Setting Up Virtual Switches

The following topics describe how to set up virtual switches in the Firepower System:

Virtual Switches

You can configure a 7000 or 8000 Series device in a Layer 2 deployment so that it provides packet switching between two or more networks. In a Layer 2 deployment, you can configure virtual switches to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets.

When you configure a virtual switch, the switch initially broadcasts packets through every available port on the switch. Over time, the switch uses tagged return traffic to learn which hosts reside on the networks connected to each port.

A virtual switch must contain two or more switched interfaces to handle traffic. For each virtual switch, traffic becomes limited to the set of ports configured as switched interfaces. For example, if you configure a virtual switch with four switched interfaces, packets sent in through one port for broadcast can only be sent out of the remaining three ports on the switch.

When you configure a physical switched interface, you must assign it to a virtual switch. You can also define additional logical switched interfaces on a physical port as needed. You can group multiple physical interfaces into a single logical switched interface called a link aggregation group (LAG). This single aggregate logical link provides higher bandwidth, redundancy, and load-balancing between two endpoints.

Caution If a Layer 2 deployment fails for any reason, the device no longer passes traffic.

Switched Interface Configuration

You can set up switched interfaces to have either physical or logical configurations. You can configure physical switched interfaces for handling untagged VLAN traffic. You can also create logical switched interfaces for handling traffic with designated VLAN tags.

In a Layer 2 deployment, the system drops any traffic received on an external physical interface that does not have a switched interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical switched interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical switched interface, it also drops the packet.

The system handles traffic that has been received with VLAN tags on switched interfaces by stripping the outermost VLAN tag on ingress before any rules evaluation or forwarding decisions. Packets leaving the device through a VLAN-tagged logical switched interface are encapsulated with the associated VLAN tag on egress.

Note that if you change the parent physical interface to inline or passive, the system deletes all the associated logical interfaces.

Switched Interface Configuration Notes

You can configure one or more physical ports on a managed device as switched interfaces. You must assign a physical switched interface to a virtual switch before it can handle traffic. You can configure link mode settings and MDI/MDIX settings only for copper interfaces.

Note Interfaces on 8000 Series appliances do not support half-duplex options.

For each physical switched interface, you can add multiple logical switched interfaces. You must associate each logical interface with a VLAN tag to handle traffic received by the physical interface with that specific tag. You must assign a logical switched interface to a virtual switch to handle traffic.

When configuring a switched interface, the range within which you can set the MTU can vary depending on the Firepower System device model and interface type.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

To edit an existing logical switched interface, click the edit icon () next to the interface.

When you delete a logical switched interface, you remove it from the physical interface where it resides, as well as the virtual switch and security zone it is associated with.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Configuring Physical Switched Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to configure the switched interface, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Next to the interface you want to configure as a switched interface, click **Edit** ( ).

Step 4 Click the **Switched** tab.

Step 5 If you want to associate the switched interface with a security zone, do one of the following:

- Choose an existing security zone from the **Security Zone** drop-down list.
- Choose **New** to add a new security zone; see Creating Security Zone and Interface Group Objects.

Step 6 If you want to associate the switched interface with a virtual switch, do one of the following:

- Choose an existing virtual switch from the **Virtual Switch** drop-down list.
- Choose **New** to add a new virtual switch; see Adding Virtual Switches, on page 7.

Step 7 Check the **Enabled** check box to allow the switched interface to handle traffic.

Note If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.

Step 8 From the **Mode** drop-down list, choose an option to designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to auto negotiate speed and duplex settings.

Mode settings are available only for copper interfaces.

Interfaces on 8000 Series appliances do not support half-duplex options.

Step 9 From the **MDI/MDIX** drop-down list, choose an option to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

By default, MDI/MDIX is set to Auto-MDIX, which automatically handles switching between MDI and MDIX to attain link.

Step 10 In the **MTU** field, enter a maximum transmission unit (MTU), which designates the largest size packet allowed.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Adding Logical Switched Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to add the switched interface, click the edit icon ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Choose **Add Logical Interface** from the **Add** drop-down menu.

Step 4 Click **Switched**.

Step 5 From the **Interface** drop-down list, choose the physical interface that will receive the VLAN-tagged traffic.

Step 6 In the **VLAN Tag** field, enter a tag value that gets assigned to inbound and outbound traffic on this interface.

The tag value can be any integer from 1 to 4094.

Step 7 If you want to associate the switched interface with a security zone, do one of the following:

- Choose an existing security zone from the **Security Zone** drop-down list.
- Choose **New** to add a new security zone; see Creating Security Zone and Interface Group Objects.

Step 8 If you want to associate the switched interface with a virtual switch, do one of the following:

- Choose an existing virtual switch from the **Virtual Switch** drop-down list.
- Choose **New** to add a new virtual switch; see Adding Virtual Switches, on page 7.

Step 9 Check the **Enabled** check box to allow the switched interface to handle traffic.

If you clear the check box, the interface becomes disabled and administratively taken down. If you disable a physical interface, you also disable all of the logical interfaces associated with it.

Step 10 In the **MTU** field, enter a maximum transmission unit (MTU), which designates the largest size packet allowed.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios

Deleting Logical Switched Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the managed device that contains the switched interface you want to delete, click the edit icon ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Next to the logical switched interface you want to delete, click the delete icon ( ).

Step 4 When prompted, confirm that you want to delete the interface.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Virtual Switch Configuration

Before you can use switched interfaces in a Layer 2 deployment, you must configure virtual switches and assign switched interfaces to them. A virtual switch is a group of switched interfaces that process inbound and outbound traffic through your network.

Virtual Switch Configuration Notes

You can add virtual switches from the Virtual Switches tab of the Device Management page. The Virtual Switches tab displays a list of all the virtual switches you have configured on a device. The page includes summary information about each switch.

Table 1: Virtual Switches Table View Fields

Field	Description
Name	The name of the virtual switch.
Interfaces	All switched interfaces that are assigned to the virtual switch. Interfaces that you have disabled from the Interfaces tab are not available.
Hybrid Interface	The optionally configured hybrid interface that ties the virtual switch to a virtual router.
Unicast Packets	Unicast packet statistics for the virtual switch, including: • Unicast packets received • Unicast packets forwarded (excludes drops by host) • Unicast packets unintentionally dropped
Broadcast Packets	Broadcast packet statistics for the virtual switch, including: • Broadcast packets received • Broadcast packets forwarded • Broadcast packets unintentionally dropped

You can also add switches as you configure switched interfaces. You can assign only switched interfaces to a virtual switch. If you want to create a virtual switch before you configure the switched interfaces on your managed devices, you can create an empty virtual switch and add interfaces to it later.

Tip To edit an existing virtual switch, click the edit icon ( ) next to the switch.

Adding Virtual Switches

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device where you want to add the virtual switch, click **Edit** ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Switches** tab.

Step 4 Click **Add Virtual Switch**.

Step 5 Enter a name in the **Name** field.

Step 6 From the **Available** list, choose one or more switched interfaces to add to the virtual switch.

Tip Interfaces that you have disabled from the Interfaces tab are not available; disabling an interface after you add it removes it from the configuration.

Step 7 Click **Add**.

Step 8 If you want to tie the virtual switch to a virtual router, choose a hybrid interface from the **Hybrid Interface** drop-down list.

Step 9 Optionally, configure advanced settings for the switch; see Advanced Virtual Switch Settings, on page 7

Step 10 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Logical Hybrid Interfaces

Advanced Virtual Switch Settings

Adding Static MAC Entries

Over time, a virtual switch learns MAC addresses by tagging return traffic from the network. You can manually add a static MAC entry, which designates that a MAC address resides on a specific port. Regardless of whether you ever receive traffic from that port, the MAC address remains static in the table. You can specify one or more static MAC addresses for each virtual switch.

Enabling Spanning Tree Protocol (STP) and Dropping Bridge Protocol Data Units (BPDU)

STP is a network protocol used to prevent network loops. BPDUs are exchanged through the network, carrying information about network bridges. The protocol uses BPDUs to identify and select the fastest network links, if there are redundant links in the network. If a network link fails, Spanning Tree fails over to an existing alternate link.

Note Cisco strongly recommends that you enable STP when configuring a virtual switch that you plan to deploy in a 7000 or 8000 Series device high-availability pair. Only enable STP if your virtual switch switches traffic between multiple network interfaces.

If your virtual switch routes traffic between VLANs, similar to a router on a stick, BPDUs enter and exit the device through different logical switched interfaces, but the same physical switched interface. As a result, STP identifies the device as a redundant network loop, which can cause issues in certain Layer 2 deployments. To prevent this, you can configure the virtual switch at the domain level to have the device drop BPDUs when monitoring traffic. You can only drop BPDUs if you disable STP.

Note Drop BPDUs only if your virtual swtich routes traffic between VLANs on a single physical interface.

Enabling Strict TCP Enforcement

To maximize TCP security, you can enable strict enforcement, which blocks connections where the three-way handshake was not completed. Strict enforcement also blocks:

- non-SYN TCP packets for connections where the three-way handshake was not completed
- non-SYN/RST packets from the initiator on a TCP connection before the responder sends the SYN-ACK
- non-SYN-ACK/RST packets from the responder on a TCP connection after the SYN but before the session is established
- SYN packets on an established TCP connection from either the initiator or the responder

Note that if you associate the virtual switch with a logical hybrid interface, the switch uses the same strict TCP enforcement setting as the virtual router associated with the logical hybrid interface. You cannot specify strict TCP enforcement on the switch in this case.

Configuring Advanced Virtual Switch Settings

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that contains the virtual switch you want to edit, click the edit icon ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Switches** tab.

Step 4 Next to the virtual switch that you want to edit, click the edit icon ( ).

Step 5 Click the **Advanced** tab.

Step 6 To add a static MAC entry, click **Add**.

Step 7 In the **MAC Address** field, enter the address using the standard format of six groups of two hexadecimal digits separated by colons (for example, 01:23:45:67:89:AB).

Note Broadcast addresses (00:00:00:00:00:00 and FF:FF:FF:FF:FF:FF) cannot be added as static MAC addresses.

Step 8 From the **Interface** drop-down list, choose the interface where you want to assign the MAC address.

Step 9 Click **OK**.

Step 10 If you want to enable the Spanning Tree Protocol, check the **Enable Spanning Tree Protocol** check box.

Step 11 If you want to enable strict TCP enforcement, check the **Strict TCP Enforcement** check box.

If you associate the virtual switch with a logical hybrid interface, this option does not appear and the switch uses the same setting as the virtual router associated with the logical hybrid interface.

Step 12 If you want to drop BPDUs at the domain level, check the **Drop BPDUs** check box.

Step 13 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Deleting Virtual Switches

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

When you delete a virtual switch, any switched interfaces assigned to the switch become available for inclusion in another switch.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the managed device that contains the virtual switch you want to delete, click the edit icon ( ).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Switches** tab.

Step 4 Next to the virtual switch that you want to delete, click the delete icon ( ).

Step 5 When prompted, confirm that you want to delete the virtual switch.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.