SYNGRESS®

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

SYNGRESS®

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 ìMakersî) of this book (ìthe 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.

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

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 or fax to 781-681-3585.

Acknowledgments

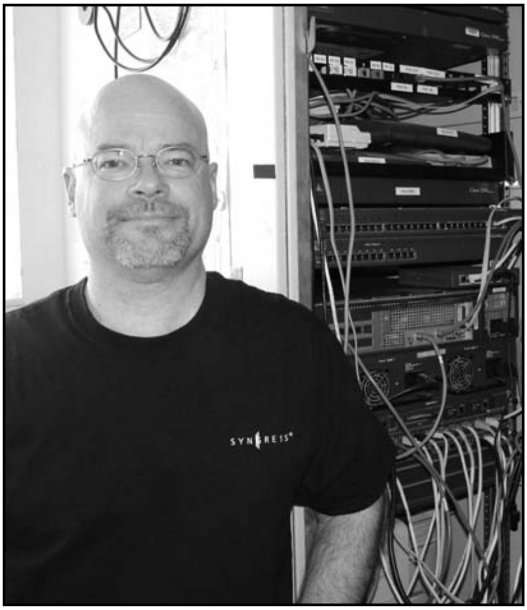
Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

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

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), 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.

Contents

Chapter 8 Configuring Authentication, Authorization, and Accounting 309

Chapter 10 Configuring Virtual Private Networking 401

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