Quick Start Guide

Cisco ASA Services Module

Related Documentation

To access all documents related to this product, go to:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

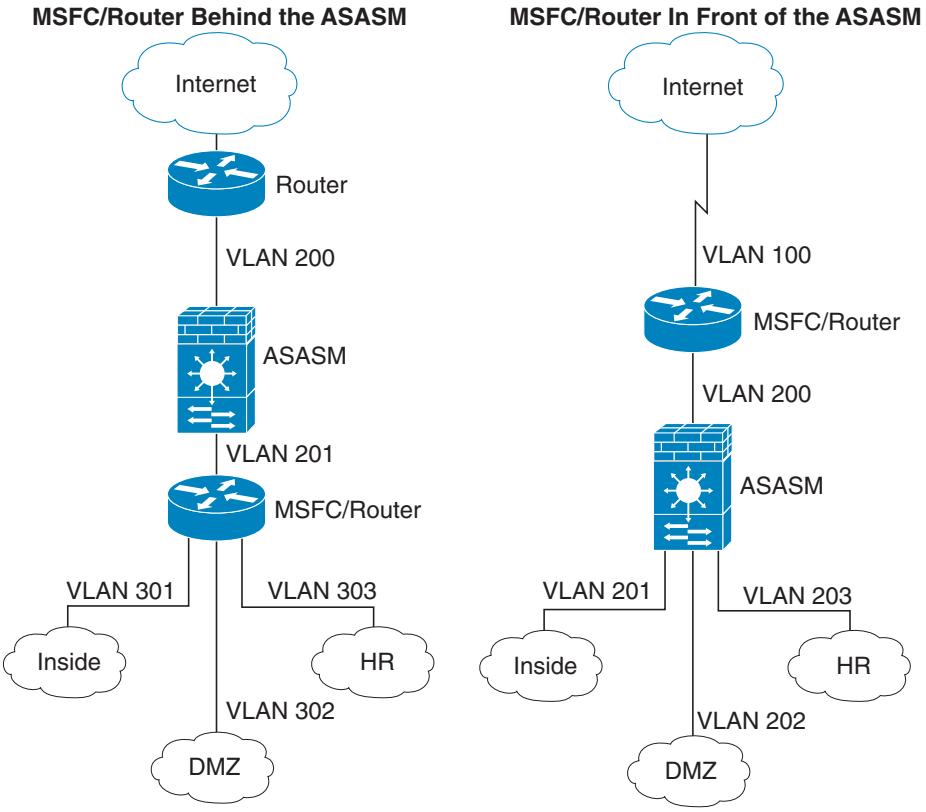
1 About the ASA Services Module in the Switch Network

For switch and software compatibility with the ASA Services Module (ASASM), see the following: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html. The switch runs Cisco IOS software on both the switch supervisor engine and the integrated Multilayer Switch Feature Card (MSFC). The ASASM runs its own operating system.

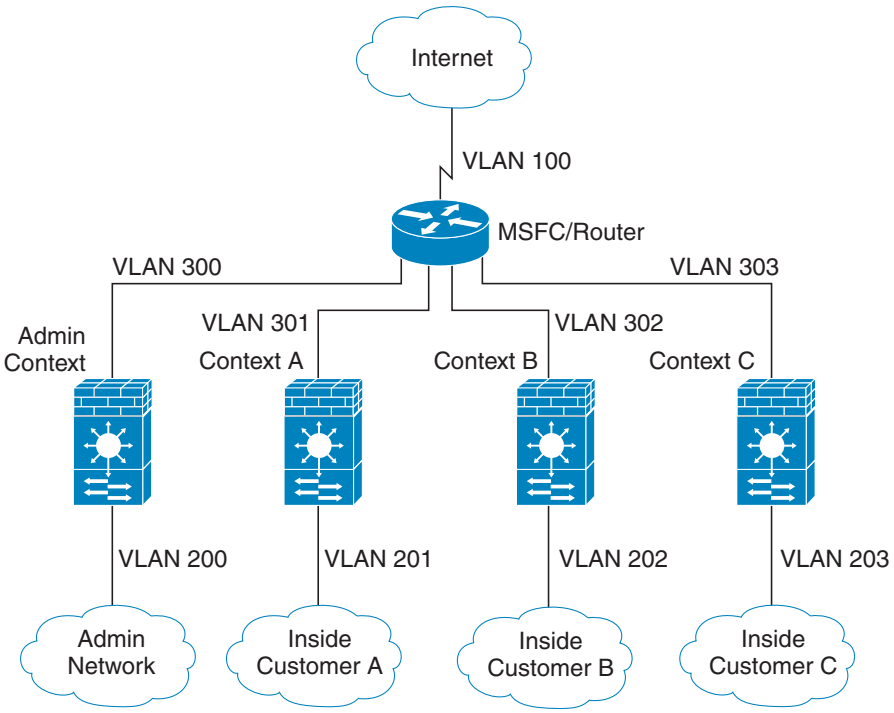
The connection between the ASASM and the switch is a single 20-GB interface.

Although you need the MSFC as part of your system, you do not have to use it. If you choose to do so, you can assign one or more VLAN interfaces to the MSFC (known as switched virtual interfaces (SVIs)). You can alternatively use an external router instead of the MSFC.

In single context mode, you can place the MSFC or router in front of the ASASM or behind the ASASM; location depends on the VLANs that you assign to the ASASM interfaces.



For multiple context mode, if you place the MSFC or router behind the ASASM, you should only connect it to a single context. If you connect it to multiple contexts, the MSFC/router will route between the contexts, which might not be your intention. The typical scenario for multiple contexts is to use a router in front of all the contexts to route between the Internet and the switched networks.



2 Verify the Module Installation

Verify that the switch acknowledges the ASASM and has brought it online. (If you need to install your ASASM, see the module installation guide on Cisco.com.)

Step 1 Enter the following command to ensure that the Status column shows "Ok" for the ASASM:

show module [**switch** {**1** |**2**}] [*mod-num* | **all**]

For a switch in a VSS, enter the **switch** argument.

Example:

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
 2     3  ASA Service Module                      WS-SVC-ASA-SM1     SAD143502E8

Mod MAC addresses                          Hw     Fw           Sw           Status
--- -------------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
...
```

3 Assign VLANs to the ASA Services Module

The ASASM does not include any external physical interfaces. Instead, it uses VLAN interfaces passed down from the supervisor. Perform the following steps at the switch CLI to pass down VLANs from the supervisor.

Before You Begin

- Assign up to 16 firewall VLAN groups to each ASASM. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- See also VLAN Guidelines and Limitations, page 10.

Procedure

Step 1 At the switch CLI, assign VLANs to a firewall group:

firewall vlan-group *firewall_group_num vlan_range*

Example:

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 58-63
Router(config)# firewall vlan-group 52 64,66-74
```

Step 2 Assign the firewall groups to the ASASM:

firewall [**switch** {**1** |**2**}] **module** *module_number* **vlan-group** *firewall_group_num*

Example:

```
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

For a switch in a VSS, enter the **switch** argument.

Examples

The following example shows how to configure private VLANs on the switch by assigning the primary VLAN to the ASASM:

Step 1 At the switch CLI, add the primary VLAN 200 to a firewall VLAN group, and assign the group to the ASASM:

```
firewall vlan-group 10 200
firewall module 5 vlan-group 10
```

Step 2 Designate VLAN 200 as the primary VLAN:

```
vlan 200
  private-vlan primary
```

Step 3 Designate only one secondary isolated VLAN. Designate one or more secondary community VLANs.

```
vlan 501
  private-vlan isolated
vlan 502
  private-vlan community
vlan 503
  private-vlan community
```

Step 4 Associate the secondary VLANs to the primary VLAN:

```
vlan 200
  private-vlan association 501-503
```

Step 5 Classify the port mode. The mode of interface f1/0/1 is host. The mode of interface f1/0/2 is promiscuous.

```
interface f1/0/1
  switchport mode private-vlan host
interface f1/0/2
  switchport mode private-vlan promiscuous
```

Step 6 Assign VLAN membership to the host port. Interface f1/0/1 is a member of primary VLAN 200 and secondary isolated VLAN 501.

```
interface f1/0/1
  switchport private-vlan host-association 200 501
```

Step 7 Assign VLAN membership to the promiscuous interface. Interface f1/0/2 is a member of primary VLAN 200. Secondary VLANs 501-503 are mapped to the primary VLAN.

```
interface f1/0/2
  switchport private-vlan mapping 200 501-503
```

Step 8 If inter-VLAN routing is desired, configure a primary SVI and then map the secondary VLANs to the primary.

```
interface vlan 200
  private-vlan mapping 501-503
```

4 Use the MSFC as a Directly-Connected Router

If you want to use the MSFC as a directly-connected router (for example, as the default gateway connected to the ASASM outside interface), then add an ASASM VLAN interface to the MSFC as a switched virtual interface (SVI).

Procedure

Step 1 (Optional) At the switch CLI, enable multiple SVIs:

```
firewall multiple-vlan-interfaces
```

By default, you can add only one SVI; to understand the caveats for multiple SVIs, see SVI Guidelines, page 10.

Step 2 Add a VLAN interface to the MSFC:

interface vlan *vlan_number*

Example:

```
Router(config)# interface vlan 100
```

Step 3 Set the IP address for this interface on the MSFC:

ip address *address mask*

Example:

```
Router(config)# ip address 192.168.1.2 255.255.255.0
```

Step 4 Enable the interface:

```
no shutdown
```

Examples

The following example shows a typical configuration with multiple SVIs:

```
firewall vlan-group 50 55-57
firewall vlan-group 51 70-85
firewall module 8 vlan-group 50-51
firewall multiple-vlan-interfaces
interface vlan 55
  ip address 10.1.1.1 255.255.255.0
  no shutdown
interface vlan 56
  ip address 10.1.2.1 255.255.255.0
  no shutdown
```

5 Log Into the ASA Services Module

From the switch CLI, you can connect to a virtual console session on the ASASM.

Procedure

Step 1 Connect to the ASASM:

service-module session [**switch** {**1** | **2**}] **slot** *number*

Example:

```
Router# service-module session slot 4
ciscoasa>
```

For a switch in a VSS, enter the **switch** argument.

You access user EXEC mode.

Step 2 Access privileged EXEC mode, which is the highest privilege level:

enable

Enter the enable password at the prompt. By default, the password is blank.

Step 3 Access global configuration mode:

configure terminal

Log Out of the ASA Services Module

If you do not log out of the ASASM, the console connection persists; there is no timeout. To end the ASASM console session and access the switch CLI, perform the following steps.

To kill another user's active connection, which may have been unintentionally left open, see the configuration guide.

Procedure

Step 1 To return to the switch CLI, type:

Ctrl-Shift-6, x

You return to the switch prompt.

Note: Shift-6 on US and UK keyboards issues the caret (^) character. If you have a different keyboard and cannot issue the caret (^) character as a standalone character, you can temporarily change the escape character to a different character. In Cisco IOS, before you session to the ASASM, use the **terminal escape-character** *ascii_number* command. For example, to temporarily change the sequence to Ctrl-w, x, enter **terminal escape-character 23**.

6 Configure ASDM Connectivity

Because the ASASM does not have physical interfaces, it does not come pre-configured for ASDM access; you must configure ASDM access using the CLI on the ASASM.

Step 1 (Optional) Enable transparent firewall mode:

```
firewall transparent
```

This command clears your configuration. See the configuration guide for more information.

Step 2 Do one of the following to configure a management interface, depending on your mode:

- Routed mode—

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

Example:

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

The **security_level** is a number between 1 and 100, where 100 is the most secure.

- Transparent mode—Configure a bridge virtual interface and assign a management VLAN to the bridge group.

```
interface bvi bvi_number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

Example:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

The **security_level** is a number between 1 and 100, where 100 is the most secure.

Step 3 (For directly-connected management hosts) Enable DHCP for the management host on the management interface network:

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

Example:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

Make sure you do not include the management address in the range.

Step 4 (For remote management hosts) Configure a route to the management hosts:

route *management_ifc management_host_ip mask gateway_ip* **1**

Example:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

Step 5 Enable the HTTP server for ASDM:

http server enable

Step 6 Allow the management host to access ASDM:

http *ip_address mask interface_name*

Example:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
ciscoasa(config)# http 10.1.1.0 255.255.255.0 management
```

Step 7 Save the configuration:

write memory

Step 8 (Optional) Set the mode to multiple mode:

mode multiple

When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM. See the configuration guide for more information.

7 Launch ASDM

Using ASDM, you can use wizards to configure basic and advanced features. ASDM is a graphical user interface that allows you to manage the ASASM from any location by using a web browser.

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Step 1 On the PC connected to the ASASM management VLAN, launch a web browser.

Step 2 In the Address field, enter the following URL:

https://*management_ip_address***/admin**

The Cisco ASDM web page appears.

Step 3 Click **Run Startup Wizard**.

Step 4 Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

Step 5 Leave the username and password fields empty, and click **OK**. The main ASDM window appears and the Startup Wizard opens.

8 Run ASDM Wizards

Run the Startup Wizard

Run the **Startup Wizard** (choose **Wizards > Startup Wizard**) so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...

(Optional) Allow Access to Public Servers Behind the ASA Services Module

The **Configuration > Firewall > Public Servers** pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASASM, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.

(Optional) Run VPN Wizards

You can configure VPN using the following wizards (**Wizards > VPN Wizards**):

- Site-to-Site VPN Wizard—Creates an IPsec site-to-site tunnel between two ASASMs.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASASM for remote users with full VPN tunneling to corporate resources. The ASASM policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- Clientless SSL VPN Wizard—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASASM using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. ACLs can be applied to restrict or allow access to specific corporate resources.
- IPsec (IKEv1) Remote Access VPN Wizard—Configures IPsec VPN remote access for the Cisco IPsec client.

(Optional) Run Other Wizards

You can optionally run the following additional wizards in ASDM. There may be other wizards available as well.

- High Availability and Scalability Wizard

  Configure failover, VPN load balancing, or ASA clustering.
- Packet Capture Wizard

  Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

9 Advanced Configuration

To continue configuring your ASASM, see the documents available for your software version at:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

10 Reference

Guidelines for the ASA Services Module

VLAN Guidelines and Limitations

- Use VLAN IDs 2 to 1001.
- You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information. See also the example in Assign VLANs to the ASA Services Module, page 4.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.
- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.
- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

SPAN Reflector Guidelines

In Cisco IOS software Version 12.2SXJ1 and earlier, for each ASASM in a switch, the SPAN reflector feature is enabled. This feature allows multicast traffic (and other traffic that requires a central rewrite engine) to be switched when coming from the ASASM. The SPAN reflector feature uses one SPAN session. To disable this feature, enter the following command:

```
no monitor session servicemodule
```

ASA and Cisco IOS Feature Interaction Guidelines

Some ASASM features interact with Cisco IOS features. The following features involve Cisco IOS software:

- Virtual Switching System (VSS)—No ASASM configuration is required.
- Autostate—The supervisor informs the ASASM when the last interface on a given VLAN has gone down, which assists in determining whether or not a failover switch is required.
- Clearing entries in the supervisor MAC address table on a failover switch—No ASASM configuration is required.
- Version compatibility—The ASASM will be automatically powered down if the supervisor/ASASM version compatibility matrix check fails.

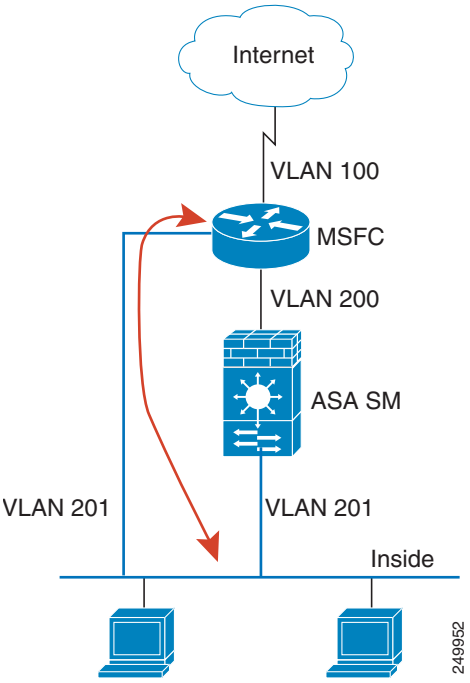
SVI Guidelines

If you want to use the MSFC as a directly connected router (for example, as the default gateway connected to the ASASM outside interface), then add an ASASM VLAN interface to the MSFC as a switched virtual interface (SVI).

For security reasons, by default, you can configure one SVI between the MSFC and the ASASM; you can enable multiple SVIs, but be sure you do not misconfigure your network.

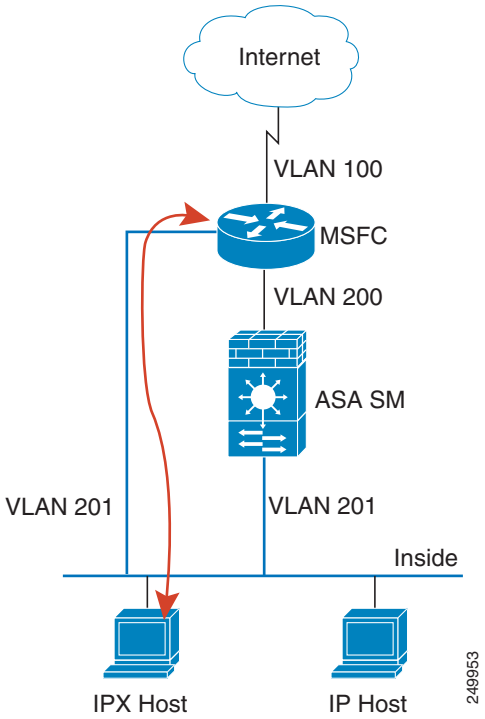
For example, with multiple SVIs, you could accidentally allow traffic to pass around the ASASM by assigning both the inside and outside VLANs to the MSFC. (See Figure 1.)

Figure 1 Multiple SVI Misconfiguration



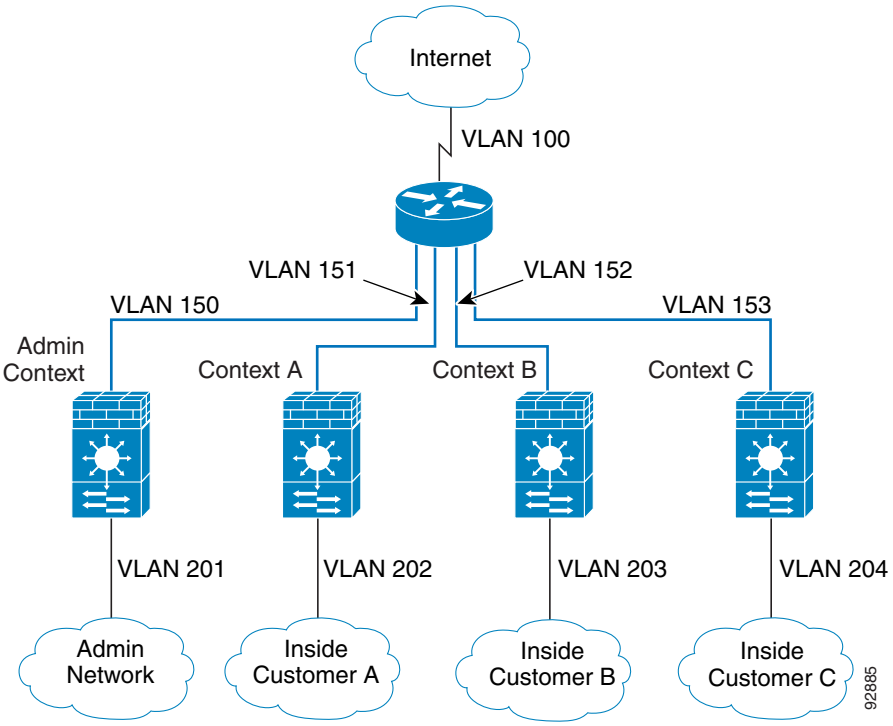
You might need to bypass the ASASM in some network scenarios. Figure 2 shows an IPX host on the same Ethernet segment as IP hosts. Because the ASASM in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the ASASM for IPX traffic. Make sure that you configure the MSFC with an access list that allows only IPX traffic to pass on VLAN 201.

Figure 2 Multiple SVIs for IPX



For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface (see Figure 3). You might also choose to use multiple SVIs in routed mode so that you do not have to share a single VLAN for the outside interface.

Figure 3 Multiple SVIs in Multiple Context Mode



Switch Configuration Guidelines for ASA Failover

- Assign VLANs to the Secondary ASA Services Module—Because both units require the same access to the inside and outside networks, you must assign the same VLANs to both ASASMs on the switch(es).
- Add a Trunk Between a Primary Switch and Secondary Switch—If you are using inter-switch failover, then you should configure an 802.1Q VLAN trunk between the two switches to carry the failover and state links. The trunk should have QoS enabled so that failover VLAN packets, which have a CoS value of 5 (higher priority), are treated with higher priority in these ports. To configure the EtherChannel and trunk, see the documentation for your switch.
- Ensure Compatibility with Transparent Firewall Mode—To avoid loops when you use failover in transparent mode, use switch software that supports BPDU forwarding. Do not enable LoopGuard globally on the switch if the ASASM is in transparent mode. LoopGuard is automatically applied to the internal EtherChannel between the switch and the ASASM, so after a failover and a failback, LoopGuard causes the secondary unit to be disconnected because the EtherChannel goes into the err-disable state.
- Enable Autostate Messaging for Rapid Link Failure Detection—The supervisor engine can send autostate messages to the ASASM about the status of physical interfaces associated with ASASM VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASASM that the VLAN is down. This information lets the ASASM declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASASM takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

  The switch supervisor sends an autostate message to the ASASM when:

  – The last interface belonging to a VLAN goes down.
  – The first interface belonging to a VLAN comes up.

  To enable autostate messaging in Cisco IOS software, enter the following command:

  ```
  firewall autostate
  ```

  Autostate messaging is disabled by default.

Reset the ASA Services Module

This section describes how to reset the ASASM. You might need to reset the ASASM if you cannot reach it through the CLI or an external Telnet session. The reset process might take several minutes.

Procedure

Step 1 Reset the ASASM:

hw-module [**switch** {**1** |**2**}] **module** *slot* **reset**

Example:

```
Router# hw-module module 9 reset

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

For a switch in a VSS, enter the **switch** argument.

The *slot* argument indicates the slot number in which the module is installed. To view the slots where the ASASM is installed, enter the **show module** command.

Note To reset the ASASM when you are already logged in to it. enter either the **reload** or **reboot** command.

Monitoring the ASA Services Module

To monitor the ASASM, enter one of the following commands on the switch:

Command	Purpose
show firewall module [*mod-num*] **state**	Verifies the state of the ASA.
show firewall module [*mod-num*] **traffic**	Verifies that traffic is flowing through the ASA.
show firewall module [*mod-num*] **version**	Shows the software version of the ASA.
show firewall multiple-vlan-interfaces	Indicates the status of multiple VLAN interfaces (enabled or disabled).
show firewall vlan-group	Displays all configured VLAN groups.
show interface vlan	Displays the status and information about the configured VLAN interface.

History for the ASA Services Module

The following table lists each feature change and the platform release in which it was implemented.

Feature Name	Platform Releases	Feature Information
ASA Services Module support on the Catalyst 6500 switch	8.5(1)	The ASASM is a high-performance security services module for the Catalyst 6500 series switch, which you configure according to the procedures in this chapter. We introduced or modified the following commands: **firewall transparent, mac address auto, firewall autostate** (IOS), **interface vlan**.
ASA Services Module support on the Cisco 7600 switch	9.0(1)	The Cisco 7600 series now supports the ASASM.
Support for private VLANs	9.1(2)	You can use private VLANs with the ASASM. Assign the primary VLAN to the ASASM; the ASASM automatically handles secondary VLAN traffic. There is no configuration required on the ASASM for this feature; see the switch configuration guide for more information.