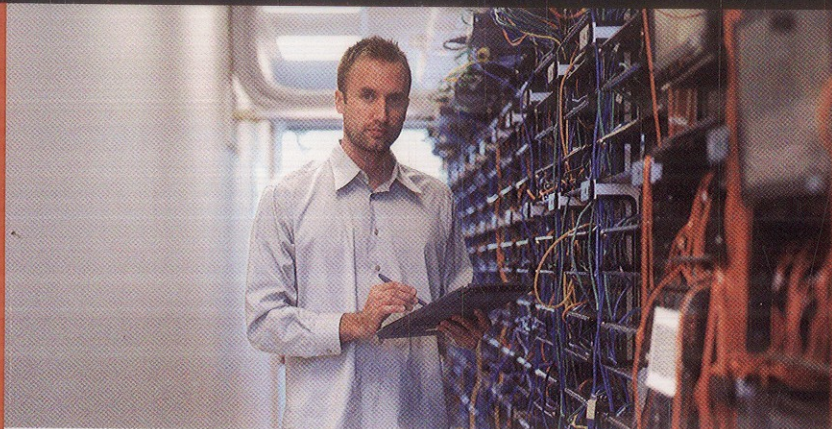




SECURITY

Cisco ASA, PIX, and FWSM Firewall Handbook

Second Edition

The complete guide to the most popular Cisco
ASA 8.0 and FWSM 3.2 firewall security features

Contents

Foreword xxii

Introduction xxiii

Chapter 1 Firewall Overview 3

1-1: Overview of Firewall Operation 4

Initial Checking 5

Xlate Lookup 6

Conn Lookup 7

ACL Lookup 8

Uauth Lookup 8

Inspection Engine 9

1-2: Inspection Engines for ICMP, UDP, and TCP 9

ICMP Inspection 10

A Case Study in ICMP Inspection 12

UDP Inspection 13

TCP Inspection 15

Additional TCP Connection Controls 17

TCP Normalization 18

Other Firewall Operations 19

1-3: Hardware and Performance 19

1-4: Basic Security Policy Guidelines 21

Further Reading 24

Chapter 2 Configuration Fundamentals 27

2-1: User Interface 27

User Interface Modes 28

User Interface Features 29

Entering Commands 29

Command Help 31

Command History 32

Searching and Filtering Command Output 32

Terminal Screen Format 34

2-2: Firewall Features and Licenses 34

Upgrading a License Activation Key 40

2-3: Initial Firewall Configuration 41

Chapter 3 Building Connectivity 45

3-1: Configuring Interfaces	45
Surveying Firewall Interfaces	46
Configuring Interface Redundancy	48
Basic Interface Configuration	50
Interface Configuration Examples	58
Configuring IPv6 on an Interface	60
Testing IPv6 Connectivity	67
Configuring the ARP Cache	68
Configuring Interface MTU and Fragmentation	70
Configuring an Interface Priority Queue	73
Displaying Information About the Priority Queue	77
Firewall Topology Considerations	77
Securing Trunk Links Connected to Firewalls	79
Bypass Links	81
3-2: Configuring Routing	83
Using Routing Information to Prevent IP Address Spoofing	84
Configuring Static Routes	86
Static Route Example	89
Favoring Static Routes Based on Reachability	89
Reachable Static Route Example	92
Configuring RIP to Exchange Routing Information	95
RIP Example	97
Configuring EIGRP to Exchange Routing Information	97
An EIGRP Configuration Example	101
Configuring OSPF to Exchange Routing Information	101
OSPF Routing Scenarios with a Firewall	102
OSPF Used Only on the Inside	102
OSPF Used Only on the Outside	102
OSPF Used on Both Sides of the Firewall (Same Autonomous System)	103
OSPF Used on Both Sides of the Firewall (Different Autonomous Systems)	104
Configuring OSPF	105
Redistributing Routes from Another Source into OSPF	112
OSPF Example	115
3-3: DHCP Server Functions	116
Using the Firewall as a DHCP Server	117
DHCP Server Example	120
Updating Dynamic DNS from a DHCP Server	120
Verifying DDNS Operation	123
Relaying DHCP Requests to a DHCP Server	124
DHCP Relay Example	125

3-4: Multicast Support	126
Multicast Overview	126
Multicast Addressing	127
Forwarding Multicast Traffic	128
Multicast Trees	128
Reverse Path Forwarding	128
IGMP: Finding Multicast Group Recipients	129
IGMPv1	129
IGMPv2	130
PIM: Building a Multicast Distribution Tree	130
PIM Sparse Mode	131
PIM RP Designation	136
Configuring PIM	137
Using a Multicast Boundary to Segregate Domains	142
Filtering PIM Neighbors	143
Filtering Bidirectional PIM Neighbors	144
Configuring Stub Multicast Routing (SMR)	145
Configuring IGMP Operation	147
Stub Multicast Routing Example	150
PIM Multicast Routing Example	151
Verifying IGMP Multicast Operation	151
Verifying PIM Multicast Routing Operation	152

Chapter 4 Firewall Management 157

4-1: Using Security Contexts to Make Virtual Firewalls	157
Security Context Organization	158
Sharing Context Interfaces	158
Issues with Sharing Context Interfaces	161
Solving Shared Context Interface Issues with Unique MAC Addresses	165
Configuration Files and Security Contexts	168
Guidelines for Multiple-Context Configuration	169
Initiating Multiple-Context Mode	170
Navigating Multiple Security Contexts	173
Context Prompts	173
Changing a Session to a Different Context	174
Configuring a New Context	174
Context Definition Example	180
Allocating Firewall Resources to Contexts	185
Verifying Multiple-Context Operation	191
4-2: Managing the Flash File System	192
Navigating an ASA or FWSM Flash File System	194
Administering an ASA or FWSM Flash File System	196
Using the PIX 6.3 Flash File System	200

Identifying the Operating System Image	200
Upgrading an Image from the Monitor Prompt	202
Upgrading an Image from an Administrative Session	206
Upgrading an Image Automatically	211
4-3: Managing Configuration Files	211
Managing the Startup Configuration	211
Selecting a Startup Configuration File	212
Displaying the Startup Configuration	213
Saving a Running Configuration	214
Viewing the Running Configuration	214
Saving the Running Configuration to Flash Memory	214
Saving the Running Configuration to a TFTP Server	216
Forcing the Running Configuration to Be Copied Across a Failover Pair	217
Forcing the Startup (Nonvolatile) Configuration to Be Cleared	218
Importing a Configuration	218
Entering Configuration Commands Manually	218
Merging Configuration Commands from Flash Memory	219
Merging Configuration Commands from a TFTP Server	219
Merging Configuration Commands from a Web Server	220
Merging Configuration Commands from an Auto Update Server	221
4-4: Automatic Updates with an Auto Update Server	221
Configuring a Firewall as an Auto Update Client	221
Verifying Auto Update Client Operation	227
Configuring a Firewall as an Auto Update Server	228
4-5: Managing Administrative Sessions	232
Console Connection	232
Telnet Sessions	234
SSH Sessions	235
ASDM/PDM Sessions	238
Starting the ASDM or PDM Application from a Web Browser	240
Starting ASDM from a Local Application	241
User Session Banners	243
Monitoring Administrative Sessions	244
4-6: Firewall Reloads and Crashes	246
Reloading a Firewall	246
Reloading a Firewall Immediately	246
Reloading a Firewall at a Specific Time and Date	247
Reloading a Firewall After a Time Interval	247
Obtaining Crash Information	248
Controlling Crashinfo Creation	249
Generating a Test Crashinfo Image	249

	Forcing an Actual Firewall Crash	250
	Viewing the Crashinfo Information	250
	Deleting the Previous Crashinfo File Contents	251
4-7:	Monitoring a Firewall with SNMP	251
	Overview of Firewall SNMP Support	252
	Firewall MIBs	253
	Firewall SNMP Traps	255
	SNMP Configuration	256
Chapter 5	Managing Firewall Users	261
5-1:	Managing Generic Users	262
	Authenticating and Authorizing Generic Users	262
	Accounting of Generic Users	263
5-2:	Managing Users with a Local Database	264
	Authenticating with Local Usernames	265
	Authorizing Users to Access Firewall Commands	267
	Accounting of Local User Activity	272
5-3:	Defining AAA Servers for User Management	271
5-4:	Configuring AAA to Manage Administrative Users	280
	Enabling AAA User Authentication	281
	Enabling AAA Command Authorization	283
	Enabling AAA Command Accounting	286
5-5:	Configuring AAA for End-User Cut-Through Proxy	287
	Authenticating Users Passing Through	287
	Authorizing User Activity with TACACS+ Servers	291
	Authorizing User Activity with RADIUS Servers	294
	Keeping Accounting Records of User Activity	299
	AAA Cut-Through Proxy Configuration Examples	300
5-6:	Firewall Password Recovery	302
	Recovering ASA Password	302
	Recovering a PIX Password	306
	Recovering an FWSM Password	307
Chapter 6	Controlling Access Through the Firewall	311
6-1:	Routed and Transparent Firewall Modes	311
	Configuring a Transparent Firewall	314
6-2:	Address Translation	323
	Defining Access Directions	323
	Outbound Access	323
	Inbound Access	324
	Same-Security Access	324

Types of Address Translation	325
Handling Connections Through an Address Translation	328
UDP and TCP Connection Limits	329
Limiting Embryonic Connections	330
TCP Initial Sequence Numbers	331
Static NAT	331
Policy NAT	335
Identity NAT	338
NAT Exemption	340
Dynamic Address Translation (NAT or PAT)	341
Dynamic NAT and PAT Example	346
Controlling Traffic	348
Controlling Access with Medium Security Interfaces	349
6-3: Controlling Access with Access Lists	352
Compiling Access Lists	352
Configuring an Access List	353
Adding an ACE to an Access List	354
Manipulating Access Lists	357
Adding Descriptions to an Access List	359
Defining a Time Range to Activate an ACE	360
Access List Examples	362
Defining Object Groups	363
Defining Network Object Groups	364
Defining Protocol Object Groups	365
Defining ICMP Type Object Groups	367
Defining Basic Service Object Groups	369
Defining an Enhanced Service Object Group	370
Using Object Groups in an Access List	373
Logging ACE Activity	379
Monitoring Access Lists	380
6-4: Shunning Traffic	382
Shun Example	384
Chapter 7 Inspecting Traffic	389
7-1: Filtering Content	389
Configuring Content Filters	390
Content-Filtering Examples	396
Using a Web Cache for Better HTTP Performance	396
7-2: Defining Security Policies in a Modular Policy Framework	397
Classifying Layers 3 and 4 Traffic	398
Match Against a Destination Port Number	400

Match Against an Access List	400
Match Against QoS Parameters	402
Match Against a Range of Real-Time Transport Protocol (RTP) Port Numbers	404
Match Against a VPN Tunnel Group	405
Match All Traffic	405
Match Default Traffic	405
Classifying Management Traffic	406
Defining a Layer 3/4 Policy	406
Set Connection Limits on the Matched Traffic	409
Adjust TCP Options for the Matched Traffic	412
Send the Matched Traffic to an IPS Module	415
Send the Matched Traffic to a CSC Module	416
Use a Policier to Limit the Matched Traffic Bandwidth	417
Give Priority Service (LLQ) to Matched Traffic	420
Default Policy Definitions	421
7-3: Application Inspection	423
Configuring Application Inspection	426
Matching Text with Regular Expressions	433
Configuring DCERPC Inspection	437
Configuring DNS Inspection	438
Configuring ESMTP Inspection	441
Configuring FTP Inspection—ASA 7.2(1) or Later	443
Configuring FTP Inspection—FWSM and ASA 7.0-7.1	445
Configuring GTP Inspection—ASA 7.2(1) and Later	446
Configuring GTP Inspection—FWSM and ASA 7.0-7.1	448
Configuring H.323 Inspection	449
Configuring HTTP Inspection—ASA 7.2(1) and Later	451
Configuring HTTP Inspection—FWSM and ASA 7.0-7.1	455
Configuring ICMP Inspection	460
Configuring Instant Messaging (IM) Inspection	462
Configuring IPsec Passthru Inspection	464
Configuring MGCP Inspection—ASA 7.2(1) and later	465
Configuring an MGCP Map—FWSM and ASA 7.0-7.1	467
Configuring NetBIOS Inspection	468
Configuring RADIUS Accounting Inspection	468
Configuring SNMP Inspection	470

Chapter 8 Increasing Firewall Availability with Failover 473

8-1: Firewall Failover Overview	473
How Failover Works	475
Firewall Failover Roles	477
Detecting a Firewall Failure	480
Failover Communication	481

Active-Active Failover Requirements 482

8-2: Configuring Firewall Failover 484

8-3: Firewall Failover Configuration Examples 498

Active-Standby Failover Example with PIX Firewalls 498

Active-Standby Failover Example with FWSM 500

Active-Active Failover Example 501

Primary Firewall Configuration 503

Secondary Firewall Configuration 504

Allocating Interfaces to the Contexts 505

Configuring Interfaces in Each Context 506

8-4: Managing Firewall Failover 508

Displaying Information About Failover 508

Displaying the Current Failover Status 510

Displaying the LAN-Based Failover Interface Status 512

Displaying a History of Failover State Changes 513

Debugging Failover Activity 513

Monitoring Stateful Failover 514

Manually Intervening in Failover 516

Forcing a Role Change 516

Resetting a Failed Firewall Unit 517

Reloading a Hung Standby Unit 517

Executing Commands on a Failover Peer 517

8-5: Upgrading Firewalls in Failover Mode 519

Manually Upgrading a Failover Pair 520

Automatically Upgrading a Failover Pair 524

Chapter 9 Firewall Load Balancing 527

9-1: Firewall Load Balancing Overview 527

9-2: Firewall Load Balancing in Software 530

IOS FWLB Configuration Notes 531

IOS FWLB Configuration 535

IOS Firewall Load-Balancing Example 540

Basic Firewall Configuration 541

Outside IOS FWLB Configuration 543

Inside IOS FWLB Configuration 545

Displaying Information About IOS FWLB 546

IOS FWLB Output Example 547

9-3: Firewall Load Balancing in Hardware 549

FWLB in Hardware Configuration Notes 551

CSM FWLB Configuration	552
CSM Firewall Load-Balancing Example	561
CSM Components Needed	562
Basic Firewall Configuration	563
Outside CSM FWLB Configuration	565
Inside CSM Configuration	567
Displaying Information About CSM FWLB	569
CSM FWLB Output Example	569

9-4: Firewall Load-Balancing Appliance	571
CSS FWLB Configuration	572
CSS Appliance Firewall Load-Balancing Example	574
Basic Firewall Configuration	575
Outside CSS FWLB Configuration	578
Inside CSS FWLB Configuration	578
Displaying Information About CSS FWLB	579

Chapter 10 Firewall Logging 581

10-1: Managing the Firewall Clock	581
Setting the Clock Manually	582
Setting the Clock with NTP	584
10-2: Generating Logging Messages	587
Syslog Server Suggestions	589
Logging Configuration	591
<i>Configuring Basic Logging Parameters</i>	593
Log to an Interactive Firewall Session	595
Log to the Firewall's Internal Buffer	597
Log to an SNMP Management Station	599
Logging to a Syslog Server	600
Logging to a Secure Syslog Server Using SSL	604
Logging to an E-mail Address	611
Logging to an ASDM Management Application	613
Verifying Message Logging Activity	614
Manually Testing Logging Message Generation	615
10-3: Fine-Tuning Logging Message Generation	615
Pruning Messages	616
Changing the Message Severity Level	616
Access List Activity Logging	617
10-4: Analyzing Firewall Logs	619

Chapter 11 Verifying Firewall Operation 625

- 11-1: Checking Firewall Vital Signs 625
 - Using the Syslog Information 626
 - Checking System Resources 627
 - Firewall CPU Load 627
 - Firewall Memory 633
 - Checking Stateful Inspection Resources 636
 - Xlate Table Size 636
 - Conn Table Size 637
 - Checking Firewall Throughput 638
 - ASDM 638
 - Syslog 639
 - Traffic Counters 640
 - Perfmon Counters 643
 - Checking Inspection Engine and Service Policy Activity 645
 - Checking Failover Operation 646
 - Verifying Failover Roles 646
 - Verifying Failover Communication 647
 - Determining if a Failover Has Occurred 650
 - Determining the Cause of a Failover 652
 - An Example of Finding the Cause of a Failover 653
 - Intervening in a Failover Election 655
 - Checking Firewall Interfaces 655
 - Interface Name and Status 657
 - Interface Control 657
 - Interface Addresses 658
 - Inbound Packet Statistics 659
 - ~~Outbound Packet Statistics 660~~
 - Traffic Statistics 662
 - Packet Queue Status 662
- 11-2: Watching Data Pass Through a Firewall 666
 - Using Capture 667
 - Defining a Capture Session 667
 - Getting Results from a Capture Session 673
 - Using a Capture Session to Display Trunk Contents 675
 - Copying Capture Buffer Contents 676
 - Controlling a Capture Session 680
 - A Capture Example 681
 - Using the ASDM Packet Capture Wizard 683
 - Capturing FWSM Packets Inside the Switch 686
 - Using Debug Packet 689
- 11-3: Verifying Firewall Connectivity 691

Step 1: Test with Ping Packets	695
Step 2: Check the ARP Cache	698
Step 3: Check the Routing Table	700
Step 4: Use Traceroute to Verify the Forwarding Path	700
Using Traceroute on a Host	702
Using Traceroute on the Firewall	703
Step 5: Check the Access Lists	705
Step 6: Verify the Address Translation and Connection Tables	709
Monitoring Translations	709
Monitoring Connections	711
Monitoring Specific Hosts	715
Clearing Xlate Table Entries	717
Adjusting Table Timeout Values	717
Step 7: Look for Active Shuns	718
Step 8: Check User Authentication	720
Authentication Proxy (Uauth)	720
Content Filtering	721
Step 9: See What Has Changed	722

Chapter 12 ASA Modules 725

12-1: Initially Configuring an ASA SSM	726
Preparing the ASA for SSM Management Traffic	726
Connecting and Configuring the SSM Management Interface	727
12-2: Configuring the CSC SSM	729
Configuring the ASA to Divert Traffic to the CSC SSM	730
Configuring the Initial CSC SSM Settings	733
Repairing the Initial CSC Configuration	738
Connecting to the CSC Management Interface	740
Configuring Automatic Updates	741
Configuring CSC Inspection Policies	744
Configure Web (HTTP) Inspection Policies	745
Configuring URL Blocking	745
Configuring URL Filtering Rules	746
Configuring URL Filtering Settings	748
Configuring HTTP File Blocking	751
Configuring HTTP Scanning	751
Configuring File Transfer (FTP) Inspection Policies	753
Configuring Mail (SMTP and POP3) Inspection Policies	755
Scanning SMTP Traffic	756
Filtering SMTP Content	758
Detecting Spam SMTP E-mail	759
Configuring General SMTP Mail Handling	763
Scanning POP3 Traffic	765

Detecting Spam in POP3 E-mail 767

Filtering POP3 Content 768

12-3: Configuring the AIP SSM 769

Initially Configuring the AIP 769

Managing the AIP 773

Updating the AIP License 773

Manually Updating the AIP Code or Signature Files 774

Automatically Updating AIP Image and Signature Files 775

IPS Policies 777

Working with Signature Definitions 777

Working with Event Action Rules 777

Working with Anomaly Detection Policies 778

AIP Interfaces 780

IPS Virtual Sensors 781

Appendix A Well-Known Protocol and Port Numbers 787

Appendix B Security Appliance Logging Messages 797

Index 846