



# CHAPTER 9

## Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance

---

This chapter describes how to configure the switch ports and VLAN interfaces of the ASA 5505 adaptive security appliance.



### Note

---

To configure interfaces of other models, see [Chapter 7, “Configuring Interfaces in Single Mode.”](#)

---

This chapter includes the following sections:

- [Interface Overview, page 9-1](#)
- [Configuring VLAN Interfaces, page 9-5](#)
- [Configuring Switch Ports, page 9-11](#)

## Interface Overview

This section describes the ports and interfaces of the ASA 5505 adaptive security appliance, and includes the following topics:

- [Understanding ASA 5505 Ports and Interfaces, page 9-2](#)
- [Maximum Active VLAN Interfaces for Your License, page 9-2](#)
- [Default Interface Configuration, page 9-4](#)
- [VLAN MAC Addresses, page 9-4](#)
- [Power Over Ethernet, page 9-4](#)
- [Monitoring Traffic Using SPAN, page 9-4](#)
- [Security Level Overview, page 9-5](#)

## Understanding ASA 5505 Ports and Interfaces

The ASA 5505 adaptive security appliance supports a built-in switch. There are two kinds of ports and interfaces that you need to configure:

- Physical switch ports—The adaptive security appliance has eight Fast Ethernet switch ports that forward traffic at Layer 2, using the switching function in hardware. Two of these ports are PoE ports. See the [“For same security interfaces, you can configure established commands for both directions.” section on page 9-5](#) for more information. You can connect these interfaces directly to user equipment such as PCs, IP phones, or a DSL modem. Or you can connect to another switch.
- Logical VLAN interfaces—In routed mode, these interfaces forward traffic between VLAN networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces forward traffic between the VLANs on the same network at Layer 2, using the configured security policy to apply firewall services. See the [“Maximum Active VLAN Interfaces for Your License” section](#) for more information about the maximum VLAN interfaces. VLAN interfaces let you divide your equipment into separate VLANs, for example, home, business, and Internet VLANs.

To segregate the switch ports into separate VLANs, you assign each switch port to a VLAN interface. Switch ports on the same VLAN can communicate with each other using hardware switching. But when a switch port on VLAN 1 wants to communicate with a switch port on VLAN 2, then the adaptive security appliance applies the security policy to the traffic and routes or bridges between the two VLANs.

**Note**

---

Subinterfaces are not available for the ASA 5505 adaptive security appliance.

---

## Maximum Active VLAN Interfaces for Your License

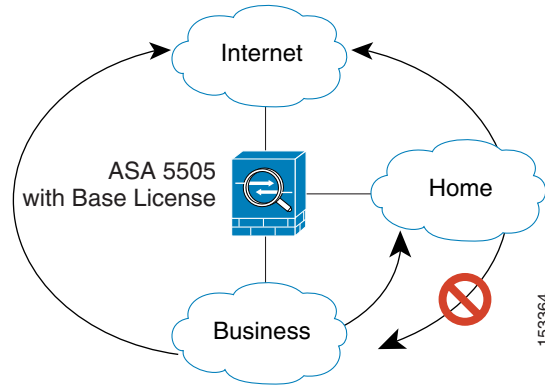
In transparent firewall mode, you can configure two active VLANs in the Base license and three active VLANs in the Security Plus license, one of which must be for failover.

In routed mode, you can configure up to three active VLANs with the Base license, and up to 20 active VLANs with the Security Plus license.

An active VLAN is a VLAN with a **nameif** command configured.

With the Base license, the third VLAN can only be configured to initiate traffic to one other VLAN. See [Figure 9-1](#) for an example network where the Home VLAN can communicate with the Internet, but cannot initiate contact with Business.

**Figure 9-1** ASA 5505 Adaptive Security Appliance with Base License



With the Security Plus license, you can configure 20 VLAN interfaces. You can configure trunk ports to accommodate multiple VLANs per port.

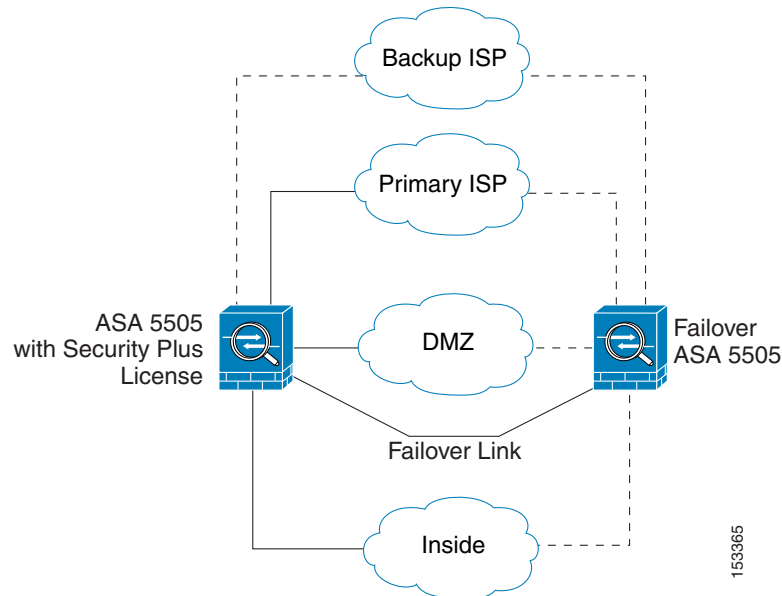


**Note**

The ASA 5505 adaptive security appliance supports Active/Standby failover, but not Stateful failover.

See [Figure 9-2](#) for an example network.

**Figure 9-2** ASA 5505 Adaptive Security Appliance with Security Plus License



## Default Interface Configuration

If your adaptive security appliance includes the default factory configuration, your interfaces are configured as follows:

- The outside interface (security level 0) is VLAN 2.  
Ethernet0/0 is assigned to VLAN 2 and is enabled.  
The VLAN 2 IP address is obtained from the DHCP server.
- The inside interface (security level 100) is VLAN 1  
Ethernet 0/1 through Ethernet 0/7 are assigned to VLAN 1 and is enabled.  
VLAN 1 has IP address 192.168.1.1.

Restore the default factory configuration using the **configure factory-default** command.

Use the procedures in this chapter to modify the default configuration, for example, to add VLAN interfaces.

If you do not have a factory default configuration, all switch ports are in VLAN 1, but no other parameters are configured.

## VLAN MAC Addresses

In routed firewall mode, all VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses.

In transparent firewall mode, each VLAN has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses.

## Power Over Ethernet

Ethernet 0/6 and Ethernet 0/7 support PoE for devices such as IP phones or wireless access points. If you install a non-PoE device or do not connect to these switch ports, the adaptive security appliance does not supply power to the switch ports.

If you shut down the switch port from the [Edit Switch Port](#) dialog box, you disable power to the device. Power is restored when you enter reenable it.

To view the status of PoE switch ports, including the type of device connected (Cisco or IEEE 802.3af), use the **show power inline** command.

## Monitoring Traffic Using SPAN

If you want to monitor traffic that enters or exits one or more switch ports, you can enable SPAN, also known as switch port monitoring. The port for which you enable SPAN (called the destination port) receives a copy of every packet transmitted or received on a specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor all traffic; without SPAN, you would have to attach a sniffer to every port you want to monitor. You can only enable SPAN for one destination port.

You can only enable SPAN monitoring using the Command Line Interface tool by entering the **switchport monitor** command. See the **switchport monitor** command in the *Cisco Security Appliance Command Reference* for more information.

## Security Level Overview

Each VLAN interface must have a security level in the range 0 to 100 (from lowest to highest). For example, you should assign your most secure network, such as the inside business network, to level 100. The outside network connected to the Internet can be level 0. Other networks, such as a home network can be in between. You can assign interfaces to the same security level.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

For some security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For some security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - SQL\*Net inspection engine—If a control connection for the SQL\*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the adaptive security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For some security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for some security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For some security interfaces, you can configure **established** commands for both directions.

## Configuring VLAN Interfaces

For information about how many VLANs you can configure, see the [“Maximum Active VLAN Interfaces for Your License”](#) section on page 9-2.



### Note

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover communications. See [Chapter 15, “High Availability,”](#) to configure the failover link.

If you enabled Easy VPN, you cannot add or delete VLAN interfaces, nor can you edit the security level or interface name. We suggest that you finalize your interface configuration before you enable Easy VPN.

This section includes the following topics:

- [Interfaces > Interfaces, page 9-6](#)
- [Add/Edit Interface > General, page 9-8](#)
- [Add/Edit Interface > Advanced, page 9-10](#)

## Interfaces > Interfaces

The Interfaces tab displays configured VLAN interfaces. You can add or delete VLAN interfaces, and also enable communication between interfaces on the same security level or enable traffic to enter and exit the same interface.

Transparent firewall mode allows only two interfaces to pass through traffic.

### Fields

- Name—Displays the interface name.
- Switch Ports—Shows the switch ports assigned to this VLAN interface.
- Enabled—Indicates if the interface is enabled, Yes or No.
- Security Level—Displays the interface security level between 0 and 100. By default, the security level is 0.
- IP Address—Displays the IP address, or in transparent mode, the word “native.” Transparent mode interfaces do not use IP addresses. To set the IP address for the context or the security appliance, see the [Management IP Address](#) pane.
- Subnet Mask—For routed mode only. Displays the subnet mask.
- Restrict Traffic Flow—Shows if this interface is restricted from initiating contact to another VLAN. With the Base license, you can only configure a third VLAN if you use this option to limit it.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the Restrict Traffic Flow option on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

If you already have two VLAN interfaces configured with a name, be sure to enable the Restrict Traffic Flow option before you name the third interface; the adaptive security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance.



**Note** If you upgrade to the Security Plus license, you can remove this option and achieve full functionality for this interface. If you leave this option enabled, this interface continues to be limited even after upgrading.

- Backup Interface—Shows the backup ISP interface for this interface. If this interface fails, the backup interface takes over.

The backup interface does not pass through traffic unless the default route through the primary interface fails. This option is useful for Easy VPN; when the backup interface becomes the primary, the security appliance moves the VPN rules to the new primary interface.

To ensure that traffic can pass over the backup interface in case the primary fails, be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. To configure dual ISP support, see the [“Static Route Tracking” section on page 11-41](#).

- **VLAN**—Shows the VLAN ID for this interface.
- **Management Only**—Indicates if the interface allows traffic to the security appliance or for management purposes only.
- **MTU**—Displays the MTU. By default, the MTU is 1500.
- **Active MAC Address**—Shows the active MAC address, if you assigned one manually on the [Add/Edit Interface > Advanced](#) tab.
- **Standby MAC Address**—Shows the standby MAC address (for failover), if you assigned one manually.
- **Description**—Displays a description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description.
- **Add**—Adds an interface. If you enabled Easy VPN, you cannot add VLAN interfaces.
- **Edit**—Edits the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot edit the interface in this pane. If you enabled Easy VPN, you cannot edit the security level or interface name.
- **Delete**—Deletes the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot delete the interface in this pane. If you enabled Easy VPN, you cannot delete VLAN interfaces.
- **Enable traffic between two or more interfaces which are configured with same security levels**—Enables communication between interfaces on the same security level. If you enable same security interface communication, you can still configure interfaces at different security levels as usual.
- **Enable traffic between two or more hosts connected to the same interface**—Enables traffic to enter and exit the same interface.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Add/Edit Interface > General

The Add/Edit Interface > General tab lets you add or edit a VLAN interface.

If you intend to use an interface for failover, do not configure the interface in this dialog box; instead, use the [Failover: Setup](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored.

If you enabled Easy VPN, you cannot edit the security level or interface name. We suggest that you finalize your interface configuration before you enable Easy VPN.

After you assign the interface as the failover link or state link, you cannot edit or delete the interface from the Interfaces pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

### Fields

- Switch Ports—Assigns switch ports to this VLAN interface.
  - Available Switch Ports—Lists all switch ports, even if they are currently assigned to a different interface.
  - Selected Switch Ports—Lists the switch ports assigned to this interface.
  - Add—Adds a selected switch port to the interface. You see the following message:
 

*“switchport is associated with name interface. Adding it to this interface, will remove it from name interface. Do you want to continue?”*

 Click **OK** to add the switch port.
  - Remove—Removes a switch port from an interface. Because the default VLAN interface for switch ports is VLAN 1, removing a switch port from an interface essentially just reassigns that switch port to VLAN 1.
- Enable Interface—Enables this interface to pass traffic. In addition to this setting, you need to set an IP address (for routed mode) and a name before traffic can pass according to your security policy.
- Dedicate this interface to management only—Sets the interface to accept traffic to the security appliance only, and not through traffic. You cannot set a primary or backup ISP interface to be management only.
- Interface Name—Sets an interface name up to 48 characters in length.
- Security Level—Sets the security level between 0 (lowest) and 100 (highest). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.
- IP Address—For routed mode only, sets the IP address.
  - Use Static IP—Manually sets the IP address.
    - IP address—Sets the IP address.
    - Subnet Mask—Sets the subnet mask.
  - Obtain Address via DHCP—Dynamically sets the IP address using DHCP.
    - Obtain Default Route Using DHCP—Obtains a default route from the DHCP server so that you do not need to configure a default static route.
    - Renew DHCP Lease—Renews the DHCP lease.

**Retry Count**—Sets the number of times between 4 and 16 that the security appliance resends a DHCP request if it does not receive a reply after the first attempt. The total number of attempts is the retry count plus the first attempt. For example, if you set the retry count to 4, the security appliance sends up to 5 DHCP requests.

**DHCP Learned Route Metric**—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.

**Enable tracking**—Check this checkbox to enable route tracking for DHCP-learned routes.




---

**Note** Route tracking is only available in single, routed mode.

---

**Track ID**—A unique identifier for the route tracking process. Valid values are from 1 to 500.

**Track IP Address**—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.

**SLA ID**—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.

**Monitor Options**—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.

- Use PPPoE—Dynamically sets the IP address using PPPoE.

**Group Name**—Specify a group name.

**PPPoE Username**—Specify the username provided by your ISP.

**PPPoE Password**—Specify the password provided by your ISP.

**Confirm Password**—Specify the password provided by your ISP.

**PPP Authentication**—Select either PAP, CHAP, or MSCHAP. PAP passes cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

**Store Username and Password in Local Flash**—Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

**IP Address and Route Settings**—displays the PPPoE IP Address and Route Settings dialog where you can choose addressing and tracking options. See the [“PPPoE IP Address and Route Settings” section on page 7-9](#).

- **Description**—Sets an optional description up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

**Add/Edit Interface > Advanced**

The Add/Edit Interface > Advanced tab lets you set the MTU, VLAN ID, MAC addresses, and other options.

**Fields**

- **MTU**—Sets the MTU from 300 to 65,535 bytes. The default is 1500 bytes. For multiple context mode, set the MTU in the context configuration.
- **VLAN ID**—Sets the VLAN ID for this interface between 1 and 4090. If you do not want to assign the VLAN ID, ASDM assigns one for you randomly.
- **Mac Address Cloning**—Manually assigns MAC addresses.

By default in routed mode, all VLANs use the same MAC address. In transparent mode, the VLANs use unique MAC addresses. You might want to set unique VLANs or change the generated VLANs if your switch requires it, or for access control purposes.

- **Active Mac Address**—Assigns a MAC address to the interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.
- **Standby Mac Address**—For use with failover, set the Standby Mac Address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.
- **Block Traffic**—Restrict this VLAN interface from initiating contact to another VLAN.

With the Base license, you can only configure a third VLAN if you use this option to limit it.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside business network, and a third VLAN assigned to your home network. The home network does not need to access the business network, so you can use the Restrict Traffic Flow option on the home VLAN; the business network can access the home network, but the home network cannot access the business network.

If you already have two VLAN interfaces configured with a name, be sure to enable the Restrict Traffic Flow option before you name the third interface; the adaptive security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance and will not allow you to configure one.

**Note**

If you upgrade to the Security Plus license, you can remove this option and achieve full functionality for this interface. If you leave this option enabled, this interface continues to be limited even after upgrading.

- Block Traffic from this Interface to—Choose a VLAN ID in the list.
- Select Backup Interface—Shows the backup ISP interface for this interface. If this interface fails, the backup interface takes over. The backup interface does not pass through traffic unless the default route through the primary interface fails. This option is useful for Easy VPN; when the backup interface becomes the primary, the security appliance moves the VPN rules to the new primary interface.

To ensure that traffic can pass over the backup interface in case the primary fails, be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. To configure dual ISP support, see the “[Static Route Tracking](#)” section on page 11-41.

- Backup Interface—Choose a VLAN ID in the list.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Configuring Switch Ports

This section describes how to configure switch ports, and includes the following topics:

- [Interfaces > Switch Ports](#), page 9-11
- [Edit Switch Port](#), page 9-12



### Caution

The ASA 5505 adaptive security appliance does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the adaptive security appliance does not end up in a network loop.

## Interfaces > Switch Ports

The Switch Ports tab displays the switch port parameters.

### Fields

- Switch Port—Lists the switch ports in the security appliance.
- Enabled—Shows if the switch port is enabled, Yes or No.
- Associated VLANs—Lists the VLAN interfaces to which the switch port is assigned. A trunk switch port can be associated with multiple VLANs.
- Associated Interface Names—Lists the VLAN interface names.

- **Mode**—The mode, Access or Trunk. Access ports can be assigned to one VLAN. Trunk ports can carry multiple VLANs using 802.1Q tagging. Trunk mode is available only with the Security Plus license.
- **Protected**—Shows if this switch port is protected, Yes or No. This option prevents the switch port from communicating with other protected switch ports on the same VLAN. You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the Protected option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
- **Edit**—Edits the switch port.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

## Edit Switch Port

The Edit Switch Port dialog box lets you configure the mode, assign a switch port to a VLAN, and set the Protected option.

### Fields

- **Switch Port**—*Display only*. Shows the selected switch port ID.
- **Enable Switch Port**—Enables this switch port.
- **Mode and VLAN IDs**—Sets the mode and the assigned VLANs.
  - **Access VLAN ID**—Sets the mode to access mode. Enter the VLAN ID to which you want to assign this switch port. By default, the VLAN ID is derived from the VLAN interface configuration in [Interfaces > Interfaces](#). You can change the VLAN assignment in this dialog box. Be sure to apply the change to update the [Interfaces > Interfaces](#) tab with the new information. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN from the [Interfaces > Interfaces](#) tab and specify the switch port in the [Add/Edit Interface > General](#) tab rather than specifying it in this dialog box; in either case, you need to add the VLAN on the [Interfaces > Interfaces](#) tab and assign the switch port to it.
  - **Trunk VLAN IDs**—Sets the mode to trunk mode using 802.1Q tagging. Trunk mode is available only with the Security Plus license. Enter the VLAN IDs to which you want to assign this switch port, separated by commas. Trunk ports do not support untagged packets; there is no native VLAN support, and the adaptive security appliance drops all packets that do not contain a tag specified in this command. If the VLANs are already in your configuration, after you apply the change, the [Interfaces > Interfaces](#) tab shows this switch port added to each VLAN. If you want to specify a VLAN that has not yet been added, we suggest you add the VLAN from the

[Interfaces > Interfaces](#) tab and specify the switch port in the [Add/Edit Interface > General](#) tab rather than specifying it in this dialog box; in either case, you need to add the VLAN on the [Interfaces > Interfaces](#) tab and assign the switch port to it.

- **Isolated**—This option prevents the switch port from communicating with other protected switch ports on the same VLAN. You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the Protected option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.
  - **Isolated**—Sets this switch port as a protected port.
- **Duplex**—Lists the duplex options for the interface, including Full, Half, or Auto. The Auto setting is the default. If you set the duplex to anything other than Auto on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.
- **Speed**—The Auto setting is the default. If you set the speed to anything other than Auto on PoE ports Ethernet 0/6 or 0/7, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power. The default Auto setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to Auto to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

