

Internet Firewalls — *and* — **Network Security** **Second Edition**



Chris Hare

Karanjit Siyan

New Riders Publishing



Indianapolis, Indiana



INTERNET FIREWALLS AND NETWORK SECURITY, SECOND EDITION

Internet Firewalls and Network Security, Second Edition

By Chris Hare and Karanjit Siyan

Published by:
New Riders Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Copyright © 1996 by New Riders Publishing

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Library of Congress Cataloging-in-Publication Data

Hare, Chris, 1962-

Internet firewalls and network security / Chris Hare, Karanjit Siyan. -- 2nd ed.

p. cm.

Siyan's name appears first on the earlier edition.

Includes bibliographical references and index.

ISBN 1-56205-632-8

1. Computer networks--Security measures. 2. Internet (Computer network)--Security measures. I. Siyan, Karanjit, 1954- .

II. Title.

TK5105.875.I57H36 1996

005.8--dc20

96-28232

CIP

Warning and Disclaimer

This book is designed to provide information about the Internet. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author(s) and New Riders Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the disks or programs that may accompany it.

PUBLISHER *Don Fowley*

PUBLISHING MANAGER *Emmett Dulaney*

MARKETING MANAGER *Mary Foote*

MANAGING EDITOR *Carla Hall*



ABOUT THE AUTHORS

Chris Hare is a senior network security analyst for the System Security Consulting Group at Northern Telecom Ltd. (Nortel), where his activities include policy development, consulting, and secure electronic commerce. He started working in computer-based technology in 1986, after studying health sciences. Since that time he has worked in programming, system administration, quality assurance, training, network management, consulting, and technical management positions.

Chris became the first SCO-authorized instructor in Canada in 1988 and has taught Unix courses all over the world. He also has taught system administration, shell and C programming, TCP/IP, and X Windows.

As a professional writer, Chris has authored almost twenty articles for *Sys Admin* magazine and coauthored several books for New Riders Publishing, including *Inside Unix*, *Internet Firewalls and Network Security*, *Building an Internet Server with Linux*, and the *Internet Security Professional Reference*.

Chris lives in Ottawa, Canada with his wife Terri and their children Meagan and Matthew.

Karanjit Siyan, Ph.D. is president of Kinetics Corporation. He has authored international seminars on Solaris & SunOS, TCP/IP networks, PC Network Integration, Novell networks, Windows NT, and Expert Systems using Fuzzy Logic. He teaches advanced technology seminars in the United States, Canada, Europe, and the Far East. Dr. Siyan has published articles in *Dr. Dobbs Journal*, *The C Users Journal*, and *Databased Advisor*, and is actively involved in Internet research. Dr. Siyan has been involved with Unix systems programming and administration since his graduate days at the University of California at Berkeley when BSD Unix was being developed. He holds a Ph.D. in computer science, and his dissertation topic was “Fuzzy Logic and Neural Networks for Computer Network Management.” Before working as an independent consultant, Karanjit worked as a senior member of technical staff at ROLM Corporation. As part of his consulting work, Karanjit has written a number of custom compiler and operating system developmental tools. His other interests include Novell-based, Windows NT-based, and OS/2 networks. He holds an ECNE certification for Novell-based networks and Microsoft Certified Professional for Windows NT, and has written a number of books for Macmillan Computer Publishing. Karanjit Siyan is based in Montana where he lives with his wife, Dei.



TRADEMARK ACKNOWLEDGMENTS

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. New Riders Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

ACQUISITIONS EDITOR

Karen Scott

SENIOR EDITOR

Sarah Kearns

DEVELOPMENT EDITOR

Kristin Evan

PROJECT EDITOR

Lillian Duggan

COPY EDITOR

Susan Christopherson

TECHNICAL EDITOR

John Linn

ASSOCIATE MARKETING MANAGER

Tamara Apple

ACQUISITIONS COORDINATOR

Stacia Mellinger

PUBLISHER'S ASSISTANT

Karen Opal

COVER DESIGNERS

Jay Corpus, Aren Howell

BOOK DESIGNER

Sandra Schroeder

PRODUCTION MANAGER

Kelly Dobbs

PRODUCTION TEAM SUPERVISOR

Laurie Casey

GRAPHICS IMAGE SPECIALISTS

Stephen Adams, Dan Harris, Clint Lahnen, Laura Robbins

PRODUCTION ANALYSTS

*Jason Hand, Bobbi Satterfield,
SA Springer*

PRODUCTION TEAM

Angela Calvert, Kim Cofer, Terrie Deemer, Tricia Flodder, Pamela Volk, Karen Walsh

INDEXER

Erika Millen



ACKNOWLEDGMENTS

From Chris Hare

I would like to acknowledge the assistance of several people who have contributed to this second edition. To Mike Martineau of iSTAR Internet for providing an ISDN connection and some computing equipment for the Internet connection; to David Cross and Frank Rosano of Milkyway Networks for providing the Black Hole software and hardware. A special thank you to Steve Bourgeois of Milkyway Networks who answered what seemed like an endless barrage of questions and provided general all-around moral and technical support.

And to my wife Terri for her love and patience while I worked through many nights—she only had to endure the grumpy mornings.

From Karanjit Siyan

One of the more pleasurable tasks of being an author is to thank the people responsible for the success of a book. My heartfelt thanks to my wife Dei for her love and support. I wish to thank my father Ahal Sing and my mother Tejinder, my brothers Harjee and Jagjit, and my sisters Kookie and Dolly. Thanks also to Margaret Cooper Scott, Cathryn and Bob Foley, Craig and Lydia Cooper, Robert and Janie Cooper, Heidi and Steve Bynum, Barbara and Edward L. Scott (Scotty), and Jacquelyn McGregor for their love and support. Special thanks to Mother, Saint Germain, El Morya, Babaji, and Bhagwan Krishna. Without their spiritual support, this book would not have been possible.

Others who deserve credit are Bob Sanregret and Anders Amundson, who initially got me interested in writing teaching materials on computer networks. I also wish to thank the many people at Learning Tree for their help and support and permission to use some viewgraphs from the courses I have authored for them. In particular I would like to thank John Moriarty, Rick Adamson, Dr. David Collins, and Eric Garen. I wish to thank John Rutkai for his advice in selecting server components that I needed for writing this book.

I wish to acknowledge the many people who have helped me along the way: Harpreet Sandhu, Bill Duby, Angela, Michael Anaast, and Janice Culliford; my students Lisa, Debi, Sheri, Rondi, and Linda; Edward and Mary Kramer, Daniel Gottsegen, David Stanfield, Dr. Wagner, Bill Joy, Professor Ramamoorthy, Professor G. S. Sanyal, Professor “M,” Professor Kumar Subramaniam, Professor Mahabalipuram, Marti Lichtanski, Rex Cardinale, Dave Ford, mathematician D. R. Kaprekar, Mr. Gadre, Mr. Misra, and Mr. Hoffmann.

I also wish to thank the following individuals for their help in providing me with information on their firewall products: Maurius Nacht of CheckPoint Corporation; Rick Kuzuski and Bob Harvey of Internet Security Corporation for the FireWall-1 Gateway product; Robert M. Darden and Keith Ker of Trusted Information Systems, Inc. for the Gauntlet and TIS Firewall Toolkit; and Sarah Glinka of Advanced Network & Services (ANS), Inc. for the InterLock product.

Many thanks to the staff of Macmillan Computer Publishing. In particular, I wish to thank Emmett Dulaney and Jim LeValley for their encouragement throughout the development of this book. Thanks to the project editor, Lillian Duggan, for her editorial skills, and to Mary Foote, the Marketing Manager, for her patience and willingness to listen to my suggestions.

CONTENTS AT A GLANCE

<i>Introduction</i>	<i>1</i>
---------------------------	----------

PART I ❖ NETWORK SECURITY BACKGROUND

<i>1 Understanding TCP/IP</i>	<i>7</i>
<i>2 Security</i>	<i>59</i>
<i>3 Designing a Network Policy</i>	<i>97</i>
<i>4 The One-Time Password Authentication System</i>	<i>159</i>

PART II ❖ SCREENING ROUTERS AND FIREWALLS

<i>5 An Introduction to Screening Routers</i>	<i>201</i>
<i>6 Packet Filters</i>	<i>237</i>
<i>7 PC Packet Filtering</i>	<i>283</i>
<i>8 Firewall Architecture and Theory</i>	<i>325</i>
<i>9 Firewall Implementations</i>	<i>355</i>
<i>10 The TIS Firewall Toolkit</i>	<i>421</i>
<i>11 Black Hole</i>	<i>501</i>

PART III ❖ APPENDICES

<i>A List of Worksheets</i>	<i>545</i>
<i>B Sources of Information</i>	<i>547</i>
<i>C Vendor List</i>	<i>555</i>
<i>D The OPIE and Log Daemon Manual Pages</i>	<i>557</i>
<i>Index</i>	<i>585</i>



TABLE OF CONTENTS

Introduction	1
PART I ♣ NETWORK SECURITY BACKGROUND	
1 Understanding TCP/IP	7
The History of TCP/IP	8
Exploring Addresses, Subnets, and Host Names	9
<i>Address Classes</i>	10
<i>Subnets</i>	12
<i>Classless Addresses and CIDR</i>	15
<i>Host Names</i>	16
Working with Network Interfaces	18
<i>Configuration Using ifconfig</i>	19
Reviewing the Network Configuration Files	22
<i>The /etc/hosts File</i>	22
<i>The /etc/ethers File</i>	23
<i>The /etc/networks File</i>	23
<i>The etc/protocols File</i>	24
<i>The etc/services File</i>	24
<i>The etc/inetd.conf File</i>	25
Understanding the Network Access Files	26
<i>The /etc/hosts.equiv File</i>	26
<i>The .rhosts File</i>	26
<i>User and Host Equivalency</i>	27
Examining TCP/IP Daemons	28
<i>The slink Daemon</i>	28
<i>The ldsocket Daemon</i>	28
<i>The cpd Daemon</i>	29
<i>The Line Printer Daemon (lpd)</i>	29
<i>The SNMP Daemon (snmpd)</i>	29
<i>The RARP Daemon (rarpd)</i>	29
<i>The BOOTP Daemon (bootpd)</i>	30
<i>The Route Daemon (routed)</i>	30
<i>The Domain Name Server (named)</i>	31
<i>The System Logger (syslogd)</i>	31



<i>inetd—The Super-Server</i>	32
<i>The RWHO Daemon (rwhod)</i>	32
Exploring TCP/IP Utilities	32
<i>Administration Commands</i>	32
<i>User Commands</i>	48
Summary	57
2 Security	59
Examining Security Levels	60
<i>Level D1</i>	60
<i>Level C1</i>	60
<i>Level C2</i>	61
<i>Level B1</i>	62
<i>Level B2</i>	62
<i>Level B3</i>	62
<i>Level A</i>	62
Canadian Security	62
<i>Level EAL-1</i>	63
<i>Level EAL-2</i>	63
<i>Level EAL-3</i>	63
<i>Level EAL-4</i>	63
<i>Level EAL-5</i>	64
<i>Level EAL-6</i>	64
<i>Level EAL-7</i>	64
Examining Local Security Issues	64
<i>Security Policies</i>	65
<i>The Password File</i>	65
<i>The Shadow Password File</i>	67
<i>The Dialup Password File</i>	68
<i>The Group File</i>	70
Password Aging and Control	72
Vandals and Passwords	75
<i>Understanding How Vandals Break Passwords</i>	76
C2 Security and the Trusted Computing Base	78
Understanding Network Equivalency	80
<i>Host Equivalency</i>	80
<i>User Equivalency</i>	82

TABLE OF CONTENTS



Defining Users and Groups	83
Understanding Permissions	84
<i>A Review of Standard Permissions</i>	84
<i>Root and NFS</i>	87
Exploring Data Encryption Methods	87
<i>How Passwords Are Encrypted</i>	87
<i>Encrypting Files</i>	89
Examining Kerberos Authentication	90
<i>Understanding Kerberos</i>	91
<i>Disadvantages of Kerberos</i>	91
Understanding IP Spoofing	92
Summary	92
Acknowledgments	93
A Sample Program	93
3 Designing a Network Policy	97
Network Security Planning	98
Site Security Policy	98
Approach to Security Policy	99
Ensuring Responsibility for the Security Policy	102
Risk Analysis	102
Identifying Resources	106
Identifying the Threats	106
<i>Defining Unauthorized Access</i>	107
<i>Risk of Disclosure of Information</i>	107
<i>Denial of Service</i>	108
Network Use and Responsibilities	108
Identifying Who Is Allowed Use of Network Resources	109
<i>Identifying the Proper Use of a Resource</i>	109
<i>Determining Who Is Authorized to Grant Access and Approve Usage</i>	111
<i>Determining User Responsibilities</i>	116
<i>Determining the Responsibilities of System Administrators</i>	117
<i>What to Do with Sensitive Information</i>	117
Plan of Action When Security Policy Is Violated	118
<i>Response to Policy Violations</i>	118
<i>Response to Policy Violations by Local Users</i>	119
<i>Response Strategies</i>	119



<i>Defining Responsibilities of Being a Good Citizen on the Internet ...</i>	122
<i>Contacts and Responsibilities to External Organizations</i>	123
Interpreting and Publicizing the Security Policy	123
Identifying and Preventing Security Problems	124
<i>Access Points</i>	125
<i>Improperly Configured Systems</i>	127
<i>Software Bugs</i>	128
<i>Insider Threats</i>	128
<i>Physical Security</i>	128
<i>Confidentiality</i>	129
Implementing Cost-Effective Policy Controls	130
Selecting the Policy Control	130
Using Fallback Strategies	131
Detecting and Monitoring Unauthorized Activity	131
Monitoring System Use	131
Monitoring Mechanisms	132
Monitoring Schedule	133
Reporting Procedures	134
<i>Account Management Procedures</i>	134
<i>Configuration Management Procedures</i>	135
<i>Recovery Procedures</i>	136
Problem Reporting Procedures for System Administrators	139
Protecting Network Connections	139
Using Encryption to Protect the Network	140
<i>Data Encryption Standard (DES)</i>	141
<i>Crypt</i>	142
<i>Privacy Enhanced Mail (PEM)</i>	142
<i>Pretty Good Privacy</i>	142
<i>Origin Authentication</i>	143
<i>Information Integrity</i>	144
<i>Using Checksums</i>	144
<i>Cryptographic Checksums</i>	145
<i>Using Authentication Systems</i>	145
<i>Using Smart Cards</i>	146
Using Kerberos	146
Keeping Up-to-Date	146
Mailing Lists	147
<i>Uix Security Mailing Lists</i>	148
<i>The Risks Forum List</i>	148

TABLE OF CONTENTS



<i>The VIRUS-L List</i>	149
<i>The Bugtraq List</i>	149
<i>The Computer Underground Digest</i>	150
<i>The CERT Mailing List</i>	150
<i>The CERT-TOOLS Mailing List</i>	151
<i>The TCP/IP Mailing List</i>	151
<i>The SUN-NETS Mailing List</i>	151
Newsgroups	152
Security Response Teams	153
<i>Computer Emergency Response Team</i>	153
<i>DDN Security Coordination Center</i>	154
<i>NIST Computer Security Resource and Response Clearinghouse</i>	155
<i>DOE Computer Incident Advisory Capability (CIAC)</i>	156
<i>NASA Ames Computer Network Security Response Team</i>	156
Summary	157
4 The One-Time Password Authentication System	159
What Is OTP?	160
The History of OTP	162
Implementing OTP	163
<i>Deciding Which Version of OTP to Use</i>	165
<i>How S/KEY and OPIE Work</i>	166
Bellcore S/KEY Version 1.0	167
U. S. Naval Research Laboratories OPIE	168
<i>Obtaining the OPIE Source Code</i>	168
<i>Compiling the OPIE Code</i>	170
<i>Testing the Compiled Programs</i>	172
Installing OPIE	177
<i>The OPIE Components</i>	180
LogDaemon 5.0	183
<i>Obtaining the LogDaemon Code</i>	184
<i>Compiling the LogDaemon Code</i>	185
<i>Testing the Compiled Programs</i>	187
<i>Installing LogDaemon</i>	189
<i>The LogDaemon Components</i>	189
Using the S/KEY and OPIE Calculators	191
<i>Unix</i>	191
<i>Macintosh</i>	192
<i>Microsoft Windows</i>	193
<i>External Calculators</i>	193



Putting OTP into Practice	194
Security Notes Regarding /bin/login	196
Using OTP and X Windows	196
Getting More Information	197
Summary	198

PART II ❖ SCREENING ROUTERS AND FIREWALLS

5	An Introduction to Screening Routers	201
	Clarifying Definitions	202
	<i>Zones of Risk</i>	202
	<i>The OSI Reference Model and Screening Routers</i>	203
	<i>Layers of the OSI Model</i>	204
	<i>Screening Routers and Firewalls in Relationship to the</i> <i>OSI Model</i>	224
	Understanding Packet Filtering	225
	<i>Packet Filtering and Network Policy</i>	225
	<i>A Simple Model for Packet Filtering</i>	226
	<i>Packet Filter Operations</i>	227
	<i>Packet Filter Design</i>	229
	<i>Packet Filter Rules and Full Associations</i>	233
	Summary	235
6	Packet Filters	237
	Implementing Packet Filter Rules	238
	<i>Defining Access Lists</i>	238
	<i>Using Standard Access Lists</i>	239
	<i>Using Extended Access Lists</i>	240
	<i>Filtering On Incoming and Outgoing Terminal Calls</i>	243
	Examining Packet Filter Placement and Address Spoofing	244
	<i>Packet Filter Placement</i>	244
	<i>Filtering On Input and Output Ports</i>	245
	Examining Protocol-Specific Issues in Packet Filtering	248
	<i>Filtering FTP Network Traffic</i>	248
	<i>Filtering TELNET Network Traffic</i>	269
	<i>Filtering X-Windows Sessions</i>	270
	<i>Packet Filtering and the UDP Transport Protocol</i>	271
	<i>Packet Filtering ICMP</i>	273
	<i>Packet Filtering RIP</i>	274

TABLE OF CONTENTS



Example Screening Router Configurations	275
<i>Case Study 1</i>	275
<i>Case Study 2</i>	276
<i>Case Study 3</i>	278
Summary	281
7 PC Packet Filtering	283
PC-Based Packet Filter	284
<i>The KarlBridge Packet Filter</i>	284
<i>The Drawbridge Packet Filter</i>	304
Summary	322
8 Firewall Architecture and Theory	325
Examining Firewall Components	326
<i>Dual-Homed Host</i>	327
<i>Bastion Hosts</i>	335
<i>Screened Subnets</i>	349
<i>Application-Level Gateways</i>	350
Summary	354
9 Firewall Implementation	355
The TCP Wrapper	356
<i>Example 1</i>	357
<i>Example 2</i>	357
<i>Example 3</i>	358
<i>Example 4</i>	358
The FireWall-1 Gateway	358
<i>Resource Requirements for FireWall-1</i>	359
<i>Overview of FireWall-1 Architecture</i>	359
<i>FireWall-1 Control Module</i>	363
<i>Network Objects Manager</i>	364
<i>Services Manager</i>	367
<i>Rules-Base Manager</i>	368
<i>Log Viewer</i>	373
<i>Examples of FireWall-1 Applications</i>	375
<i>Performance of FireWall-1</i>	376
<i>FireWall-1 Rules Language</i>	377
<i>Obtaining Information on FireWall-1</i>	379



ANS InterLock	379
<i>Resource Requirements for InterLock</i>	381
<i>Overview of InterLock</i>	381
<i>Configuring InterLock</i>	383
<i>The InterLock ACRB</i>	385
<i>InterLock Proxy Application Gateway Services</i>	387
<i>Additional Source of Information on ANS InterLock</i>	395
Trusted Information Systems Gauntlet	395
<i>Configuration Examples Using Gauntlet</i>	397
<i>Configuring Gauntlet</i>	398
<i>User's View of Using the Gauntlet Firewall</i>	401
The TIS Firewall Toolkit	404
<i>Building the TIS Firewall Toolkit</i>	405
<i>Configuring the Bastion Host with Minimal Services</i>	408
<i>Installing the Toolkit Components</i>	410
<i>The Network Permissions Table</i>	413
Summary	420
10 The TIS Firewall Toolkit	421
Understanding TIS	422
Where to Get TIS Toolkit	422
Compiling under SunOS 4.1.3 and 4.1.4	423
Compiling under BSDI	423
<i>Code Changes</i>	424
Installing the Toolkit	424
Preparing for Configuration	426
Configuring TCP/IP	430
<i>IP Forwarding</i>	430
The netperm Table	431
Configuring netacl	433
<i>Connecting with netacl</i>	436
<i>Restarting inetd</i>	437
Configuring the Telnet Proxy	438
<i>Connecting through the Telnet Proxy</i>	441
<i>Host Access Rules</i>	442
<i>Verifying the Telnet Proxy</i>	443
Configuring the rlogin Gateway	444
<i>Connecting through the rlogin Proxy</i>	447
<i>Host Access Rules</i>	448
<i>Verifying the rlogin Proxy</i>	448



Configuring the FTP Gateway	449
<i>Host Access Rules</i>	451
<i>Verifying the FTP Proxy</i>	452
<i>Connecting through the FTP Proxy</i>	453
<i>Allowing FTP with netacl</i>	454
Configuring the Sendmail Proxy smap and smapd	454
<i>Installing the smap Client</i>	455
<i>Configuring the smap Client</i>	455
<i>Installing the smapd Application</i>	457
<i>Configuring the smapd Application</i>	457
<i>Configuring DNS for smap</i>	459
Configuring the HTTP Proxy	460
<i>Non-Proxy-Aware HTTP Clients</i>	462
<i>Using a Proxy-Aware HTTP Client</i>	463
<i>Host Access Rules</i>	463
Configuring the X Windows Proxy	466
Understanding the Authentication Server	467
<i>The Authentication Database</i>	469
<i>Adding Users</i>	472
<i>The Authentication Shell—authmgr</i>	476
<i>Database Management</i>	477
<i>Authentication at Work</i>	479
Using plug-gw for Other Services	480
<i>Configuring plug-gw</i>	481
<i>plug-gw and NNTP</i>	482
<i>plug-gw and POP</i>	485
The Companion Administrative Tools	487
<i>portscan</i>	487
<i>netscan</i>	488
<i>Reporting Tools</i>	489
<i>The Authentication Server Report</i>	491
<i>The Service Denial Report</i>	492
<i>The FTP Usage Report</i>	494
<i>The HTTP Usage Report</i>	494
<i>The netacl Report</i>	495
<i>The Mail Usage Report</i>	496
<i>The Telnet and rlogin Usage Report</i>	497
Where to Go for Help	498



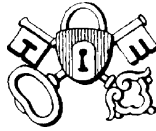
11	Black Hole	501
	Understanding Black Hole	502
	<i>System Requirements</i>	504
	<i>Black Hole Core Modules</i>	506
	<i>Black Hole Extension Modules</i>	509
	Network Design with Black Hole	510
	<i>Remembering the Security Policy</i>	512
	Using the Black Hole Interface	512
	Understanding the Policy Database	514
	<i>Policy and Rule Resolution</i>	519
	Services, Users, and Rules	521
	<i>Rules</i>	521
	<i>Users and User Maintenance</i>	521
	Configuring Black Hole	528
	<i>Configuring an Internal and External DNS</i>	528
	<i>Configuring Application Services</i>	531
	Generating Reports	537
	For More Information	541
	Summary	541

PART III ♦ APPENDIXES

A	List of Worksheets	545
B	Sources of Information	547
	Tools	548
	<i>Tcpwrapper and Portmapper</i>	548
	<i>Firewall Kit</i>	548
	<i>Bellcore S/Key</i>	549
	<i>One-Time Passwords In Everything (OPIE)</i>	549
	<i>Swatch Logfile Monitor</i>	549
	<i>Tcpdump</i>	549
	<i>TAMU Tiger</i>	550
	<i>COPS</i>	550
	<i>Crack</i>	550
	<i>SATAN</i>	551
	<i>Passwd+</i>	551
	<i>npasswd</i>	551
	<i>Tripwire</i>	551



Finding Commercial Firewall Vendors	552
Exploring Firewall and Security Mailing Lists	552
<i>Firewall Mailing Lists</i>	552
<i>Security Forms</i>	553
C Vendor List	555
D The Opie and Log Daemon Manual Pages	557
The OPIE Man Pages	558
<i>opieftpd</i>	558
<i>opiekey</i>	561
<i>opeipasswd</i>	563
<i>opeinfo</i>	564
<i>opielogin</i>	565
<i>opiesu</i>	567
The Log Daemon Manual Pages	568
<i>ftpd</i>	568
<i>key</i>	572
<i>keyinfo</i>	572
<i>keyinit</i>	573
<i>rexecd</i>	574
<i>rlogind</i>	576
<i>rshd</i>	577
<i>skey.access</i>	579
<i>skeysh</i>	582
<i>su</i>	582
<i>telnetd</i>	584
Index	585



INTRODUCTION

*I*NTERNET FIREWALLS AND NETWORK SECURITY, SECOND EDITION is designed for system administrators and interested users who realize the risks involved in connecting a computer system to the Internet.

In days of old, brick walls were built between buildings in apartment complexes so that if a fire broke out, it would not spread from one building to another. Quite naturally, the walls were called “firewalls.”

When you connect your LAN to the Internet, you are enabling your users to reach and communicate with the outside world. At the same time, however, you are enabling the outside world to reach and interact with your LAN. Firewalls, in their barest sense, are routers through which the data traffic flows. If intruders attempt unauthorized access to your network, you stop them at the firewall and do not allow them any further into the system.



WHO SHOULD READ THIS BOOK

Internet Firewalls and Network Security, Second Edition is designed for advanced users and system administrators. It contains information and procedures for the average networked site and represents many hours spent troubleshooting and administering that environment.

HOW THIS BOOK HELPS YOU

The information presented in Part I provides an overview of security and TCP/IP. Being the protocol of the Internet, it is important to understand how TCP/IP works and what utilities are available. It also is important to understand the concept of security and why it is necessary to limit access to resources.

Part II covers firewalls and screening routers. Not only are various theories and hypothetical examples discussed, but real-world examples are given. Over-the-counter products are discussed, as well as tool kits that enable you to build your own firewall from scratch.

Part III, the appendix section, offers a quick way to locate key information. Appendix A lists the sample worksheets contained in the chapters and where they can be found. Appendix B lists sources of more information. Appendix C provides a list of vendors. Appendix D provides the manual pages for OPIE and Log Daemon, two forms of the one-time password authentication system.

CONVENTIONS USED IN THIS BOOK

Throughout this book, certain conventions are used to help you distinguish the various elements of firewalls, system files, and sample data. Before you look ahead, you should spend a moment examining these conventions.

- ❖ Shortcut keys and key combinations are found in the text where appropriate. In most applications, for example, Shift+Ins is the shortcut key combination for the Paste command.

- ❖ Key combinations appear in the following formats:

KEY1+KEY2. When you see a plus sign (+) between key names, you should hold down the first key while pressing the second key. Then release both keys.

KEY1, KEY2. When a comma (,) appears between key names, you should press and release the first key and then press and release the second key.



- ❖ Information you type is in **bold**. This convention applies to individual letters and numbers, as well as words or phrases. It does not apply, however, to special keys, such as Enter, Esc, or Ctrl.
- ❖ New terms appear in *italic*.
- ❖ Text displayed on-screen but not as part of an application, such as system prompts and messages, appear in a special, computer, typeface.

SPECIAL TEXT USED IN THIS BOOK

Throughout this book you will find examples of special text. These passages have been given special treatment so you can instantly recognize their significance and easily find them for future reference.

NOTES, TIPS, AND WARNINGS

Internet Firewalls and Network Security, Second Edition features many special sidebars, which are set apart from the normal text by icons. The book includes three distinct types of sidebars: Notes, Tips, and Warnings.

A *note* includes “extra” information you should find useful, but which complements the discussion at hand instead of being a direct part of it. A note might describe special situations that arise when you use a firewall under certain circumstances, and tell you what steps to take when such situations arise. Notes also might explain ways to avoid problems with your software and hardware.



A *tip* provides quick instructions for getting the most from your firewall implementation as you follow the steps outlined in the general discussion. A tip might show you ways to conserve memory in some setups, speed up a procedure, or perform one of many timesaving and system-enhancing techniques.





WARNING



A *warning* tells you when a procedure might be dangerous, that is, when you run the risk of losing data, locking your system, or even damaging your hardware. Warnings generally explain ways to avoid such losses, or describe the steps you can take to remedy them.

NEW RIDERS PUBLISHING

The staff of New Riders Publishing is committed to bringing you the very best in computer reference material. Each New Riders book is the result of months of work by authors and staff who research and refine the information contained within its covers.

As part of this commitment to you, the NRP reader, New Riders invites your input. Please let us know whether you enjoy this book, if you have trouble with the information and examples presented, or if you have a suggestion for the next edition.

Please note, though, that New Riders' staff cannot serve as a technical resource for firewalls, security, or questions about software- or hardware-related problems. Please refer to the documentation that accompanies your product or to the application's Help systems.

If you have a question or comment about any New Riders book, there are several ways to contact New Riders Publishing. We will respond to as many readers as we can. Your name, address, or phone number never becomes part of a mailing list or is used for any purpose other than to help us continue to bring you the best books possible. You can write us at the following address:

New Riders Publishing
Attn: Associate Publisher
201 W. 103rd Street
Indianapolis, IN 46290

If you prefer, you can fax New Riders Publishing at (317)581-4670.

You can send electronic mail to New Riders at the following Internet address:

edulaney@newriders.mcp.com

NRP is an imprint of Macmillan Computer Publishing. To obtain a catalog of information, or to purchase any Macmillan Computer Publishing book, call (800)428-5331.

Thank you for selecting *Internet Firewalls and Network Security, Second Edition*!