
Configure Firewalls



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

An interface facilitates the entry of traffic into a network and the exit of traffic from a network. A Versa Operating System™ (VOS™) firewall provides a mechanism to implement security policies on traffic that enters and exits the firewall using the interface. This article describes how to configure a VOS device to be a standalone firewall instance.

VOS Firewall Deployment Overview

You can deploy a VOS firewall in the following ways:

- Virtual-wire deployment
- Layer 2 deployment
- Layer 3 deployment
- Physical NICs
- Virtual NICs

Virtual-Wire Deployment

VOS devices support virtual wire, which is also referred to as bump in the wire. A virtual wire on a VOS device consists of two interfaces that are configured as an inline pair. If traffic flows through a physical wire and the wire is snipped, two ends are created on the wire where the cut is made. You plug these two ends of the physical wire into the two virtual interfaces configured on the VOS device, which allows the VOS device to emulate a virtual wire that connects both ends of the physical wire. The traffic received on either end of the physical wire is forwarded to the other interface of the virtual wire. You can apply firewall policies to virtual wire interfaces to enforce the security policies on all the traffic received at both the ends of the physical wire that terminates on the virtual wire interface. The traffic is forwarded on the physical wire only if the security policy allows the traffic to be forwarded.

Note that virtual-wire interfaces do not have IP addresses.

For interfaces that do not require VLAN support, create a single subinterface and set the VLAN tag value to 0.

Layer 2 Deployment

VOS devices support VLAN-based subinterfaces. An interface whose name start with vni is a VLAN-tagged traffic interface. Examples of interfaces names are vni-0 and vni-1.

For interfaces that require VLAN support, you create multiple subinterfaces, where each subinterface maps to an individual VLAN ID. For each tenant hosted on the VOS device, the traffic is identified using one or more subinterfaces. These subinterfaces map to the corresponding VLAN IDs.

Layer 3 Deployment

VOS devices support routed, or Layer 3, interfaces. The interface associated with each physical network interface (PNIC) or virtual network interface (VNIC) is configured with an IP address. Based on the routing configuration, the traffic from the tenant is forwarded to the interfaces on the VOS device. The VOS device supports several routing instances or virtual routing functions (VRFs). Each VRF is associated with one or more interfaces on the VOS device, and the VOS device supports static routing, BGP, and OSPF.

The traffic of a particular tenant enters a VOS device because the IP address of the routed interface is the next-hop address of the tenant traffic's final destination. You can apply firewall policies on the traffic entering a VOS device, and the traffic is routed to the next hop (based on routing configuration) only if the security policy allows the traffic to be forwarded.

You can install a VOS firewall device as a bare metal or a virtual machine (VM). The security policies are applied to the traffic that enters the firewall through physical or virtual interfaces. The VOS firewall recognizes VLAN tags for incoming traffic and adds the appropriate VLAN tags to the outbound traffic.

Physical NIC Deployment

You can deploy the VOS firewall on a bare-metal device to implement security protection for traffic from a PNIC. When you configure traffic on a PNIC, you may encounter one of the following scenarios:

- Non-VLAN Traffic—Traffic that is not tagged with VLAN and enters the firewall using PNIC is mapped to a single tenant.
- VLAN Traffic—Traffic tagged with VLAN is mapped to one or more tenant. The VOS device creates a unique subinterface for each VLAN. Use one or more VLAN to configure the traffic identification for each tenant hosted on the VOS device.

Virtual NIC Deployment

You can deploy the VOS firewall on a VM to implement security protection for traffic from a VNIC. You use a hypervisor, such as VMware ESXi or KVM, to create a VNIC and map it to the PNIC on which the hypervisor is running or to a specific VLAN for traffic tagged with VLAN that enter the network using PNIC.



The following are typical scenarios for configuring traffic on a VNIC:

- VLAN-mapped VNIC— If the VNIC is mapped by the hypervisor to a specific VLAN for the traffic that enters through the PNIC, then when the traffic enters the firewall through the VNIC, the VLAN is already stripped by the hypervisor. Therefore, all the traffic that enters through the VNIC is mapped to a single tenant. In this scenario, a single VNIC cannot support traffic from multiple tenants.
- PNIC-mapped VNIC with non-VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is not VLAN tagged, all traffic that enters through the VNIC is mapped to a single tenant.
- PNIC-mapped VNIC with VLAN traffic—When the hypervisor directly maps the VNIC to the PNIC without any VLAN stripping and if the traffic that enters the firewall through the VNIC is VLAN tagged, traffic that belongs to different VLANs is mapped to one or more tenants.
- You create a unique subinterface for each VLAN. You can configure the traffic identification using one or more VLANs for each tenant hosted on the VOS device.

Configure Physical and Virtual NICs

For VOS firewalls, you configure a single Layer 3 interface or multiple Layer 3 interfaces for untagged routed traffic, and then you connect the firewall to an adjacent device using a trunk to define a Layer 3 subinterface for traffic with a specific VLAN tag. For each Ethernet port that you configure as a Layer 3 interface, you can define an additional logical Layer 3 interface (as a subinterface) for each VLAN tag. The subinterface handles the traffic received by the port. In multitenant environments, you use untagged Layer 3 subinterfaces so that each tenant's traffic leaves the firewall without VLAN tags.

To configure a PNIC or VNIC and a subinterface:

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces > Ethernet in the left menu bar.
4. Click the  Add icon. In the Add Ethernet Interface popup window, enter information for the following fields.

Add Ethernet Interface

Ethernet
Aggregate Ethernet

Interface*
vni
0
1
Disable

Description

Tags

Promiscuous
Virtual Wire
Mirror Interface

PPPoE base Interface

MTU
1400

Bandwidth
Others

Uplink (Kbps)
5000
Downlink (Kbps)
5000

Auto Configuration
URI

Sub-interfaces
Aggregate Member

Unit
VLAN ID
IP Address/Mask
DHCP V4
DHCP V6
MTU

IPv4
IPv6

NO SUB-INTERFACES ADDED

OK
Cancel

Field	Description
Interface	Enter the vni interface port and slot numbers.
Disable	Click to not activate the interface after you configure it.
Description	Enter a description for this interface. It can be a text string up to 255 characters.
Tags	Enter tags for the Ethernet interface.
Promiscuous	Click to have the interface accept all data packet sent towards it.
Virtual Wire	Click if the interface is part of a virtual wire.
Mirror Interface	Click to create a copy of the interface.
PPPoE Data Interface	Click to have the interface act as a Point-to-Point Protocol over Ethernet (PPPoE) interface. In a PPPoE session, the device encapsulates each PPP frame in an Ethernet frame and transports the frames over an Ethernet loop.
MTU	Enter the maximum transmission unit size, in bytes, of the largest protocol data unit that the port can receive or transmit. <i>Range: 68 through 9000 bytes</i>
Bandwidth Tab	
◦ Uplink	Enter the link bandwidth for uploading data, in Kbps.
◦ Downlink	Enter the link bandwidth for downloading data, in Kbps.
◦ Autoconfiguration	Click to perform an automated test of the device's downlink and uplink transmission bandwidth.
◦ URI	Enter the URL of the website to use for autoconfiguration testing.
Others Tab	
◦ Link Speed	Enter the speed of the link.



◦ Link Mode	Select the mode to use on the link. For example, aut duplex.
-------------	--

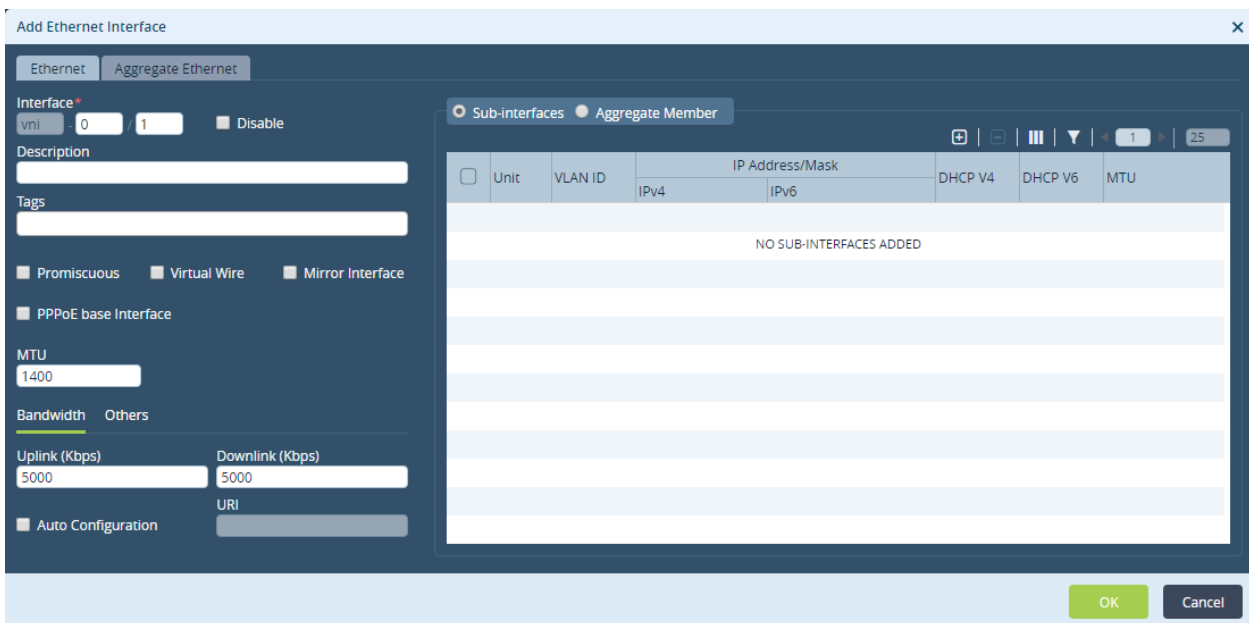
5. Select the Aggregate Ethernet tab, and create an aggregate Ethernet interface. For more information, see [Configure Aggregate Interfaces](#), below.
6. Click OK to add the interface to the PNIC/VNIC.


Configure VLAN-Based Subinterfaces

VLAN interfaces route Layer 3 VLAN traffic to non-VLAN destinations. You can define a VLAN interface for each Ethernet port that is configured as Layer 2 interface to allow VLAN traffic to be routed to Layer 3 destinations outside the VLAN.

To create a VLAN-based subinterface:

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces > Ethernet in the left menu bar.
4. Click the  Add icon to add an Ethernet interface. The Add Ethernet Interface popup window displays.



5. Select the Ethernet tab, click the Subinterfaces option, and click the  Add icon. The Add Subinterface popup window displays. Enter information for the following fields.

Add Sub-Interface

Unit*
103

Description

VLAN ID
103

MTU

☐ Disable

IPv4

IPv6

☒ Static Address

Static Address

☐ IP Address/Mask

78.78.78.2/4

☐ DHCP V4

Route Preference

Disable Broadcast Flag

Reachability Monitor

☐ Enable ICMP

Interval

Threshold

FQDN

Directed Broadcast

Static ARP

VRRP

Standby

Subnet Address/Mask*
78.78.78.2/4

Host IP Address*

MAC Address*


No Records to Display

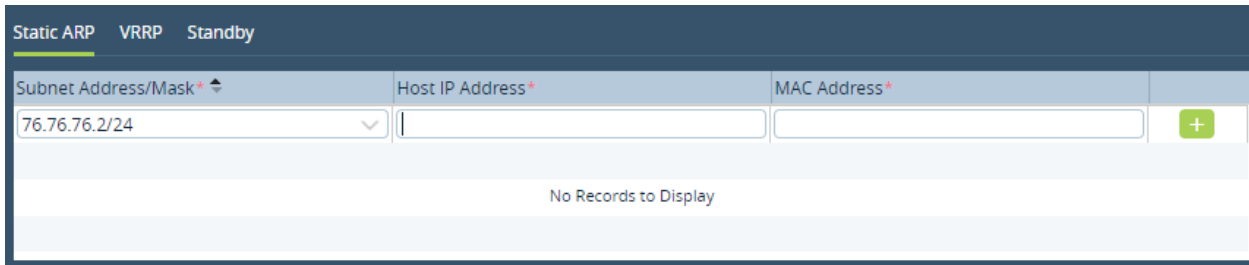
OK

Cancel


Field	Description
Unit	Enter the unit number of the subinterface. An interface can have up to 4095 subinterfaces.
VLAN ID	Enter the virtual LAN ID. <i>Range:</i> 0 through 4094
Disable	Click to not activate the subinterface after you configure it.
Description	Enter a description for the subinterface. It can be a maximum of 255 characters.
MTU	Enter the maximum transmission unit size, in bytes, of largest protocol data unit (PDU) that the port can receive or transmit. <i>Range:</i> 68 through 9000 bytes
IPv4 (Tab)	
◦ Static Address	Click to configure a static IPv4 address for the subinterface.
◦ DHCPv4	Click to use DHCPv4 to obtain an address for the subinterface.
◦ Route Preference	Enter the preference for the traffic route. A lower value indicates a higher preference.
◦ Disable Broadcast Flag	Click to disable broadcast on the subinterface's network.
◦ Reachability Monitor	Configure ICMP to monitor subinterface reachability.
◦ Enable ICMP	Click to enable ICMP on the subinterface.
◦ Interval	Enter the time interval after which ICMP reports error messages.
◦ Threshold	Enter the maximum number of ICMP error messages to report.
◦ FQDN	Enter the fully qualified domain name for the subnet.

◦ Directed Broadcast	Click to enable directed broadcast, which sends broadcast packets targeted at hosts in a specified subnet.
IPv6 (Tab)	
◦ Static Address	Click to configure a static IPv6 address for the subinterface.
◦ IPv6 Interface Mode	Select the IPv6 interface mode: <ul style="list-style-type: none"> ◦ Host ◦ Router
◦ FQDN	Enter the fully qualified domain name for the subnet.
◦ Delegated Prefix Pool	Enter the name and IP address of the delegated prefix pool.
◦ DHCPv6	Click to use DHCPv6 to obtain an address for the subinterface.

6. Select the Static ARP tab to configure a static MAC address for an IP address. Enter information for the following fields, and then click the  Add icon.



Field	Description
Subnet Address/Mask	Select the address of the subnet
Host IP Address	Enter an IP address that is within the subnet.
MAC Address	Enter the MAC address of the device.

7. Select the VRRP tab, and then click the  Add icon. The Add VRRP Group popup window displays. In this window you configure a VRRP primary and a VRRP secondary device in redundancy mode, which is a high

availability (HA) mode in which the VRRP secondary device takes over as the primary device when the primary device is down.

Add Sub-interface > Add VRRP Group

GeneralTrack

Group ID*

1

Address*

78.78.78.2/24

Priority

100

Inherit Configuration

Interface Name

vni-0/1.103

VRRP Group Id

Preempt Mode

Preempt

Advertisements Threshold

3

Warmup Interval (sec)

30

Virtual Address *

IP Address*

78.78.78.78

+

-

Fast Interval (msec)

1000


☒ Accept Data

OK

Cancel

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

Field	Description
Group ID	Enter the ID of the VRRP group.
Address	Enter the IP address of the VRRP group.
Priority	Assign a priority to the group. A higher priority indicates that the VRRP device is a primary device.
Inherit Configuration	Select to inherit the properties of another subinterface's configuration.
◦ Interface Name	Select the interface whose properties to inherit.
◦ VRRP Group ID	Select the VRRP group ID for the interface.
Preempt Mode	<p>Select the preemption mode:</p> <ul style="list-style-type: none"> ◦ Preempt—Secondary device takes over when the primary device is down. The original primary device takes over again when it recovers from the failure. ◦ No Preempt—Secondary device takes over when the primary device is down. The original primary device continues to function as the secondary device even after it recovers from the failure.
Advertisements Threshold	Enter the number of keep alive messages that are exchanged between the VRRP primary and secondary devices.
Warmup Interval	Enter how long the subinterface waits, in seconds to determine which VRRP device is the primary device and which is the secondary.
Virtual Address	Select the virtual address or addresses to assign to the VRRP device.
Fast Interval	(For VRRPv3.) Enter how long keepalive messages are exchanged between the primary and secondary devices, in milliseconds.
Accept Data	Click to have the subinterface accept data when it is received. Otherwise, the data is routed to another interface.

9. Select the Track tab, and enter information for the following fields, and then click the  Add icon where applicable.



Field	Description
HA Slave Priority Cost	Enter the backup priority of the VRRP instance. The backup priority must be less than the cost configured for the primary device.
Priority Hold Time	Enter the hold time. When this time expires, the secondary device takes over as the primary device.
Interface (Tab)	
◦ Name	Select the interface on which to configure VRRP.
◦ Priority Cost	Enter the priority cost of the interface. <i>Range: 1 through 254</i>
Routes (Tab)	
◦ Prefix	Enter the route prefix.
◦ Routing Instance	Select a routing instance
◦ Priority Cost	Enter the priority cost from 1 through 254.
Monitors (Tab)	
◦ Name	Select a monitor name.
◦ Priority Cost	Enter the priority cost. <i>Range: 1 through 254</i>

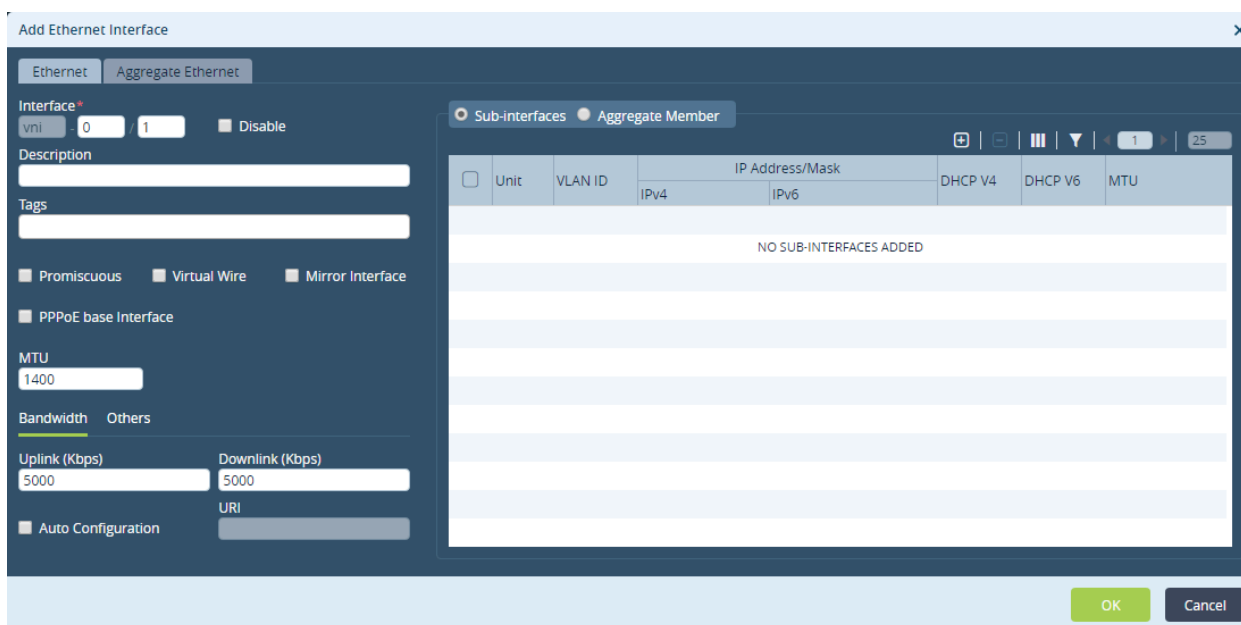
10. Click OK.

Configure Aggregate Interfaces

You can combine multiple interfaces to create a single logical aggregate Ethernet interface. The aggregate Ethernet interface handles all the traffic of the mapped interfaces. You can apply firewall policies to the aggregate interfaces to enforce security policies on traffic that belongs to any interface that is mapped to the aggregate interface.

To create an aggregate Ethernet interface:

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Interfaces > Ethernet in the left menu bar.
4. Click the  Add icon to add an Ethernet interface. The Add Ethernet Interface popup window displays.
5. In the Ethernet tab, click Aggregate Member and enter information for the following fields.



Field	Description
Interface	Select the name of the aggregate Ethernet interface.
LACP Priority	Enter the interface's LACP priority value. LACP combines the priority number with the router's MAC address to form the system ID, which is used during negotiation with other systems.

6. Select the Aggregate Ethernet tab, and enter information for the following fields.

Add Ethernet Interface

EthernetAggregate Ethernet

Interface*ae1System ID/MACDisable

Description

Tags

MTU1400Virtual WirePromiscuous

Sub-InterfacesLACP


UnitVLAN IDIP Address/MaskDHCP V4DHCP V6MTU

IPv4IPv6

NO SUB-INTERFACES ADDED

OKCancel

Field	Description
Interface	Enter the interface port number. Note that the name of the aggregate interface starts with ae.
System ID/MAC	Enter the MAC address of the interface.
Disable	Click to not activate the interface after you configure it.
Description	Enter a brief description of the interface.
Tags	Enter a keyword or phrase that allows you to filter the captive portal action. This is useful when you have many interfaces and want to view those that are tagged with a particular keyword.
MTU	Enter the maximum transmission unit size, in bytes, of largest protocol data unit the port can receive or transmit in bytes. <i>Range: 68 through 9000 bytes</i>
Virtual Wire	Click to have the interface become part of a virtual wire.
Promiscuous	Click to have the interface accept all the data packets that it receives.
Subinterface (Tab)	Select to create subinterfaces.
LACP (Tab)	Select to configure an LACP system priority, which you can configure on each router running LACP. LACP combines the system priority and the router MAC address of the router to create the LACP system ID, and it uses the system priority when negotiating with other systems.

- Click the Subinterfaces tab, and then click the  Add icon. In the Add Subinterfaces popup window, enter information for the fields. For more information, see [Configure VLAN-Based Subinterfaces](#), above.

Add Sub-Interface

Unit* VLAN ID ☐ Disable

Description MTU

IPv4 IPv6

☒ Static Address ☐ DHCP V4

Static Address

Static Address
<input type="checkbox"/> IP Address/Mask <input type="button" value="+"/> <input type="button" value="-"/>
<input type="checkbox"/> 78.78.78.2/4
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>

Route Preference ☐ Disable Broadcast Flag

Reachability Monitor

☐ Enable ICMP

FQDN ☐ Directed Broadcast

Static ARP VRRP Standby

Subnet Address/Mask*	Host IP Address*	MAC Address*	
<input type="text" value="78.78.78.2/4"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>
No Records to Display			

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

Sub-interfaces LACP

System Priority Max Links Periodicity

Mode

Field	Description
System Priority	Enter the LACP system priority value. LACP combines the priority number with the router's MAC address to form the system ID, which is used during negotiation with other systems.
Max Links	Enter the maximum number of LACP links.
Periodicity	Select the frequency for LACP
Mode	Select the LACP mode: <ul style="list-style-type: none"> ◦ Active ◦ Passive


9. Click OK.

Configure Tunnel Interfaces

Two VOS devices establish an IPsec tunnel and HA between them, and they use the tunnel for VPN traffic termination. The VOS devices support site-to-site VPN or SD-WAN traffic. An SD-WAN setup has multiple tunnel interfaces that connect a VOS branch device with a Controller node. You can apply firewall policies to the tunnel interfaces to enforce security policies on traffic that is extracted or decrypted from the tunnel after VPN termination.

Tunnel interface names start with tvi. Examples of tunnel interface names are tvi-0 and tvi-1.

To configure a tunnel interface:

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller node 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. The Add Tunnel Interface popup window displays.

Add Tunnel Interface

Tunnel
Pseudo Tunnel
PPPoE

Interface*

tvi
0
1

☐ Disable
☐ Mirror Interface

Description

MTU
1400

Mode
IPsec

Tunnel Type
Point-to-point IPsec tunnel

Sub-interfaces

	Unit	IP Address/Mask		DHCP V6
		IPv4	IPv6	
<input type="checkbox"/>	0			<input type="checkbox"/>
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

OK

Cancel


4. Select the Tunnel tab, and enter information for the following fields.

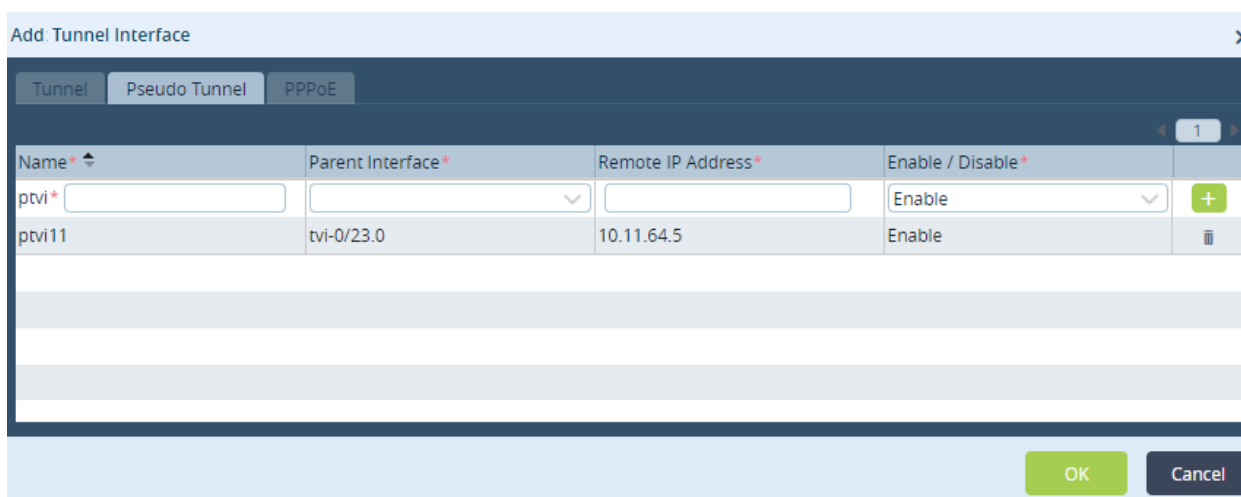
Field	Description
Interface	Enter the slot and port number for the tunnel interface. Note that a tunnel interface always has a tvi prefix.
Disable	Click to not activate the interface after you configure it.
Description	Enter a brief description of the tunnel interface.
MTU	Maximum transmission unit size, in bytes, of largest protocol data unit that the port can receive or transmit. <i>Range: 68 through 9000 bytes</i>
Mode	Select the tunnel interface mode: <ul style="list-style-type: none"> ◦ IPsec—For IPsec configurations. ◦ Redundancy—For HA configurations.
Tunnel Type	Select the tunnel type: <ul style="list-style-type: none"> ◦ Ethernet-over-GRE—Use to allow customers to leverage existing low-end residential gateways to provide mobility services to mobile nodes. ◦ Paired ◦ Point-to-multipoint clear-text SD-WAN tunnel. ◦ Point-to-multipoint GRE tunnel—Use GRE to send packets from one network to another over the internet or an insecure network. ◦ Point-to-multipoint IPsec tunnel—Use to protect site-to-site traffic between networks. ◦ Point-to-multipoint secure SD-WAN tunnel. ◦ Point-to-multipoint VXLAN tunnel—Virtual Extensible LAN (VXLAN) is a network virtualization technology. It addresses endpoints, which terminate VXLAN tunnels and may be either virtual or physical switch ports. These are known as VXLAN tunnel endpoints (VTEPs). ◦ Point-to-point GRE tunnel—Use to enable the IPsec configuration between a local Controller and a Controller in the cloud. ◦ Point-to-point IPsec tunnel ◦ Point-to-point IPv6 GRE tunnel

	<ul style="list-style-type: none"> ◦ PPPoE—Use with DSL services in which individual users connect to a DSL modem over Ethernet.
Subinterface	<p>Select a subinterface and enter values for the following parameters:</p> <ul style="list-style-type: none"> ◦ Unit—Unit number of the subinterface. Enter a value of 0 to disable VLAN ID. ◦ IP Address/Mask—IP address and subnet mask of the subinterface.

6. Click OK.

Configure a Pseudo-Tunnel Interface

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller node 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. The Add Tunnel Interface popup window displays.
4. Select the Tunnel tab, and enter information for the following fields.



Add Tunnel Interface

Tunnel Pseudo Tunnel PPPoE

Name *	Parent Interface *	Remote IP Address *	Enable / Disable *
ptvi*			Enable
ptvi11	tvi-0/23.0	10.11.64.5	Enable

OK Cancel

Field	Description
Name	Enter a name for the pseudo-tunnel interface. A pseudo-tunnel interface has the prefix ptvi.
Parent Interface	Select the parent interface for the pseudo-tunnel.
Remote IP Address	Enter the IP address of the remote Controller node.
Enable/Disable	<p>Select enable to activate the pseudo-tunnel after you configure it.</p> <p>Select disable to not activate the pseudo-tunnel after you configure it.</p>

- Click OK.



Configure a Virtual Wire

A virtual wire binds two Ethernet ports together, allowing transparent installation of a VOS firewall in the network with minimum configuration. A virtual wire accepts all traffic or traffic with selected VLAN tags. It does not provide switching or routing services.

The two virtual network interfaces (vni interfaces) that form a virtual wire must have identical subinterfaces.

When you configure a virtual wire, you do not need to change the configuration of neighboring network devices.

To create a virtual wire:

- In the Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a Controller node in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking  > Virtual Wires in the left menu bar.
- Click the  Add icon. The Add Virtual Wire popup window displays. Enter information for the following fields.

Field	Description
Name	Enter a name for the virtual wire.
Interface1	Select the first interface.
Interface2	Select the second interface.
Link-State Passthrough	Select to inform the second interface about the state of the first interface. For example, if you select this and the first interface is down, traffic must be sent through an alternate route to the second interface.
Multicast firewalling	Currently not supported.

5. Click OK.

Troubleshoot Firewalls

To troubleshoot firewall-related issues, issue the following commands:

- **show orgs org *tenant-name* statistics traffic**
- **show orgs org *tenant-name* statistics security-implicit**
- **show orgs org *tenant-name* sessions summary**
- **show orgs org *tenant-name* sessions brief**
- **show orgs org *tenant-name* sessions detail**
- **show orgs org-services *tenant-name* security dos-policies**
- **show orgs org-services *tenant-name* security access-policies**

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Interfaces](#)