

**4 FREE BOOKLETS**

YOUR SOLUTIONS MEMBERSHIP



# Cisco PIX Firewalls

Configure, Manage, & Troubleshoot

**#1 Best-Selling PIX Book**

**Completely Updated for Cisco PIX Version 7.0**

- Master Robust IPsec VPN Services, Firewall Services Module, High-Availability Services, Management Center, and Much More
- Ease Your Migration to 7.0 with the Bonus, Downloadable, 600-Page E-book Covering PIX Software 6.x
- Perfect Study Tool for Cisco Secure PIX Firewall Advanced Exam

**Thorsten Behrens**

**Brian Browne**

**Ido Dubrawsky**

**Umer Khan**

**Daniel Kligerman**

**Michael Sweeney**

**Charles Riley** Technical Editor

# Register for Free Membership to

**s o l u t i o n s @ s y n g r e s s . c o m**

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2004*, Brian Caswell and Jay Beale's *Snort 2.1 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real-time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy-to-search Web page, providing you with the concise, easy-to-access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.



# Cisco PIX Firewalls

Configure, Manage, & Troubleshoot

**Thorsten Behrens**  
**Brian Browne**  
**Ido Dubrawsky**  
**Daniel Kligerman**  
**Michael Sweeney**

**Charles Riley** Technical Editor  
**Umer Khan** Technical Reviewer

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively iMakersî) of this book (ithe Workî) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®”, “Ask the Author UPDATE®”, and “Hack Proofing®”, are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library™”, “Mission Critical™”, and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

#### **KEY SERIAL NUMBER**

001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	GHFDDD5638
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

#### **PUBLISHED BY**

Syngress Publishing, Inc.  
800 Hingham Street  
Rockland, MA 02370

#### **Cisco PIX Firewalls: Configure, Manage, & Troubleshoot**

Copyright © 2005 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-59749-004-0

EDT: 000231

Publisher: Andrew Williams

Acquisitions Editor: Gary Byrne

Technical Editor: Charles Riley

Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien

Copy Editor: Adrienne Rebello and  
Beth Roberts

Indexer: Julie Kawabata

Distributed by O'Reilly Media, Inc. in the United States and Canada.

For information on rights and translations, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email [matt@syngress.com](mailto:matt@syngress.com) or fax to 781-681-3585.



# Acknowledgments

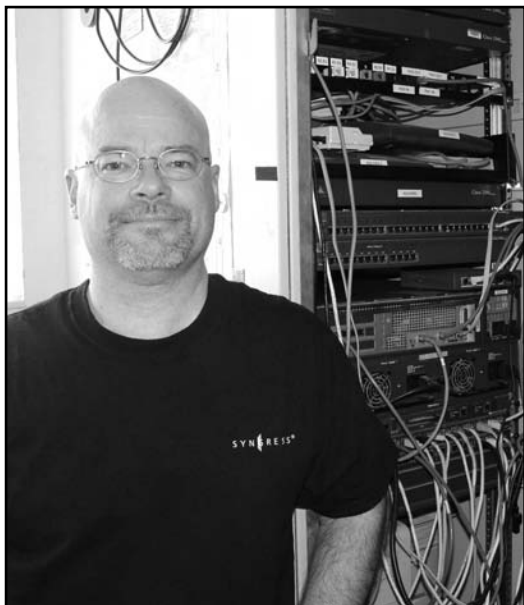
Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, Rob Bullington, and Aileen Berg.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.



Coauthor Mike Sweeney in his  
DWC'd-out Test Lab.

We would not have been able to publish this book without the professional, prompt, and friendly service provided by the great people at Duane Whitlow & Co., Inc., which provided the rented Cisco equipment that we used to write this book. As we tested the PIX 7.0 beta, we needed fast delivery of multiple boxes with very specific configurations for use in our test lab. All of the folks at DWC made sure that we had exactly what we needed, when we needed it, and where we needed it. No problems. No hassles. We would like to extend a special thank you to Duane, Conrad, and the rest of the DWC team.

—Syngress Publishing

---

## DUANE WHITLOW & Co., Inc.

Since 1977, Duane Whitlow & Co. Inc. has specialized in providing both new and used IBM and plug-compatible computer equipment to computer users worldwide. In these ever-changing times, recent focus has centered on buy, sell, lease, and short-term rental of used Cisco System networking equipment.

Meeting specific needs using multiple platforms and systems integration is our specialty. For example: Short-term rentals of Cisco System Products for corporate customers, training companies and students studying for their Cisco Certification are unique programs from DWC that are specifically designed for those special needs.

**Duane Whitlow & Co., Inc.**

**[www.dwc-computer.com](http://www.dwc-computer.com)**

**4950 Keller Springs Rd., Ste 415**

**Addison, TX 75001**

**Phone 800/977-7473 or 972/931-3001 Fax 972/931-3340**

**email: [duane@dwc-computer.com](mailto:duane@dwc-computer.com) or**

**[conrad@dwc-computer.com](mailto:conrad@dwc-computer.com)**

# Technical Editor and Foreword Contributor



**Charles Riley**, along with Methuselah, has spent some time specializing in networking and security. He remembers reverse engineering Basic code to enlarge the ship in Canyon Cruiser on the Commodore 64, causing its wings to scrape the pixilated walls. Shortly afterward, he was forced to resign from the middle school computer club. Had there been appropriate security in place at the time, life might have taken a different turn.

The career of Charles spans decades, starting as a young cowherd at the tender age of 6. At less than 4 feet tall, and while other children were watching *Captain Kangaroo*, Charles was herding several tons of walking, unpredictable beef into a large barn. From there, it was a logical transition to herding packets through a network, and sheltering them behind a firewall.

Charles has coauthored and edited several books, including *Routing and Configuring Cisco Voice over IP, Second Edition*, and *The Best Damn Cisco Internetworking Book Period* (Syngress Publishing, ISBN: 1-931836-91-4). He has designed and implemented robust networking solutions for large Fortune 500 and privately held companies. Charles started as an U.S. Army telecommunications specialist at Fort Huachuca, Arizona, eventually finishing his Army career as the network manager of the 7th Army Training Command in Grafenwoehr, Germany. Charles graduated from the University of Central Florida in 1989.

He'd like express his gratitude and love to his beloved wife, Rene'. Her belief and love lifted him to greater heights than he ever thought possible. Rene' first saw the writer in the cowherd, and then proceeded to make everything wonderful. To his daughter, Tess, who has the potential to soar so high; he is eagerly looking forward to seeing you do so. He wishes to thank you both for the time and support.



# Contributing Authors



**Michael Sweeney** (CCNA, CCDA, CCNP, MCSE, SCP) is the owner of the Network Security consulting firm Packetattack.com. Packetattack.com specialties are network design and troubleshooting, wireless network design, security, and analysis. The Packetattack team uses such industry standard tools as NAI Sniffer, AiroPeekNX, and Airmagnet. Packetattack.com also provides digital forensic analysis services.

Michael has been a contributing author for Syngress for the books *Cisco Security Specialist Guide to PIX Firewalls*, ISBN: 1-931836-63-9; *Cisco Security Specialist Guide to Secure Intrusion Detection Systems*, ISBN: 1-932266-69-0; and *Building DMZs For Enterprise Networks*, ISBN: 1-931836-88-4. Through PacketPress, Michael has also published *Securing Your Network Using Linux*, ISBN: 1-411621-77-8.

Michael graduated from the University of California, Irvine, extension program with a certificate in communications and network engineering. Michael currently resides in Orange, CA, with his wife, Jeanne, and daughters, Amanda and Sara.



**Brian Browne** (CISSP) is the Principal Consultant with Edoxa, Inc., and provides both strategic and technical information security consulting. He has 14 years of experience in the field of information security and is skilled in all phases, from security management through hands-on implementation. His specific security experience includes Sarbanes-Oxley and HIPAA gap analysis and remediation, vulnerability assessments, network security, firewall architecture, virtual private networks (VPN), UNIX security, Windows Active Directory security, and public key infrastructure (PKI). He also

conducts application performance assessments and network capacity planning using Opnet IT Guru. Brian resides in Willow Grove, PA, with his wife, Lisa and daughter, Marisa.



**Daniel Kligerman** (B.Sc, CCSE, CCIE #13999) is the Manager of the Data Diagnostic Centre at TELUS National Systems, responsible for the support and management of enterprise customers' data and VoIP networks. Daniel was the technical editor of *Check Point Next Generation with Application Intelligence Security Administration* (Syngress, ISBN: 1-932266-89-5) and the contributing author of *Building DMZs for Enterprise Networks* (Syngress, ISBN: 1-931836-88-4), *Check Point NG VPN-1/Firewall-1 Advanced Configuration and Troubleshooting* (Syngress, ISBN: 1-931836-97-3), *Nokia Network Security Solutions Handbook* (Syngress, ISBN: 1-931836-70-1), and *Check Point Next Generation Security Administration* (Syngress, ISBN: 1-928994-74-1). He resides in Toronto, Canada, with his wife, Merita.

**Thorsten Behrens** (CCMSE, CCSE+, CCNA, CNE) is a Senior Security Engineer with Integralis' Managed Security Services Team. Thorsten's specialties include Check Point FireWall-1, Cisco PIX, and ISS RealSecure. Thorsten is a German national who delights his neighbors in Springfield, MA, with bagpipe practice sessions.



**Ido Dubrawsky** (CCNA, CCDA, SCSA, CISSP) is a Senior Security Consultant with SBC's Callisma consulting practice. Previously, Ido was a Network Security Architect working in the SAFE architecture group of Cisco Systems, Inc. His responsibilities include research into network security design and implementation. Previously, Ido was a member of Cisco's Secure Consulting Services in Austin, TX, where he conducted security posture assessments and penetration tests for clients as well as provided technical consulting for security design reviews. Ido was one of the codevelopers of

the Secure Consulting Services wireless network assessment toolset. His strengths include Cisco routers and switches, PIX firewalls, the Cisco Intrusion Detection System, and the Solaris operating system. His specific interests are in

vulnerability assessments, penetration testing, freeware detection systems, and network performance monitoring. Ido holds bachelor's and master's degrees from the University of Texas at Austin in Aerospace Engineering and is a long-time member of USENIX and SAGE. He has written numerous articles covering Solaris security and network security for Sysadmin as well as the online SecurityFocus. He is a contributor to *Hack Proofing Sun Solaris 8* (Syngress Publishing, ISBN: 1-928994-44-X) and *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9). He currently resides in Silver Spring, MD, with his family.



## Technical Reviewer and Contributor

**Umer Khan** (CCIE #7410, MCSE, SCSA, SCNA, CCA, SCE, CNX) is the Manager of Networking, Telecommunications, and Windows Infrastructure at Broadcom Corporation ([www.broadcom.com](http://www.broadcom.com)), where he enjoys the challenging and fast-paced IT environment. Umer's teams are responsible for the design, implementation, and support of a broad range of Broadcom's global IT infrastructure, some of which include LAN, MAN, WAN, 802.11 wireless, PBX, VoIP, VPN, firewall, cellular, Windows server, Active Directory, Citrix, Microsoft Exchange, SQL, IIS, Biztalk, VMware, authentication, content load balancing, caching, audio/video conferencing, and audio/video distribution technologies.

Umer has contributed toward several publications, including the *Sun Certified System Administrator for Solaris 8 Study Guide* (ISBN: 007-212369-9) and *Sniffer Pro: Network Optimization and Troubleshooting Handbook* (Syngress, ISBN: 1-93-183657-4). He was also the technical editor for *Cisco Security Specialist's Guide to PIX Firewalls* (Syngress, ISBN: 1-931836-63-9). Umer completed his bachelor's in computer engineering at Illinois Institute of Technology. His personal Web site is located at [www.umer-khan.net](http://www.umer-khan.net).

# Contents

<b>Foreword</b> .....	<b>xxv</b>
<b>Chapter 1 Introduction to Security and Firewalls</b> .....	<b>1</b>
Introduction .....	2
The Importance of Security .....	2
What Is Information Security? .....	2
The Early Days of Information Security .....	4
Insecurity and the Internet .....	4
The Threats Grow .....	5
Attacks .....	6
Creating a Security Policy .....	8
Cisco's Security Wheel .....	10
Securing the Environment .....	11
Monitoring Activity .....	13
Testing Security .....	13
Improving Security .....	15
Firewall Concepts .....	15
What Is a Firewall? .....	16
Types of Firewalls .....	18
Packet Filters .....	18
Stateful Inspection Packet Filters .....	19
Application Proxies .....	20
Inbound and Outbound .....	21
Firewall Interfaces: Inside, Outside, and DMZ .....	22
Firewall Policies .....	24
Address Translation .....	25
Static Translation .....	26
Dynamic Translation .....	27
Port Address Translation .....	28

Virtual Private Networking . . . . .	28
Cisco Security Certifications . . . . .	30
Cisco Firewall Specialist . . . . .	30
Requirements . . . . .	30
Cisco Certified Security Professional . . . . .	31
Requirements . . . . .	31
Cisco Certified Internetwork Expert Security . . . . .	32
The Qualification (Written) Exam . . . . .	32
The Lab Exam . . . . .	32
The CSPFA Exam . . . . .	34
Exam Objectives . . . . .	34
Summary . . . . .	37
Solutions Fast Track . . . . .	37
Frequently Asked Questions . . . . .	39
<b>Chapter 2 Introduction to PIX Firewalls . . . . .</b>	<b>41</b>
Introduction . . . . .	42
Cisco PIX Version 7.0 . . . . .	42
Major Changes to Cisco PIX 7.0 . . . . .	43
What's New in PIX 7.0? . . . . .	44
Commands New to 7.0 . . . . .	44
Modified Commands . . . . .	45
What Commands Do We Bid Farewell To? . . . . .	45
PIX Firewall Features . . . . .	45
Embedded Operating System . . . . .	46
The Adaptive Security Algorithm . . . . .	46
State . . . . .	48
Security Levels . . . . .	50
How ASA Works . . . . .	50
Technical Details for ASA . . . . .	51
User Datagram Protocol . . . . .	55
Advanced Protocol Handling . . . . .	56
VPN Support . . . . .	57
URL Filtering . . . . .	58
Address Translation . . . . .	58
High Availability . . . . .	58
PIX Hardware . . . . .	59

Models .....	59
PIX 501 .....	61
PIX 506E .....	61
PIX 515E .....	62
PIX 525 .....	62
PIX 535 .....	63
Cisco Firewall Services Module .....	63
Software Licensing and Upgrades .....	63
Licensing .....	64
Upgrading Software .....	66
Preliminary Upgrade to 6.3 .....	67
Upgrade from 6.3 to 7.0 Code .....	69
Downgrading from 7.0 to 6.3 .....	74
Management Access .....	75
Console Port .....	75
USB .....	77
Telnet .....	77
SSH .....	77
Web .....	77
Password Recovery .....	78
Command-Line Interface .....	80
Administrative Access Modes .....	80
Basic Commands .....	83
Hostname and Domain Name .....	84
Configuring Interfaces .....	85
The interface Command .....	85
The nameif Command .....	86
The security-level Command .....	86
The ip address Command .....	86
Static Routes .....	87
Password Configuration .....	89
Basic Security (What Is Configured by Default Out of the Box) .....	90
Managing Configurations .....	90
Configuration Commands .....	90
Configure .....	90

Write . . . . .	91
Copy . . . . .	91
Show . . . . .	92
The configure Command . . . . .	94
Initializing Images . . . . .	95
Powercycle . . . . .	95
Reload . . . . .	95
Factory Default Configurations . . . . .	95
Cisco Catalyst 6500 Series Firewall Services Module . . . . .	98
IP Version 6 (IPv6) . . . . .	99
IPv4 vs. IPv6 . . . . .	99
Header Comparison . . . . .	100
IPv6 Addresses . . . . .	100
IPv6 Address Space . . . . .	102
The Fundamentals of IPv6 Addresses . . . . .	103
Summary . . . . .	106
Solutions Fast Track . . . . .	108
Frequently Asked Questions . . . . .	110

## **Chapter 3 PIX Firewall Operations . . . . .113**

Introduction . . . . .	114
Security Contexts . . . . .	115
The Bare Minimum: Outbound Traffic . . . . .	117
Configuring Dynamic Address Translation . . . . .	117
Blocking Outbound Traffic (Defining an Access List) . . . . .	122
Access Lists . . . . .	122
Opening Your Network: Allowing Inbound Traffic . . . . .	130
Static Address Translation . . . . .	130
Access Lists . . . . .	132
ICMP Access Lists . . . . .	133
Port Redirection . . . . .	135
Enabling/Disabling of ACL Entries (New) . . . . .	136
Outbound ACLs (New) . . . . .	137
Time-Based ACLs (New) . . . . .	139
NAT Control (New) . . . . .	141
Bypassing NAT . . . . .	141
Identity NAT . . . . .	142

NAT Exemption . . . . .	142
Static Identity NAT . . . . .	143
Policy NAT . . . . .	144
Object Grouping . . . . .	145
Configuring and Using Object Groups . . . . .	146
ICMP-Type Object Groups . . . . .	146
Network Object Groups . . . . .	147
Protocol Object Groups . . . . .	147
Service Object Groups . . . . .	148
TurboACLs . . . . .	149
Conduit and Outbound . . . . .	150
Case Study . . . . .	150
Summary . . . . .	156
Solutions Fast Track . . . . .	158
Frequently Asked Questions . . . . .	159
<b>Chapter 4 Adaptive Security Device Manager . . . . .</b>	<b>161</b>
Introduction . . . . .	162
Features, Limitations, and Requirements . . . . .	162
Supported PIX Firewall Hardware and Software Versions	163
PIX Device Requirements . . . . .	163
Host Requirements for Running ASDM . . . . .	164
Adaptive Security Device Manager Limitations . . . . .	164
Unsupported Commands . . . . .	164
Unsupported Characters . . . . .	165
ASDM CLI Does Not Support Interactive	
Commands . . . . .	165
Printing from ASDM . . . . .	166
Installing, Configuring, and Launching ASDM . . . . .	166
Preparing for Installation . . . . .	166
Installing or Upgrading ASDM . . . . .	167
Obtaining a DES Activation Key . . . . .	167
Configuring the PIX Firewall for Network	
Connectivity . . . . .	168
Installing a TFTP Server . . . . .	168
Upgrading the PIX Firewall and Configuring	
the DES Activation Key . . . . .	168



Installing or Upgrading ASDM on the PIX Device	169
Enabling and Disabling ASDM	170
Launching ASDM	171
Configuring the PIX Firewall Using ASDM	182
Using the Startup Wizard	182
Configuring System Properties	187
The AAA Menu	189
The Advanced Menu	191
The ARP Static Table Menu	195
The Auto Update Menu	195
The DHCP Services Menu	196
The DNS Client Menu	198
The Failover Menu	199
The History Metrics Category	201
The IP Audit Menu	201
The Logging Menu	203
The Priority Queue Category	207
The SSL Category	208
The SunRPC Server Category	208
The URL Filtering Category	208
Configuring VPNs Using ASDM	210
Configuring a Site-to-Site VPN Using ASDM	210
Configuring a Remote Access VPN Using ASDM	216
Summary	225
Solutions Fast Track	226
Frequently Asked Questions	227
<b>Chapter 5 Application Inspection</b>	<b>229</b>
New Features in PIX 7.0	230
Supporting and Securing Protocols	230
TCP, UDP, ICMP, and the PIX Firewall	231
Application Layer Protocol Inspection	234
Defining a Traffic Class	235
Associating a Traffic Class with an Action	239
Customizing Application Inspection Parameters	240
Applying Inspection to an Interface	240

Domain Name Service .....	240
Remote Procedure Call .....	241
SQL*Net .....	243
Internet Locator Service and Lightweight Directory Access Protocol .....	244
HTTP Inspection .....	245
FTP Inspection .....	246
Active versus Passive Mode .....	246
ESMTP Inspection .....	249
ICMP Inspection .....	250
H.323 .....	250
Simple Network Management Protocol (SNMP) ..	251
Voice and Video Protocols .....	252
SIP .....	252
CTIQBE .....	252
SCCP .....	253
Real-Time Streaming Protocol (RTSP), NetShow, and VDO Live .....	253
Summary .....	254
Solutions Fast Track .....	255
Frequently Asked Questions .....	256
<b>Chapter 6 Filtering, Intrusion Detection, and Attack Management .....</b>	<b>259</b>
Introduction .....	260
Filtering Web and FTP Traffic .....	260
Filtering URLs .....	260
Websense and Sentian by N2H2 .....	261
Fine-Tuning and Monitoring the Filtering Process ..	262
Configuring HTTP URL Filtering .....	266
Configuring HTTPS Filtering .....	267
Setting Up FTP Filtering .....	267
Active Code Filtering .....	268
Filtering Java Applets .....	269
Filtering ActiveX Objects .....	270
Virus Filtering; Spam, Adware, Malware, and Other-Ware Filtering .....	270

TCP Attack Detection and Response . . . . .	271
PIX Intrusion Detection . . . . .	273
Supported Signatures . . . . .	273
Configuring Intrusion Detection/Auditing . . . . .	276
Disabling Signatures . . . . .	278
Configuring Shunning . . . . .	279
Attack Containment and Management . . . . .	279
Placing Limits on Fragmentation . . . . .	279
SYN FloodGuard . . . . .	281
The TCP Intercept Feature . . . . .	281
Preventing IP Spoofing . . . . .	282
Other Ways the PIX Can Prevent, Contain, or	
Manage Attacks . . . . .	283
Configuring Connection Limits and Timeouts . . . . .	283
Preventing MAC Address Spoofing . . . . .	284
Summary . . . . .	286
Solutions Fast Track . . . . .	286
Frequently Asked Questions . . . . .	288
<b>Chapter 7 Services . . . . .</b>	<b>289</b>
Introduction . . . . .	290
DHCP Functionality . . . . .	290
DHCP Servers . . . . .	290
Cisco IP Phone-Related Options . . . . .	292
DHCP Relay . . . . .	293
DHCP Clients . . . . .	293
PPPoE . . . . .	294
EasyVPN . . . . .	297
EasyVPN Server . . . . .	297
Routing and the PIX Firewall . . . . .	298
Unicast Routing . . . . .	298
Static Routes . . . . .	299
RIP . . . . .	300
OSPF . . . . .	301
Network Address Translation as a Routing Mechanism	302
Multicast Routing . . . . .	302
Stub Multicast Routing . . . . .	303

PIM Multicast Routing .....	304
BGP through PIX Firewall .....	304
Queuing and Policing .....	305
Summary .....	306
Solutions Fast Track .....	306
Frequently Asked Questions .....	308

## **Chapter 8 Configuring Authentication, Authorization, and Accounting .....309**

Introduction .....	310
New and Changed Commands in 7.0 .....	310
Introducing AAA Concepts .....	311
Authentication .....	314
Authorization .....	315
Accounting .....	315
AAA Security Protocols .....	315
RADIUS .....	315
How RADIUS Works .....	316
TACACS+ .....	318
How TACACS+ Works .....	319
Optional Security Protocols and Methods .....	321
AAA Servers .....	322
Configuring Console Authentication .....	322
Configuring Local Authentication .....	323
Configuring Local AAA Using the ASDM .....	326
Configuring Command Authorization .....	326
Configuring Local Command Authorization .....	328
Configuring TACACS+ and RADIUS Console Authentication .....	329
Configuring TACACS+ Command Authorization ...	333
Configuring Authentication for Traffic through the Firewall	337
Configuring Cut-through Proxy .....	337
Virtual HTTP .....	340
Virtual Telnet .....	342
Configuring Authorization for Traffic through the Firewall	343
Configuring Accounting for Traffic through the Firewall ..	344
Summary .....	346

Solutions Fast Track .....347

Frequently Asked Questions .....349

**Chapter 9 PIX Firewall Management .....351**

    Introduction .....352

    Configuring Logging .....352

        Logging Levels .....353

        Dropped and Changed Syslog Messages from 6.x .....354

        Logging Facility .....362

        Local Logging .....363

            Buffered Logging .....363

            Console Logging .....364

            Terminal Logging .....364

        Remote Logging via Syslog .....365

        Disabling Specific Syslog Messages .....370

    Configuring Remote Access .....371

        Secure Shell .....372

            Enabling SSH Access .....372

            Troubleshooting SSH .....377

        Telnet .....379

            Restrictions .....381

    Configuring Simple Network Management Protocol .....381

        Configuring System Identification .....382

        Configuring Polling .....383

        Configuring Traps .....385

        Managing SNMP on the PIX .....386

    Configuring System Date and Time .....387

        Setting and Verifying the Clock and Time Zone .....387

        Configuring and Verifying the Network Time Protocol .....390

            NTP Authentication .....392

        Management Using the Cisco PIX Adaptive

            Security Device Manager (ASDM) .....394

    Summary .....397

    Solutions Fast Track .....398

    Frequently Asked Questions .....399

**Chapter 10 Configuring Virtual Private Networking 401**

Introduction .....	402
What's New in PIX 7.0 .....	403
IPsec Concepts .....	403
IPsec .....	404
Internet Key Exchange .....	408
Security Associations .....	411
Certificate Authority Support .....	415
Configuring a Site-to-Site VPN .....	416
Planning .....	416
Allowing IPsec Traffic .....	418
Enabling IKE .....	418
Creating an ISAKMP Protection Suite .....	419
Defining an ISAKMP Preshared Key .....	420
Configuring Certificate Authority Support .....	420
Configuring Crypto Access-Lists .....	427
Defining a Transform Set .....	429
Bypassing Network Address Translation .....	430
Configuring a Crypto Map .....	430
Troubleshooting .....	432
Remote Access—Configuring Support for the Cisco	
Software VPN Client .....	433
Enabling IKE and Creating an ISAKMP Protection Suite	434
Defining a Transform Set .....	435
Crypto Maps .....	435
Tunnel Groups and Group Policies .....	436
Address Pool Configuration .....	436
Split Tunneling .....	437
NAT Issues .....	438
Authentication against Radius, TACACS+, SecurID, or	
Active Directory .....	438
Automatic Client Update .....	439
Configuring Client Firewall Requirements .....	439
Sample Configurations of PIX and VPN Clients .....	440
Summary .....	444
Solutions Fast Track .....	444
Frequently Asked Questions .....	446

<b>Chapter 11 Configuring Failover</b>	<b>.447</b>
Introduction	.448
Failover Concepts	.448
Failover Requirements	.448
Active/Standby and Active/Active Failover	.449
The Failover Link	.451
Stateful Failover	.452
Failure Detection	.454
Configuration Synchronization, and Command Replication	.455
IP and MAC Addresses Used	.456
Configuring and Monitoring Failover	.458
Configuring and Monitoring Cable-Based Active/Standby Failover	.458
Configuring and Monitoring LAN-Based Active/Standby Failover	.465
Configuring Cable-Based Active/Active Failover	.468
Configuring LAN-Based Active/Active Failover	.469
Advanced Failover Control and Configurations	.469
Forcing Failover	.470
Disabling Failover	.470
Failover Authentication and Encryption	.470
HTTP Replication	.471
Failure Detection Parameters	.471
Failover Preemption	.473
Summary	.473
Solutions Fast Track	.474
Frequently Asked Questions	.476
<b>Chapter 12 Troubleshooting and Performance Monitoring</b>	<b>.477</b>
Introduction	.478
Troubleshooting Hardware and Cabling	.479
Troubleshooting PIX Hardware	.480
Troubleshooting PIX Cabling	.491
Troubleshooting Connectivity	.494
Checking Addressing	.495

Checking Routing . . . . .	497
Failover Cable . . . . .	501
Checking Translation . . . . .	502
Checking Access . . . . .	505
Troubleshooting IPsec . . . . .	507
IKE . . . . .	509
IPsec . . . . .	512
Capturing Traffic . . . . .	515
Displaying Captured Traffic . . . . .	516
Display on the Console . . . . .	516
Display to a Web Browser . . . . .	517
Downloading Captured Traffic . . . . .	517
Support Options as Troubleshooting Tools . . . . .	518
Monitoring and Troubleshooting Performance . . . . .	519
CPU Performance Monitoring . . . . .	520
The show cpu usage Command . . . . .	521
The show processes Command . . . . .	521
The show perfinon Command . . . . .	523
Memory Performance Monitoring . . . . .	524
The show memory Command . . . . .	525
The show xlate Command . . . . .	525
The show conn Command . . . . .	525
The show block Command . . . . .	526
Network Performance Monitoring . . . . .	526
The show interface Command . . . . .	526
The show traffic Command . . . . .	527
Identification (IDENT) Protocol and PIX Performance . . . . .	527
Summary . . . . .	529
Solutions Fast Track . . . . .	530
Frequently Asked Questions . . . . .	531
<b>Index . . . . .</b>	<b>533</b>

**Note:** Throughout this book, *italics* or angled brackets <,> indicate specific information or values (IP addresses, port numbers, etc.) with must be filled in for your specific configuration.





# Foreword

“Always do right. This will gratify some of the people and astonish the rest.”—Mark Twain

“Always firewall. That will inconvenience some of the attackers and impede the rest.”—Charles Riley (apologies to Mr. Twain)

You hold in your hand a book that was given life to aid our fellow security professionals, our brothers and sisters in the trenches of information warfare engaged in protecting the information and networks in their charge. But you are not alone; the tools in the endless war between protectors of the information and the attackers who would own that information have advanced and improved greatly. Witness the overhaul of the PIX operating system in version 7.0, the main subject of this book.

Version 7.0 makes many improvements to the code, including adding long-desired features. Version 7.0 also gives the “Old Yeller” treatment to commands that are no longer relevant or can no longer do the job. For example, the conduit command with its awkward syntax is no more. Cisco has made the commands more like its mainstream IOS, although there are a few holdouts that mark version 7.0 as a PIX operating system. These commands are among many detailed in this book.

Each chapter has been carefully organized and developed to provide maximum coverage of version 7.0. In assembling this book, the mission of our team was to provide you, our reader, with a font of information that will allow you to master 7.0 and use it for your own purposes. The result is the 12 chapters that make up this book:

Chapter 1 Introduction to Security and Firewalls

Chapter 2 Introduction to PIX Firewalls

Chapter 3 PIX Firewall Operations

Chapter 4 Adaptive Security Device Manager

Chapter 5 Application Inspection

Chapter 6 Filtering, Intrusion Detection, and Attack Management

Chapter 7 Services

Chapter 8 Configuring Authentication, Authorization, and Accounting

Chapter 9 PIX Firewall Management

Chapter 10 Configuring Virtual Private Networking

Chapter 11 Configuring Failover

Chapter 12 Troubleshooting and Performance Monitoring

Version 7.0 introduces contexts, something that might be new to many readers.

PIX firewalls running 7.0 can run either in routed mode (where they are aware of and participate in IP routing) or in transparent mode where the firewall

silently performs its function, but is not seen as a hop in the path to a destination.

Contexts are just one of the many changes that Cisco made to version

7.0. For more, read on—and thank you for being part of the vanguard of information security.

When it comes to protecting your networks and data,

Shakespeare put it best in Henry V:

From this day to the ending of the world,  
But we in it shall be remember'd;  
We few, we happy few, we band of brothers;  
For he to-day that sheds his blood with me  
Shall be my brother; be he ne'er so vile,  
This day shall gentle his condition:  
And gentlemen in England now a-bed  
Shall think themselves accursed they were not here,  
And hold their manhoods cheap whiles any speaks

—Charles Riley  
*HoH Consultants LLC*

# Chapter 1

## Introduction to Security and Firewalls

### Solutions in this chapter:

- The Importance of Security
- Creating a Security Policy
- Cisco's Security Wheel
- Firewall Concepts
- Cisco Security Certifications

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

# Introduction

In an age where our society relies so heavily on electronic communication, the need for information security is continuously increasing. Given the value and confidential nature of the information that exists on today's networks, CIOs are investing very heavily in security. Without security, a company can suffer from theft or alteration of data, legal ramifications, and other issues that all result in monetary losses. Consequently, corporations are realizing the need to create and enforce an information security policy. Furthermore, companies are now experiencing significant pressure from external regulators and governance rules such as Sarbanes-Oxley.

In this chapter, you will learn about why information security is necessary. We also look at how and why security policies are created and how security needs to be handled as a process. We look at firewalls in general, explore the different types of firewalls available in the market, and learn basic concepts about how firewalls work. Finally, we discuss the three relevant security certifications that Cisco offers in the context of PIX firewalls: the Cisco Firewall Specialist, the Cisco Certified Security Professional (CCSP), and the Cisco Certified Internet Expert (CCIE) Security.

## The Importance of Security

Over the last couple of decades, many companies began to realize that their most valuable assets were not only their buildings or factories, but also the intellectual property and other information that flowed internally within the company, as well as outwardly to suppliers and customers. Company managers, used to dealing with risk in their business activities, started to think about what might happen if their key business information fell into the wrong hands, perhaps a competitor's. For a while, this risk was not too large, due to how and where that information was stored. *Closed systems* was the operative phrase. Key business information, for the most part, was stored on servers accessed via dumb terminals or terminal emulators and had few interconnections with other systems. Any interconnections tended to be over private leased lines to a select few locations, either internal to the company or to a trusted business partner.

However, over the last 10 years or so, the Internet has changed how businesses operate, and there has been an amazing acceleration in the interconnectedness of organizations, systems, and networks. Entire corporate networks have access to the Internet, often at multiple points. This proliferation has created risks to sensitive information and business-critical systems where they had never existed before. The importance of information security in the business environment has now been underscored, as has the need for skilled, dedicated practitioners of this specialty.

## What Is Information Security?

We have traditionally thought of security as consisting of people, sometimes with guns, watching over and guarding tangible assets such as a stack of money or a research lab. Maybe they sat at a desk and watched via closed-circuit cameras installed around the property. These