

Contents

Foreword	xxiii
Introduction	xxv
Chapter 1 Introduction to Security and Firewalls	1
Introduction	2
The Importance of Security	2
What Is Information Security?	3
The Early Days of Information Security	5
Insecurity and the Internet	5
The Threats Grow	6
Attacks	7
Creating a Security Policy	8
Cisco's Security Wheel	11
Securing the Environment	12
Monitoring Activity	14
Testing Security	15
Improving Security	17
Firewall Concepts	17
What Is a Firewall?	17
Types of Firewalls	19
Packet Filters	20
Stateful Inspection Packet Filters	21
Application Proxies	22
Firewall Interfaces: Inside, Outside, and DMZ	23
Firewall Policies	26
Address Translation	26
Static Translation	27
Dynamic Translation	28
Port Address Translation	29

Virtual Private Networking	29
Cisco Security Certifications	31
Cisco Security Specialist 1	31
Requirements	32
Cisco Certified Internetwork Expert Security	32
The Written Test	33
The Lab Exam	33
CSPFA: The Exam	34
Exam Objectives	34
Summary	37
Solutions Fast Track	38
Frequently Asked Questions	40
Chapter 2 Introduction to PIX Firewalls	43
Introduction	44
PIX Firewall Features	44
Embedded Operating System	45
The Adaptive Security Algorithm	46
State	47
Security Levels	49
How ASA Works	49
Technical Details for ASA	50
User Datagram Protocol	54
Advanced Protocol Handling	55
VPN Support	56
URL Filtering	57
NAT and PAT	57
High Availability	59
PIX Hardware	59
Models	59
PIX 501	61
PIX 506	61
PIX 506E	61
PIX 515	61
PIX 515E	62
PIX 520	62
PIX 525	63
PIX 535	63

The Console Port	63
Software Licensing and Upgrades	65
Licensing	67
Upgrading Software	67
Password Recovery	69
The Command-Line Interface	71
Factory Default Configurations	71
PIX 501 and 506E	71
PIX 515E, 525, and 535	72
Administrative Access Modes	72
Basic Commands	75
Hostname and Domain Name	76
Configuring Interfaces	76
Static Routes	78
Password Configuration	78
Managing Configurations	79
The write Command	79
The copy Command	80
The configure Command	81
Resetting the System	82
The reload Command	82
Summary	83
Solutions Fast Track	85
Frequently Asked Questions	88

Chapter 3 Passing Traffic 91

Introduction	92
Allowing Outbound Traffic	92
Configuring Dynamic Address Translation	93
Identity NAT and NAT Bypass	97
Blocking Outbound Traffic	100
Access Lists	100
Outbound/Apply	109
Allowing Inbound Traffic	111
Static Address Translation	112
Access Lists	113
Conduits	113
ICMP	114

Port Redirection	115
TurboACLs	116
Object Grouping	117
Configuring and Using Object Groups	118
ICMP-Type Object Groups	118
Network Object Groups	119
Protocol Object Groups	119
Service Object Groups	120
Case Study	122
Access Lists	124
Conduits and Outbound/Apply	127
Summary	130
Solutions Fast Track	130
Frequently Asked Questions	132

Chapter 4 Advanced PIX Configurations 135

Introduction	136
Handling Advanced Protocols	136
File Transfer Protocol	141
Active vs. Passive Mode	141
Domain Name Service	146
Simple Mail Transfer Protocol	148
Hypertext Transfer Protocol	150
Remote Shell	150
Remote Procedure Call	152
Real-Time Streaming Protocol, NetShow, and VDO Live	153
SQL*Net	157
H.323 and Related Applications	159
Skinny Client Control Protocol	161
Session Initiation Protocol	162
Internet Locator Service and Lightweight	
Directory Access Protocol	164
Filtering Web Traffic	165
Filtering URLs	166
Websense and N2H2	167
Fine-Tuning and Monitoring the Filtering Process	169
Active Code Filtering	173
Filtering Java Applets	174
Filtering ActiveX Objects	174

Configuring Intrusion Detection	175
Supported Signatures	175
Configuring Auditing	179
Disabling Signatures	181
Configuring Shunning	182
DHCP Functionality	182
DHCP Clients	183
DHCP Servers	185
Cisco IP Phone-Related Options	189
Other Advanced Features	189
Fragmentation Guard	189
AAA Floodguard	191
SYN Floodguard	192
Reverse-Path Forwarding	194
Unicast Routing	197
Static and Connected Routes	197
Routing Information Protocol	199
Stub Multicast Routing	202
SMR Configuration with Clients on a More Secure Interface	204
SMR Configuration with Clients on a Less Secure Interface	206
Access Control and Other Options	207
PPPoE	209
Summary	212
Solutions Fast Track	213
Frequently Asked Questions	215

Chapter 5 Configuring Authentication, Authorization, and Accounting 217

Introduction	218
AAA Concepts	218
Authentication	221
Authorization	222
Accounting	223
AAA Protocols	223
RADIUS	223
TACACS+	225

Cisco Secure ACS for Windows	228
Introduction and Features	229
Installing and Configuring Cisco Secure ACS	230
Adding an NAS to Cisco Secure ACS	237
Adding a User to Cisco Secure ACS	240
Configuring Console Authentication	242
Configuring Local Console Authentication	243
Configuring RADIUS and TACACS+	
Console Authentication	244
Configuring TACACS+ Enable Console	
Authentication in Cisco Secure ACS	246
Configuring Command Authorization	250
Configuring Local Command Authorization	251
Configuring TACACS+ Command Authorization	252
Configuring Cisco Secure ACS to Support	
TACACS+ Command Authorization	253
Defining the Shell Command Authorization Set	255
Assigning the Command Authorization	
Set to Users or Groups	258
Enabling Command Authorization	
on the PIX Firewall	260
Configuring Authentication for Traffic Through the Firewall	260
Configuring Cut-Through Proxy	260
Virtual HTTP	266
Virtual Telnet	268
Configuring Authorization for Traffic Through the Firewall	270
Configuring Accounting for Traffic Through the Firewall	272
Configuring Downloadable Access Lists	275
Configuring Named Downloadable Access Lists	275
Configuring Downloadable Access Lists Without Names	280
Summary	282
Solutions Fast Track	283
Frequently Asked Questions	287
Chapter 6 Configuring System Management	289
Introduction	290
Configuring Logging	290
Local Logging	291
Buffered Logging	292

Console Logging	293
Terminal Logging	293
Syslog	293
Logging Levels	299
Logging Facility	302
Disabling Specific Syslog Messages	303
Configuring Remote Access	304
Secure Shell	305
Enabling SSH Access	306
Troubleshooting SSH	311
Telnet	314
Restrictions	315
HTTP Via the PIX Device Manager	316
Configuring Simple Network Management Protocol	316
Configuring System Identification	317
Configuring Polling	318
Configuring Traps	320
Configuring System Date and Time	321
Setting and Verifying the Clock and Time Zone	322
Configuring and Verifying the Network Time Protocol	324
NTP Authentication	325
Summary	327
Solutions Fast Track	328
Frequently Asked Questions	330

Chapter 7 Configuring Virtual Private Networking 333

Introduction	334
IPsec Concepts	334
IPsec	335
IPsec Core Layer 3 Protocols: ESP and AH	335
IPsec Communication Modes: Tunnel and Transport	338
Internet Key Exchange	340
Security Associations	343
Certificate Authority Support	348
Configuring Site-to-Site IPsec Using IKE	349
Planning	349
Allowing IPsec Traffic	350
Enabling IKE	352

Creating an ISAKMP Protection Suite	352
Defining an ISAKMP Pre-Shared Key	354
Configuring Certificate Authority Support	354
Configuring the Hostname and Domain Name	356
Generating an RSA Key Pair	356
Specifying a CA to Be Used	357
Configuring CA Parameters	358
Authenticating the CA	358
Enrolling with the CA	360
Configuring Crypto Access Lists	362
Defining a Transform Set	364
Bypassing Network Address Translation	365
Configuring a Crypto Map	366
Troubleshooting	369
Configuring Site-to-Site IPsec Without IKE (Manual IPsec)	369
Configuring Point-to-Point Tunneling Protocol	372
Overview	373
Configuration	375
Setting Up Windows 2000 Clients	380
Configuring Layer 2 Tunneling Protocol with IPsec	383
Overview	384
Dynamic Crypto Maps	384
Configuration	386
Setting Up the Windows 2000 Client	389
Configuring Support for the Cisco Software VPN Client	390
Mode Configuration	391
Extended Authentication	392
VPN Groups	394
Sample Configurations of PIX and VPN Clients	397
Summary	407
Solutions Fast Track	408
Frequently Asked Questions	410
Chapter 8 Configuring Failover	413
Introduction	414
Failover Concepts	414
Configuration Replication	417
IP and MAC Addresses Used for Failover	418

Failure Detection	419
Stateful Failover	420
Standard Failover Using a Failover Cable	422
Configuring and Enabling Failover	423
Monitoring Failover	430
Failing Back	432
Disabling Failover	433
LAN-Based Failover	434
Configuring and Enabling Failover	434
Monitoring Failover	440
Failing Back	443
Disabling Failover	443
Summary	444
Solutions Fast Track	444
Frequently Asked Questions	446
Chapter 9 PIX Device Manager	449
Introduction	450
Features, Limitations, and Requirements	450
Supported PIX Firewall Hardware and Software Versions	451
PIX Device Requirements	451
Requirements for a Host Running the PIX Device Management Client	452
PIX Device Manager Limitations	454
Installing, Configuring, and Launching PDM	455
Preparing for Installation	455
Installing or Upgrading PDM	455
Obtaining a DES Activation Key	456
Configuring the PIX Firewall For Network Connectivity	457
Installing a TFTP Server	457
Upgrading the PIX Firewall and Configuring the DES Activation Key	458
Installing or Upgrading PDM on the PIX device	458
Enabling and Disabling PDM	459
Launching PDM	460
Configuring the PIX Firewall Using PDM	466
Using the Startup Wizard	467

Configuring System Properties	474
The Interfaces Category	475
The Failover Category	476
The Routing Category	478
The DHCP Server Category	480
The PIX Administration Category	481
The Logging Category	490
The AAA Category	491
The URL Filtering Category	492
The Auto Update Category	494
The Intrusion Detection Category	495
The Advanced Category	497
The Multicast Category	498
The History Metrics Category	499
Maintaining Hosts and Networks	500
Configuring Translation Rules	505
Configuring Access Rules	512
Access Rules	513
AAA Rules	517
Filter Rules	518
Configuring VPN	519
Configuring a Site-to-Site VPN	521
Configuring for the Cisco Software VPN Client	525
Monitoring the PIX Firewall Using PDM	532
Sessions and Statistics	534
Graphs	537
VPN Connection Graphs	539
System Graphs	540
Connection Graphs	541
Miscellaneous Graphs	543
Interface Graphs	544
Monitoring and Disconnecting Sessions	547
Summary	548
Solutions Fast Track	549
Frequently Asked Questions	551

Chapter 10 Troubleshooting and Performance Monitoring	553
Introduction	554
Troubleshooting Hardware and Cabling	555
Troubleshooting PIX Hardware	556
Troubleshooting PIX Cabling	567
Troubleshooting Connectivity	570
Checking Addressing	571
Checking Routing	573
Checking Translation	580
Checking Access	583
Troubleshooting IPsec	588
IKE	591
IPsec	594
Capturing Traffic	597
Displaying Captured Traffic	599
Display on the Console	599
Display to a Web Browser	600
Downloading Captured Traffic	600
Monitoring and Troubleshooting Performance	602
CPU Performance Monitoring	604
The show cpu usage Command	605
The show processes Command	606
The show perfinon Command	608
Memory Performance Monitoring	609
The show memory Command	609
The show xlate Command	610
The show conn Command	610
The show block Command	610
Network Performance Monitoring	611
The show interface Command	611
The show traffic Command	612
Identification (IDENT) Protocol and PIX Performance	613
Summary	614
Solutions Fast Track	615
Frequently Asked Questions	617
Index	619