



Configuring the Adaptive Security Appliance

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

This chapter includes the following sections:

- [About the Factory Default Configuration, page 5-1](#)
- [About the Adaptive Security Device Manager, page 5-3](#)
- [Using the Startup Wizard, page 5-4](#)
- [What to Do Next, page 5-7](#)

About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. The ASA 5505 comes preconfigured with

- Two VLANs: VLAN 1 and VLAN2
- VLAN 1 has the following properties:
 - Named “inside”
 - Allocated switch ports Ethernet 0/1 through Ethernet 0/7

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

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

The default configuration that ships with the adaptive security appliance, in most cases, is sufficient for your basic deployment. However, you can modify the default configuration so that you can customize the security policy to suit your deployment. To modify the default settings, you can use the ASDM or the CLI. In ASDM, run the Startup Wizard to change the following settings from their factory default settings:

- Hostname
- Domain name
- Administrative passwords
- IP address of the outside interface
- Interfaces such as DMZ interfaces
- Address translation rules
- Dynamic IP address settings for the inside interface

For more information about configuring the adaptive security appliance by using ASDM, see the online Help.

For more information about using the CLI configuration, see the *Cisco Security Appliance Command Line Configuration Guide*.

About the Adaptive Security Device Manager



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

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

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface. For more information, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

Using the Startup Wizard

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

This section describes how to use the Startup Wizard to set basic configuration parameters. This section includes the following topics:

- [Before Launching the Startup Wizard, page 5-4](#)
- [Running the Startup Wizard, page 5-5](#)

Before Launching the Startup Wizard

Before you launch the Startup Wizard, perform the following steps:

-
- Step 1** Enable Java and Javascript in your web browser.
- Step 2** Make sure that you can access the Internet.
- Step 3** Obtain the following information:
- A unique hostname to identify the adaptive security appliance on your network.
 - The domain name.
 - The IP addresses of your outside interface, inside interface, and any other interfaces to be configured.
 - IP addresses for hosts that should have administrative access to this device using HTTPS for ASDM, SSH, or Telnet.
 - The privileged mode password for administrative access.
 - The IP addresses to use for NAT or PAT address translation, if any.
 - The IP address range for the DHCP server.
 - The IP address for the WINS server.
 - Static routes to be configured.
 - If you want to create a DMZ, you must create a third VLAN and assign ports to that VLAN. (By default, there are two VLANs configured.)

- Interface configuration information: whether traffic is permitted between interfaces at the same security level, and whether traffic is permitted between hosts on the same interface.
 - If you are configuring an Easy VPN hardware client, the IP addresses of primary and secondary Easy VPN servers; whether the client is to run in client or network extension mode; and user and group login credentials to match those configured on the primary and secondary Easy VPN servers.
-

Running the Startup Wizard

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

-
- Step 1** If you have not already done so, connect a PC to a switch port on the ASA 5505.
- a. Locate an Ethernet cable, which has an RJ-45 connector on each end.
 - b. Connect one RJ-45 connector to the switch port.
 - c. Connect the other end of the Ethernet cable to the Ethernet port on your computer or to your management network.

- Step 2** Start ASDM.
- a. On the PC connected to the ASA 5505, open a web browser.
 - b. In the address field of the web browser, enter the following URL:
https://192.168.1.1/.



Note

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

- c. In the window that requires you to choose the method you want to use to run the ASDM software, choose either to download the ASDM Launcher or to run the ASDM software as a Java applet.

Using the Startup Wizard

- Step 3** In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.
- Step 4** Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.
- The ASDM main window appears.

The screenshot displays the Cisco ASDM 5.2 main window. The interface includes a menu bar (File, Options, Tools, Wizards, Help), a toolbar with icons for Home, Configuration, Monitoring, Back, Forward, Packet Tracer, Refresh, Save, and Help, and a search field. The main content area is divided into several sections:

- Device Information:** Shows Host Name: SecurityAppliance 1, ASA Version: 7.2(0)72, ASDM Version: 5.2(0)30, Firewall Mode: Routed, Total Flash: 64 MB, and Total Memory: 512 MB. Device Uptime is 1d 1h 48m 24s and Device Type is ASA/PIX.
- VPN Status:** Shows IKE Tunnels: 0, WebVPN Tunnels: 0, and SVC Tunnels: 0.
- System Resources Status:** Contains two graphs: CPU Usage (percent) and Memory Usage (MB). Both show low usage levels.
- Interface Status:** A table showing the status of interfaces:

Interface	IP Address/Mask	Line	Link	Kbps
dmz	10.30.30.1/24	down	down	0
inside	10.10.10.1/24	down	down	0
management	172.23.62.22/24	up	up	5
outside	209.165.200.225/24	down	down	0
- Traffic Status:** Contains two graphs: Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps). Both show zero activity.

The status bar at the bottom indicates "Device configuration loaded successfully.", the user is "admin", and the time is 5/10/06 1:08:18 AM PDT.

- Step 5** From the Wizards menu, choose **Startup Wizard**.
- Step 6** Follow the instructions in the Startup Wizard to set up your adaptive security appliance.

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

**Note**

Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using ASDM.

From the ASDM main window, click **Configuration > Properties > Device Administration > ICMP Rules**. Add an entry for the outside interface. Set the IP address to 0.0.0.0, the netmask to 0.0.0.0, and the Action to deny.

What to Do Next

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

To Do This...	See...
Configure the adaptive security appliance to protect a DMZ web server	Chapter 6, “Scenario: DMZ Configuration”
Configure the adaptive security appliance for remote-access VPN	Chapter 7, “Scenario: IPSec Remote-Access VPN Configuration”
Configure the adaptive security appliance for site-to-site VPN	Chapter 8, “Scenario: Site-to-Site VPN Configuration”
Configure the adaptive security appliance as an Easy VPN remote device	Chapter 9, “Scenario: Easy VPN Hardware Client Configuration”

