Your Short Cut to Knowledge

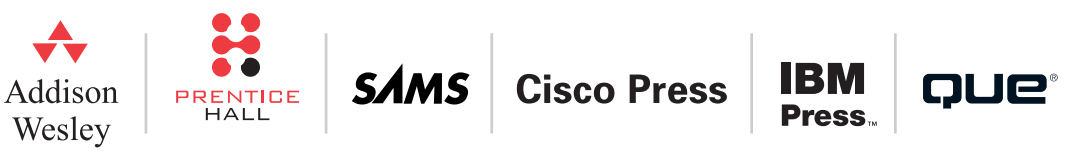
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



Section 2: Initial ASA Configuration

This section covers configuration fundamentals for a Cisco ASA. This section covers basic command-line interface (CLI) configuration, but mainly focuses on configuring the ASA through the graphical Adaptive Security Device Manager (ASDM).

CLI and ASDM Connection

There are two ways to configure a Cisco ASA: through the CLI, or through the ASDM.

Both the CLI and ASDM offer benefits for configuration, and people disagree as to the best method. The CLI versus GUI configuration argument has been around since the days of UNIX versus Windows. The CLI is fast, after you have mastered it, but the GUI is very intuitive and easier to configure, especially with the wizard quick-configuration options now available.

CLI

The CLI is the historic way in which all Cisco devices were configured. This is a command-based interface similar to a UNIX- or DOS-based operating system. Commands are typed through a terminal connection to the ASA, and these are then written to the configuration. The CLI is powerful and fast, but learning how to use the CLI is like learning another language.

NOTE
Because Telnet is sent in clear text and SSH is an encrypted session, you should always use SSH to connect to any network device.

You can either connect to the CLI through the console port using a console cable or by using Telnet or Secure Shell (SSH).

Using a console cable is called an out-of-band connection, and using Telnet or SSH is called an in-band connection.

When you initially connect to an ASA, you are greeted with the following prompt:

```
ciscoasa>
```

 Please see page 132 for more details.

This is called unprivileged mode and is represented by the > after the hostname. Entering **enable** at this prompt places you into privileged EXEC mode, and you will see the following prompt:

```
ciscoasa#
```

From privileged EXEC mode, you can then enter the configuration mode to enter configuration commands into the ASA. The **show** and **debug** commands to monitor and troubleshoot the ASA are also entered in privileged EXEC mode.

ASDM

You access the ASDM through a web browser. ASDM is a Java-based application, so any modern browser that supports Java will suffice (for instance, Safari, Firefox, or Internet Explorer). The connection to ASDM is over SSL, so the configuration is always encrypted between the client and the ASA through the web browser.

Because you have to connect to ASDM through a browser interface, you must configure an IP address on the inside interface to enable you to connect your browser to it. The next section covers interface configuration in more depth.

NOTE
You can use the quick-configuration system to configure the initial parameters of the ASA to facilitate ASDM connection, but we are providing the basic configuration commands without using the quick configuration.

In addition to setting the IP address, you must enter some other basic configuration commands via the CLI to the ASA to configure the initial connection to the ASDM.

We will now run through the necessary commands on an ASA that has a blank configuration. The commands shown are the bare minimum to enable a connection to the ASDM.

Because this is an ASA with a blank configuration, the only way to connect is via the CLI using a serial connection.

The first step is to assign an IP address to the inside interface of the ASA. To enter these commands, you need to be in configuration mode on the ASA. We assume from this point forward that you are in configuration mode; the prompt shows which configuration mode is required:

```
ciscoasa#configuration terminal
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#ip address 192.168.1.254 255.255.255.0
```

 Please see page 132 for more details.

NOTE

For these examples, the configuration from a Cisco ASA 5505 is used. The ASA 5505 has a built-in eight-port switch with no fixed interfaces. IP addresses on the ASA 5505 are configured to VLAN interfaces, and then the VLANs are assigned to the Ethernet interfaces. For other ASA models, the IP address is added straight to the corresponding Ethernet interface.

Because this VLAN is going to be the inside network, we now have to name the VLAN interface as the inside interface:

```
Ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
```

When the **nameif** command is entered, because the value is **inside**, the default security level of 100 is attributed to the VLAN interface.

VLAN1 is now configured as the inside interface with the IP address of 192.168.254.1/24. By default, all ports are in VLAN1, so we now need to tell the ASA 5505 which physical Ethernet port is the inside connection. In this example, we are using Ethernet0/1 as the inside interface, so we enter the following commands to bring up Ethernet0/1, because by default all ports are in an administrative shutdown mode:

```
ciscoasa(config)#interface ethernet0/1
ciscoasa(config-if)#no shutdown
```

Running a **show interface** for Ethernet0/1 now displays the following:

```
ciscoasa#show interface ethernet0/1
Interface Ethernet0/1 "", is up, line protocol is up
  Hardware is 88E6095, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 001b.53a0.4e91, MTU not set
        IP address unassigned
        16423 packets input, 1256399 bytes, 0 no buffer
        Received 896 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 switch ingress policy drops
        6518 packets output, 5096677 bytes, 0 underruns
```

 Please see page 132 for more details.

```
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collisions, 0 deferred
0 lost carrier, 0 no carrier
0 rate limit drops
0 switch egress policy drops
```

We can see that the interface is up. We should now be able to ping the inside interface of the ASA 5505 from a workstation connected to the 192.168.1.0/24 network and be able to ping workstations on the 192.168.1.0/24 network from the ASA 5505.

The next step is to configure a secure password on the ASA. We are about to provide access to the web-based administration interface of the ASA, so we want to ensure that it is protected and locked down with authentication.

We will set an enable password on the ASA:

```
ciscoasa(config)#enable password securepassword
```

The preceding line creates the enable password *securepassword*. Obviously, you would replace this with a very secure, strong password.

At this point, the interface is up and has a valid IP address configured. However, we must complete a couple more steps to facilitate a connection to the ASDM. Running a browser to https://192.168.1.254 at this point will return with a "Page Not Found" message.

The ASA has a built-in web server. This is what serves the ASDM to users requesting it through their browsers. By default, this web server is not enabled.

The internal web server in the ASA is enabled with the following command:

```
ciscoasa(config)#http server enable
```

This enables the HTTP server on the ASA, but if you tried a connection to the ASDM, you still would not be able to connect. This failure to connect results because the ASA operates in a closed policy, unlike the HTTPS server on a router.

 Please see page 132 for more details.

On the ASA, all connections to the HTTP server are denied by default, and you must enter a configuration command to specify the IP addresses that are allowed to access the ASDM. On a router, by default all IP addresses can connect to the HTTP server, and you must create an access list to restrict this access.

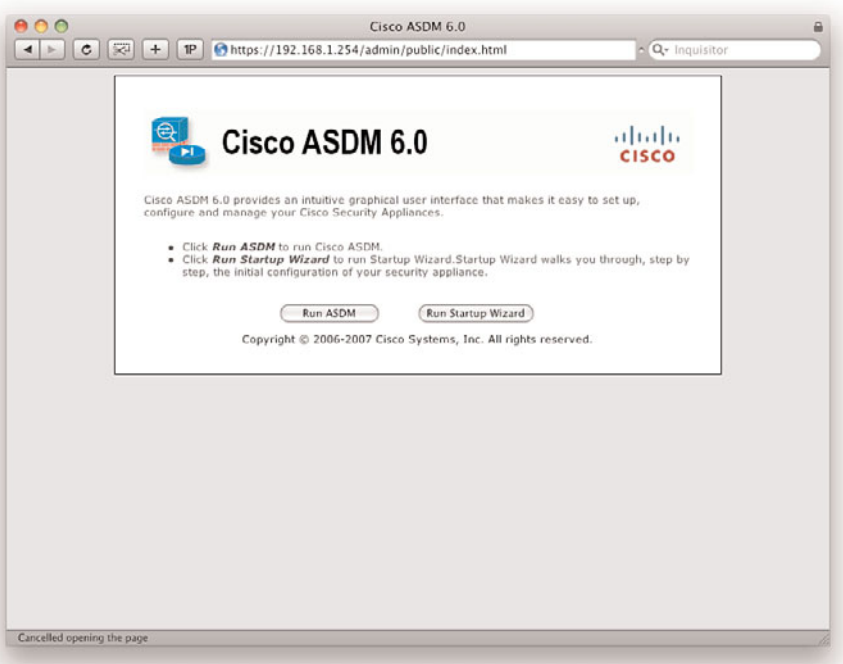
In this example, we want to allow the whole inside network access to the ASDM:

```
ciscoasa(config)#http 192.168.1.0 255.255.255.0 inside
```

The preceding command allows all hosts on the 192.168.1.0/24 network, which is located on the inside interface, access to the ASDM.

Connecting now with a web browser to https://192.168.1.254 will display the initial ASDM connection screen shown in Figure 7.

FIGURE 7
ASDM Connection Screen



 Please see page 132 for more details.