

---

## Configure Flow Mirroring

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

Versa Operating System™ (VOS™) devices support Layer 3 flow mirroring for lawful interception, security forensics, and enhanced data analytics. A VOS device mirrors the packets based on a match criteria, and then it sends the filtered packets to a packet collection device over a physical virtual network interface (vni) or a tunnel virtual interface (tvi). Flow mirroring can mirror any packets, including egress packets (packets sent by the VOS device), ingress packets (packets received by the VOS device), and packets that are transiting the VOS device. You can use the VOS web interface to enable host-bound services for ingress and egress packets.


You can configure flow mirroring on an Ethernet interface or on a GRE or an IPsec tunnel.

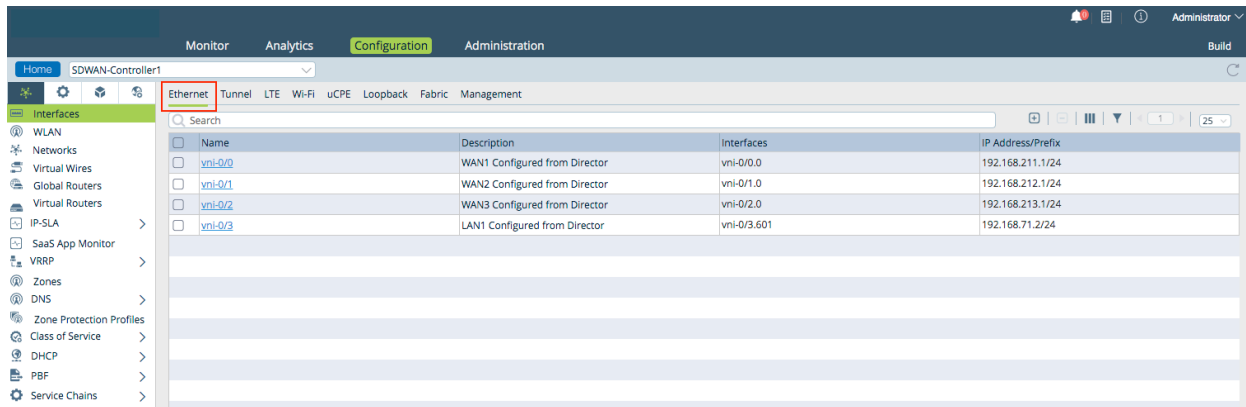
If the mirror interface is an Ethernet interface, the source and destination MAC addresses in the Layer 2 header are set to the interface's MAC address. To support mirroring of packets that must match certain application or URL categories, packets are replicated and then retained until the application is identified or the URL category is determined.

Note that packet mirroring cannot determine the IP address for ingress NATed packets.

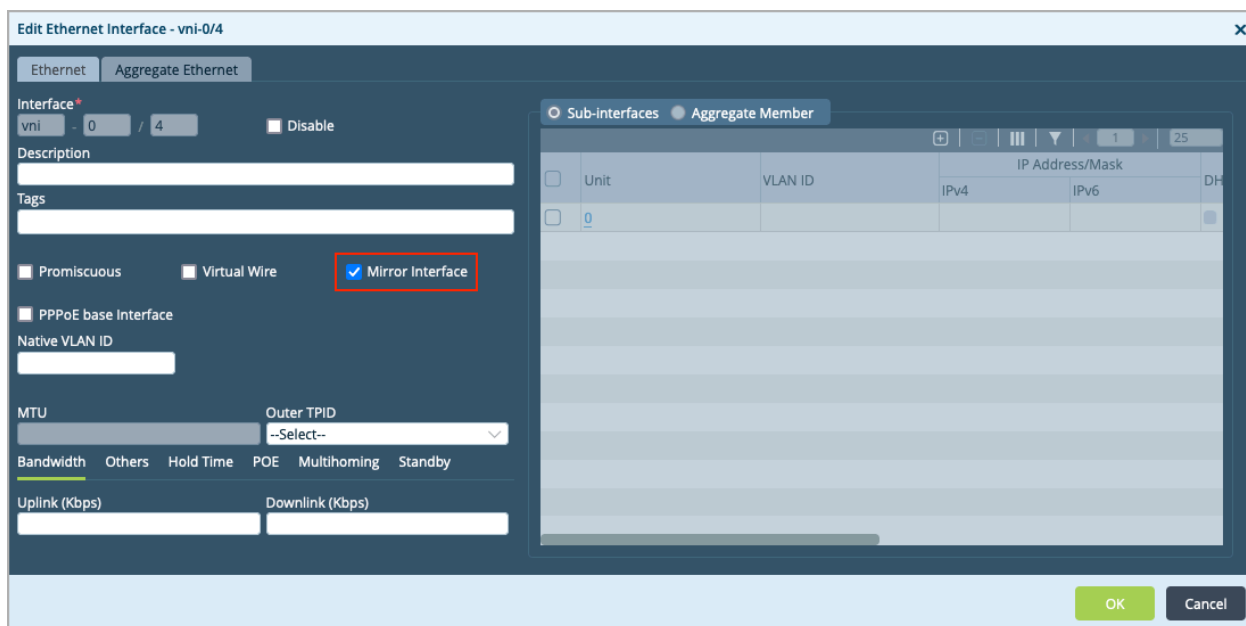
---

## Configure Flow Mirroring on an Ethernet Interface

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces in the left menu bar.
4. Select the Ethernet tab in the horizontal menu bar.



- Click the Add icon to create a new Ethernet interface for flow mirroring, or select an interface in the main pane to edit an existing Ethernet interface. The Add/Edit Ethernet Interface popup window displays.
- Select the Ethernet tab.
- Click Mirror Interface to enable flow mirroring on the Ethernet interface. Note that when you configure an Ethernet interface as a mirror interface, the MTU, Subinterfaces, and Aggregate Member fields are grayed out, and you cannot configure values for these fields. For information configuring other Ethernet interface properties, see [Configure Interfaces](#).



- Click OK.
- Select Others > Service Nodes > Service Node Groups in the left menu bar.
- In the main pane, select default-sng, for the default service node group. The Edit Service Node Group popup window displays.
- In the Services group of fields, click TDF (for traffic detection function) in the Available Services table to move it to

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Common\\_Configuration/Configure\\_Flow\\_...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Flow_...)

Updated: Wed, 23 Oct 2024 08:24:57 GMT

Copyright © 2024, Versa Networks, Inc.

the Selected Services table.

Edit Service Node Group - default-sng

Name\*

default-sng

Service Node Group ID\*

0

Description

Tags

Type

Internal

Elastic Policy

--Select--

Egress Interface

--Select--

Ingress Interface

--Select--

Service Function Egress Address

Service Function Ingress Address

Services\*

Available Services

Add All

Search

adc

stateful-firewall

Selected Services

Remove All

Search

cgnat

nextgen-firewall

ipsec


sdwan

tdf

OK

Cancel

12. Click OK.

13. Select Others  > Organization > Limits in the left menu bar.

Organization Name	Appliance Owner	Services	Service Node Groups	Service Node Group Clus...	Peak Rate (pps)	Peak Rate (Kbps)	Peak Burst Size	Session Rate	Session...
Tenant5	False	sdwan	default-sng						
Tenant6	False	sdwan	default-sng						
Tenant7	False	sdwan	default-sng						
Tenant8	False	sdwan	default-sng						
Tenant9	False	sdwan	default-sng						
provider-org	True	cgnat nextgen-firewall tdf	default-sng						

14. Select an organization in the main pane. You must select an organization whose Appliance Owner field status is True. The Edit Organization Limit popup window displays.

### Edit Organization Limit - provider-org

- General
- Traffic Identification
- Resources
- Services
- Local Node Groups

☐ Available Service Node Groups

☐ default-sng

☐ Available Service Node Group Cluster

☐ Services
 

- ☐ cgnat
- ☐ nextgen-firewall
- ☐ tdf

OK

Cancel

15. Select the Services tab.
16. In the Services field, click the Add icon and add the TDF service.
17. Click OK.
18. Select Services > TDF > Traffic Mirroring Policy in the left menu bar.
19. Select the Policies tab in the horizontal menu bar, and then click the Add icon. The Add Policies popup window displays. Enter information for the following fields.

Add Policies

Name\*


Description

Tags

OK

Cancel

Field	Description
Name (Mandatory)	Enter the name of the traffic-mirroring policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the policy. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

20. Click OK.
21. Select the Rules tab in the horizontal menu bar, and then click the  Add icon. The Add Rules popup window displays.
22. (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup window displays.
  - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

Configure Rule Order
✕

Please choose from the following where the new rule to be inserted.  
Rule will be added at bottom as default.

☒ Insert At Bottom  
☐ Insert At Top

Ok

- b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:

Configure Rule Order
✕

Please choose from the following where the new rule to be inserted  
from selected rule p1.  
Rule will be added at bottom as default.

☒ Insert At Bottom  
☐ Insert At Top  
☐ Insert Before Selected Rule  
☐ Insert After Selected Rule

Ok







- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Rule popup window displays.
23. Select the General tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter the name of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the rule. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

22. Select the Source/Destination tab, and enter information for the following fields.

The screenshot shows the 'Add Rules' dialog box with the 'Source/Destination' tab selected. The dialog contains the following fields and controls:

- Source Zone:** A list box with a '+ New Zone' button at the bottom.
- Destination Zone:** A list box with a '+ New Zone' button at the bottom.
- Source Site Name:** A list box with a '+ New Site Name' button at the bottom.
- Destination Site Name:** A list box with a '+ New Site Name' button at the bottom.
- Source Address:** A list box with a '+ New Address Group' and '+ New Address' button at the bottom.
- Destination Address:** A list box with a '+ New Address Group' and '+ New Address' button at the bottom.
- Source Address Negate:** A checkbox.
- Destination Address Negate:** A checkbox.
- Routing Instance:** A dropdown menu with '--Select--' as the current selection.
- Egress Routing Instance:** A dropdown menu with '--Select--' as the current selection.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Field	Description
Source Zone	Source zones to which to apply the rule. The rule applies to traffic received from any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Destination Zone	Destination zones to which to apply the rule. The rule applies to traffic sent to any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Source Site Name	Source sites to which to apply the rule. Click the  Add icon to add sites.
Destination Site Name	Destination sites to which to apply the rule. Click the  Add icon to add sites.
Source Address	Source addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Source Address Negate	Select to apply the rule to any source addresses except the ones in the Source Address field.
Destination Address	Destination addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Destination Address Negate	Select to apply the rule to any destination addresses except the ones in the Destination Address field.
Routing Instance	Select the ingress routing instance to which to apply the rule.
Egress Routing Instance	Select the egress routing instance to which to apply the rule.

23. Click OK.

24. Select the Enforce tab, and enter information for the following fields.



Field	Description
Ingress	Click to mirror ingress traffic on the VOS device. <i>Default:</i> Disabled
Egress	Click to mirror the egress traffic on the VOS device. <i>Default:</i> Disabled
Mirror Interface	Select the interface on which to mirror the traffic.
Packet Count Per Flow	Enter the number of packets per flow to be mirrored. <i>Range:</i> 0 through 4294967295 <i>Default:</i> None

25. Select the Headers/Schedule, Applications/URL, and Users/Groups tabs and configure any necessary information.
26. Click OK.

## Configure Flow Mirroring on an Ethernet Interface Using the CLI

1. Create a qualifier interface, which acts as a mirror interface. This interface can be a vni, an IPsec, or a GRE interface.

```
admin@Branch1-cli(config)% set interfaces vni-0/4 unit 0 enable true
admin@Branch1-cli(config)% set interfaces vni-0/4 mirror-interface
```

Note: You cannot configure an IP address for this interface, and you cannot assign this interface to any organization or routing interface.

2. Enable the traffic-mirroring service on the VOS device and add the TDF service in an available service node group. Doing this introduces flow mirroring as a new service in the TDF service set.

```
admin@Branch1-cli(config)% set service-node-groups default-sng services tdf
```

3. Configure a traffic-monitoring policy rule in the organizational services:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
policy-name rules rule-name
```

4. Create a policy match criteria for the packets to mirror on the mirror interface:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
example-policy1 rules example-rule1 match
```

5. Create a policy action criteria to define the action to take when packets match the match criteria:



```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
example-policy1 rules example-rule1 set
```

---

## Configure Flow Mirroring over a GRE Tunnel

This section describes how to configure flow mirroring over a GRE tunnel. Flow mirroring over a GRE tunnel adds the following fields to the packet header:

Outer MAC	Outer IP Header	GRE	Mirrored IP/IPv6 Packets
-----------	-----------------	-----	--------------------------

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces > Tunnel in the left menu bar.
4. Click the  Add icon. The Add Tunnel Interface popup window displays.
5. Select the Tunnel tab, and then click Mirror Interface to enable flow mirroring on the tunnel. In the Tunnel Type field, select Point-To-Point GRE Tunnel.

Add Tunnel Interface

Tunnel

Pseudo Tunnel

PPPoE

Interface\*

tvi
0
/
43

☐ Disable
☒ Mirror Interface

Description

MTU

1400

Mode

IPsec

Tunnel Type

Point-to-point GRE tunnel

Source\*

1.1.1.1

Destination\*

2.2.2.2

Routing Instance\*


Global

Sub-interfaces

	Unit	IP Address/Mask		DHCP V6	Interface Mode	VLAN ID	VLAN ID List
		IPv4	IPv6				
<input type="checkbox"/>	0			<input type="checkbox"/>			
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

OK

Cancel

6. Click OK.
7. Select Others  > Service Nodes > Service Node Groups in the left menu bar.
8. Select default-sng in the main pane. The Edit Service Node Group popup window displays.
9. In the Services group of fields, click TDF in the Available Services table to move it to the Selected Services table.

Edit Service Node Group - default-sng

Name\*

default-sng

Service Node Group ID\*

0

Description

Tags

Type

Internal

Elastic Policy

--Select--

Egress Interface

--Select--

Ingress Interface

--Select--

Service Function Egress Address

Service Function Ingress Address

Services\*

Available Services

Add All

Search

adc

stateful-firewall

ipsec

tdf

secure-access

Selected Services

Remove All

Search

cgnat


nextgen-firewall

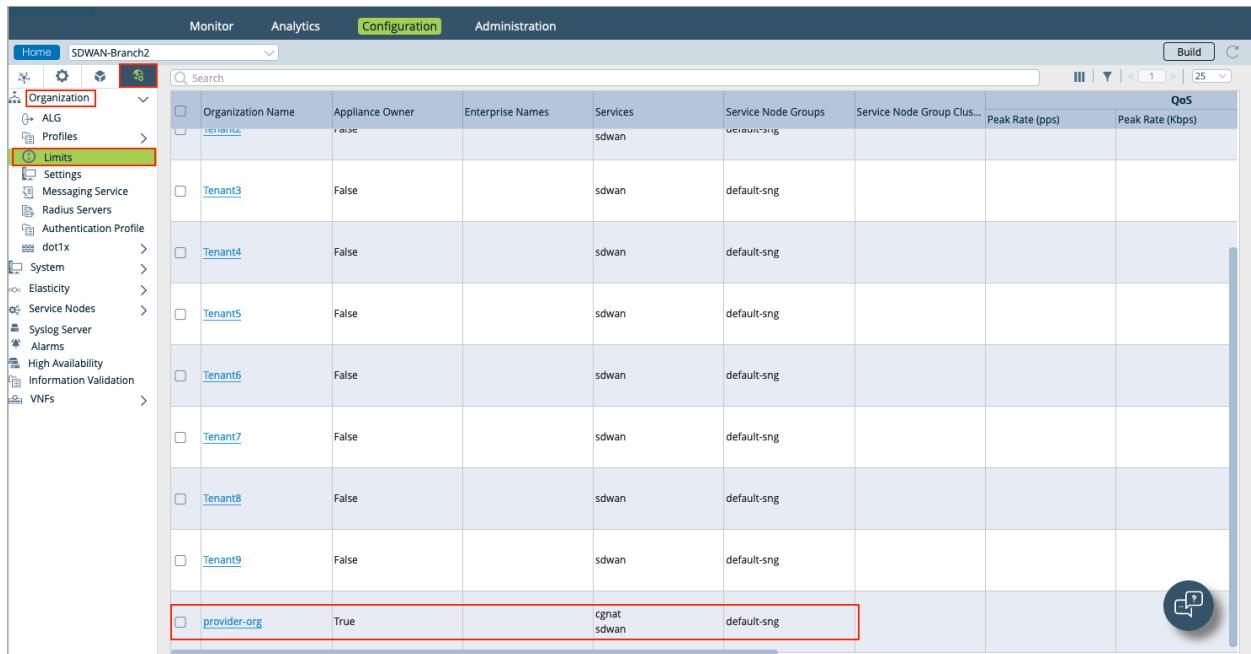
sdwan

OK

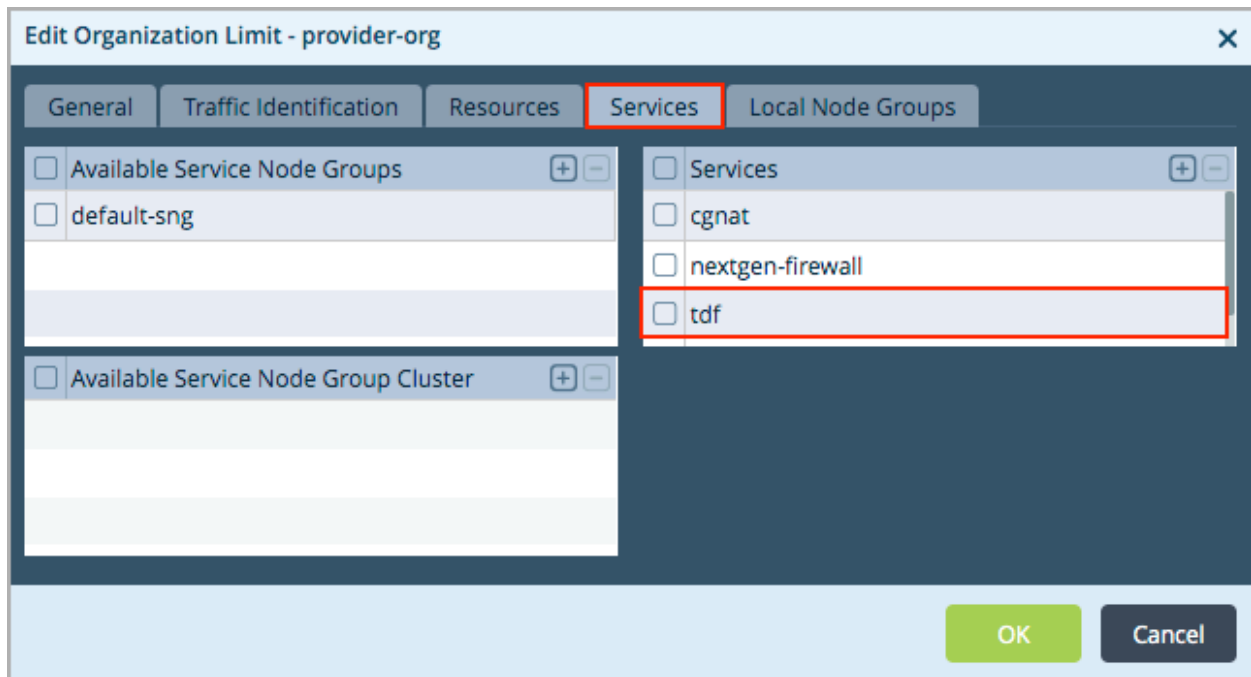
Cancel

10. Click OK.



11. Select Others  > Organization > Limits in the left menu bar.

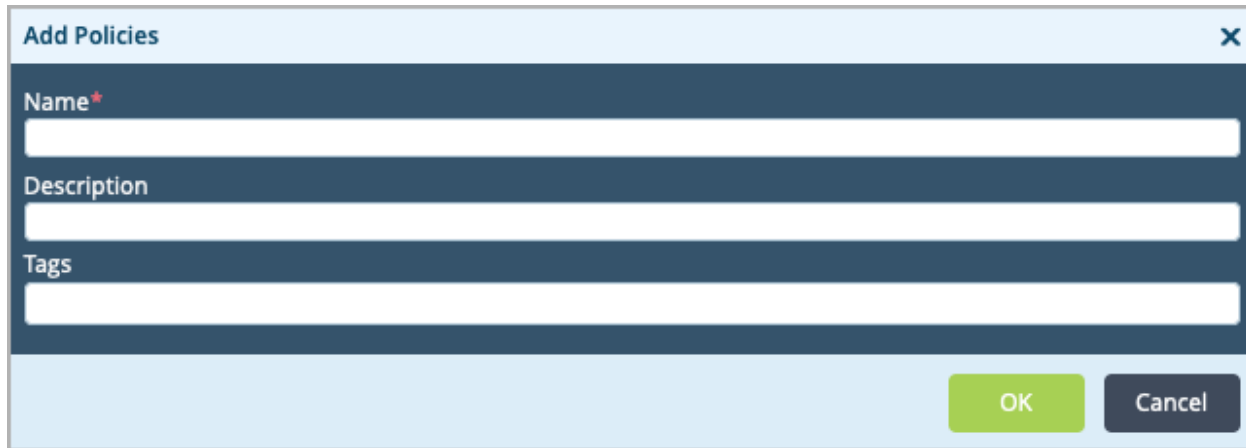


12. Select an organization in the main pane. You must select an organization whose Appliance Owner field status is True. The Edit Organization Limit popup window displays.




13. Select the Services tab.
14. In the Services field, click the  Add icon and add the TDF service.
15. Click OK.

16. Select Services  > TDF > Traffic Mirroring Policy in the left menu bar.
17. Select the Policies tab in the horizontal menu bar, and click the  Add icon. The Add Policies popup window displays. Enter information for the following fields.



The image shows a 'Add Policies' popup window with a light blue header and a dark blue body. It contains three text input fields labeled 'Name\*', 'Description', and 'Tags'. At the bottom right, there are two buttons: 'OK' (green) and 'Cancel' (dark blue).

Field	Description
Name (Required)	Enter a name of the traffic-mirroring policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the policy. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

18. Click OK.
19. Select the Rules tab in the horizontal menu bar, and click the  Add icon. The Add Rules popup window displays.
20. (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup window displays.
  - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

Configure Rule Order
✕

Please choose from the following where the new rule to be inserted.  
Rule will be added at bottom as default.

☒ Insert At Bottom  
☐ Insert At Top

Ok

- b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:

Configure Rule Order
✕

Please choose from the following where the new rule to be inserted  
from selected rule p1.  
Rule will be added at bottom as default.

☒ Insert At Bottom  
☐ Insert At Top  
☐ Insert Before Selected Rule  
☐ Insert After Selected Rule

Ok

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
- d. Click OK. The Add Rule popup window displays.
21. Select the General tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter the name of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the rule. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None







22. Select the Source/Destination tab, and enter information for the following fields.

The screenshot shows the 'Add Rules' dialog box with the 'Source/Destination' tab selected. The dialog is divided into several sections for configuring rule parameters:

- Source Zone:** A list of zones with a '+ New Zone' button at the bottom.
- Destination Zone:** A list of zones with a '+ New Zone' button at the bottom.
- Source Site Name:** A list of site names with a '+ New Site Name' button at the bottom.
- Destination Site Name:** A list of site names with a '+ New Site Name' button at the bottom.
- Source Address:** A list of address groups with a '+ New Address Group' and '+ New Address' button at the bottom.
- Destination Address:** A list of address groups with a '+ New Address Group' and '+ New Address' button at the bottom.
- Source Address Negate:** A checkbox to toggle negation for source addresses.
- Destination Address Negate:** A checkbox to toggle negation for destination addresses.
- Routing Instance:** A dropdown menu to select a routing instance.
- Egress Routing Instance:** A dropdown menu to select an egress routing instance.

At the bottom right, there are 'OK' and 'Cancel' buttons.



Field	Description
Source Zone	Source zones to which to apply the rule. The rule applies to traffic received from any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Destination Zone	Destination zones to which to apply the rule. The rule applies to traffic sent to any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Source Site Name	Source sites to which to apply the rule. Click the  Add icon to add sites.
Destination Site Name	Destination sites to which to apply the rule. Click the  Add icon to add sites.
Source Address	Source addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Source Address Negate	Select to apply the rule to any source addresses except the ones in the Source Address field.
Destination Address	Destination addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Destination Address Negate	Select to apply the rule to any destination addresses except the ones in the Destination Address field.
Routing Instance	Select the ingress routing instance to which to apply the rule.
Egress Routing Instance	Select the egress routing instance to which to apply the rule.

23. Click OK.

24. Select the Enforce tab, and enter information for the following fields.

Field	Description
Ingress	Select to mirror ingress traffic on the VOS device. <i>Default:</i> Disabled
Egress	Select to mirror the egress traffic on the VOS device. <i>Default:</i> Disabled
Mirror Interface	Select the interface on which to mirror the traffic.
Packet Count Per Flow	Enter the number of packets per flow to be mirrored. <i>Range:</i> 0 through 4294967295 <i>Default:</i> None

25. Select the Headers/Schedule, Applications/URL, and Users/Groups tabs and configure any necessary information.
26. Click OK.

## Configure Flow Mirroring over a GRE Tunnel Using the CLI

1. Create a GRE tunnel to use for flow mirroring:

```
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/3 unit 0 enable true
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/3 mirror-interface
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/3 type gre tunnel source 1.1.1.1 destination 2.2.2
```

2. Enable the traffic-mirroring service on the VOS device, and add the TDF service in an available service node group. Doing this introduces flow mirroring as a new service in the TDF service set.

```
admin@Branch1-cli(config)% set service-node-groups default-sng services tdf
```

3. Configure a traffic-monitoring policy rule in an organization service:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
policy-name rules rule-name
```

4. Create policy match criteria for the packets to mirror on the mirror interface:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies  
example-policy1 rules example-rule1 match
```

5. Create policy action criteria to define the action to take when packets match the match criteria:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies  
example-policy1 rules example-rule1 set
```



---

## Configure Flow Mirroring over an IPsec Tunnel

This section describes how to configure the flow mirroring over an IPsec tunnel. Flow mirroring over an IPsec tunnel adds the following fields to the packet header:

Outer MAC	Outer IP Header	ESP	Encrypted Mirrored IP/IPv6 Packets
-----------	-----------------	-----	------------------------------------

To configure flow mirroring over an IPsec tunnel:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces > Tunnel in the left menu bar.
4. Click the  Add icon. The Add Tunnel Interface popup window displays.
5. Select the Tunnel tab, and then click Mirror Interface to enable flow mirroring on the IPsec tunnel. In the Tunnel Type field, select Point-To-Point IPsec Tunnel.

**Add Tunnel Interface**

**Tunnel** Pseudo Tunnel PPPoE

Interface\* tvi 0 / 43 ☐ Disable ☒ Mirror Interface

Description

MTU 1400 Mode IPsec

Tunnel Type Point-to-point IPsec tunnel

**Sub-interfaces**

<input type="checkbox"/>	Unit	IP Address/Mask		DHCP V6	Interface Mode	VLAN ID	VLAN ID List
		IPv4	IPv6				
<input type="checkbox"/>	0			<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			
<input type="checkbox"/>				<input type="checkbox"/>			

OK Cancel

6. Click OK.
7. Create IPsec profiles. For more information, see the Configure IPsec Profiles section in the [Create and Manage Staging and Post-Staging Templates](#) article.
8. Select Others > Service Nodes > Service Node Groups in the left menu bar.
9. In the main pane, select default-sng. The Edit Service Node Group popup window displays.
10. In the Services group of fields, click TDF in the Available Services table to move it to the Selected Services table.

Edit Service Node Group - default-sng

Name\*

default-sng

Service Node Group ID\*

0

Description

Tags

Type

Internal

Elastic Policy

--Select--

Egress Interface

--Select--

Ingress Interface

--Select--

Service Function Egress Address

Service Function Ingress Address

Services\*

Available Services

Add All

Search

adc

>

stateful-firewall

>

ipsec

>

tdf

>

secure-access

>

Selected Services

Remove All

Search

cgnat

×

nextgen-firewall

×


sdwan

×

OK

Cancel

11. Click OK.

12. Select Others  > Organization > Limits in the left menu bar.

13. Select an organization in the main pane. You must select an organization whose Appliance Owner field status is True. The Edit Organization Limit popup window displays.

**Edit Organization Limit - provider-org**

General Traffic Identification Resources **Services** Local Node Groups

☐ Available Service Node Groups + -

☐ default-sng

☐ Available Service Node Group Cluster + -

☐ Services + -

☐ cgnat

☐ nextgen-firewall

☒ tdf

OK Cancel

14. Select the Services tab.
15. In the Services field, click the + Add icon and add the TDF service.
16. Click OK.
17. Select Services > TDF > Traffic Mirroring Policy in the left menu bar.
18. Select the Policies tab in the horizontal menu bar, and click the + Add icon. The Add Policies popup window displays. Enter information for the following fields.

**Add Policies**


Name\*


Description

Tags

OK Cancel

Field	Description
Name (Mandatory)	Enter the name of the traffic-mirroring policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the policy. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the policy. Tags allow you to locate a policy when you perform a filtered search of all policies.  <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

19. Click OK.
20. Select the Rules tab in the horizontal menu bar, and click the  Add icon. The Edit Rules popup window displays.
21. (For Releases 21.2.1 and later.) If you have already added one or more rules, the Configure Rule Order popup window displays.
  - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.

Configure Rule Order 

Please choose from the following where the new rule to be inserted.

Rule will be added at bottom as default.

☒ Insert At Bottom

☐ Insert At Top

Ok

- b. If you select a rule and then click the Add icon, the Configure Rule Order popup window displays the following options:

Configure Rule Order
X

Please choose from the following where the new rule to be inserted from selected rule p1.  
Rule will be added at bottom as default.

☒ Insert At Bottom  
☐ Insert At Top  
☐ Insert Before Selected Rule  
☐ Insert After Selected Rule

Ok

- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
  - d. Click OK. The Add Rule popup window displays.
22. Select the General tab, and enter information for the following fields..

Field	Description
Name (Required)	Enter the name of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Description	Enter a description of the rule. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None
Tags	Enter a text string or phrase to associate with the rule. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

23. Select the Source/Destination tab, and enter information for the following fields.



Add Rules

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

☐ Source Zone

+
-

☐ Destination Zone

+
-

☐ Source Site Name

+
-

☐ Destination Site Name

+
-

+ New Zone

+ New Zone

☐ Source Address

+
-

☐ Destination Address

+
-

+ New Address Group
+ New Address

+ New Address Group
+ New Address

☐ Source Address Negate

☐ Destination Address Negate

Routing Instance







--Select--

Egress Routing Instance

--Select--

OK

Cancel

Field	Description
Source Zone	Source zones to which to apply the rule. The rule applies to traffic received from any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Destination Zone	Destination zones to which to apply the rule. The rule applies to traffic sent to any interface in the zone. Click the  Add icon to add zones. Click + New Zone to create a new zone.
Source Site Name	Source sites to which to apply the rule. Click the  Add icon to add sites.
Destination Site Name	Destination sites to which to apply the rule. Click the  Add icon to add sites.
Source Address	Source addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Source Address Negate	Select to apply the rule to any source addresses except the ones in the Source Address field.
Destination Address	Destination addresses to which to apply the rule. Click the  Add icon to add addresses. Click + New Address Group to create a new address group. Click + New Address to create a new address.
Destination Address Negate	Select to apply the rule to any destination addresses except the ones in the Destination Address field.
Routing Instance	Select the ingress routing instance to which to apply the rule.
Egress Routing Instance	Select the egress routing instance to which to apply the rule.

24. Click OK.

25. Select the Enforce tab, and enter information for the following fields.

Field	Description
Ingress	Click to mirror ingress traffic on the VOS device. <i>Default: Disabled</i>
Egress	Click to mirror the egress traffic on the VOS device. <i>Default: Disabled</i>
Mirror Interface	Select the interface on which to mirror the traffic.
Packet Count Per Flow	Enter the number of packets per flow to be mirrored.  <i>Range: 0 through 4294967295</i> <i>Default: None</i>

26. Select the Headers/Schedule, Applications/URL, and Users/Groups tabs and configure any necessary information.
27. Click OK.

## Configure Flow Mirroring over an IPsec Tunnel Using the CLI

1. Configure an IPsec tunnel interface to use for flow mirroring:

```
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/2 enable true
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/2 mirror-interface
admin@SDWAN-Branch1-cli(config)% set interfaces tvi-0/2 unit 0 enable true
```

2. Enable the traffic-mirroring service on the VOS device, and add TDF service in an available service node group. Doing this introduces flow mirroring as a new service in the TDF service set.

```
admin@Branch1-cli(config)% set service-node-groups default-sng services tdf
```

3. Configure a traffic-monitoring policy rule in an organization service:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
policy-name rules rule-name
```

4. Create policy match criteria for the packets to mirror on the mirror interface:

```
admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies
```

| **example-policy1 rules example-rule1 match**

5. Create policy action criteria to define the action to take when packets match the match criteria:

| **admin@Branch5-cli(config)% set orgs org-services example-org-name1 traffic-mirroring policies example-policy1 rules example-rule1 set**

---

## Verify Flow-Mirroring Operation

To verify flow-mirroring operation, view information about the mirrored ingress and egress packets:

```
admin@VOS# show debug vsf nfp module stats brief
ID Module Input   Input   Output  Output  Data   Data
          Packet Drop    Packet Drop    Hold
-----
30 mirror 4097    0       2063    0       0      0
```

---

## Supported Software Information

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

- Releases 21.2.1 and later support configuring rule order for traffic mirroring policy rules for Ethernet interfaces, GRE tunnels, and IPsec tunnels.

---

## Additional Information

[Configure Interfaces](#)