Configure NPU Policy-Based Forwarding

For supported software information, click here.

Normally, packets are forwarded based on entries in the Layer 2 forwarding table or Layer 3 routing table. For Versa Networks devices that use network processing (NPU) switching hardware, including CSG3000, CSX4000, and CSG5000 series devices, you can configure NPU access control list (ACL) policies that affect how Layer 2 and Layer 3 packets are forwarded.

An ACL policy consists of the following components:

- ACL policy name, which identifies the ACL.
- ACL policy rules, which define the conditions for matching packets and the actions to take when packets match.

An ACL policy can have one or more rules, and the rules are evaluated in order in which they are listed in the ACL policy until a match occurs. When a rule matches, the action associated with that rule is applied to the traffic, and no further rules in the ACL policy are evaluated.

You device ACL policies for an organization (also called a tenant). Each tenant can have a maximum of one ACL policy.

You can configure the following types of NPU ACL policies:

- Layer 2 IPv4 and IPv6
- Layer 3 IPv4 (single wide)
- Layer 3 IPv4 (double wide)
- Layer 3 IPv6

Single-wide and double-wide Layer 3 IPv4 NPU ACLs are identical, except for the rule match conditions. More memory is allocated for double-wide ACL policies, which allows you to match not just destination and source ports, but also destination and source port ranges.

By default, Layer 2 and Layer 3 NPU ACLs can match any switching or routing packets. The primary difference between Layer 2 and Layer 3 ACLs is the match attributes: Layer 2 ACLs can match all Layer 3 ACL fields plus additional Layer 2 fields.

Layer 2 and Layer 3 NPU ACLs are mutually exclusive. Layer 2 ACLs apply only to switching packets, and Layer 3 ACLs apply only to routing packets.

With NPU policy, you can also configure traffic mirroring, which allows a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.

Layer 2 NPU Ingress ACL Overview

Layer 2 NPU ingress ACLs allow you to create policy filters that match fields in the Layer 2 headers of packets arriving at a LAN Ethernet (enet) interface, and then set an action to take on matching packets.

With Layer 2 NPU ingress ACLs, you can match packets based on the following fields in the packet headers:

- Destination IPv4 address
- Destination IPv6 address
- Destination MAC address
- Destination port range
- DSCP
- Ether type
- ICMPv4
- ICMPv6
- IP protocol
- Layer 4 destination port
- Layer 4 source port
- Source MAC address
- Source IPv4 address
- Source IPv6 address
- Source port range
- Tunnel type

For Layer 2 NPU ingress ACLs, you can set the following actions to occur when a packet matches:

- Permit, or allow, the packet.
- Deny, or block, the packet.
- Count the packet.
- Send the packet to the CPU for further processing.
- Apply traffic policers, which send the packet for processing by the service engine that you define in a QoS profile.

Layer 3 NPU Ingress ACL Overview

Layer 3 NPU ingress ACLs for IPv4 and IPv6 allow you to create policy filters that match fields in the headers of packets arriving at a LAN Ethernet (enet) interface, and then set an action to take based on matching packets.

The fields that the you can match in the ACLs depend on the switch hardware's ternary content addressable memory (TCAM), which is the space in hardware where access lists (ACLs) are stored. The TCAM memory is allocated by slicing it into units, and the ACL fields you can match depend on the number of slices allocated for the feature, which is called the feature width.

Layer 3 NPU ACL policy affects only IPv4 and IPv6 routed packets. For tunneled packets, if the match specifies the tunnel type as VXLAN, the packets are processed by service chaining. For non-tunneled packets, all packets are processed by service chaining without the need to set the tunnel type match of VXLAN.

With Layer 3 NPU IPv4 ingress ACLs, you can match packets based on the following fields in the IPv4 packet headers:

- Destination IPv4 address
- DSCP value
- IP protocol tunnel type
- ICMP message type
- Layer 3 IRB
- Layer 4 destination port
- Layer 4 destination port range (for double-wide ACLs only).
- Layer 4 source port
- Layer 4 source port range (for double-wide ACLs only).
- Source IPv4 address
- VRF

With Layer 3 NPU IPv6 ingress ACLs, you can match packets based on the following fields in the IPv6 packet headers:

- Destination IPv6 address
- DSCP value
- IP protocol tunnel type
- ICMP message type
- Layer 3 IRB
- Layer 4 destination port
- Layer 4 source port
- Source IPv6 address
- VRF

For Layer 3 NPU ACLs for IPv4 and IPv6, you can set the following actions to occur when a packet matches:

- Permit, or allow, the packet.
- Deny, or block, the packet.
- Count the packet.
- Send the packet to the CPU for further processing.
- Apply traffic policers, which send the packet for processing by the service engine that you define in a QoS profile.

Policer Overview

Policing is a method for limiting the traffic that is allowed to pass through an interfaces. You specified the allowed rates of traffic, and traffic that exceeds these rate thresholds is dropped.

When you configure policing on interfaces at the edge of a network, you can control the maximum rate of traffic that is transmitted or received on the interfaces. When the traffic flow is less than the maximum rate, it is transmitted whereas traffic. When the traffic flow reaches and then exceeds the maximum rate, it is dropped.

To police traffic for NPU ACL policies, you configure QoS profiles and then you associate a profile with an ACL rule when you configure the action to take when a packet matches the rule. In the QoS profile, you specify the type of policer and the traffic rates.

Before discussing the types of policers, it is necessary to define policer terminology.

Policers track both normal and bursty flows of traffic. Policers use the following terms to describe normal traffic flows on an interface:

- CIR—Committed information rate, in bits per second (bps). CIR is the average rate of traffic that can pass through an interface.
- PIR—Peak information rate, in bps. PIR is the maximum rate of traffic that can pass through an interface. The PIR value must be equal to or greater than the CIR value.

Policers use the following terms to describe bursty traffic flows on an interface:

- CBS—Committed burst size, in bytes per second (Bps). CBS is the average volume of burst traffic that can pass through an interface.
- PBS—Peak burst size, in bytes per second. PBS is the maximum volume of burst traffic that can pass through an interface. The PBS value must be equal to or greater than the CBS value.

Policers can mark traffic to reflect the traffic rate. The traffic is marked by applying a color, either green, yellow, or red.

In NPU ACL rules, you can configure three types of policers, which are described in the following table.

		Mark Packets as		
Policer Type	**Values Evaluated**	**Green**	**Yellow**	**Red**
Single rate, two color	CIR, CBS	When rate falls below CIR and CBS thresholds *Default action:* Allow packets to pass	NA	Rate exceeds CIR and CBS thresholds *Default action:* Drop packets

		Mark Packets as		
Policer Type	**Values Evaluated**	**Green**	**Yellow**	**Red**
Single rate, three color	CIR, CBS, PBS	When rate falls below CIR, CBS, and PBS thresholds *Default action:* Allow packets to pass	When rate falls between CBS and PBS thresholds *Default action:* Allow packets to pass	Rate exceeds CIR, CBS, or PBS threshold *Default action:* Drop packets
Two rate, three color	CIR, CBS, PIR, PBS	When rate falls below CIR, CBS, PIR, and PBS thresholds *Default action:* Allow packets to pass	When rate falls between CIR/CBS and PIR/PBS thresholds *Default action:* Allow packets to pass	Rate exceeds CIR/ CBS and PIR/PBS thresholds *Default action:* Drop packets

As a policer is examining traffic arriving on an interface, it can note whether the packets are already marked with a color. You can configure the policer to take its action based on whether the color marking is present:

- Color blind—When an IP packet arrives at the interface, the traffic is policed without examining the DSCP values for packet loss priority (PLP) bits that may have been set by an upstream network node.
- Color aware—When an IP packet arrives at the interface, the policer examines the PLP markings that may have been set by an upstream network node and then places the packet in the correct token bucket. There are two buckets, committed and peak rate. Currently, the VOS software does not support color-aware policing.

ACL Policy Actions

Packets can match Layer 2, Layer 3 single-wide, and Layer 3 double-wide ACL policies. When a packet matches all three ACLs, the action for the Layer 2 ACL has the highest priority and the action for the Layer 3 double-wide ACL has the lowest priority. The result is that the Layer 2 ACL action is the action taken, with the following exceptions:

- The Layer 2 ACL action is Permit and one or both of the other two actions is Service. In these cases, the action taken is Service.
- The Layer 2 ACL action is Policer Drop and one or both of the other two actions is Service. In these cases, the action taken is both Policer Drop and Service.

The following table defines that action that is taken if a packet matches Layer 2, Layer 3 single-wide, and Layer 3 double-wide ACLs.

Layer 2 ACL Match Action	Layer 3 Single-Wide ACL Match Action	Layer 3 Double-Wide ACL Match Action	Action Taken
Permit	Permit	Permit	Permit
Drop	Permit	Permit	Drop
Permit	Permit	Drop	Permit
Drop	Permit	Drop	Drop
Permit	Drop	Permit	Permit
Drop	Drop	Permit	Drop
Permit	Drop	Drop	Permit
Drop	Drop	Drop	Drop
Service	Permit	Permit	Service
Service	Permit	Drop	Service
Service	Drop	Permit	Service
Service	Drop	Drop	Service
Permit	Permit	Service	Service
Drop	Permit	Service	Drop
Permit	Drop	Service	Service
Drop	Drop	Service	Drop
Permit	Service	Permit	Service
Drop	Service	Permit	Drop
Permit	Service	Drop	Service
Drop	Service	Drop	Drop
Service	Permit	Service	Service
Service	Drop	Service	Service
Service	Service	Permit	Service
Service	Service	Drop	Service

Permit	Service	Service	Service
Drop	Service	Service	Drop
Service	Service	Service	Service
Policer Drop	Permit	Permit	Policer Drop
Policer Drop	Permit	Drop	Policer Drop
Policer Drop	Drop	Permit	Policer Drop
Policer Drop	Drop	Drop	Policer Drop
Permit	Permit	Policer Drop	Permit
Drop	Permit	Policer Drop	Drop
Permit	Drop	Policer Drop	Permit
Drop	Drop	Policer Drop	Drop
Permit	Policer Drop	Permit	Permit
Drop	Policer Drop	Permit	Drop
Permit	Policer Drop	Drop	Permit
Drop	Policer Drop	Drop	Drop
Policer Drop	Permit	Policer Drop	Policer Drop
Policer Drop	Drop	Policer Drop	Policer Drop
Policer Drop	Policer Drop	Permit	Policer Drop
Policer Drop	Policer Drop	Drop	Policer Drop
Permit	Policer Drop	Policer Drop	Permit
Drop	Policer Drop	Policer Drop	Drop
Policer Drop	Policer Drop	Policer Drop	Policer Drop
Policer Drop	Permit	Service	Policer Drop + Service
Policer Drop	Service	Permit	Policer Drop + Service
Policer Drop	Service	Service	Policer Drop + Service
Permit	Service	Policer Drop	Service

Service	Service	Policer Drop	Service
Service	Permit	Policer Drop	Service
Permit	Policer Drop	Service	Service
Service	Policer Drop	Permit	Service
Service	Policer Drop	Service	Service
Policer Drop	Service	Policer Drop	Policer Drop + Service
Policer Drop	Drop	Policer Drop	Policer Drop
Policer Drop	Policer Drop	Service	Policer Drop + Service
Policer Drop	Policer Drop	Drop	Policer Drop
Service	Policer Drop	Policer Drop	Service
Drop	Policer Drop	Policer Drop	Drop
Policer Drop	Policer Drop	Policer Drop	Policer Drop
Permit	Service	Policer Drop + Service	Service
Service	Service	Policer Drop + Service	Service
Service	Permit	Policer Drop + Service	Service
Permit	Policer Drop + Service	Service	Service
Service	Policer Drop + Service	Permit	Service
Service	Policer Drop + Service	Service	Service
Policer Drop + Service	Service	Policer Drop + Service	Policer Drop + Service
Policer Drop + Service	Drop	Policer Drop + Service	Policer Drop + Service
Policer Drop + Service	Policer Drop + Service	Service	Policer Drop + Service
Policer Drop + Service	Policer Drop + Service	Drop	Policer Drop + Service
Service	Policer Drop + Service	Policer Drop + Service	Service
Drop	Policer Drop + Service	Policer Drop + Service	Drop
Policer Drop + Service	Policer Drop + Service	Policer Drop + Service	Policer Drop + Service

Configure Layer 2 Ingress ACLs

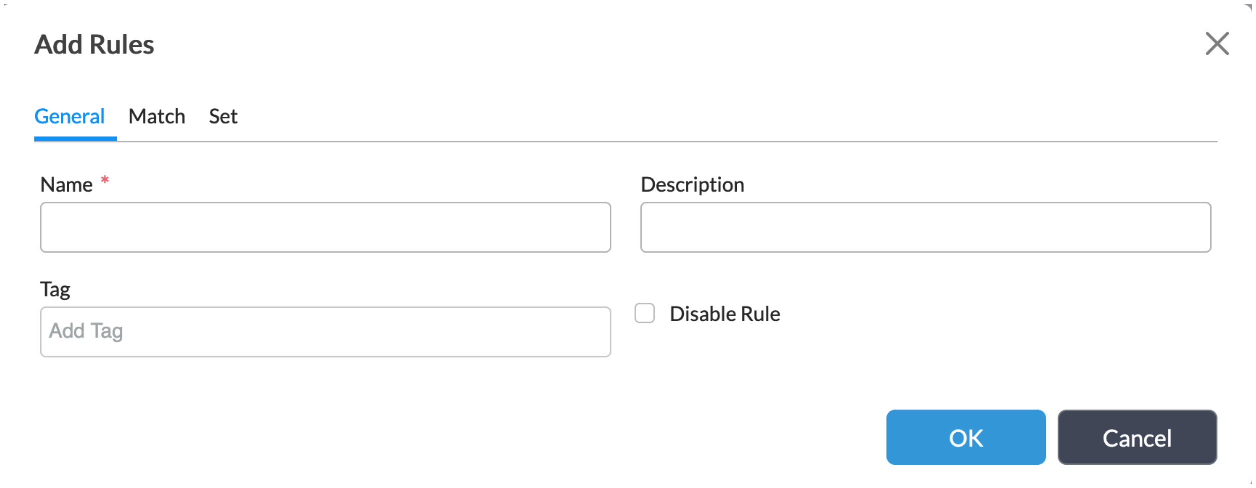
For each tenant or branch, you can configure one Layer 2 ACL policy. The ACL policy is applied on ingress, when packets are arriving at a LAN Ethernet (enet) interface.

To configure a Layer 2 IPv4 NPU 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.
4. Select the Policies tab, and then click the + Add icon or the + Add button. In the Add Policies popup window, enter information for the following fields.

Field	**Description**
Name (Required)	Enter a name for the NPU ACL policy. The name can be up to 255 characters. If a name is already present in the field, such as Default-Policy, delete the type and enter a new one.
Description	Enter a text description for the NPU ACL policy.

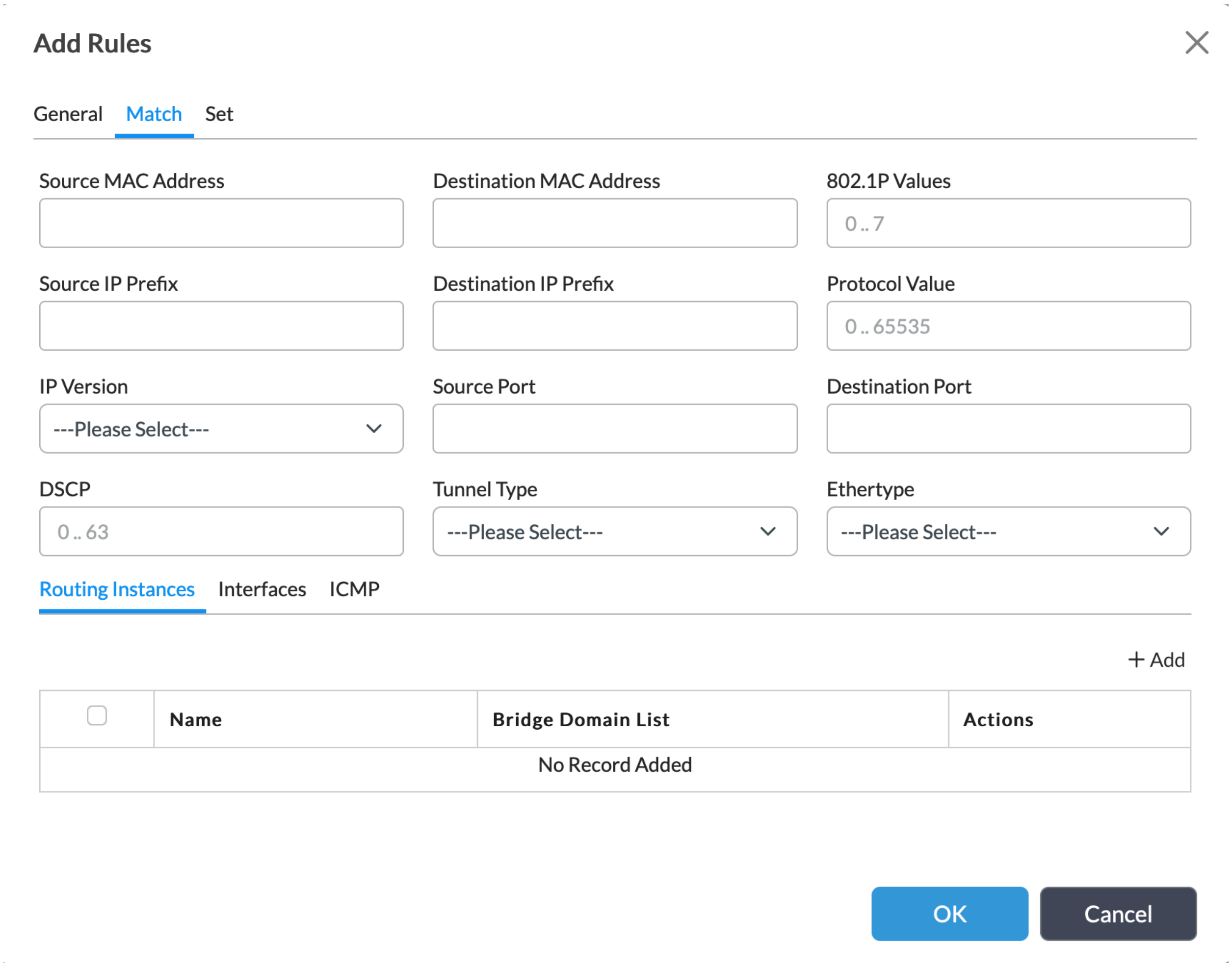
5. Click OK.
6. Select the Rules tab, and then click the + Add icon or the + Add button. The Add Rules popup window displays.



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

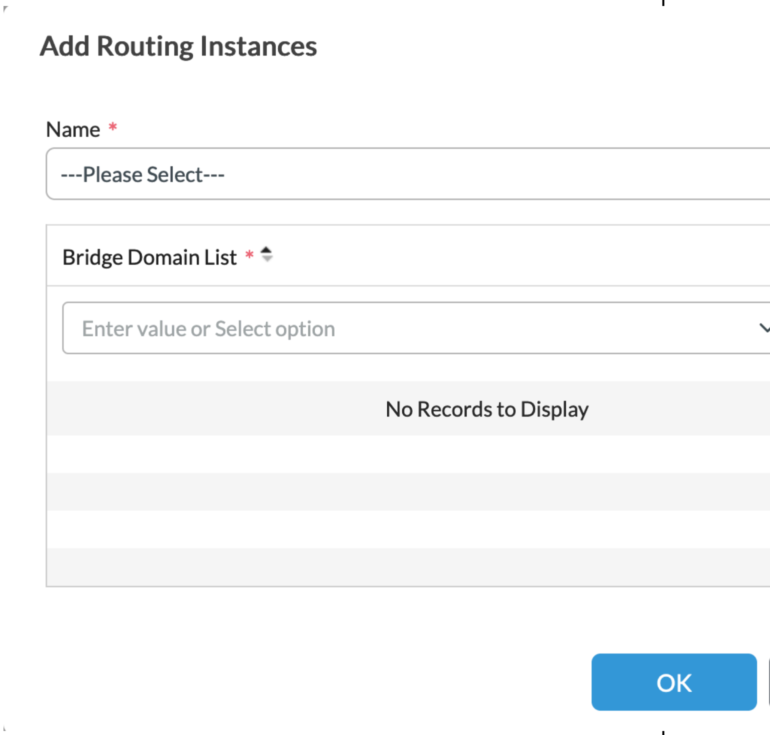
Field	Description
Name (Required)	Enter a name for the NPU ACL policy rule. The name can be up to 255 characters.
Description	Enter a text description for the NPU ACL policy rule.
Tag	Enter one or more text strings that describe the policy rule. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to search objects. You can specify multiple tags.
Disable	Click to not activate the ACL policy rule when you commit the configuration.

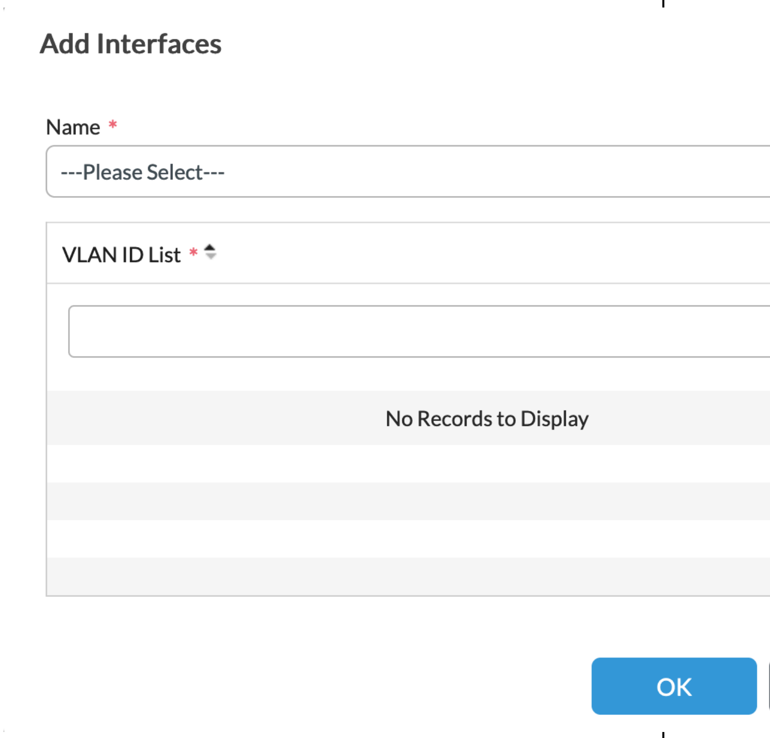
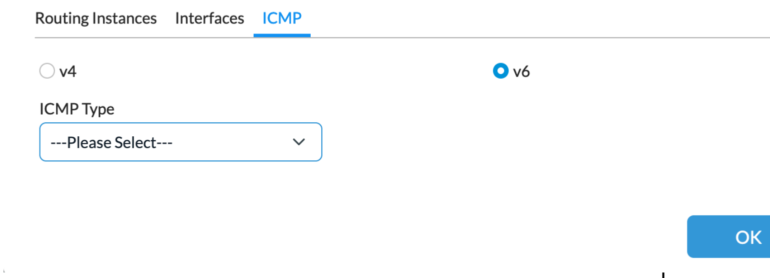
8. Select the Match tab to configure the conditions for a packet to match the ACL policy rule. Then enter information for the following fields.



□	Name	Bridge Domain List	Actions
No Record Added			

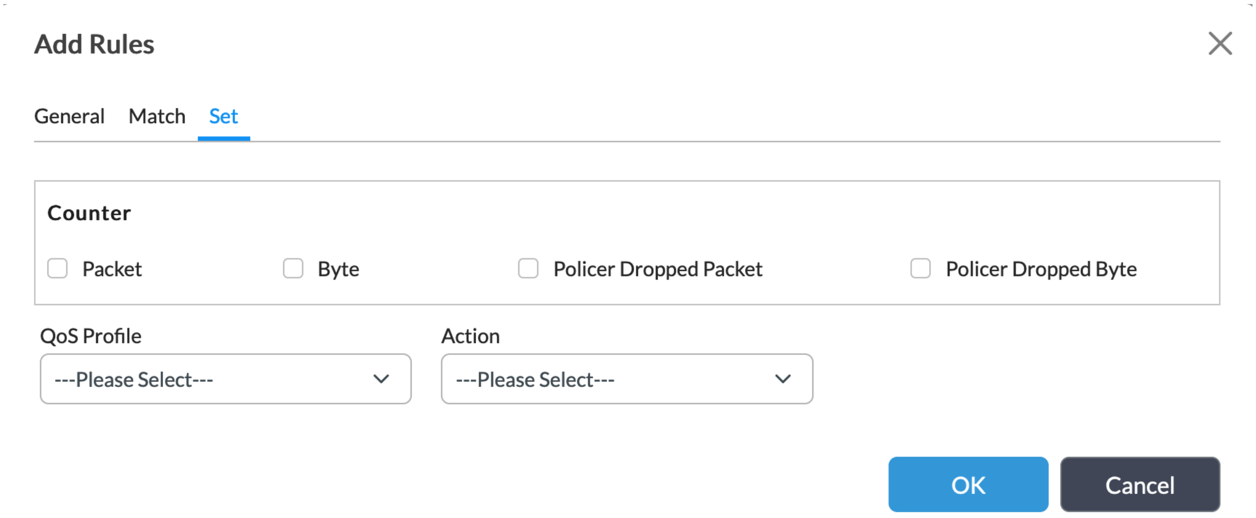
Field	Description
Source MAC Address	Enter the source MAC address to match.
Destination MAC Address	Enter the destination MAC address to match.
802.1P Value	Enter the 802.1P value to match. *Range:* 0 through 7 *Default:* None
Source IP Prefix	Enter the source IP prefix to match.
Destination IP Prefix	Enter the destination IP prefix to match.
Protocol Value	Enter the number of the protocol to match.
IP Version	Select the IP version to match ◦ IPv4 ◦ IPv6
Source Port	Enter the source port number to match.
Destination Port	Enter the destination port number to match.
DSCP	Enter the differentiated services code point (DSCP) value to match
Tunnel Type	Select the tunnel type: ◦ VXLAN
Ether Type	Select the Ether type to match by: ◦ Ethertype Name—Select to match by name, and then in the Ether Type field, select one of the following: ▪ ARP ▪ IPv4 ▪ IPv6 ◦ Ethertype Value—Select to match by value, and then in the Ether Type Value field, enter a

	numeric value.
Routing Instance (Tab)	Select the routing instance from which the packet is received. Click the + Add icon, and in the Add Routing Instances popup window, enter information for the following fields, and then click OK.  Add Routing Instances Name * ---Please Select--- Bridge Domain List * Enter value or Select option No Records to Display OK
◦ Name	Select the routing instance from which the packet is received.
◦ Bridge Domain List	Click the + Add icon and add a bridge domain from which the packet is received.
Interfaces (Group of Fields)	Select the Layer 3 interface or IRB from which the packet is received. Click the + Add icon, and in the Add Interfaces popup window, enter information for the following fields, and then click OK.

	 Add Interfaces Name * ---Please Select--- VLAN ID List * No Records to Display OK
◦ Name	Select the name of the interface on which the packet is received.
◦ VLAN ID List	Click the + Add icon and add the VLAN from which the packet is received.
ICMP (Group of Fields)	Select the ICMP packet type to match.  Routing Instances Interfaces ICMP ○ v4 ● v6 ICMP Type ---Please Select--- OK
◦ v4	Click to match ICMPv4 messages.
◦ v6	Click to match IPCMv6 messages.

◦ ICMP Type	Select the type of ICMP message to match: ◦ Destination Unreachable ◦ Echo Reply ◦ Echo Request ◦ Information Query ◦ Information Response ◦ Multicast Listener Done ◦ Multicast Listener Query ◦ Multicast Listener Request ◦ Neighbor Advertisement ◦ Neighbor Solicitation ◦ Packet Too Large ◦ Parameter Problem ◦ Redirect ◦ Router Advertisement ◦ Router Renumbering ◦ Router Solicitation ◦ Time Exceeded

9. Select the Set tab to configure the action or actions to take when a packet matches the ACL policy rule. Then enter information for the following fields.



Add Rules

Counter

□ Packet □ Byte □ Policer Dropped Packet □ Policer Dropped Byte

QoS Profile: ---Please Select---

Action: ---Please Select---

Field	Description
Counter (Group of Fields)	Configure packet and byte counters.
◦ Packet	Click to count packets that match the NPU ACL policy rule.
◦ Byte	Click to count bytes that match the NPU ACL policy rule.
◦ Policer Dropped Packet	Click to count packets dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
◦ Policer Dropped Byte	Click to count bytes dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
QoS Profile	Select the QoS policy to apply to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.
Action	Select the action to apply to packets that match the ACL policy rule: ◦ Allow—Permit, or accept, the packet. ◦ Deny—Bloc, the packet. ◦ Service PIC—Service physical interface card (PIC). The service PIC enables Layer 2 and Layer 3 services on traffic that flows through the device, known as service chaining. This service chaining directs traffic internally from the NPU into the x86 processor. Select Service PIC to apply services such as antivirus filtering, firewalls, and traffic engineering to packets that match the policy rules. Then in the Service Actions field, select the action.
Service Actions	If you select the Service PIC action, select the action: ◦ Host—Send the packet to the VOS device's CPU to perform additional Layer 4 through Layer 7 processing.

10. Select the QoS Profiles tab to configure traffic rate policers to apply to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.

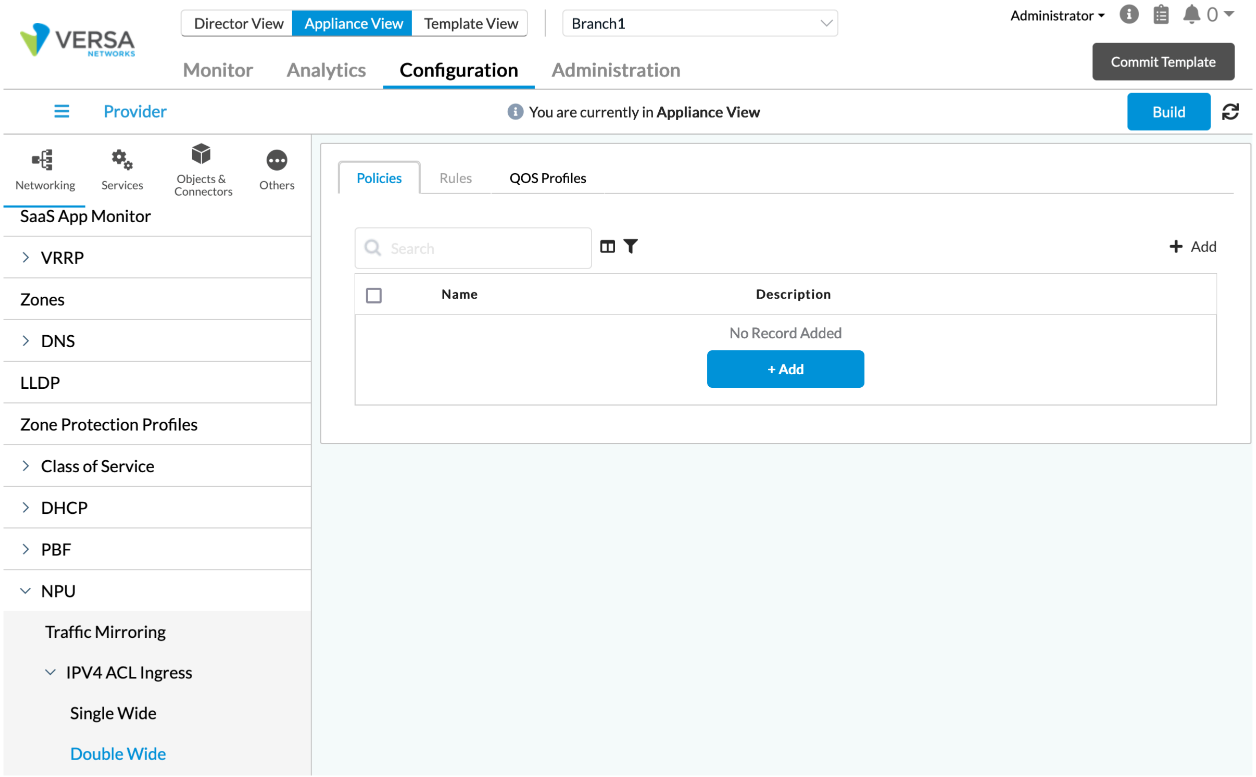
11. Click OK.

Configure Layer 3 IPv4 Ingress ACLs

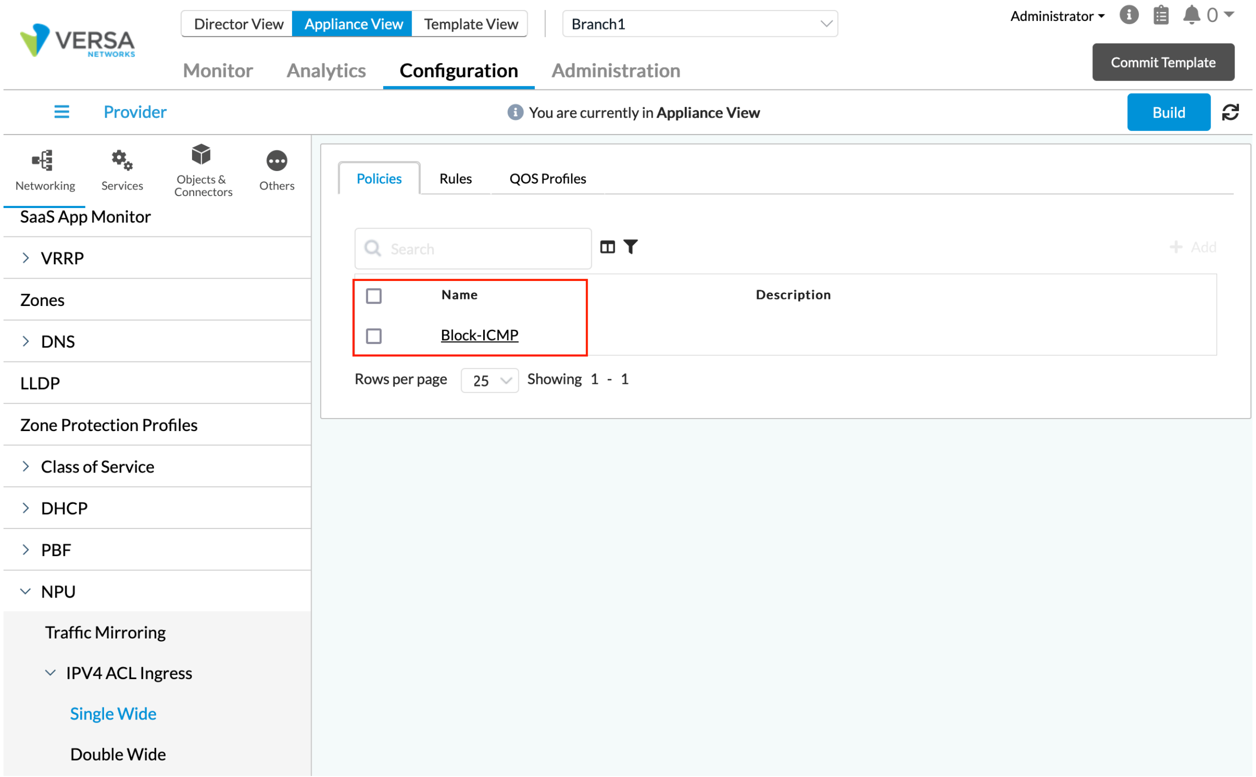
For each tenant or branch, you can configure one single-wide NPU ACL policy and one double-wide NPU ACL policy.

To configure a Layer 3 IPv4 ingress NPU ACL:

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 the name of an organization in the Organization field in the horizontal menu bar.
   d. Click the name of a VOS device. The view changes to Appliance view.
2. Select the Configuration tab is selected in the top menu bar.
3. Select Networking > NPU > IPv4 ACL Ingress in the left menu bar.
4. Select the type of Layer 3 IPv4 NPU ACL to configure:
   - Single Wide—Use single-wide ACL matching options.
   - Double Wide—Use double-wide ACL matching options.
5. If no policy has been configured, the following screen displays:



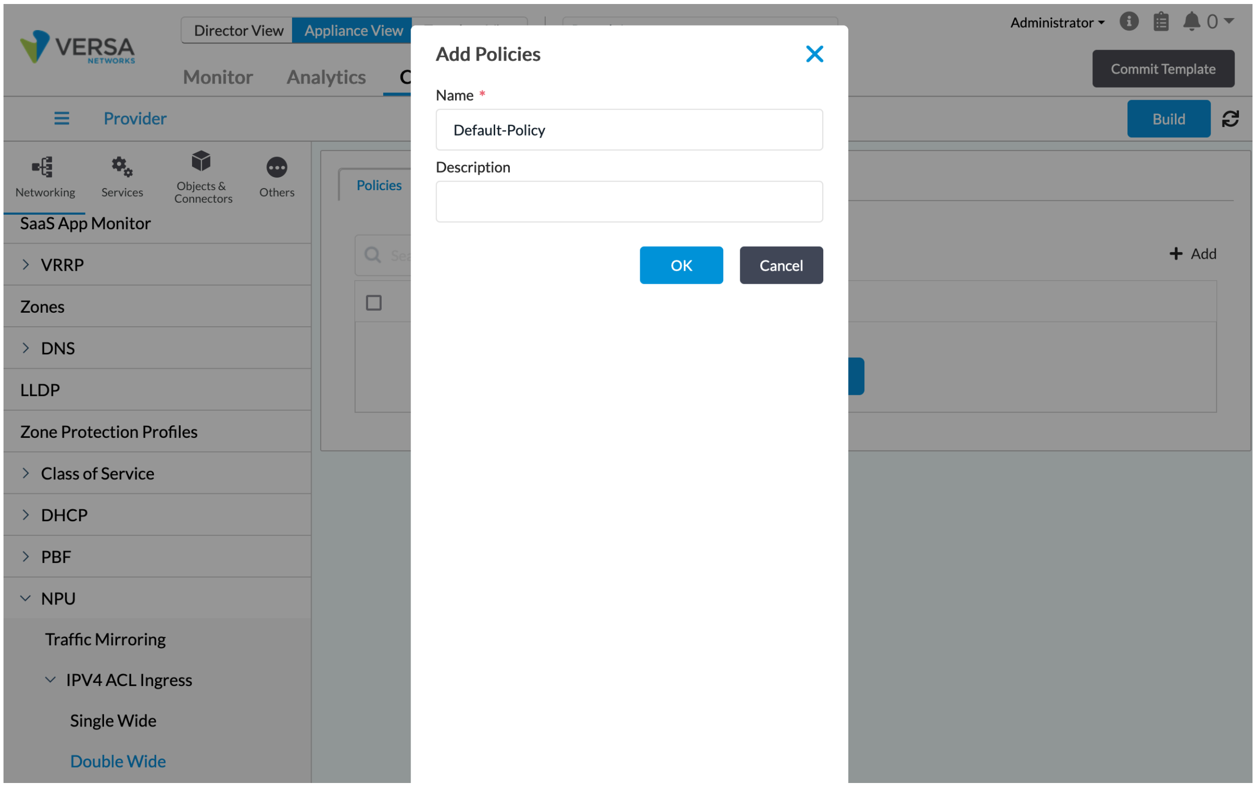
If a policy has already been configured, a screen similar to the following displays:



□	Name	Description
□	Block-ICMP	

Rows per page 25 Showing 1 - 1

6. Select the Policies tab, and then click the + Add icon or the + Add button. In the Add Policies popup window, enter information for the following fields.



Add Policies

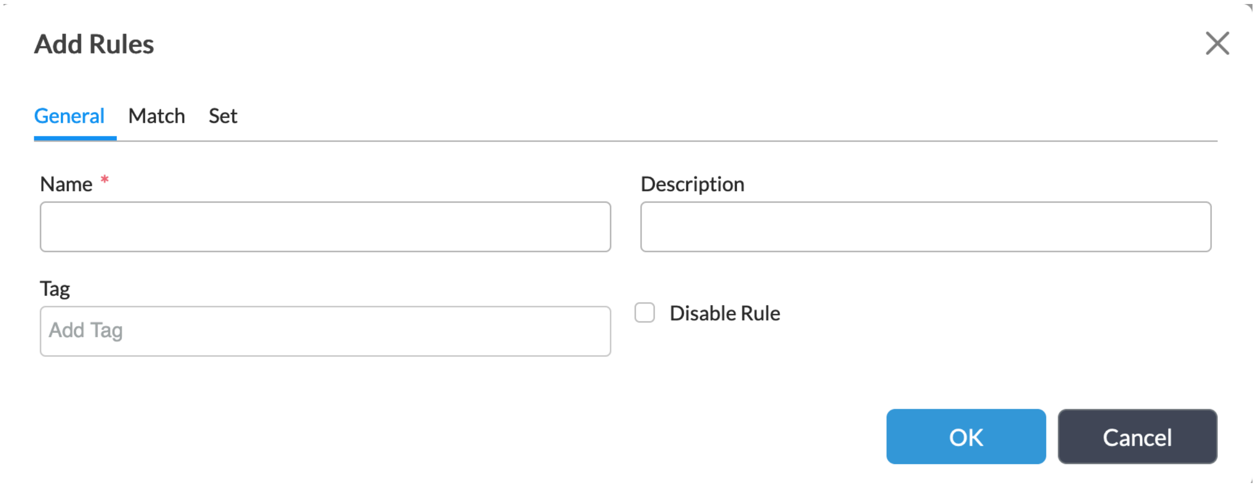
Name *

Default-Policy

Description

Field	Description
Name (Required)	Enter a name for the NPU ACL policy. The name can be up to 255 characters. If a name is already present in the field, such as Default-Policy, delete the type and enter a new one.
Description	Enter a text description for the NPU ACL policy.

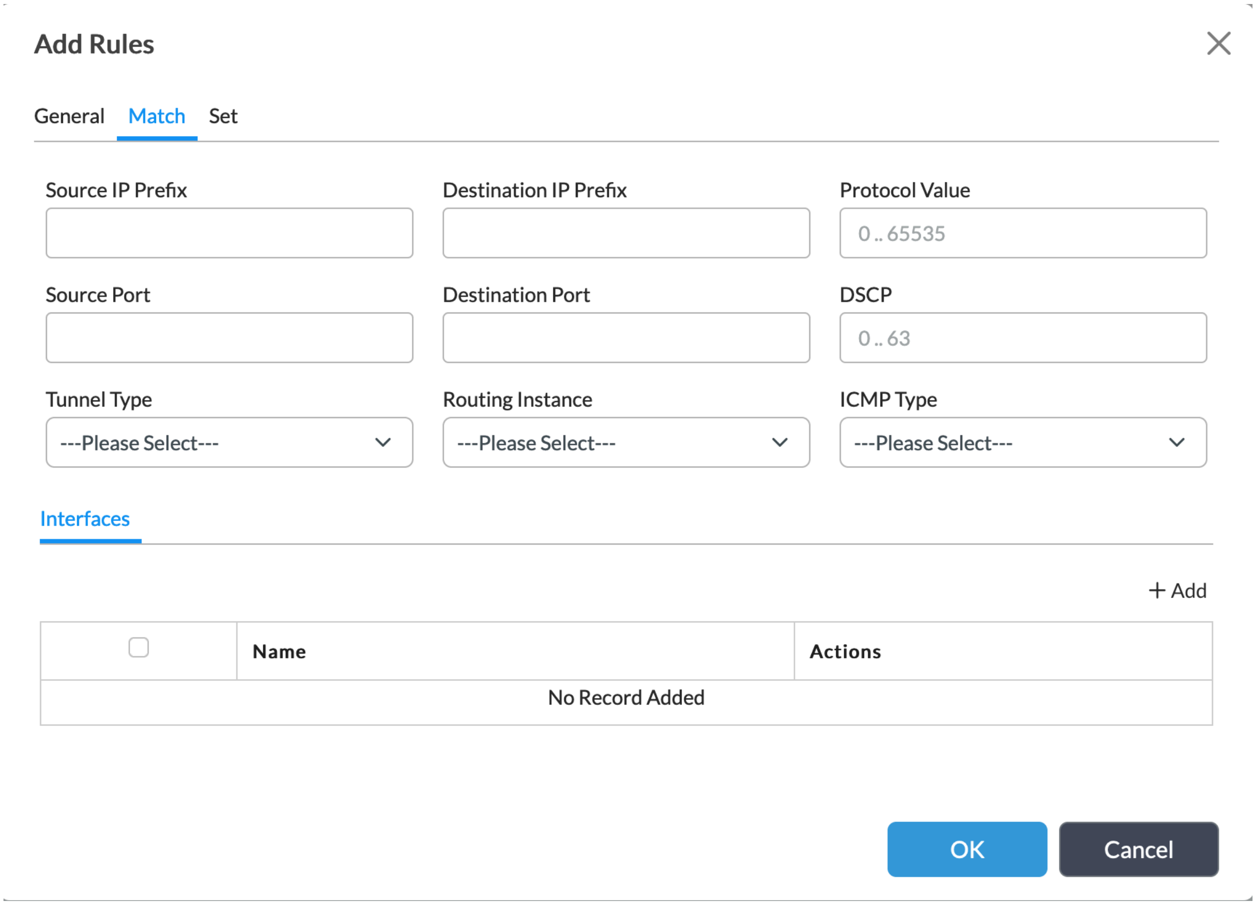
7. Click OK.
8. Select the Rules tab, and then click the + Add icon or the + Add button. The Add Rules popup window displays.



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

Field	Description
Name (Required)	Enter a name for the NPU ACL policy rule. The name can be up to 255 characters.
Description	Enter a text description for the NPU ACL policy rule.
Tag	Enter one or more text strings that describe the policy rule. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to search objects. You can specify multiple tags.
Disable	Click to not activate the ACL policy rule when you commit the configuration.

10. Select the Match tab to configure the conditions for a packet to match the ACL policy rule. Then enter information for the following fields.



Add Rules

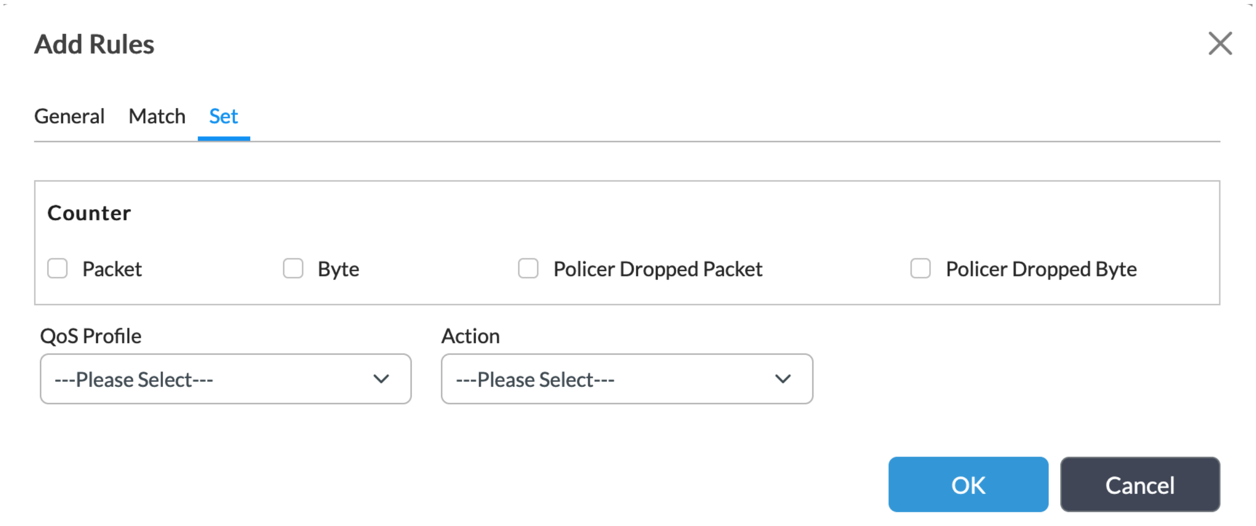
Source IP Prefix	Destination IP Prefix	Protocol Value
		0 .. 65535
Source Port	Destination Port	DSCP
		0 .. 63
Tunnel Type	Routing Instance	ICMP Type
---Please Select---	---Please Select---	---Please Select---

□	Name	Actions
	No Record Added	

Field	Description
Source IP Prefix	Enter the source IP address and prefix.
Destination IP Prefix	Enter the destination IP address and prefix.
Protocol Value	Enter a TCP or UDP protocol number.
Source Port	Enter the source port number.
Source Port Range	For double-wide ACL policy rules only, enter the source port or port range for the WAN interface; for example, 2100 or 200-300. The maximum range is 32 ports.
Destination Port	Enter the destination port number.
Destination Port Range	For double-wide ACL policy rules only, enter the destination port or port range for the WAN interface; for example, 2100 or 200-300. The maximum range is 32 ports.
DSCP	Enter a differentiated services code point (DSCP) value.
Tunnel Type	Select the tunnel type: ◦ VXLAN
Routing Instance	Select the routing instance on which the packet is received.
ICMP Type	Select the type of ICMP message to match: ◦ Destination Unreachable ◦ Echo Reply ◦ Echo Request ◦ Information Query ◦ Information Response ◦ Multicast Listener Done ◦ Multicast Listener Query ◦ Multicast Listener Request ◦ Neighbor Advertisement ◦ Neighbor Solicitation ◦ Packet Too Large

	◦ Parameter Problem ◦ Redirect ◦ Router Advertisement ◦ Router Renumbering ◦ Router Solicitation ◦ Time Exceeded
Interfaces (Group of Fields)	Click the + Add icon, and in the Add Interfaces popup window, in the Name field, select the Layer 3 interface or IRB on which the packet is received. Then click OK.

11. Select the Set tab to configure the action or actions to take when a packet matches the ACL policy rule. Then enter information for the following fields.



Field	**Description**
Counter (Group of Fields)	Configure packet and byte counters.
◦ Packet	Click to count packets that match the ACL policy rule.
◦ Byte	Click to count bytes that match the ACL policy rule.
◦ Policer Dropped Packet	Click to count packets dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
◦ Policer Dropped Byte	Click to count bytes dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
QoS Profile	Select the QoS policy to apply traffic policers to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.
Action	Select the action to apply to packets that match the ACL policy rule: ◦ Allow—Permit, or accept, the packet. ◦ Deny—Bloc, the packet. ◦ Service PIC—The service PIC enables Layer 2 and Layer 3 services on traffic that flows through the device, known as service chaining. This service chaining directs traffic internally from the NPU into the x86 processor. Select Service PIC to apply services such as antivirus filtering, firewalls, and traffic engineering to packets that match the policy rules. Then in the Service Actions field, select the action.
Service Actions	If you select the Service PIC Action, select the action: ◦ Host—Send the packet to the VOS device's CPU to perform additional Layer 4 through Layer 7 processing.

12. Select the QoS Profiles tab to configure traffic rate policers to apply to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.

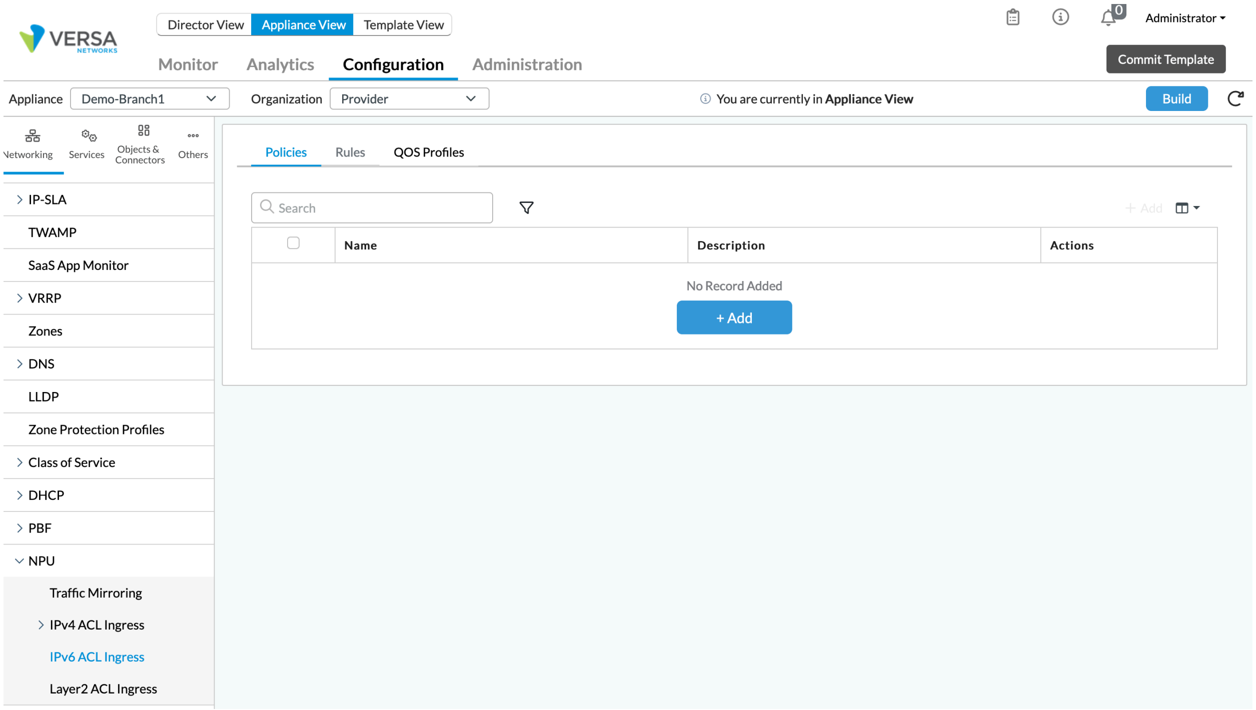
13. Click OK.

Configure Layer 3 IPv6 Ingress ACLs

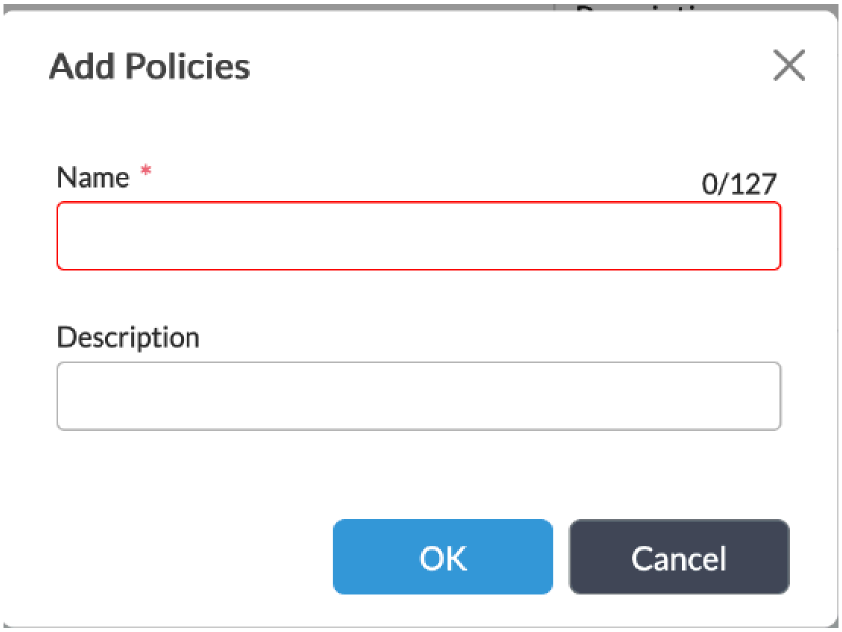
For each tenant or branch, you can configure one Layer 3 IPv6 ingress ACL policy.

To configure a Layer 3 IPv6 ingress NPU ACL:

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 the name of an organization in the Organization field in the horizontal menu bar.
    d. Click the name of a VOS device. The view changes to Appliance view.
2. Select the Configuration tab is selected in the top menu bar.
3. Select Networking > NPU > IPv6 ACL Ingress in the left menu bar.
4. If no policy has been configured, the following screen displays:

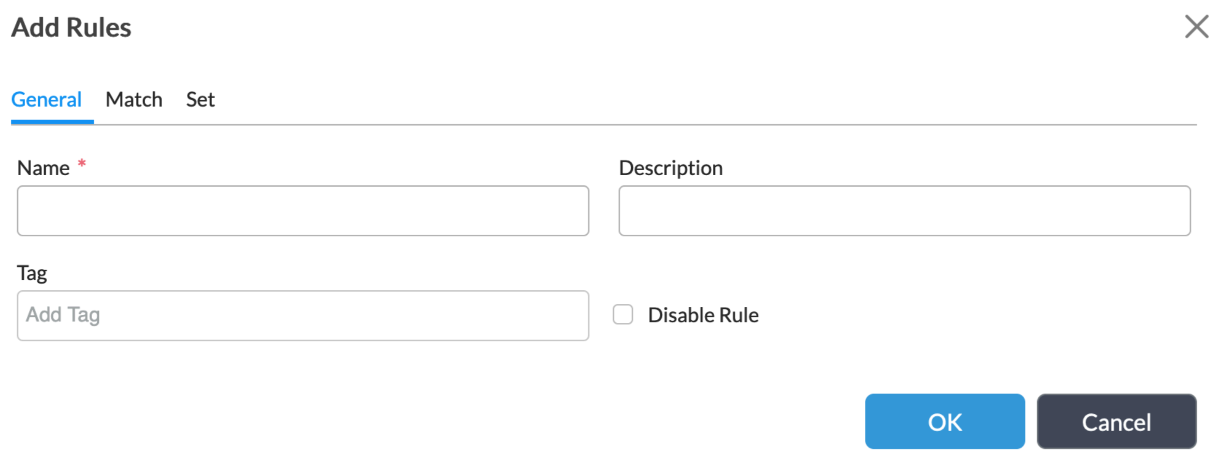


5. Select the Policies tab, and then click the + Add icon or the + Add button. In the Add Policies popup window, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the IPv6 ACL ingress policy. The name can be up to 255 characters. If a name is already present in the field, such as Default-Policy, delete the type and enter a new one.
Description	Enter a text description for the policy.

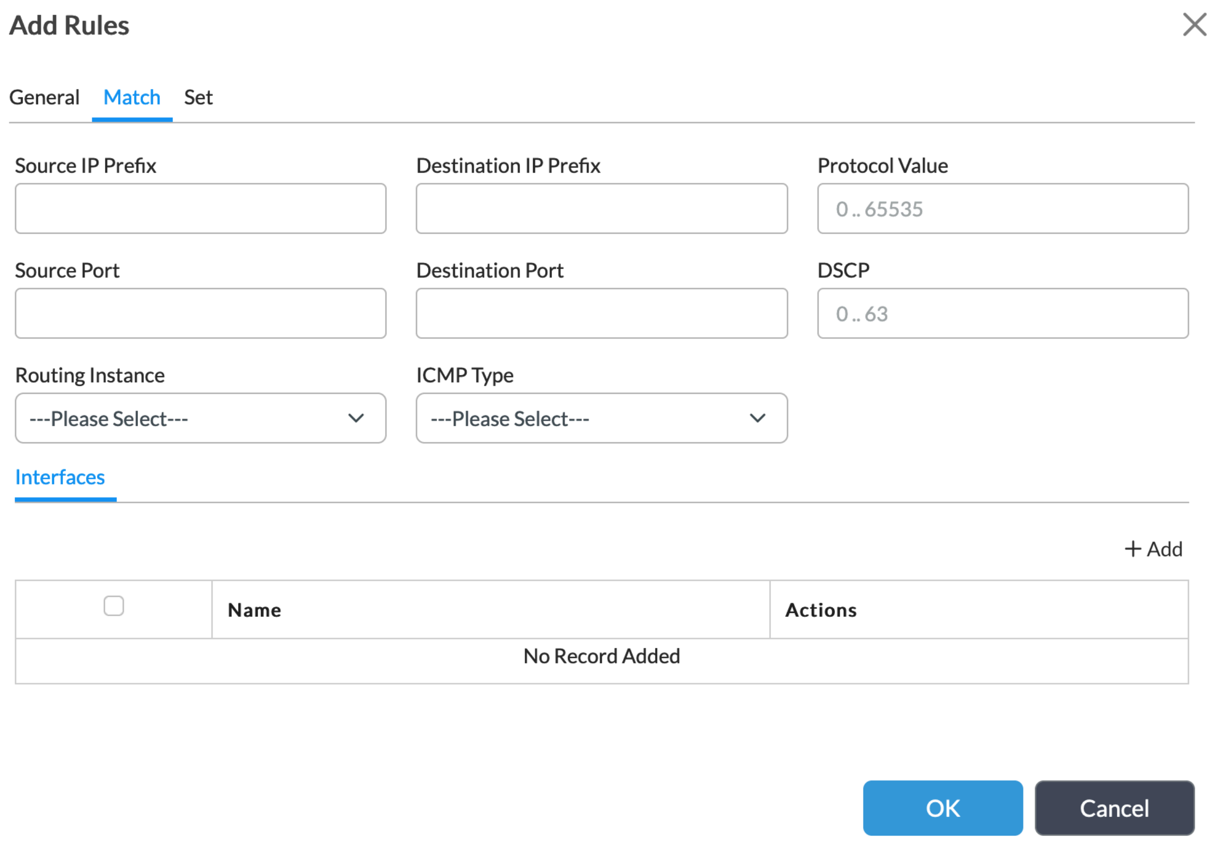
6. Click OK.
7. Select the Rules tab, and then click the + Add icon or the + Add button. The Add Rules popup window displays.



8. Select the General tab, and then enter information for the following fields.

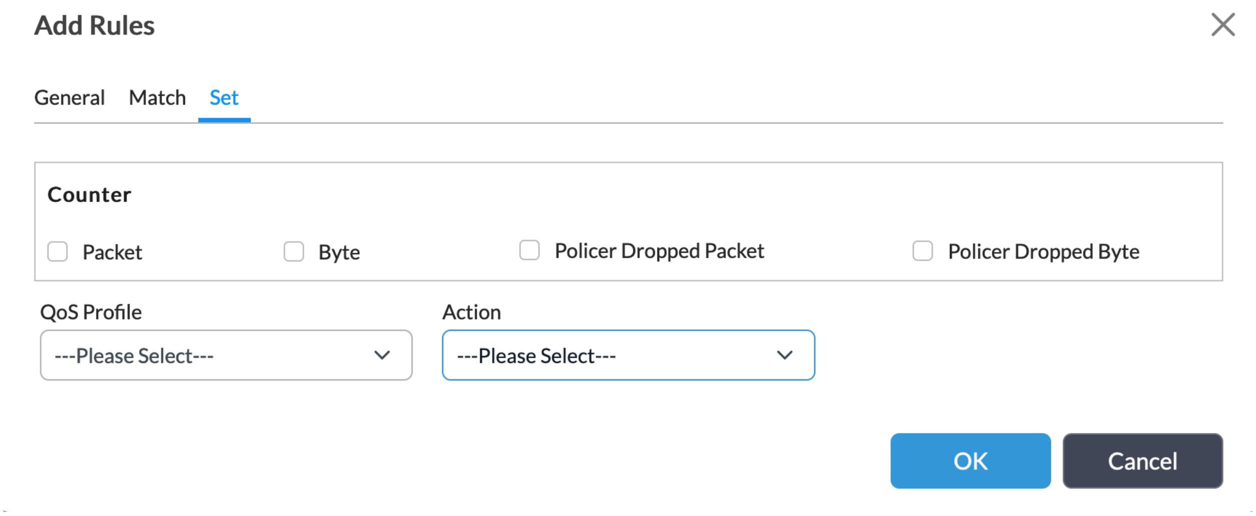
Field	Description
Name (Required)	Enter a name for the IPv6 ACL ingress policy rule. The name can be up to 255 characters.
Description	Enter a text description for the policy rule.
Tag	Enter one or more text strings that describe the policy rule. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to search objects. You can specify multiple tags.
Disable	Click to not activate the ACL policy rule when you commit the configuration.

9. Select the Match tab to configure the conditions for a packet to match the ACL policy rule. Then enter information for the following fields.



Field	Description
Source IP Prefix	Enter the source IP address and prefix.
Destination IP Prefix	Enter the destination IP address and prefix.
Protocol Value	Enter a TCP or UDP protocol number.
Source Port	Enter the source port number.
Destination Port	Enter the destination port number.
DSCP	Enter a differentiated services code point (DSCP) value.
Routing Instance	Select the routing instance in which the packet is received.
ICMP Type	Select the type of ICMP message to match: ◦ Destination Unreachable ◦ Echo Reply ◦ Echo Request ◦ Information Query ◦ Information Response ◦ Multicast Listener Done ◦ Multicast Listener Query ◦ Multicast Listener Request ◦ Neighbor Advertisement ◦ Neighbor Solicitation ◦ Packet Too Large ◦ Parameter Problem ◦ Redirect ◦ Router Advertisement ◦ Router Renumbering ◦ Router Solicitation ◦ Time Exceeded
Interfaces (Group of Fields)	Click the + Add icon, and in the Add Interfaces popup window, in the Name field, select the Layer 3 interface or IRB on which the packet is received. Then click OK.

10. Select the Set tab to configure the action or actions to take when a packet matches the ACL policy rule. Then enter information for the following fields.


Add Rules
General
Match
Set
Counter
□ Packet
□ Byte
□ Policer Dropped Packet
□ Policer Dropped Byte
QoS Profile
---Please Select---
Action
---Please Select---
OK
Cancel

Field	Description
Counter (Group of Fields)	Configure packet and byte counters.
◦ Packet	Click to count packets that match the NPU ACL policy rule.
◦ Byte	Click to count bytes that match the NPU ACL policy rule.
◦ Policer Dropped Packet	Click to count packets dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
◦ Policer Dropped Byte	Click to count bytes dropped by the policer. When the rate of packets received at a port exceeds the committed information rate (CIR) value, the packet is classified as red and it is dropped.
QoS Profile	Select the QoS policy to apply traffic policers to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.
Action	Select the action to apply to packets that match the ACL policy rule: ◦ Allow—Permit, or accept, the packet. ◦ Deny—Bloc, the packet. ◦ Service PIC—The service PIC enables Layer 2 and Layer 3 services on traffic that flows through the device, known as service chaining. This service chaining directs traffic internally from the NPU into the x86 processor. Select Service PIC to apply services such as antivirus filtering, firewalls, and traffic engineering to packets that match the policy rules. Then in the Service Actions field, select the action.
Service Actions	If you select the action Service PIC, select the action: ◦ Host—Send the packet to the VOS device's CPU to perform additional Layer 4 through Layer 7 processing.

11. Select the QoS Profiles tab to configure traffic rate policers to apply to packets that match the ACL policy rule. For more information, see Configure QoS Profiles, below.
12. Click OK.

Configure QoS Profiles

You can associate a traffic policer with an NPU ACL to control the amount of traffic allowed by the ACL. To define a traffic policers, you configure a QoS profile. In the QoS profile, you can choose one of the following types of policers:

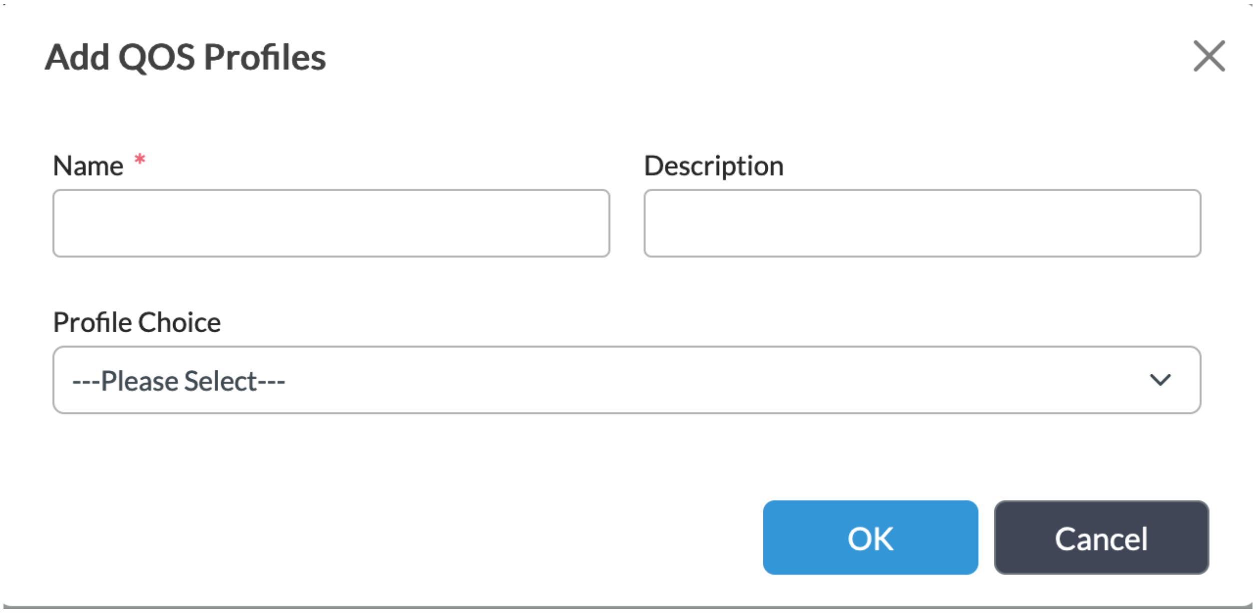
- Single-rate-two-color-policer
- Single-rate-three-color-policer
- Two-rate-three-color-policer

- QoS Profile tab: Name, Description, Profile Choice (select: Single-Rate, Two-Color Policer, Single-Rate, Three-Color Policer, Two-Rate, Three-Color Policer)

For each tenant or branch, you can configure one single-wide NPU ACL policy and one double-wide NPU ACL policy.

To configure a QoS profile to associate with an NPU ACL policy:

1. Select Director View in the top menu bar.
2. Select Devices > Devices in the horizontal menu bar.
3. Click the name of an appliance. The view changes to Appliance view.
4. Select the Configuration tab in the top menu bar.
5. Select Networking > NPU in the left menu bar.
6. Select the type of NPU ACL policy:
    a. IPv4 ACL Ingress, Single Wide
    b. IPv4 ACL Ingress, Double Wide
    c. IPv6 ACL Ingress
    d. Layer 2 ACL Ingress
7. Select the QoS Profiles tab in the horizontal menu bar.
8. Click the + Add icon or button. In the Add QoS Profiles popup window, enter information for the following fields.



Add QOS Profiles

Name *

Description

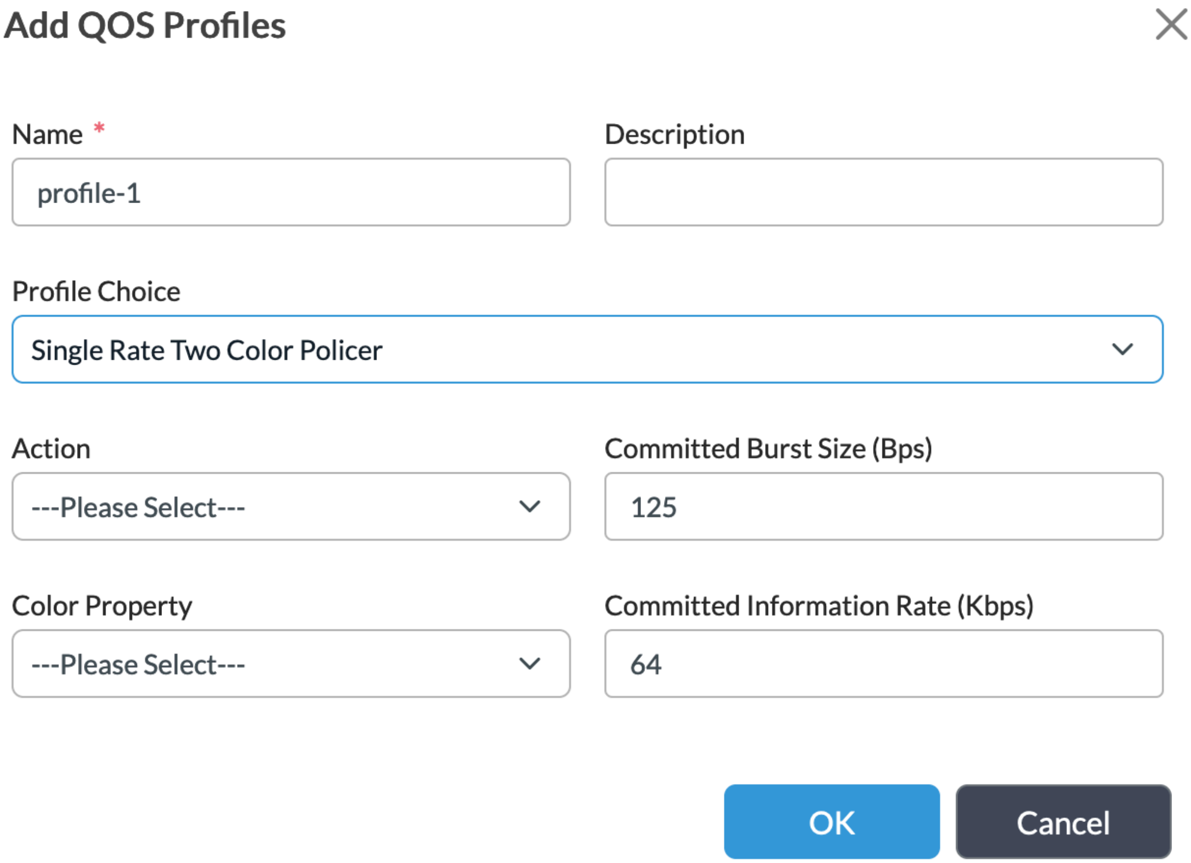
Profile Choice

---Please Select---

Field	Description
Name (Required)	Enter a name for the QoS profile. The name can be up to 255 characters.
Description	Enter a text description for the QoS profile.
Profile Choice	Select the type of profile to use to limit traffic on the interface: ◦ Single-Rate, Two-Color Policer—Configure a policer that consider the CIR and CBS values when limiting traffic flow. If the traffic rate falls below both values, the packets are marked as green. If the packet rate exceeds both the CIR and CBS thresholds, the packets are marked as red. By default, packets that are marked as green are allowed to pass, and those marked as red are dropped. ◦ Single-Rate, Three-Color Policer—Configure a policer that considers the CIR, CBS, and PBS values when limiting traffic flow. If the traffic rate falls below the CIR, CBS, and PBS values, the packets are marked as green. If the traffic rate falls between CBS and PBS thresholds, the packets are marked as yellow. If the packet rate exceeds either the CIR, CBS, or PBS values, the packets are marked as red. By default, packets that are marked as green or yellow are allowed to pass, and those marked as red are dropped. ◦ Two-Rate, Three-Color Policer—Configure a policer that considers the CIR, CBS, PIR, and PBS values when limiting traffic flow. If the traffic rate falls below the CIR, CBS, PIR, and PBS values, the packets are marked as green. If the packet rate is between CIR/CBS and PIR/PBS thresholds, the packets are marked as yellow. If the packet rate exceeds the both CIR/CBS and PIR/PBS threshold, the packets are marked as red. By default, packets that are marked as green or yellow are allowed to pass, and those marked as red are dropped.
Action	Select the action to take when packets match the configured policer properties: ◦ Allow—Allow the packets to pass. This is the implicit action.

Color Property	Select how to handle a received packet that is already marked with a color: ◦ Color Aware—Examine a packet's PLP markings and then place the packet in the correct token bucket. Currently, this option is not supported. ◦ Color Blind—Police the traffic without examining the DSCP values for PLP.
Committed Burst Size	Enter the CBS value, in bytes per second (Bps). The CBS is the average volume of burst traffic that can pass through an interface. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Committed Information Rate	Enter the CIR value, in kilobits per second (Kbps). The CIR is the average rate of traffic that can pass through an interface. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps
Peak Burst Size	For three-color policers only, enter the PBS value, in bytes per second (Bps). The PBS is the maximum volume of burst traffic that can pass through an interface. The PBS value must be equal to or greater than the CBS value. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Peak Information Rate	For two-rate, three-color policers only, enter the PIR value, in kilobits per second (Kbps). The PIR is the maximum rate of traffic that can pass through an interface. The PIR value must be equal to or greater than the CIR value. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps

9. If you select the Single-Rate, Two-Color Policer in the Profile Choice field, enter information for the following fields.



Add QOS Profiles

Name * profile-1

Description

Profile Choice: Single Rate Two Color Policer

Action: ---Please Select---

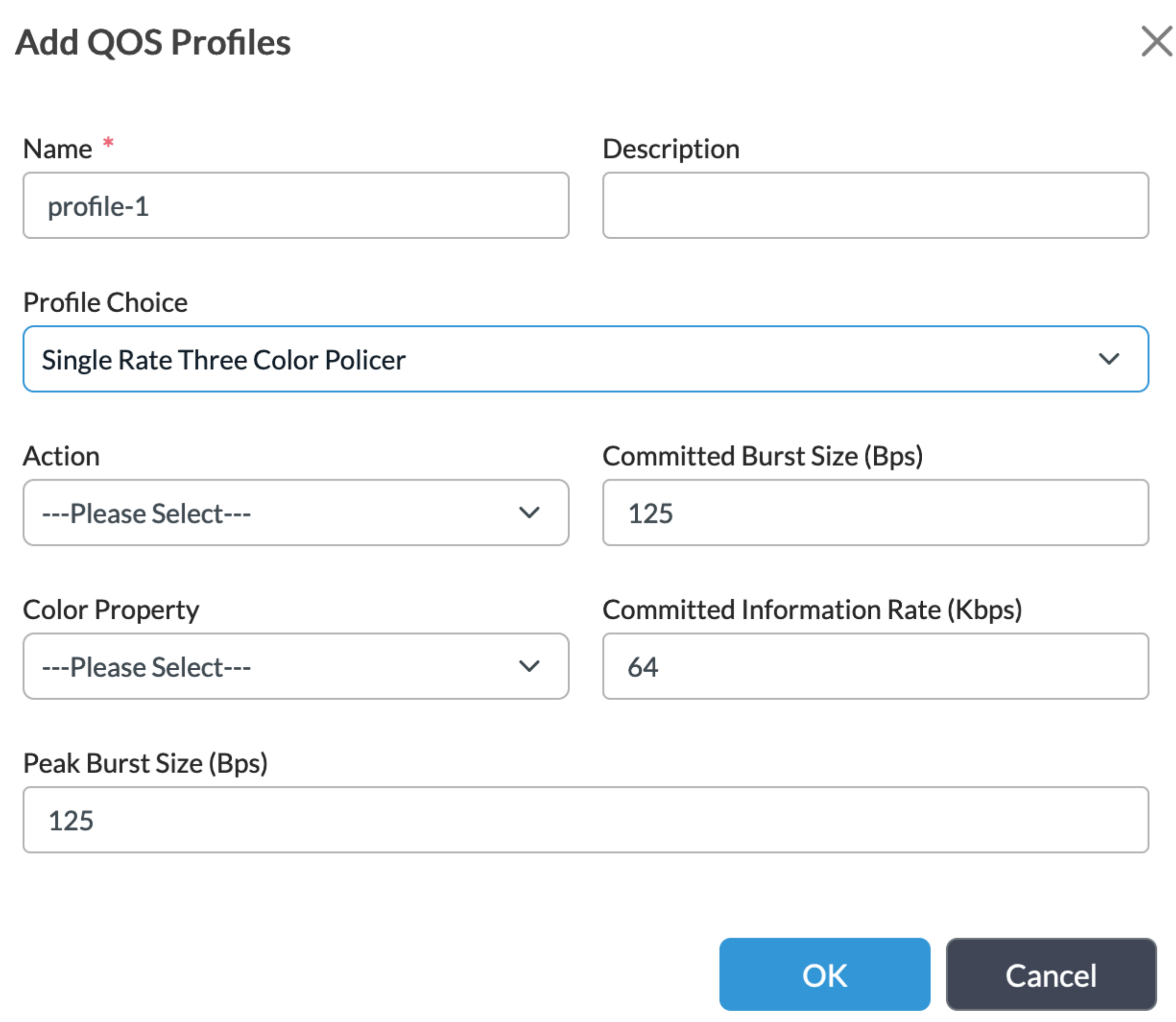
Committed Burst Size (Bps): 125

Color Property: ---Please Select---

Committed Information Rate (Kbps): 64

Field	Description
Action	Select the action to take when packets match the configured policer properties: ◦ Allow—Allow the packets to pass. This is the implicit action.
Color Property	Select how to handle a received packet that is already marked with a color: ◦ Color Aware—Examine a packet's PLP markings and then place the packet in the correct token bucket. Currently, this option is not supported. ◦ Color Blind—Police the traffic without examining the DSCP values for PLP.
Committed Burst Size	Enter the CBS value, in bytes per second (Bps). The CBS is the average volume of burst traffic that can pass through an interface. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Committed Information Rate	Enter the CIR value, in kilobits per second (Kbps). The CIR is the average rate of traffic that can pass through an interface. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps

10. If you select the Single-Rate, Three-Color Policer in the Profile Choice field, enter information for the following fields.



Add QOS Profiles

Name *

profile-1

Description

Profile Choice

Single Rate Three Color Policer

Action

---Please Select---

Committed Burst Size (Bps)

125

Color Property

---Please Select---

Committed Information Rate (Kbps)

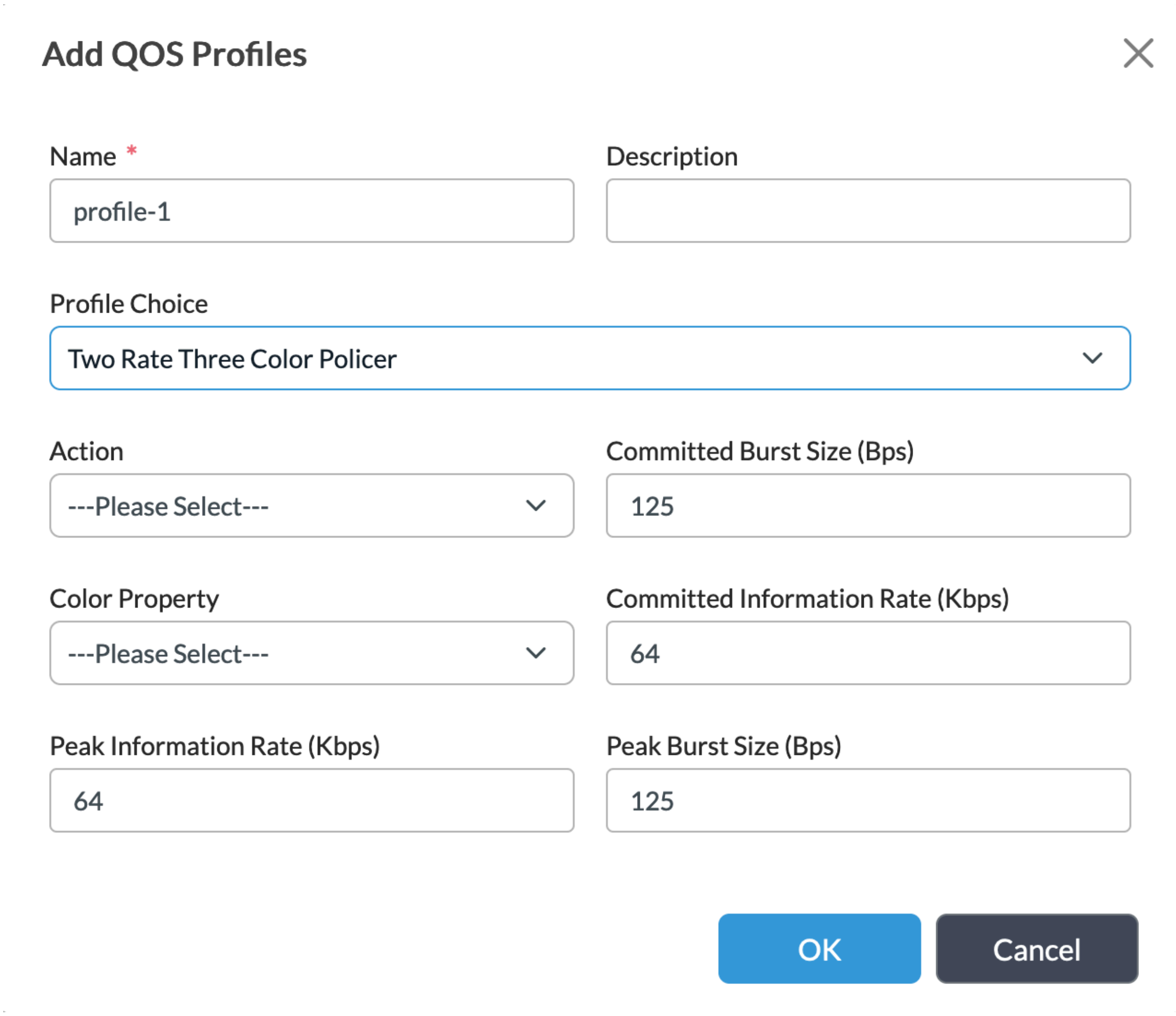
64

Peak Burst Size (Bps)

125

Field	Description
Action	Select the action to take when packets match the configured policer properties: ◦ Allow—Allow the packets to pass. This is the implicit action.
Color Property	Select how to handle a received packet that is already marked with a color: ◦ Color Aware—Examine a packet's PLP markings and then place the packet in the correct token bucket. Currently, this option is not supported. ◦ Color Blind—Police the traffic without examining the DSCP values for PLP.
Committed Burst Size	Enter the CBS value, in bytes per second (Bps). The CBS is the average volume of burst traffic that can pass through an interface. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Committed Information Rate	Enter the CIR value, in kilobits per second (Kbps). The CIR is the average rate of traffic that can pass through an interface. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps
Peak Burst Size	Enter the PBS value, in bytes per second (Bps). The PBS is the maximum volume of burst traffic that can pass through an interface. The PBS value must be equal to or greater than the CBS value. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second

11. If you select the Single-Rate, Three-Color Policer in the Profile Choice field, enter information for the following fields.



Add QOS Profiles

Name * profile-1

Description

Profile Choice: Two Rate Three Color Policer

Action: ---Please Select---

Committed Burst Size (Bps): 125

Color Property: ---Please Select---

Committed Information Rate (Kbps): 64

Peak Information Rate (Kbps): 64

Peak Burst Size (Bps): 125

Field	Description
Action	Select the action to take when packets match the configured policer properties: ◦ Allow—Allow the packets to pass. This is the implicit action.
Color Property	Select how to handle a received packet that is already marked with a color: ◦ Color Aware—Examine a packet's PLP markings and then place the packet in the correct token bucket. Currently, this option is not supported. ◦ Color Blind—Police the traffic without examining the DSCP values for PLP.
Committed Burst Size	Enter the CBS value, in bytes per second (Bps). The CBS is the average volume of burst traffic that can pass through an interface. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Committed Information Rate	Enter the CIR value, in kilobits per second (Kbps). The CIR is the average rate of traffic that can pass through an interface. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps
Peak Burst Size	Enter the PBS value, in bytes per second (Bps). The PBS is the maximum volume of burst traffic that can pass through an interface. The PBS value must be equal to or greater than the CBS value. *Range:* 125 through 4294967295 bytes per second *Default:* 125 bytes per second
Peak Information Rate	Enter the PIR value, in kilobits per second (Kbps). The PIR is the maximum rate of traffic that can pass

	through an interface. The PIR value must be equal to or greater than the CIR value. *Range*: 64 through 4294967295 bytes per second *Default:* 64 Kbps

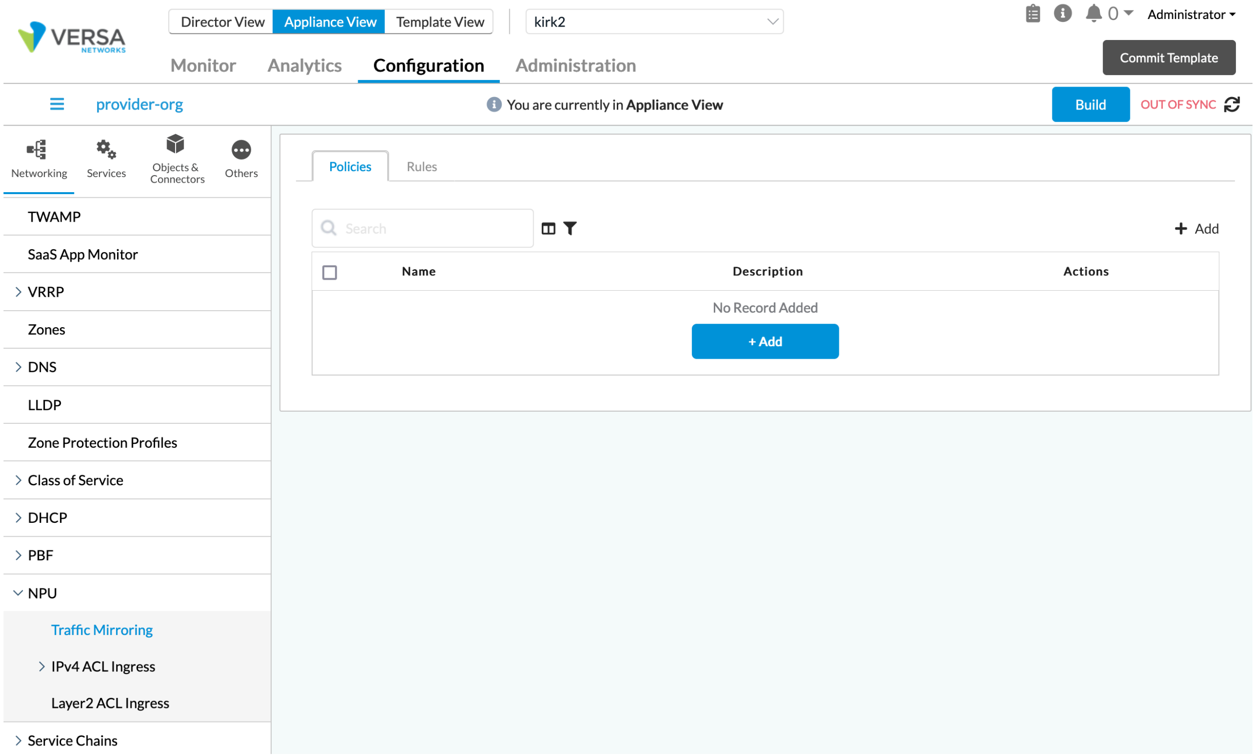
12. Click OK.

Configure Traffic Mirroring

Traffic mirroring lets you copy network traffic from an interface and send the traffic to out-of-band security and monitoring appliances for additional processing, including content inspection, threat monitoring, and troubleshooting. The VOS traffic mirroring supports switched port analyzer (SPAN) mirroring, in which the SPAN session sends a copy (mirror) of the traffic to another interface on the VOS device.

To configure a traffic mirroring NPU ACL policy:

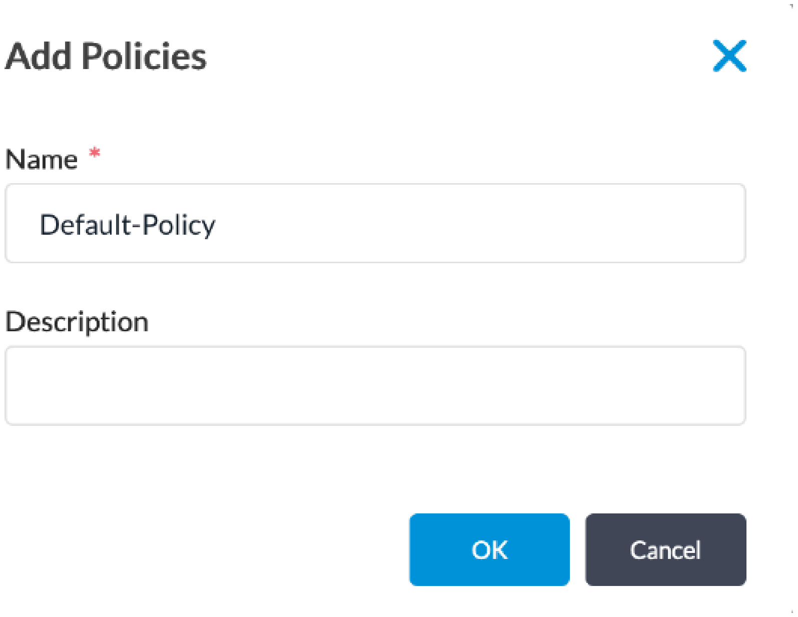
1. Select Director View in the top menu bar.
2. Select Devices > Devices in the horizontal menu bar.
3. Click the name of an appliance. The view changes to Appliance view.
4. Select the Configuration tab in the top menu bar.
5. Select Networking > NPU > Traffic Mirroring in the left menu bar.



You are currently in **Appliance View**

No Record Added

6. Select the Policies tab in the horizontal menu.
7. Click the + Add icon or button. In the Add Profiles popup window, enter information for the following fields.



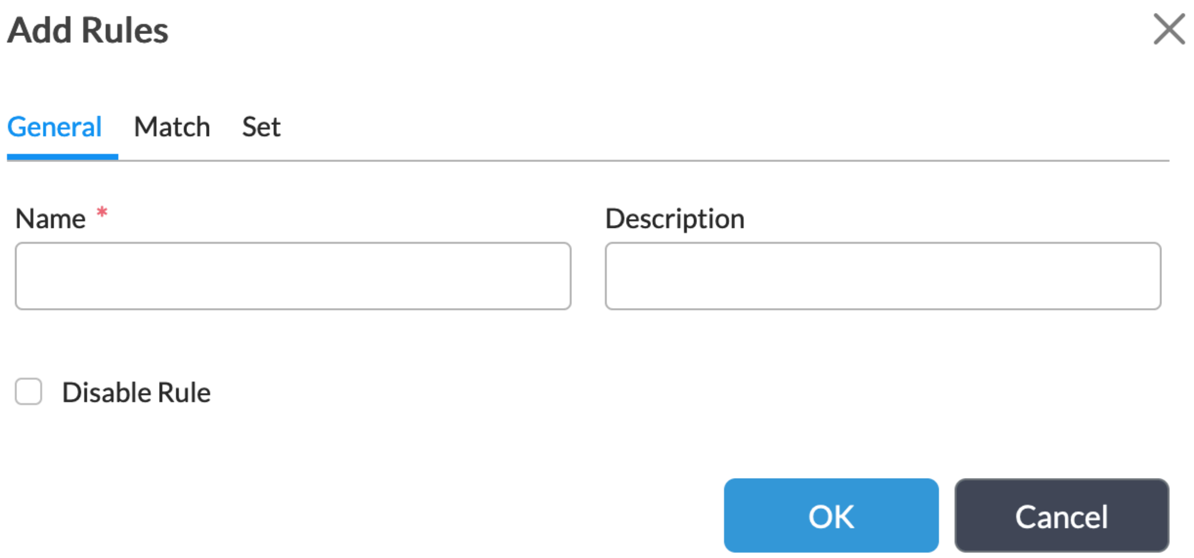
Add Policies

Name *: Default-Policy

Description:

Field	Description
Name (Required)	Enter a name for the NPU ACL traffic-mirroring policy.
Description	Enter a text description for the NPU traffic-mirroring policy rule.

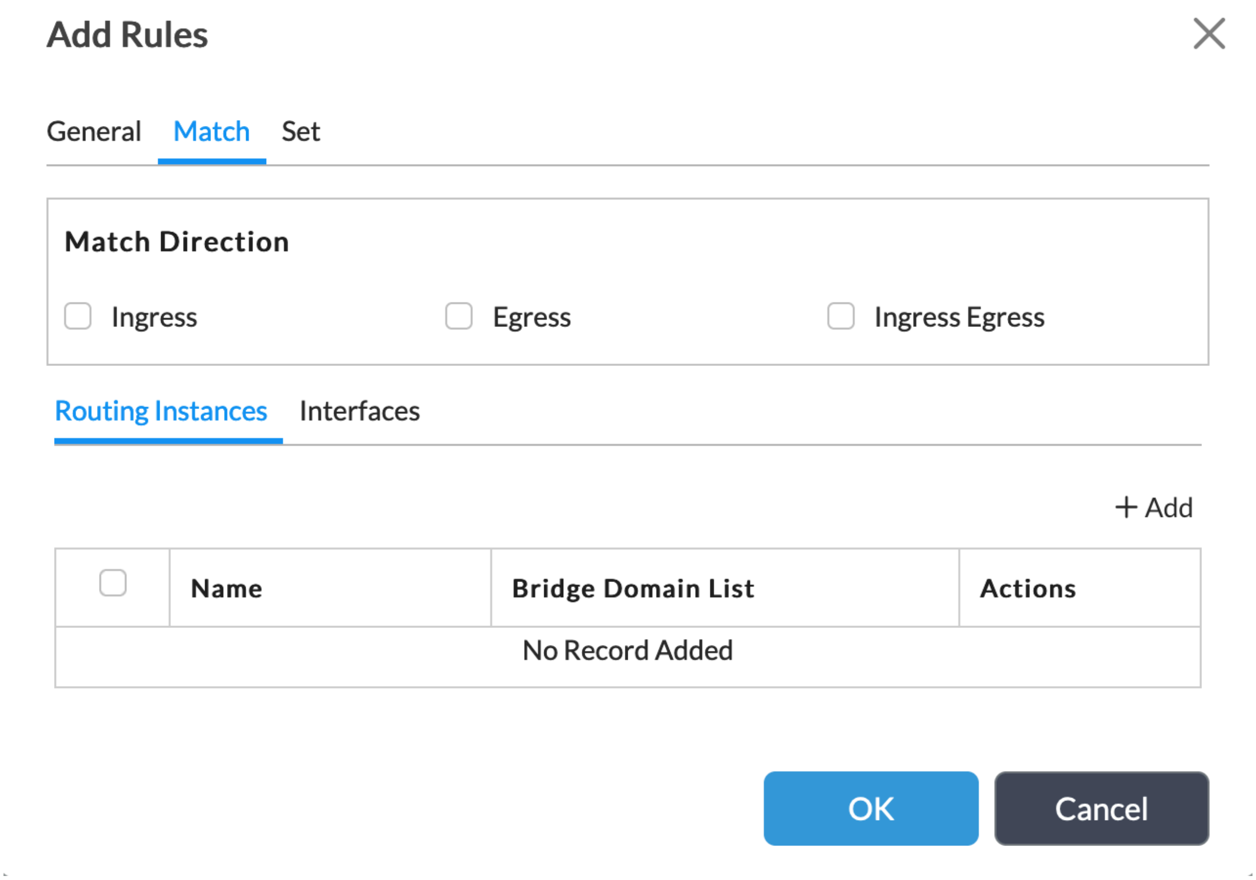
8. Click OK.
9. Select the Rules tab in the horizontal menu bar.
10. Click the + Add icon or button. The Add Rules popup window.



11. Select the General tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the NPU ACL traffic mirroring policy.
Description	Enter a text description for the NPU ACL policy rule.
Disable Rule	Click to disable the rule when you commit the configuration.

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



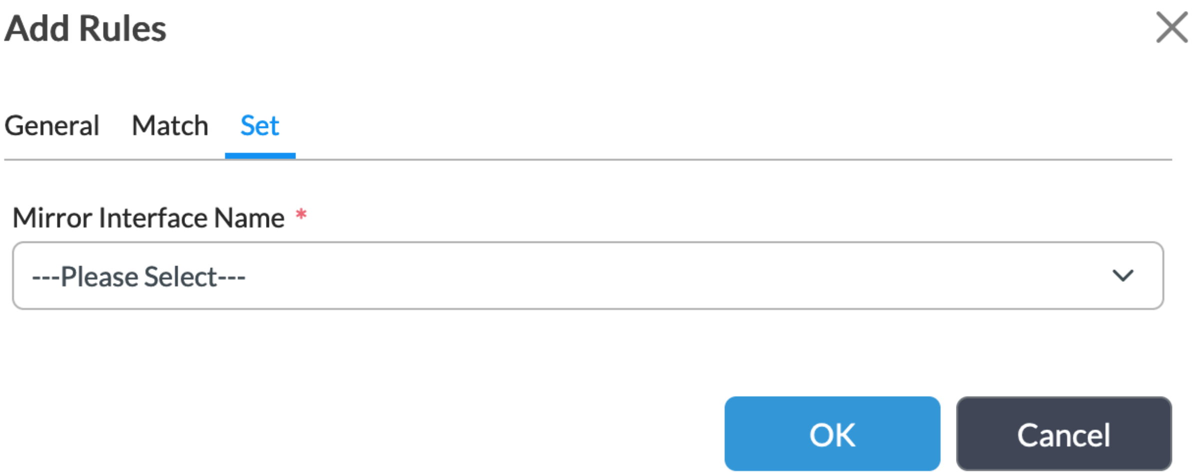
Match Direction

□ Ingress □ Egress □ Ingress Egress

□	Name	Bridge Domain List	Actions
No Record Added			

Field	Description
Match Direction (Group of Fields)	
◦ Ingress	Click to have the rule match incoming traffic.
◦ Egress	Click to have the rule match outgoing traffic.
◦ Ingress Egress	Click to have the rule match both incoming and outgoing traffic.
Routing Instances (Tab)	Select the routing instances to which to apply the rule.
◦ + Add icon	Click to add a new routing instance. The Add Routing Instances popup window displays.
◦ Name	Select the name of the routing instance.
◦ Bridge Domain List	Select the name of the bridge domain within the routing instance.
◦ OK	Click OK to add the new routing instance to the rule.
Interfaces (Tab)	Select the interfaces to which to apply the rule.The Add Interfaces popup window displays.
◦ Name	Select the name of the interface and interface port to which to apply the rule.

13. Select the Set tab, and enter information for the following field.



Add Rules

Mirror Interface Name *

---Please Select---

Field	Description
Mirror Interface Name	Select the name of the interface to which to mirror the traffic.

14. Click OK.

Software Release Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

Configure Interfaces
Configure Layer 2 Forwarding
Configure Policy-Based Forwarding
Configure SD-WAN Policy