CCNP Security Firewall 642-617 Quick Reference

Andrew Mason

Cisco Press

CCNP Security Firewall 642-617

Quick Reference

Andrew Mason

ciscopress.com

Table of Contents

About the Author

Andrew G. Mason, CCIE No. 7144, CISSP, is a security consultant and co-founder of the UK based RandomStorm Limited. Andrew has 19 years experience in the IT industry, working in Internet security for the past several years. He is involved in the design and implementation of security deployments for numerous clients based upon Cisco technology. He is also a CHECK Team Leader and leads penetration tests for many UK and international clients.

About the Technical Editor:

Max Leitch, CCIE No. 20178, is a network and security architect/engineer and an independent consultant. He holds CCNP, CCDP, CCSP, and CCIE Security certifications.

Section 2:

Basic Connectivity and Device Management

This section starts to look at the configuration of the Cisco ASA and covers the fundamentals for providing basic connectivity and device management. 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

You can configure a Cisco ASA in two ways: 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 intuitive and easier to configure, especially with the wizard quick-configuration options now available.

ASDM is the preferred configuration method for the ASA. Various configuration wizards exist within ASDM that are not available via the CLI alone. The logging and monitoring functionality that the ASDM provides cannot be replicated within the CLI.

Command Line Interface (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.

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.

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.

You can either connect to the CLI through the console port using a console cable or by using Telnet or Secure Shell (SSH). A Cisco console cable is provided with every ASA because this is the normal initial method to connect to the device for the initial configuration.

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

When you first purchase an ASA, you need to configure the ASA through the CLI to configure the initial network settings that enable you to connect to the device using ASDM, which is provided through a web interface, so basic IP settings need to be initially configured.

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

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

```
ciscoasa>
```

This is an unprivileged mode and is represented by the **>** after the hostname.

Entering **enable** at this prompt places you into privileged EXEC mode, and you 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. This is similar to the EXEC modes found within IOS on a Cisco router or switch.

ASDM

ASDM is an acronym for the ASA Security Device Manager (ASDM), which it is the main graphical way to configure, manage, and monitor your ASA Firewall.

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, Chrome, 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.

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.

You now run through the necessary commands on an ASA that has a default blank configuration. The commands shown are the bare minimum to enable a connection to the ASDM and are as far as you need to take the CLI in most cases. 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. The inside interface is the interface on the inside or trusted part of your network. The outside interface is the interface on the outside or untrusted part of your network.

NOTE

For these examples, the configuration from a Cisco ASA 5505 is used, which 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.

To enter these configuration commands, you need to be in configuration mode on the ASA. From this point forward, you should be 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
```

Because this VLAN is going to be the inside network, you now need 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. In contrast to this, the default security level of 0 would be applied to the interface if you name the interface outside.

VLAN1 is now configured as the inside interface with the IP address of 192.168.1.254/24. By default, all ports are in VLAN1, so you now need to tell the ASA 5505 which physical Ethernet port is the inside connection. In this example, you use

Ethernet0/1 as the inside interface, so 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
        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
```

You can see that the interface is up. You can now ping the inside interface of the ASA 5505 from a workstation connected to the 192.168.1.0/24 network and 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. You can provide access to the web-based administration interface of the ASA, so ensure that it is protected and locked down with authentication.

By default there is no password set on the ASA, and anybody can connect to it via the console connection if they have physical access to the device.

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 secure, strong password in line with your corporate password policy.

At this point, the interface is up and has a valid IP address configured. However, you 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 returns with a Page Not Found error 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 could not connect. This failure to connect results because the ASA operates in a closed policy, unlike the HTTPS server on a router.

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, you want to allow the entire inside network access to the ASDM:

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

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

CCNP Security Firewall 642-617 Quick Reference

Andrew Mason

Technical Editor: **Max Leitch**

Copyright © 2011 Pearson Education

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

First Printing January 2011

ISBN-10: 0-13-256643-5

ISBN-13: 978-0-13-256643-8

Warning and Disclaimer

This book is designed to provide information about the CCNP Security Firewall exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc

Trademark Acknowledgments

All terms mentioned in this ebook that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this ebook should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical ebooks of the highest quality and value. Each ebook is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this ebook, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please be sure to include the ebook title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this ebook when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**