



CHAPTER 3

Getting Started

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

- [Accessing the Appliance Command-Line Interface, page 3-1](#)
- [Configuring ASDM Access for Appliances, page 3-2](#)
- [Starting ASDM, page 3-6](#)
- [Factory Default Configurations, page 3-10](#)
- [Working with the Configuration, page 3-16](#)
- [Applying Configuration Changes to Connections, page 3-20](#)

Accessing the Appliance Command-Line Interface

For initial configuration, access the CLI directly from the console port. Later, you can configure remote access using Telnet or SSH according to [Chapter 37, “Configuring 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 6, “Configuring 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:

hostname>

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:

hostname> **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 the “[Configuring the Hostname, Domain Name, and Passwords](#)” section on page 10-1 to change the enable password.

The prompt changes to the following:

```
hostname#
```

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

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

```
hostname# configure terminal
```

The prompt changes to the following:

```
hostname(config)#
```

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

Configuring ASDM Access for Appliances

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

- [Accessing ASDM Using the Factory Default Configuration, page 3-2](#)
- [Accessing ASDM Using a Non-Default Configuration \(ASA 5505\), page 3-3](#)
- [Accessing ASDM Using a Non-Default Configuration \(ASA 5510 and Higher\), page 3-5](#)

Accessing ASDM Using the Factory Default Configuration

With a factory default configuration (see the “[Factory Default Configurations](#)” section on page 3-10), ASDM connectivity is preconfigured 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 5510 and higher—The interface to which you connect to ASDM is Management 0/0.
- The default management address is 192.168.1.1.
- The clients allowed to access ASDM must be on the 192.168.1.0/24 network. The default configuration enables DHCP so your management station can be assigned an IP address in this range. To allow other client IP addresses to access ASDM, see the “[Configuring ASA Access for ASDM, Telnet, or SSH](#)” section on page 37-1.

To launch ASDM, see the “[Starting ASDM](#)” section on page 3-6.



Note To change to multiple context mode, see the “[Enabling or Disabling Multiple Context Mode](#)” section on [page 6-15](#). After changing to multiple context mode, you can access ASDM from the admin context using the network settings above.

Accessing ASDM Using a Non-Default Configuration (ASA 5505)

If you do not have a factory default configuration, or want to change to transparent firewall mode, perform the following steps. See also the sample configurations in the “[ASA 5505 Default Configuration](#)” section on [page 3-12](#).

Prerequisites

Access the CLI according to the “[Accessing the Appliance Command-Line Interface](#)” section on [page 3-1](#).

Detailed Steps

	Command	Purpose
Step 1	(Optional) <code>firewall transparent</code>	Enables transparent firewall mode. This command clears your configuration. See the “ Setting the Firewall Mode ” section on page 5-9 for more information.
Step 2	Example: <code>hostname(config)# firewall transparent</code>	

Step 2	Do one of the following to configure a management interface, depending on your mode: Routed mode: <code>interface vlan number</code> <code> ip address ip_address [mask]</code> <code> nameif name</code> <code> security-level level</code>	Configures an interface in routed mode. The security-level is a number between 1 and 100, where 100 is the most secure.
	Example: <code>hostname(config)# interface vlan 1</code> <code>hostname(config-if)# ip address</code> <code>192.168.1.1 255.255.255.0</code> <code>hostname(config-if)# nameif inside</code> <code>hostname(config-if)# security-level 100</code>	

■ Configuring ASDM Access for Appliances

Command	Purpose
<p>Transparent mode:</p> <pre>interface bvi number ip address ip_address [mask]</pre> <pre>interface vlan number bridge-group bvi_number nameif name security-level level</pre> <p>Example:</p> <pre>hostname(config)# interface bvi 1 hostname(config-if)# ip address 192.168.1.1 255.255.255.0 hostname(config)# interface vlan 1 hostname(config-if)# bridge-group 1 hostname(config-if)# nameif inside hostname(config-if)# security-level 100</pre>	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.
<p>Step 3</p> <pre>interface ethernet 0/n switchport access vlan number no shutdown</pre> <p>Example:</p> <pre>hostname(config)# interface ethernet 0/1 hostname(config-if)# switchport access vlan 1 hostname(config-if)# no shutdown</pre>	Enables the management switchport and assigns it to the management VLAN.
<p>Step 4</p> <pre>dhcpd address ip_address-ip_address interface_name dhcpd enable interface_name</pre> <p>Example:</p> <pre>hostname(config)# dhcpd address 192.168.1.5-192.168.1.254 inside hostname(config)# dhcpd enable inside</pre>	<p>Enables DHCP for the management host on the management interface network. Make sure you do not include the management address in the range.</p> <p>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.</p>
<p>Step 5</p> <pre>http server enable</pre> <p>Example:</p> <pre>hostname(config)# http server enable</pre>	Enables the HTTP server for ASDM.
<p>Step 6</p> <pre>http ip_address mask interface_name</pre> <p>Example:</p> <pre>hostname(config)# http 192.168.1.0 255.255.255.0 inside</pre>	Allows the management host to access ASDM.
<p>Step 7</p> <pre>write memory</pre> <p>Example:</p> <pre>hostname(config)# write memory</pre>	Saves the configuration.
<p>Step 8</p> <p>To launch ASDM, see the “Starting ASDM” section on page 3-6.</p>	Launches ASDM.

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
```

Accessing ASDM Using a Non-Default Configuration (ASA 5510 and Higher)

If you do not have a factory default configuration, or want to change the firewall or context mode, perform the following steps.

Prerequisites

Access the CLI according to the “[Accessing the Appliance Command-Line Interface](#)” section on page 3-1.

Detailed Steps

	Command	Purpose
Step 1	(Optional) <code>firewall transparent</code>	Enables transparent firewall mode. This command clears your configuration. See the “ Setting the Firewall Mode ” section on page 5-9 for more information.
Step 2	Example: hostname(config)# firewall transparent <code>interface management 0/0 ip address ip_address mask nameif name security-level number no shutdown</code>	Configures the Management 0/0 interface. The security-level is a number between 1 and 100, where 100 is the most secure.

Starting ASDM

	Command	Purpose
Step 3	<code>dhcpd address ip_address-ip_address interface_name dhcpd enable interface_name</code>	Enables DHCP for the management host on the management interface network. Make sure you do not include the Management 0/0 address in the range.
	Example: <code>hostname(config)# dhcpd address 192.168.1.2-192.168.1.254 management hostname(config)# dhcpd enable management</code>	
Step 4	<code>http server enable</code>	Enables the HTTP server for ASDM.
	Example: <code>hostname(config)# http server enable</code>	
Step 5	<code>http ip_address mask interface_name</code>	Allows the management host to access ASDM.
	Example: <code>hostname(config)# http 192.168.1.0 255.255.255.0 management</code>	
Step 6	<code>write memory</code>	Saves the configuration.
	Example: <code>hostname(config)# write memory</code>	
Step 7	(Optional) <code>mode multiple</code>	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 6, “Configuring Multiple Context Mode,” for more information.
	Example: <code>hostname(config)# mode multiple</code>	
Step 8	To launch ASDM, see the “Starting ASDM” section on page 3-6.	Launches ASDM.

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
```

Starting ASDM

You can start ASDM using two methods:

- ASDM-IDM Launcher (Windows only)—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 application to your PC; however you need separate applications for each ASA IP address.

**Note**

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

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

- [Connecting to ASDM for the First Time, page 3-7](#)
- [Starting ASDM from the ASDM-IDM Launcher, page 3-8](#)
- [Starting ASDM from the Java Web Start Application, page 3-8](#)
- [Using ASDM in Demo Mode, page 3-9](#)

**Note**

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.

Connecting to ASDM for the First Time

To connect to ASDM for the first time to download the ASDM-IDM Launcher or Java Web Start application, perform the following steps:

-
- Step 1** From a supported web browser on the ASA network, enter the following URL:

`https://interface_ip_address/admin`

Where *interface_ip_address* is the management IP address of the ASA. See the [“Configuring ASDM Access for Appliances” section on page 3-2](#) for more information about management access.

See the ASDM release notes for your release for the requirements to run ASDM.

The ASDM launch page appears with the following buttons:

- **Install ASDM Launcher and Run ASDM** (Windows only)
- **Run ASDM**
- **Run Startup Wizard**

- Step 2** To download the Launcher:

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

Starting ASDM

- b. Enter the username and password, and click **OK**. For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, 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. See the “[Starting ASDM from the ASDM-IDM Launcher](#)” section on page 3-8 to use the Launcher to connect to ASDM.

Step 3 To use the Java Web Start application:

- a. Click **Run ASDM or Run Startup Wizard**.
 - b. Save the application to your PC when prompted. You can optionally open it instead of saving it.
 - c. See the “[Starting ASDM from the Java Web Start Application](#)” section on page 3-8 to use the Java Web Start application to connect to ASDM.
-

Starting ASDM from the ASDM-IDM Launcher

To start ASDM from the ASDM-IDM Launcher, perform the following steps.

Prerequisites

Download the ASDM-IDM Launcher according to the “[Connecting to ASDM for the First Time](#)” section on page 3-7.

Detailed Steps

Step 1 Start the ASDM-IDM Launcher application.

Step 2 Enter or choose the ASA IP address or hostname to which you want to connect. To clear the list of IP addresses, click the trash can icon next to the Device/IP Address/Name field.

Step 3 Enter your username and your password, and then click **OK**.

For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, enter your username and associated password.

If there is a new version of ASDM on the ASA, the ASDM Launcher automatically downloads the new version and requests that you update the current version before starting ASDM.

The main ASDM window appears.

Starting ASDM from the Java Web Start Application

To start ASDM from the Java Web Start application, perform the following steps.

Prerequisites

Download the Java Web Start application according to the “[Connecting to ASDM for the First Time](#)” section on page 3-7.

Detailed Steps

-
- Step 1** Start the Java Web Start application.
- Step 2** Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.
- Step 3** Enter the username and password, and click **OK**. For a factory default configuration, leave these fields empty. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. With HTTPS authentication enabled, enter your username and associated password.
- The main ASDM window appears.
-

Using ASDM in Demo Mode

The ASDM Demo Mode, a separately installed application, lets you run ASDM without having a live device available. In this mode, you can do the following:

- Perform configuration and selected monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or ASA features using the ASDM interface.
- Perform configuration and monitoring tasks with the CSC SSM.
- Obtain simulated monitoring and logging data, including real-time syslog messages. The data shown is randomly generated; however, the experience is identical to what you would see when you are connected to a real device.

This mode has been updated to support the following features:

- For global policies, an ASA in single, routed mode and intrusion prevention
- For object NAT, an ASA in single, routed mode and a firewall DMZ.
- For the Botnet Traffic Filter, an ASA in single, routed mode and security contexts.
- Site-to-Site VPN with IPv6 (Clientless SSL VPN and IPsec VPN)
- Promiscuous IDS (intrusion prevention)
- Unified Communication Wizard

This mode does not support the following:

- Saving changes made to the configuration that appear in the GUI.
- File or disk operations.
- Historical monitoring data.
- Non-administrative users.
- These features:
 - File menu:

■ Factory Default Configurations

- Save Running Configuration to Flash
- Save Running Configuration to TFTP Server
- Save Running Configuration to Standby Unit
- Save Internal Log Buffer to Flash
- Clear Internal Log Buffer
- Tools menu:
 - Command Line Interface
 - Ping
 - File Management
 - Update Software
 - File Transfer
 - Upload Image from Local PC
 - System Reload
 - Toolbar/Status bar > Save
 - Configuration > Interface > Edit Interface > Renew DHCP Lease
 - Configuring a standby device after failover
- Operations that cause a rereading of the configuration, in which the GUI reverts to the original configuration:
 - Switching contexts
 - Making changes in the Interface pane
 - NAT pane changes
 - Clock pane changes

To run ASDM in Demo Mode, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Download the ASDM Demo Mode installer, <i>asdm-demo-version.msi</i> , from the following location:
http://www.cisco.com/cisco/web/download/index.html . |
| Step 2 | Double-click the installer to install the software. |
| Step 3 | Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the Start menu. |
| Step 4 | Check the Run in Demo Mode check box.
The Demo Mode window appears. |
-

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 5510 and higher—The factory default configuration configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration.

The factory default configuration is available only for routed firewall mode and single context mode. See [Chapter 6, “Configuring Multiple Context Mode,”](#) for more information about multiple context mode. See [Chapter 5, “Configuring the Transparent or Routed Firewall,”](#) 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 3-11](#)
- [ASA 5505 Default Configuration, page 3-12](#)
- [ASA 5510 and Higher Default Configuration, page 3-16](#)

Restoring the Factory Default Configuration

This section describes how to restore the 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.

■ Factory Default Configurations

Detailed Steps

Using the CLI:

	Command	Purpose
Step 1	<code>configure factory-default [ip_address [mask]]</code>	<p>Restores the factory default configuration.</p> <p>If you specify the <i>ip_address</i>, 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.</p> <p>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.</p>
Step 2	<code>write memory</code>	<p>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.</p>

What to Do Next

See the “Working with the Configuration” section on page 3-16 to start configuring the ASA.

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 3-12](#)
- [ASA 5505 Transparent Mode Sample Configuration, page 3-14](#)

ASA 5505 Routed Mode Default Configuration

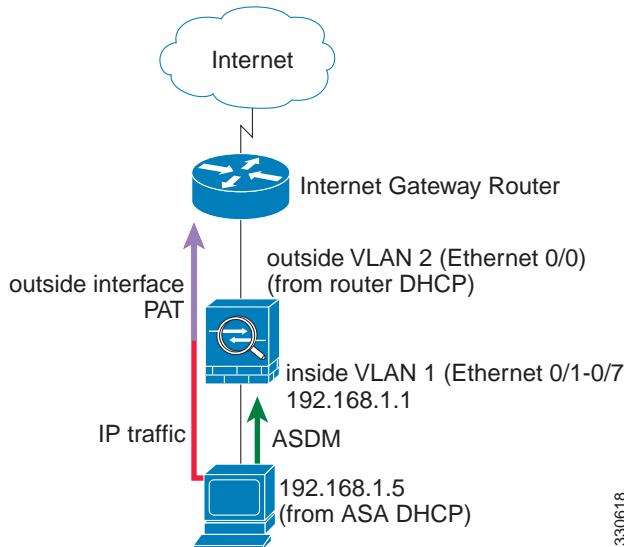
The default factory configuration for the ASA 5505 configures the following:

- 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 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 3-1](#) shows the traffic flow for an ASA 5505 in routed mode.

Figure 3-1 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
```

■ Factory Default Configurations

```

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

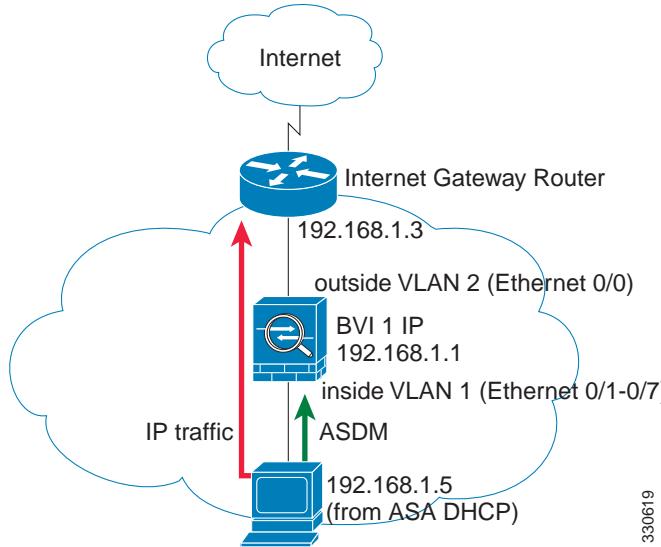
```

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 the “[MAC Address vs. Route Lookups](#)” section on page 5-6.
- [Figure 3-2](#) shows the traffic flow for an ASA 5505 in transparent mode.

Figure 3-2 ASA 5505 Transparent Mode



330619

```

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

```

Working with the Configuration

```
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 5510 and Higher Default Configuration

The default factory configuration for the ASA 5510 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 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
```

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 81, “Managing 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 6, “Configuring Multiple Context Mode.”](#)

This section includes the following topics:

- [Saving Configuration Changes, page 3-17](#)
- [Copying the Startup Configuration to the Running Configuration, page 3-18](#)

- [Viewing the Configuration, page 3-19](#)
- [Clearing and Removing Configuration Settings, page 3-19](#)
- [Creating Text Configuration Files Offline, page 3-20](#)

Saving Configuration Changes

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

- [Saving Configuration Changes in Single Context Mode, page 3-17](#)
- [Saving Configuration Changes in Multiple Context Mode, page 3-17](#)

Saving Configuration Changes in Single Context Mode

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

Command	Purpose
<code>write memory</code>	Saves the running configuration to the startup configuration. Note The copy running-config startup-config command is equivalent to the write memory command.
Example: hostname# write memory	

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 3-17](#)
- [Saving All Context Configurations at the Same Time, page 3-18](#)

Saving Each Context and System Separately

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

Command	Purpose
<code>write memory</code>	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.
Example: hostname# write memory	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
<code>write memory all [/noconfirm]</code> Example: hostname# 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
<code>copy startup-config running-config</code>	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.
<code>reload</code>	Reloads the ASA, which loads the startup configuration and discards the running configuration.
<code>clear configure all</code> <code>copy startup-config running-config</code>	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
<code>show running-config</code>	Views the running configuration.
<code>show running-config command</code>	Views the running configuration of a specific command.
<code>show startup-config</code>	Views the startup configuration.

Clearing and Removing Configuration Settings

To erase settings, enter one of the following commands.

Command	Purpose
<code>clear configure configurationcommand [level2configurationcommand]</code>	<p>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 <i>level2configurationcommand</i>.</p> <p>Example: <code>hostname(config)# clear configure aaa</code></p> <p>For example, to clear the configuration for all aaa commands, enter the following command:</p> <pre>hostname(config)# clear configure aaa</pre> <p>To clear the configuration for only aaa authentication commands, enter the following command:</p> <pre>hostname(config)# clear configure aaa authentication</pre>
<code>no configurationcommand [level2configurationcommand] qualifier</code>	<p>Disables the specific parameters or options of a command. In this case, you use the no command to remove the specific configuration identified by <i>qualifier</i>.</p> <p>Example: <code>hostname(config)# no nat (inside) 1</code></p> <p>For example, to remove a specific nat command, enter enough of the command to identify it uniquely as follows:</p> <pre>hostname(config)# no nat (inside) 1</pre>

■ Applying Configuration Changes to Connections

Command	Purpose
<code>write erase</code>	Erases the startup configuration.
Example: <code>hostname(config)# write erase</code>	
<code>clear configure all</code>	Erases the running configuration. Note In multiple context mode, if you enter <code>clear configure all</code> 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.
Example: <code>hostname(config)# clear configure all</code>	

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 81, “Managing 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 “`hostname(config)#`”:

```
hostname(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 A, “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 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: hostname(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 <i>ip_address</i> 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: hostname(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.

■ Applying Configuration Changes to Connections