CHAPTER 4

Getting Started

This chapter describes how to get started with your ASA. This chapter includes the following sections:

- Accessing the Console for Command-Line Interface, page 4-1
- Configuring ASDM Access, page 4-8
- Starting ASDM, page 4-17
- Factory Default Configurations, page 4-18
- Working with the Configuration, page 4-25
- Applying Configuration Changes to Connections, page 4-29
- Reloading the ASA, page 4-30

Accessing the Console for Command-Line Interface

- Accessing the Appliance Console, page 4-1
- Accessing the ASA Services Module Console, page 4-2
- Accessing the ASAv Console, page 4-6

Accessing the Appliance Console

For initial configuration, access the CLI directly from the console port. Later, you can configure remote access using Telnet or SSH according to Chapter 43, “Management Access.” If your system is already in multiple context mode, then accessing the console port places you in the system execution space. See Chapter 7, “Multiple Context Mode,” for more information about multiple context mode.

Detailed Steps

Step 1 Connect a PC to the console port using the provided console cable, and connect to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

See the hardware guide for your ASA for more information about the console cable.

Step 2 Press the **Enter** key to see the following prompt:

```
ciscoasa>
```

This prompt indicates that you are in user EXEC mode. Only basic commands are available from user EXEC mode.

Step 3 To access privileged EXEC mode, enter the following command:

```
ciscoasa> enable
```

The following prompt appears:

```
Password:
```

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

Step 4 Enter the enable password at the prompt.

By default, the password is blank, and you can press the **Enter** key to continue. See Configuring the Hostname, Domain Name, and Passwords, page 15-1 to change the enable password.

The prompt changes to:

```
ciscoasa#
```

To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

Step 5 To access global configuration mode, enter the following command:

```
ciscoasa# configure terminal
```

The prompt changes to the following:

```
ciscoasa(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Accessing the ASA Services Module Console

For initial configuration, access the command-line interface by connecting to the switch (either to the console port or remotely using Telnet or SSH) and then connecting to the ASASM. This section describes how to access the ASASM CLI.

- Information About Connection Methods, page 4-2
- Logging Into the ASA Services Module, page 4-3
- Logging Out of a Console Session, page 4-5
- Killing an Active Console Connection, page 4-5
- Logging Out of a Telnet Session, page 4-6

Information About Connection Methods

From the switch CLI, you can use two methods to connect to the ASASM:

- Virtual console connection—Using the **service-module session** command, you create a virtual console connection to the ASASM, with all the benefits and limitations of an actual console connection.

  Benefits include:

  - The connection is persistent across reloads and does not time out.
  - You can stay connected through ASASM reloads and view startup messages.
  - You can access ROMMON if the ASASM cannot load the image.
  - No initial password configuration is required.

  Limitations include:

  - The connection is slow (9600 baud).
  - You can only have one console connection active at a time.
  - You cannot use this command in conjunction with a terminal server where **Ctrl-Shift-6**, **x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6**, **x** is also the sequence to escape the ASASM console and return to the switch prompt. Therefore, if you try to exit the ASASM console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the switch, the ASASM console session is still active; you can never exit to the switch prompt. You must use a direct serial connection to return the console to the switch prompt. In this case, either change the terminal server or switch escape character in Cisco IOS software, or use the Telnet **session** command instead.

Note Because of the persistence of the console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection. See Logging Out of a Console Session, page 4-5 for more information.

- Telnet connection—Using the **session** command, you create a Telnet connection to the ASASM.

Note You cannot connect using this method for a new ASASM; this method requires you to configure a Telnet login password on the ASASM (there is no default password). After you set a password using the **passwd** command, you can use this method.

  Benefits include:

  - You can have multiple sessions to the ASASM at the same time.
  - The Telnet session is a fast connection.

  Limitations include:

  - The Telnet session is terminated when the ASASM reloads, and can time out.
  - You cannot access the ASASM until it completely loads; you cannot access ROMMON.
  - You must first set a Telnet login password; there is no default password.

Logging Into the ASA Services Module

For initial configuration, access the command-line interface by connecting to the switch (either to the switch console port or remotely using Telnet or SSH) and then connecting to the ASASM.

If your system is already in multiple context mode, then accessing the ASASM from the switch places you in the system execution space. See Chapter 7, "Multiple Context Mode," for more information about multiple context mode.

Later, you can configure remote access directly to the ASASM using Telnet or SSH according to Configuring ASA Access for ASDM, Telnet, or SSH, page 43-1.

Detailed Steps

	Command	Purpose
Step 1	From the switch, perform one of the following:	

	(Available for initial access.)
	service-module session [**switch** {**1** | **2**}] **slot** *number*
	Example:
	`Router# service-module session slot 3`
	`ciscoasa>`
		From the switch CLI, enter this command to gain console access to the ASASM.
		For a switch in a VSS, enter the **switch** argument.
		To view the module slot numbers, enter the **show module** command at the switch prompt.
		You access user EXEC mode.

	(Available after you configure a login password.)
	session [**switch** {**1** |**2**}] **slot** *number* **processor 1**
	You are prompted for the login password:
	`ciscoasa passwd:`
	Example:
	`Router# session slot 3 processor 1`
	`ciscoasa passwd: cisco`
	`ciscoasa>`
		From the switch CLI, enter this command to Telnet to the ASASM over the backplane.
		For a switch in a VSS, enter the **switch** argument.
		Note The **session** *slot* **processor 0** command, which is supported on other services modules, is not supported on the ASASM; the ASASM does not have a processor 0.
		To view the module slot numbers, enter the **show module** command at the switch prompt.
		Enter the login password to the ASASM. Set the password using the **passwd** command. There is no default password.
		You access user EXEC mode.

Step 2	**enable**
	Example:
	`ciscoasa> enable`
	`Password:`
	`ciscoasa#`
		Accesses privileged EXEC mode, which is the highest privilege level.
		Enter the enable password at the prompt. By default, the password is blank. To change the enable password, see Configuring the Hostname, Domain Name, and Passwords, page 15-1.
		To exit privileged EXEC mode, enter the **disable**, **exit**, or **quit** command.

Step 3	**configure terminal**
	Example:
	`ciscoasa# configure terminal`
	`ciscoasa(config)#`
		Accesses global configuration mode.
		To exit global configuration mode, enter the **disable**, **exit**, or **quit** command.

Logging Out of a Console Session

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

To kill another user's active connection, which may have been unintentionally left open, see Killing an Active Console Connection, page 4-5.

Detailed Steps

Step 1 To return to the switch CLI, type the following:

Ctrl-Shift-6, **x**

You return to the switch prompt:

```
asasm# [Ctrl-Shift-6, x]
Router#
```

Note Shift-6 on US and UK keyboards issues the caret (^) character. If you have a different keyboard and cannot issue the caret (^) character as a standalone character, you can temporarily or permanently change the escape character to a different character. Use the **terminal escape-character** *ascii_number* command (to change for this session) or the **default escape-character** *ascii_number* command (to change permanently). For example, to change the sequence for the current session to **Ctrl-w**, **x**, enter **terminal escape-character 23**.

Killing an Active Console Connection

Because of the persistence of a console connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection.

Detailed Steps

Step 1 From the switch CLI, show the connected users using the **show users** command. A console user is called "con". The Host address shown is 127.0.0.*slot*0, where *slot* is the slot number of the module.

```
Router# show users
```

For example, the following command output shows a user "con" on line 0 on a module in slot 2:

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20            00:00:02
```

Step 2 To clear the line with the console connection, enter the following command:

```
Router# clear line number
```

For example:

```
Router# clear line 0
```

Logging Out of a Telnet Session

To end the Telnet session and access the switch CLI, perform the following steps.

Detailed Steps

Step 1 To return to the switch CLI, type **exit** from the ASASM privileged or user EXEC mode. If you are in a configuration mode, enter **exit** repeatedly until you exit the Telnet session.

You return to the switch prompt:

```
asasm# exit
Router#
```

Note You can alternatively escape the Telnet session using the escape sequence **Ctrl-Shift-6**, **x**; this escape sequence lets you resume the Telnet session by pressing the **Enter** key at the switch prompt. To disconnect your Telnet session from the switch, enter **disconnect** at the switch CLI. If you do not disconnect the session, it will eventually time out according to the ASASM configuration.

Accessing the ASAv Console

By default, you can access the built-in VMware vSphere console. Alternatively, you can configure a network serial console, which has better capabilities, including copy and paste.

- Using the VMware vSphere Console, page 4-6
- Configuring a Network Serial Console Port, page 4-7

Using the VMware vSphere Console

For initial configuration or troubleshooting, access the CLI from the virtual console provided through the VMware vSphere Web Client. You can later configure CLI remote access for Telnet or SSH according to Chapter 43, "Management Access."

Prerequisites

For the vSphere Web Client, install the Client Integration Plug-In, which is required for ASAv console access.

Detailed Steps

Step 1 In the VMware vSphere Web Client, right-click the ASAv instance in the Inventory, and choose **Open Console**. Or you can click **Launch Console** on the Summary tab.

Step 2 Click in the console and press **Enter**. Note: Press **Ctrl + Alt** to release the cursor.

If the ASAv is still starting up, you see bootup messages.

When the ASAv starts up for the first time, it reads parameters provided through the OVA file and adds them to the ASAv system configuration. It then automatically restarts the boot process until it is up and running. This double boot process only occurs when you first deploy the ASAv.

If you have not yet installed a license, you see the following message repeated until you enter the activation key:

After you deploy the ASAv, you must install a CPU license. Until you install a license, throughput is limited to 1 Mbps so that you can perform preliminary connectivity tests. A CPU license is required for regular operation. You also see the following messages repeated on the console until you install a license:

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

Step 3 You see the following prompt:

```
ciscoasa>
```

This prompt indicates that you are in user EXEC mode. Only basic commands are available from user EXEC mode.

Step 4 To access privileged EXEC mode, enter the following command:

```
ciscoasa> enable
```

The following prompt appears:

```
Password:
```

Step 5 Press the **Enter** key to continue. By default, the password is blank. If you previously set an enable password, enter it instead of pressing Enter.

The prompt changes to:

```
ciscoasa#
```

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

Step 6 To access global configuration mode, enter the following command:

```
ciscoasa# configure terminal
```

The prompt changes to the following:

```
ciscoasa(config)#
```

You can begin to configure the ASAv from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Configuring a Network Serial Console Port

For a better console experience, you can configure a network serial port singly or attached to a virtual serial port concentrator (vSPC) for console access. See the VMware vSphere documentation for details about each method. On the ASAv, you must send the console output to a serial port instead of to the virtual console. This section describes how to enable the serial port console.

Detailed Steps

Step 1 Configure a network serial port in VMware vSphere. See the VMware vSphere documentation.

Step 2 On the ASAv, create a file called "use_ttyS0" in the root directory of disk0. This file does not need to have any contents; it just needs to exist at this location:

disk0:/use_ttyS0

- From ASDM, you can upload an empty text file by that name using the Tools > File Management dialog box.
- At the vSphere console, you can copy an existing file (any file) in the file system to the new name. For example:

```
ciscoasa(config)# cd coredumpinfo
ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
```

Step 3 Reload the ASAv.

- From ASDM, choose **Tools > System Reload**.
- At the vSphere console, enter **reload**.

The ASAv stops sending to the vSphere console, and instead sends to the serial console. See Using the VMware vSphere Console, page 4-6 for information about privileged EXEC and global configuration modes.

Step 4 Telnet to the vSphere host IP address and the port number you specified when you added the serial port; or Telnet to the vSPC IP address and port.

Configuring ASDM Access

- Configuring ASDM Access for Appliances and the ASAv, page 4-8
- Configuring ASDM Access for the ASA Services Module, page 4-13

Configuring ASDM Access for Appliances and the ASAv

ASDM access requires some minimal configuration so that you can communicate over the network with a management interface. This section includes the following topics:

- ASDM Access and the Factory Default Configuration, page 4-8
- Customizing ASDM Access (ASA 5505), page 4-9
- Customizing ASDM Access (ASA 5512-X and Higher, ASAv), page 4-11

ASDM Access and the Factory Default Configuration

With a factory default configuration (see Factory Default Configurations, page 4-18), ASDM connectivity is pre-configured with default network settings. Connect to ASDM using the following interface and network settings:

- The management interface depends on your model:

  - ASA 5505—The switch port to which you connect to ASDM can be any port, except for Ethernet 0/0.
  - ASA 5512-X and higher—The interface to which you connect to ASDM is Management 0/0.
  - ASAv—The interface to which you connect to ASDM is Management 0/0.
- The default management address is:
  - ASA 5505 and ASA 5512-X and higher—192.168.1.1.
  - ASAv—You set the management interface IP address during deployment.
- The clients allowed to access ASDM:
  - ASA 5505 and ASA 5512-X and higher—Clients must be on the 192.168.1.0/24 network. The default configuration enables DHCP so that your management station can be assigned an IP address in this range.
  - ASAv—You set the management client IP address during deployment. The ASAv does not act as the DHCP server for connected clients.

To launch ASDM, see Starting ASDM, page 4-17.

Note To change to multiple context mode, see Enabling or Disabling Multiple Context Mode, page 7-15. After changing to multiple context mode, you can access ASDM from the admin context using the network settings above.

Customizing ASDM Access (ASA 5505)

Use this procedure if *one or more* of the following conditions applies:

- You do not have a factory default configuration
- You want to change the management IP address
- You want to change to transparent firewall mode

See also the sample configurations in ASA 5505 Default Configuration, page 4-20.

Note For routed mode, for quick and easy ASDM access, we recommend applying the factory default configuration with the option to set your own management IP address (see Restoring the Factory Default Configuration, page 4-19). Use the procedure in this section only if you have special needs such as setting transparent mode, or if you have other configuration that you need to preserve.

Prerequisites

Access the CLI at the console port according to the Accessing the Appliance Console, page 4-1.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** `ciscoasa(config)# firewall transparent`	Enables transparent firewall mode. This command clears your configuration. See Setting the Firewall Mode, page 6-9 for more information.
Step 2	Do one of the following to configure a management interface, depending on your mode:	

	Routed mode:
	interface vlan *number*
	nameif *name*
	security-level *level*
	ip address *ip_address* [*mask*]
	Example:
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
		Configures an interface in routed mode. The security-level is a number between 1 and 100, where 100 is the most secure.

	Transparent mode:
	interface bvi *number*
	ip address *ip_address* [*mask*]
	interface vlan *number*
	bridge-group *number*
	nameif *name*
	security-level *level*
	Example:
	`ciscoasa(config)# interface bvi 1`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# bridge-group 1`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
		Configures a bridge virtual interface and assigns a management VLAN to the bridge group. The security-level is a number between 1 and 100, where 100 is the most secure.

Step 3	**interface ethernet 0/1**
	switchport access vlan *number*
	no shutdown
	Example:
	`ciscoasa(config)# interface ethernet 0/1`
	`ciscoasa(config-if)# switchport access vlan 1`
	`ciscoasa(config-if)# no shutdown`
		Enables the management switchport and assigns it to the management VLAN.

	Command	Purpose

Step 4	**dhcpd address** *ip_address***-***ip_address* *interface_name*
	dhcpd enable *interface_name*
	Example:
	`ciscoasa(config)# dhcpd address 192.168.1.5-192.168.1.254 inside`
	`ciscoasa(config)# dhcpd enable inside`
		Sets the DHCP pool for the management network. Make sure you do not include the VLAN interface address in the range.
		Note By default, the IPS module, if installed, uses 192.168.1.2 for its internal management address, so be sure not to use this address in the DHCP range. You can later change the IPS module management address using the ASA if required.

Step 5	**http server enable** **Example:** `ciscoasa(config)# http server enable`	Enables the HTTP server for ASDM.
Step 6	**http** *ip_address mask interface_name* **Example:** `ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside`	Allows the management host(s) to access ASDM.
Step 7	**write memory** **Example:** `ciscoasa(config)# write memory`	Saves the configuration.
Step 8	To launch ASDM, see Starting ASDM, page 4-17.	

Examples

The following configuration converts the firewall mode to transparent mode, configures the VLAN 1 interface and assigns it to BVI 1, enables a switchport, and enables ASDM for a management host:

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
interface ethernet 0/1
    switchport access vlan 1
    no shutdown
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

Customizing ASDM Access (ASA 5512-X and Higher, ASAv)

Use this procedure if *one or more* of the following conditions applies:

- You do not have a factory default configuration
- You want to change the management IP address
- You want to change to transparent firewall mode

- You want to change to multiple context mode

Note For routed, single mode, for quick and easy ASDM access, we recommend applying the factory default configuration with the option to set your own management IP address (see Restoring the Factory Default Configuration, page 4-19). Use the procedure in this section only if you have special needs such as setting transparent or multiple context mode, or if you have other configuration that you need to preserve.

Prerequisites

Access the CLI at the console port according to the Accessing the Appliance Console, page 4-1 or Accessing the ASAv Console, page 4-6.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** `ciscoasa(config)# firewall transparent`	Enables transparent firewall mode. This command clears your configuration. See Setting the Firewall Mode, page 6-9 for more information.

Step 2	**interface management 0/0**
	   nameif *name*
	   security-level *level*
	   no shutdown
	   ip address *ip_address mask*
	Example:
	`ciscoasa(config)# interface management 0/0`
	`ciscoasa(config-if)# nameif management`
	`ciscoasa(config-if)# security-level 100`
	`ciscoasa(config-if)# no shutdown`
	`ciscoasa(config-if)# ip address`
	`192.168.1.1 255.255.255.0`
		Configures the Management 0/0 interface. The security-level is a number between 1 and 100, where 100 is the most secure.

Step 3	**dhcpd address** *ip_address-ip_address interface_name*
	dhcpd enable *interface_name*
	Example:
	`ciscoasa(config)# dhcpd address`
	`192.168.1.2-192.168.1.254 management`
	`ciscoasa(config)# dhcpd enable management`
		Sets the DHCP pool for the management network. Make sure you do not include the Management 0/0 address in the range.

Step 4	(For remote management hosts)
	route *management_ifc management_host_ip mask gateway_ip* **1**
	Example:
	`ciscoasa(config)# route management`
	`10.1.1.0 255.255.255.0 192.168.1.50`
		Configures a route to the management hosts.

	Command	Purpose
Step 5	**http server enable** **Example:** `ciscoasa(config)# http server enable`	Enables the HTTP server for ASDM.
Step 6	**http** *ip_address mask interface_name* **Example:** `ciscoasa(config)# http 192.168.1.0 255.255.255.0 management`	Allows the management host(s) to access ASDM.
Step 7	**write memory** **Example:** `ciscoasa(config)# write memory`	Saves the configuration.
Step 8	(Optional, ASA 5512-X and higher only) **mode multiple** **Example:** `ciscoasa(config)# mode multiple`	Sets the mode to multiple mode. When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM. See Chapter 7, "Multiple Context Mode," for more information.
Step 9	To launch ASDM, see Starting ASDM, page 4-17.	

Examples

The following configuration converts the firewall mode to transparent mode, configures the Management 0/0 interface, and enables ASDM for a management host:

```
firewall transparent
interface management 0/0
    ip address 192.168.1.1 255.255.255.0
    nameif management
    security-level 100
    no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

Configuring ASDM Access for the ASA Services Module

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

Prerequisites

- Assign a VLAN interface to the ASASM according to the Assigning VLANs to the ASA Services Module, page 2-5.

- Connect to the ASASM and access global configuration mode according to the Accessing the ASA Services Module Console, page 4-2.

Detailed Steps

	Command	Purpose
Step 1	(Optional) **firewall transparent** **Example:** `ciscoasa(config)# firewall transparent`	Enables transparent firewall mode. This command clears your configuration. See Setting the Firewall Mode, page 6-9 for more information.
Step 2	Do one of the following to configure a management interface, depending on your mode:	

	Routed mode:
	interface vlan *number*
	   ip address *ip_address* [*mask*]
	   nameif *name*
	   security-level *level*
	Example:
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
		Configures an interface in routed mode. The **security-level** is a number between 1 and 100, where 100 is the most secure.

	Transparent mode:
	interface bvi *number*
	   ip address *ip_address* [*mask*]
	interface vlan *number*
	   bridge-group *bvi_number*
	   nameif *name*
	   security-level *level*
	Example:
	`ciscoasa(config)# interface bvi 1`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# bridge-group 1`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
		Configures a bridge virtual interface and assigns a management VLAN to the bridge group. The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 3	(For directly-connected management hosts)
	dhcpd address *ip_address-ip_address interface_name*
	dhcpd enable *interface_name*
	Example:
	`ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside`
	`ciscoasa(config)# dhcpd enable inside`
		Enables DHCP for the management host on the management interface network. Make sure you do not include the management address in the range.

	Routed mode:
	interface vlan *number*
	   ip address *ip_address* [*mask*]
	   nameif *name*
	   security-level *level*
	
	Example:
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
		Configures an interface in routed mode. The **security-level** is a number between 1 and 100, where 100 is the most secure.

	Transparent mode:
	interface bvi *number*
	   ip address *ip_address* [*mask*]
	
	interface vlan *number*
	   bridge-group *bvi_number*
	   nameif *name*
	   security-level *level*
	
	Example:
	`ciscoasa(config)# interface bvi 1`
	`ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0`
	
	`ciscoasa(config)# interface vlan 1`
	`ciscoasa(config-if)# bridge-group 1`
	`ciscoasa(config-if)# nameif inside`
	`ciscoasa(config-if)# security-level 100`
		Configures a bridge virtual interface and assigns a management VLAN to the bridge group. The **security-level** is a number between 1 and 100, where 100 is the most secure.

Step 3	(For directly-connected management hosts)
	dhcpd address *ip_address*-*ip_address interface_name*
	dhcpd enable *interface_name*
	
	Example:
	`ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside`
	`ciscoasa(config)# dhcpd enable inside`
		Enables DHCP for the management host on the management interface network. Make sure you do not include the management address in the range.

	Command	Purpose
Step 6	**http** *ip_address mask interface_name* **Example:** `ciscoasa(config)# http 192.168.1.0 255.255.255.0 management`	Allows the management host to access ASDM.
Step 7	**write memory** **Example:** `ciscoasa(config)# write memory`	Saves the configuration.
Step 8	(Optional) **mode multiple** **Example:** `ciscoasa(config)# mode multiple`	Sets the mode to multiple mode. When prompted, confirm that you want to convert the existing configuration to be the admin context. You are then prompted to reload the ASASM. See Chapter 7, "Multiple Context Mode," for more information.
Step 9	To launch ASDM, see Starting ASDM, page 4-17.	

Examples

The following routed mode configuration configures the VLAN 1 interface and enables ASDM for a management host:

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

The following configuration converts the firewall mode to transparent mode, configures the VLAN 1 interface and assigns it to BVI 1, and enables ASDM for a management host:

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

Starting ASDM

You can start ASDM using two methods:

- ASDM-IDM Launcher—The Launcher is an application downloaded from the ASA using a web browser that you can use to connect to any ASA IP address. You do not need to re-download the launcher if you want to connect to other ASAs. The Launcher also lets you run a virtual ASDM in Demo mode using files downloaded locally.
- Java Web Start—For each ASA that you manage, you need to connect with a web browser and then save or launch the Java Web Start application. You can optionally save the shortcut to your PC; however you need separate shortcuts for each ASA IP address.

Within ASDM, you can choose a different ASA IP address to manage; the difference between the Launcher and Java Web Start functionality rests primarily in how you initially connect to the ASA and launch ASDM.

ASDM allows multiple PCs or workstations to each have one browser session open with the same ASA software. A single ASA can support up to five concurrent ASDM sessions in single, routed mode. Only one session per browser per PC or workstation is supported for a specified ASA. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a maximum of 32 total connections for each ASA.

This section describes how to connect to ASDM initially, and then launch ASDM using the Launcher or the Java Web Start.

Detailed Steps

Step 1 On the PC you specified as the ASDM client, enter the following URL:

```
https://asa_ip_address/admin
```

The ASDM launch page appears with the following buttons:

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

Step 2 To download the Launcher:

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

b. Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. Note: If you enabled HTTPS authentication, enter your username and associated password.

c. Save the installer to your PC, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

d. Enter the management IP address, leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

Step 3 To use Java Web Start:

a. Click **Run ASDM** or **Run Startup Wizard**.

b. Save the shortcut to your PC when prompted. You can optionally open it instead of saving it.

c. Start Java Web Start from the shortcut.

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

e. Leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

Factory Default Configurations

The factory default configuration is the configuration applied by Cisco to new ASAs.

- ASA 5505—The factory default configuration configures interfaces and NAT so that the ASA is ready to use in your network immediately.
- ASA 5512-X and higher—The factory default configuration configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration.
- ASAv—As part of deployment, the deployment configuration configures an interface for management so that you can connect to it using ASDM, with which you can then complete your configuration. You can also configure failover IP addresses.
- ASASM—No default configuration. See Accessing the ASA Services Module Console, page 4-2 to start configuration.

The factory default configuration is available only for routed firewall mode and single context mode. See Chapter 7, "Multiple Context Mode," for more information about multiple context mode. See Chapter 6, "Transparent or Routed Firewall Mode," for more information about routed and transparent firewall mode. For the ASA 5505, a sample transparent mode configuration is provided in this section.

Note In addition to the image files and the (hidden) default configuration, the following folders and files are standard in flash memory: log/, crypto_archive/, and coredumpinfo/coredump.cfg. The date on these files may not match the date of the image files in flash memory. These files aid in potential troubleshooting; they do not indicate that a failure has occurred.

This section includes the following topics:

- Restoring the Factory Default Configuration, page 4-19
- Restoring the ASAv Deployment Configuration, page 4-20
- ASA 5505 Default Configuration, page 4-20
- ASA 5512-X and Higher Default Configuration, page 4-24
- ASAv Deployment Configuration, page 4-24

Restoring the Factory Default Configuration

This section describes how to restore the factory default configuration.

Note On the ASASM, restoring the factory default configuration simply erases the configuration; there is no factory default configuration.

Limitations

This feature is available only in routed firewall mode; transparent mode does not support IP addresses for interfaces. In addition, this feature is available only in single context mode; an ASA with a cleared configuration does not have any defined contexts to configure automatically using this feature.

Detailed Steps

	Command	Purpose

Step 1	**`configure factory-default`** `[`*`ip_address`*
	`[`*`mask`*`]]`
	Example:
	`ciscoasa(config)# configure`
	`factory-default 10.1.1.1 255.255.255.0`
		Restores the factory default configuration. For the ASAv, this command erases the deployment configuration and applies the same factory default configuration as for the ASA 5512-X and above.
		If you specify the *ip_address*, then you set the inside or management interface IP address, depending on your model, instead of using the default IP address of 192.168.1.1. The **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.
		Note This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA after restoring the factory configuration, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.

	ASAv Only:
	`write erase`
	Example:
	`ciscoasa(config)# configure`
	`factory-default 10.1.1.1 255.255.255.0`
		For the ASAv, the **write erase** command

Step 2	**`write memory`**
	Example:
	`active(config)# write memory`
		Saves the default configuration to flash memory. This command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.

What to Do Next

See Working with the Configuration, page 4-25 to start configuring the ASA.

Restoring the ASAv Deployment Configuration

This section describes how to restore the ASAv deployment configuration.

Detailed Steps

	Command	Purpose
Step 1	For failover: Power off the standby unit.	To prevent the standby unit from becoming active, you must power it off. If you leave it on, when you erase the active unit configuration, then the standby unit becomes active. When the former active unit reloads and reconnects over the failover link, the old configuration will sync from the new active unit, wiping out the deployment configuration you wanted.

Step 2	On the Active unit:
	`write erase`
	Example:
	`ciscoasa(config)# write erase`
		For the ASAv, the **write erase** command restores the deployment configuration after you reload.
		Note The ASAv boots the current running image, so you are not reverted to the original boot image.
		Do not save the configuration.

Step 3	**`reload`**
	Example:
	`active(config)# reload`
		Reloads the ASAv and loads the deployment configuration.

Step 4	For failover: Power on the standby unit.	After the active unit reloads, power on the standby unit. The deployment configuration will sync to the standby unit.

ASA 5505 Default Configuration

The default configuration is available for routed mode only. This section describes the default configuration and also provides a sample transparent mode configuration that you can copy and paste as a starting point. This section includes the following topics:

- ASA 5505 Routed Mode Default Configuration, page 4-20
- ASA 5505 Transparent Mode Sample Configuration, page 4-22

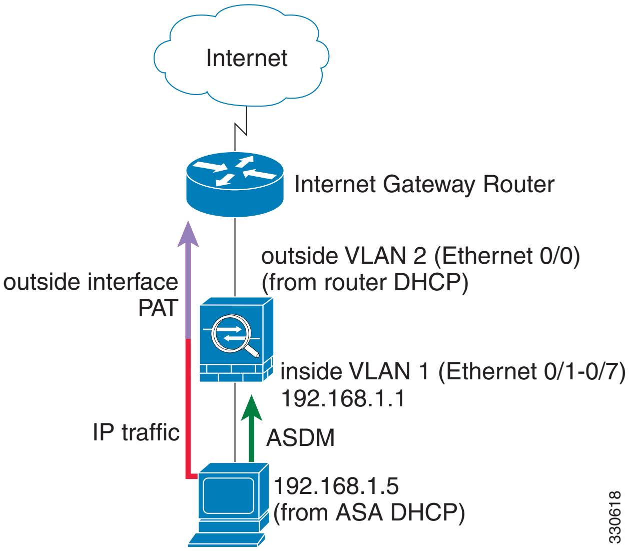
ASA 5505 Routed Mode Default Configuration

The default factory configuration for the ASA 5505 configures the following:

- Interfaces—Inside (VLAN 1) and outside (VLAN 2).

- Switchports enabled and assigned—Ethernet 0/1 through 0/7 switch ports assigned to inside. Ethernet 0/0 assigned to outside.
- IP addresses— Outside address from DHCP; inside address set manually to 192.168.1.1/24.
- Network address translation (NAT)—All inside IP addresses are translated when accessing the outside using interface PAT.
- Traffic flow—IPv4 and IPv6 traffic allowed from inside to outside (this behavior is implicit on the ASA). Outside users are prevented from accessing the inside.
- DHCP server—Enabled for inside hosts so that a PC connecting to the inside interface receives an address between 192.168.1.5 and 192.168.1.254. DNS, WINS, and domain information obtained from the DHCP client on the outside interface is passed to the DHCP clients on the inside interface.
- Default route—Derived from DHCP.
- ASDM access—Inside hosts allowed.

Figure 4-1 ASA 5505 Routed Mode



The configuration consists of the following commands:

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
```

```
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
object network obj_any
   subnet 0 0
   nat (inside,outside) dynamic interface
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

Note For testing purposes, you can allow ping from inside to outside by enabling ICMP inspection. Add the following commands to the default configuration:

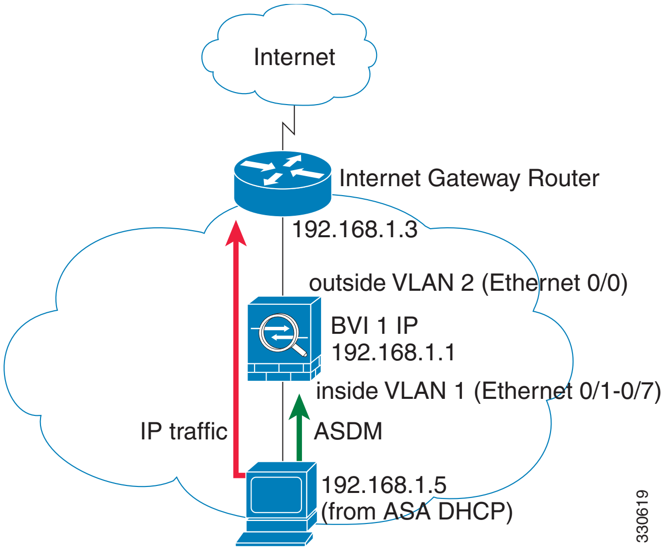
```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5505 Transparent Mode Sample Configuration

When you change the mode to transparent mode, the configuration is erased. You can copy and paste the following sample configuration at the CLI to get started. This configuration uses the default configuration as a starting point. Note the following areas you may need to modify:

- IP addresses—The IP addresses configured should be changed to match the network to which you are connecting.
- Static routes—For some kinds of traffic, static routes are required. See MAC Address vs. Route Lookups, page 6-5.

Figure 4-2 ASA 5505 Transparent Mode



```
firewall transparent
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface bvi 1
   ip address 192.168.1.1 255.255.255.0
interface vlan2
   nameif outside
   security-level 0
   bridge-group 1
   no shutdown
interface vlan1
   nameif inside
   security-level 100
   bridge-group 1
   no shutdown
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
```

Note For testing purposes, you can allow ping from inside to outside by enabling ICMP inspection. Add the following commands to the sample configuration:

```
policy-map global_policy
   class inspection_default
      inspect icmp
```

ASA 5512-X and Higher Default Configuration

The default factory configuration for the ASA 5512-X and higher configures the following:

- Management interface—Management 0/0 (management).
- IP address—The management address is 192.168.1.1/24.
- DHCP server—Enabled for management hosts so that a PC connecting to the management interface receives an address between 192.168.1.2 and 192.168.1.254.
- ASDM access—Management hosts allowed.

The configuration consists of the following commands:

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASAv Deployment Configuration

When you deploy the ASAv, you can pre-set many parameters that let you connect to the Management 0/0 interface using ASDM. A typical configuration includes the following settings:

- Management 0/0 interface:
  - Named “management”
  - IP address or DHCP
  - Security level 0
  - Management-only
- Static route from the management interface to the management host IP address through the default gateway
- ASDM server enabled
- ASDM access for the management host IP address

- (Optional) Failover link IP addresses for GigabitEthernet 0/8, and the Management 0/0 standby IP address.

See the following configuration for a standalone unit:

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
```

See the following configuration for a primary unit in a failover pair:

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address standby standby_ip
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

Working with the Configuration

This section describes how to work with the configuration. The ASA loads the configuration from a text file, called the startup configuration. This file resides by default as a hidden file in internal flash memory. You can, however, specify a different path for the startup configuration. (For more information, see Chapter 44, “Software and Configurations.”)

When you enter a command, the change is made only to the running configuration in memory. You must manually save the running configuration to the startup configuration for your changes to remain after a reboot.

The information in this section applies to both single and multiple security contexts, except where noted. Additional information about contexts is in Chapter 7, “Multiple Context Mode.”

This section includes the following topics:

- Saving Configuration Changes, page 4-26
- Copying the Startup Configuration to the Running Configuration, page 4-27
- Viewing the Configuration, page 4-28
- Clearing and Removing Configuration Settings, page 4-28
- Creating Text Configuration Files Offline, page 4-29

Saving Configuration Changes

This section describes how to save your configuration and includes the following topics:

- Saving Configuration Changes in Single Context Mode, page 4-26
- Saving Configuration Changes in Multiple Context Mode, page 4-26

Saving Configuration Changes in Single Context Mode

To save the running configuration to the startup configuration, enter the following command:

Command	Purpose
write memory **Example:** `ciscoasa# write memory`	Saves the running configuration to the startup configuration. **Note** The **copy running-config startup-config** command is equivalent to the **write memory** command.

Saving Configuration Changes in Multiple Context Mode

You can save each context (and system) configuration separately, or you can save all context configurations at the same time. This section includes the following topics:

- Saving Each Context and System Separately, page 4-26
- Saving All Context Configurations at the Same Time, page 4-27

Saving Each Context and System Separately

To save the system or context configuration, enter the following command within the system or context:

Command	Purpose
write memory **Example:** `ciscoasa# write memory`	Saves the running configuration to the startup configuration. For multiple context mode, context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server. **Note** The **copy running-config startup-config** command is equivalent to the **write memory** command.

Saving All Context Configurations at the Same Time

To save all context configurations at the same time, as well as the system configuration, enter the following command in the system execution space:

Command	Purpose
write memory all [**/noconfirm**] **Example:** `ciscoasa# write memory all /noconfirm`	Saves the running configuration to the startup configuration for all contexts and the system configuration. If you do not enter the **/noconfirm** keyword, you see the following prompt: `Are you sure [Y/N]:` After you enter **Y**, the ASA saves the system configuration and each context. Context startup configurations can reside on external servers. In this case, the ASA saves the configuration back to the server you identified in the context URL, except for an HTTP or HTTPS URL, which do not let you save the configuration to the server.

After the ASA saves each context, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- For contexts that are not saved because the context is locked, the following message appears:

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context 'a' , context 'x' , context 'z' .
  ```

  A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- For contexts that are not saved because of bad sectors in the flash memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

Copying the Startup Configuration to the Running Configuration

Copy a new startup configuration to the running configuration using one of the following options.

Command	Purpose
copy startup-config running-config	Merges the startup configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.
reload	Reloads the ASA, which loads the startup configuration and discards the running configuration.
clear configure all **copy startup-config running-config**	Loads the startup configuration and discards the running configuration without requiring a reload.

Viewing the Configuration

The following commands let you view the running and startup configurations.

Command	Purpose
show running-config	Views the running configuration.
show running-config *command*	Views the running configuration of a specific command.
show startup-config	Views the startup configuration.

Clearing and Removing Configuration Settings

To erase settings, enter one of the following commands.

Command	Purpose
clear configure *configurationcommand* [*level2configurationcommand*]	Clears all the configuration for a specified command. If you only want to clear the configuration for a specific version of the command, you can enter a value for *level2configurationcommand*.
Example: ciscoasa(config)# clear configure aaa	For example, to clear the configuration for all **aaa** commands, enter the following command: ciscoasa(config)# **clear configure aaa** To clear the configuration for only **aaa authentication** commands, enter the following command: ciscoasa(config)# **clear configure aaa authentication**
no *configurationcommand* [*level2configurationcommand*] *qualifier*	Disables the specific parameters or options of a command. In this case, you use the **no** command to remove the specific configuration identified by *qualifier*.
Example: ciscoasa(config)# no nat (inside) 1	For example, to remove a specific **nat** command, enter enough of the command to identify it uniquely as follows: ciscoasa(config)# **no nat (inside) 1**

Command	Purpose
write erase **Example:** `ciscoasa(config)# write erase`	Erases the startup configuration. **Note** For the ASAv, this command restores the deployment configuration after a reload. To erase the configuration completely, use the **clear configure all** command.
clear configure all **Example:** `ciscoasa(config)# clear configure all`	Erases the running configuration. **Note** In multiple context mode, if you enter **clear configure all** from the system configuration, you also remove all contexts and stop them from running. The context configuration files are not erased, and remain in their original location. This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.

Creating Text Configuration Files Offline

This guide describes how to use the CLI to configure the ASA; when you save commands, the changes are written to a text file. Instead of using the CLI, however, you can edit a text file directly on your PC and paste a configuration at the configuration mode command-line prompt in its entirety, or line by line. Alternatively, you can download a text file to the ASA internal flash memory. See Chapter 44, "Software and Configurations," for information on downloading the configuration file to the ASA.

In most cases, commands described in this guide are preceded by a CLI prompt. The prompt in the following example is "ciscoasa(config)#":

```
ciscoasa(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted as follows:

```
context a
```

For additional information about formatting the file, see Appendix 51, "Using the Command-Line Interface."

Applying Configuration Changes to Connections

When you make security policy changes to the configuration, all *new* connections use the new security policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. **show** command output for old connections reflect the old configuration, and in some cases will not include data about the old connections.

For example, if you remove a QoS **service-policy** from an interface, then re-add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output.

To ensure that all connections use the new policy, you need to disconnect the current connections so that they can reconnect using the new policy.

To disconnect connections, enter one of the following commands.

Detailed Steps

Command	Purpose
clear local-host [*ip_address*] [**all**] **Example:** `ciscoasa(config)# clear local-host all`	This command reinitializes per-client run-time states such as connection limits and embryonic limits. As a result, this command removes any connection that uses those limits. See the **show local-host all** command to view all current connections per host. With no arguments, this command clears all affected through-the-box connections. To also clear to-the-box connections (including your current management session), use the **all** keyword. To clear connections to and from a particular IP address, use the *ip_address* argument.
clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]] **Example:** `ciscoasa(config)# clear conn all`	This command terminates connections in any state. See the **show conn** command to view all current connections. With no arguments, this command clears all through-the-box connections. To also clear to-the-box connections (including your current management session), use the **all** keyword. To clear specific connections based on the source IP address, destination IP address, port, and/or protocol, you can specify the desired options.

Reloading the ASA

To reload the ASA, enter the following command:

Command	Purpose
reload **Example:** `ciscoasa (config)# reload`	Reloads the ASA. **Note** In multiple context mode, you can only reload from the system execution space.