



Resource: Getting Started with the AIP-SSM

Overview

This document includes the following topics:

- Objectives
- AIP-SSM Overview
- AIP-SSM SW Loading
- Initial AIP-SSM ASDM Configuration
- Configure a Security Policy on the Security Appliance
- Summary

Objectives

Upon completion of this document, the student will be able to perform the following tasks:

- Compare and contrast promiscuous and in-line modes.
- Explain the steps necessary to load software on a AIP-SSM
- Configure the AIP-SSM setup parameters
- Configure a security policy on an ASA security appliance using ASDM

AIP-SSM Overview

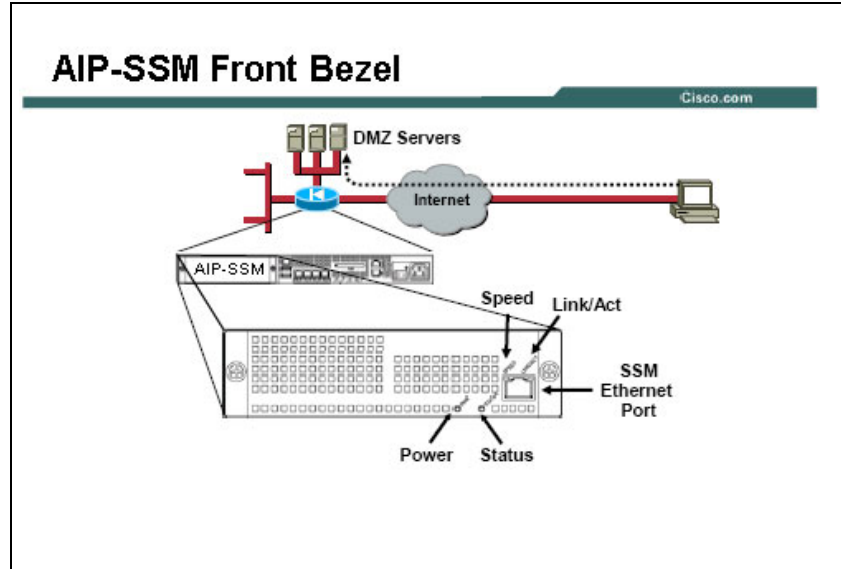


Figure 1 AIP-SSM Front Bezel

LED	Color	State	Description
Pwr	Green	On	On when the security appliance has power
Status	Green	Flashing	When the power-up diagnostics are running or the system is booting.
		Solid	Green when the system has passed power-up diagnostics.
	Amber	Solid	Amber when the power-up diagnostics have failed.
Speed	Green	Flashing	When there is network activity.
Link/Act	Green	Solid	When data is passing through the interface.

Figure 2 AIP-SSM LEDs

Cisco.com



[Cisco.com](http://www.cisco.com)



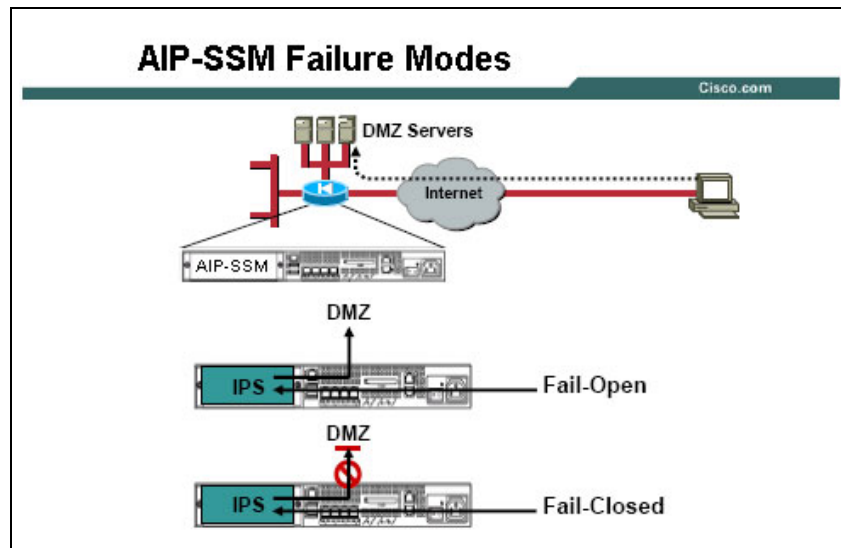


Figure 5 AIP-SSM Failure Modes

This topic is an overview of the AIP-SSM module.

There are two AIP SSM models, the AIP SSM-10 and the AIP SSM-20. Both modules look identical but the ASA SSM-20 has a faster processor and more memory than the AIP SSM-10. Only one module can populate the slot at a time. On the front bezel of the AIP-SSM module, there are 4 LEDs and one 10/100/1000 Ethernet port [1].

The table in Figure [2] lists the state of the AIP-SSM LEDs.

Remove power to the ASA 5500 before installing or removing the AIP-SSM module.

The AIP-SSM supports an internal Gigabit Ethernet and a 10/100 Ethernet interface to the ASA 5500 main card [3]. The Gigabit Ethernet interface is the primary IPS data-path interface for both inline and promiscuous IPS packets. An internal 10/100 Ethernet interface provides a control channel with the ASA 5500 main card. The external 10/100/1000 Ethernet interface is primarily used for downloading AIP-SSM software and ASDM access to the AIP-SSM module.

An AIP-SSM can be configured to operate in one of two IDS modes, promiscuous or in-line. In promiscuous mode, the AIP module is not in the traffic packet flow. The ASA security appliance administrator can configure a security policy (using standard rules and ACLs) to identify traffic that will be copied and passed to the AIP-SSM module. The AIP-SSM module performs analysis of the “copy” of the traffic. A significant benefit of operating an IDS module in promiscuous mode is that the IDS

module doesn't affect the packet flow (e.g., no performance or operational reliability issues with the forwarded traffic). The drawback to operating in a promiscuous mode, however, is that the AIP-SSM module may not stop malicious traffic from reaching its intended target. The "response actions" implemented by modules in promiscuous mode are typically post event responses and often require assistance from other networking devices (e.g., routers, firewalls) to respond to an attack. The argument can be successfully made that modules operating in promiscuous mode cannot "prevent," only react to an attack. Most IDS products on the market today operate in promiscuous mode.

Operating in an in-line mode, the IDS module is inserted directly into the traffic flow. The ASA security appliance administrator configures a security policy (using standard rules and ACLs) to identify traffic that will be passed directly to the AIP-SSM module. An in-line IDS module sits in the data-path allowing the sensor to "stop" attacks by dropping malicious traffic before it reaches the intended target providing a "protective" service.

It is important to note that not only is the AIP-SSM module processes information on the packet "envelop" (layers 3 and 4) but it is also analyzes the contents/payload of the packets for more sophisticated embedded attacks (layers 3 to 7). This deeper analysis will allow the system to identify and stop/block attacks that would normally pass through a traditional firewall device.

The administrator also needs to configure what action should be taken if the AIP-SSM module fails. "Fail-open" or "fail-closed" refers to what should happen to the traffic flow if the AIP-SSM fails for any reason (either hardware or software malfunction) [5]. With fails-open configured, if the AIP-SSM module fails, traffic will continue to flow. When operating in promiscuous mode, AIP-SSM modules are typically configured for fail-open. With fail-closed enabled, traffic will cease flowing if the IDS fails for any reason.

Before the AIP-SSM module can start to inspect and analyze traffic, three steps need to be performed. The administrator should verify, or load and verify, the IPS operating software on the AIP-SSM module. After verifying the IPS software, the administrator should configure the initial setup of the AIP-SSM module. Lastly, the administrator should configure an IPS policy in the ASA 5500. Each of these steps is discussed in more depth later in this document.

AIP-SSM SW Loading

show module [all <i>slot</i> [details recover]]	
all	Shows information for SSM, slot 1, and system, slot
details	Shows additional version information
recover	Shows the settings for the hw-module module recover command
<i>slot</i>	Specifies the SSM slot information.

Figure 1 The show module Command

Model	The model of this SSM
Serial Number	Serial number of the SSM
Hardware version	Hardware version of the SSM
Firmware version	Firmware version of the SSM
Software Version	Software version of the SSM
Status	<p>The status of the module as follows:</p> <ul style="list-style-type: none">• Initializing – The SSM is being detected and the control communication is being initialized by the system.• Up – The SSM has completed initialization by the system. For the system in slot 0, the status is Up Sys.• Unresponsive – The system encountered an error communicating with this SSM.• Reloading – The SSM is reloading.• Shutting – The SSM is shutting down.• ShuttingDown – The SSM is shut down.• Recover – The SSM is attempting to download a recovery image.

Figure 2 The show module Fields

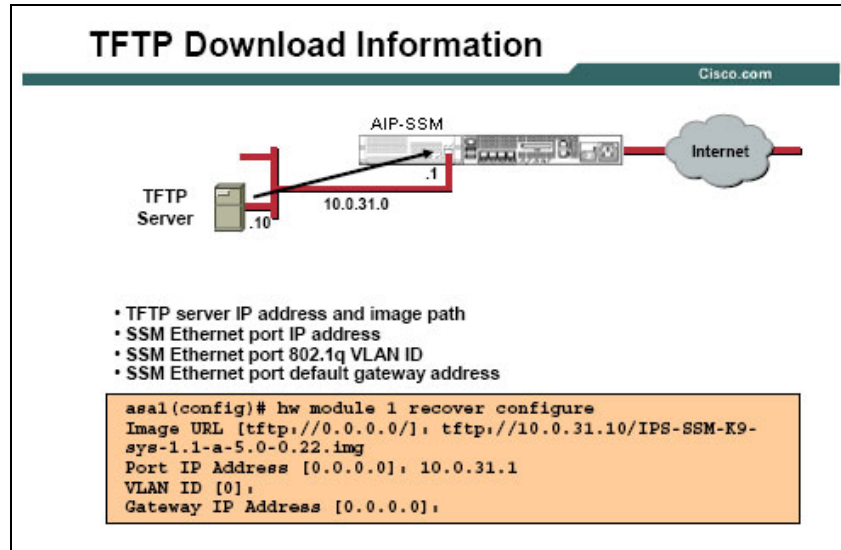


Figure 3 TFTP Download Information

hw-module <i>module slot</i> recover { boot stop configure [url <i>tftp_url</i> ip <i>port_ip_address</i> gateway <i>gateway_ip_address</i> vlan <i>vlan_id</i>]}	
boot	Initiates recovery of this SSM and downloads a recovery image according to the configure settings. The SSM then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter any network parameters after the configure keyword, you are prompted for the information.
gateway	The gateway IP address for access to the TFTP server through the SSM management interface.
ip <i>port_ip_address</i>	The IP address of the SSM management interface.
slot	Specifies the SSM slot number
stop	Stops the recovery action, and stops downloading the recovery image. The SSM boots from the original image.
url <i>tftp_url</i>	The URL for the image on a TFTP server, in the following format: tftp://server/[path/]filename
vlan <i>vlan_id</i>	Sets the VLAN ID for the management interface.

Figure 4 The **hw-module module 1** Command Syntax

Recover IPS Image

Cisco.com

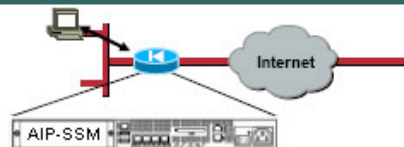
```
asa1(config)# debug module
debug module-boot enabled at level 1
asa1(config)# hw module 1 recover boot

The module in slot 1 will be recovered. This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa1(config)# VThe module in slot 1 is unresponsive.
VThe module in slot 1 is recovering.
Slot-1 8> tftp IPS-SSM-R9-asa-1.1-a-5.0-0.22.img#10.0.31.10
Slot-1 9> .....
.....
VThe module in slot 1 is recovering.
Slot-1 10> .....
.....
Slot-1 79> .....
Slot-1 80> Received 23140374 bytes
Slot-1 81> Launching TFTP Image...
VThe module in slot 1 is recovering.
VThe module in slot 1 is recovering.
VThe module in slot 1 is recovering.
VThe module in slot 1 is recovering.
Slot-1 82> Launching BootLoader...
VThe module in slot 1 is recovering.
VThe module in slot 1 is recovering.
```

Figure 5 Recover IPS Image

AIP-SSM Initialized

Cisco.com



```
asa1# show module 1

Mod Card Type                      Model          Serial No.
-----
 1 ASA 5500 Series Security Services Module-10  ASA-SSM-10    12345678

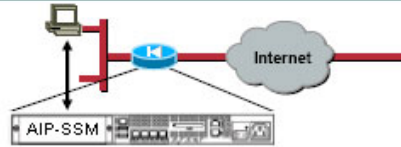
Mod MAC Address Range              Hw Version    Pw Version    Sw Version
-----
 1 000b.fcfc.0170 to 000b.fcfc.0170  1.0           1.0(7)2       5.0(0.22)S129.0

Mod Status
-----
 1 Up
```

Figure 6 AIP-SSM Initialized

Initiate a Session with the AIP-SSM

Cisco.com



```
asa1# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.

login: cisco
Password: <cisco>
You are required to change your password immediately (password
aged)
Changing password for cisco
(current) UNIX password: <cisco>
New password: <training>
Retype new password: <training>
sensor#
```

Figure 7 Initiate a Session with the AIP-SSM

Session Setup Default

Cisco.com

```
sensor# setup

--- System Configuration Dialog ---

Current Configuration:

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

Figure 8 Session Setup Default

Session Setup Command

Cisco.com

```
sensor# setup
*****
Continue with configuration dialog?[yes]: <yes>
Enter host name[sensor]: sensor1
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.0.1.41/24,10.0.1.1
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.0.1.0/24
Permit:
*****

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: 2
Warning: Reboot is required before the configuration change will take effect
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: yes
```

Figure 9 Session setup Command

The show module 1 detail Command

Cisco.com

```
asa1# show module 1 detail
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-10
Model:          ASA-SSM-10
Hardware version: 1.0
Serial Number:   0
Firmware version: 1.0(7)2
Software version: 5.0(0.22)S129.0
Status:          Up
Mgmt IP addr:    10.0.1.41

Mgmt web ports:  443

Mgmt TLS enabled: true
```

Figure 10 The show module 1 detail Command

The administrator can use the **show module 1** command to view module 1 configuration. The administrator can view such statistics as hardware version, software version, firmware version, and status of the AIP-SSM module.

The context for the command is shown in Figure [1].

The **show module** fields are shown in Figure [2].

The administrator can use the **hw-module module 1 recover** command to load a recovery software image to the AIP-SSM from a TFTP server. This is a two step process. The administrator must first define the SSM and TFTP server network parameters and then initiate the download.

Adding the **configure** keyword to the command enables the administrator to define the SSM and TFTP server network parameters. In the example in Figure [3], the TFTP server IP address is 10.0.31.10 while the external AIP-SSM Ethernet connector IP address is 10.0.31.1. The TFTP Server will download the AIP-SSM-K9-sys-1.1-a-5.0-0.22.img image file to the AIP-SSM module.

The syntax for the command is shown in Figure [4].

The administrator can utilize the **hw-module module 1 recover boot** command to initiate the TFTP download of the image defined in the **hw-module module 1 recover configure** command. To aid in the download, the administrator can enable the **module-boot debug** command. A sample of a download is displayed in the example in Figure [5]. The full debug output was truncated to fit in the window. Please be patient, downloading the image, launching the image, launching the bootloader, and recovering the module takes approximately 5 minutes to complete.

Once the SSM module is initialized, the administrator can use the **show module 1** command to view the status of the module.

From the **show module 1** window, the administrator can view the model type, MAC address, serial number, hardware version, firmware version, and software version of the AIP-SSM module. The administrator can also determine the status of the module.

In the example in Figure [6], notice the module is in the Up status and IPS software version 5.0(0.22)S129.0 is loaded on the module.

Once the SSM is in the “Up” status, the administrator can open a Telnet session with the module via the security appliance command line. To initiate a Telnet session, enter the **session 1** command at the CLI command prompt. Entering the **session 1** command for the first time, the administrator is prompted for the default login prompt, User name cisco and password cisco.

After entering the default login and password, the administrator is immediately prompted to change the password. In the example in Figure [7], the password was changed to training. After changing the password, the default sensor# command prompt is displayed. To end a session, enter **exit** or **Ctrl+Shift+6** then the **x** key.

After installing and loading software on the AIP-SSM module, the administrator must initialize the AIP-SSM module using the **setup** command. With the **setup** command, the administrator can configure basic AIP-SSM settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, and time settings. After initializing the AIP-SSM, the administrator is

ready to configure intrusion prevention using either the ASDM, or the CLI.

The example in Figure [8] displays the default setup parameters. Notice the default IP address of the external Ethernet connector is 10.0.9.201/24.

To communicate with ASDM, the administrator may need to change some of the default session > setup parameters such as the IP interface and current access list. A description of the **setup** command parameters is as follows:

- Enter host name[sensor]: – Name of the sensor. The hostname can be a string of 1 to 64 characters that matches the pattern `^[A-Za-z0-9_/-]+$`. The default is sensor. You receive an error message if the name contains a space or exceeds 64 alphanumeric characters.
- Enter IP interface[10.1.9.201/24,10.1.9.1]: – IP address of the external AIP-SSM Ethernet interface. The default is 10.1.9.201. The default mask corresponding to the IP address is /24, or 255.255.255.0. Default gateway address is 10.1.9.1.
- Enter telnet-server status[disabled]: – Enables or disables Telnet for remote access to the sensor. Telnet is not a secure access service and therefore is disabled by default.
- Enter web-server port[443]: – TCP port used by the web server. The default is 443 for HTTPS. You receive an error message if you enter a value out of the range of 1 to 65535.
- Modify current access list?[no]: – IP address of the hosts or networks that have permission to access the sensor. By default there are no entries.

In the example in Figure [9], the IP address of the external Ethernet connector was changed to 10.0.1.41/24. Hosts on the 10.0.1.0/24 subnet are permitted to access the module.

The administrator can utilize the **show module 1 detail** command to view AIP-SSM hardware and software details including remote management configuration. In the example in Figure [10], a device manager can access the AIP-SSM module through the AIP-SSM external interface at IP address is 10.0.1.41, AIP-SSM web server port is 443, and management TLS/SSL is enabled.

Initial AIP-SSM ASDM Configuration

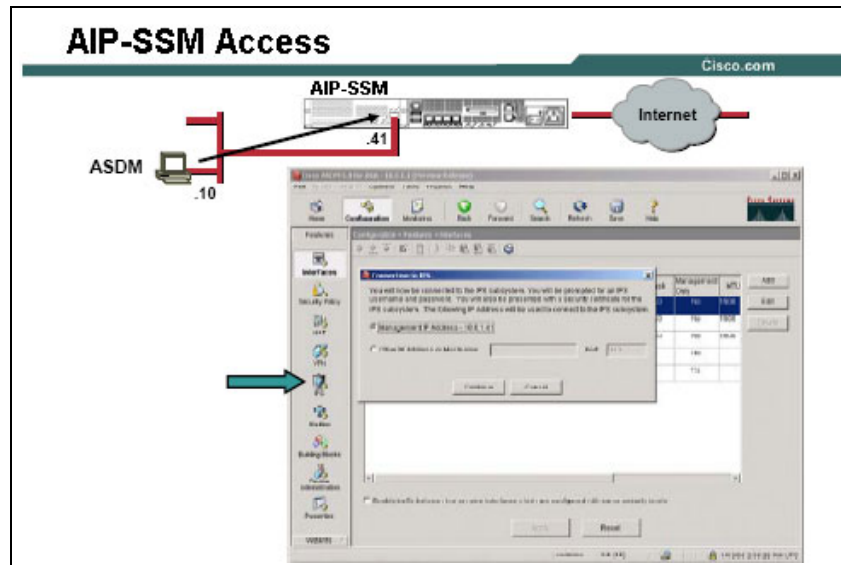


Figure 1 AIP-SSM Access

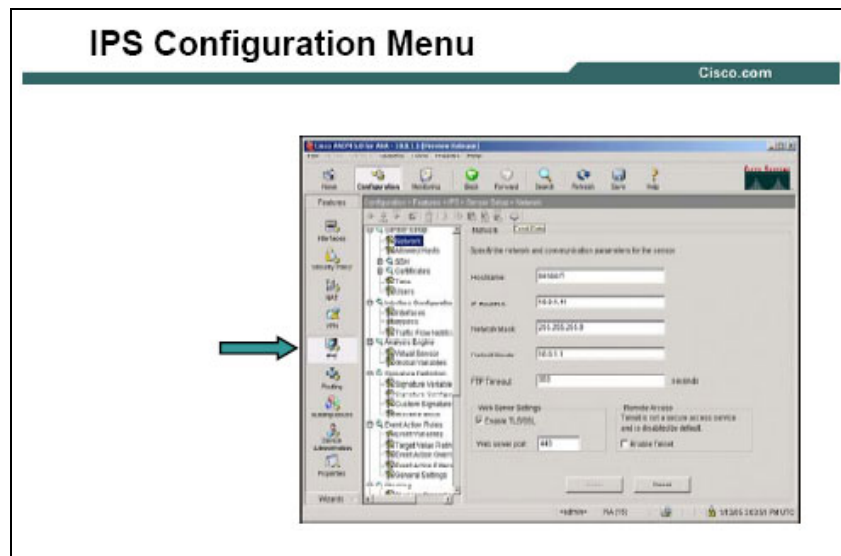


Figure 2 IPS Configuration Menu

Allowed Administrative Hosts

Cisco.com

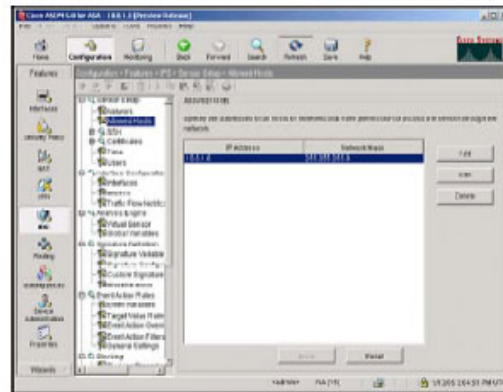


Figure 3 Allowed Administrative Hosts

Add Users

Cisco.com

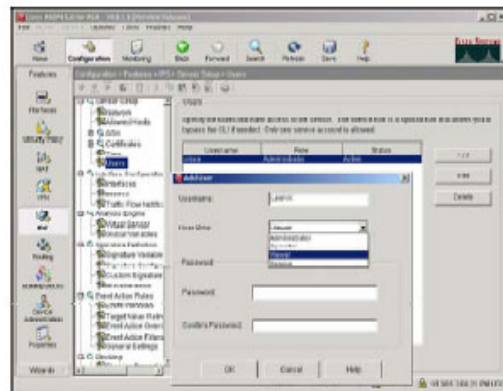


Figure 4 Add Users

After installing the AIP-SSM module, the administrator initialized the module using the **session > setup** command from CLI. With the setup command, the administrator configured basic sensor settings, including the hostname, IP interfaces, Web server port, access control lists, and time settings. After initializing the AIP-SSM module, the administrator can now communicate with the module utilizing ASDM.

To access the AIP-SSM module from ASDM, click the **IPS** icon under the features column [1]. The connecting to IPS popup window appears. The IP address referenced by the Management Address prompt in the popup window refers to the IP address of the external Ethernet interface of AIP-SSM module. Click the

Management IP address button and then click **continue**. If a route exists between the ASDM PC and the external Ethernet interface on the AIP-SSM module, the AIP-SSM session login prompt should open.

The administrator can configure intrusion prevention either using the ASDM or through the CLI. Enabling an administrator to access the AIP-SSM module is covered in this document. Configuring IPS analysis engine, signature definition, event action rules, and such are not covered in this course. To learn more about IPS and how to the configure IPS feature set, it is recommended that you refer to the documentation on Cisco.com.

If connectivity exists between the PC and the AIP-SSM, the administrator is prompted for their User name and password. Click **Yes** to continue.

Use the Network window to specify network and communication parameters for the AIP-SSM module [2]. After the administrator uses the setup command to initialize the sensor, the network and communication parameter values appear in the Network window. If the administrator needs to change these parameters, they can do so from the Network window.

Use the Allowed Hosts window to specify hosts or networks that have permission to access the AIP-SSM module [3]. After the administrator uses the setup command to initialize the AIP-SSM module, the allowed hosts parameter values appear on the Allowed Hosts window. If the administrator needs to change these parameters, they can do so from the Allowed Hosts window. The administrator must add the management host, such as ASDM, IDM, IDS MC and the monitoring host, such as IDS Security Monitor, to the allowed hosts list, otherwise they will not be able to communicate with the AIP-SSM module. IDM, IDS MC, and IDS Security Monitor are not covered in this document. To learn about these products, you should refer to the documentation on Cisco.com.

ASDM permits only one user to log in at a time. If another user tries to log in, a message says the first user is logged in. The administrator can create and remove users from the AIP-SSM [4]. Each user is associated with a role that controls what that user can and cannot modify.

There are four user roles:

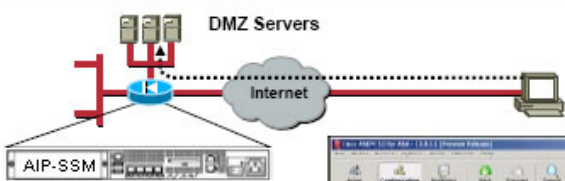
- Viewers – Can view configuration and events, but cannot modify any configuration data except their user passwords.
- Operators – Can view everything and can modify the following options:

- Signature tuning (priority, disable or enable)
 - Virtual sensor definition
 - Managed routers
 - Their user passwords
- Administrators – Can view everything and can modify all options that operators can modify in addition to the following:
 - Sensor addressing configuration
 - List of hosts allowed to connect as configuration or viewing agents
 - Assignment of physical sensing interfaces
 - Enable or disable control of physical interfaces
 - Add and delete users and passwords
 - Generate new SSH host keys and server certificates
- Service – Only one user with service privileges can exist on a AIP-SSM module. The service role is a special role that allows a service user to bypass the CLI if needed. Only one service account is allowed.

Configure a Security Policy on the Security Appliance

Create a Security Policy

Cisco.com



Create a Security Policy

- Identify a class of traffic
- Associate IPS policy with class of traffic
- Activate the policy globally or on an interface

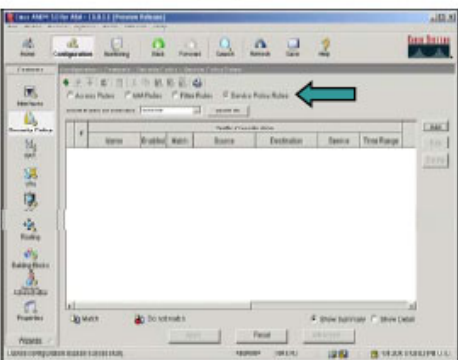
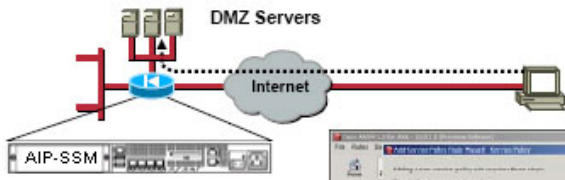


Figure 1 Create a New Security Policy

Create a Service Policy

Cisco.com



Create a Service-Policy

- Enable policy
 - globally, or
 - on an interface
- Policy name

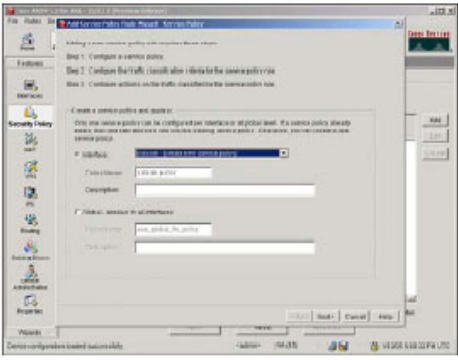


Figure 2 Create a Service Policy

Identify a Class of Traffic

Cisco.com

Class of traffic

- Create a traffic class
- Defining traffic matching criteria

Figure 3 Identify a Class of Traffic

Define Traffic Matching Criteria

Cisco.com

Any Host

Figure 4 Define Traffic Matching Criteria

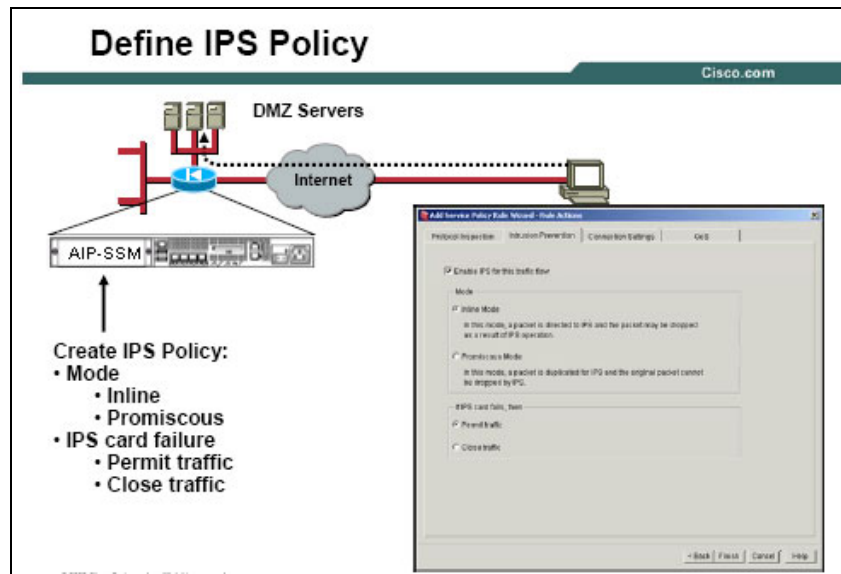


Figure 5 Define IPS Policy

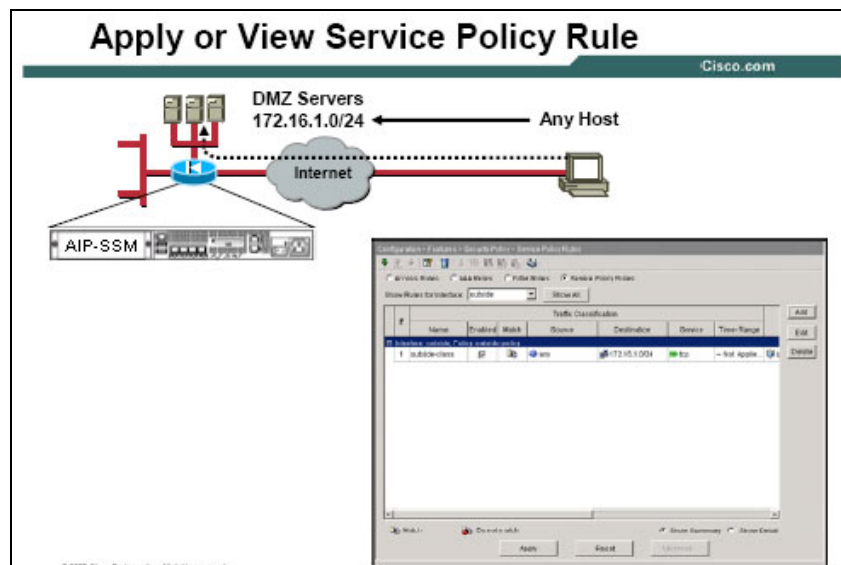


Figure 6

This topic explains how to configure an IPS service policy on the ASA security appliance. The last step in the process is to create a security policy on the ASA security appliance. A security policy enables the ASA security appliance to pre-filter then pass selected traffic to the AIP-SSM module for inspection and analysis. This level of interaction between the ASA security appliance and AIP-SSM module enables the IPS system to operate at greater efficiency. The AIP-SSM module only analyzes a subset of the total bandwidth, the relevant traffic, and filters out non-relevant traffic. The administrator can apply a security policy to an interface or globally to every interface.

To create an IPS service policy from ASDM, select the **Security Policy** Icon and click the **Service Policy Rules** button [1].

The Service Policy dialog box enables the administrator to add a new service policy rule [2]. The new security policy rule can be applied to a specific interface such as the outside or inside interface. Or, the service policy rule can be applied globally to all interfaces.

A description of the **Create a Service Policy and Apply to Group** box parameters is as follows:

- **Interface** button – Applies the rule to a specific interface. This selection is required if the administrator wants to match traffic based on the source or destination IP address using an ACL.
- **Interface** drop-down list – Specifies the interface to which the rule applies.
- **Description** box – Provides a text description of the policy.
- **Global - applies to all interfaces button** – Applies the rule to all interfaces.
- **Policy Name** – Specifies the name of the global service policy. Only one global service policy is allowed and it cannot be renamed.
- **Description** box – Provides a text description of the policy.

After the administrator defines a service policy, they define a traffic class next. The administrator defines the criteria used by the ASA security appliance to identify which traffic will be routed to the AIP-SSM module for inspection and analysis. The **Traffic Classification Criteria** dialog box enables the administrator to specify the criteria they want to use to match traffic to which the security policy rule applies. First the administrator defines a traffic class name.

- **Create a new traffic class** – Identifies the name of the new traffic class.
- **Description** – Provides a text description of the new traffic class.

Next, the administrator defines the matching criteria. The available matching criteria choices are as follows:

- **Any traffic button** – Matches all traffic regardless of the traffic type.
- **Source and destination IP address (uses ACL)** – Matches traffic based on the source and destination IP address, using an ACL. This selection is only available if you apply the rule to a specific interface using an Interface Service Policy.
- **Default Inspection Traffic button** – Uses the criteria specified in the default inspection traffic policy.
 - **Limit inspection between source and destination IP address (uses ACL) checkbox** – Excludes traffic from the default inspection traffic policy based on source and destination IP address. This selection is only available if you apply the rule to a specific interface using an Interface Service Policy.
- **TCP or UDP destination port button** – Matches traffic based on the TCP or UDP destination port.
- **RTP range button** – Matches traffic based on a range of RTP ports.
- **IP Precedence button** – Matches traffic based on the IP precedence model of QoS.
- **IP DiffServ CodePoints (DSCP) button** – Matches traffic based on the Differentiated Services model of QoS.
- **Tunnel Group button** – Matches traffic based on the tunnel group.

In the example in Figure [3], the administrator selected the **Source and destination IP address (uses ACL)** button. The traffic inspected and analyzed by the AIP-SSM module is identified by the source and destination addresses.

The **Source and destination IP address** dialog box appears when you select **Source and destination IP address (uses ACL)** or **Limit inspection between source and destination IP address (uses ACL)** on the **Traffic Match Criteria** dialog box. This dialog window enables the administrator to identify the traffic to which a service policy rule applies based on the IP address of the sending or receiving host. In the example in Figure [4], the traffic criteria is a packet with any source IP address from the outside destined to the DMZ subnet 172.16.1.0/24.

The **Intrusion Prevention** tab enables the administrator to configure the Intrusion Prevention (IPS) action to take on the selected a traffic class [5]. This window appears only if the AIP-SSM is installed in the security appliance.

- **Enable IPS for this traffic flow** check box – Enables or disables intrusion prevention for this traffic flow. When this check box is selected, the other parameters in this window become active.
- **Mode** group box – Configures the operating mode for intrusion prevention
 - **Inline Mode** option button – Selects Inline Mode, in which a packet is directed to IPS. The packet might be dropped as a result of the IPS operation.
 - **Promiscuous Mode** option button – Selects Promiscuous Mode, in which IPS operates on a duplicate of the original packet. The original packet cannot be dropped.
- **If IPS card fails, then** group box – Configures the action to take if the AIP-SSM becomes inoperable.
 - **Permit traffic** option button – Permit traffic if the AIP-SSM fails
 - **Close traffic** option button – Block traffic if the AIP-SSM fails.

The last step is to apply the service policy rule. Click **Apply** to initiate the new IPS service policy. In the example in Figure [6], the outside traffic class defined as those packets from any source to a destination address of 172.16.1.0/24 will be inspected and analyzed by the AIP-SSM module.

Summary

There are two AIP-SSM models, SSM-10 and SSM-20.

- Use the **hw module 1 recover** command to load the initial AIP-SSM software image.
- Use the session command to configure the initial AIP-SSM setup.
- Use ASDM, or CLI, to configure IPS inspection and analyze parameters.