create an SGT Object, above.
10. Click OK.

Monitor Microsegmentation Policies and Statistics

To monitor a microsegmentation policy:

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 device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the provider organization in the left menu bar.
4. Select the Services tab in the horizontal menu bar.
5. Select NGFW > Microsegmentation, and then select the microsegmentation policy. The table displays the rules associated with the microsegmentation policy and the number of times each rule has been used in evaluating traffic.



Organization: Tenant1

You are currently in Appliance View

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

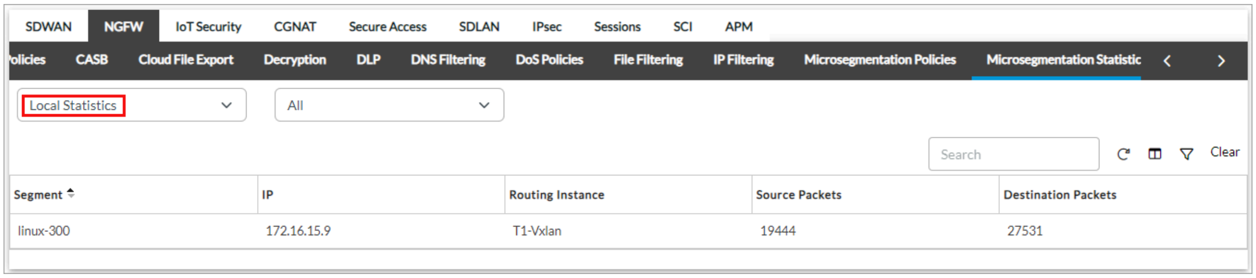
Reachable | SYNC: IN_SYNC
Up since: Tue Oct 3 08:45:52 2023

Default-Policy

Name	Hit Count
rule1	0

To view statistics about microsegments:

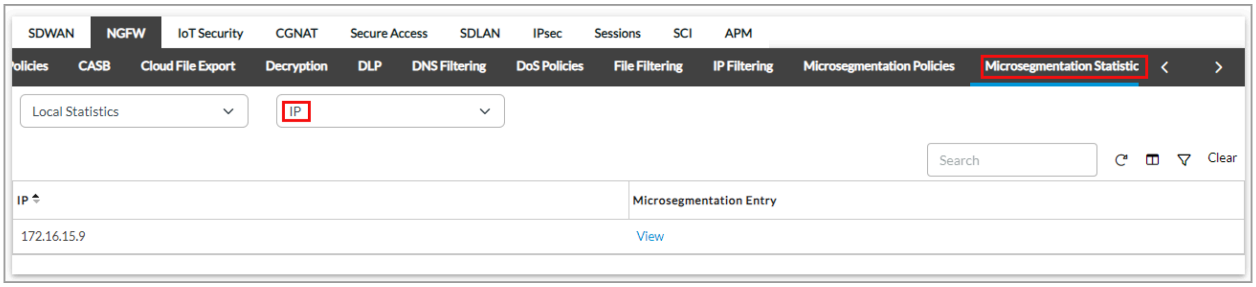
1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
    c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the provider organization in the left menu bar.
4. Select the Services tab in the horizontal menu bar.
5. Select NGFW > Microsegmentation Statistics.
6. In the first filter field, select Local Statistics, and then select All, IP address, Routing Instance, or Segment in the second filter field. For example:
    a. Select Local Statistics and All to display all information about a microsegment:



Local Statistics | All

Segment	IP	Routing Instance	Source Packets	Destination Packets
linux-300	172.16.15.9	T1-Vxlan	19444	27531

    b. Select Local Statistics and IP to display IP address information about a microsegment:

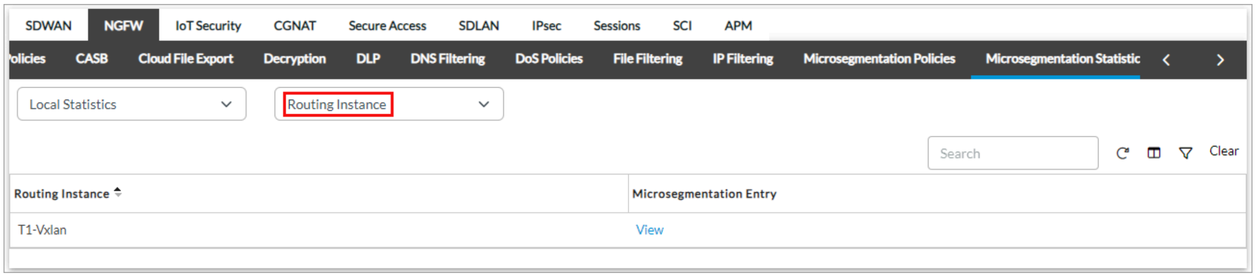


Local Statistics

IP

IP	Microsegmentation Entry
172.16.15.9	View

c. Select Local Statistics and Routing Instance to display routing instance information about a microsegment:

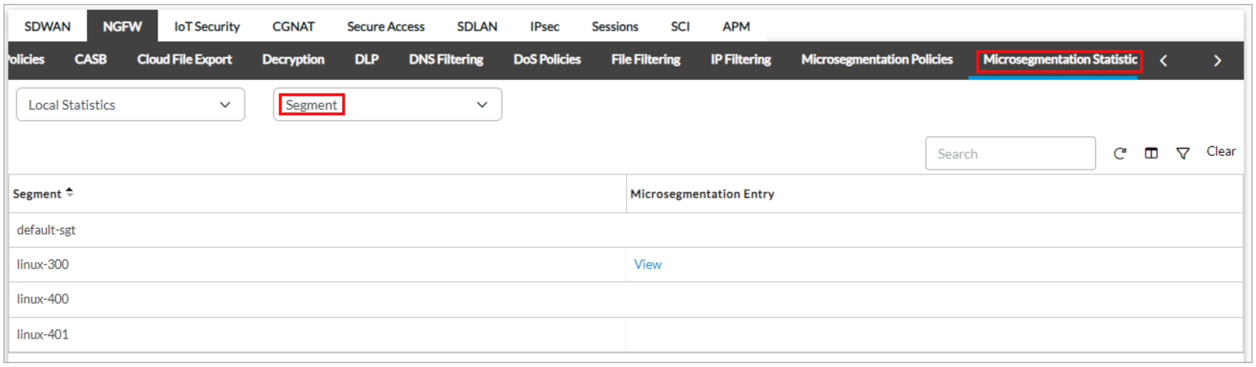


Local Statistics

Routing Instance

Routing Instance	Microsegmentation Entry
T1-Vxlan	View

d. Select Local Statistics and Segment to display microsegment information:

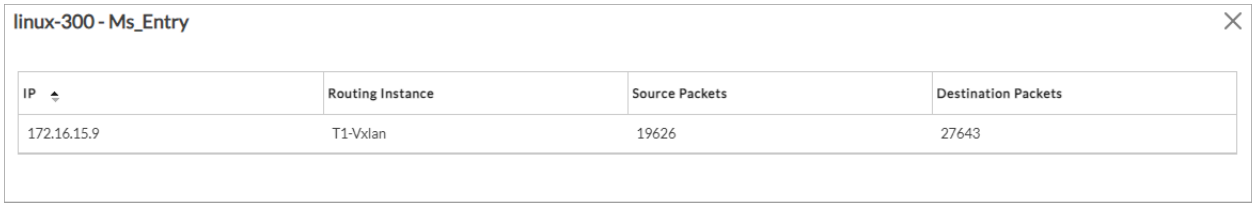


Local Statistics

Segment

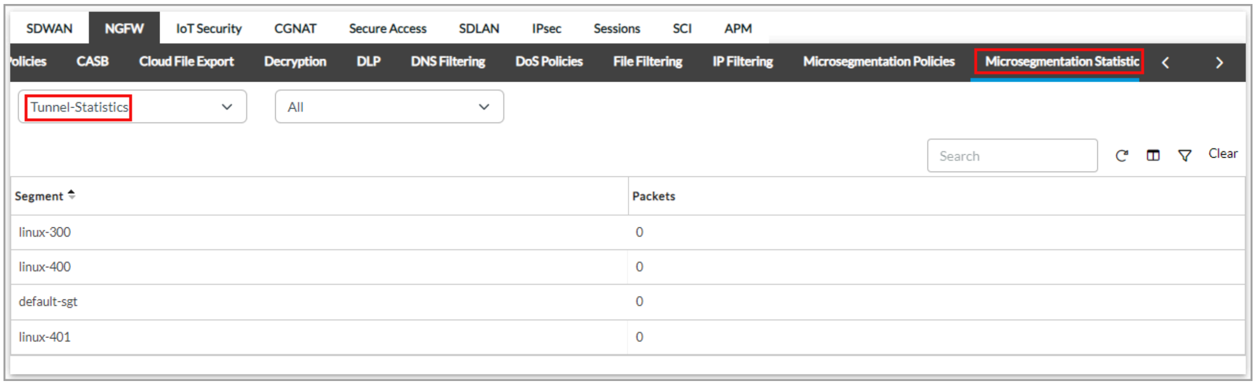
Segment	Microsegmentation Entry
default-sgt	
linux-300	View
linux-400	
linux-401	

e. Click View in any of the windows to display more details:


linux-300 - Ms_Entry

IP	Routing Instance	Source Packets	Destination Packets
172.16.15.9	T1-Vxlan	19626	27643

7. To view tunnel details about a microsegement, select Tunnel Statistics in the first filter field and All, which is the only option in the second filter field.

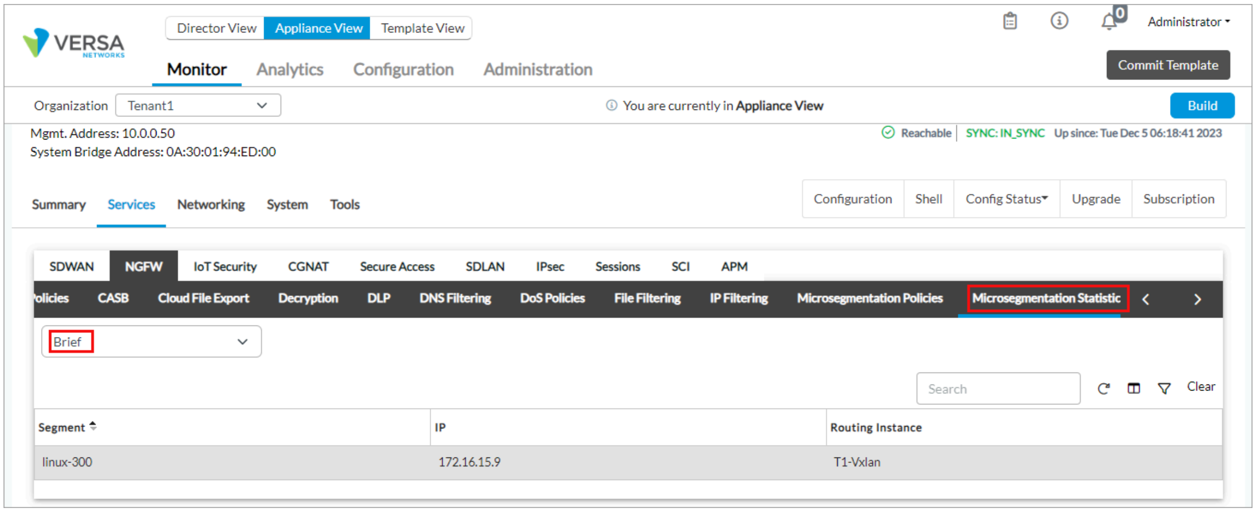


Tunnel-Statistics

All

Segment	Packets
linux-300	0
linux-400	0
default-sgt	0
linux-401	0

8. To view brief microsegment statistics, select Brief.



Organization Tenant1

You are currently in Appliance View

Mgmt. Address: 10.0.0.50
System Bridge Address: 0A:30:01:94:ED:00

Reachable SYNC: IN_SYNC Up since: Tue Dec 5 06:18:41 2023

Brief

Segment	IP	Routing Instance
linux-300	172.16.15.9	T1-Vxlan

Supported Software Information

Releases 22.1.3 and later support all content described in this article.

Additional Information

Configure IoT Security
Configure NGFW
Configure NPU Policy-Based Forwarding
Configure User and Group Policy
Manage Files and Folders
Use the Versa SASE Client Application