Cisco ASA for Accidental Administrators®

Version 1.1

Corrected Table of Contents

Contents

PRELUDE

CHAPTER 1: Understanding Firewall Fundamentals

What Do Firewalls Do? 5

Types of Firewalls 6

Classification of Firewalls 8

Need a refresher on the OSI Reference Model? 8

Firewall Spectrum 9

Stateful Inspection 9

Established Connections 9

Adaptive Security Algorithm 10

An Overview of Cisco Security Appliances 10

Cisco Small Office and Branch Office ASA Security Appliances 10

Cisco Internet Edge and Enterprise Data Center ASA Security Appliances 12

Memory on the Cisco ASA Security Appliance 12

The Cisco ASA 5505 Chassis 13

The Rear Panel 14

Controlling the Appliance from its Serial Cable Console Interface 14

Navigating in the Cisco Command Line 16

Getting Help in the Command Line 17

Help in the ASDM 19

Command Shorthand Abbreviation 19

Password Recovery 19

Password Recovery on the ASA Security Appliance 20

ASA Software Version 20

Hands-On Exercise 1.1: Connecting to the Security Appliance's Console Port 21

Hands-On Exercise 1.2: Password Recovery on the Security Appliance 23

Erasing the Stored Configuration 27

Hands-On Exercise 1.3: Removing the Existing Configuration 27

Some ASA Basics 28

Network Address Translation (NAT) 28

If You Are Using an ASA Software Version Prior to 8.3(1) 29

Understanding VLANs and Security Levels 30

Security Levels 30

AAA: Authentication, Authorization, and Accounting 31

Basics of Encryption Including Single Key and PKI 32

Understanding the Eight Basic Commands on a Cisco ASA Security Appliance 33

Just Beyond the Basics 36

Sample Base Configuration 37

Configuring NAT Prior to Software Version 8.3(1) 38

Hands-On Exercise 1.4: Using the Eight Commands Required to Enable Basic Firewall Functionality 39

Configure Port Address Translation 42

If the ASA Doesn't Accept the Port Address Translation Commands 42

Test the Configuration 43

Adaptive Security Device Manager 43

Hands-On Exercise 1.5: Removing the Existing Configuration on Your Security Appliance and Installing the Factory Default Configuration 44

Hands-On Exercise 1.6: Using ASDM to Build an Initial Configuration on Your ASA 46

What is Smart Call Home? 52

Hands-On Exercise 1.7: Previewing Commands 52

CHAPTER 2:
Backing Up and Restoring Configurations and Software Images

Analyzing the Base Configuration of the Security Appliance 53

Saving Your ASA's Base Configuration 53

Hands-On Exercise 2.1: Confirm Network Connectivity 54

Hands-On Exercise 2.2: Review and Backup Configuration Information 55

Backing Up Your Configuration and Your Software 59

Hands-On Exercise 2.3: Install and Configure the TFTP Server Software on Your PC 59

Hands-On Exercise 2.4: The Cisco ASA Configuration Backup Process 60

Hands-On Exercise 2.5: The Cisco ASA Configuration Restore Process 61

Backing Up, Upgrading, and Restoring the Software Image 62

Hands-On Exercise 2.6: Backup Your ASA's Software to the TFTP Server 62

Upgrading the ASA Software Image 63

Hands-On Exercise 2.7: Upgrading the ASA Software in the Command Line Environment 64

Hands-On Exercise 2.8: Upgrading the ASDM Software in the Command Line Environment 66

Hands-On Exercise 2.9: Upgrading Software Directly from Cisco in the ASDM 68

Hands-On Exercise 2.10: Restore the ASA Software in a Fault Condition 73

A Third-Party Software and Configuration Management Tool 74

CHAPTER 3:
Sending Logging Output to a Syslog Server

Using syslogd with the Security Appliance 75

Hands-On Exercise 3.1: Sending Logging Output to a Syslog Server 76

CHAPTER 4:
Remote Management Options

Remote Console Access 79

Hands-On Exercise 4.1: Configuring and Using Telnet 81

Hands-On Exercise 4.2: Testing the Telnet Configuration 82

Hands-On Exercise 4.3: Configuring and Using SSH (Secure Shell) 83

Hands-On Exercise 4.4: Test the SSH Configuration 84

Configuring and Managing Remote Management through ASDM 85

CHAPTER 5:
Logon Banners and Authentication, Authorization, and Accounting

Configuring Banners 87

How to Configure a Banner 88

Hands-On Exercise 5.1: Creating CLI Banners on the Security Appliance..........................89

Hands-On Exercise 5.2: Test the Banner Configuration 90

Hands-On Exercise 5.3: Configuring an ASDM Banner 90

Displaying and Clearing Banners 92

Configuring Authentication, Authorization, and Accounting (AAA) 92

Hands-On Exercise 5.4: Configuring Usernames and Local Authentication........................94

Hands-On Exercise 5.5: Testing the Configuration 98

How to Use Active Directory to Authenticate RADIUS Users 99

Hands-On Exercise 5.6: How to Configure RADIUS
on a Windows Server 2012 Computer 99

Hands-On Exercise 5.7: Configuring SSH Authentication through Active Directory 111

CHAPTER 6:
Configuring the Appliance as a DHCP Server

Configuring DHCP on an ASA Security Appliance 115

Hands-On Exercise 6.1: Reconfiguring Your DHCP Server... 116

If You're Running an Earlier Version of the ASA Software 118

CHAPTER 7:
Access Control Lists

Understanding Access Control Lists 121

Rules for Access-Control Lists 122

Types of Access-Control Lists 122

ACL Syntax 122

Using Access-Control Lists 125

Understanding Network Address Translation (NAT) 127

CHAPTER 8:
Virtual Private Networking (VPNs)

Understanding the Purpose and Types of Virtual Private Networks 131

VPN Protocols 133

Hands-On Exercise 8.1: Configuring Site-to-Site VPNs Using the Command Line Interface 135

Configuring a Site-to-Site VPN Using the GUI-based Wizard 143

Hands-On Exercise 8.2: Configuring Site-to-Site VPNs Using the ASDM 144

Remote Access VPNs 150

Hands-On Exercise 8.3: Configuring a Cisco AnyConnect Remote Access VPN 151

Hands-On Exercise 8.4: Configuring ASA VPN Authentication through Active Directory Using RADIUS 163

Hands-On Exercise 8.5: Configuring LDAP Authentication 165

Hands-On Exercise 8.6: Configuring Kerberos Authentication 167

Hands-On Exercise 8.7: Configuring the ASA as a Network Time Protocol Client 169

Creating a Web-Based SSL VPN 170

Hands-On Exercise 8.8: Configuring a Web-Based SSL VPN 170

How to Install an SSL Digital Certificate for Use with an SSL VPN 174

Hands-On Exercise 8.9: Installing an SSL Digital Certificate 175

Hands-On Exercise 8.10: Enabling the SSL Certificate 180

Enhancing the Web VPN Portal with Plug-Ins 181

Installing Plug-Ins on the Security Appliance 182

Hands-On Exercise 8.11: Installing and Removing Plug-Ins 183

To Troubleshoot and Test the Configuration 185

CHAPTER 9:
De-Militarized Zones (DMZs)

Understanding a De-Militarized Zone 187

Hands-On Exercise 9.1: Configuring a DMZ........ 189

Hands-On Exercise 9.2: Installing the Abyss Web Server Software 194

Hands-On Exercise 9.3: Allowing Inside Hosts and Internet Hosts Access to the DMZ Web Server........ 195

Hands-On Exercise 9.4: Using the ASDM to Configure a DHCP Server 196

CHAPTER 10:
Filtering Content

Options for Filtering Content and Threat Detection 199

Hands-On Exercise 10.1: Filtering Dynamic Content 203

Auditing for Vulnerabilities Using Port Scanning 204

Hands-On Exercise 10.2: Analyzing Potential Vulnerabilities with Port Scanning 204

CHAPTER 11:
Configuring Transparent Mode

Understanding Transparent Mode 207

Hands-On Exercise 11.1: Viewing and Changing the Mode 209

POSTLUDE

APPENDICES

Appendix A: Security Fundamentals........ 216

Appendix B: Understanding Security Contexts 224

Appendix C: The Tools of the Book 226

Appendix D: Table of Figures 227

INDEX