Cisco ASA 5500 Series Getting Started Guide

For the Cisco ASA 5510, ASA 5520, ASA 5540, and ASA 5550

Software Version 8.3

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: DOC-78-19186-01
Text Part Number: 78-19186-01

Cisco ASA 5500 Series Getting Started Guide

CONTENTS

iii

CHAPTER 1

Before You Begin

Use the following table to find the installation and configuration steps that are required for your implementation of the Cisco ASA 5500 series adaptive security appliance.

The adaptive security appliance implementations included in this document are as follows:

- ASA 5500, page 1-1
- ASA 5500 with AIP SSM, page 1-2
- ASA 5500 with CSC SSM, page 1-3
- ASA 5500 with 4GE SSM, page 1-4
- ASA 5550, page 1-5
- Related Documents, page 1-5

ASA 5500

To Do This ...	See ...
Install the chassis	Chapter 4, “Installing the ASA 5500, ASA 5510, ASA 5520, and ASA 5540”

Connect interface cables	Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms"
Perform initial setup of the adaptive security appliance	Chapter 7, "Configuring the Adaptive Security Appliance"
Configure the adaptive security appliance for your implementation	Chapter 8, "Scenario: DMZ Configuration" Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration" Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client" Chapter 11, "Scenario: SSL VPN Clientless Connections" Chapter 12, "Scenario: Site-to-Site VPN Configuration"
Configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Operate the system on a daily basis	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

ASA 5500 with AIP SSM

To Do This ...	**See ...**
Install the chassis	Chapter 4, "Installing the ASA 5500, ASA 5510, ASA 5520, and ASA 5540"
Install the AIP SSM	Chapter 5, "Installing Optional SSMs"

Connect interface cables	Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms"
Perform initial setup the adaptive security appliance	Chapter 7, "Configuring the Adaptive Security Appliance"
Configure the adaptive security appliance for AIP SSM	Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration"
Configure IPS software for intrusion prevention	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI* *Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

ASA 5500 with CSC SSM

To Do This ...	See ...
Install the chassis	Chapter 4, "Installing the ASA 5500, ASA 5510, ASA 5520, and ASA 5540"
Install the CSC SSM	Chapter 5, "Installing Optional SSMs"
Connect interface cables	Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms"
Perform initial setup of the adaptive security appliance	Chapter 7, "Configuring the Adaptive Security Appliance"

Configure the adaptive security appliance for content security	Chapter 14, "Configuring the CSC SSM"
Configure the CSC SSM	*Cisco Content Security and Control SSM Administrator Guide*
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI* *Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

ASA 5500 with 4GE SSM

To Do This ...	**See ...**
Install the chassis	Chapter 4, "Installing the ASA 5500, ASA 5510, ASA 5520, and ASA 5540"
Install the 4GE SSM	Chapter 5, "Installing Optional SSMs"
Connect interface cables	Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms"
Perform initial setup of the adaptive security appliance	Chapter 7, "Configuring the Adaptive Security Appliance"

Install the fiber optic module	Chapter 5, "Installing Optional SSMs"
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI* *Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

ASA 5550

To Do This ...	See ...
Install the chassis Install the fiber optic module, if any Connect interface cables	Chapter 3, "Installing the ASA 5550"
Perform initial setup of the adaptive security appliance	Chapter 7, "Configuring the Adaptive Security Appliance"
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI* *Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

Related Documents

For more information, see the following documentation:

- *Documentation Roadmap for the Cisco ASA 5500 Series*
- *Cisco ASA 5500 Series Release Notes*
- *Release Notes for Cisco ASDM*

- *Cisco ASA 5500 Series Command Reference*
- *Cisco ASA 5500 Series Configuration Guide using the CLI*
- *Cisco ASA 5500 Series System Log Messages*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*
- *Open Source Software Licenses for ASA and PIX Security Appliances*

CHAPTER 2

Maximizing Throughput on the ASA 5550

Note This chapter applies only to the Cisco ASA 5550.

The Cisco ASA 5550 adaptive security appliance is designed to deliver maximum throughput when configured according to the guidelines described in this chapter.

This chapter includes the following sections:

Embedded Network Interfaces

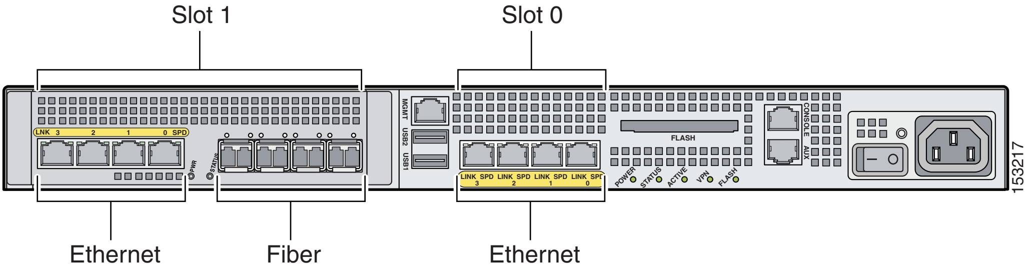
The adaptive security appliance has two internal buses providing copper Gigabit Ethernet and fiber Gigabit Ethernet connectivity:

- Slot 0 (corresponding to Bus 0) has four embedded copper Gigabit Ethernet ports
- Slot 1 (corresponding to Bus 1) has four embedded copper Gigabit Ethernet ports and four embedded SFPs that support fiber Gigabit Ethernet connectivity

Note To establish fiber connectivity on the adaptive security appliance, you must order and install SFP modules for each fiber port you want to use. For more information on fiber ports and SFP modules, see the "Installing SFP Modules" section on page 3-6.

Figure 2-1 shows the embedded ports on the Cisco ASA 5550.

Figure 2-1 Embedded Ports on the ASA 5550



Note Although Slot 1 has four copper Ethernet ports and four fiber Ethernet ports, you can use only four Slot 1 ports at a time. For example, you could use two Slot 1 copper ports and two fiber ports, but you cannot use fiber ports if you are already using all four Slot 1 copper ports.

Balancing Traffic to Maximize Throughput

To maximize traffic throughput, configure the adaptive security appliance so that traffic is distributed equally between the two buses in the device. To achieve this, lay out the network so that all traffic flows through both Bus 0 (Slot 0) and Bus 1 (Slot 1), entering through one bus and exiting through the other.

In Figure 2-2 and Figure 2-3, network traffic is distributed so that all traffic flows through both buses in the device, enabling the adaptive security appliance to deliver maximum throughput.

Figure 2-2 Traffic Evenly Distributed for Maximum Throughput (Copper to Copper)

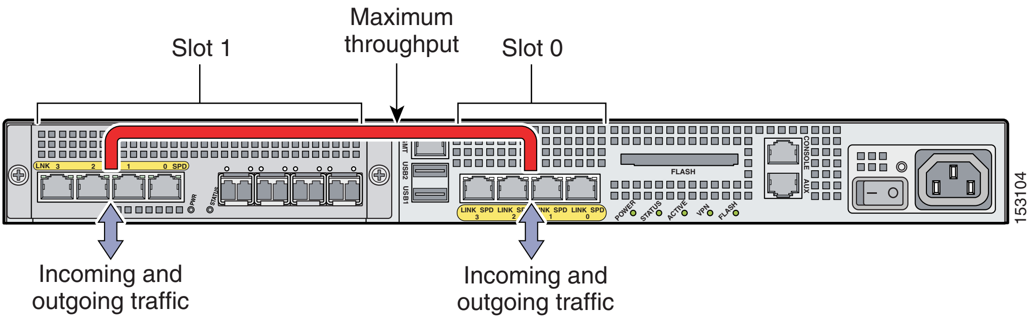


Figure 2-3 Traffic Evenly Distributed for Maximum Throughput (Copper to Fiber)

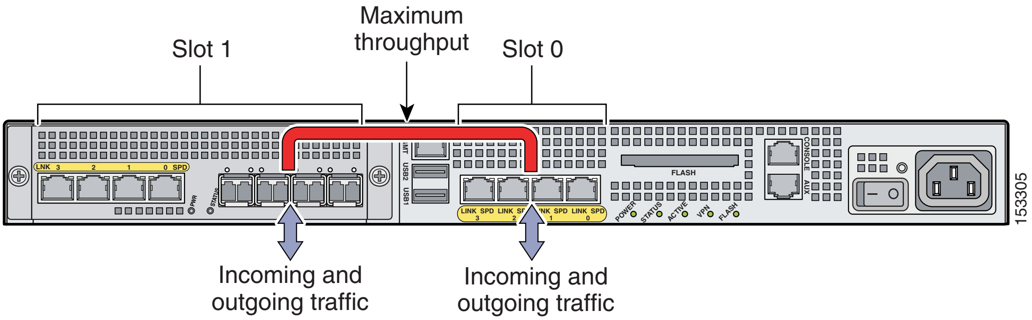
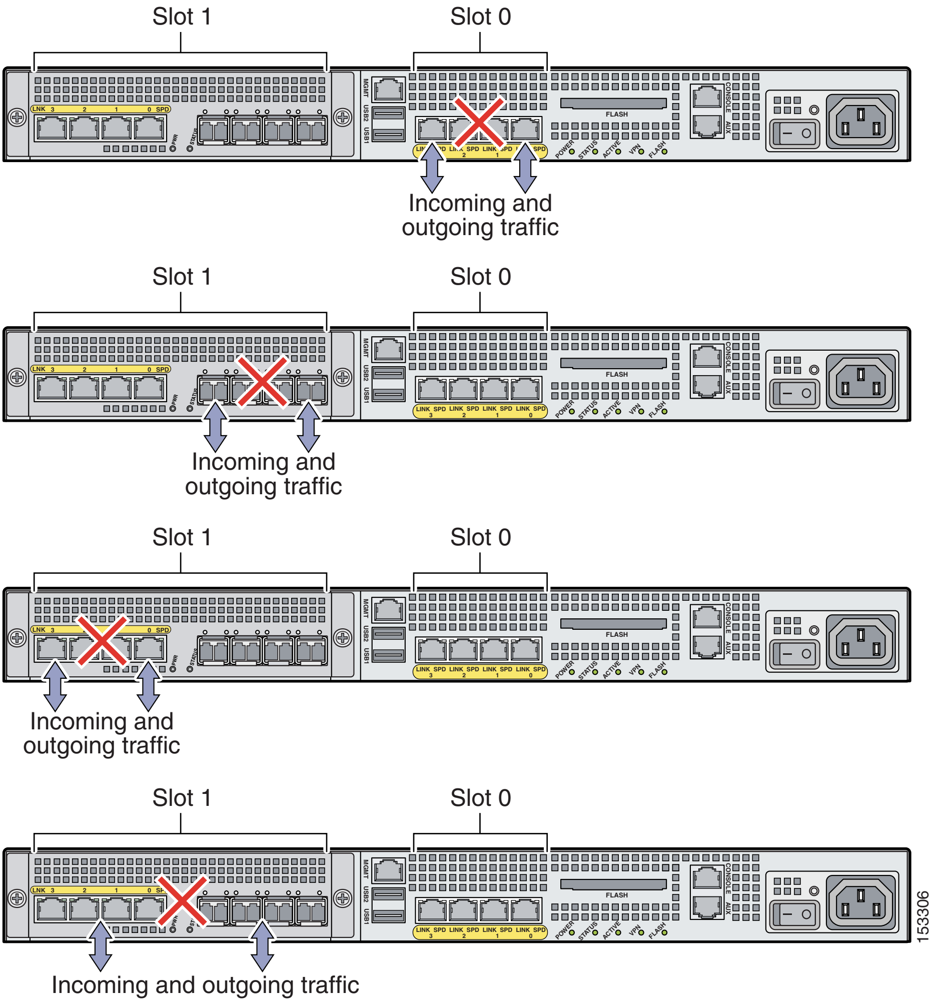


Figure 2-4 illustrates several configurations that do not enable the adaptive security appliance to deliver maximum throughput because network traffic flows through only one bus on the device.

Figure 2-4 Configurations Not Enabling Maximum Throughput



Note You can use the **show traffic** command to see the traffic throughput over each bus. For more information about using the command, see the *Cisco ASA 5500 Series Command Reference*.

What to Do Next

Continue with Chapter 3, "Installing the ASA 5550."

CHAPTER 3

Installing the ASA 5550

Caution Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

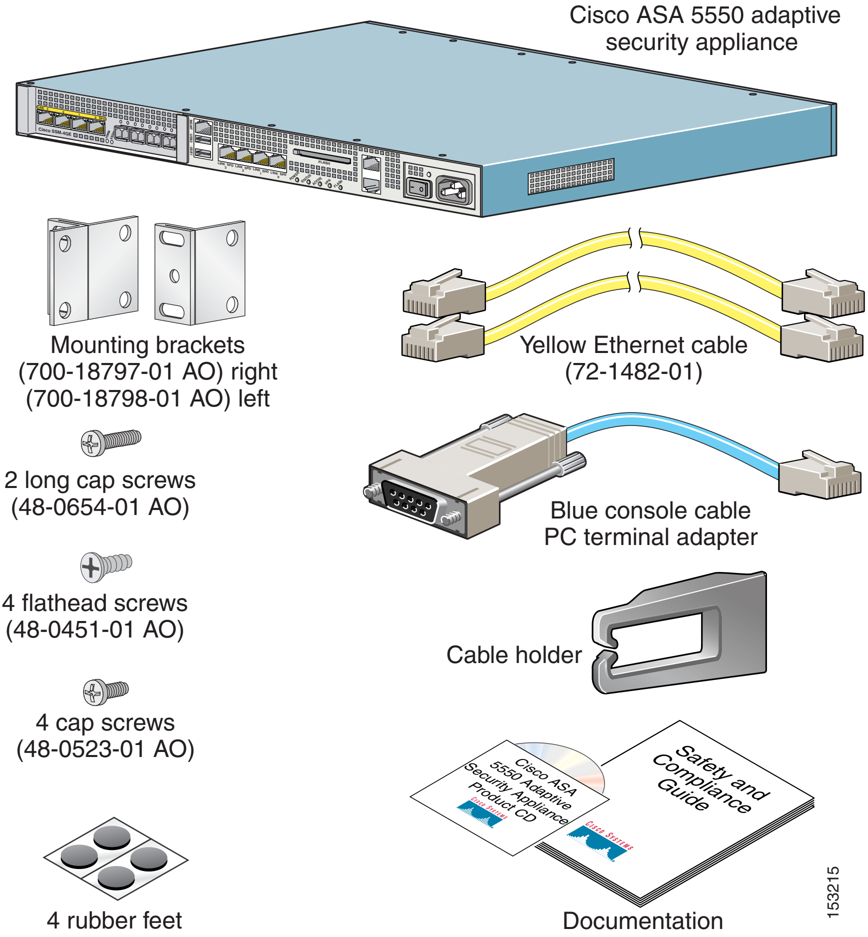
Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 49

This chapter describes the ASA 5550 adaptive security appliance and rack-mount and installation procedures for the adaptive security appliance. This chapter includes the following sections:

Verifying the Package Contents

Verify the contents of the packing box, shown in Figure 3-1, to ensure that you have received all items necessary to install the Cisco ASA 5550.

Figure 3-1 Contents of ASA 5550 Package


Cisco ASA 5550 adaptive security appliance
Mounting brackets (700-18797-01 AO) right (700-18798-01 AO) left
Yellow Ethernet cable (72-1482-01)
2 long cap screws (48-0654-01 AO)
Blue console cable PC terminal adapter
4 flathead screws (48-0451-01 AO)
Cable holder
4 cap screws (48-0523-01 AO)
Cisco ASA 5550 Adaptive Security Appliance Product CD
Safety and Compliance Guide
4 rubber feet
Documentation
153215

Installing the Chassis

This section describes how to rack-mount and install the adaptive security appliance. You can mount the adaptive security appliance in a 19-inch rack (with a 17.5- or 17.75-inch opening).

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety.**

The following information can help plan equipment rack installation:

- Allow clearance around the rack for maintenance.
- When mounting a device in an enclosed rack ensure adequate ventilation. An enclosed rack should never be overcrowded. Make sure that the rack is not congested, because each unit generates heat.
- When mounting a device in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- If the rack contains only one unit, mount the unit at the bottom of the rack.
- If the rack is partially filled, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If the rack contains stabilizing devices, install the stabilizers prior to mounting or servicing the unit in the rack.

Warning **Before performing any of the following procedures, ensure that the power source is off. (AC or DC). To ensure that power is removed from the DC circuit, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

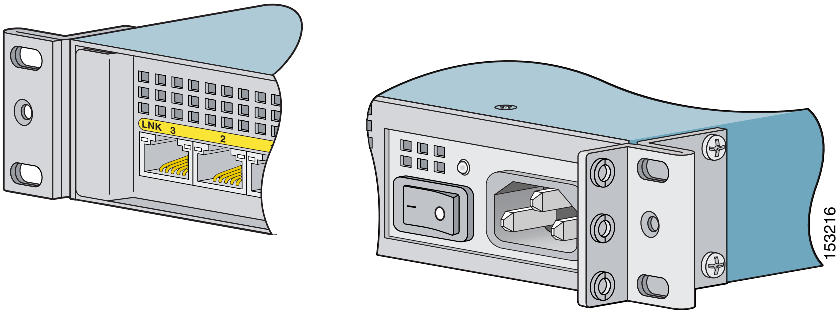
Rack-Mounting the Chassis

To rack-mount the chassis, perform the following steps:

Note You can use the mounting brackets to mount the chassis to the front or the back of the rack, with the front panel or the rear panel of the chassis facing outward.

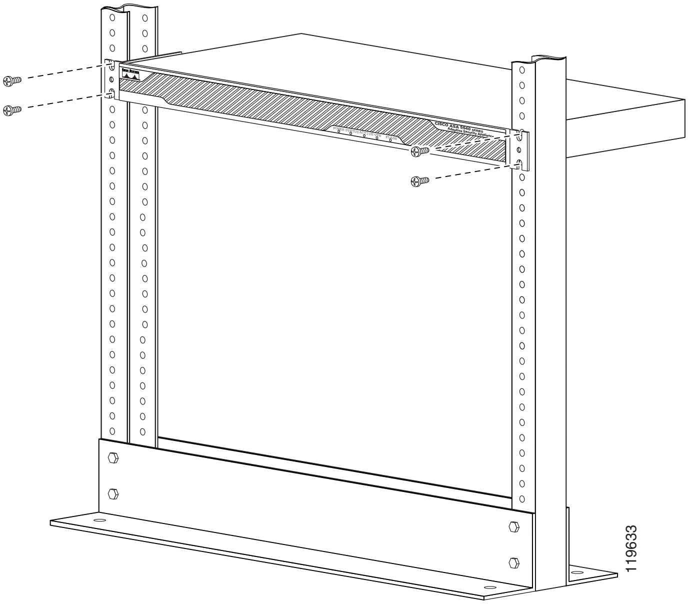
Step 1 Attach the rack-mount brackets to the chassis using the supplied screws. Attach the brackets to the holes as shown in Figure 3-2. After the brackets are secured to the chassis, you can rack-mount it.

Figure 3-2 Installing the Right and Left Brackets



Step 2 Attach the chassis to the rack using the supplied screws, as shown in Figure 3-3.

Figure 3-3 ***Rack-Mounting the Chassis***



Note Figure 3-2 shows the rack mounting brackets attached to the rear of the chassis while Figure 3-3 shows the rack mounting brackets attached to the front of the chassis. You can attach the mounting brackets to the front or the rear of the chassis so that you can have the front panel or the rear panel of the chassis facing outward. Figure 3-2 shows the brackets attached to the rear so you can see how that configuration appears while Figure 3-3 shows the brackets attached to the front so that you can see how that configuration appears. In Step 1 and Step 2, you will choose to have either the brackets rear mounted or front mounted but not both.

To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Installing SFP Modules

The adaptive security appliance uses a field-replaceable SFP module to establish fiber Gigabit Ethernet connections.

This section describes how to install and remove SFP modules in the adaptive security appliance. This section includes the following topics:

- SFP Module, page 3-6
- Installing an SFP Module, page 3-8

SFP Module

The SFP (Small Form-Factor Pluggable) module is a hot-swappable input/output device that plugs into the fiber ports.

Note If you install an SFP module after the switch has powered on, you must reload the adaptive security appliance to enable the SFP module.

Table 3-1 lists the SFP modules that are supported by the adaptive security appliance.

Table 3-1 Supported SFP Modules

SFP Module	Type of Connection	Cisco Part Number
1000BASE-LX/LH	Fiber	GLC-LH-SM=
1000BASE-SX	Fiber	GLC-SX-MM=

The 1000BASE-LX/LH and 1000BASE-SX SFP modules are used to establish fiber connections. Use fiber cables with LC connectors to connect to an SFP module. The SFP modules support 850 to 1550 nm nominal wavelengths. The cables must not exceed the required cable length for reliable communications. Table 3-2 lists the cable length requirements.

Table 3-2 Cabling Requirements for Fiber-Optic SFP Modules

SFP Module	62.5/125 micron Multimode 850 nm Fiber	50/125 micron Multimode 850 nm Fiber	62.5/125 micron Multimode 1310 nm Fiber	50/125 micron Multimode 1310 nm Fiber	9/125 micron Single-mode 1310 nm Fiber
LX/LH	—	—	550 m at 500 Mhz-km	550 m at 400 Mhz-km	10 km
SX	275 m at 200 Mhz-km	550 m at 500 Mhz-km	—	—	—

Use only Cisco-certified SFP modules on the adaptive security appliance. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the adaptive security appliance.

Note Only SFP modules certified by Cisco are supported on the adaptive security appliance.

Caution Protect your SFP modules by inserting clean port plugs into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules: The optics do not work correctly when obstructed with dust.

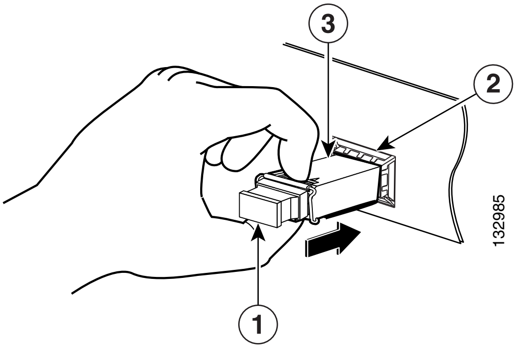
Warning **Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 70

Installing an SFP Module

To install an SFP module in a fiber port in Slot 1, perform the following steps:

Step 1 Line up the SFP module with the port and slide the SFP module into the port slot until it locks into position as shown in Figure 3-4.

Figure 3-4 Installing an SFP Module



1	Port plug	3	SFP module
2	Port slot		

Caution Do not remove the port plugs from the SFP module until you are ready to connect the cables.

Step 2 Remove the port plug; then connect the network cable to the SFP module.

Step 3 Connect the other end of the cable to your network. For more information on connecting the cables, see Chapter 3, "Connecting Interface Cables."

Caution The latching mechanism used on many SFP modules locks them into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP module.

Ports and LEDs

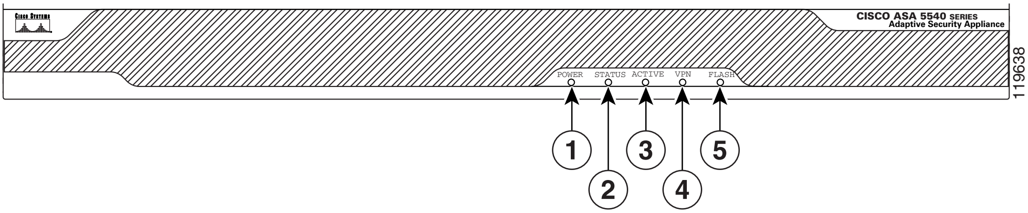
This section describes the front and rear panels. Figure 3-5 shows the front panel LEDs. This section includes the following topics:

- Front Panel LEDs, page 3-9
- Rear Panel LEDs and Ports in Slot 0, page 3-10
- Ports and LEDs in Slot 1, page 3-12

Front Panel LEDs

Figure 3-5 shows the LEDs on the front panel of the adaptive security appliance.

Figure 3-5 Front Panel LEDs



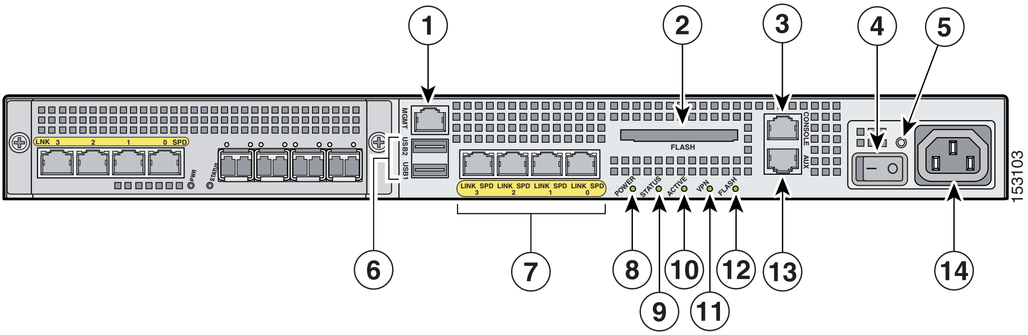
	LED	Color	State	Description
1	Power	Green	On	The system has power.

	LED	Color	State	Description
2	Status	Green	Flashing	The power-up diagnostics are running or the system is booting.
			Solid	The system has passed power-up diagnostics.
		Amber	Solid	The power-up diagnostics have failed.
3	Active	Green	Flashing	There is network activity.
4	VPN	Green	Solid	VPN tunnel is established.
5	Flash	Green	Solid	The CompactFlash is being accessed.

Rear Panel LEDs and Ports in Slot 0

Figure 3-6 shows the rear panel LEDs and ports in Slot 0.

Figure 3-6 Rear Panel LEDs and Ports on Slot 0 (AC Power Supply Model Shown)



1	Management Port[1]	**6**	USB 2.0 interfaces[2]	**11**	VPN LED
2	External CompactFlash slot	**7**	Network interfaces[3]	**12**	Flash LED
3	Serial Console port	**8**	Power indicator LED	**13**	AUX port
4	Power switch	**9**	Status indicator LED	**14**	Power connector
5	Power indicator LED	**10**	Active LED		

[1] The management 0/0 interface is a Fast Ethernet interface designed for management traffic only.

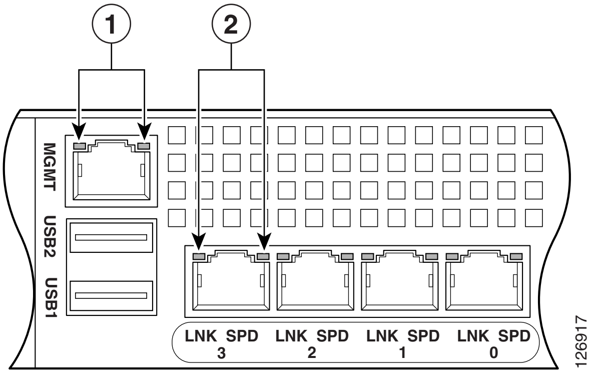
[2] Reserved for future use.

3. GigabiteEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

For more information on the Management Port, see the **management-only** command in the *Cisco ASA 5500 Series Command Reference*.

Figure 3-7 shows the adaptive security appliance rear panel LEDs.

Figure 3-7 Rear Panel Link and Speed Indicator LEDs



1	MGMT indicator LEDs	**2**	Network interface LEDs

Table 3-3 lists the rear MGMT and Network interface LEDs.

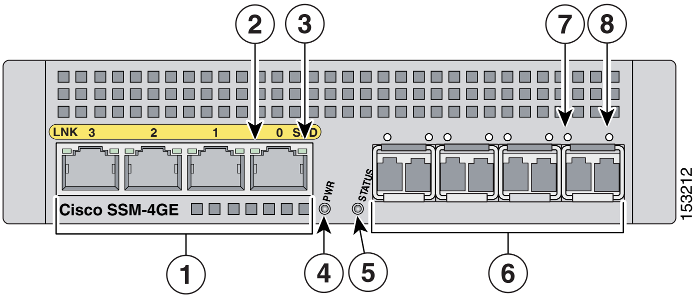
Table 3-3 Link and Speed LEDs

Indicator	Color	Description
Left side	Solid green	Physical link
	Green flashing	Network activity
Right side	Not lit	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps

Ports and LEDs in Slot 1

Figure 3-8 illustrates the ports and LEDs in Slot 1.

Figure 3-8 Ports and LEDs in Slot 1



1	Copper Ethernet ports	**5**	Status LED
2	RJ-45 Link LED	**6**	Fiber Ethernet ports
3	RJ-45 Speed LED	**7**	SFP Link LED
4	Power LED	**8**	SFP Speed LED

Note Figure 3-8 shows SFP modules installed in the fiber Ethernet ports. You must order and install the SFP modules if you want to establish fiber Ethernet connectivity. For more information on fiber ports and SFP modules, see the "Installing SFP Modules" section on page 3-6.

Table 3-4 describes the LEDs in Slot 1.

Table 3-4 LEDs on Bus G1

	LED	Color	State	Description
2, 7	LINK	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.

Table 3-4 LEDs on Bus G1 (continued)

	LED	Color	State	Description
3, 8	SPEED	Off	10 MB	There is no network activity.
		Green	100 MB	There is network activity at 100 Mbps.
		Amber	1000 MB (GigE)	There is network activity at 1000 Mbps.
4	POWER	Green	On	The system has power.
5	STATUS	Green	Flashing	The system is booting.
		Green	Solid	The system booted correctly.
		Amber	Solid	The system diagnostics failed.

Connecting Interface Cables

This section describes how to connect the appropriate cables to the Console, Auxiliary, Management, copper Ethernet, and fiber Ethernet ports.

To connect cables to the network interfaces, perform the following steps:

Step 1 Place the chassis on a flat, stable surface, or in a rack (if you are rack-mounting it).

Step 2 Connect to the Management port.

The adaptive security appliance has a dedicated interface for device management that is referred to as the Management0/0 port. The Management0/0 port is a Fast Ethernet interface. This port is similar to the Console port, but the Management0/0 port only accepts incoming traffic to the adaptive security appliance.

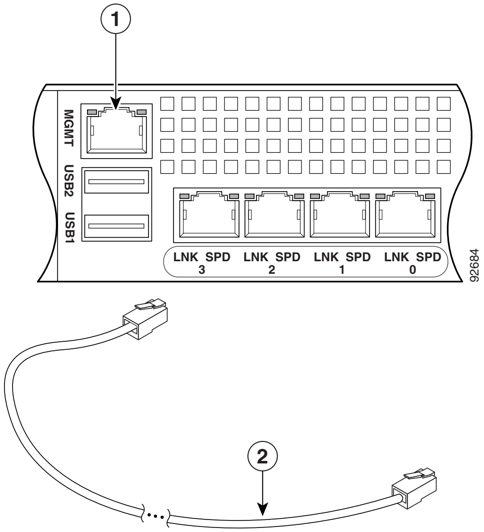
Note You can configure any interface to be a management-only interface using the **management-only** command. You can also disable management-only mode on the management interface. For more information about this command, see the **management-only** command in the *Cisco ASA 5500 Series Command Reference*.

a. Locate an Ethernet cable, which has an RJ-45 connector on each end.

b. Connect one RJ-45 connector to the Management0/0 port, as shown in Figure 3-9.

c. Connect the other end of the Ethernet cable to the Ethernet port on your computer or to your management network.

Figure 3-9 Connecting to the Management Port



1	Management port	**2**	RJ-45 to RJ-45 Ethernet cable

Step 3 Connect to the Console port.

a. Before connecting a computer or terminal to any ports, check to determine the baud rate of the serial port. The baud rate of the computer or terminal must match the default baud rate (9600 baud) of the Console port of the adaptive security appliance.

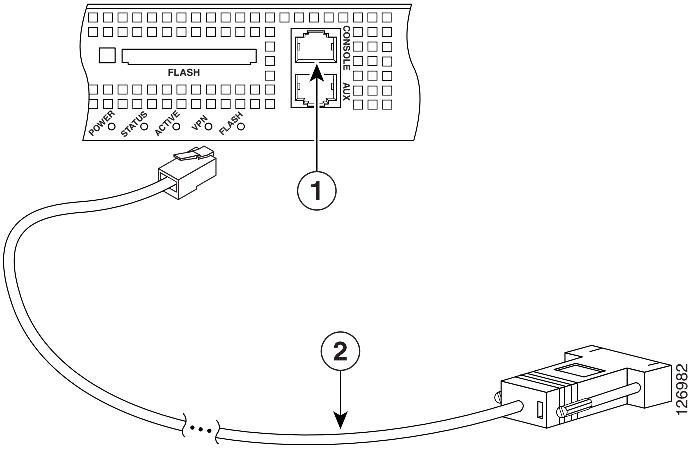
Set up the terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and Flow Control (FC) = Hardware.

b. Locate the serial console cable, which has an RJ-45 connector on one end and a DB-9 connector on the other end for the serial port on your computer.

c. Connect the RJ-45 connector to the Console port of the adaptive security appliance as shown in Figure 3-10.

d. Connect the DB-9 connector to the console port on your computer.

Figure 3-10 Connecting the Console Cable



1	RJ-45 Console port	**2**	RJ-45 to DB-9 console cable

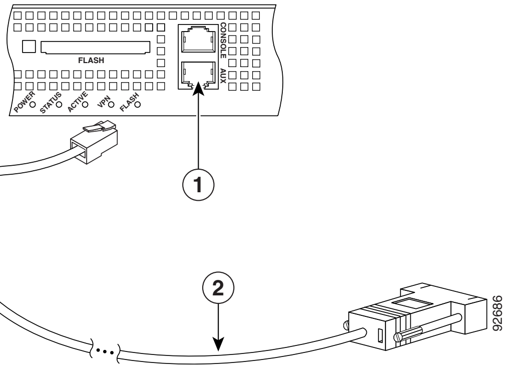
Step 4 Connect to the Auxiliary port (labeled AUX).

a. Locate the serial console cable, which has an RJ-45 connector on one end and a DB-9 connector on the other end for the serial port on your computer.

b. Connect the RJ-45 connector of the cable to the Auxiliary port (labeled AUX) on the adaptive security appliance, as shown in Figure 3-11.

c. Connect the other end of the cable, the DB-9 connector, to the serial port on your computer.

Figure 3-11 Connecting to the AUX Port



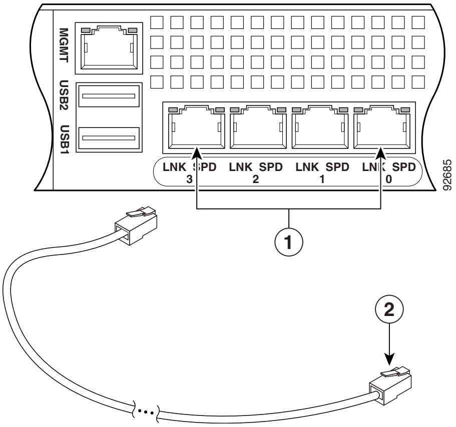
1	RJ-45 AUX port	2	RJ-45 to DB-9 console cable

Step 5 Connect to copper Ethernet ports to be used for network connections. Copper Ethernet ports are available both in Slot 0 and Slot 1.

Note You must use a port in Slot 0 for the inside interface, and a port in Slot 1 for the outside interface.

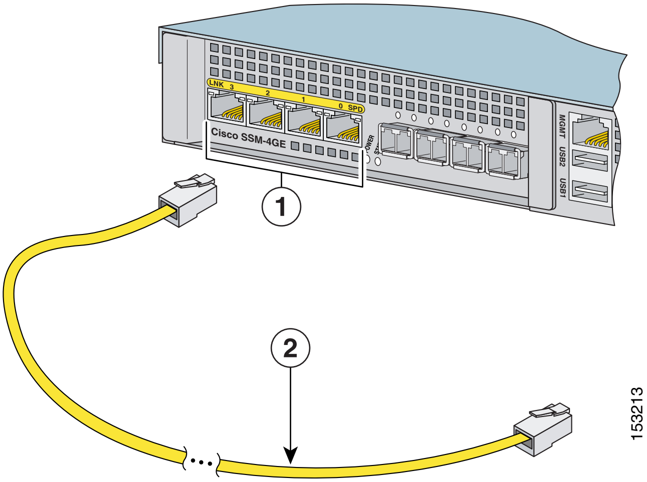
a. Connect one end of an Ethernet cable to a copper Ethernet port, as shown in Figure 3-12 and Figure 3-13.

Figure 3-12 Connecting to a Copper Ethernet Interface in Slot 0



1	Copper Ethernet ports	**2**	RJ-45 connector

Figure 3-13 Connecting to a Copper Ethernet Interfaces in Slot 1



1	Copper Ethernet ports	**2**	RJ-45 connector

b. Connect the other end of the Ethernet cable to a network device, such as a router, switch or hub.

Step 6 Connect to fiber Ethernet ports to be used for network connections.

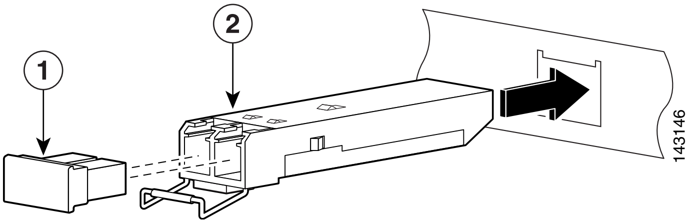
Note Slot 1 contains four copper Ethernet ports and four fiber Ethernet ports. You can use both types of ports, but you can only have a total of four Slot 1 ports in use at a time. For example, you could use two copper Ethernet ports and two fiber Ethernet ports.

For each fiber port you want to use, perform the following steps:

a. Install the SFP module:

- Insert and slide the SFP module into the fiber port until you hear a click. The click indicates that the SFP module is locked into the port.
- Remove the port plug from the installed SFP as shown in Figure 3-14.

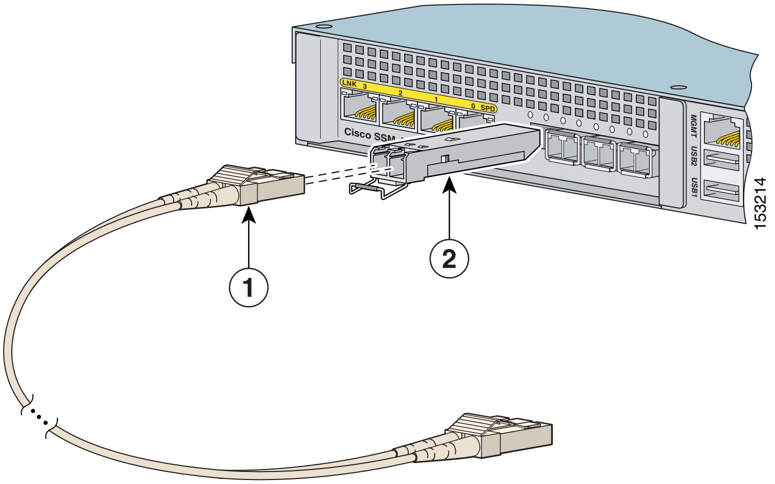
Figure 3-14 Removing the Fiber Port Plug



1	Port plug	**2**	SFP module

b. Connect the LC connector to the SFP module as shown in Figure 3-15.

Figure 3-15 Connecting the LC Connector



1	LC connector	2	SFP module

c. Connect the other end of the cable to a network device, such as a router, switch, or hub.

Step 7 Connect the power cord to the adaptive security appliance and plug the other end to the power source.

Step 8 Power on the chassis.

What to Do Next

Continue with Chapter 7, "Configuring the Adaptive Security Appliance."

CHAPTER 4

Installing the ASA 5500, ASA 5510, ASA 5520, and ASA 5540

Note This chapter does not apply to the ASA 5550.

Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 49

Caution Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

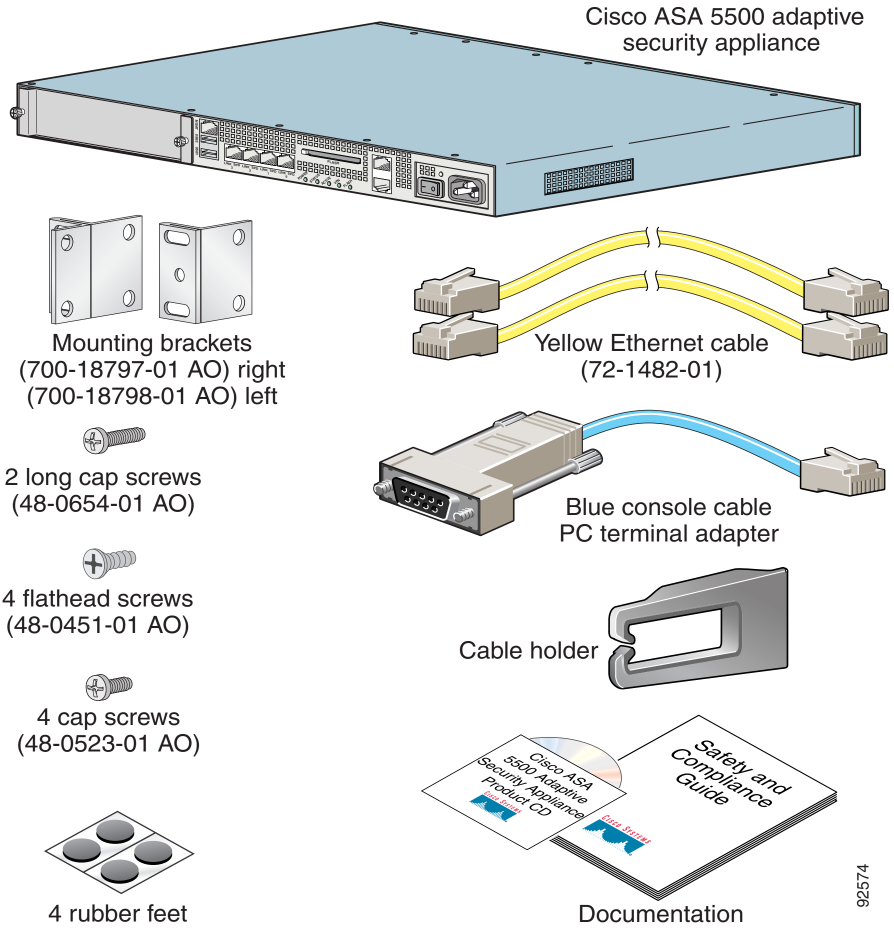
This chapter provides a product overview and describes the memory requirements, rack-mount, and installation procedures for the adaptive security appliance. This chapter includes the following sections:

Note The illustrations in this document show the Cisco ASA 5540 adaptive security appliance. The Cisco ASA 5510 adaptive security appliance and Cisco ASA 5520 adaptive security appliance are identical, containing the same back panel features and indicators.

Verifying the Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install your Cisco ASA 5500 series adaptive security appliance.

Figure 4-1 Contents of ASA 5500 Package


Cisco ASA 5500 adaptive security appliance
Mounting brackets (700-18797-01 AO) right (700-18798-01 AO) left
Yellow Ethernet cable (72-1482-01)
2 long cap screws (48-0654-01 AO)
Blue console cable PC terminal adapter
4 flathead screws (48-0451-01 AO)
Cable holder
4 cap screws (48-0523-01 AO)
Cisco ASA 5500 Adaptive Security Appliance Product CD
Safety and Compliance Guide
4 rubber feet
Documentation
92574

Installing the Chassis

This section describes how to rack-mount and install the adaptive security appliance. You can mount the adaptive security appliance in a 19-inch rack (with a 17.5- or 17.75-inch opening).

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety.**

The following information can help plan equipment rack installation:

- Allow clearance around the rack for maintenance.
- When mounting a device in an enclosed rack ensure adequate ventilation. An enclosed rack should never be overcrowded. Make sure that the rack is not congested, because each unit generates heat.
- When mounting a device in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- If the rack contains only one unit, mount the unit at the bottom of the rack.
- If the rack is partially filled, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If the rack contains stabilizing devices, install the stabilizers prior to mounting or servicing the unit in the rack.

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Rack-Mounting the Chassis

To rack-mount the chassis, perform the following steps:

Note You can use the mounting brackets to mount the chassis to the front or the back of the rack, with the front panel or the rear panel of the chassis facing outward.

Step 1 Attach the rack-mount brackets to the chassis using the supplied screws. Attach the brackets to the holes as shown in Figure 4-2 and Figure 4-3. After the brackets are secured to the chassis, you can rack-mount it.

Figure 4-2 Installing the Left Bracket on the Rear Panel of the Chassis

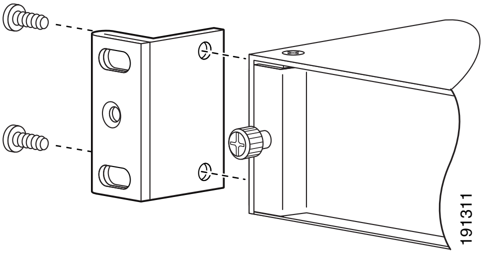
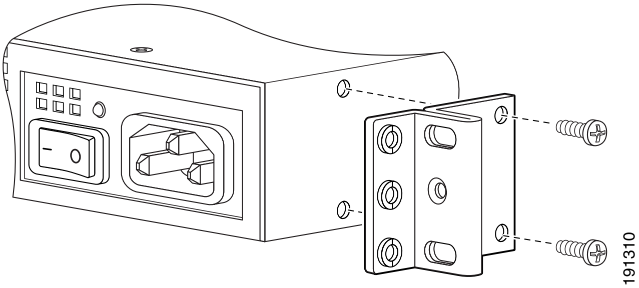
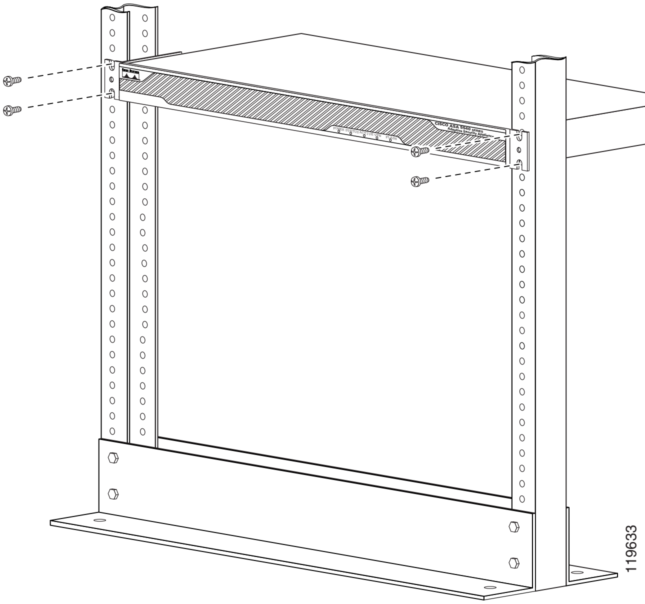


Figure 4-3 Installing the Right Bracket on the Rear Panel of the Chassis



Step 2 Attach the chassis to the rack using the supplied screws, as shown in Figure 4-4.

Figure 4-4 Rack-Mounting the Chassis



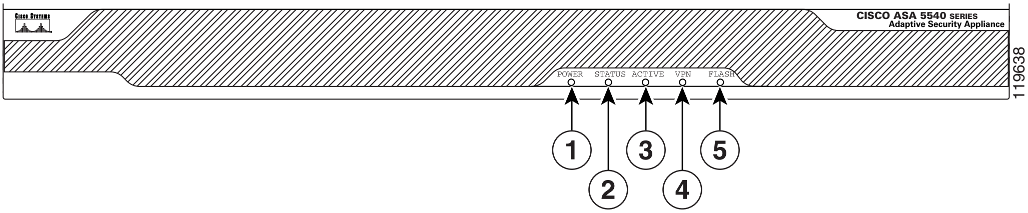
Note Figure 4-2 and Figure 4-3 show the rack mounting brackets attached to the rear of the chassis while Figure 4-4 shows the rack mounting brackets attached to the front of the chassis. You can attach the mounting brackets to the front or the rear of the chassis so that you can have the front panel or the rear panel of the chassis facing outward.
Figure 4-2 and Figure 4-3 show the brackets attached to the rear so you can see how that configuration appears while Figure 4-4 shows the brackets attached to the front so that you can see how that configuration appears. In Step 1 and Step 2, you will choose to have either the brackets rear mounted or front mounted but not both.

To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Ports and LEDs

This section describes the front and rear panels. Figure 4-5 shows the front panel LEDs.

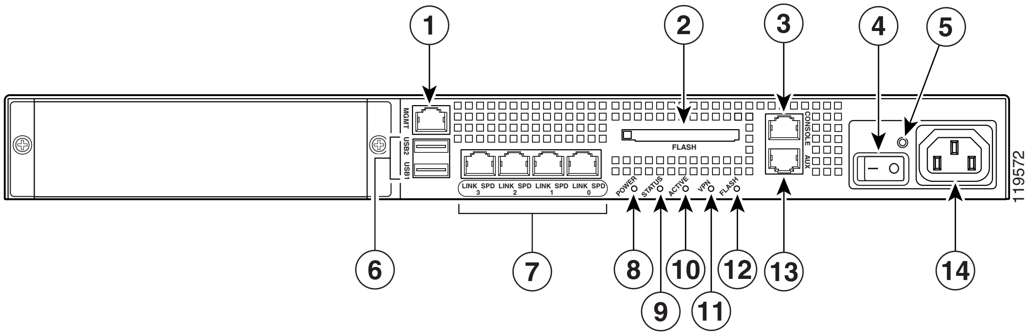
Figure 4-5 Front Panel LEDs



	LED	Color	State	Description
1	Power	Green	On	The system has power.
2	Status	Green	Flashing	The power-up diagnostics are running or the system is booting.
			Solid	The system has passed power-up diagnostics.
		Amber	Solid	The power-up diagnostics have failed.
3	Active	Green	Solid	This is the active failover device.
		Amber	Solid	This is the standby failover device.
4	VPN	Green	Solid	VPN tunnel is established.
5	Flash	Green	Solid	The CompactFlash is being accessed.

Figure 4-6 shows the rear panel features for the adaptive security appliance.

Figure 4-6 Rear Panel LEDs and Ports (AC Power Supply Model Shown)



1	Management Port[1]	**6**	USB 2.0 interfaces[2]	**11**	VPN LED
2	External CompactFlash slot	**7**	Network interfaces[3]	**12**	Flash LED
3	Serial Console port	**8**	Power indicator LED	**13**	AUX port
4	Power switch	**9**	Status indicator LED	**14**	Power connector
5	Power indicator LED	**10**	Active LED		

[1] The management 0/0 interface is a Fast Ethernet interface designed for management traffic only.

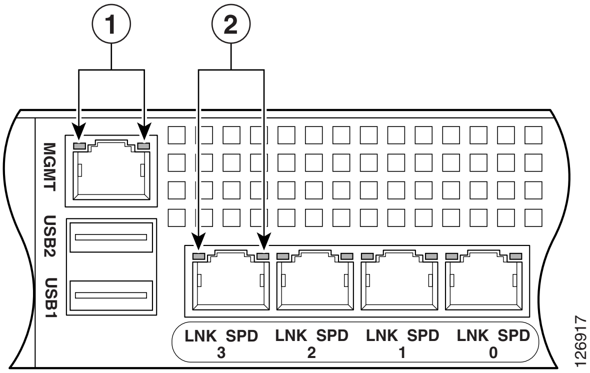
[2] Not supported at this time.

[3] GigabiteEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

For more information on the Management Port, see the "Management-Only" section in the *Cisco ASA 5500 Series Command Reference.*

Figure 4-7 shows the adaptive security appliance rear panel LEDs.

Figure 4-7 Rear Panel Link and Speed Indicator LEDs



1	MGMT indicator LEDs	**2**	Network interface LEDs

Table 4-1 lists the rear MGMT and Network interface LEDs.

Table 4-1 Link and Speed LEDs

Indicator	Color	Description
Left side	Solid green Green flashing	Physical link Network activity
Right side	Not lit Green Amber	10 Mbps 100 Mbps 1000 Mbps

Note The ASA 5510 adaptive security appliance only supports 10/100BaseTX. The ASA 5520 adaptive security appliance and the ASA 5540 adaptive security appliance support 1000BaseT.

What to Do Next

Continue with one of the following chapters.

To Do This...	See ..
Install SSMs you purchased but that have not yet been installed	Chapter 5, "Installing Optional SSMs"
Continue with connecting interface cables	Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms"

CHAPTER 5

Installing Optional SSMs

Note This chapter does not apply to the ASA 5550.

This chapter provides information about installing optional SSMs (Security Services Modules) and their components. You only need to use the procedures in this chapter if you purchased an optional SSM and it is not yet installed.

This chapter includes the following sections:

- Cisco 4GE SSM, page 5-1
- Cisco AIP SSM and CSC SSM, page 5-8
- What to Do Next, page 5-10

Cisco 4GE SSM

The 4GE Security Services Module (SSM) has eight Ethernet ports: four 10/100/1000 Mbps, copper, RJ-45 ports or four optional 1000 Mbps, Small Form-Factor Pluggable (SFP) fiber ports.

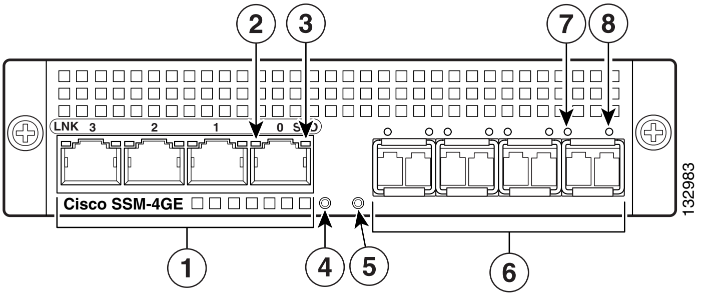
This section describes how to install and replace the Cisco 4GE SSM in the adaptive security appliance. This section includes the following topics:

- 4GE SSM Components, page 5-2
- Installing the Cisco 4GE SSM, page 5-3
- Installing the SFP Modules, page 5-4

4GE SSM Components

Figure 5-1 lists the Cisco 4GE SSM ports and LEDs.

Figure 5-1 Cisco 4GE SSM Ports and LEDs



1	RJ-45 ports	**5**	Status LED
2	RJ-45 Link LED	**6**	SFP ports
3	RJ-45 Speed LED	**7**	SFP Link LED
4	Power LED	**8**	SFP Speed LED

Note Figure 5-1 shows SFP modules installed in the port slots. You must order and install the SFP modules if you want to use this feature. For more information on SFP ports and modules, see the "Installing the SFP Modules" section on page 5-4.

Table 5-1 describes the Cisco 4GE SSM LEDs.

Table 5-1 Cisco 4GE SSM LEDs

	LED	Color	State	Description
2, 7	LINK	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.

Table 5-1 Cisco 4GE SSM LEDs (continued)

	LED	Color	State	Description
3, 8	SPEED	Off Green Amber	10 MB	There is no network activity.
			100 MB	There is network activity at 100 Mbps.
			1000 MB (GigE)	There is network activity at 1000 Mbps.
4	POWER	Green	On	The system has power.
5	STATUS	Green	Flashing	The system is booting.
		Green	Solid	The system booted correctly.
		Amber	Solid	The system diagnostics failed.

Installing the Cisco 4GE SSM

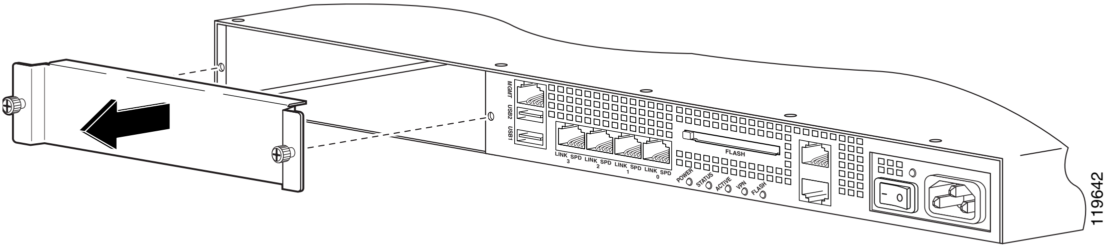
To install a new Cisco 4GE SSM for the first time, perform the following steps:

Step 1 Power off the adaptive security appliance.

Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

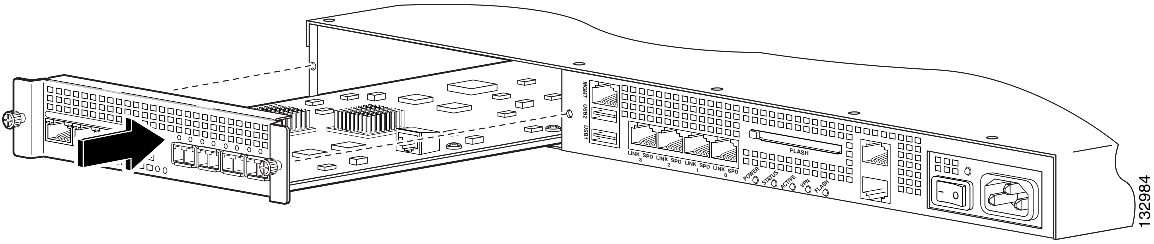
Step 3 Remove the two screws (as shown in Figure 5-2) at the left rear end of the chassis, and remove the slot cover.

Figure 5-2 Removing the Screws from the Slot Cover



Step 4 Insert the Cisco 4GE SSM through the slot opening as shown in Figure 5-3.

Figure 5-3 Inserting the Cisco 4GE SSM into the Slot



Step 5 Attach the screws to secure the Cisco 4GE SSM to the chassis.

Step 6 Power on the adaptive security appliance.

Step 7 Check the LEDs. If the Cisco 4GE SSM is installed properly the STATUS LED flashes during boot up and is solid when operational.

Step 8 Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see Chapter 6, "Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms."

Installing the SFP Modules

The SFP (Small Form-Factor Pluggable) is a hot-swappable input/output device that plugs into the SFP ports. The following SFP module types are supported:

- Long wavelength/long haul 1000BASE-LX/LH (GLC-LH-SM=)
- Short wavelength 1000BASE-SX (GLC-SX-MM=)

This section describes how to install and remove the SFP modules in the adaptive security appliance to provide optical Gigabit Ethernet connectivity. This section includes the following topics:

- SFP Module, page 5-5
- Installing the SFP Module, page 5-6

SFP Module

The adaptive security appliance uses a field-replaceable SFP module to establish Gigabit connections.

Note If you install an SFP module after the switch has powered on, you must reload the adaptive security appliance to enable the SFP module.

Table 5-2 lists the SFP modules that are supported by the adaptive security appliance.

Table 5-2 Supported SFP Modules

SFP Module	Type of Connection	Cisco Part Number
1000BASE-LX/LH	Fiber-optic	GLC-LH-SM=
1000BASE-SX	Fiber-optic	GLC-SX-MM=

The 1000BASE-LX/LH and 1000BASE-SX SFP modules are used to establish fiber-optic connections. Use fiber-optic cables with LC connectors to connect to an SFP module. The SFP modules support 850 to 1550 nm nominal wavelengths. The cables must not exceed the required cable length for reliable communications. Table 5-3 lists the cable length requirements.

Table 5-3 Cabling Requirements for Fiber-Optic SFP Modules

SFP Module	62.5/125 micron Multimode 850 nm Fiber	50/125 micron Multimode 850 nm Fiber	62.5/125 micron Multimode 1310 nm Fiber	50/125 micron Multimode 1310 nm Fiber	9/125 micron Single-mode 1310 nm Fiber
LX/LH	—	—	550 m at 500 Mhz-km	550 m at 400 Mhz-km	10 km
SX	275 m at 200 Mhz-km	550 m at 500 Mhz-km	—	—	—

Use only Cisco certified SFP modules on the adaptive security appliance. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the adaptive security appliance.

Note Only SFP modules certified by Cisco are supported on the adaptive security appliance.

Caution Protect your SFP modules by inserting clean dust plugs into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back in the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules: The optics do not work correctly when obstructed with dust.

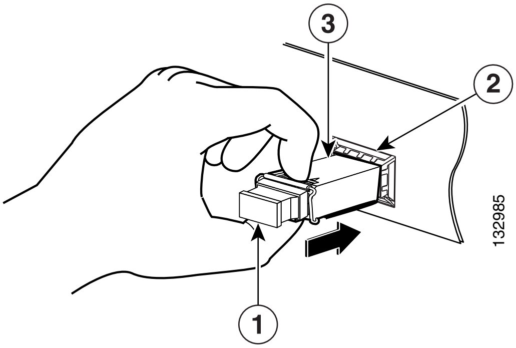
Warning **Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 70

Installing the SFP Module

To install the SFP module in the Cisco 4GE SSM, perform the following steps:

Step 1 Line up the SFP module with the port and slide the SFP module into the port slot until it locks into position as shown in Figure 5-4.

Figure 5-4 Installing an SFP Module



1	Optical port plug	**3**	SFP module
2	SFP port slot		

⚠ **Caution** Do not remove the optical port plugs from the SFP until you are ready to connect the cables.

Step 2 Remove the Optical port plug; then connect the network cable to the SFP module.

Step 3 Connect the other end of the cable to your network. For more information on connecting the cables, see Chapter 6, “Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms.”

⚠ **Caution** The latching mechanism used on many SFPs locks them into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP.

Cisco AIP SSM and CSC SSM

The ASA 5500 series adaptive security appliance supports the AIP SSM (Advanced Inspection and Prevention Security Services Module) and the CSC SSM (Content Security Control Security Services Module), also referred to as the intelligent SSM.

The AIP SSM runs advanced IPS software that provides security inspection. There are two models of the AIP SSM: the AIP SSM 10 and the AIP SSM 20. Both types look identical, but the AIP SSM 20 has a faster processor and more memory than the AIP SSM 10. Only one module (the AIP SSM 10 or the AIP SSM 20) can populate the slot at a time.

Table 5-4 lists the memory specifications for the AIP SSM 10 and the AIP SSM 20.

Table 5-4 SSM Memory Specifications

SSM	CPU	DRAM
AIP SSM 10	2.0 GHz Celeron	1.0 GB
AIP SSM 20	2.4 GHz Pentium 4	2.0 GB

For more information on the AIP SSM, see the *Cisco ASA 5500 Series Configuration Guide using the CLI.*

The CSC SSM runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. For more information on the CSC SSM, see the *Cisco ASA 5500 Series Configuration Guide using the CLI.*

This section describes how to install and replace the SSM in the adaptive security appliance. Figure 5-5 lists the SSM LEDs.

Figure 5-5 SSM LEDs

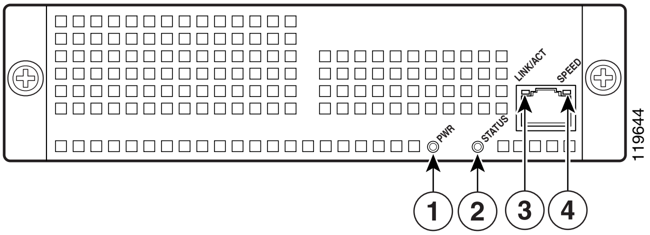


Table 5-5 describes the SSM LEDs.

Table 5-5 SSM LEDs

	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green	Flashing	The system is booting.
			Solid	The system has passed power-up diagnostics.
3	LINK/ACT	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Green	100 MB	There is network activity.
		Amber	1000 MB (GigE)	There is network activity.

Installing an SSM

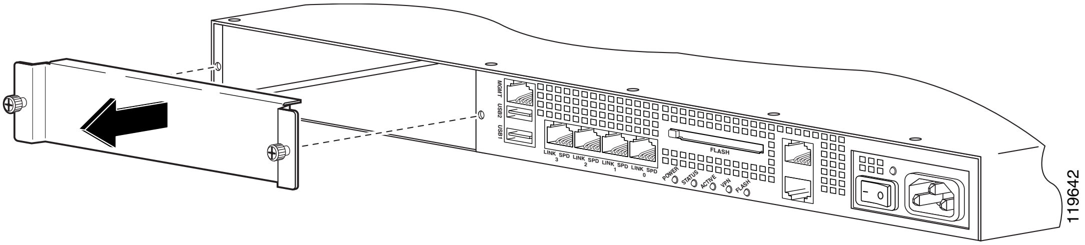
To install a new SSM, perform the following steps:

Step 1 Power off the adaptive security appliance.

Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

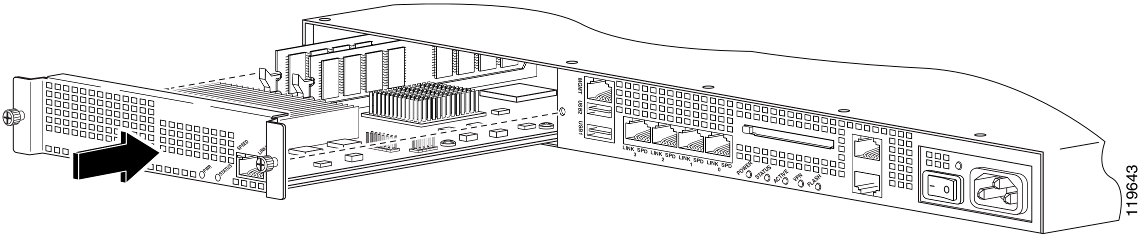
Step 3 Remove the two screws (as shown in Figure 5-6) at the left rear end of the chassis, and remove the slot cover.

Figure 5-6 Removing the Screws from the Slot Cover



Step 4 Insert the SSM into the slot opening as shown in Figure 5-7.

Figure 5-7 Inserting the SSM into the Slot



Step 5 Attach the screws to secure the SSM to the chassis.

Step 6 Power on the adaptive security appliance. Check the LEDs. If the SSM is installed properly, the POWER LED is solid green and the STATUS LED flashes green.

Step 7 Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices.

What to Do Next

Continue with Chapter 6, “Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms.”

CHAPTER 6

Connecting Interface Cables on the ASA 5500, ASA 5510, ASA 5520, and ASA 5540 Platforms

Note This chapter does not apply to the ASA 5550.

This chapter describes how to connect the cables to the Console, Auxiliary, Management, 4GE SSM, and SSM ports. In this document, SSM refers to an intelligent SSM, the AIP SSM, or CSC SSM.

Note The 4GE SSM, AIP SSM, and CSC SSM are optional security services modules. If your adaptive security appliance does not include these modules, continue with Chapter 7, "Configuring the Adaptive Security Appliance."

Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 49

Caution Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

This chapter includes the following sections:

Connecting Interface Cables

This section describes how to connect the appropriate cables to the Console, Management, copper Ethernet, and fiber Ethernet ports.

Note The RJ-45 Auxiliary port (labeled AUX on the chassis) is reserved for internal use at Cisco. The port is not functional in shipping versions of the chassis; therefore, customers cannot connect to this port to run the adaptive security appliance CLI.

To connect cables to the network interfaces, perform the following steps:

Step 1 Place the chassis on a flat, stable surface, or in a rack (if you are rack-mounting it).

Step 2 Connect to the Management port.

The adaptive security appliance has a dedicated interface for device management that is referred to as the Management0/0 port. The Management0/0 port is a Fast Ethernet interface. This port is similar to the Console port, but the Management0/0 port only accepts incoming traffic to the adaptive security appliance.

Note You can configure any interface to be a management-only interface using the **management-only** command. You can also disable management-only mode on the management interface. For more information about this command, see the **management-only** command in the *Cisco ASA 5500 Series Command Reference*.

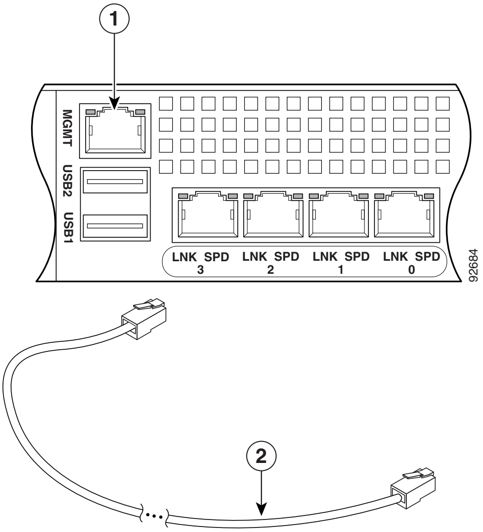
a. Locate an Ethernet cable, which has an RJ-45 connector on each end.

b. Connect one RJ-45 connector to the Management0/0 port, as shown in Figure 6-1.

c. Connect the other end of the Ethernet cable to the Ethernet port on your computer or to your management network.

Note When connecting a computer directly to the management port on the adaptive security appliance, use a crossover Ethernet cable. When connecting a computer to the adaptive security appliance through a hub or switch, use a straight through Ethernet cable to connect the hub or switch to the management port.

Figure 6-1 Connecting to the Management Port



1	Management port	**2**	RJ-45 to RJ-45 Ethernet cable

Step 3 Connect to the Console port.

a. Before connecting a computer or terminal to any ports, check to determine the baud rate of the serial port. The baud rate must match the default baud rate (9600 baud) of the Console port of the adaptive security appliance.

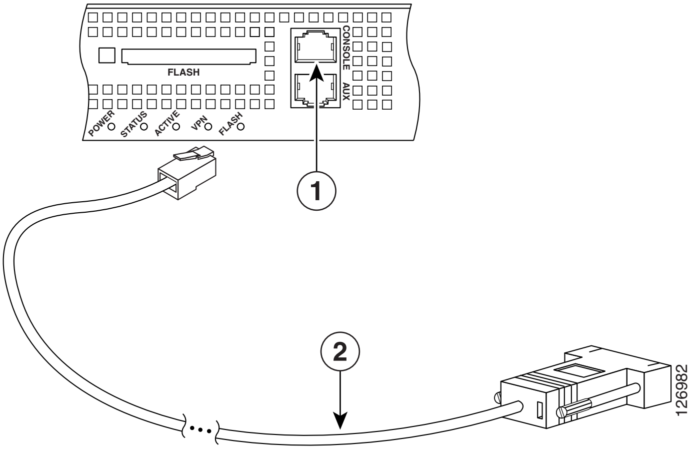
Set up the terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and Flow Control (FC) = Hardware.

b. Locate the serial console cable, which has an RJ-45 connector on one end and a DB-9 connector on the other end for the serial port on your computer.

c. Connect the RJ-45 connector to the Console port of the adaptive security appliance as shown in Figure 6-2.

d. Connect the DB-9 connector to the console port on your computer.

Figure 6-2 Connecting the Console Cable



1	RJ-45 Console port	**2**	RJ-45 to DB-9 console cable

Connecting to SSMs

SSMs are optional; this procedure is necessary only if you have installed an SSM on the adaptive security appliance.

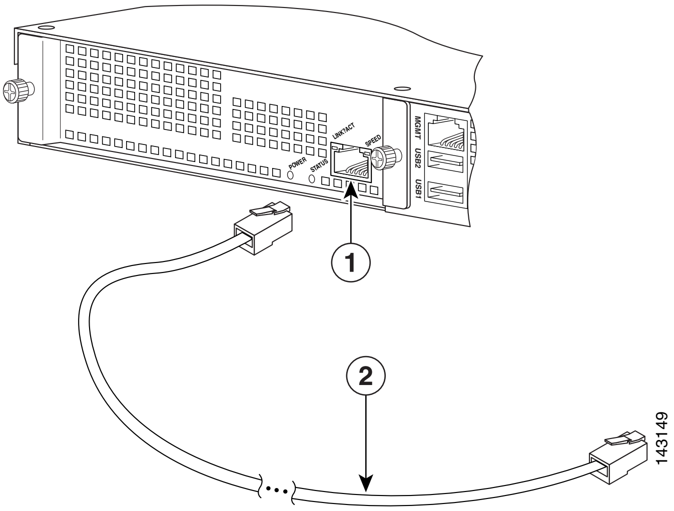
Note This procedure does not apply to the 4GE SSM. See Connecting to a 4GE SSM, page 6-6 for information about connecting to the 4GE SSM.

To connect to an SSM, perform the following steps:

Step 1 Connect one RJ-45 connector to the management port on the SSM, as shown in Figure 6-3.

Step 2 Connect the other end of the RJ-45 cable to your network devices.

Figure 6-3 Connecting to the SSM Management Port



1	SSM management port	2	RJ-45 to RJ-45 cable

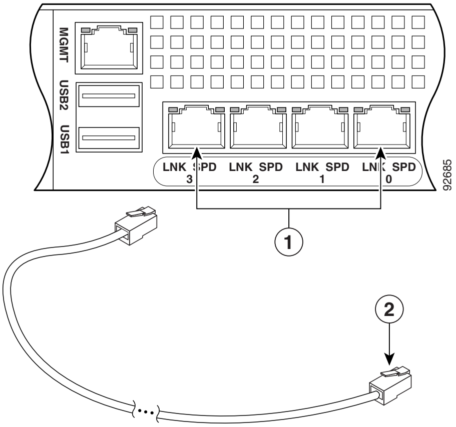
Step 3 Connect to Ethernet ports to be used for network connections.

a. Connect the RJ-45 connector to the Ethernet port.

b. Connect the other end of the Ethernet cable to your network device, such as a router, switch or hub.

Note You can use any unused Ethernet interface on the device as the failover link. The failover link interface is not configured as a normal networking interface; it should only be used for the failover link. You can connect the LAN-based failover link by using a dedicated switch with no hosts or routers on the link or by using a crossover Ethernet cable to link the units directly. For more information, see the Configuring Failover chapter in the *Cisco ASA 5500 Series Configuration Guide using the CLI*. See also Chapter 4, "Ports and LEDs"for information about the Ethernet interfaces.

Figure 6-4 Connecting Cables to Network Interfaces



1	RJ-45 Ethernet ports	**2**	RJ-45 connector

Connecting to a 4GE SSM

The 4GE SSM is optional; therefore, this step is necessary only if you have installed a 4GE SSM on the adaptive security appliance.

To connect to a 4GE SSM, perform the following steps:

Step 1 Connect to copper Ethernet ports to be used for network connections.

a. Connect one end of an Ethernet cable to a copper Ethernet port.

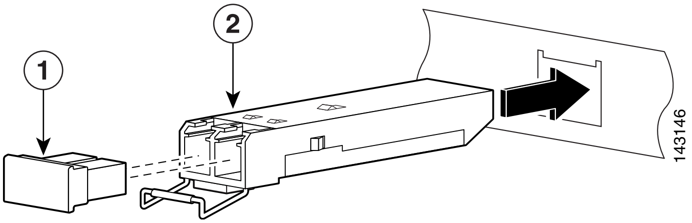
b. Connect the other end of the Ethernet cable to a network device, such as a router, switch or hub.

Step 2 Connect to fiber Ethernet ports to be used for network connections. For each fiber port you want to use, perform the following steps:

a. Install the SFP module:

- Insert and slide the SFP module into the fiber port until you hear a click. The click indicates that the SFP module is locked into the port.
- Remove the port plug from the installed SFP as shown in Figure 6-5.

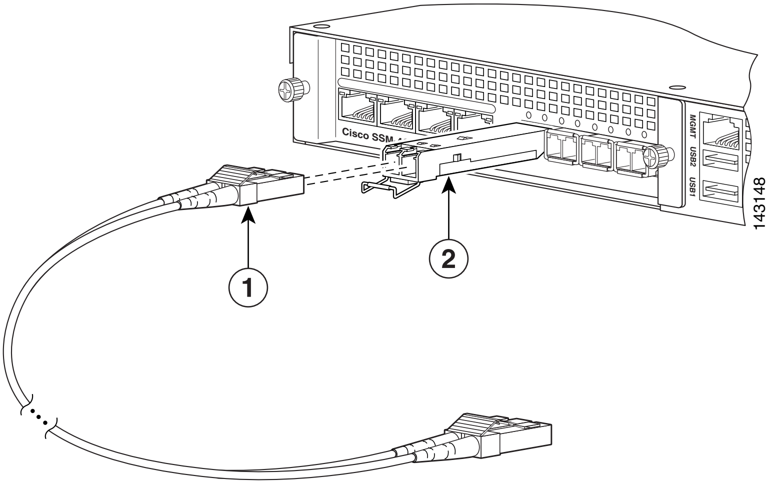
Figure 6-5 Removing the Fiber Port Plug



1	Port plug	2	SFP module

- Connect the LC connector to the SFP module as shown in Figure 6-6.

Figure 6-6 Connecting the LC Connector



b. Connect the other end of the cable to a network device, such as a router, switch, or hub.

Powering On the Adaptive Security Appliance

To power on the adaptive security appliance, perform the following steps:

Step 1 Connect the power cord to the adaptive security appliance and plug the other end to the power source.

Step 2 Power on the chassis.

What to Do Next

Continue with Chapter 7, "Configuring the Adaptive Security Appliance."

CHAPTER 7

Configuring the Adaptive Security Appliance

This chapter describes the initial configuration of the adaptive security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI). The procedures in this chapter describe how to configure the adaptive security appliance using ASDM.

This chapter includes the following sections:

About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. The ASA 5500 series comes preconfigured with the following:

- Two VLANs: VLAN 1 and VLAN2
- VLAN 1 has the following properties:
  - Named “inside”

  - Allocated switch ports Ethernet 0/1 through Ethernet 0/7
  - Security level of 100
  - Allocated switch ports Ethernet 0/1 through 0/7
  - IP address of 192.168.1.1 255.255.255.0
- VLAN2 has the following properties:
  - Named “outside”
  - Allocated switch port Ethernet 0/0
  - Security level of 0
  - Configured to obtain its IP address using DHCP
- Inside interface to connect to the device and use ASDM to complete your configuration.

By default, the adaptive security appliance Inside interface is configured with a default DHCP address pool. This configuration enables a client on the inside network to obtain a DHCP address from the adaptive security appliance to connect to the appliance. Administrators can then configure and manage the adaptive security appliance using ASDM.

Using the CLI for Configuration

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface.

You can get step-by-step examples of how to configure basic remote access and LAN-to-LAN connections in the CLI itself by using the **vpnsetup ipsec-remote-access steps** and **vpnsetup site-to-site steps** commands. For more information about these commands, see the *Cisco ASA 5500 Series Command Reference*.

For step-by-step configuration procedures for all functional areas of the adaptive security appliance, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Using the Adaptive Security Device Manager for Configuration

The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that allows you to manage and monitor the adaptive security appliance. The web-based design provides secure access so that you can connect to and manage the adaptive security appliance from any location by using a web browser.

Cisco Adaptive Security Device Manager

Version 6.3(1)

© 2001-2010 Cisco Systems, Inc.
All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

In addition to complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the adaptive security appliance.

This section includes the following topics:

- Preparing to Use ASDM, page 7-4
- Gathering Configuration Information for Initial Setup, page 7-4
- Installing the ASDM Launcher, page 7-5
- Starting ASDM with a Web Browser, page 7-8

Preparing to Use ASDM

Before you can use ASDM, perform the following steps:

Step 1 If you have not already done so, connect the MGMT interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.

Step 2 Configure your PC to use DHCP (to receive an IP address automatically from the adaptive security appliance), which enables the PC to communicate with the adaptive security appliance and the Internet as well as to run ASDM for configuration and management tasks.

Alternatively, you can assign a static IP address to your PC by selecting an address in the 192.168.1.0 subnet. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)

When you connect other devices to any of the inside ports, make sure that they do not have the same IP address.

Note The MGMT interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

Step 3 Check the LINK LED on the MGMT interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub turn solid green.

Gathering Configuration Information for Initial Setup

Gather the following information to be used with the ASDM Startup Wizard:

- A unique hostname to identify the adaptive security appliance on your network.
- The domain name.

- The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
- IP addresses for hosts that should have administrative access to this device using HTTPS for ASDM, SSH, or Telnet.
- The privileged mode password for administrative access.
- The IP addresses to use for NAT or PAT address translation, if any.
- The IP address range for the DHCP server.
- The IP address for the WINS server.
- Static routes to be configured.
- If you want to create a DMZ, you must create a third VLAN and assign ports to that VLAN. (By default, there are two VLANs configured.)
- Interface configuration information: whether traffic is permitted between interfaces at the same security level, and whether traffic is permitted between hosts on the same interface.
- If you are configuring an Easy VPN hardware client, the IP addresses of primary and secondary Easy VPN servers; whether the client is to run in client or network extension mode; and user and group login credentials to match those configured on the primary and secondary Easy VPN servers.

Installing the ASDM Launcher

You can launch ASDM in either of two ways: by downloading the ASDM Launcher software so that ASDM runs locally on your PC, or by enabling Java and JavaScript in your web browser and accessing ASDM remotely from your PC. This procedure describes how to set up your system to run ASDM locally.

To install the ASDM Launcher, perform the following steps:

Step 1 On the PC connected to the switch or hub, launch an Internet browser.

a. In the address field of the browser, enter this URL: **https://192.168.1.1/admin**.

Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the “**s**” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

The Cisco ASDM splash screen appears.

b. Click **Install ASDM Launcher and Run ASDM**.

c. In the dialog box that requires a username and password, leave both fields empty. Click **OK**.

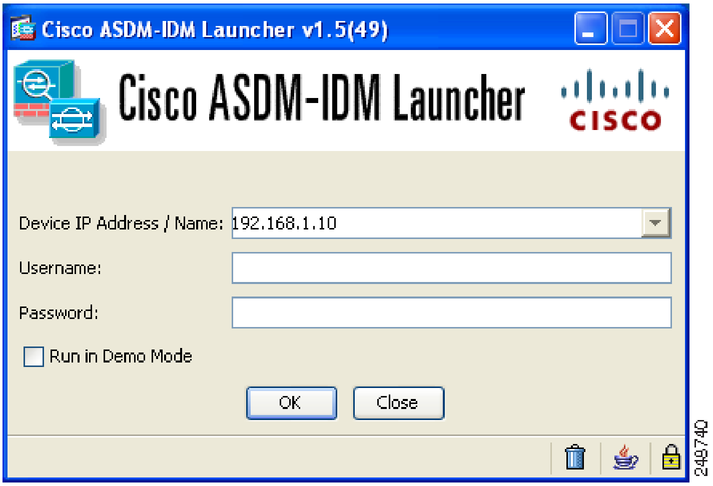
d. Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

e. When the File Download dialog box opens, click **Open** to run the installation program directly. It is not necessary to save the installation software to your hard drive.

f. When the InstallShield Wizard appears, follow the instructions to install the ASDM Launcher software.

Step 2 From your desktop, start the Cisco ASDM Launcher software.

A dialog box appears.



Device IP Address / Name: 192.168.1.10
Username:
Password:
□ Run in Demo Mode

Step 3 Enter the IP address or the host name of your adaptive security appliance.

Step 4 Enter the IP address or host name of your adaptive security appliance.

Step 5 Leave the Username and Password fields blank.

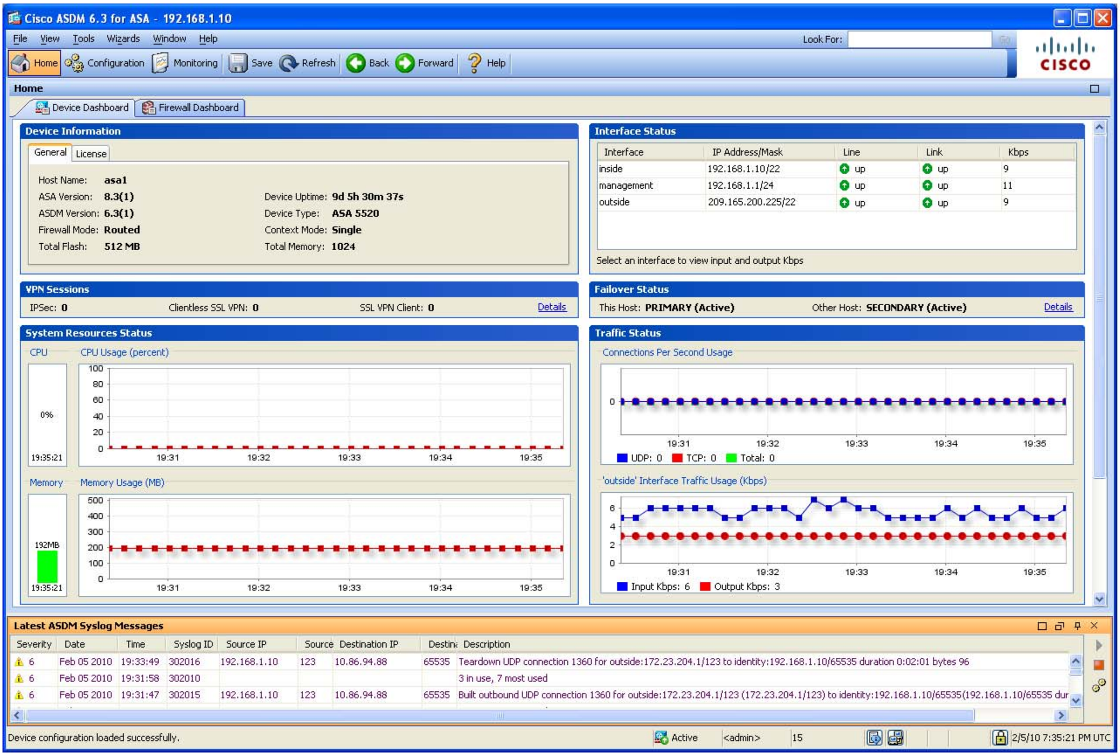
Note By default, there is no Username and Password set for the Cisco ASDM Launcher.

Step 6 Click **OK**.

Step 7 If you receive a security warning containing a request to accept a certificate, click **Yes**.

The ASA checks to see if there is updated software and if so, downloads it automatically.

The main ASDM window appears.



Device Information

General | License

Host Name: **asa1**
ASA Version: **8.3(1)**
ASDM Version: **6.3(1)**
Firewall Mode: **Routed**
Total Flash: **512 MB**
Device Uptime: **9d 5h 30m 37s**
Device Type: **ASA 5520**
Context Mode: **Single**
Total Memory: **1024**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.10/22	up	up	9
management	192.168.1.1/24	up	up	11
outside	209.165.200.225/22	up	up	9

Select an interface to view input and output Kbps

VPN Sessions

IPSec: **0** Clientless SSL VPN: **0** SSL VPN Client: **0** Details

Failover Status

This Host: **PRIMARY (Active)** Other Host: **SECONDARY (Active)** Details

System Resources Status

Traffic Status

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin:	Description
6	Feb 05 2010	19:33:49	302016	192.168.1.10	123	10.86.94.88	65535	Teardown UDP connection 1360 for outside:172.23.204.1/123 to identity:192.168.1.10/65535 duration 0:02:01 bytes 96
6	Feb 05 2010	19:31:58	302010					3 in use, 7 most used
6	Feb 05 2010	19:31:47	302015	192.168.1.10	123	10.86.94.88	65535	Built outbound UDP connection 1360 for outside:172.23.204.1/123 (172.23.204.1/123) to identity:192.168.1.10/65535(192.168.1.10/65535 dur

Device configuration loaded successfully. Active <admin> 15 2/5/10 7:35:21 PM UTC

248741

ASDM starts and the main window appears.

Starting ASDM with a Web Browser

To run ASDM in a web browser, enter the factory default IP address in the address field: **https://192.168.1.1/admin/**.

Note Remember to add the “**s**” in “**https**” or the connection fails. HTTP over SSL (HTTP) provides a secure connection between your browser and the adaptive security appliance.

The Main ASDM window appears.

Running the ASDM Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your adaptive security appliance. With a few steps, the Startup Wizard enables you to configure the adaptive security appliance so that it allows packets to flow securely between the inside network and the outside network.

To use the Startup Wizard to set up a basic configuration for the adaptive security appliance, perform the following steps:

Step 1 From the Wizards menu at the top of the ASDM window, choose Startup Wizard.

Step 2 Follow the instructions in the Startup Wizard to set up your adaptive security appliance.

For information about any field in the Startup Wizard, click **Help** at the bottom of the window.

Note If you get an error requesting a DES license or a 3DES-AES license, see Appendix A, “Obtaining a 3DES/AES License” for information.

Note Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using ASDM. From the ASDM main page, click **Configuration > Properties > ICMP Rules**. Add an entry for the outside interface. Set the IP address to 0.0.0.0, the netmask to 0.0.0.0, and Action to deny.

What to Do Next

Configure the adaptive security appliance for your deployment using one or more of the following chapters.

To Do This...	See...
Configure the adaptive security appliance to protect a DMZ web server	Chapter 8, “Scenario: DMZ Configuration”
Configure the adaptive security appliance for remote-access VPN	Chapter 9, “Scenario: IPsec Remote-Access VPN Configuration”
Configure the adaptive security appliance for SSL VPN connections using software clients	Chapter 10, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure the adaptive security appliance for SSL VPN connections using a web browser	Chapter 11, “Scenario: SSL VPN Clientless Connections”
Configure the adaptive security appliance for site-to-site VPN	Chapter 12, “Scenario: Site-to-Site VPN Configuration”

CHAPTER 8

Scenario: DMZ Configuration

A demilitarized zone (DMZ) is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

This chapter includes the following sections:

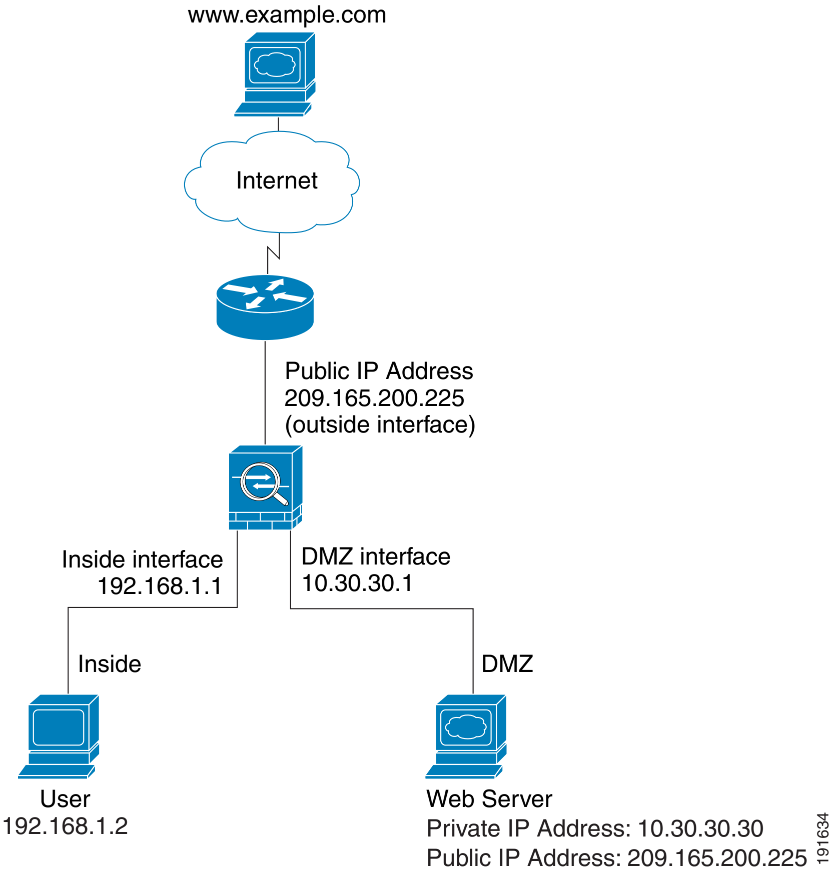
- Example DMZ Network Topology, page 8-1
- Configuring the Adaptive Security Appliance for a DMZ Deployment, page 8-8
- What to Do Next, page 8-23

Example DMZ Network Topology

The chapter describes how to configure a DMZ deployment of the adaptive security appliance as shown in Figure 8-1.

In this example, the web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server.

Figure 8-1 Network Layout for DMZ Configuration Scenario



This example scenario has the following characteristics:

- The web server is on the DMZ interface of the adaptive security appliance.
- Clients on the inside network can access the web server in the DMZ and can also communicate with devices on the Internet.
- Clients on the Internet are permitted HTTP access to the DMZ web server; all other traffic coming from the Internet is denied.
- The network has one IP address that is publicly available: the outside interface of the adaptive security appliance (209.165.200.225). This public address is shared by the adaptive security appliance and the DMZ web server.

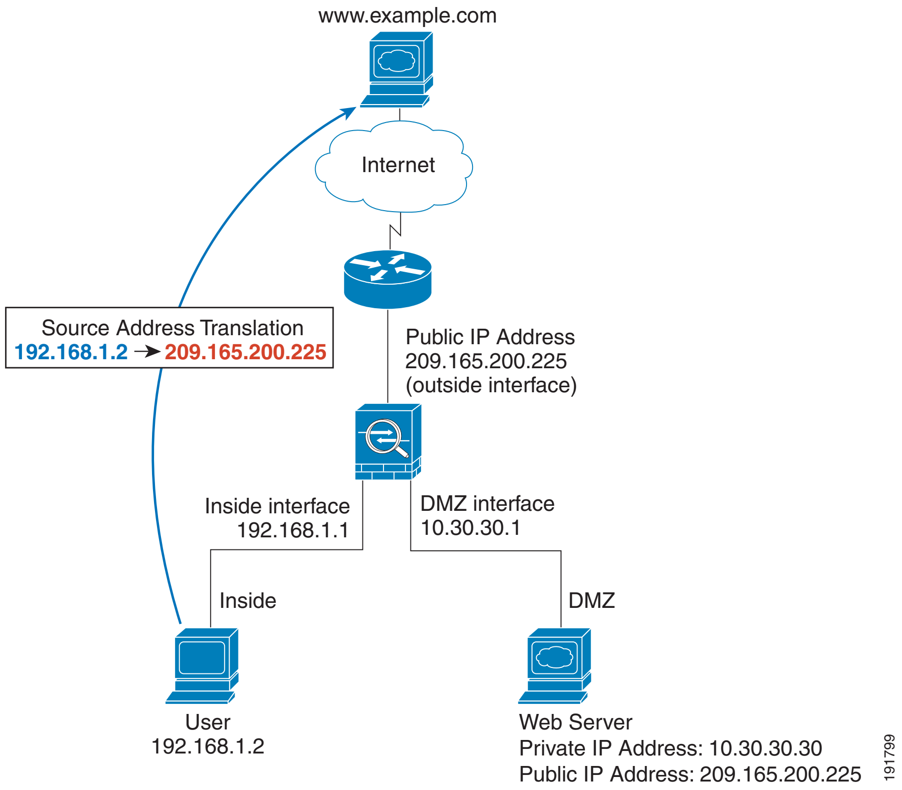
This section includes the following topics:

- An Inside User Visits a Web Server on the Internet, page 8-3
- An Internet User Visits the DMZ Web Server, page 8-4
- An Inside User Visits the DMZ Web Server, page 8-6

An Inside User Visits a Web Server on the Internet

Figure 8-2 shows the traffic flow through the adaptive security appliance when an inside user requests an HTTP page from a web server on the Internet.

Figure 8-2 An Inside User Visits an Internet Web Server



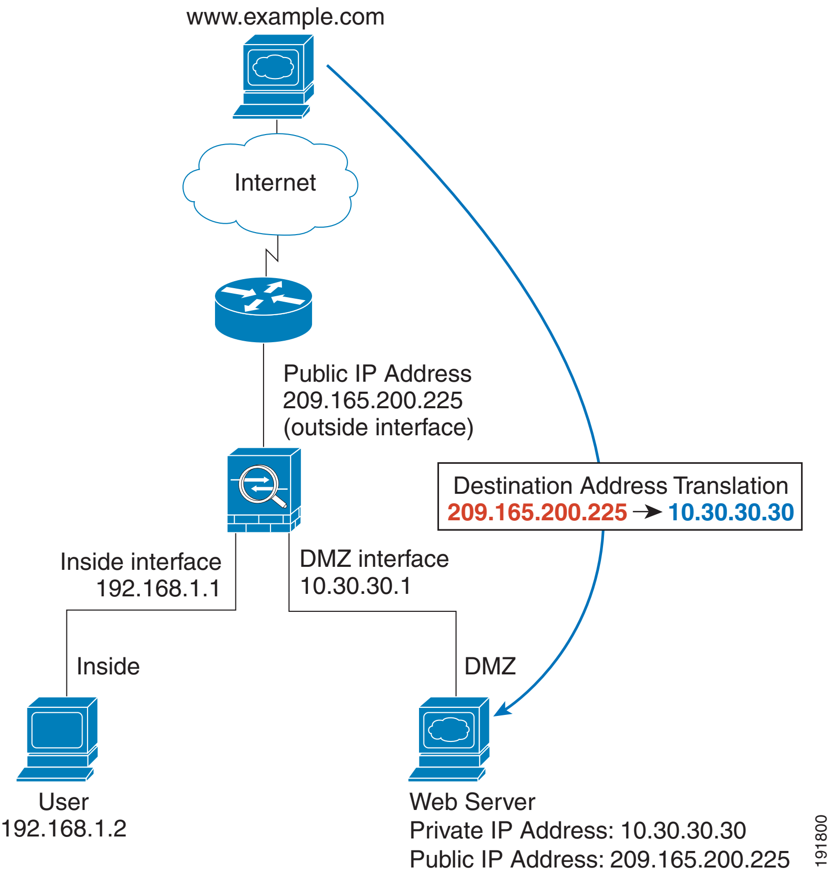
When an inside user requests an HTTP page from a web server on the Internet, data moves through the adaptive security appliance as follows:

1. The user on the inside network requests a web page from www.example.com.
2. The adaptive security appliance receives the packet and, because it is a new session, verifies that the packet is allowed.
3. The adaptive security appliance performs Network Address Translation (NAT) to translate the local source address (192.168.1.2) to the public address of the outside interface (209.165.200.225).
4. The adaptive security appliance records that a session is established and forwards the packet from the outside interface.
5. When www.example.com responds to the request, the packet goes through the adaptive security appliance using the established session.
6. The adaptive security appliance uses NAT to translate the public destination (209.165.200.225) address to the local user address, 192.168.1.2.
7. The adaptive security appliance forwards the packet to the inside user.

An Internet User Visits the DMZ Web Server

Figure 8-3 shows the traffic flow through the adaptive security appliance when a user on the Internet requests a web page from the DMZ web server.

Figure 8-3 An Outside User Visits the DMZ Web Server



When a user on the Internet requests an HTTP page from the DMZ web server, traffic flows through the adaptive security appliance as follows:

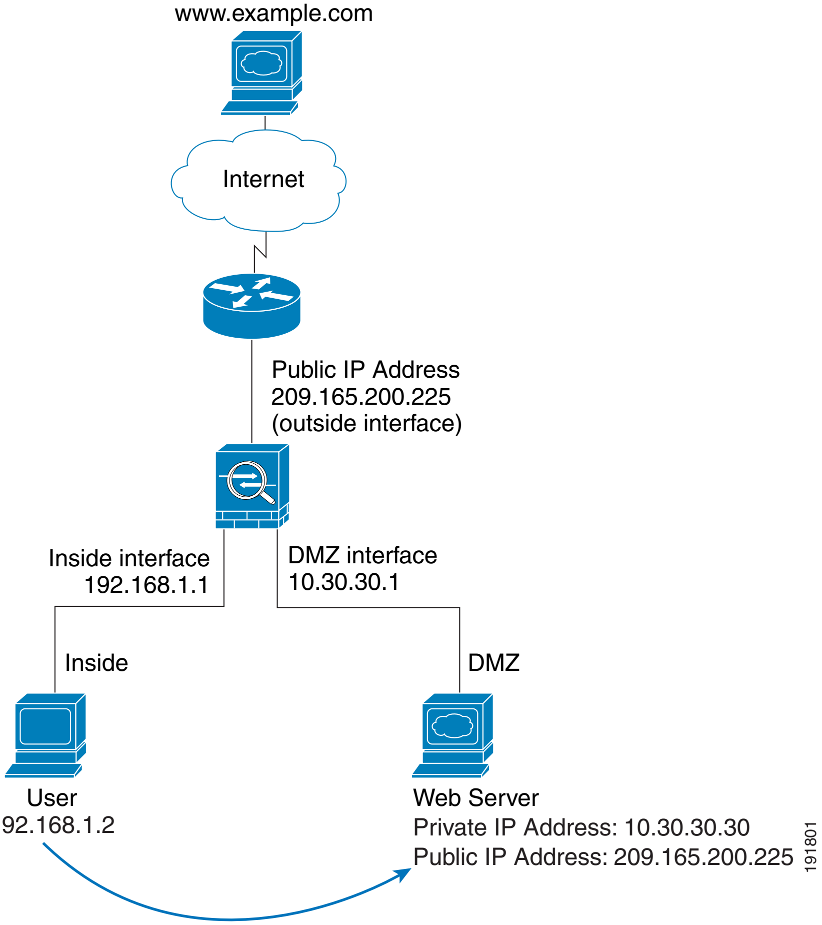
1. A user on the outside network requests a web page from the DMZ web server using the public IP address of the adaptive security appliance (209.165.200.225, the IP address of the outside interface).
2. The adaptive security appliance receives the packet and, because it is a new session, verifies that the packet is allowed.

3. The adaptive security appliance translates the destination address to the local address of the DMZ web server (10.30.30.30) and forwards the packet through the DMZ interface.
4. When the DMZ web server responds to the request, the adaptive security appliance translates the local address of the DMZ web server (10.30.30.30) to the public address of the DMZ web server (209.165.200.225).
5. The adaptive security appliance forwards the packet to the outside user.

An Inside User Visits the DMZ Web Server

Figure 8-4 shows an inside user accessing the DMZ web server.

Figure 8-4 An Inside User Visits a Web Server on the DMZ



In Figure 8-4, the adaptive security appliance permits HTTP traffic originating from inside clients and destined for the DMZ web server. Because the internal network does not include a DNS server, internal client requests for the DMZ web server are handled as follows:

1. A lookup request is sent to the DNS server of the ISP. The public IP address of the DMZ web server is returned to the client.

2. The internal client requests a web page from the public IP address of the DMZ web server. The adaptive security appliance receives the request on its inside interface.
3. The adaptive security appliance translates the public IP address of the DMZ web server to its real address (209.165.200.225 -> 10.30.30.30) and forwards the request out of its DMZ interface to the web server.
4. When the DMZ web server responds to the request, the adaptive security appliance receives the data on its DMZ interface and forwards the data out of its inside interface to the user.

The procedures for creating this configuration are detailed in the remainder of this chapter.

Configuring the Adaptive Security Appliance for a DMZ Deployment

This section describes how to use ASDM to configure the adaptive security appliance for the configuration scenario shown in Figure 8-1. The procedure uses sample parameters based on the scenario.

This configuration procedure assumes that the adaptive security appliance already has interfaces configured for the inside interface, the outside interface, and the DMZ interface. Be sure that the DMZ interface security level is set between 0 and 100. (A common choice is 50.)

Note If you need to set up interfaces on the adaptive security appliance, you can use the Startup Wizard in ASDM. For more information about using the Startup Wizard, see Chapter 7, “Configuring the Adaptive Security Appliance.”

The section includes the following topics:

- Configuration Requirements, page 8-9
- Information to Have Available, page 8-10
- Enabling Inside Clients to Communicate with Devices on the Internet, page 8-10

- Enabling Inside Clients to Communicate with Devices on the Internet, page 8-10
- Enabling Inside Clients to Communicate with the DMZ Web Server, page 8-10
- Configuring Static PAT for Public Access to the DMZ Web Server (Port Forwarding), page 8-17
- Providing Public HTTP Access to the DMZ Web Server, page 8-20

The remainder of this chapter provides instructions for how to implement this configuration.

Configuration Requirements

This DMZ deployment of the adaptive security appliance requires configuration rules as follows.

So That...	Create These Rules...
Internal clients can request information from web servers on the Internet	The adaptive security appliance comes with a default configuration that permits inside clients access to devices on the Internet. No additional configuration is required.
Internal clients can request information from the DMZ web server	• A NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to its public IP address (10.30.30.30 to 209.165.200.225). • A NAT rule between the inside and DMZ interfaces that translates the real addresses of the internal client network. In this scenario, the real IP address of the internal network is "translated" to itself, that is, the real IP address of the internal network is used when internal clients communicate with the DMZ web server (10.30.30.30).
External clients can request information from the DMZ web server	• An address translation rule between the outside and DMZ interfaces that translates the public IP address of the DMZ web server to its private IP address (209.165.200.225 to 10.30.30.30). • An access control rule permitting incoming HTTP traffic that is destined for the DMZ web server.

Information to Have Available

Before you begin this configuration procedure, gather the following information:

- Internal IP address of the server inside the DMZ that you want to make available to clients on the public network (in this scenario, a web server).
- Public IP addresses to be used for servers inside the DMZ. (Clients on the public network will use the public IP address to access the server inside the DMZ.)
- Client IP address to substitute for internal IP addresses in outgoing traffic (in this scenario the IP address of the outside interface). Outgoing client traffic will appear to come from this address so that the internal IP address is not exposed.

Enabling Inside Clients to Communicate with Devices on the Internet

To permit internal clients to request content from devices on the Internet, the adaptive security appliance translates the real IP addresses of internal clients to the external address of the outside interface (that is, the public IP address of the adaptive security appliance). Outgoing traffic appears to come from this address.

Enabling Inside Clients to Communicate with the DMZ Web Server

In this procedure, you configure the adaptive security appliance to allow internal clients to communicate securely with the web server in the DMZ. To accomplish this, you must configure a translation rule.

Configure a NAT rule between the DMZ and inside interfaces that translates the real IP address of the DMZ web server to its public IP address (10.30.30.30 to 209.165.200.225).

This is necessary because when an internal client sends a DNS lookup request, the DNS server returns the public IP address of the DMZ web server.

Note Because there is not a DNS server on the inside network, DNS requests must exit the adaptive security appliance to be resolved by a DNS server on the Internet.

This section includes the following topics:

- Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces, page 8-11
- Translating the Public Address of the Web Server to its Real Address on the Inside Interface, page 8-14

Translating Internal Client IP Addresses Between the Inside and DMZ Interfaces

To configure NAT to translate internal client IP addresses between the inside interface and the DMZ interface, perform the following steps:

Step 1 In the **Configuration** > **Firewall** > **NAT Rules** pane, click the green + (plus) icon and choose and choose **Add "Network Object" NAT Rule**.

The Add Network Object dialog box appears.

Step 2 Fill in the following values:

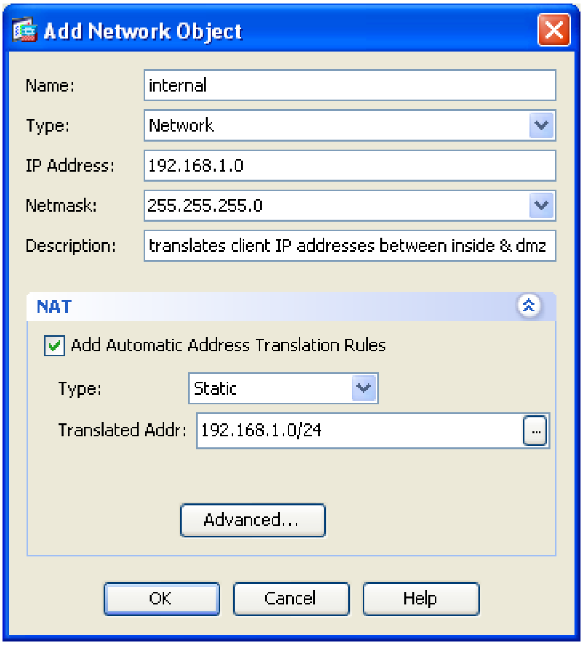
- In the Name field, enter the object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.
- From the Type drop-down list, choose Network.
- In the IP Address field, enter the real IP address of the client or network. In this scenario, the IP address of the network is 192.168.1.0.
- In the Netmask field, enter the subnet mask if the IP address is an IPv4 address, or enter the prefix if the IP address is an IPv6 address.
- (Optional) In the Description field, enter a description of the network object (up to 200 characters in length).

Note If the NAT section is hidden, click NAT to expand the section.

Step 3 Check the Add Automatic Translation Rules check box.

Step 4 From the Type drop-down list, choose Static.

Step 5 In the Translated Addr. field, enter the IP address of the internal client or network, or click ..., and choose an the address from the Browse Translated Addr dialog box. In the IP Address field, enter In this scenario, the IP address of the network is 192.168.1.0.



Add Network Object

Name: internal

Type: Network

IP Address: 192.168.1.0

Netmask: 255.255.255.0

Description: translates client IP addresses between inside & dmz

NAT

☑ Add Automatic Address Translation Rules

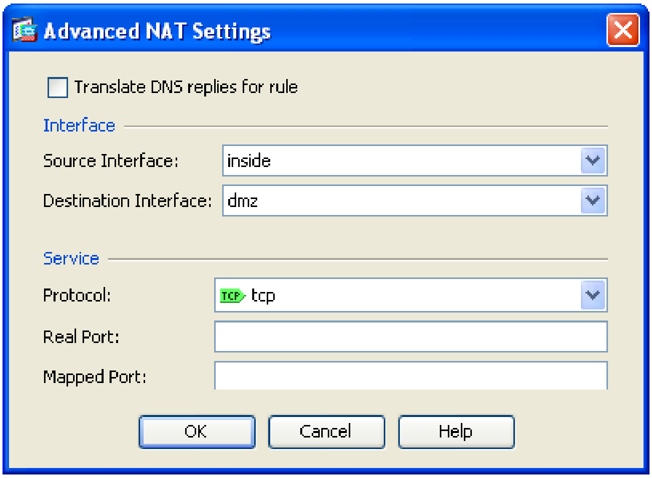
Type: Static

Translated Addr: 192.168.1.0/24

Step 6 Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.

- In the Source Interface drop-down list, choose the Inside interface.
- In the Destination Interface drop-down list, choose the DMZ interface.

  These two settings specify the real and/or mapped interfaces where this NAT rule should apply.



Advanced NAT Settings

□ Translate DNS replies for rule

Interface

Source Interface: inside

Destination Interface: dmz

Service

Protocol: tcp

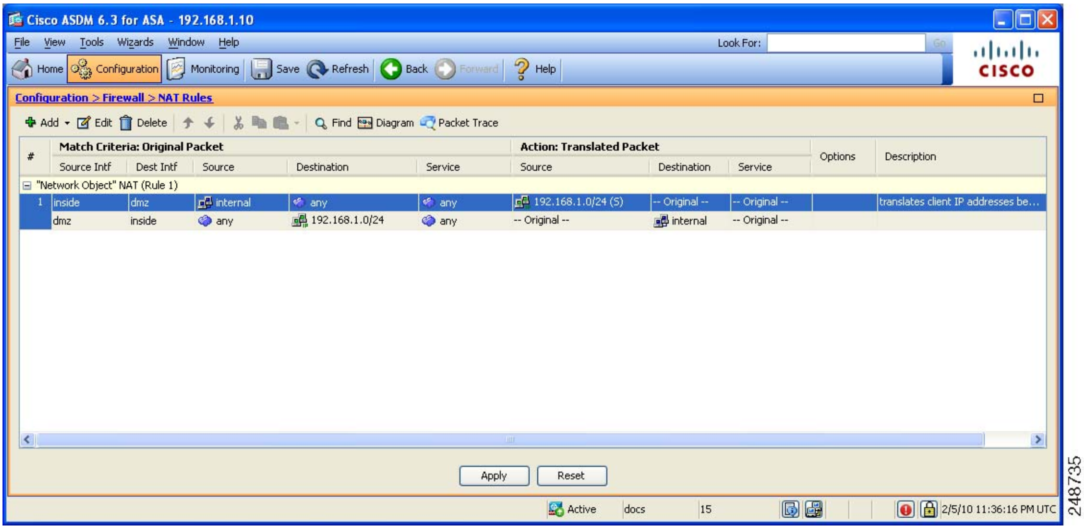
Real Port:

Mapped Port:

Step 7 Click **OK**. You return to the Add Network Object dialog box.

Step 8 Click **OK** to add the rule and return to the list of Address Translation Rules.

Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following.



Cisco ASDM 6.3 for ASA - 192.168.1.10

Configuration > Firewall > NAT Rules

#	Match Criteria: Original Packet					Action: Translated Packet			Options	Description
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
"Network Object" NAT (Rule 1)										
1	inside	dmz	internal	any	any	192.168.1.0/24 (S)	-- Original --	-- Original --		translates client IP addresses be...
	dmz	inside	any	192.168.1.0/24	any	-- Original --	internal	-- Original --		

Step 9 Click **Apply** to complete the adaptive security appliance configuration changes.

Translating the Public Address of the Web Server to its Real Address on the Inside Interface

To configure a NAT rule that translates the public IP address of the web server to its real IP address, perform the following steps:

Step 1 In the **Configuration** > **Firewall** > **NAT Rules** pane, click the green + (plus) icon and choose and choose **Add "Network Object" NAT Rule**.

The Add Network Object dialog box appears.

Step 2 Fill in the following values:

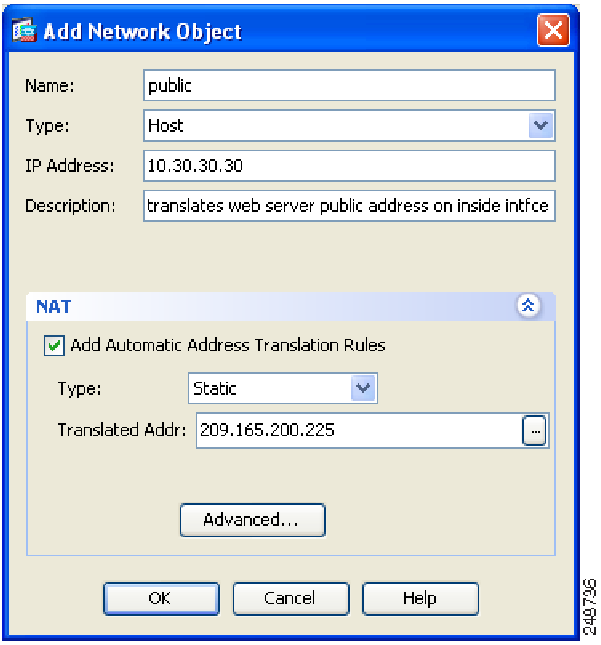
- In the Name field, enter the object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.
- From the Type drop-down list, choose Host.
- In the IP Address field, enter the real (private) address of the DMZ web server. In this scenario, the IP address is 10.30.30.30.
- (Optional) In the Description field, enter a description of the network object (up to 200 characters in length).

Note If the NAT section is hidden, click NAT to expand the section.

Step 3 Check the Add Automatic Translation Rules check box.

Step 4 From the Type drop-down list, choose Static.

Step 5 In the Translated Addr. field, enter the public address (or mapped address) of the DMZ web server, or click ..., and choose an the address from the Browse Translated Addr dialog box. In this scenario, the IP address is 209.165.200.225.



Add Network Object

Name: public

Type: Host

IP Address: 10.30.30.30

Description: translates web server public address on inside intfce

NAT

☑ Add Automatic Address Translation Rules

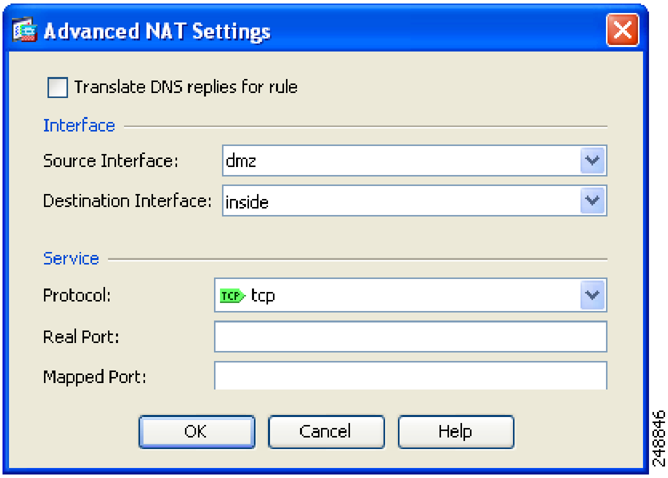
Type: Static

Translated Addr: 209.165.200.225

Step 6 Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.

- In the Source Interface drop-down list, choose the DMZ interface.
- In the Destination Interface drop-down list, choose the Inside interface.

These two settings specify the real and/or mapped interfaces where this NAT rule should apply.



Advanced NAT Settings

□ Translate DNS replies for rule

Interface

Source Interface: dmz

Destination Interface: inside

Service

Protocol: tcp

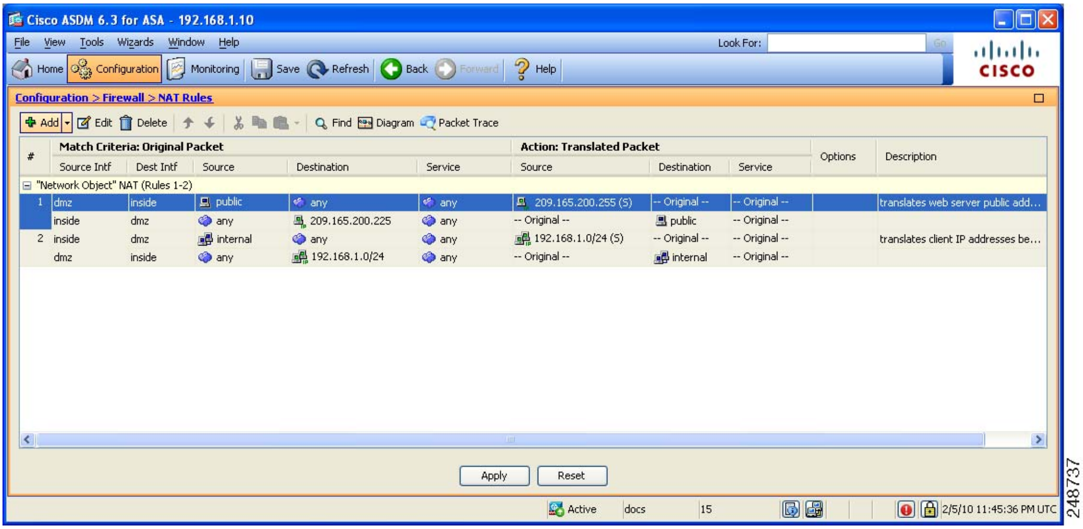
Real Port:

Mapped Port:

Step 7 Click **OK**. You return to the Add Network Object dialog box.

Step 8 Click **OK** to add the rule and return to the list of Address Translation Rules.

Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following.



Cisco ASDM 6.3 for ASA - 192.168.1.10

Configuration > Firewall > NAT Rules

#	Match Criteria: Original Packet					Action: Translated Packet			Options	Description
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
"Network Object" NAT (Rules 1-2)										
1	dmz	inside	public	any	any	209.165.200.255 (S)	-- Original --	-- Original --		translates web server public add...
	inside	dmz	any	209.165.200.225	any	-- Original --	public	-- Original --		
2	inside	dmz	internal	any	any	192.168.1.0/24 (S)	-- Original --	-- Original --		translates client IP addresses be...
	dmz	inside	any	192.168.1.0/24	any	-- Original --	internal	-- Original --		

Step 9 Click **Apply** to complete the adaptive security appliance configuration changes.

Configuring Static PAT for Public Access to the DMZ Web Server (Port Forwarding)

The DMZ web server needs to be accessible by all hosts on the Internet. This configuration requires translating the private IP address of the DMZ web server to a public IP address, which allows outside HTTP clients to access the web server without being aware of the adaptive security appliance. In this scenario the DMZ web server shares a public IP address with the outside interface of the adaptive security appliance (209.165.200.225).

To map the real web server IP address (10.30.30.30) statically to a public IP address (209.165.200.225), perform the following steps:

Step 1 In the **Configuration** > **Firewall** > **NAT Rules** pane, click the green + (plus) icon and choose and choose **Add "Network Object" NAT Rule**.

The Add Network Object dialog box appears.

Step 2 Fill in the following values:

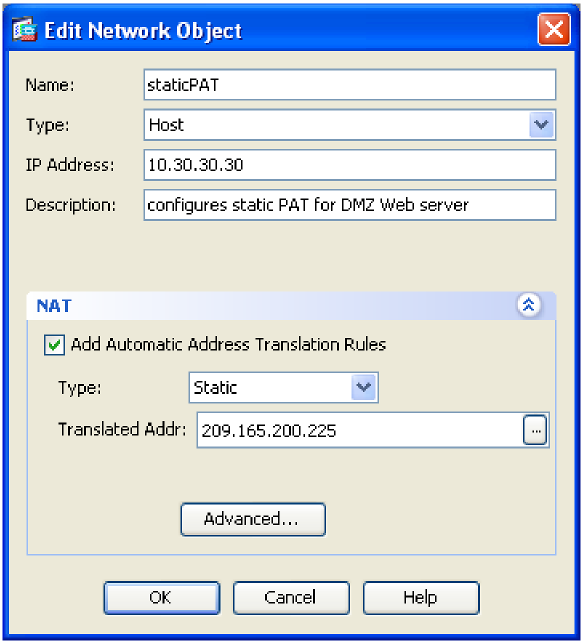
- In the Name field, enter the object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or less.
- From the Type drop-down list, choose Host.
- In the IP Address field, enter the real IP address of the DMZ web server. In this scenario, the IP address is 10.30.30.30.
- (Optional) In the Description field, enter a description of the network object (up to 200 characters in length).

Note If the NAT section is hidden, click NAT to expand the section.

Step 3 Check the Add Automatic Translation Rules check box.

Step 4 From the Type drop-down list, choose Static.

Step 5 In the Translated Addr. field, enter the public IP address to be used for the web server. This is the IP address for the specified interface, in this case, the outside interface, or click ..., and choose an the address from the Browse Translated Addr dialog box.



Edit Network Object

Name: staticPAT

Type: Host

IP Address: 10.30.30.30

Description: configures static PAT for DMZ Web server

NAT

☑ Add Automatic Address Translation Rules

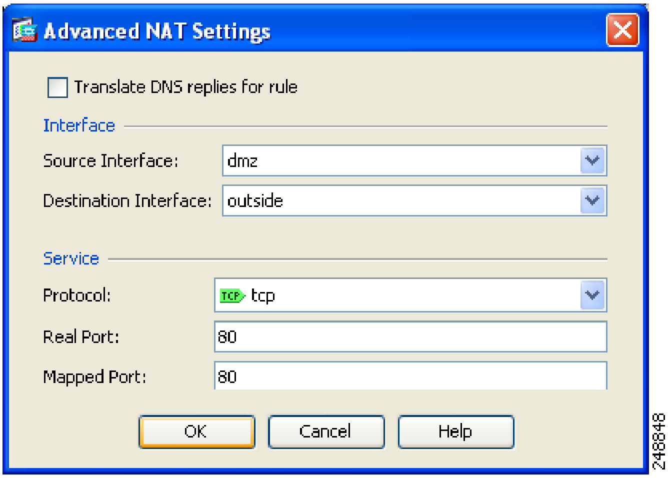
Type: Static

Translated Addr: 209.165.200.225

Step 6 Click **Advanced**, and configure the following options in the Advanced NAT Settings dialog box.

- In the Source Interface drop-down list, choose the DMZ interface.
- In the Destination Interface drop-down list, choose the Outside interface.

  These two settings specify the real and/or mapped interfaces where this NAT rule should apply.
- To configure static NAT with port translation, under Service, choose the tcp from the Protocol drop-down list.
- In the Real Port field, enter 80.
- In the Mapped Port field, enter 80.


Advanced NAT Settings

□ Translate DNS replies for rule

Interface

Source Interface: dmz

Destination Interface: outside

Service

Protocol: tcp

Real Port: 80

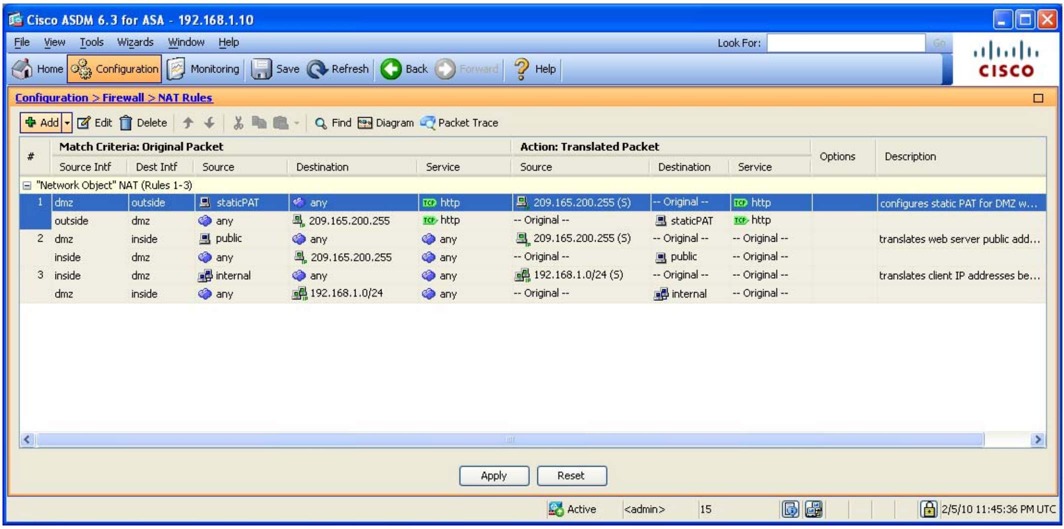
Mapped Port: 80

Because there is only one public IP address, it is necessary to use Port Address Translation to translate the IP address of the DMZ web server to the public IP address (IP address of the Outside interface) of the adaptive security appliance.

Step 7 Click **OK**. You return to the Add Network Object dialog box.

Step 8 Click **OK** to add the rule and return to the list of Address Translation Rules.

Confirm that the rule was created the way you expected. The displayed configuration should be similar to the following.


Cisco ASDM 6.3 for ASA - 192.168.1.10
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Apply Reset
Active <admin> 15 2/5/10 11:45:36 PM UTC

#	Match Criteria: Original Packet					Action: Translated Packet			Options	Description
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service		
"Network Object" NAT (Rules 1-3)										
1	dmz	outside	staticPAT	any	http	209.165.200.255 (S)	-- Original --	http		configures static PAT for DMZ w...
	outside	dmz	any	209.165.200.255	http	-- Original --	staticPAT	http		
2	dmz	inside	public	any	any	209.165.200.255 (S)	-- Original --	-- Original --		translates web server public add...
	inside	dmz	any	209.165.200.255	any	-- Original --	public	-- Original --		
3	inside	dmz	internal	any	any	192.168.1.0/24 (S)	-- Original --	-- Original --		translates client IP addresses be...
	dmz	inside	any	192.168.1.0/24	any	-- Original --	internal	-- Original --		

248849

Step 9 Click **Apply** to complete the adaptive security appliance configuration changes.

Providing Public HTTP Access to the DMZ Web Server

By default, the adaptive security appliance denies all traffic coming in from the public network. To permit traffic coming from the Internet to access the DMZ web server, you must configure an access control rule permitting incoming HTTP traffic destined for the DMZ web server.

This access control rule specifies the interface of the adaptive security appliance that processes the traffic, that the traffic is incoming, the origin and destination of the traffic, and the type of traffic protocol and service to be permitted.

In this section, you create an access rule that permits incoming HTTP traffic originating from any host or network on the Internet, if the destination of the traffic is the web server on the DMZ network. All other traffic coming in from the public network is denied.

To configure the access control rule, perform the following steps:

Step 1 In the main ASDM window, do the following:

a. Click the **Configuration** tool.

b. In the Firewall pane, click **Access Rules**.

c. Click the green plus icon, then choose **Add Access Rule**.

The Add Access Rule dialog box appears.

Step 2 In the Add Access Rule dialog box, do the following:

a. From the Interface drop-down list, choose **Outside**.

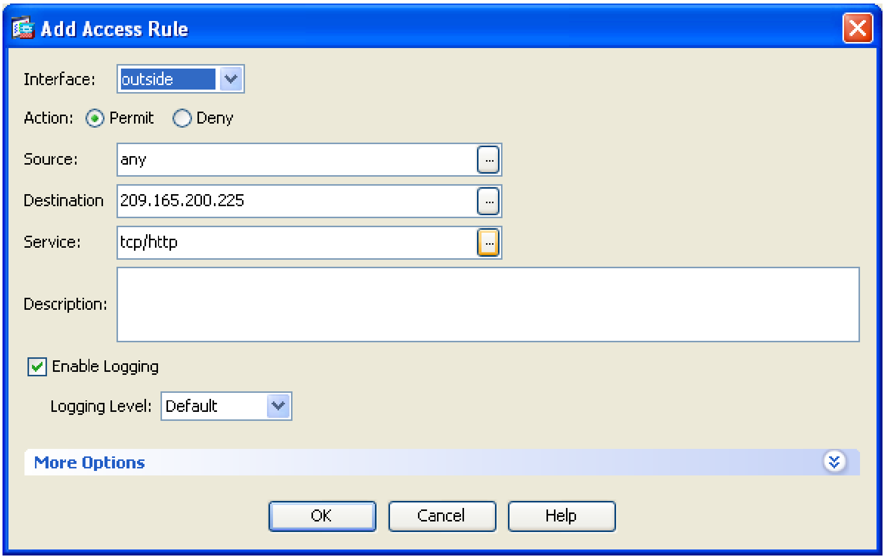
b. Click the **Permit Action** radio button.

c. In the Source field, enter Any.

d. In the Destination field, enter the public IP address of the web server (209.165.200.225).

e. In the Service field, enter TCP/HTTP.

At this point, the entries in the Add Access Rule dialog box should be similar to the following:



Add Access Rule

Interface: outside

Action: ● Permit ○ Deny

Source: any

Destination 209.165.200.225

Service: tcp/http

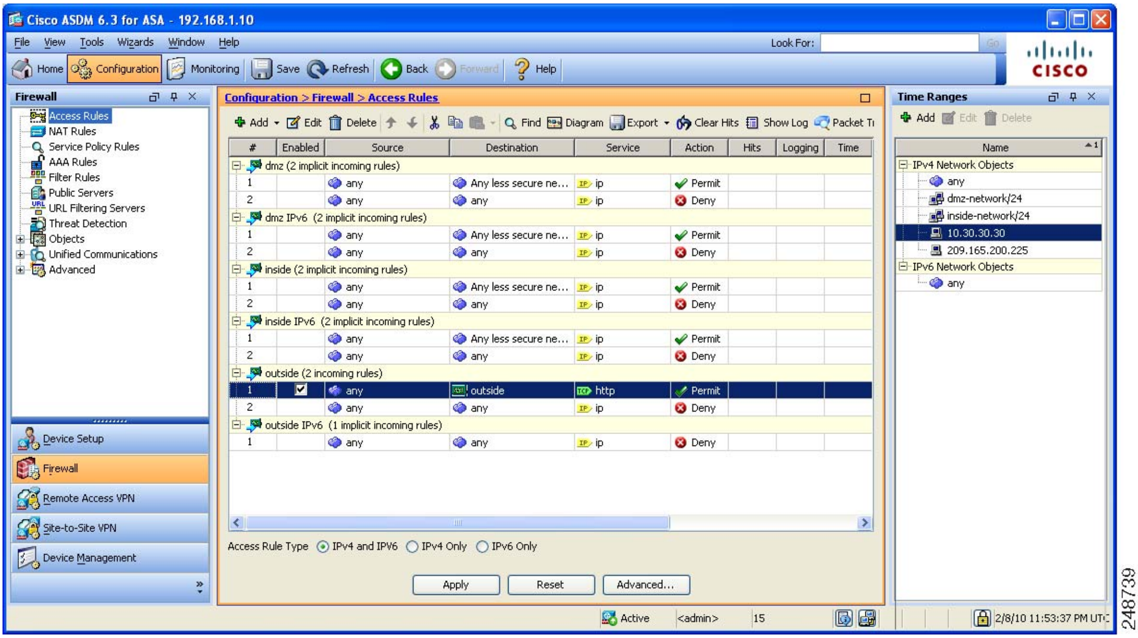
Description:

☑ Enable Logging

Logging Level: Default

f. Click **OK** to return to the Security Policy > Access Rules pane.

The displayed configuration should be similar to the following.



#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time
dmz (2 implicit incoming rules)								
1		any	Any less secure ne...	ip	✓ Permit			
2		any	any	ip	Deny			
dmz IPv6 (2 implicit incoming rules)								
1		any	Any less secure ne...	ip	✓ Permit			
2		any	any	ip	Deny			
inside (2 implicit incoming rules)								
1		any	Any less secure ne...	ip	✓ Permit			
2		any	any	ip	Deny			
inside IPv6 (2 implicit incoming rules)								
1		any	Any less secure ne...	ip	✓ Permit			
2		any	any	ip	Deny			
outside (2 incoming rules)								
1	☑	any	outside	http	✓ Permit			
2		any	any	ip	Deny			
outside IPv6 (1 implicit incoming rules)								
1		any	any	ip	Deny			

Access Rule Type ● IPv4 and IPv6 ○ IPv4 Only ○ IPv6 Only

Verify that the information you entered is accurate.

Click **Apply** to save the configuration changes to the configuration that the adaptive security appliance is currently running.

Clients on the public network can now resolve HTTP requests for content from the DMZ web server, while keeping the private network secure.

Step 3 If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the adaptive security appliance solely to protect a web server in a DMZ, you have completed the initial configuration. You may want to consider performing some of the following additional steps.

To Do This...	See...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This...	See...
Configure a remote-access VPN	Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration"
Configure an SSL VPN for Cisco AnyConnect software clients	Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client"
Configure a browser-based SSL VPN	Chapter 11, "Scenario: SSL VPN Clientless Connections"
Configure a site-to-site VPN	Chapter 12, "Scenario: Site-to-Site VPN Configuration"

CHAPTER 9

Scenario: IPsec Remote-Access VPN Configuration

This chapter describes how to use the adaptive security appliance to accept remote-access IPsec VPN connections. A remote-access VPN allows you to create secure connections, or tunnels, across the Internet, which provides secure access to off-site users. In this type of VPN configuration, remote users must be running the Cisco VPN client to connect to the adaptive security appliance.

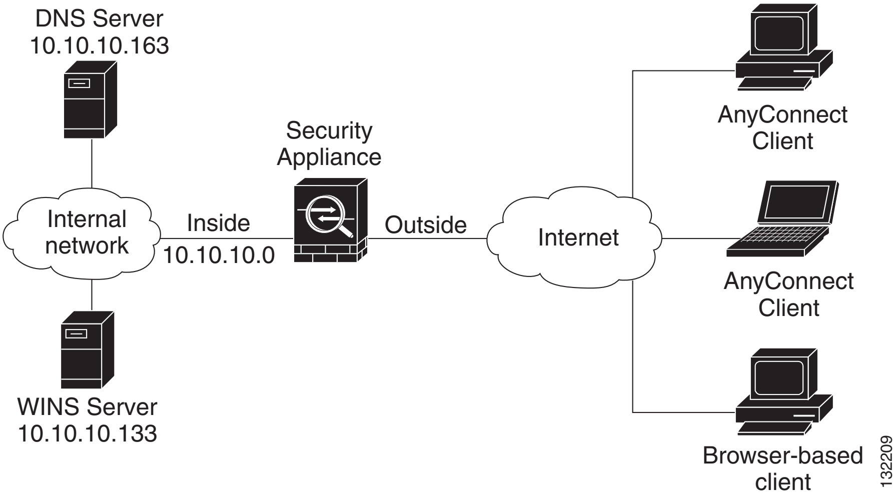
If you are implementing an Easy VPN solution, this chapter describes how to configure the Easy VPN server (sometimes called a headend device).

This chapter includes the following sections:

Example IPsec Remote-Access VPN Network Topology

Figure 9-1 shows an adaptive security appliance configured to accept requests from and establish IPsec connections with VPN clients, such as a Cisco Easy VPN software or hardware clients, over the Internet.

Figure 9-1 Network Layout for Remote Access VPN Scenario



Implementing the IPsec Remote-Access VPN Scenario

This section describes how to configure the adaptive security appliance to accept IPsec VPN connections from remote clients and devices. If you are implementing an Easy VPN solution, this section describes how to configure an Easy VPN server (also known as a headend device).

Values for example configuration settings are taken from the remote-access scenario illustrated in Figure 9-1.

This section includes the following topics:

- Information to Have Available, page 9-3
- Configuring an IPsec Remote-Access VPN, page 9-3
- Selecting VPN Client Types, page 9-5
- Specifying the VPN Tunnel Group Name and Authentication Method, page 9-6
- Specifying a User Authentication Method, page 9-7

Information to Have Available

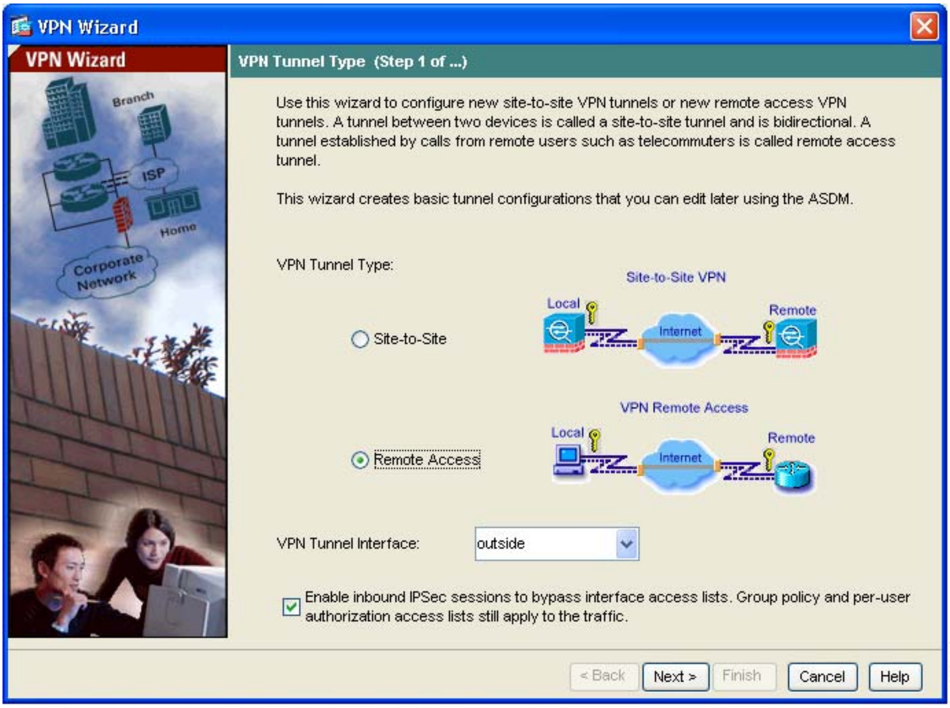
Before you begin configuring the adaptive security appliance to accept remote access IPsec VPN connections, make sure that you have the following information available:

- Range of IP addresses to be used in an IP pool. These addresses are assigned to remote VPN clients as they are successfully connected.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- Networking information to be used by remote clients when connecting to the VPN, including the following:
  - IP addresses for the primary and secondary DNS servers
  - IP addresses for the primary and secondary WINS servers
  - Default domain name
  - List of IP addresses for local hosts, groups, and networks that should be made accessible to authenticated remote clients

Configuring an IPsec Remote-Access VPN

To configure a remote-access VPN, perform the following steps:

Step 1 In the main ASDM window, choose **IPsec VPN Wizard** from the Wizards drop-down menu. The VPN Wizard Step 1 screen appears.



VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

○ Site-to-Site

● Remote Access

VPN Tunnel Interface: outside

☑ Enable inbound IPSec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

153910

Step 2 In Step 1 of the VPN Wizard, perform the following steps:

a. Click the **Remote Access** radio button.

b. From the drop-down list, choose **Outside** as the enabled interface for the incoming VPN tunnels.

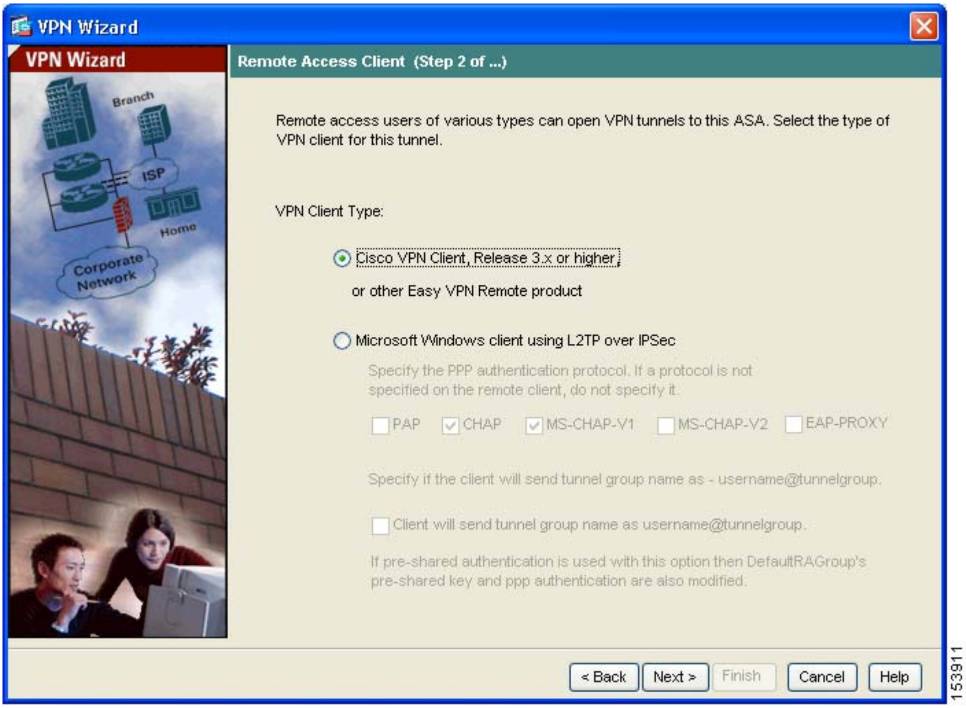
c. Click **Next** to continue.

Selecting VPN Client Types

In Step 2 of the VPN Wizard, perform the following steps:

Step 1 Specify the type of VPN client that will enable remote users to connect to this adaptive security appliance. For this scenario, click the **Cisco VPN Client** radio button.

You can also use any other Cisco Easy VPN remote product.



Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.

VPN Client Type:

● Cisco VPN Client, Release 3.x or higher,
or other Easy VPN Remote product

○ Microsoft Windows client using L2TP over IPSec

Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.

□ PAP ☑ CHAP ☑ MS-CHAP-V1 □ MS-CHAP-V2 □ EAP-PROXY

Specify if the client will send tunnel group name as - username@tunnelgroup.

□ Client will send tunnel group name as username@tunnelgroup.

If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.

Step 2 Click **Next** to continue.

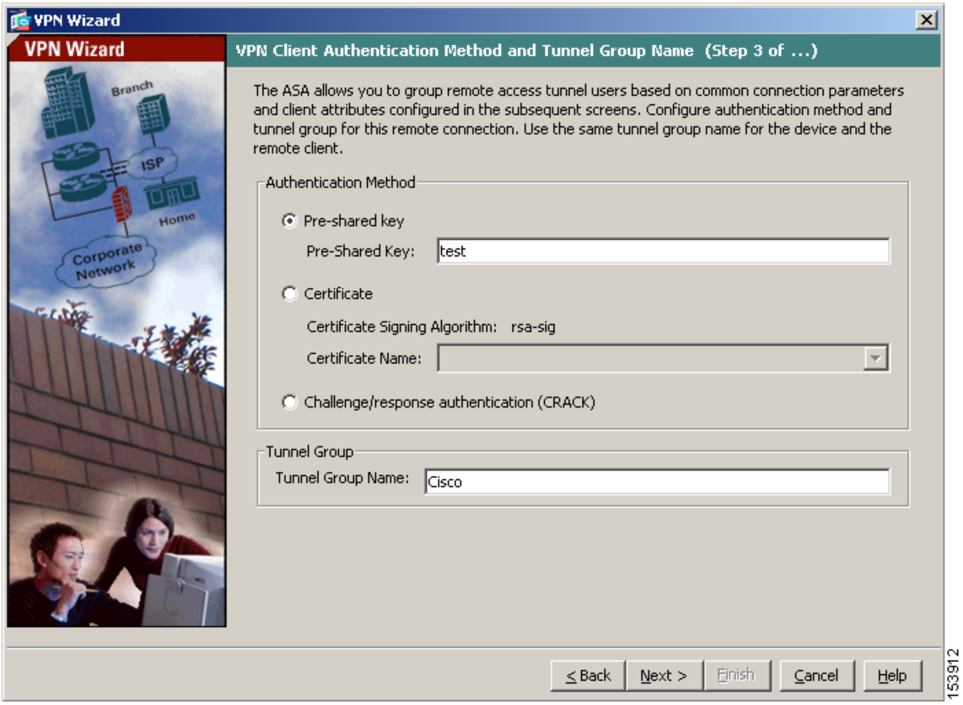
Specifying the VPN Tunnel Group Name and Authentication Method

In Step 3 of the VPN Wizard, perform the following steps:

Step 1 Specify the type of authentication that you want to use by performing one of the following steps:

- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPsec negotiations.
- To use digital certificates for authentication, click the **Certificate** radio button, choose the Certificate Signing Algorithm from the drop-down list, and then choose a preconfigured trustpoint name from the drop-down list.

  If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM windows.
- Click the **Challenge/Response Authentication** (**CRACK**) radio button to use that method of authentication.



VPN Client Authentication Method and Tunnel Group Name (Step 3 of ...)

The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client.

Authentication Method

- ● Pre-shared key
  - Pre-Shared Key: test
- ○ Certificate
  - Certificate Signing Algorithm: rsa-sig
  - Certificate Name:
- ○ Challenge/response authentication (CRACK)

Tunnel Group

Tunnel Group Name: Cisco

Step 2 Enter a Tunnel Group Name (such as “Cisco”) for the set of users that use common connection parameters and client attributes to connect to this adaptive security appliance.

Step 3 Click **Next** to continue.

Specifying a User Authentication Method

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, Kerberos, and LDAP).

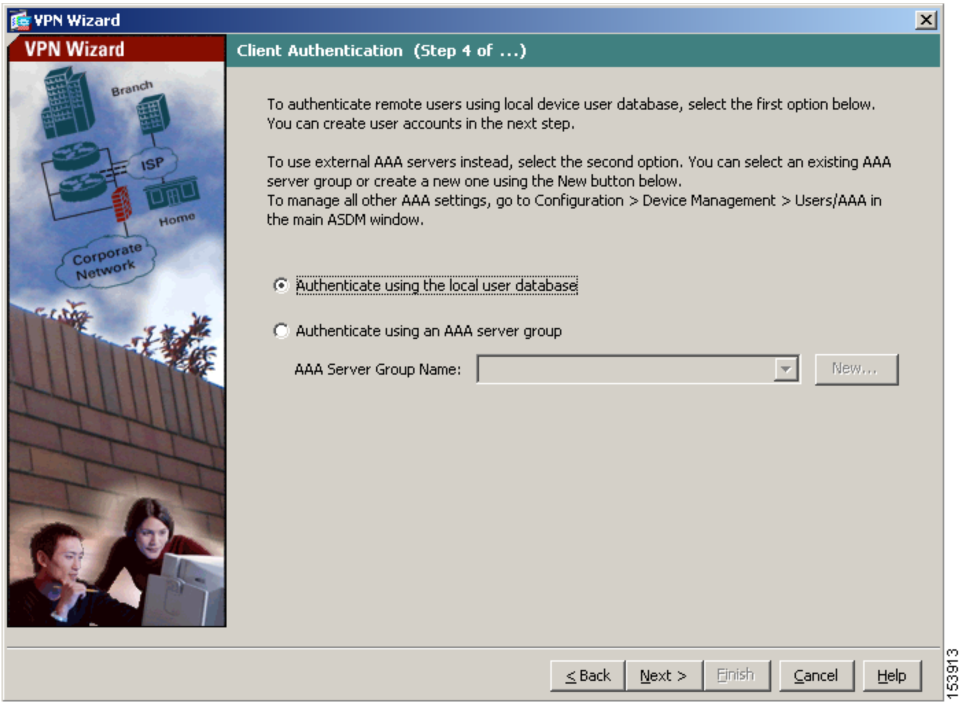
In Step 4 of the VPN Wizard, perform the following steps:

Step 1 If you want to authenticate users by creating a user database on the adaptive security appliance, click the **Authenticate Using the Local User Database** radio button.

Step 2 If you want to authenticate users with an external AAA server group:

a. Click the **Authenticate Using an AAA Server Group** radio button.

b. Choose a preconfigured server group from the Authenticate using a AAA server group drop-down list, or click **New** to add a new AAA server group.



VPN Wizard

Client Authentication (Step 4 of ...)

To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step.

To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.
To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.

● Authenticate using the local user database

○ Authenticate using an AAA server group

AAA Server Group Name:

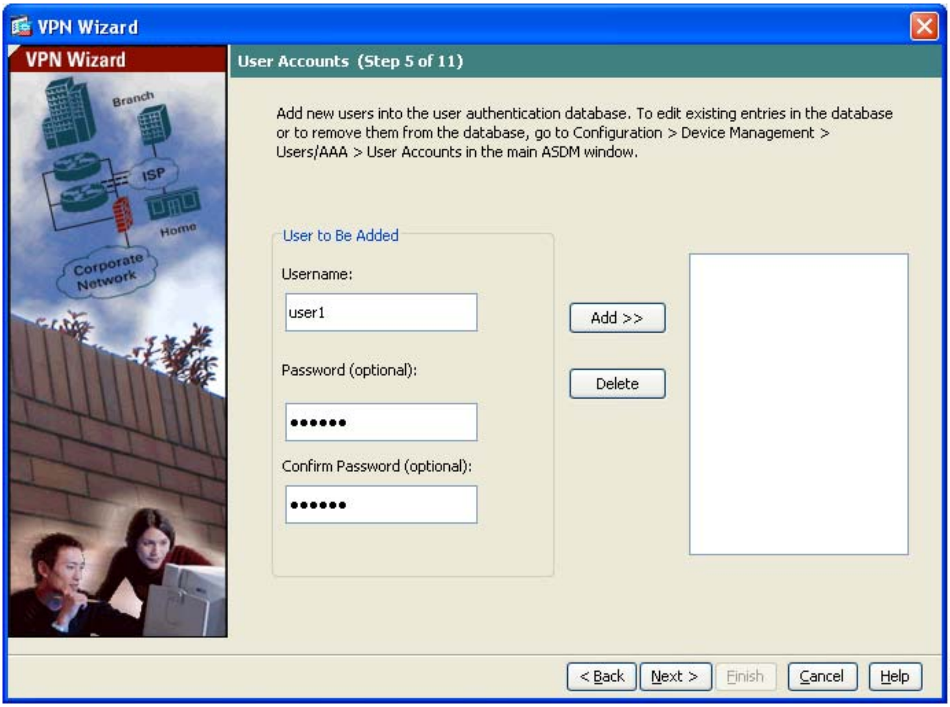
Step 3 Click **Next** to continue.

(Optional) Configuring User Accounts

If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

In Step 5 of the VPN Wizard, perform the following steps:

Step 1 To add a new user, enter a username and password, and then click **Add**.



User Accounts (Step 5 of 11)

Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.

User to Be Added

Username: user1

Password (optional): ••••••

Confirm Password (optional): ••••••

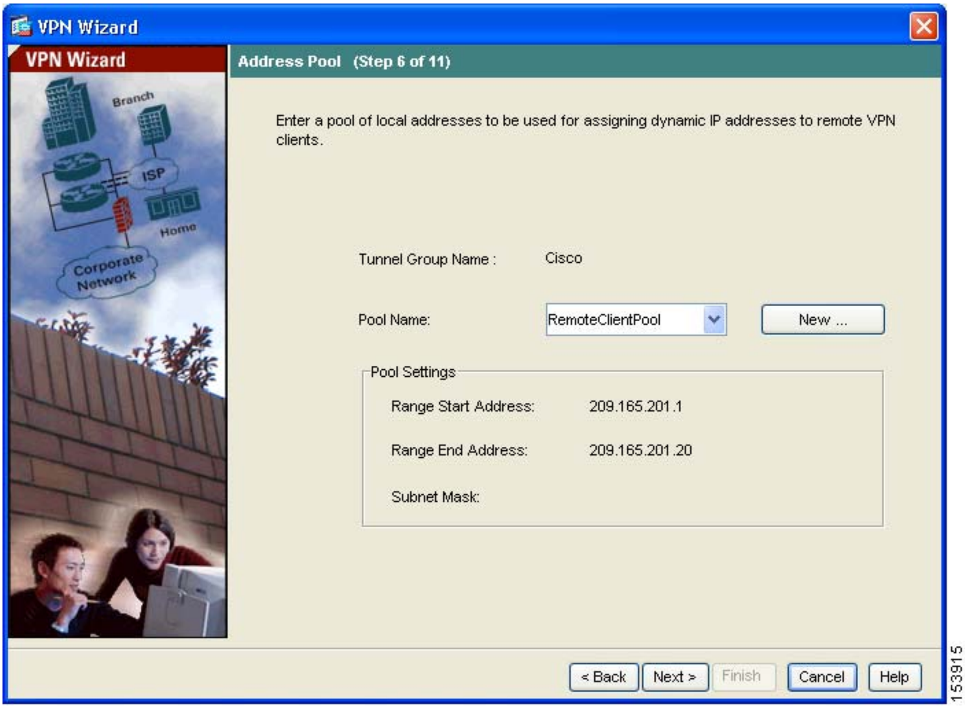
Step 2 When you have finished adding new users, click **Next** to continue.

Configuring Address Pools

For remote clients to gain access to your network, you must configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.201.1–209.165.201.20.

In Step 6 of the VPN Wizard, perform the following steps:

Step 1 Enter a pool name or choose a preconfigured pool from the Pool Name drop-down list.



VPN Wizard

Address Pool (Step 6 of 11)

Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.

Tunnel Group Name : Cisco

Pool Name: RemoteClientPool

Pool Settings

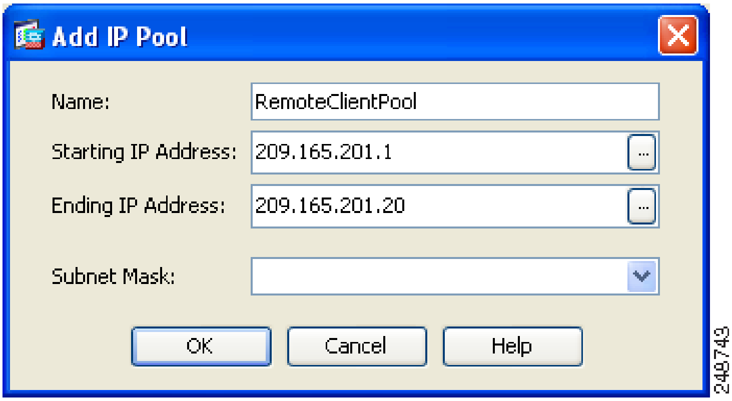
Range Start Address: 209.165.201.1

Range End Address: 209.165.201.20

Subnet Mask:

Alternatively, click **New** to create a new address pool.

The Add IP Pool dialog box appears.



Add IP Pool

Name: RemoteClientPool

Starting IP Address: 209.165.201.1

Ending IP Address: 209.165.201.20

Subnet Mask:

Step 2 In the Add IP Pool dialog box, do the following:

a. Enter the Starting IP address and Ending IP address of the range.

b. (Optional) Enter a subnet mask or choose a subnet mask for the range of IP addresses from the Subnet Mask drop-down list.

c. Click **OK** to return to Step 6 of the VPN Wizard.

Step 3 Click **Next** to continue.

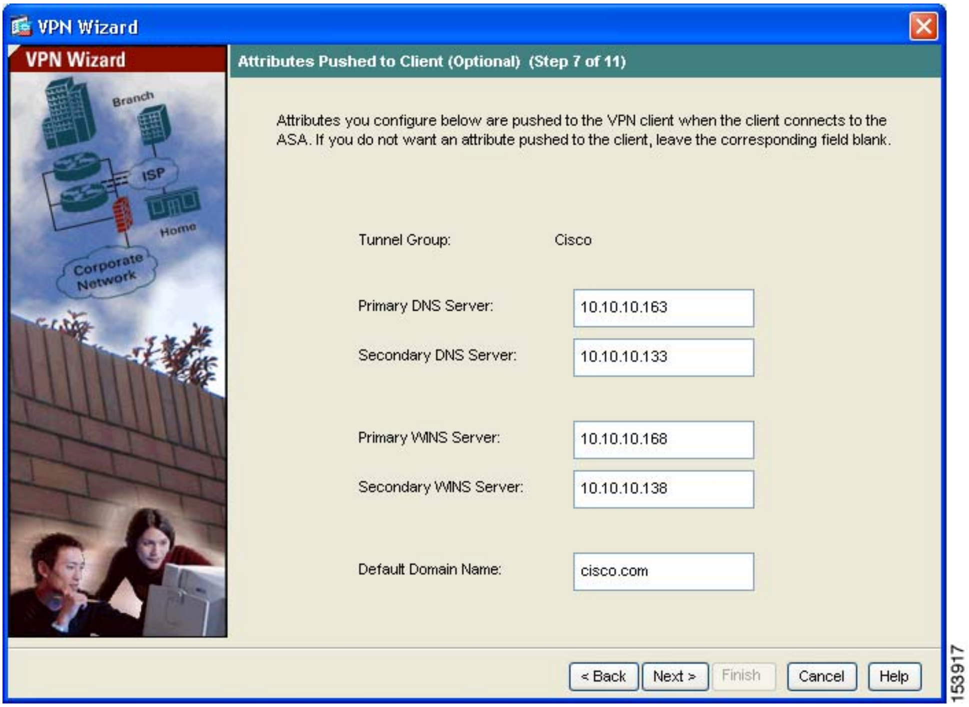
Configuring Client Attributes

To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Instead of configuring each remote client individually, you can provide the client information to ASDM. The adaptive security appliance pushes this information to the remote client or Easy VPN hardware client when a connection is established.

Make sure that you specify the correct values, or remote clients will not be able to use DNS names for resolution or use Windows networking.

In Step 7 of the VPN Wizard, perform the following steps:

Step 1 Enter the network configuration information to be pushed to remote clients.



Attributes Pushed to Client (Optional) (Step 7 of 11)

Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.

Tunnel Group: Cisco

Primary DNS Server: 10.10.10.163

Secondary DNS Server: 10.10.10.133

Primary WINS Server: 10.10.10.168

Secondary WINS Server: 10.10.10.138

Default Domain Name: cisco.com

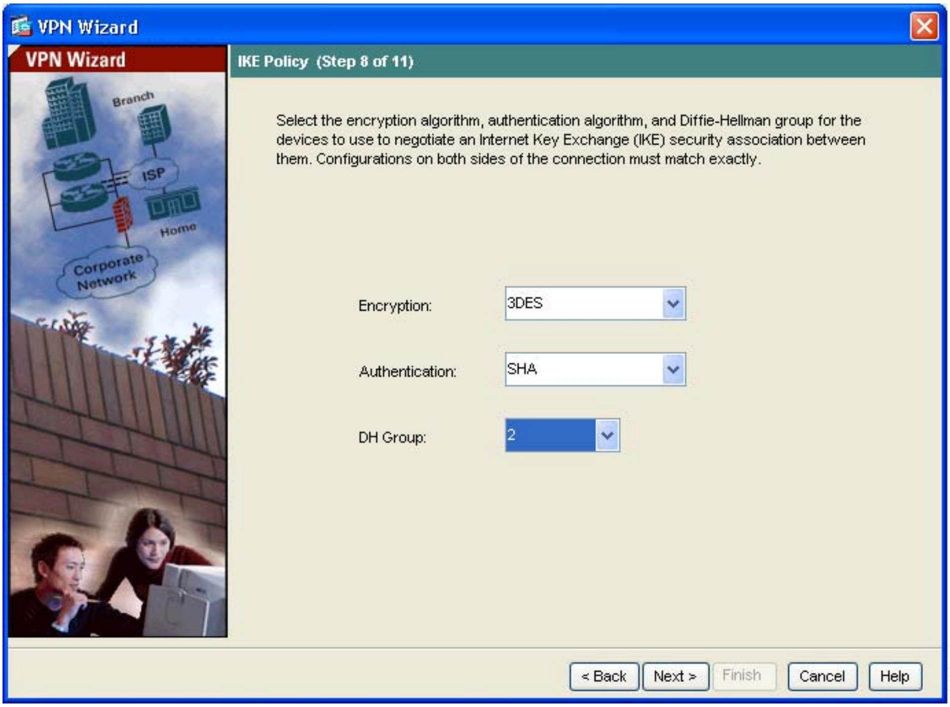
Step 2 Click **Next** to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels.

To specify the IKE policy in Step 8 of the VPN Wizard, perform the following steps:

Step 1 Choose the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5/7) used by the adaptive security appliance during an IKE security association.



VPN Wizard

IKE Policy (Step 8 of 11)

Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

DH Group: 2

Step 2 Click **Next** to continue.

Specifying Address Translation Exception and Split Tunneling

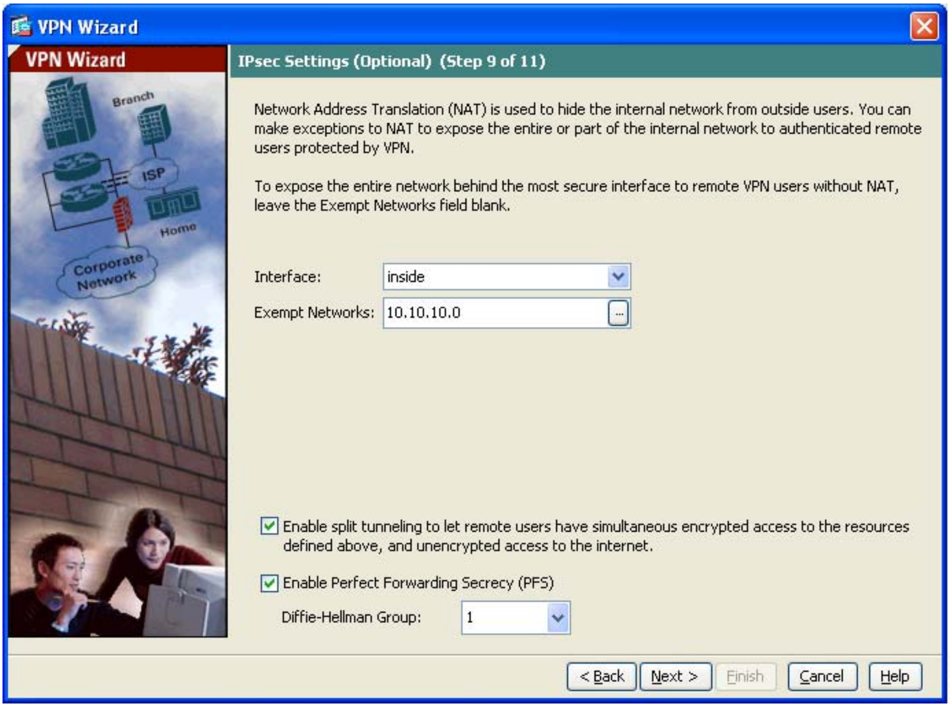
Split tunneling enables remote-access IPsec clients to send packets conditionally over an IPsec tunnel in encrypted form or to a network interface in text form.

The adaptive security appliance uses Network Address Translation (NAT) to prevent internal IP addresses from being exposed externally. You can make exceptions to this network protection by identifying local hosts and networks that should be made accessible to authenticated remote users.

In Step 9 of the VPN Wizard, perform the following steps:

Step 1 Specify hosts, groups, and networks that should be in the list of internal resources made accessible to authenticated remote users.

To add or remove hosts, groups, and networks dynamically from the Selected Hosts/Networks area, click **Add** or **Delete**, respectively.



IPsec Settings (Optional) (Step 9 of 11)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.

Interface: inside

Exempt Networks: 10.10.10.0

☑ Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

☑ Enable Perfect Forwarding Secrecy (PFS)

Diffie-Hellman Group: 1

Step 2 To enable split tunneling, check the **Enable Split Tunneling** check box. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

Step 3 To enable perfect forwarding secrecy (PFS), check the **Enable Perfect Forwarding Secrecy** check box. Enabling PFS sets the size of the numbers to use in generating Phase 2 IPsec keys.

PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless PFS is enabled. PFS uses Diffie-Hellman techniques to generate the keys. PFS ensures that a session key derived from a set of long-term public and private keys is not compromised if one of the private keys is compromised in the future.

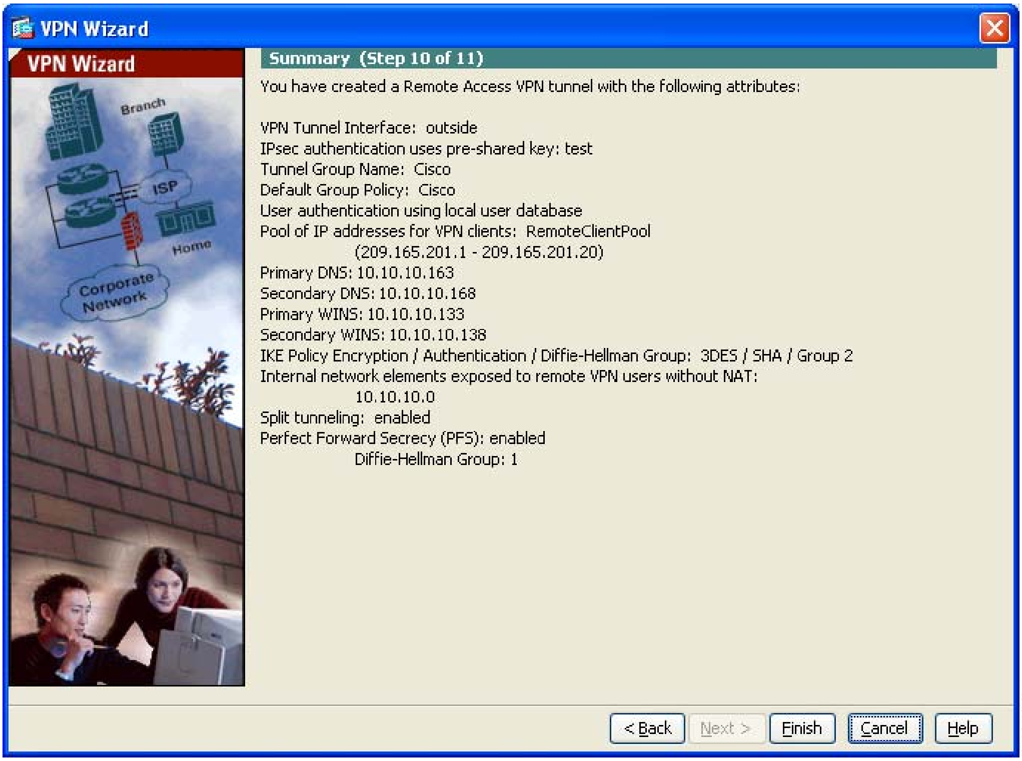
Note PFS must be enabled on both sides of the connection.

Step 4 Select the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The default, Group 2 (1024-bit Diffie-Hellman), requires less CPU time to execute but is less secure than Group 5 (1536-bit). Group 7 is for use with the Movian VPN client, but works with any peer that supports Group 7 (ECC).

Step 5 Click **Next** to continue.

Verifying the Remote-Access VPN Configuration

In Step 10 of the VPN Wizard, review the configuration attributes for the new VPN tunnel. The displayed configuration should be similar to the following:



You have created a Remote Access VPN tunnel with the following attributes:

```
VPN Tunnel Interface:  outside
IPsec authentication uses pre-shared key: test
Tunnel Group Name:  Cisco
Default Group Policy:  Cisco
User authentication using local user database
Pool of IP addresses for VPN clients:  RemoteClientPool
            (209.165.201.1 - 209.165.201.20)
Primary DNS: 10.10.10.163
Secondary DNS: 10.10.10.168
Primary WINS: 10.10.10.133
Secondary WINS: 10.10.10.138
IKE Policy Encryption / Authentication / Diffie-Hellman Group:  3DES / SHA / Group 2
Internal network elements exposed to remote VPN users without NAT:
            10.10.10.0
Split tunneling:  enabled
Perfect Forward Secrecy (PFS): enabled
            Diffie-Hellman Group: 1
```

If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

To establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers, obtain the Cisco VPN client software.

For more information about the Cisco Systems VPN client, see the following URL: http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html.

If you are deploying the adaptive security appliance solely in a remote-access VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps.

To Do This...	See...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This...	See...
Configure an SSL VPN for the Cisco AnyConnect software client	Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client"
Configure a clientless (browser-based) SSL VPN	Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client"
Configure a site-to-site VPN	Chapter 12, "Scenario: Site-to-Site VPN Configuration"

CHAPTER 10

Scenario: Configuring Connections for a Cisco AnyConnect VPN Client

This chapter describes how to configure the adaptive security appliance so that remote users can establish SSL connections using a Cisco AnyConnect VPN client.

This chapter includes the following sections:

About SSL VPN Client Connections

To begin the process of using the SSL VPN Client (AnyConnect), remote users enter in their browser the IP address or FQDN of the SSL VPN interface of the adaptive security appliance. The browser connects to the SSL VPN-enabled interface and displays the login screen.

Note Administrative rights are required the first time the Cisco AnyConnect VPN client is installed or downloaded.

After downloading, the client installs and configures itself and then establishes a secure SSL connection. When the connection terminates, the client software either remains or uninstalls itself, depending on how you configure the adaptive security appliance.

If a remote user has previously established an SSL VPN connection and the client software is not instructed to uninstall itself, when the user authenticates, the adaptive security appliance examines the client version and upgrades if it necessary.

Obtaining the Cisco AnyConnect VPN Client Software

The adaptive security appliance obtains the AnyConnect VPN client software from the Cisco website. This chapter provides instructions for configuring the SSL VPN using a configuration Wizard. You can download the Cisco SSL VPN software during the configuration process.

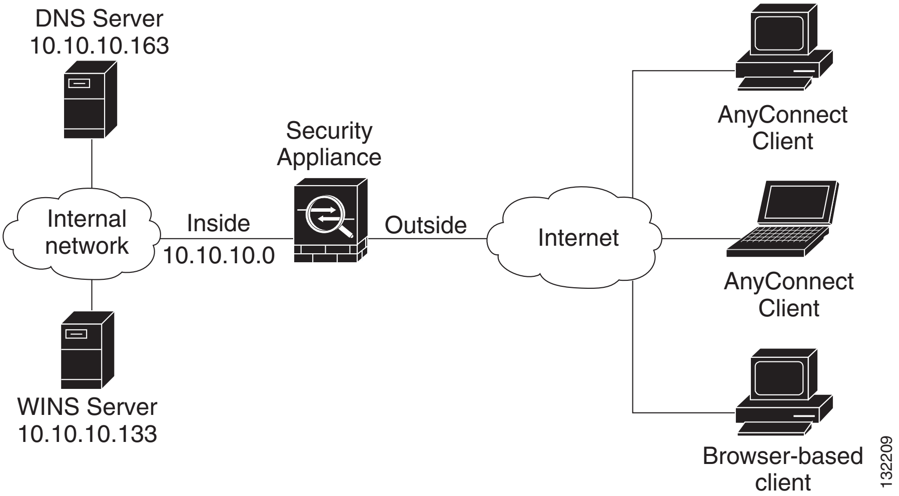
Users can download the AnyConnect VPN client from the adaptive security appliance, or it can be installed manually on the remote PC by the system administrator. For more information about installing the client software manually, see the *Cisco AnyConnect VPN Client Administrator Guide*.

The adaptive security appliance pushes the client software based on the group policy or username attributes of the user establishing the connection. You can configure the adaptive security appliance to automatically push the client each time the user establishes a connection, or you can configure it to prompt the remote user to specify whether to download the client. In the latter case, if the user does not respond, you can configure the adaptive security appliance either to push the client after a timeout period or present the SSL VPN login screen.

Example Topology Using AnyConnect SSL VPN Clients

Figure 10-1 shows an adaptive security appliance configured to accept requests for and establish SSL connections from clients running the AnyConnect SSL VPN software. The adaptive security appliance can support connections to both clients running the AnyConnect VPN software and browser-based clients.

Figure 10-1 Network Layout for SSL VPN Scenario



Implementing the Cisco SSL VPN Scenario

This section describes how to configure the adaptive security appliance to accept Cisco AnyConnect SSL VPN connections. Values for example configuration settings are taken from the SSL VPN scenario illustrated in Figure 10-1.

This section includes the following topics:

- Information to Have Available, page 10-4
- Configuring the Adaptive Security Appliance for the Cisco AnyConnect VPN Client, page 10-5

- Specifying the SSL VPN Interface, page 10-6
- Specifying a User Authentication Method, page 10-7
- Specifying a Group Policy, page 10-8
- Configuring the Cisco AnyConnect VPN Client, page 10-9
- Verifying the Remote-Access VPN Configuration, page 10-11

Information to Have Available

Before you begin configuring the adaptive security appliance to accept AnyConnect SSL VPN connections, make sure that you have the following information available:

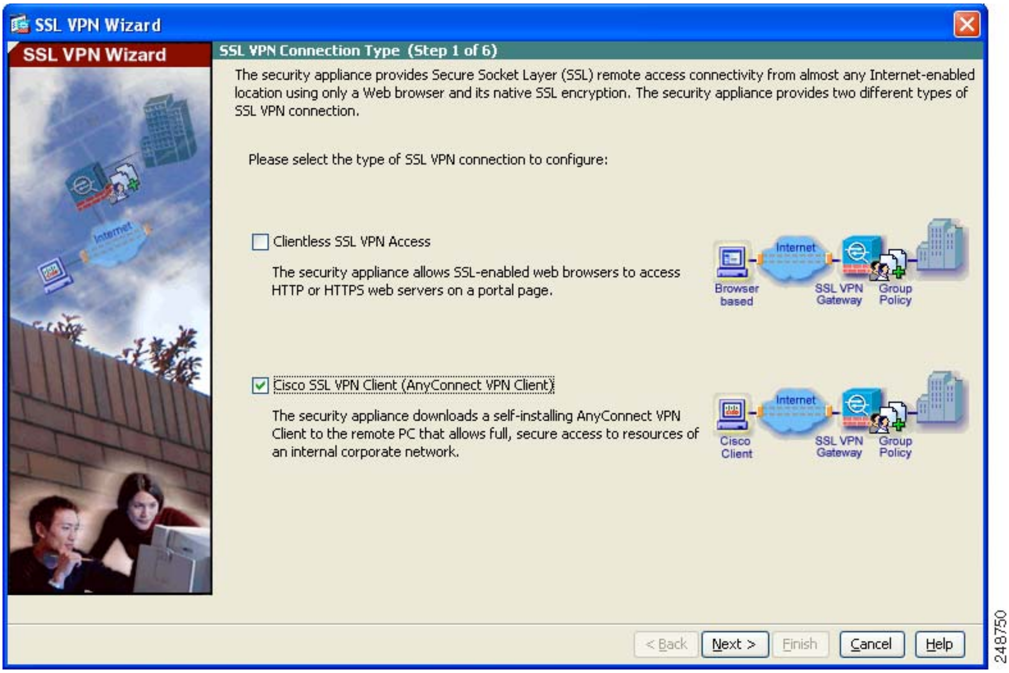
- Name of the interface on the adaptive security appliance to which remote users will connect.
- Digital certificate

  The adaptive security appliance generates a self-signed certificate by default. However, for enhanced security you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.
- Range of IP addresses to be used in an IP pool. These addresses are assigned to SSL AnyConnect VPN clients as they are successfully connected.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- If you are using a AAA server for authentication:
  - AAA Server group name
  - Authentication protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)
  - IP address of the AAA server
  - Interface of the adaptive security appliance to be used for authentication
  - Secret key to authenticate with the AAA server

Configuring the Adaptive Security Appliance for the Cisco AnyConnect VPN Client

To begin the configuration process, perform the following steps:

Step 1 In the main ASDM window, choose **SSL VPN Wizard** from the Wizards drop-down menu. The SSL VPN Wizard Step 1 screen appears.



SSL VPN Wizard

SSL VPN Connection Type (Step 1 of 6)

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. The security appliance provides two different types of SSL VPN connection.

Please select the type of SSL VPN connection to configure:

□ Clientless SSL VPN Access

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

☑ Cisco SSL VPN Client (AnyConnect VPN Client)

The security appliance downloads a self-installing AnyConnect VPN Client to the remote PC that allows full, secure access to resources of an internal corporate network.

Step 2 In Step 1 of the SSL VPN Wizard, perform the following steps:

a. Check the **Cisco SSL VPN Client** check box.

b. Click **Next** to continue.

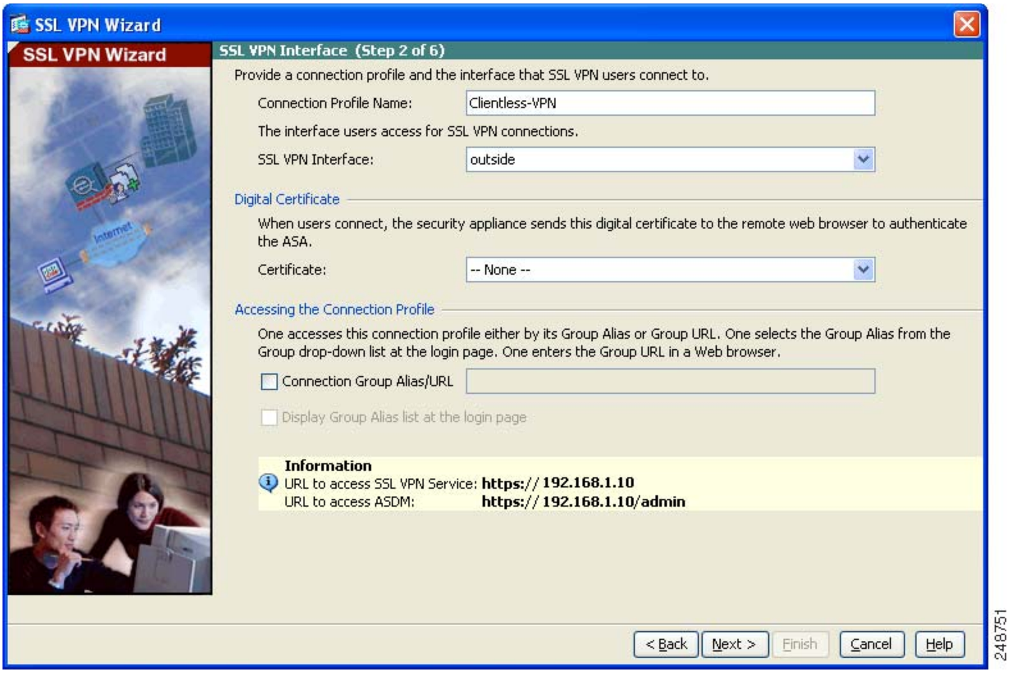
Specifying the SSL VPN Interface

In Step 2 of the SSL VPN Wizard, perform the following steps:

Step 1 Specify a Connection Name to which remote users connect.

Step 2 From the SSL VPN Interface drop-down list, choose the interface to which remote users connect. When users establish a connection to this interface, the SSL VPN portal page is displayed.

Step 3 From the Certificate drop-down list, choose the certificate the adaptive security appliance sends to the remote user to authenticate the adaptive security appliance.



SSL VPN Interface (Step 2 of 6)

Provide a connection profile and the interface that SSL VPN users connect to.

Connection Profile Name: Clientless-VPN

The interface users access for SSL VPN connections.

SSL VPN Interface: outside

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate: -- None --

Accessing the Connection Profile

One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.

□ Connection Group Alias/URL

□ Display Group Alias list at the login page

Information
URL to access SSL VPN Service: https:// 192.168.1.10
URL to access ASDM: https:// 192.168.1.10/admin

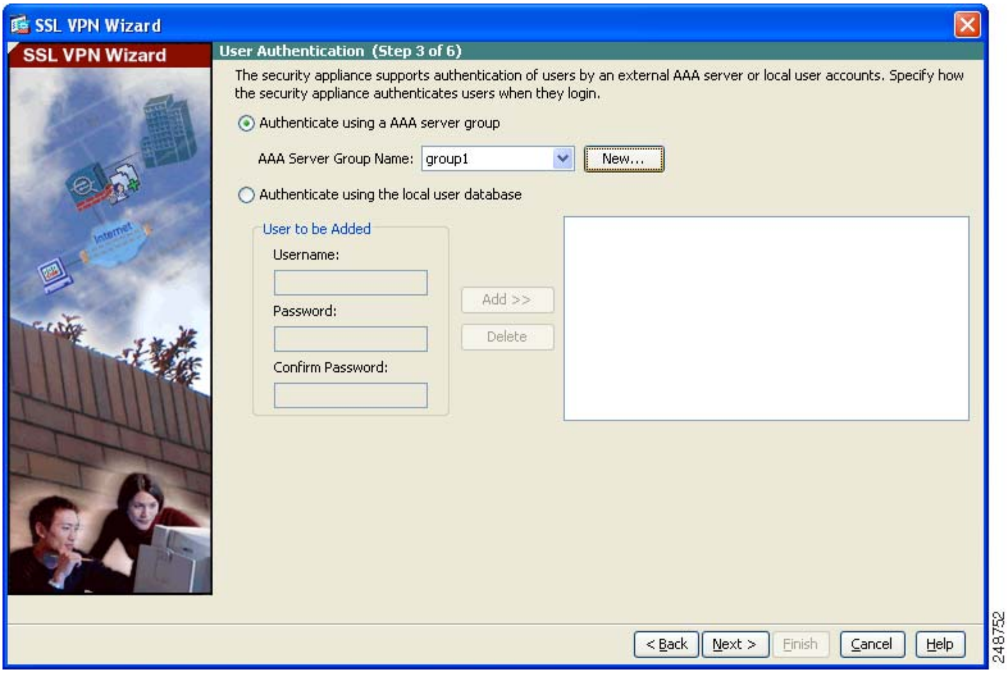
Step 4 Click **Next** to continue.

Specifying a User Authentication Method

In Step 3 of the SSL VPN Wizard, perform the following steps:

Step 1 If you are using a AAA server or server group for authentication, perform the following steps:

a. Click the **Authenticate using a AAA server group** radio button.


SSL VPN Wizard

User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

● Authenticate using a AAA server group

AAA Server Group Name: group1

○ Authenticate using the local user database

User to be Added

Username:

Password:

Confirm Password:

b. Specify a AAA Server Group Name.

c. You can either choose an existing AAA server group name from the drop down list, or you can create a new server group by clicking **New**.

To create a new AAA Server Group, click **New**. The New Authentication Server Group dialog box appears.

In this dialog box, specify the following:

- A server group name
- The Authentication Protocol to be used (RADIUS, TACACS, SDI, NT, Kerberos, LDAP)
- IP address of the AAA server
- Interface of the adaptive security appliance
- Secret key to be used when communicating with the AAA server

d. Click **OK**.

Step 2 If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

To add a new user, enter a username and password, and then click **Add**.

Step 3 When you have finished adding new users, click **Next** to continue.

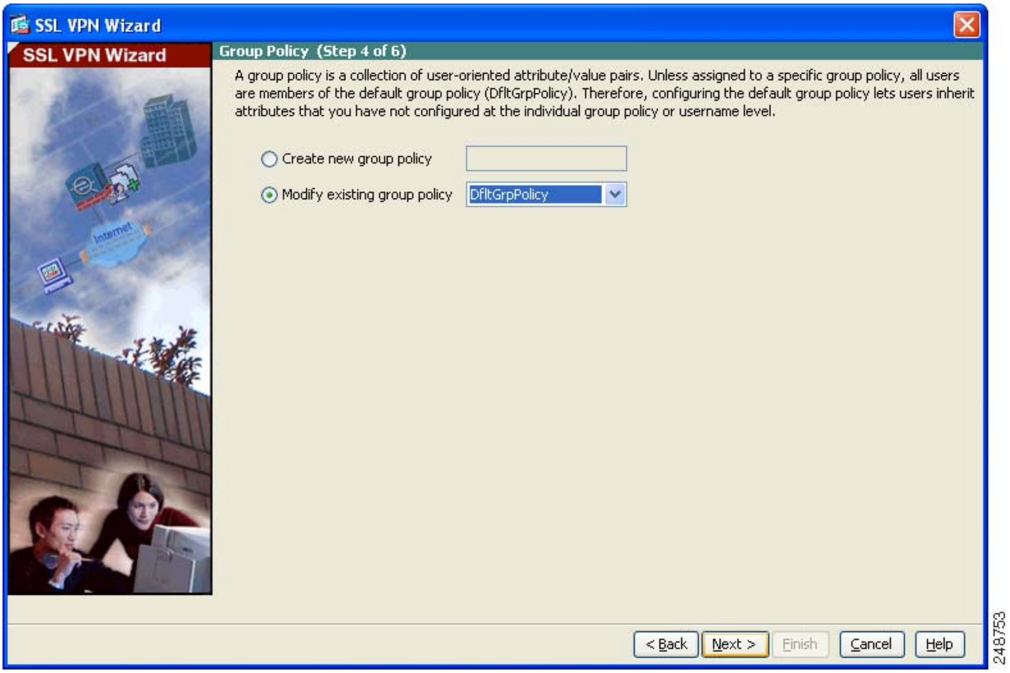
Specifying a Group Policy

In Step 4 of the SSL VPN Wizard, specify a group policy by performing the following steps:

Step 1 Click the **Create new group policy** radio button and specify a group name.

OR

Click the **Modify an existing group policy** radio button and choose a group from the drop-down list.



Group Policy (Step 4 of 6)

A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

○ Create new group policy

● Modify existing group policy: DfltGrpPolicy

Step 2 Click **Next**.

Step 3 Step 5 of the SSL VPN Wizard appears. This step does not apply to AnyConnect VPN client connections, so click **Next** again.

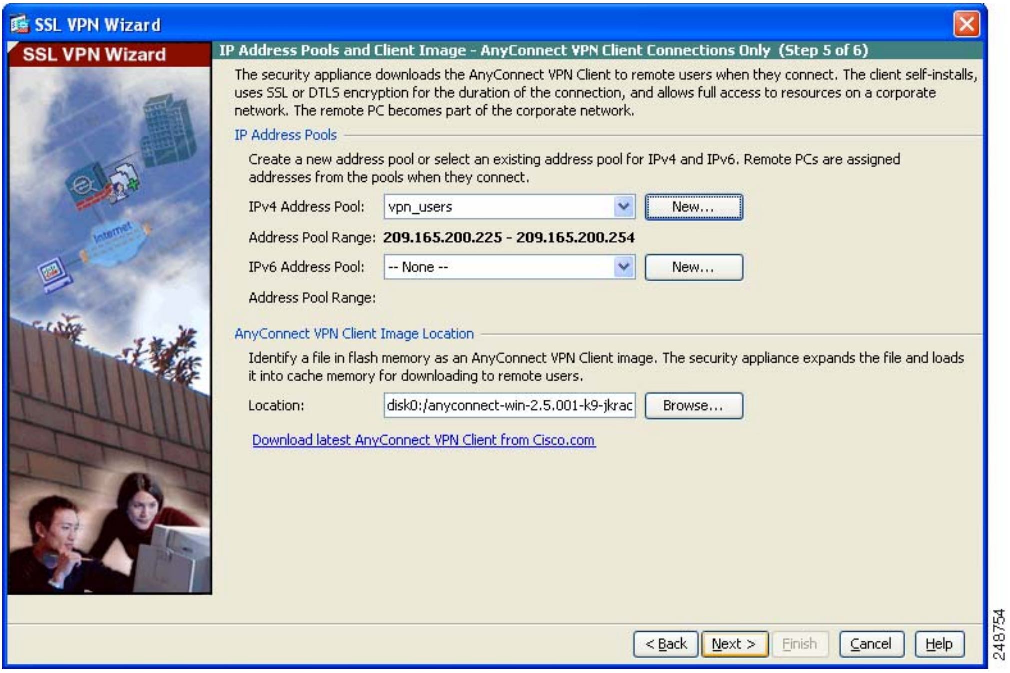
Configuring the Cisco AnyConnect VPN Client

For remote clients to gain access to your network with a Cisco AnyConnect VPN client, you must configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.200.225–209.165.200.254

You must also specify the location of the AnyConnect software so that the adaptive security appliance can push it to users.

In Step 6 of the SSL VPN Wizard, perform the following steps:

Step 1 To use a preconfigured address pool, choose the name of the pool from the IPv4 Address Pool drop-down list or the IPv6 Address Pool drop-down list.



IP Address Pools and Client Image - AnyConnect VPN Client Connections Only (Step 5 of 6)

The security appliance downloads the AnyConnect VPN Client to remote users when they connect. The client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows full access to resources on a corporate network. The remote PC becomes part of the corporate network.

IP Address Pools

Create a new address pool or select an existing address pool for IPv4 and IPv6. Remote PCs are assigned addresses from the pools when they connect.

IPv4 Address Pool: vpn_users

Address Pool Range: 209.165.200.225 - 209.165.200.254

IPv6 Address Pool: -- None --

Address Pool Range:

AnyConnect VPN Client Image Location

Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance expands the file and loads it into cache memory for downloading to remote users.

Location: disk0:/anyconnect-win-2.5.001-k9-jkrac

Download latest AnyConnect VPN Client from Cisco.com

Step 2 Alternatively, click **New** to create a new address pool.

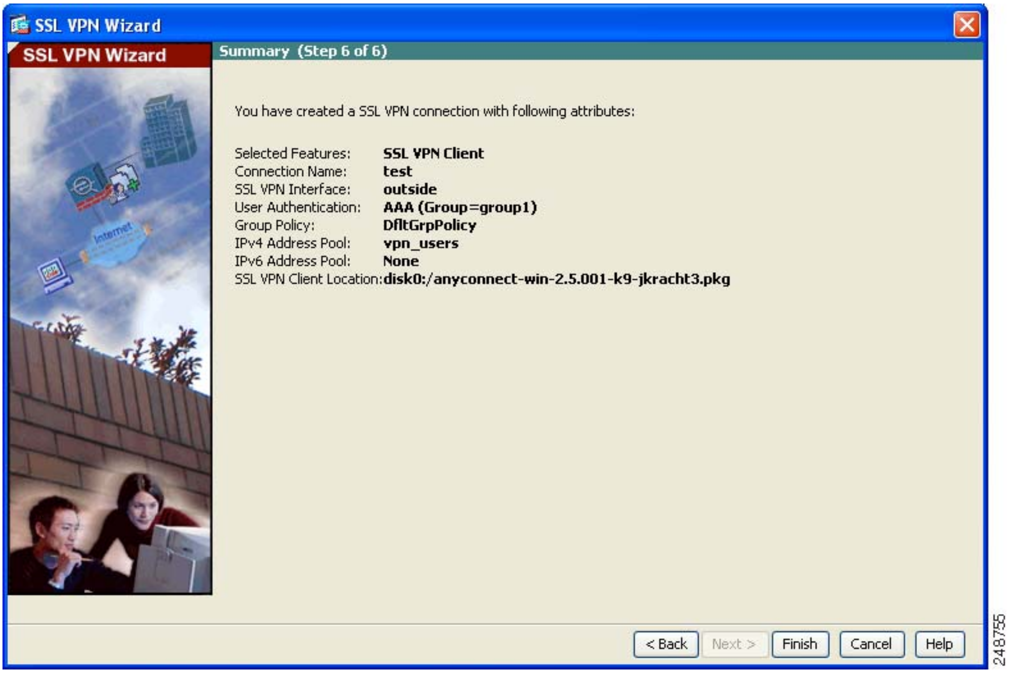
Step 3 Specify the location of the AnyConnect VPN client software image.

To obtain the most current version of the software, click Download Latest AnyConnect VPN Client from cisco.com. This downloads the client software to your PC.

Step 4 Click **Next** to continue.

Verifying the Remote-Access VPN Configuration

In Step 7 of the SSL VPN Wizard, review the configuration settings to ensure that they are correct. The displayed configuration should be similar to the following.



You have created a SSL VPN connection with following attributes:

Selected Features:	**SSL VPN Client**
Connection Name:	**test**
SSL VPN Interface:	**outside**
User Authentication:	**AAA (Group=group1)**
Group Policy:	**DfltGrpPolicy**
IPv4 Address Pool:	**vpn_users**
IPv6 Address Pool:	**None**
SSL VPN Client Location:	**disk0:/anyconnect-win-2.5.001-k9-jkracht3.pkg**

If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the adaptive security appliance solely to support AnyConnect VPN connections, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps.

To Do This...	See...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This...	See...
Configure clientless (browser-based) SSL VPN	Chapter 11, "Scenario: SSL VPN Clientless Connections"
Configure a site-to-site VPN	Chapter 12, "Scenario: Site-to-Site VPN Configuration"
Configure a remote-access IPSec VPN	Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration"

CHAPTER 11

Scenario: SSL VPN Clientless Connections

This chapter describes how to use the adaptive security appliance to accept remote access SSL VPN connections without a software client (clientless). A clientless SSL VPN allows you to create secure connections, or tunnels, across the Internet using a web browser. This provides secure access to off-site users without a software client or hardware client.

This chapter includes the following sections:

About Clientless SSL VPN

Clientless SSL VPN connections enable secure and easy access to a broad range of web resources and web-enabled applications from almost any computer on the Internet. They include the following:

- Internal websites
- Web-enabled applications
- NT/Active Directory and FTP file shares
- E-mail proxies, including POP3S, IMAP4S, and SMTPS

- MS Outlook Web Access
- MAPI
- Application Access (that is, port forwarding for access to other TCP-based applications) and Smart Tunnels

Clientless SSL VPN uses the Secure Sockets Layer (SSL) Protocol and its successor, Transport Layer Security (TLSI), to provide the secure connection between remote users and specific, supported internal resources that you configure at a central site. The adaptive security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

The network administrator provides access to resources by users of Clientless SSL VPN on a group basis.

Security Considerations for Clientless SSL VPN Connections

Clientless SSL VPN connections on the adaptive security appliance differ from remote access IPsec connections, particularly with respect to how they interact with SSL-enabled servers and the validation of certificates.

In a Clientless SSL VPN connection, the adaptive security appliance acts as a proxy between the end user web browser and target web servers. When a user connects to an SSL-enabled web server, the adaptive security appliance establishes a secure connection and validates the server SSL certificate. The end user browser never receives the presented certificate, so therefore it cannot examine and validate the certificate.

The current implementation of Clientless SSL VPN on the adaptive security appliance does not permit communication with sites that present expired certificates. Nor does the adaptive security appliance perform trusted CA certificate validation. Therefore, users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To minimize the risks involved with SSL certificates:

1. Configure a group policy that consists of all users who need Clientless SSL VPN access and enable it only for that group policy.
2. Limit Internet access for Clientless SSL VPN users, for example, by limiting which resources a user can access using a clientless SSL VPN connection. To do this, you could restrict the user from accessing general content on the Internet. Then, you could configure links to specific targets on the internal network that you want users of Clientless SSL VPN to be able to access.
3. Educate users. If an SSL-enabled site is not inside the private network, users should not visit this site over a Clientless SSL VPN connection. They should open a separate browser window to visit such sites, and use that browser to view the presented certificate.

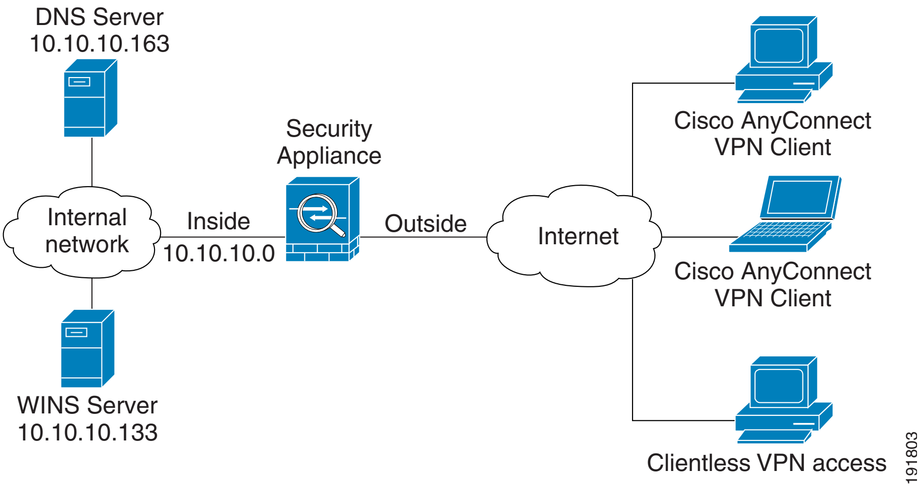
The adaptive security appliance does not support the following features for Clientless SSL VPN connections:

- NAT, reducing the need for globally unique IP addresses.
- PAT, permitting multiple outbound sessions appear to originate from a single IP address.

Example Network with Browser-Based SSL VPN Access

Figure 11-1 shows an adaptive security appliance configured to accept SSL VPN connection requests over the Internet using a web browser.

Figure 11-1 Network Layout for SSL VPN Connections



Implementing the Clientless SSL VPN Scenario

This section describes how to configure the adaptive security appliance to accept SSL VPN requests from web browsers. Values for example configuration settings are taken from the remote-access scenario illustrated in Figure 11-1.

This section includes the following topics:

- Information to Have Available, page 11-5
- Configuring the Adaptive Security Appliance for Browser-Based SSL VPN Connections, page 11-6
- Specifying the SSL VPN Interface, page 11-7
- Specifying a User Authentication Method, page 11-8
- Specifying a Group Policy, page 11-10
- Creating a Bookmark List for Remote Users, page 11-11
- Verifying the Configuration, page 11-15

Information to Have Available

Before you begin configuring the adaptive security appliance to accept remote access IPsec VPN connections, make sure that you have the following information available:

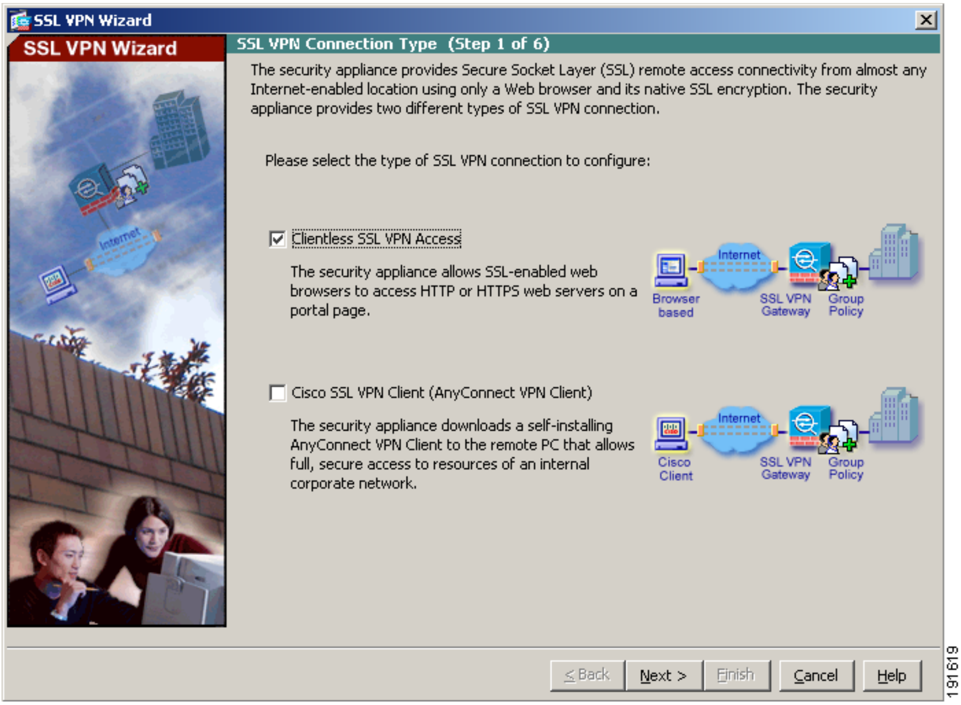
- Name of the interface on the adaptive security appliance to which remote users will connect. When remote users connect to this interface, the SSL VPN Portal Page is displayed.
- Digital certificate

  The ASA 5500 series generates a self-signed certificate by default. For improved security and to eliminate browser warning messages, you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- If you are using a AAA server for authentication, the AAA Server Group Name
- The following information about group policies on the AAA server:
  - Server group name
  - Authentication protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)
  - IP address of the AAA server
  - Interface of the adaptive security appliance to be used for authentication
  - Secret key to authenticate with the AAA server
- List of internal websites or pages you want to appear on the SSL VPN portal page when remote users establish a connection. Because this is the page users see when they first establish a connection, it should contain the most frequently used targets for remote users.

Configuring the Adaptive Security Appliance for Browser-Based SSL VPN Connections

To begin the process for configuring a browser-based SSL VPN, perform the following steps:

Step 1 In the main ASDM window, choose **SSL VPN Wizard** from the Wizards drop-down menu. The SSL VPN Feature Step 1 screen appears.



SSL VPN Connection Type (Step 1 of 6)

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. The security appliance provides two different types of SSL VPN connection.

Please select the type of SSL VPN connection to configure:

☑ Clientless SSL VPN Access

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

□ Cisco SSL VPN Client (AnyConnect VPN Client)

The security appliance downloads a self-installing AnyConnect VPN Client to the remote PC that allows full, secure access to resources of an internal corporate network.

Step 2 In Step 1 of the SSL VPN Wizard, perform the following steps:

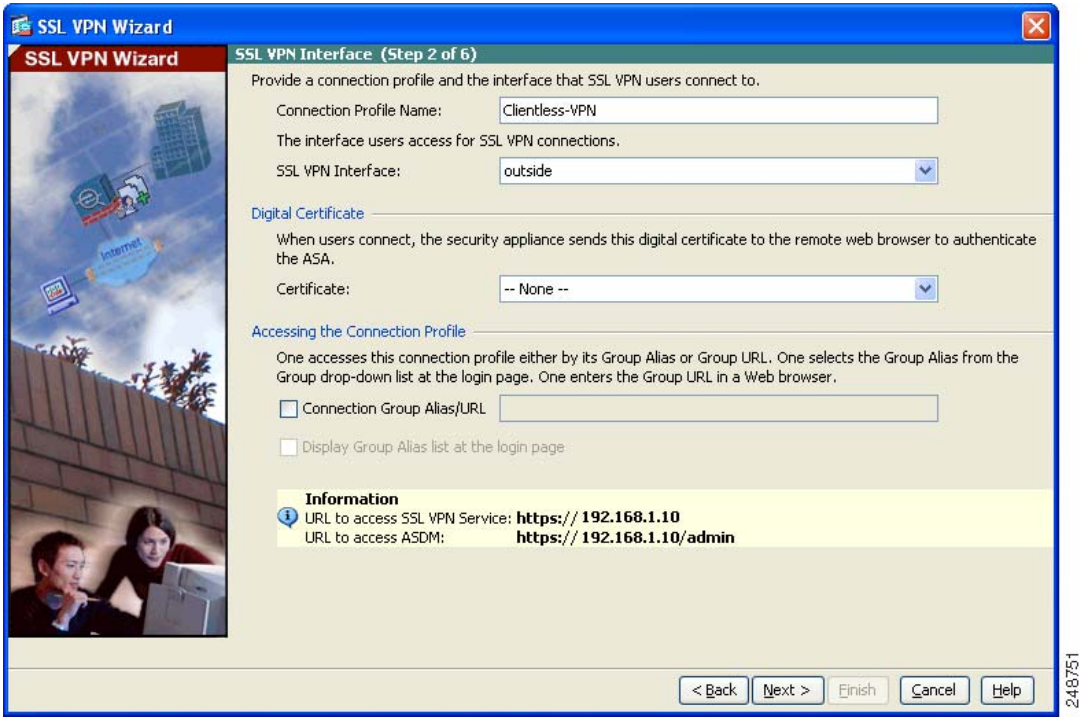
a. Check the **Browser-based SSL VPN (Web VPN)** check box.

b. Click **Next** to continue.

Specifying the SSL VPN Interface

In Step 2 of the SSL VPN Wizard, perform the following steps:

Step 1 Specify a Connection Name to which remote users connect.



SSL VPN Wizard

SSL VPN Interface (Step 2 of 6)

Provide a connection profile and the interface that SSL VPN users connect to.

Connection Profile Name: Clientless-VPN

The interface users access for SSL VPN connections.

SSL VPN Interface: outside

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate: -- None --

Accessing the Connection Profile

One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.

□ Connection Group Alias/URL

□ Display Group Alias list at the login page

Information
URL to access SSL VPN Service: https:// 192.168.1.10
URL to access ASDM: https:// 192.168.1.10/admin

Step 2 From the SSL VPN Interface drop-down list, choose the interface to which remote users connect. When users establish a connection to this interface, the SSL VPN portal page is displayed.

Step 3 From the Certificate drop-down list, choose the certificate the adaptive security appliance sends to the remote user to authenticate the adaptive security appliance.

Note The ASA 5500 series generates a self-signed certificate by default. For improved security and to eliminate browser warning messages, you may want to purchase a publicly trusted SSL VPN certificate before putting the system in a production environment.

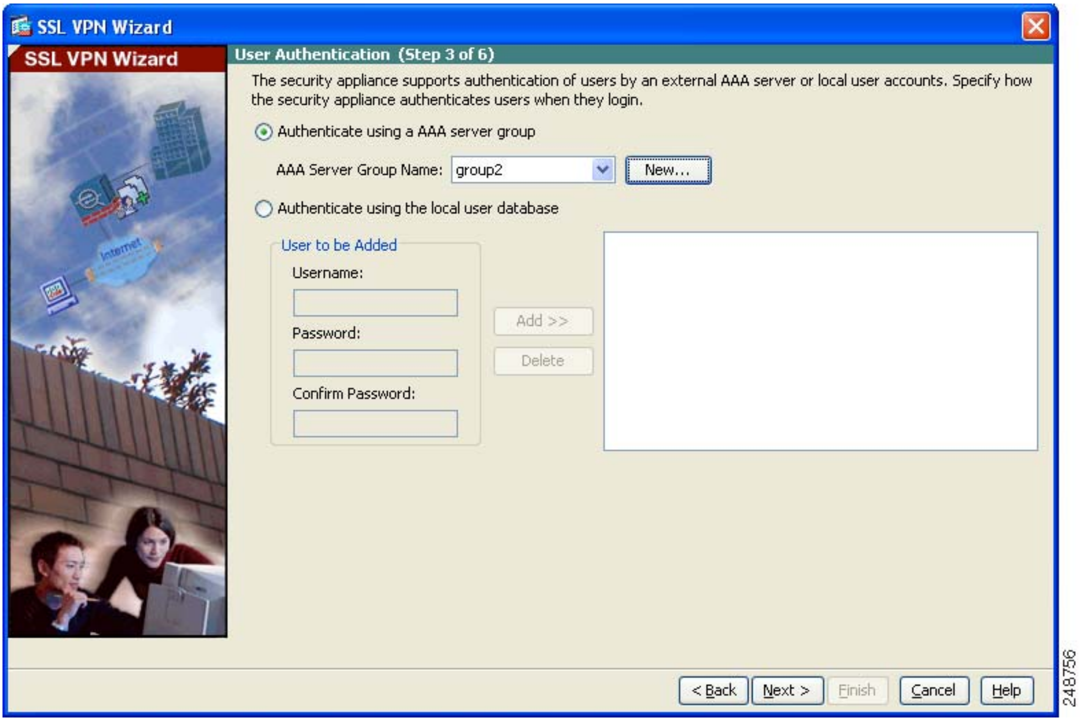
Specifying a User Authentication Method

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, Kerberos, and LDAP).

In Step 3 of the SSL VPN Wizard, perform the following steps:

Step 1 If you are using a AAA server or server group for authentication, perform the following steps:

a. Click the **Authenticate using a AAA server group** radio button.



SSL VPN Wizard

User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

● Authenticate using a AAA server group

AAA Server Group Name: group2

○ Authenticate using the local user database

User to be Added

Username:

Password:

Confirm Password:

b. Choose a preconfigured server group from the Authenticate using an AAA server group drop-down list, or click **New** to add a new AAA server group.

To create a new AAA Server Group, click **New**. The New Authentication Server Group dialog box appears.

In this dialog box, specify the following:

– A server group name

– The Authentication Protocol to be used (TACACS, SDI, NT, Kerberos, LDAP)

– IP address of the AAA server

– Interface of the adaptive security appliance

– Secret key to be used when communicating with the AAA server

Click **OK**.

Step 2 If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

To add a new user, enter a username and password, and then click **Add**.

Step 3 When you have finished adding new users, click **Next** to continue.

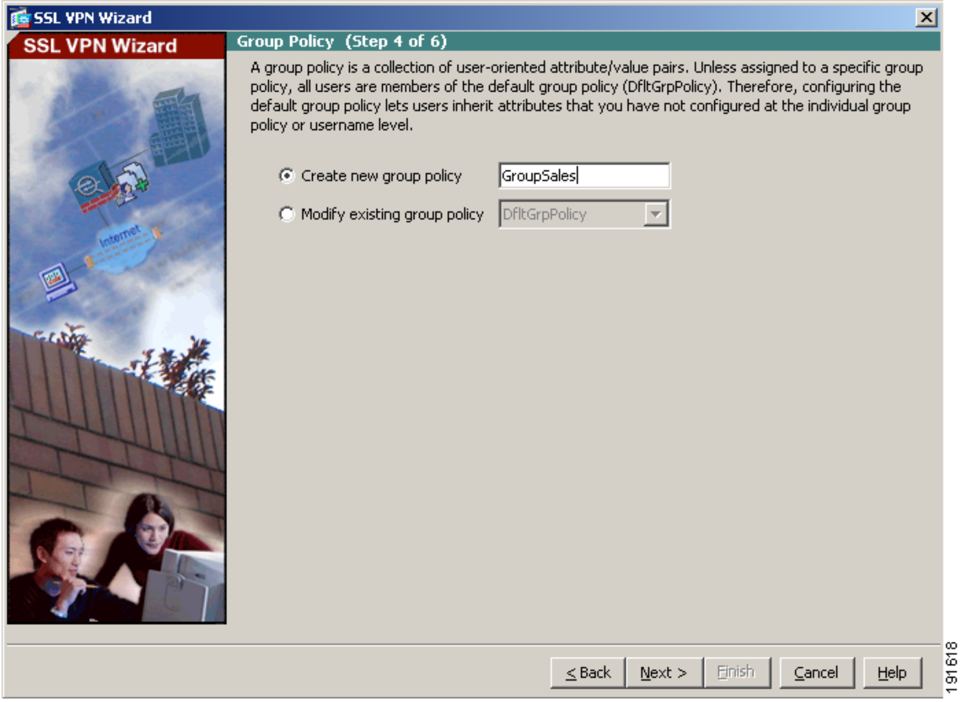
Specifying a Group Policy

In Step 4 of the SSL VPN Wizard, specify a group policy by performing the following steps:

Step 1 Click the **Create new group policy** radio button and specify a group name.

OR

Click the **Modify an existing group policy** radio button and choose a group from the drop-down list.



Group Policy (Step 4 of 6)

A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

● Create new group policy GroupSales

○ Modify existing group policy DfltGrpPolicy

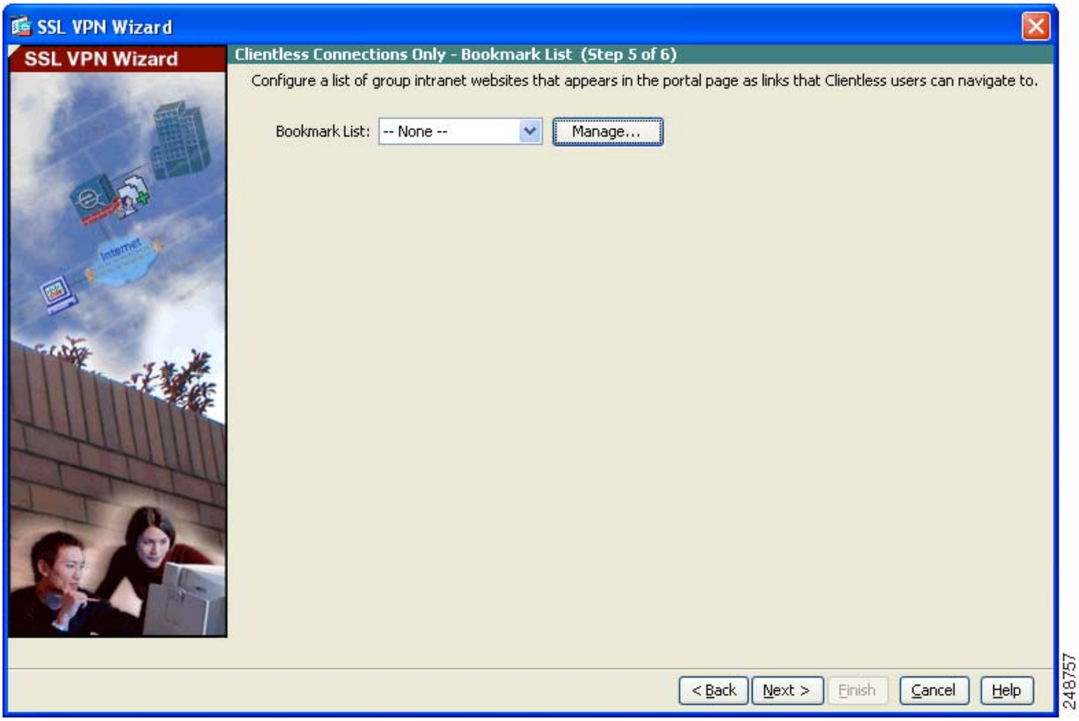
Step 2 Click **Next**.

Creating a Bookmark List for Remote Users

You can create a portal page, a special web page that comes up when browser-based clients establish VPN connections to the adaptive security appliance, by specifying a list of URLs to which users should have easy access.

In Step 5 of the SSL VPN Wizard, specify URLs to appear on the VPN portal page by performing the following steps:

Step 1 To specify an existing bookmark list, choose the Bookmark List name from the drop-down list.



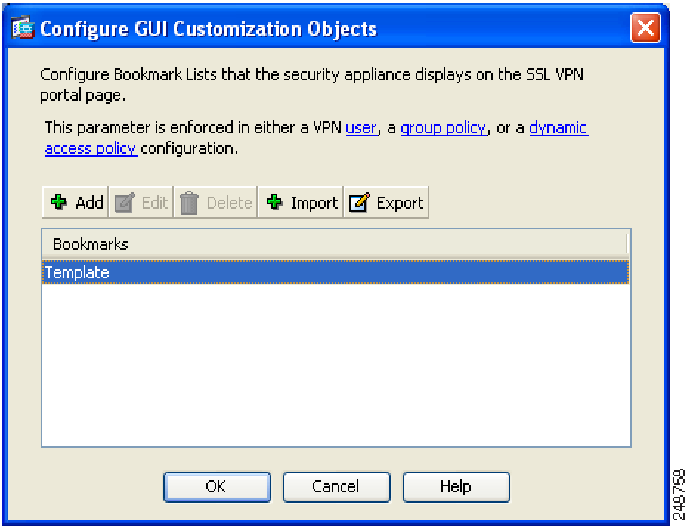
Clientless Connections Only - Bookmark List (Step 5 of 6)

Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.

Bookmark List: -- None -- Manage...

To add a new list or edit an existing list, click **Manage**.

The Configure GUI Customization Objects dialog box appears.



Configure GUI Customization Objects

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.

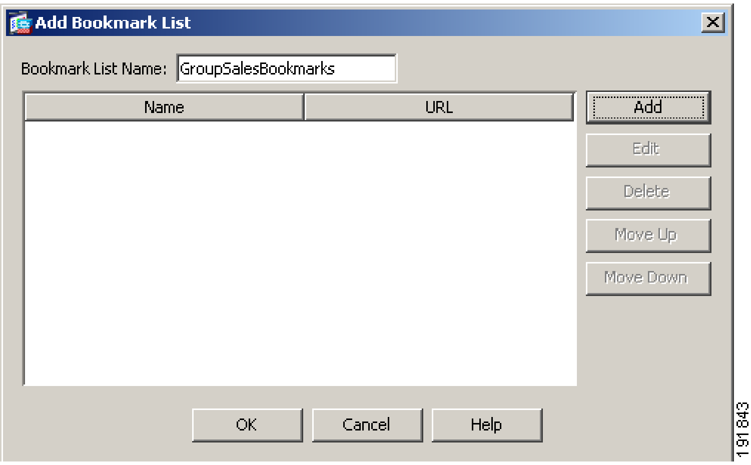
This parameter is enforced in either a VPN user, a group policy, or a dynamic access policy configuration.

Bookmarks
Template

Step 2 To create a new bookmark list, click **Add**.

To edit an existing bookmark list, choose the list and click **Edit**.

The Add Bookmark List dialog box appears.



Add Bookmark List

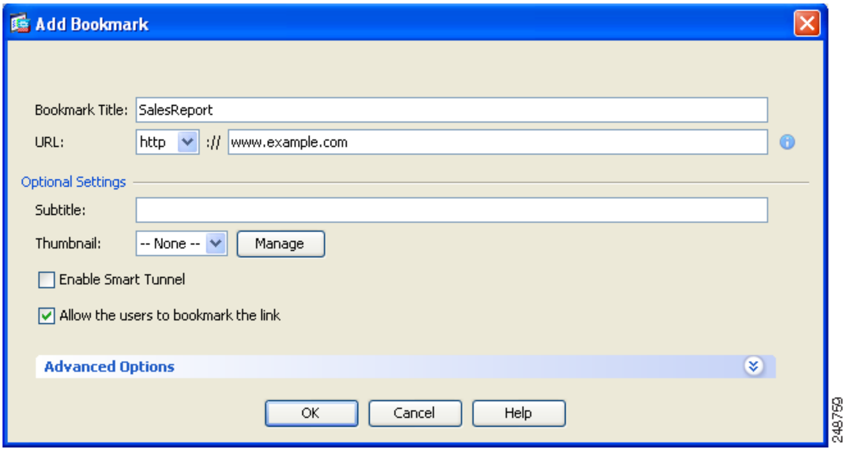
Bookmark List Name: GroupSalesBookmarks

Name	URL

Step 3 In the URL List Name field, specify a name for the list of bookmarks you are creating. This is used as the title for your VPN portal page.

Step 4 Click **Add** to add a new URL to the bookmark list.

The Add Bookmark Entry dialog box appears.



Add Bookmark

Bookmark Title: SalesReport

URL: http :// www.example.com

Optional Settings

Subtitle:

Thumbnail: -- None --

☐ Enable Smart Tunnel

☑ Allow the users to bookmark the link

Step 5 Specify a title for the list in the Bookmark Title field.

Step 6 From the URL Value drop-down list, choose the type of URL you are specifying. For example, choose http, https, ftp, and so on.

Then, specify the complete URL for the page.

Step 7 Click **OK** to return to the Add Bookmark List dialog box.

Step 8 If you are finished adding bookmark lists, click OK to return to the Configure GUI Customization Objects dialog box.

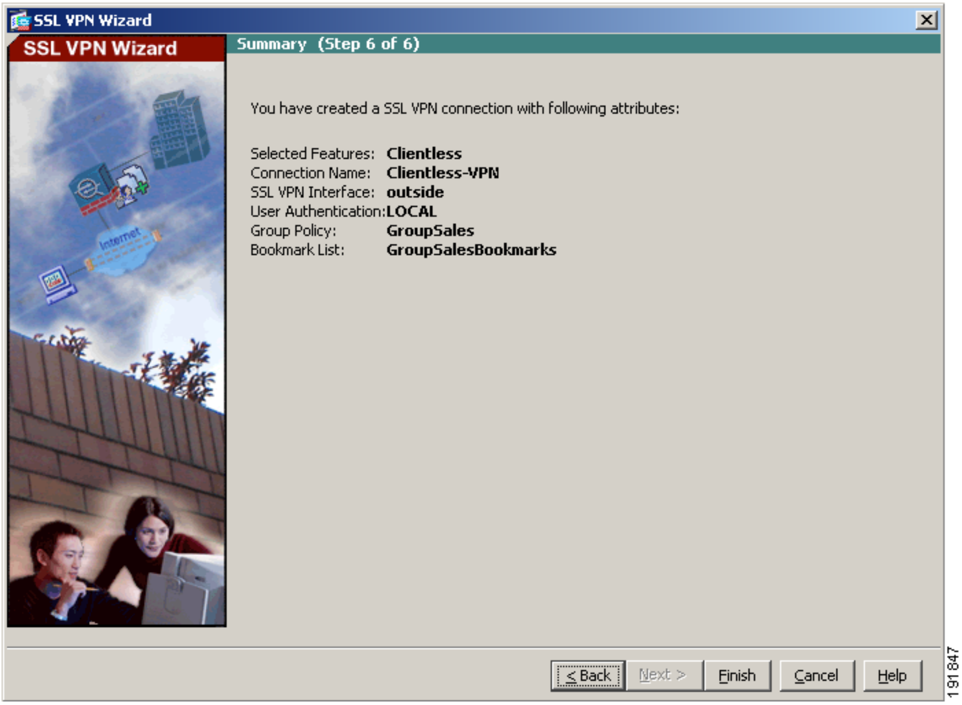
Step 9 When you are finished adding and editing bookmark lists, click **OK** to return to Step 5 of the SSL VPN Wizard.

Step 10 Choose the name of the bookmark list for this VPN group from the Bookmark List drop-down list.

Step 11 Click **Next** to continue.

Verifying the Configuration

In Step 7 of the SSL VPN Wizard, review the configuration settings to ensure that they are correct. The displayed configuration should be similar to the following.



You have created a SSL VPN connection with following attributes:

Selected Features: Clientless
Connection Name: Clientless-VPN
SSL VPN Interface: outside
User Authentication:LOCAL
Group Policy: GroupSales
Bookmark List: GroupSalesBookmarks

If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the adaptive security appliance solely in a clientless SSL VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps.

To Do This...	See...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This...	See...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 8, "Scenario: DMZ Configuration"
Configure a remote-access VPN	Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration"
Configure an AnyConnect VPN	Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client"
Configure a site-to-site VPN	Chapter 12, "Scenario: Site-to-Site VPN Configuration"

CHAPTER 12

Scenario: Site-to-Site VPN Configuration

This chapter describes how to use the adaptive security appliance to create a site-to-site VPN.

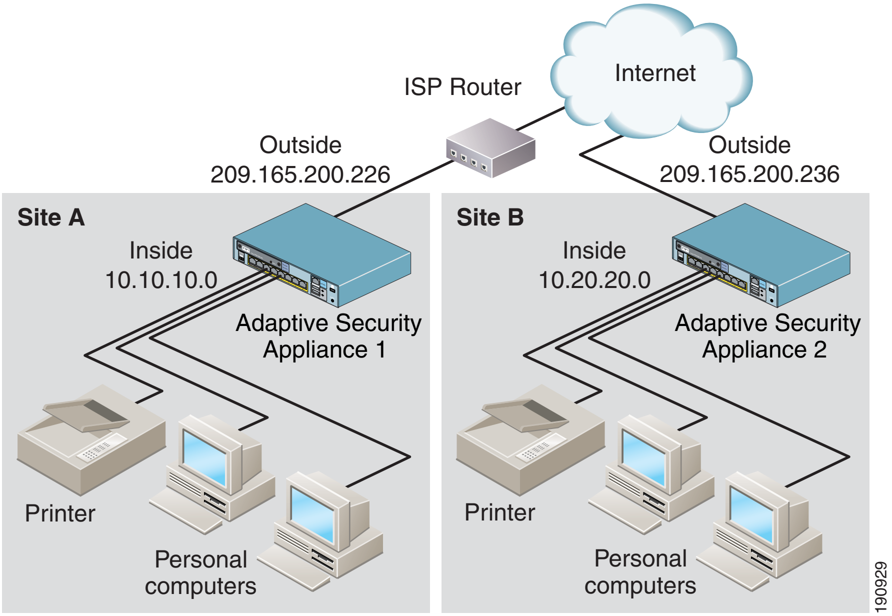
Site-to-site VPN features provided by the adaptive security appliance enable businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or tunnel, first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

This chapter includes the following sections:

Example Site-to-Site VPN Network Topology

Figure 12-1 shows an example VPN tunnel between two adaptive security appliances.

Figure 12-1 Network Layout for Site-to-Site VPN Configuration Scenario



Creating a VPN site-to-site deployment such as the one in Figure 12-1 requires you to configure two adaptive security appliances, one on each side of the connection.

Implementing the Site-to-Site Scenario

This section describes how to configure the adaptive security appliance in a site-to-site VPN deployment, using example parameters from the remote-access scenario shown in Figure 12-1.

This section includes the following topics:

- Information to Have Available, page 12-3
- Configuring the Site-to-Site VPN, page 12-3

Information to Have Available

Before you begin the configuration procedure, obtain the following information:

- IP address of the remote adaptive security appliance peer
- IP addresses of local hosts and networks permitted to use the tunnel to communicate with resources at the remote site
- IP addresses of remote hosts and networks permitted to use the tunnel to communicate with local resources

Configuring the Site-to-Site VPN

This section describes how to use the ASDM VPN Wizard to configure the adaptive security appliance for a site-to-site VPN.

This section includes the following topics:

The following sections provide detailed instructions for how to perform each configuration step.

Configuring the Security Appliance at the Local Site

Note The adaptive security appliance at the first site is referred to as Security Appliance 1 in this scenario.

To configure the Security Appliance 1, perform the following steps:

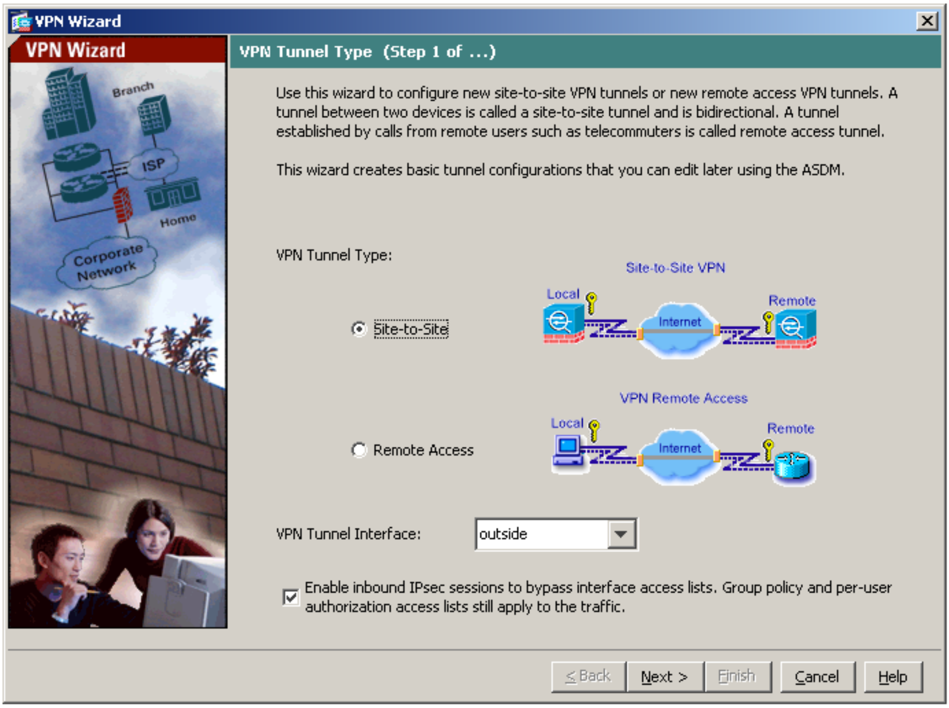
Step 1 In the main ASDM window, choose the **IPsec VPN Wizard** from the Wizards drop-down menu. ASDM opens the first VPN Wizard screen.

In Step 1 of the VPN Wizard, perform the following steps:

a. In the VPN Tunnel Type area, click the **Site-to-Site** radio button.

> **Note** The Site-to-Site VPN option connects two IPsec security gateways, which can include adaptive security appliances, VPN concentrators, or other devices that support site-to-site IPsec connectivity.

b. From the VPN tunnel Interface drop-down list, choose **Outside** as the enabled interface for the current VPN tunnel.



VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

● Site-to-Site

○ Remote Access

VPN Tunnel Interface: outside

☑ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

153904

c. Click **Next** to continue.

Providing Information About the Remote VPN Peer

The VPN peer is the system on the other end of the connection that you are configuring, usually at a remote site.

Note In this scenario, the remote VPN peer is referred to as Security Appliance 2.

In Step 2 of the VPN Wizard, perform the following steps:

Step 1 Enter the Peer IP Address (the IP address of Security Appliance 2, in this scenario 209.165.200.236) and a Tunnel Group Name (for example “Cisco”).

Step 2 Specify the type of authentication that you want to use by selecting one of the following authentication methods:

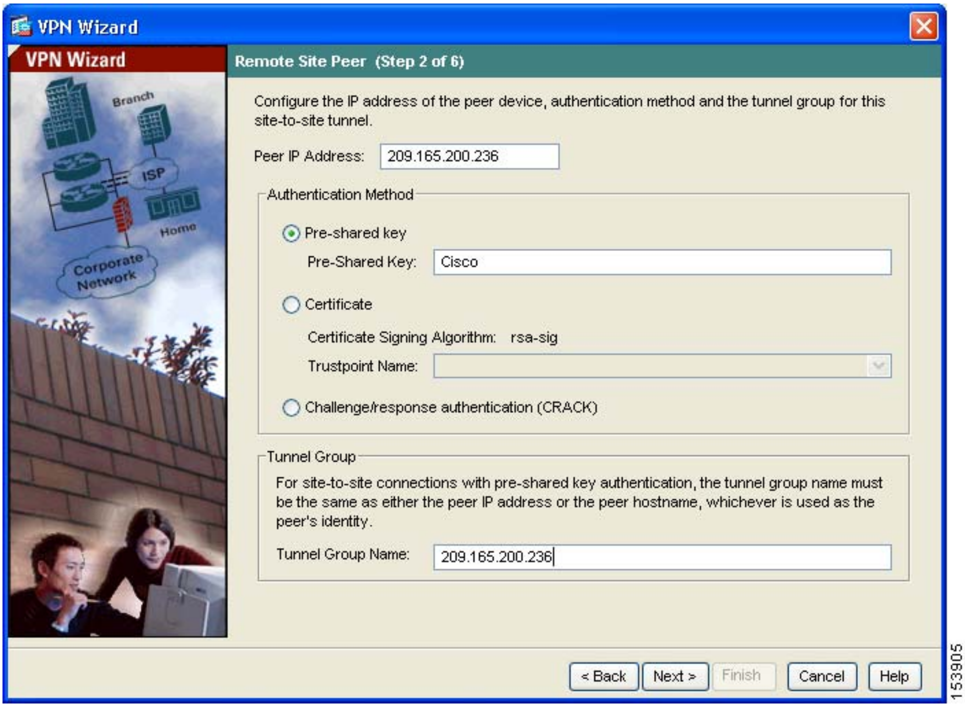
- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPsec negotiations between the adaptive security appliances.

  Note When using preshared key authentication, the Tunnel Group Name must be the IP address of the peer.

- To use digital certificates for authentication, click the **Certificate** radio button, choose the certificate signing algorithm from the Certificate Signing Algorithm drop-down list, and then choose a preconfigured trustpoint name from the Trustpoint Name drop-down list.

  If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.

- Click the **Challenge/Response Authentication** radio button to use that method of authentication.



Remote Site Peer (Step 2 of 6)

Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel.

Peer IP Address: 209.165.200.236

Authentication Method

● Pre-shared key

Pre-Shared Key: Cisco

○ Certificate

Certificate Signing Algorithm: rsa-sig

Trustpoint Name:

○ Challenge/response authentication (CRACK)

Tunnel Group

For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.

Tunnel Group Name: 209.165.200.236

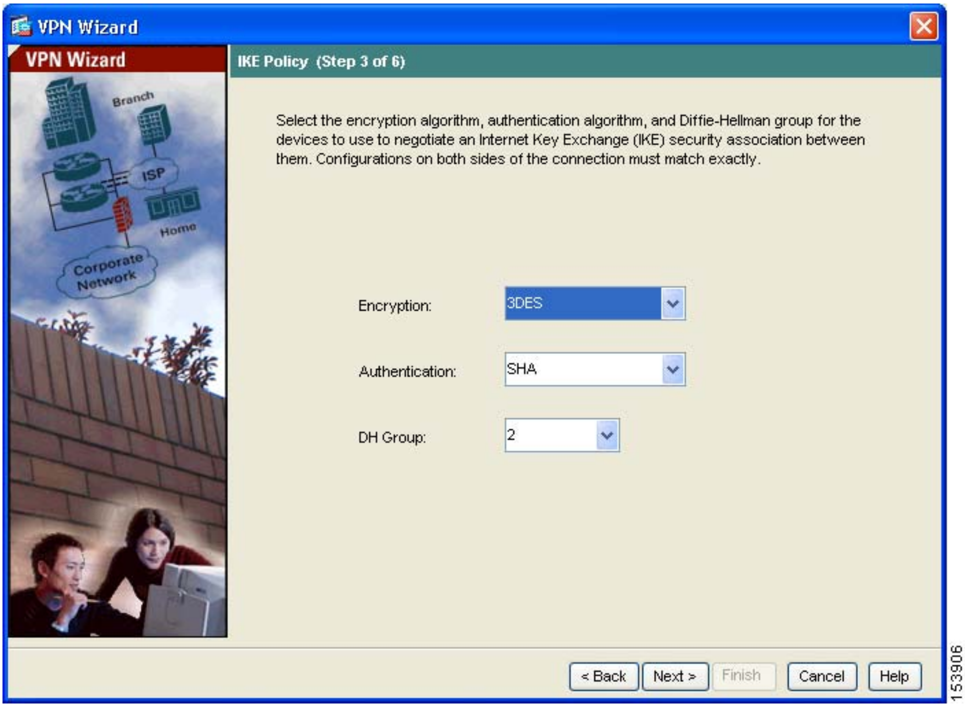
Step 3 Click **Next** to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it also provides authentication to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels between two peers.

In Step 3 of the VPN Wizard, perform the following steps:

Step 1 Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5) used by the adaptive security appliance during an IKE security association.



IKE Policy (Step 3 of 6)

Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

DH Group: 2

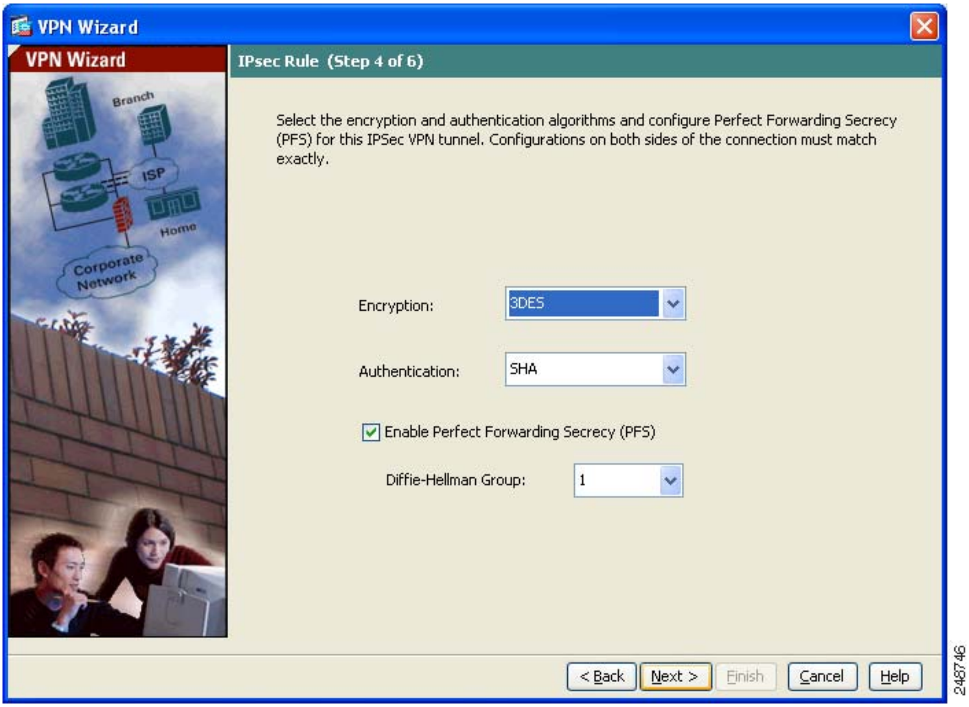
Note When configuring Security Appliance 2, enter the exact values for each of the options that you chose for Security Appliance 1. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the process.

Step 2 Click **Next** to continue.

Configuring IPsec Encryption and Authentication Parameters

In Step 4 of the VPN Wizard, perform the following steps:

Step 1 Choose the encryption algorithm (DES/3DES/AES) from the Encryption drop-down list, and the authentication algorithm (MD5/SHA) from the Authentication drop-down list.



IPsec Rule (Step 4 of 6)

Select the encryption and authentication algorithms and configure Perfect Forwarding Secrecy (PFS) for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

☑ Enable Perfect Forwarding Secrecy (PFS)

Diffie-Hellman Group: 1

Step 2 Check the **Enable Perfect Forwarding Secrecy (PFS)** check box to specify whether to use perfect forwarding secrecy, and the size of the numbers to use from the Diffie-Hellman Group drop-down list, in generating Phase 2 IPsec keys.

PFS is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless PFS is enabled. PFS uses Diffie-Hellman techniques to generate the keys.

Step 3 Click **Next** to continue.

Specifying Hosts and Networks

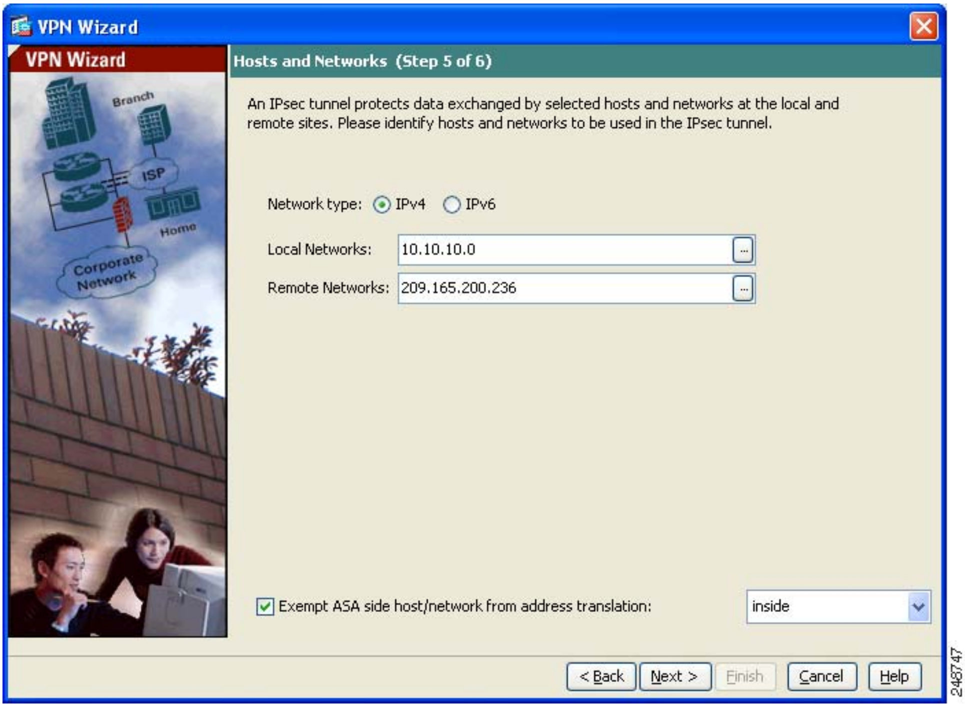
Identify hosts and networks at the local site that are permitted to use this IPsec tunnel to communicate with hosts and networks on the other side of the tunnel. Specify hosts and networks that are permitted access to the tunnel by clicking **Add** or **Delete**. In the current scenario, traffic from Network A (10.10.10.0) is encrypted by Security Appliance 1 and transmitted through the VPN tunnel.

In addition, identify hosts and networks at the remote site to be allowed to use this IPsec tunnel to access local hosts and networks. Add or remove hosts and networks dynamically by clicking **Add** or **Delete** respectively. In this scenario, for Security Appliance 1, the remote network is Network B (10.20.20.0), so traffic encrypted from this network is permitted through the tunnel.

In Step 5 of the VPN Wizard, perform the following steps:

Step 1 Enter the IP address of local networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.

Step 2 Enter the IP address of remote networks to be protected or not protected, or click the ellipsis (...) button to select from a list of hosts and networks.



Hosts and Networks (Step 5 of 6)

An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.

Network type: ● IPv4 ○ IPv6

Local Networks: 10.10.10.0

Remote Networks: 209.165.200.236

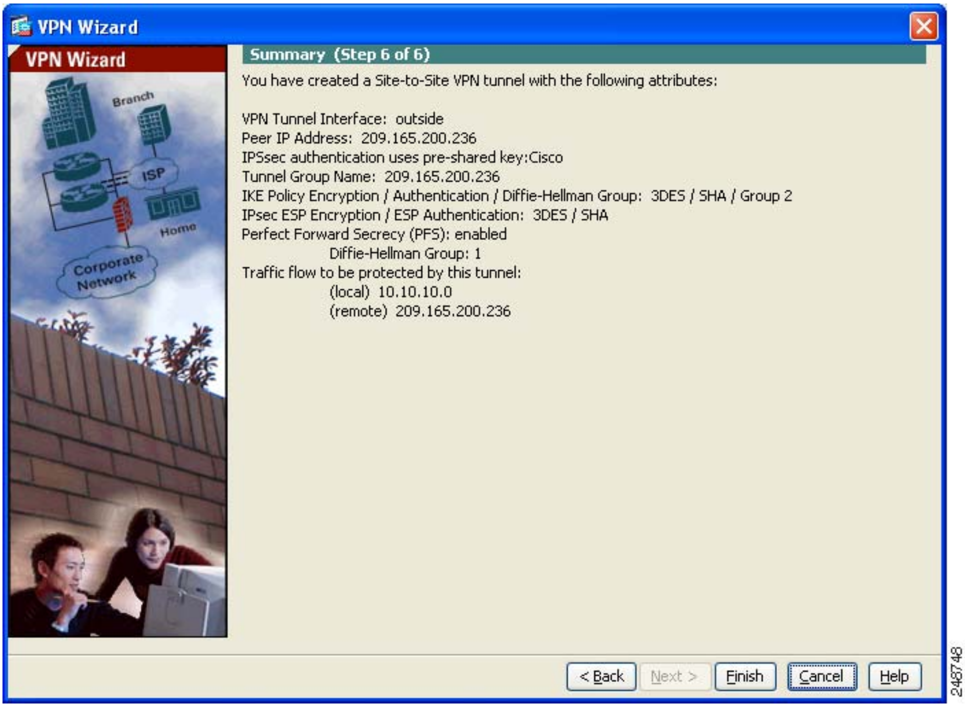
☑ Exempt ASA side host/network from address translation: inside

Step 3 If you are not using NAT or PAT, check the **Exempt ASA side host network from address translation** check box and choose the inside interface from the drop-down list.

Step 4 Click **Next** to continue.

Viewing VPN Attributes and Completing the Wizard

In Step 6 of the VPN Wizard, review the configuration list for the VPN tunnel you just created.



Summary (Step 6 of 6)

You have created a Site-to-Site VPN tunnel with the following attributes:

```
VPN Tunnel Interface:  outside
Peer IP Address:  209.165.200.236
IPSsec authentication uses pre-shared key:Cisco
Tunnel Group Name:  209.165.200.236
IKE Policy Encryption / Authentication / Diffie-Hellman Group:  3DES / SHA / Group 2
IPsec ESP Encryption / ESP Authentication:  3DES / SHA
Perfect Forward Secrecy (PFS): enabled
               Diffie-Hellman Group: 1
Traffic flow to be protected by this tunnel:
               (local)  10.10.10.0
               (remote)  209.165.200.236
```

If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

This concludes the configuration process for Security Appliance 1.

Configuring the Other Side of the VPN Connection

You have just configured the local adaptive security appliance. Next, you need to configure the adaptive security appliance at the remote site.

At the remote site, configure the second adaptive security appliance to serve as a VPN peer. Use the procedure you used to configure the local adaptive security appliance, starting with "Configuring the Security Appliance at the Local Site" section on page 12-3 and finishing with "Viewing VPN Attributes and Completing the Wizard" section on page 12-10.

Note When configuring Security Appliance 2, use the same values for each of the options that you selected for Security Appliance 1, with the exception of local hosts and networks. Mismatches are a common cause of VPN configuration failures.

For information about verifying or troubleshooting the configuration for the Site-to-Site VPN, see the section "Troubleshooting the Security Appliance" in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

For specific troubleshooting issues, see the Troubleshooting Technotes at the following location:

http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html

For help troubleshooting configuration issues, see the Configuration Examples and TechNotes at the following location:

http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html

In particular, see the technotes for Site to Site VPN (L2L) with ASA in the Troubleshooting Technotes. The troubleshooting technotes walk you through using commands like the following to troubleshoot the Site-to-site VPN configuration:

- **show run isakmp**
- **show run ipsec**
- **show run tunnel-group**
- **show run crypto map**

- **debug crypto ipsec sa**
- **debug crypto isakmp sa**

See also the *Cisco ASA 5500 Series Command Reference* for detailed information about each of these commands.

What to Do Next

If you are deploying the adaptive security appliance only in a site-to-site VPN environment, then you have completed the initial configuration. In addition, you may want to consider performing some of the following steps.

To Do This...	See...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This...	See...
Configure a remote-access VPN	Chapter 9, “Scenario: IPsec Remote-Access VPN Configuration”
Configure a clientless (browser-based) SSL VPN	Chapter 11, “Scenario: SSL VPN Clientless Connections”
Configure an SSL VPN for the Cisco AnyConnect software client	Chapter 10, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”

CHAPTER 13

Configuring the AIP SSM

The optional AIP SSM runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

If you purchased an AIP SSM, use the procedures in this chapter to:

- Configure the adaptive security appliance to identify traffic to be diverted to the AIP SSM
- Session in to the AIP SSM and run setup

Note The AIP SSM is supported in the Cisco ASA 5500 series software versions 7.0(1) and later.

You can install the AIP SSM into an ASA 5500 series adaptive security appliance. The AIP SSM runs advanced IPS software that provides a proactive, full-featured Intrusion Prevention System to stop malicious traffic, including worms and network viruses, before they can affect your network. This chapter includes the following sections:

Understanding the AIP SSM

This section includes the following topics:

- How the AIP SSM Works with the Adaptive Security Appliance, page 13-2
- Operating Modes, page 13-3
- Using Virtual Sensors, page 13-4

How the AIP SSM Works with the Adaptive Security Appliance

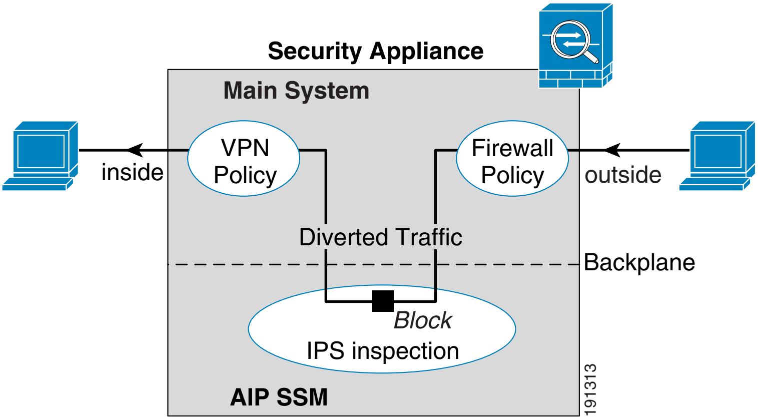
The AIP SSM runs a separate application from the adaptive security appliance. It is, however, integrated into the adaptive security appliance traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you identify traffic for IPS inspection on the adaptive security appliance, traffic flows through the adaptive security appliance and the AIP SSM in the following way:

1. Traffic enters the adaptive security appliance.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane.

   See the "Operating Modes" section on page 13-3 for information about only sending a copy of the traffic to the AIP SSM.
4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the adaptive security appliance over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the adaptive security appliance.

Figure 13-1 shows the traffic flow when running the AIP SSM in inline mode. In this example, the AIP SSM automatically blocks traffic that it identified as an attack. All other traffic is forwarded through the adaptive security appliance.

Figure 13-1 AIP SSM Traffic Flow in the Adaptive Security Appliance: Inline Mode

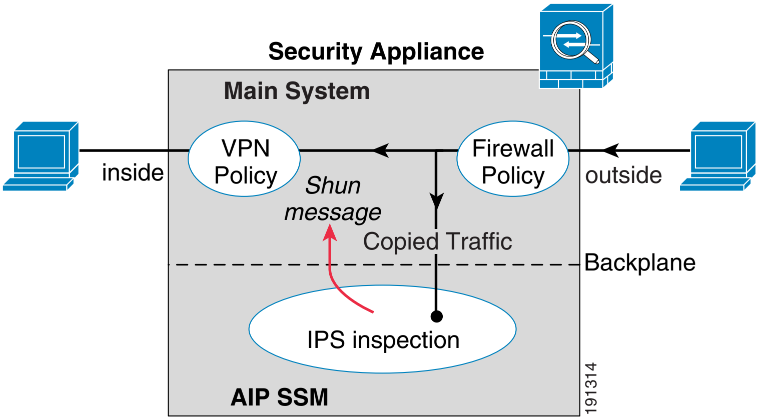


Operating Modes

You can send traffic to the AIP SSM using one of the following modes:

- Inline mode—This mode places the AIP SSM directly in the traffic flow (see Figure 13-1). No traffic that you identified for IPS inspection can continue through the adaptive adaptive security appliance without first passing through, and being inspected by, the AIP SSM. This mode is the most secure because every packet that you identify for inspection is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.
- Promiscuous mode—This mode sends a duplicate stream of traffic to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike the inline mode, in promiscuous mode the AIP SSM can only block traffic by instructing the adaptive adaptive security appliance to shun the traffic or by resetting a connection on the adaptive adaptive security appliance. Also, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the adaptive adaptive security appliance before the AIP SSM can shun it. Figure 13-2 shows the AIP SSM in promiscuous mode. In this example, the AIP SSM sends a shun message to the adaptive security appliance for traffic it identified as a threat.

Figure 13-2 AIP SSM Traffic Flow in the Adaptive Security Appliance: Promiscuous Mode



Using Virtual Sensors

The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode adaptive security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.

Figure 13-3 shows one security context paired with one virtual sensor (in inline mode), while two security contexts share the same virtual sensor.

Figure 13-3 Security Contexts and Virtual Sensors

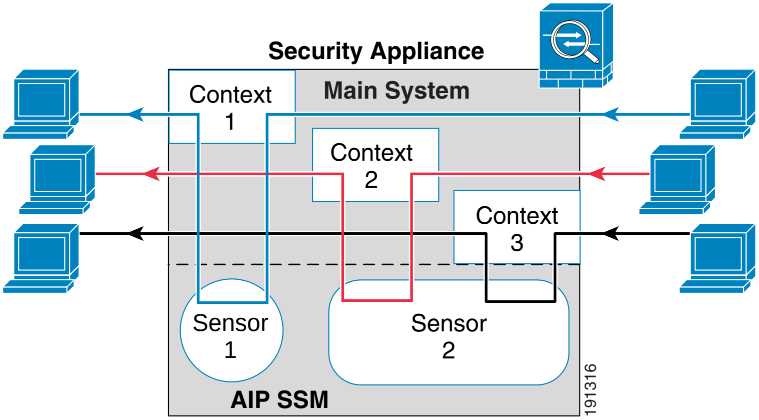
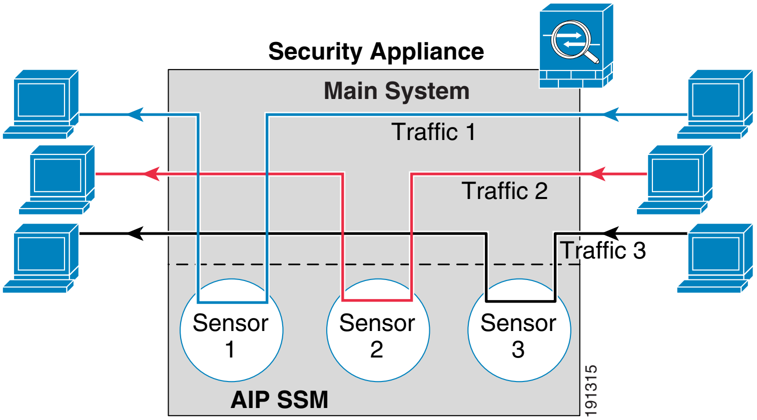


Figure 13-4 shows a single mode adaptive security appliance paired with multiple virtual sensors (in inline mode); each defined traffic flow goes to a different sensor.

Figure 13-4 Single Mode Security Appliance with Multiple Virtual Sensors



Configuring the AIP SSM

This section includes the following topics:

AIP SSM Procedure Overview

Configuring the AIP SSM is a process that includes configuration of the AIP SSM and then configuration of the ASA 5500 series adaptive security appliance:

1. Session to the AIP SSM from the adaptive security appliance. See the "Sessioning to the AIP SSM" section on page 13-6.
2. On the AIP SSM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. Configure the inspection and protection policy for each virtual sensor if you want to run the AIP SSM in multiple sensor mode. See the "Configuring the Security Policy on the AIP SSM" section on page 13-8.
3. On the ASA 5500 series adaptive security appliance in multiple context mode, specify which IPS virtual sensors are available for each context (if you configured virtual sensors). See the "Assigning Virtual Sensors to Security Contexts" section on page 13-9.
4. On the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM. See the "Diverting Traffic to the AIP SSM" section on page 13-11.

Sessioning to the AIP SSM

To begin configuring the AIP SSM, session to the AIP SSM from the adaptive adaptive security appliance. (You can alternatively connect directly to the AIP SSM management interface using SSH or Telnet.)

To session to the AIP SSM from the adaptive adaptive security appliance, perform the following steps:

Step 1 To session from the ASA 5500 series adaptive security appliance to the AIP SSM, enter the following command:

```
hostname# session 1

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

Step 2 Enter the username and password. The default username and password is "cisco."

Note The first time you log in to the AIP SSM, you are prompted to change the default password. Passwords must be at least eight characters long and not a word in the dictionary.

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United
States
and local country laws governing import, export, transfer and use.
Delivery
of Cisco cryptographic products does not imply third-party authority
to import,
export, distribute or use encryption. Importers, exporters,
distributors and
users are responsible for compliance with U.S. and local country laws.
By using
this product you agree to comply with applicable laws and regulations.
If you
are unable to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to
export@cisco.com.

***LICENSE NOTICE***
```

```
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

Note If you see the preceding license notice (which displays only in some versions of software), you can ignore the message until you need to upgrade the signature files on the AIP SSM. The AIP SSM continues to operate at the current signature level until a valid license key is installed. You can install the license key at a later time. The license key does not affect the current functionality of the AIP SSM.

Configuring the Security Policy on the AIP SSM

On the AIP SSM, to configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected, perform the following steps. To session from the adaptive security appliance to the AIP SSM, see the "Sessioning to the AIP SSM" section on page 13-6.

To configure the security policy on the AIP SSM, perform the following steps:

Step 1 To run the setup utility for initial configuration of the AIP SSM, enter the following command:

```
sensor# setup
```

Step 2 Configure the IPS security policy. If you configure virtual sensors in IPS Version 6.0 or above, you identify one of the sensors as the default. If the ASA 5500 series adaptive adaptive security appliance does not specify a virtual sensor name in its configuration, the default sensor is used.

Because the IPS software that runs on the AIP SSM is beyond the scope of this document, detailed configuration information is available in the following documents:

- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Command Reference for Cisco Intrusion Prevention System*

Step 3 When you are done configuring the AIP SSM, exit the IPS software by entering the following command:

```
sensor# exit
```

If you sessioned to the AIP SSM from the adaptive security appliance, you return to the adaptive security appliance prompt.

Assigning Virtual Sensors to Security Contexts

If the adaptive security appliance is in multiple context mode, then you can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

To assign one or more sensors to a security context, perform the following steps:

Step 1 To enter context configuration mode, enter the following command in the system execution space:

```
hostname(config)# context name
hostname(config-ctx)#
```

Step 2 To assign a virtual sensor to the context, enter the following command:

```
hostname(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

Enter this command for each sensor you want to assign to the context.

The *sensor _name* argument is the sensor name configured on the AIP SSM. To view the sensors that are configured on the AIP SSM, enter the **allocate-ips ?** command. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the AIP SSM, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the AIP SSM, the context assumes the sensor is down.

Use the *mapped_name* argument as an alias for the sensor name that can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called "sensor1" and "sensor2," then you can map the "highsec" and "lowsec" senors to sensor1 and sensor2 in context A, but map the "medsec" and "lowsec" sensors to sensor1 and sensor2 in context B.

The **default** keyword sets one sensor per context as the default sensor; if the context configuration does not specify a sensor name, the context uses this default sensor. You can only configure one default sensor per context. If you want to change the default sensor, enter the **no allocate-ips** *sensor_name* command to remove the current default sensor before you allocate a new default sensor. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.

Step 3 Repeat Step 1 and Step 2 for each context.

Step 4 To configure the context IPS policy, change to the context execution space using the following command:

```
hostname(config-ctx)# changeto context context_name
```

where the *context_name* argument is the name of the context you want to configure. Change to each context to configure the IPS security policy as described in "Diverting Traffic to the AIP SSM" section on page 13-11.

The following example assigns sensor1 and sensor2 to context A, and sensor1 and sensor3 to context B. Both contexts map the sensor names to "ips1" and "ips2." In context A, sensor1 is set as the default sensor, but in context B, no default is set so the default that is configured on the AIP SSM is used.

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/0.110-gigabitethernet0/0.115 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface
gigabitethernet0/1.230-gigabitethernet0/1.235 int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url
ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

Diverting Traffic to the AIP SSM

To identify traffic to divert from the adaptive adaptive security appliance to the AIP SSM, perform the following steps. In multiple context mode, perform these steps in each context execution space.

Step 1 To identify the traffic that you want to be inspected by the AIP SSM, add one or more class maps using the **class-map** command.

For example, you can match all traffic using the following commands:

```
hostname(config)# class-map IPS
hostname(config-cmap)# match any
```

To match specific traffic, you can match an access list:

```
hostname(config)# access list IPS extended permit ip any 10.1.1.1
255.255.255.255
hostname(config)# class-map IPS
hostname(config-cmap)# match access-list IPS
```

Step 2 To add or edit a policy map that sets the action to divert traffic to the AIP SSM, enter the following commands:

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

where the *class_map_name* is the class map from Step 1.

For example:

```
hostname(config)# policy-map IPS
hostname(config-pmap)# class IPS
```

Step 3 To divert the traffic to the AIP SSM, enter the following command:

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor {sensor_name | mapped_name}]
```

where the **inline** and **promiscuous** keywords control the operating mode of the AIP SSM. See the "Operating Modes" section on page 13-3 for more details.

The **fail-close** keyword sets the adaptive security appliance to block all traffic if the AIP SSM is unavailable.

The **fail-open** keyword sets the adaptive security appliance to allow all traffic through, uninspected, if the AIP SSM is unavailable.

If you use virtual sensors on the AIP SSM, you can specify a sensor name using the **sensor** *sensor_name* argument. To see available sensor names, enter the **ips ... sensor ?** command. Available sensors are listed. You can also use the **show ips** command. If you use multiple context mode on the adaptive security appliance, you can only specify sensors that you assigned to the context (see the "Assigning Virtual Sensors to Security Contexts" section on page 13-9). Use the *mapped_name* if configured in the context. If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM. If you enter a name that does not yet exist on the AIP SSM, you get an error, and the command is rejected.

Step 4 (Optional) To divert another class of traffic to the AIP SSM, and set the IPS policy, enter the following commands:

```
hostname(config-pmap-c)# class class_map_name2
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor sensor_name]
```

where the *class_map_name2* argument is the name of a separate class map on which you want to perform IPS inspection. See Step 3 for information about the command options.

Traffic cannot match more than one class map for the same action type; so if you want network A to go to sensorA, but want all other traffic to go to sensorB, then you need to enter the **class** command for network A before you enter the **class** command for all traffic; otherwise all traffic (including network A) will match the first **class** command, and will be sent to sensorB.

Step 5 To activate the policy map on one or more interfaces, enter the following command:

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname
```

where *policy_map_name* is the policy map you configured in Step 2. To apply the policy map to traffic on all the interfaces, use the **global** keyword. To apply the policy map to traffic on a specific interface, use the **interface** *interface_ID* option, where *interface_ID* is the name assigned to the interface with the **nameif** command.

Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic if the AIP SSM card fails for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM card fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0
255.255.255.0
```

```
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0
255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface
outside
```

What to Do Next

You are now ready to configure the adaptive security appliance for intrusion prevention. Use the following documents to continue configuring the adaptive security appliance for your implementation.

To Do This ...	See ...
Configure the IPS sensor	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
Optimize performance for the AIP SSM and CSC SSM by creating more efficient service policies	*Cisco ASA 5500 Series Configuration Guide using the CLI*

After you have configured the IPS sensory and AIP SSM software, you may want to consider performing some of the following additional steps.

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure protection of a DMZ web server	Chapter 8, "Scenario: DMZ Configuration"
Configure a remote-access VPN	Chapter 9, "Scenario: IPsec Remote-Access VPN Configuration"
Configure remote-access SSL connection for software clients	Chapter 10, "Scenario: Configuring Connections for a Cisco AnyConnect VPN Client"
Configure SSL connections for browser-based remote access	Chapter 11, "Scenario: SSL VPN Clientless Connections"
Configure a site-to-site VPN	Chapter 12, "Scenario: Site-to-Site VPN Configuration"

CHAPTER 14

Configuring the CSC SSM

The ASA 5500 series adaptive security appliance supports the CSC SSM, which runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic by scanning the FTP, HTTP, POP3, and SMTP traffic that the adaptive security appliance diverts to it.

Note The CSC SSM requires the Cisco ASA 5500 series software Version 7.1(1) or later.

This chapter includes the following sections:

About the CSC SSM

The CSC SSM maintains a file containing signature profiles of suspicious content, updated regularly from an update server at Trend Micro. The CSC SSM scans traffic it receives from the adaptive security appliance and compares it to the content profiles it obtains from Trend Micro. It then forwards legitimate content on to the adaptive security appliance for routing, or blocks and reports content that is suspicious.

In addition to obtaining content profiles from Trend Micro, system administrators can also customize the configuration so that the CSC SSM scans for additional traffic types or locations. For example, system administrators can configure the CSC SSM to block or filter specific URLs, as well as scan for FTP and e-mail parameters.

You use ASDM for system setup and monitoring of the CSC SSM. For advanced configuration of content security policies in the CSC SSM software, you access the web-based GUI for the CSC SSM by clicking links within ASDM.

This chapter describes how to configure the adaptive security appliance for the deployment. Use of the CSC SSM GUI is explained in the *Cisco Content Security and Control SSM Administrator Guide*.

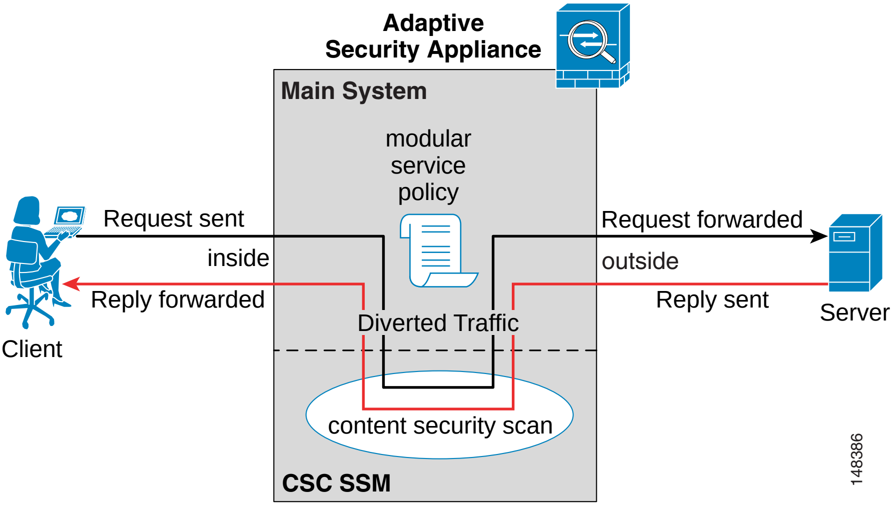
About Deploying the Adaptive Security Appliance with the CSC SSM

In a network in which the adaptive security appliance is deployed with the CSC SSM, you configure the adaptive security appliance to send to the CSC SSM only the types of traffic that you want to be scanned.

Figure 14-1 illustrates the basic traffic flow between a company network, the adaptive security appliance and CSC SSM, and the Internet. The network illustrated in Figure 14-1 includes the following:

- An adaptive security appliance with a CSC SSM installed and configured
- A service policy on the adaptive security appliance specifies which traffic is diverted to the CSC SSM for scanning

Figure 14-1 CSC SSM Traffic Flow



In this example, clients could be network users who are accessing a website, downloading files from an FTP server, or retrieving mail from a POP3 server.

In this configuration, the traffic flow is as follows:

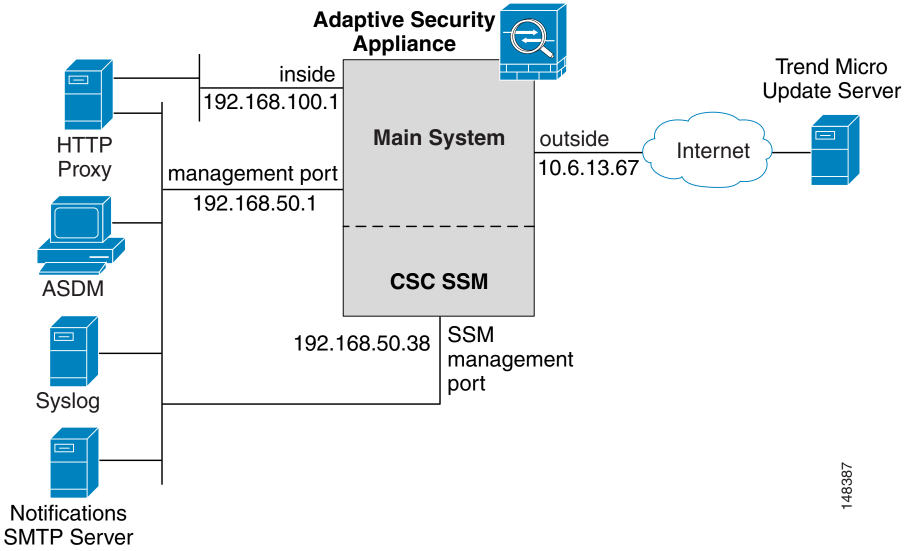
1. The client initiates a request.
2. The adaptive security appliance receives the request and forwards it to the Internet.
3. When the requested content is retrieved, the adaptive security appliance determines whether its service policies define this content type as one that should be diverted to the CSC SSM for scanning, and does so if appropriate.
4. The CSC SSM receives the content from the adaptive security appliance, scans it and compares it to its latest update of the Trend Micro content filters.
5. If the content is suspicious, the CSC SSM blocks the content and reports the event. If the content is not suspicious, the CSC SSM forwards the requested content back to the adaptive security appliance for routing.

Note The CSC SSM handles SMTP traffic somewhat differently than other content types. After the CSC SSM receives SMTP traffic and scans it, it does not forward the traffic back to the adaptive security appliance for routing. Rather, the CSC SSM forwards the SMTP traffic directly to the SMTP servers protected by the adaptive security appliance.

Scenario: Security Appliance with CSC SSM Deployed for Content Security

Figure 14-2 is an illustration of a typical deployment of the adaptive security appliance with CSC SSM.

Figure 14-2 CSC SSM Deployment Scenario



In this scenario, the customer has deployed an adaptive security appliance with a CSC SSM for content security. Of particular interest are the following points:

- The adaptive security appliance is on a dedicated management network. Although using a dedicated management network is not required, we recommend it for security purposes.
- This adaptive security appliance configuration has two management ports: one for the adaptive security appliance itself, and another for the CSC SSM. All administration hosts must be able to access both IP addresses.
- The HTTP proxy server is connected to both the inside network and the dedicated management network. This enables the CSC SSM to retrieve updated content security filters from the Trend Micro update server.
- The management network includes an SMTP server so that administrators can be notified of CSC SSM events. The management network also includes a syslog server to store logs generated by the CSC SSM.

This section includes the following topics:

- Configuration Requirements, page 14-5
- Configuring the CSC SSM for Content Security, page 14-6

Configuration Requirements

When you plan the adaptive security appliance deployment, it is critical that the network adheres to the following requirements:

- The SSM management port IP address must be accessible by the hosts used to run ASDM. However, the IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.
- The SSM management port must be able to connect to the Internet so that the CSC SSM can reach the Trend Micro update server.

Configuring the CSC SSM for Content Security

If you ordered your adaptive security appliance with the optional CSC SSM module, there are several steps you need to perform to complete the initial configuration. Some configuration steps are performed on the adaptive security appliance, and some steps are performed in the software running on the CSC SSM.

If you followed the procedures in earlier chapters of this document, at this point you have an adaptive security appliance system running with licensed software, and you have entered basic system values using the Startup Wizard. Your next steps are to configure the adaptive security appliance for a content security deployment.

The basic steps are as follows:

1. Obtain software activation key from Cisco.com.
2. Gather the information you need to configure the CSC SSM.
3. Using ASDM, verify time settings.
4. In ASDM, run the CSC setup wizard to configure the CSC SSM.
5. Using ASDM, configure the adaptive security appliance to divert traffic to the CSC SSM for scanning.

These steps are described in detail in the sections that follow.

This section includes the following topics:

- Obtain Software Activation Key from Cisco.com, page 14-6
- Gather Information, page 14-7
- Verify Time Settings, page 14-7
- Run the CSC Setup Wizard, page 14-8

Obtain Software Activation Key from Cisco.com

With the CSC SSM, you should have received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL:

`http://www.cisco.com/go/license`

After you register, you will receive activation keys by e-mail. The activation keys are required before you can complete the procedure described in the "Run the CSC Setup Wizard" section on page 14-8.

Gather Information

Before you start configuring the adaptive security appliance and the CSC SSM, gather the following information:

- IP address and netmask for the CSC SSM management port, gateway IP address and netmask. The adaptive security appliance IP address was assigned when you completed the Startup Wizard, described in Appendix A, "Obtaining a 3DES/AES License."

  Note The SSM management port IP address must be accessible by the hosts used to run ASDM. The IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.

- Hostname and domain name to be used for the CSC SSM
- DNS Server IP address
- HTTP proxy server IP address (if your network uses a proxy for HTTP access to the Internet)
- E-mail address to be used for e-mail notifications; IP address and port number of an SMTP server
- IP addresses of hosts and networks to be allowed management access to the CSC SSM

Verify Time Settings

Verify the accuracy of the adaptive security appliance time settings, including the time zone. Time accuracy is important for logging security events, automatic updates of the content filter lists on the CSC SSM and for licensing, because licenses are time sensitive.

To ensure the accuracy of time settings, perform the following tasks:

- If you control time settings manually, verify the clock settings. In ASDM, choose **Configuration > Device Setup > System Time > Clock**.
- If you are using NTP to control time settings, verify the NTP configuration. In ASDM, choose **Configuration > Device Setup > System Time > NTP**.

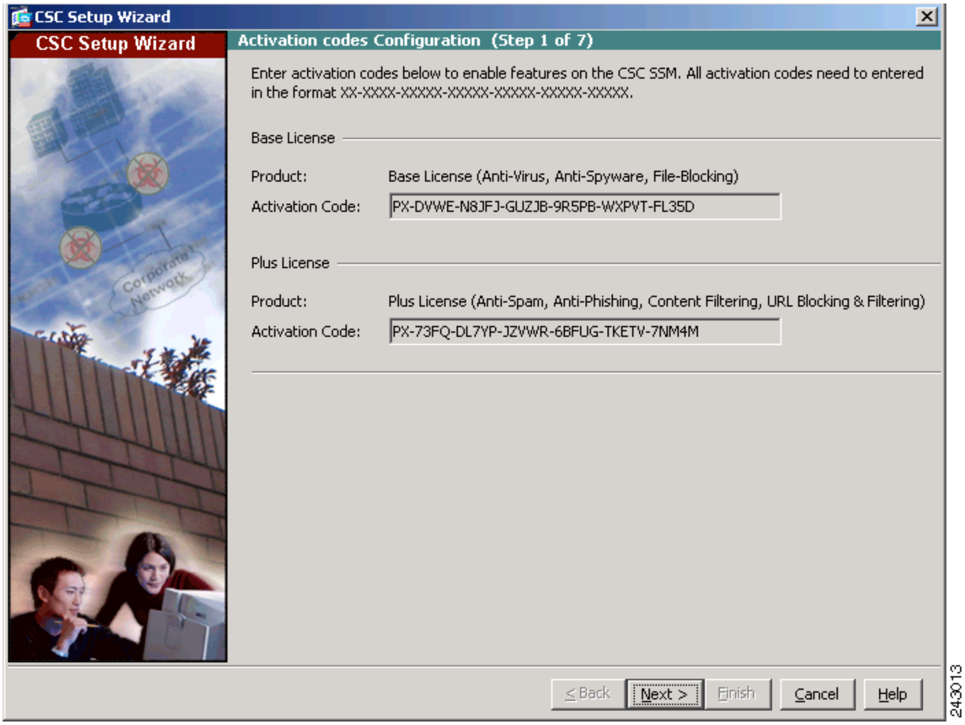
Run the CSC Setup Wizard

To run the CSC Setup Wizard, perform the following steps:

Step 1 In the ASDM main application window, choose **Configuration** > **Trend Micro Content Security > Wizard Setup > Launch Wizard Setup**.

The CSC Setup Wizard screen appears.

Step 2 In Step 1 of the CSC Setup Wizard, enter the product activation codes for the Base license and if applicable, for the Plus license. You can enter the activation code for the Plus license after the initial configuration of the CSC SSM.



Activation codes Configuration (Step 1 of 7)

Enter activation codes below to enable features on the CSC SSM. All activation codes need to entered in the format XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Base License

Product: Base License (Anti-Virus, Anti-Spyware, File-Blocking)

Activation Code: PX-DVWE-N8JFJ-GUZJB-9R5PB-WXPVT-FL35D

Plus License

Product: Plus License (Anti-Spam, Anti-Phishing, Content Filtering, URL Blocking & Filtering)

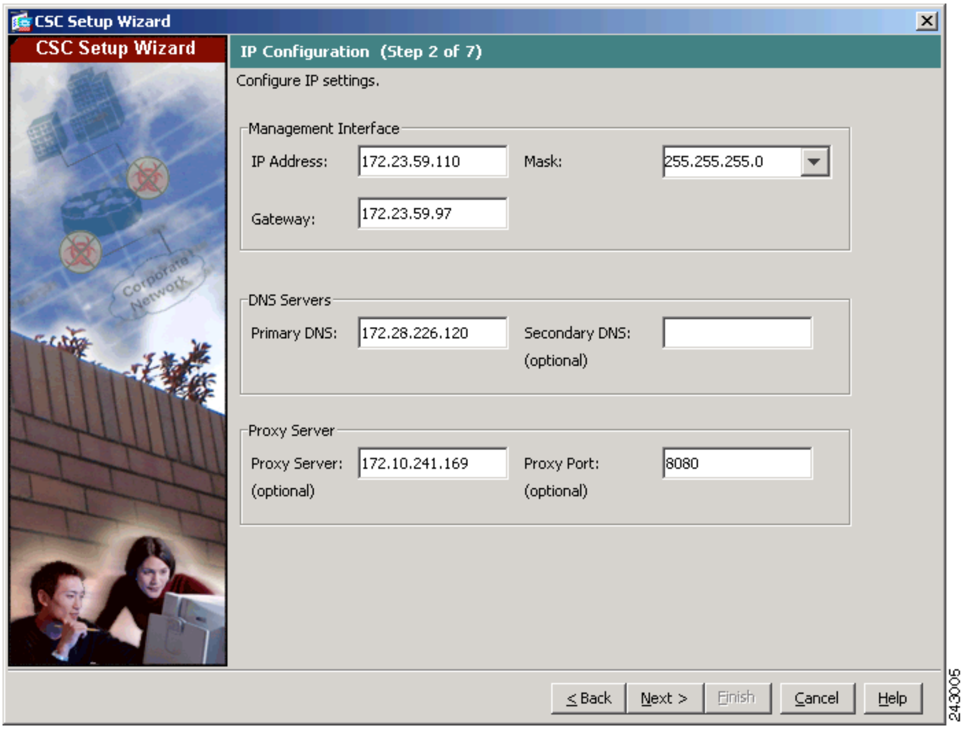
Activation Code: PX-73FQ-DL7YP-JZVWR-6BFUG-TKETV-7NM4M

Step 3 Click **Next**.

Step 4 In Step 2 of the CSC Setup Wizard, enter the following information:

- IP address, network mask, and gateway IP address for the CSC management interface
- IP address for the Primary DNS server

- (Optional) IP address and proxy port of the HTTP proxy server (only if your network uses an HTTP proxy server to send HTTP requests to the Internet)


CSC Setup Wizard

IP Configuration (Step 2 of 7)

Configure IP settings.

Management Interface

IP Address: 172.23.59.110 Mask: 255.255.255.0

Gateway: 172.23.59.97

DNS Servers

Primary DNS: 172.28.226.120 Secondary DNS: (optional)

Proxy Server

Proxy Server: (optional) 172.10.241.169 Proxy Port: (optional) 8080

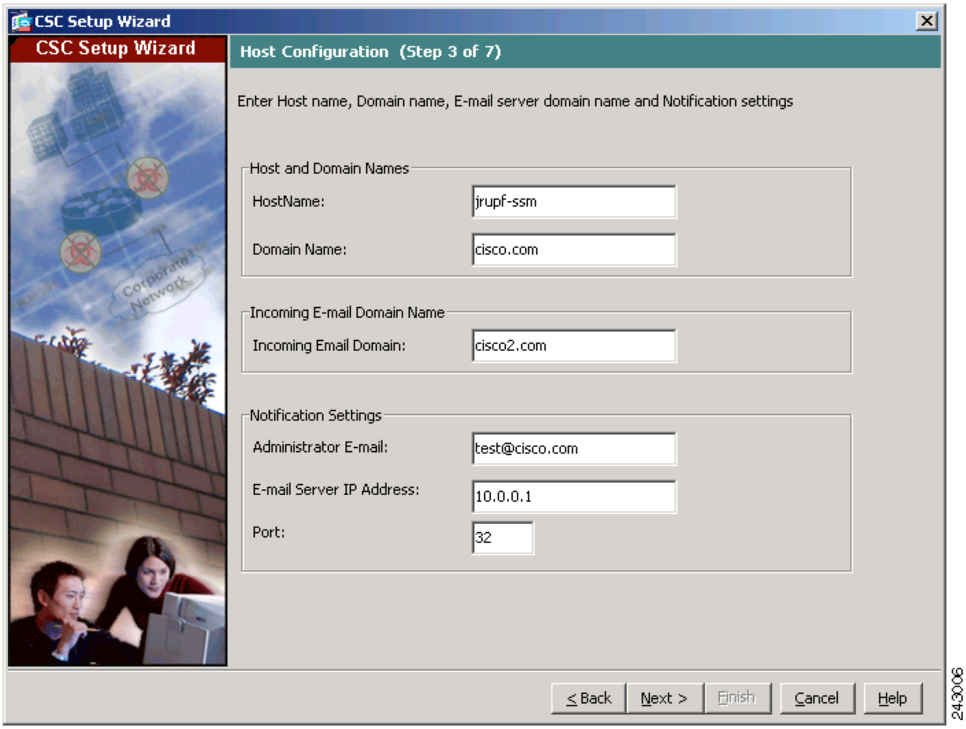
Step 5 Click **Next**.

Step 6 In Step 3 of the CSC Setup Wizard, enter the following information:

- Hostname and domain name of the CSC SSM.
- Domain name used by the local mail server as the incoming domain.

Note Anti-spam policies are applied only to e-mail traffic entering this domain.

- Administrator e-mail address, e-mail server IP address, and port to be used for notifications.



CSC Setup Wizard

Host Configuration (Step 3 of 7)

Enter Host name, Domain name, E-mail server domain name and Notification settings

Host and Domain Names

HostName: jrupf-ssm

Domain Name: cisco.com

Incoming E-mail Domain Name

Incoming Email Domain: cisco2.com

Notification Settings

Administrator E-mail: test@cisco.com

E-mail Server IP Address: 10.0.0.1

Port: 32

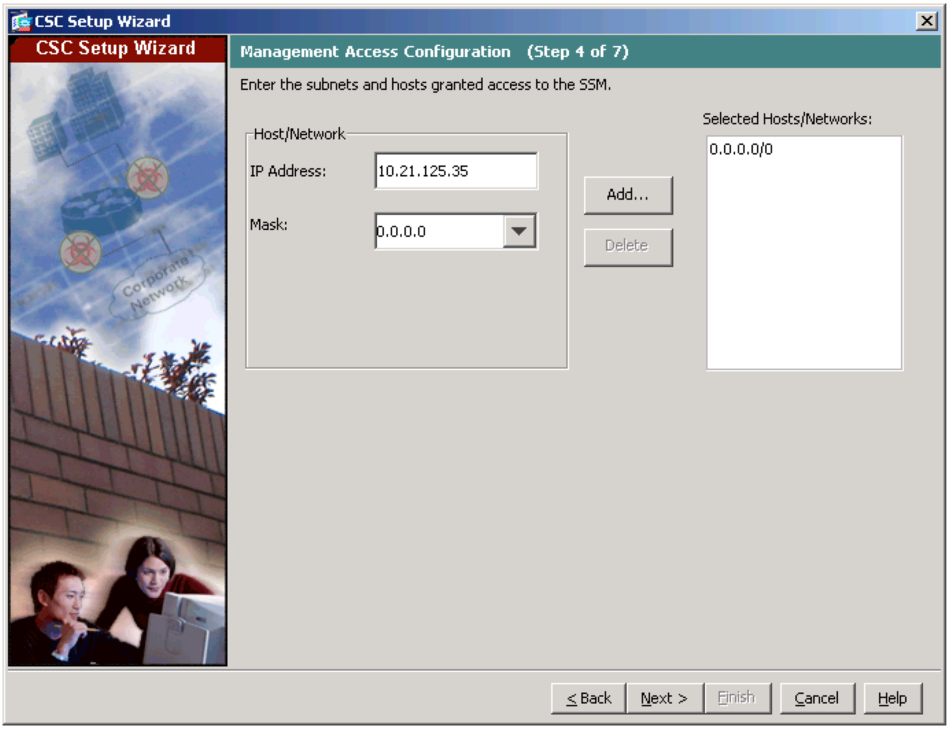
Step 7 Click **Next**.

Step 8 In Step 4 of the CSC Setup Wizard, enter the following information:

- IP address and network mask for each subnet and host that should have management access to the CSC SSM. By default, all networks have management access to the CSC SSM.

  Note For security purposes, we recommend that you restrict access to specific subnets or management hosts.

- To enter a new host and network combination of settings, click **Add**.
- To remove an existing host and network combination, choose one from the Selected Hosts/Networks list, and click **Delete**.



CSC Setup Wizard

Management Access Configuration (Step 4 of 7)

Enter the subnets and hosts granted access to the SSM.

Host/Network

IP Address: 10.21.125.35

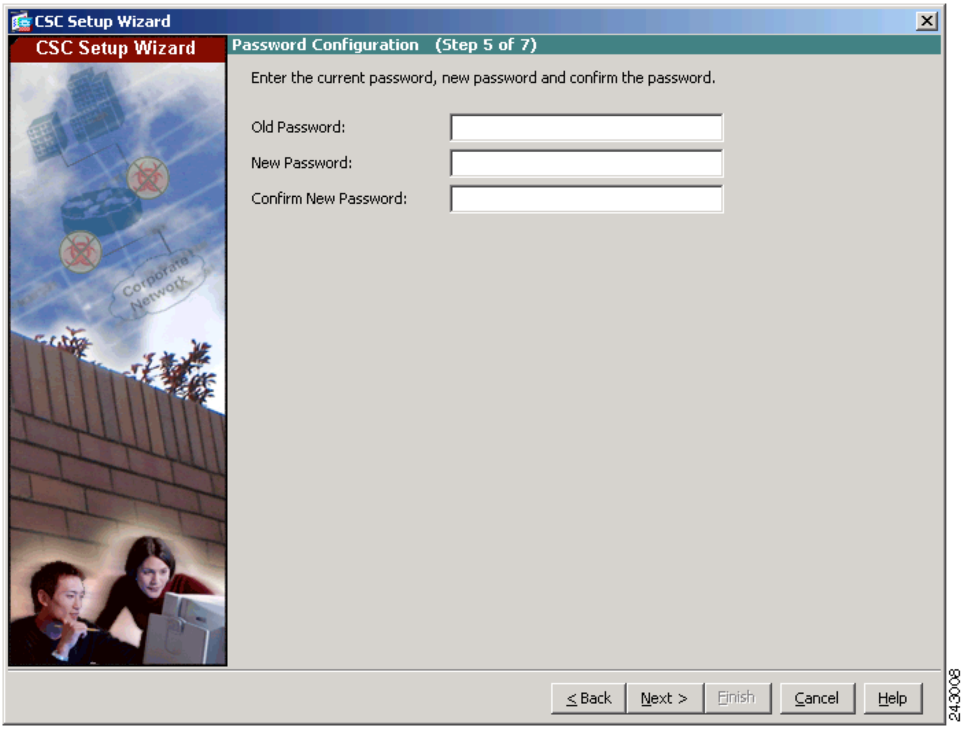
Mask: 0.0.0.0

Selected Hosts/Networks: 0.0.0.0/0

Step 9 Click **Next**.

Step 10 In Step 5 of the CSC Setup Wizard, enter the following information:

- The default factory configuration password, “cisco.”
- A new password for management access.
- Confirmation of the new password.



CSC Setup Wizard

Password Configuration (Step 5 of 7)

Enter the current password, new password and confirm the password.

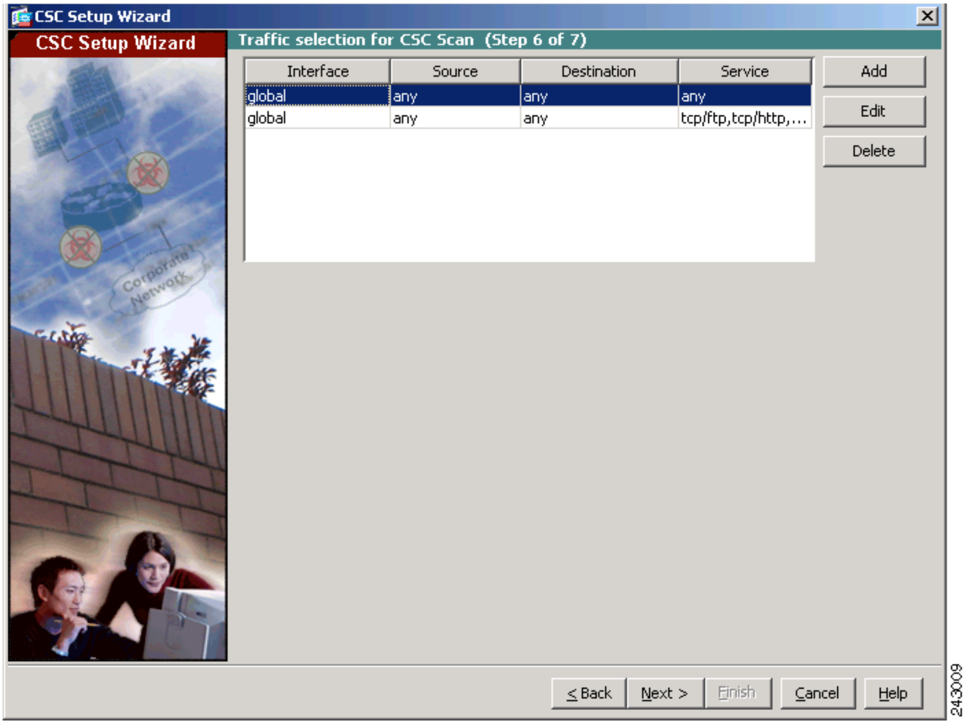
Old Password:

New Password:

Confirm New Password:

Step 11 Click **Next**.

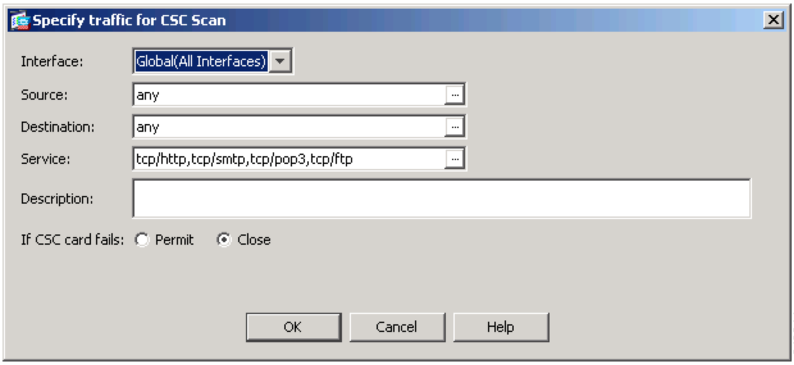
Step 12 In Step 6 of the CSC Setup Wizard, define traffic selections for CSC scanning. Click **Add**.



Traffic selection for CSC Scan (Step 6 of 7)

Interface	Source	Destination	Service
global	any	any	any
global	any	any	tcp/ftp,tcp/http,...

The Specify Traffic for CSC Scan dialog box appears.



Specify traffic for CSC Scan

Interface: Global(All Interfaces)

Source: any

Destination: any

Service: tcp/http,tcp/smtp,tcp/pop3,tcp/ftp

Description:

If CSC card fails: ○ Permit ● Close

243011

Step 13 Choose the interface from the drop-down list. Available options are global (all interfaces), inside, management, and ssm management.

Step 14 Choose the source of network traffic from the IPv4 Network Objects list, and click **OK**.

Step 15 To specify the destination of network traffic for the CSC to scan, click the ellipses to display the Browse Destination dialog box.

Step 16 Choose the destination of network traffic from the IPv4 Network Objects list, and click **OK**.

Step 17 To specify the type of service for the CSC to scan, click the ellipses to display the Browse Service dialog box.

Step 18 Choose the service(s) from the list, and click **OK**.

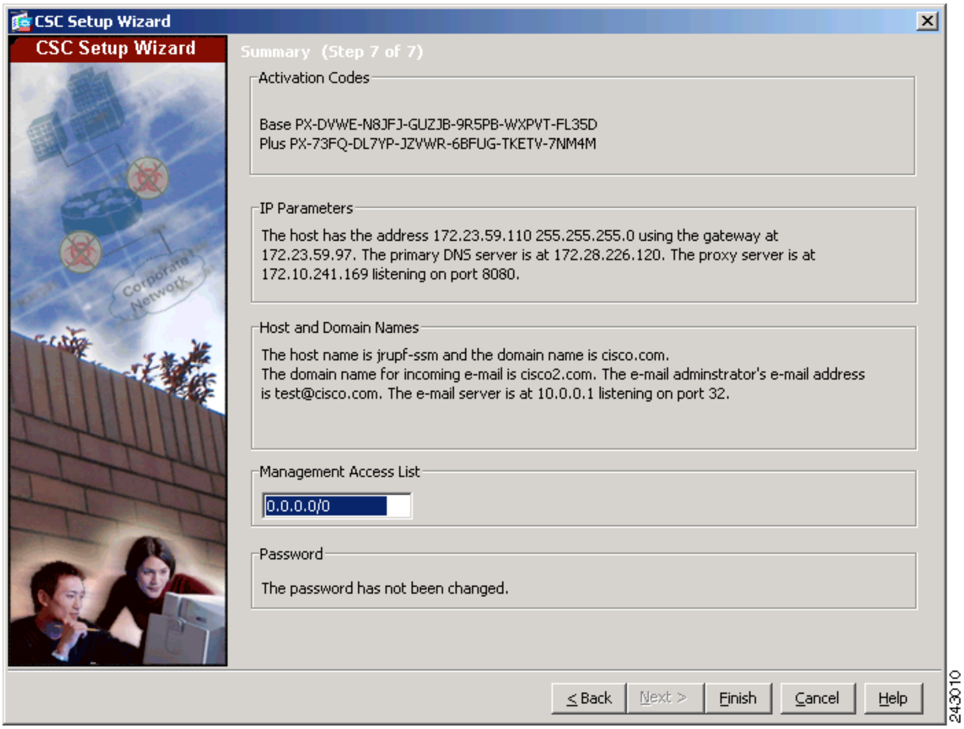
Step 19 Enter a description for the network traffic that you want the CSC to scan in the field provided.

Step 20 To specify whether or not to allow the CSC to scan network traffic if it fails, do the following:

- To allow traffic through without being scanned, click **Permit**.
- To prevent traffic from going through without being scanned, click **Deny**.
- To save your settings, click **OK**. The added traffic details appear on the Traffic Selection for CSC Scan screen.
- To discard these settings and return to the Traffic Selection for CSC Scan screen, click **Cancel**. If you click **Cancel**, ASDM displays a dialog box to confirm your decision.

Step 21 Click **Next**.

Step 22 In Step 7 of the CSC Setup Wizard, review the configuration settings that you have entered for the CSC SSM in the Summary screen.



Summary (Step 7 of 7)

Activation Codes

Base PX-DVWE-N8JFJ-GUZJB-9R5PB-WXPVT-FL35D
Plus PX-73FQ-DL7YP-JZVWR-6BFUG-TKETV-7NM4M

IP Parameters

The host has the address 172.23.59.110 255.255.255.0 using the gateway at 172.23.59.97. The primary DNS server is at 172.28.226.120. The proxy server is at 172.10.241.169 listening on port 8080.

Host and Domain Names

The host name is jrupf-ssm and the domain name is cisco.com.
The domain name for incoming e-mail is cisco2.com. The e-mail adminstrator's e-mail address is test@cisco.com. The e-mail server is at 10.0.0.1 listening on port 32.

Management Access List

0.0.0.0/0

Password

The password has not been changed.

Step 23 If you are satisfied with these settings, click **Finish**. To make changes, click **Back** until you reach the screen whose settings you want to modify.

An informational message appears, indicating that the CSC SSM is active.

By default, the CSC SSM is configured to perform content security scans that were enabled according to the license that you purchased (which may include anti-virus, anti-spam, anti-phishing, and content filtering). It is also configured to obtain periodic updates from the Trend Micro Update Server.

If you purchased the Plus license, you can create custom settings for URL blocking and URL filtering, as well as e-mail and FTP parameters. For more information, see the *Cisco Content Security and Control SSM Administrator Guide*.

What to Do Next

You are now ready to configure the Trend Micro Interscan for Cisco CSC SSM software. Use the following documents to continue configuring the adaptive security appliance for your implementation.

To Perform This Task...	See...
Configure CSC SSM software, such as advanced security policies	*Cisco Content Security and Control SSM Administrator Guide*
Configure additional CSC SSM features in ASDM, including content filtering	ASDM online help
Optimize performance for the AIP SSM and CSC SSM by creating more efficient service policies	*Cisco ASA 5500 Series Configuration Guide using the CLI*

After you have configured the CSC SSM software, you may want to perform some of the following additional steps.

To Perform This Task...	See...
Refine the existing configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following chapters provide configuration procedures for other common applications of the adaptive security appliance.

To Perform This Task...	See...
Configure protection of a DMZ web server	Chapter 8, “Scenario: DMZ Configuration”
Configure a remote-access VPN	Chapter 9, “Scenario: IPsec Remote-Access VPN Configuration”
Configure remote-access SSL connection for software clients	Chapter 10, “Scenario: Configuring Connections for a Cisco AnyConnect VPN Client”
Configure SSL connections for browser-based remote access	Chapter 11, “Scenario: SSL VPN Clientless Connections”
Configure a site-to-site VPN	Chapter 12, “Scenario: Site-to-Site VPN Configuration”

CHAPTER 15

Configuring the 4GE SSM for Fiber

The 4GE SSM (Security Services Module) has four Ethernet ports, and each port has two media type options: SFP (Small Form-Factor Pluggable) fiber or RJ 45. You can mix the copper and fiber ports using the same 4GE SSM card.

Note The 4GE SSM requires the Cisco ASA 5500 series software Version 7.1(1) or later.

This chapter includes the following sections:

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for any Ethernet interfaces you use.

Cabling 4GE SSM Interfaces

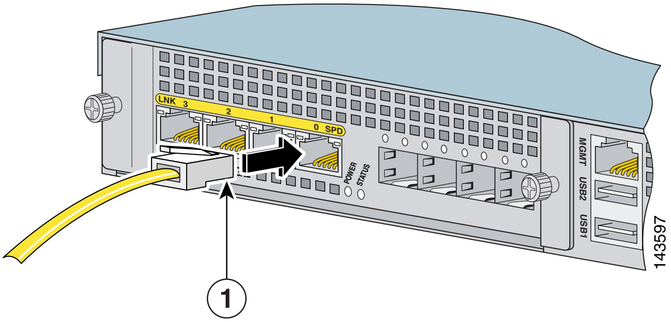
To cable 4GE SSM interfaces, perform the following steps for each port you want to connect to a network device:

Step 1 To connect an RJ-45 (Ethernet) interface to a network device, perform the following steps for each interface:

a. Locate a yellow Ethernet cable from the accessory kit.

b. Connect one end of the cable to an Ethernet port on the 4GE SSM as shown in Figure 15-1.

Figure 15-1 Connecting the Ethernet port



1	RJ-45 (Ethernet) port

c. Connect the other end of the cable to your network device.

Step 2 (Optional) If you want to use an SFP (fiber optic) port, install and cable the SFP modules as shown in Figure 15-2:

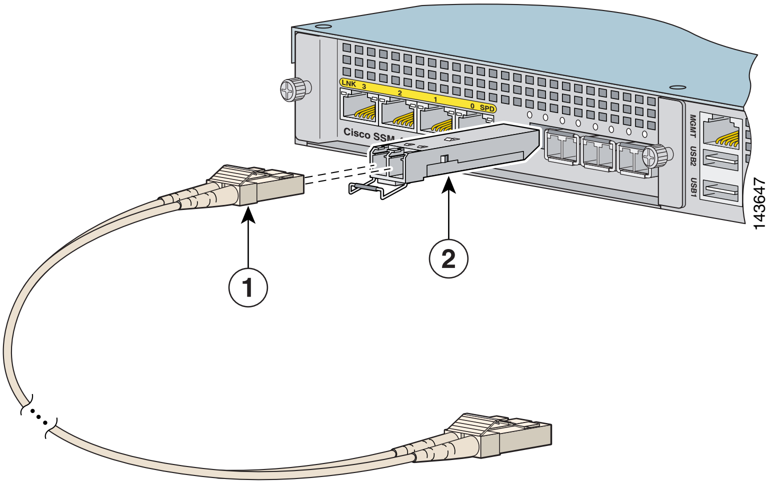
a. Insert and slide the SFP module into the SFP port until you hear a click. The click indicates that the SFP module is locked into the port.

b. Remove the optical port plugs from the installed SFP.

c. Locate the LC connector (fiber optic cable) in the 4GE SSM accessory kit.

d. Connect the LC connector to the SFP port.

Figure 15-2 Connecting the LC Connector



1	LC connector	**2**	SFP module

e. Connect the other end of the LC connector to your network device.

After you have attached any SFP ports to your network devices, you must also change the media type setting for each SFP interface. Continue with the following procedure, "Setting the 4GE SSM Media Type for Fiber Interfaces (Optional)."

Setting the 4GE SSM Media Type for Fiber Interfaces (Optional)

If you are using fiber interfaces, for each SFP interface you must change the media type setting from the default setting (Ethernet) to Fiber Connector.

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for Ethernet interfaces you use.

To set the media type for SFP interfaces using ASDM, perform the following steps starting from the main ASDM window:

Step 1 At the top of the ASDM window, click the **Configuration** tab.

Step 2 On the left side of the ASDM window, click the **Interfaces** tab.

Step 3 Click the **4GE SSM** interface and click **Edit**. The Edit Interface dialog box appears.

Step 4 Click **Configure Hardware Properties**. The Hardware Properties dialog box appears.

Step 5 From the Media Type drop-down list, choose **Fiber Connector**.

Step 6 Click **OK** to return to the Edit Interfaces dialog box, then click **OK** to return to the interfaces configuration dialog box.

Step 7 Repeat this procedure for each SFP interface.

You can also set the media type from the command line. For more information, see “Configuring Ethernet Settings and Subinterfaces” in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

What to Do Next

You have completed the initial configuration. You may want to consider performing some of the following additional steps.

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco ASA 5500 Series Configuration Guide using the CLI*
Learn about daily operations	*Cisco ASA 5500 Series Command Reference* *Cisco ASA 5500 Series System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

APPENDIX A

Obtaining a 3DES/AES License

The Cisco ASA 5500 series adaptive security appliance comes with a DES license that provides encryption. You can obtain a 3DES-AES license that provides encryption technology to enable specific features, such as secure remote management (SSH, ASDM, and so on), site-to-site VPN, and remote access VPN. You need an encryption license key to enable this license.

If you are a registered user of Cisco.com and would like to obtain a 3DES/AES encryption license, go to the following website:

http://www.cisco.com/go/license

If you are not a registered user of Cisco.com, go to the following website:

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

Provide your name, e-mail address, and the serial number for the adaptive security appliance as it appears in the **show version** command output.

Note You will receive the new activation key for your adaptive security appliance within two hours of requesting the license upgrade.

For more information on activation key examples or upgrading software, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

To use the activation key, perform the following steps:

	Command	Purpose
Step 1	`hostname#` **`show version`**	Shows the software release, hardware configuration, license key, and related uptime data.
Step 2	`hostname#` **`configure terminal`**	Enters global configuration mode.
Step 3	`hostname(config)#` **`activation-key`** *`activation-5-tuple-key`*	Updates the encryption activation key by replacing the *activation-4-tuple-key* variable with the activation key obtained with your new license. The *activation-5-tuple-key* variable is a five-element hexadecimal string with one space between each element. An example is 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e. The "0x" is optional; all values are assumed to be hexadecimal.
Step 4	`hostname(config)#` **`exit`**	Exits global configuration mode.
Step 5	`hostname#` **`copy running-config startup-config`**	Saves the configuration.
Step 6	`hostname#` **`reload`**	Reboots the adaptive security appliance and reloads the configuration.