CONTENTS

Acknowledgments xv
Introduction xvii

Part I Introduction to Firewalls and Cisco Hardware Solutions

❖ 1 **Firewall Basics 3**
Overview of Firewalls 4
What is a Firewall? 4
Choosing a Firewall 5
Firewall Components 6
Firewall Management 9
Controlling Traffic 9
OSI Reference Model 10
Firewall Layers 11
Types of Firewalls 11
Packet Filtering Firewalls 11
Functions of a Packet Filtering Firewall 12
Advantages of Packet Filtering Firewalls 12
Disadvantages of Packet Filtering Firewalls 14
Stateful Firewalls 15
Functions of a Stateful Firewall 15
Connection State Table 19
Packet Filtering Firewall Solution 20
Advantages of a Stateful Firewall 20
Disadvantages of a Stateful Firewall 20

Application Gateways (Proxy Firewalls) 20
Authentication Methods 21
Types of Application Gateway Firewalls 23
Address Translation Firewalls 27
Address Depletion 27
Address Translation Types 28
Address Translation Firewalls and Security 33
Advantages of Address Translation 34
Disadvantages of Address Translation 34
Host-Based Firewalls 35
Host-Based Firewall Abilities 35
Advantages of Host-Based Firewalls 35
Disadvantages of Host-Based Firewalls 36
Hybrid Firewalls 37
Firewall Design 37
Basic Guidelines 37
Segmentation and the DMZ 39
Placement of Firewall Components 43
Further Study 45
Web Sites 45

❖ 2 **PIX Firewall Family 47**

PIX Features 48
Finesse Operating System 48
Adaptive Security Algorithm 50
Sequence Number Randomization 53
Cut-Through Proxy 54
Policy Implementation 56
Fault Tolerance 58
PIX FOS 6.2 59
PIX Hardware 60
PIX Licensing 60
PIX 501 63
PIX 506 65
PIX 515 68
PIX 525 72
PIX 535 74
Comparison of PIX Models 77
Further Study 77
Web Sites 77

Part II PIX Setup and Traffic Filtering

❖ 3 **The PIX Command-Line Interface and Basic Configuration 81**

Access to the PIX 82
Console Access 82
Other Access Methods 83
Command-Line Interface 83
PIX Bootup Sequence 84
CLI Modes 86
Cisco IOS Router and PIX CLI Comparison 89
Setup Script Utility 92
Configuration Files 93
The configure Commands 94
The write Commands 94
Basic PIX Configuration Commands 95
Configuring the Passwords 95
Configuring the Interface 96
Configuring Routing 101
Management Commands 103
Configuring Host and Domain Names 104
Permitting IP Access to the PIX 104
Testing Connections 107
Viewing PIX Information 109
PIX Characteristics 109
Available Memory 110
Processes Running on the PIX 110
Network Configuration Example 111
Further Study 112
Web Sites 112

❖ 4 **Traffic Flow Through the PIX and Address Translation 113**

Protocol Overview 114
Overview of TCP 114
Overview of UDP 115
Translations and Connections 117
Translations 118
Connections 118
Address Translation 119
Private Addresses 119
Network Address Translation 119
Examples of Address Translation 122

Configuring Your PIX for Inside-to-Outside Access 131
  Defining the Address Pool 131
  Defining the Addresses to Translate 133
  Verifying Address Translation 137
  Address Translation Examples 138
Traffic Entering Your Network 142
  Setting Up Address Translations 142
  Allowing Traffic from Lower-Level to Higher-Level Interfaces 153
  Examples of Using Statics and Conduits 156
Viewing the PIX's Translations and Connections 158
  Viewing Active Translations 158
  Clearing the Xlate Table 160
  Viewing the Connection Table 160
Further Study 162
  Web Sites 162

❖ 5 **Filtering Traffic with Outbound Filters and Access-Lists 163**

Filtering Outbound Traffic 164
  Overview of Outbound Filters 164
  Configuring Outbound Filters 164
  Outbound Filter Processing on the PIX 166
  Examples of Filtering with Outbound Filters 167
ACLs and the PIX 172
  Comparing ACLs and Conduits/Outbound Filters 172
  Configuring and Activating ACLs 173
  ACL Configuration Examples 176
  TurboACLs 189
Object Grouping 191
  Advantages of Object Groups 192
  Syntax for Grouping Objects 192
  Object Groups for Networks 194
  Object Groups for Protocols 194
  Object Groups for Services 194
  Object Groups for ICMP Messages 195
  Examining Your Object Groups 195
  Deleting Object Groups 196
  Using Object Groups with ACLs 196
ICMP Traffic and the PIX 198
  ICMP Traffic Through the PIX 198
  ICMP Traffic Directed at the PIX 199
Further Study 201
  Web Sites 201

Part III Advanced PIX Features

❖ 6 **Web Traffic Filtering** **205**
HTTP Traffic 206
Filtering Java Applets and ActiveX Scripts 207
Configuring Java Filters 207
Configuring ActiveX Filters 209
Filtering Web Content 209
Web Filtering Process 210
Configuring Web Filtering 212
URL Filtering Example 217
Further Study 218
Web Sites 218

❖ 7 **Protocol Fixup Feature** **219**
Issues with Protocols and Applications 220
Port Numbering Issues 220
Address Translation Issues 222
Established Connections 224
Syntax of the established Command 225
Simple Example of the established Command 226
Application Inspection 226
Functions of Application Inspection 227
Limitations of Application Inspection 231
Application Inspection Configuration 232
Basic Command Syntax 232
Adding, Changing, and Removing Port Numbers 233
Verifying Your Configuration 234
Application Inspection for FTP 234
Mechanics of FTP Connections 234
Command Syntax for Application Inspection of FTP 237
Application Inspection for RSH 238
Mechanics of RSH Connections 239
Command Syntax for Application Inspection of RSH 240
Application Inspection for Skinny 240
Mechanics of Skinny Connections 241
Issues with Skinny 242
Command Syntax for Application Inspection of Skinny 243
Application Inspection for SIP 243
Mechanics of SIP Connections 244
Issues with SIP 245
Command Syntax for Application Inspection of SIP 246

Application Inspection for Multimedia Using RTSP 247
Mechanics of RTSP Connections 247
Issues with RTSP 252
Command Syntax for Application Inspection of RTSP 253
Application Inspection for H.323 253
H.323 Overview 253
Mechanics of H.323 Connections 255
CU-SeeMe 262
Netshow 263
VDOLive 264
Command Syntax for Application Inspection of H.323 . . . 264
Further Study 265
Web Sites 265

❖ 8 **Attack Guards, IDS Features, and Spoofing Protection 267**

Attack Guard Features 268
DNS Guard 269
Mail Guard 270
Flood Guard 273
Fragmentation Guard 277
Intrusion Detection System (IDS) 278
Definition of IDS 278
IDS Signatures 280
Signature Classes 282
Signature Categories and Types 283
The PIX and IDS 284
Configuring IDS on your PIX Firewall 285
Spoofing Protection 288
Spoofing Example 288
Spoofing Protection Feature of the PIX 289
Configuring Spoofing Protection 290
Spoofing Protection Configuration Example 291
Further Study 292
Books 292
Web Sites 292

Part IV **PIX Management**

❖ 9 **PIX Device Manager 295**

PDM Overview 296
Requirements for PDM 296
PIX Requirements 296
Desktop Requirements 297

Preparing to Use PDM 298
Accessing PDM 299
Using PDM 300
Wizards 301
Configuration Tabs 301
Further Study 308
Web Sites 308

❖ 10 **SNMP and Logging 309**
SNMP 310
SNMP MIBs 310
SNMP Traps 312
SNMP Configuration 313
SNMP Configuration Example 315
Date and Time 316
Setting the Date and Time on the PIX 316
Using NTP 319
Logging Events 325
Supported Transport Protocols for Syslog 325
Message Categories 325
Configuring Logging 326
Further Study 330
Web Sites 330

❖ 11 **Centralizing Security 333**
Centralizing Security 334
AAA 335
Security Protocols 335
Server and Authentication Configuration 336
Shell Access 337
Authenticating Shell Access *337*
Using Command Authorization 339
Cut-Through Proxy 341
Cut-Through Proxy Process 341
Cut-Through Proxy Authentication 342
Cut-Through Proxy Authorization 344
Other Types of Traffic 345
Using Virtual Telnet 346
Using Virtual HTTP 347
Authorizing Virtual Telnet and HTTP Connections 348
Changing Authentication Parameters 349
Limiting Proxy Connections 349
Authentication Prompts 349
Authentication Timeouts 350

Configuring Accounting 351
Testing and Troubleshooting AAA 352
Further Study 353
Web Sites 353

❖ 12 **PIX Failover** **355**

Failover Overview 356
Failover Requirements 357
Types of Failover Configurations 359
Synchronizing Information Between PIXs 363
Failover Communication Between the PIXs 365
Detecting Failures 366
When Failover Occurs 370
Initial Bootup 372
Failover Configuration 372
Command Overview 372
Verifying Failover Configuration 374
Example Configurations 382
Cable-Based Failover Configuration 382
LAN-Based Failover Configuration 387
Further Study 396
Web Sites 396

❖ 13 **Password Recovery Procedure** **397**

Password Recovery Overview 398
When to Use the Password Recovery Procedure 398
Approaches 399
Password Recovery for PIXs without a Floppy Drive 400
Password Recovery Requirements 400
Accessing Monitor Mode 401
Configuring Your PIX in Monitor Mode 402
Password Recovery Process 404
Password Recovery for PIXs with a Floppy Drive 405
Password Recovery Example 405
Further Study 407
Web Sites 407

❖ 14 **Upgrading Your PIX Firewall** **409**

Upgrading Your PIX 410
Upgrading Your FOS 410
FOS Version 5.0 and Earlier 411
FOS Version 5.1 and Later 417
Upgrading Failover Configurations 420
Downgrading Your FOS 421

Auto Update Feature 422
Configuring Auto Update 422
Verifying Auto Update 424
Entering an Activation Key 425
FOS 6.1 and Earlier 425
FOS 6.2 and Later 426
Further Study 429
Web Sites 429

❖ 15 **SOHO Environments: DHCP and PPPoE 431**
DHCP 432
Assignable Attributes 432
Using the PIX as a DHCP Server 432
Using the PIX as a DHCP Client 437
DHCP Autoconfiguration 438
PPPoE 440
Overview of PPPoE 440
PPPoE on the PIX 440
Further Study 443
Web Sites 443

Part V VPNs and the PIX Firewall

❖ 16 **IPSec Overview 447**
VPN Overview 448
Functions of a VPN 448
Encapsulation Methods 450
IPSec Overview 451
Functions of IPSec 452
Main Components of IPSec 452
Keys 452
Integrity with Hashing Functions 455
Authentication with Digital Signatures 455
Methods of IPSec Data Protection 460
Authentication Header 460
Encapsulation Security Payload 462
Setting Up an IPSec VPN Connection 464
Gathering Information 464
Steps For Setting Up an IPSec Connection 465
ISAKMP and IKE 466
Overview of the Connection Setup Process 470
Further Study 472
Web Sites 472

❖ 17 **IPSec Configuration** **473**
Preparing for IPSec Connections 474
Preparation Steps 474
Allowing IPSec Traffic into Your Network 474
Site-to-Site Connections 475
Configuring Authentication 476
Configuring IKE Phase 1 482
Configuring IKE Phase 2 484
Troubleshooting IPSec Connections 491
Example Pre-Shared Key Configuration 494
Example CA Configuration 496
Remote Access Connections 497
Dynamic Crypto Maps 498
Assigning IP Addresses to Remote Peers 501
User Authentication with XAUTH 505
Cisco VPN 3000 Client Configuration 507
The PIX as a Remote Access Client 511
Further Study 514
Web Sites 514

❖ **Index** **515**