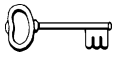
Internet Firewalls *and* Network Security

Second Edition



Chris Hare

Karanjit Siyan

New Riders Publishing New Riders Indianapolis, Indiana

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

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

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.

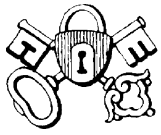
I wish to acknowledge the many people who have helped me along the way: Harpreet Sandhu, Bill Duby, Angela, Michael Anaast, and Janice Culliford; my students Lisa, Debi, Sheri, Rondi, and Linda; Edward and Mary Kramer, Daniel Gottsegen, David Stanfield, Dr. Wagner, Bill Joy, Professor Ramamoorthy, Professor 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

TABLE OF CONTENTS



INTRODUCTION

Internet 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.

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*!