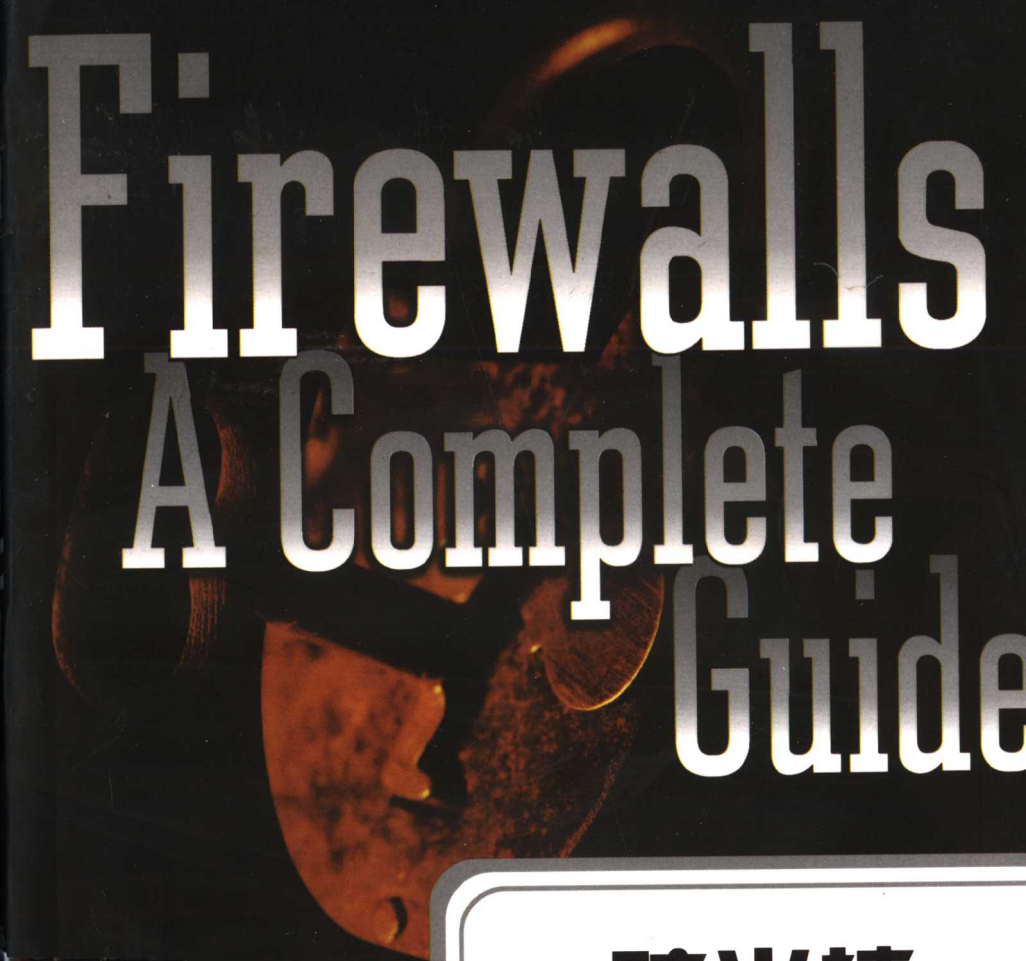
Firewalls A Complete Guide



防火墙技术指南

MARCUS GONCALVES

McGraw-Hill Book Co 世界图书出版公司

FIREWALLS A COMPLETE GUIDE

McGraw-Hill Book Co
世界图书出版公司

Firewalls: A Complete Guide

Marcus Gonçalves

McGraw-Hill
New York • San Francisco • Washington, D.C. • Auckland
Bogotá • Caracas • Lisbon • London • Madrid • Mexico City
Milan • Montreal • New Delhi • San Juan • Singapore
Sydney • Tokyo • Toronto

书　　名：Firewalls
作　　者：M. Goncalves
中 译 名：防火墙技术指南
出 版 者：世界图书出版公司北京公司
印 刷 者：北京中西印刷厂
发　　行：世界图书出版公司北京公司 (北京朝内大街 137 号　100010)
开　　本：1/32　　850×1168　　印　张: 22.125
出版年代：2001 年 4 月
书　　号：ISBN7-5062-4971-5/ TP • 63
版权登记：图字 01-2000-3660
定　　价：105.00 元

McGraw-Hill
A Division of The McGraw-Hill Companies

1 2 3 4 5 6 7 8 9 0 AGM/AGM 9 0 4 3 2 1 0 9

P/N 135641-X
PART OF ISBN 0-07-135639-8

IE ISBN 0-07-118900-9

I dedicate this book to Marcia Valeria Gonçalves and Natalia Gonçalves. They represent two generations that impacted my life in a profound way, which I'm very thankful for. They will be in my heart always.

I also dedicate this book to my wife Carla and children Samir, Andrea, and Joshua, as well as to my parents Mario and Lourdes Gonçalves, for always being there for me. I thank the Boston Church of Christ for nurturing me spiritually and helping me see the world in the right perspective.

Most importantly, I dedicate this book to God, for the talents and the gift of life he gave me and for allowing me to contribute to a better world in this way. Glory be to Him, as this book wouldn't have been possible without Him.

PREFACE

The Internet is an all-pervasive entity in today's world of computing. To cope with the "wild" Internet, several security mechanisms were developed, among them access controls, authentication schemes, and firewalls, one of the most secure methods.

However, *firewall* means different things to different people. Consider the fable from India about the blind men and the elephant. Each blind man touched a different part of the elephant and came up with a totally different description. The blind man who touched the elephant's legs described it as being similar to a tree. Another blind man touched the tail and decided an elephant was like a twig. Yet another grabbed the trunk and concluded an elephant was like a snake. To some computer professionals, even to some of those in charge of Internet security, firewalls are just "walls of fire" blocking hackers out. To others, it is only an authentication mechanism. Some other folks consider firewalls to be synonymous with routers. Obviously, a firewall is much more than any of these individually.

The problem is only compounded by the fact that for a lot of computer and security professionals, firewalls were touched upon only fleetingly in their academic careers; worse, they bumped into them at the computer room. Also, a lot of the important parts and features of firewalls are recent innovations, and thus were never covered in an academic career or most of the 1995–1998 firewall books at all, which further aggravates the problem because, until now, there has been no one single book these professionals can turn to. Their only resource has been to peruse a wide array of literature including textbooks, Web pages, computer magazines, white papers, and so on.

This book, *Firewalls: A Complete Guide*, aims to become your companion book, the one you will always want to carry with you, as it does claim to be complete! I can assure you, there may be some similar books on the market, but none is as complete as this one, and none provides a reference guide, as this one does. The other titles I know are either discussing a specific technology and strategy or a product.

Although you can compare this book to those because it also covers the firewall technologies, strategies, and all the main firewall products on the market, this book goes beyond the scope of the other books. In addition, it provides a complete reference guide of the various protocols, including the upcoming ones (IPV6, for example) and how firewalling fits into them.

In fact, this new and revised edition of the book adds another level to your expertise by discussing all the components that make the Internet,

and any other network for that matter, unsecured; it discusses and describes in detail all the protocols, standards, and APIs used in internetworking, as well as the security mechanisms, from cryptography to firewalls. Later in the book, there is an updated reference section with a complete review of the major firewall products available on the market to date, a selection of tools, applications, and many firewall demos and evaluations, which are bundled on the CD that accompanies this book.

This book is aimed primarily at network, Web, systems, LAN, and WAN administrators. But it is also targeted at the new breed of professionals, the so-called Internet Managers, as well as to anyone in need of a complete reference book on firewalls. As you read this book, you will notice that what separates it from the others is that this book is comprehensive and gives the technical information necessary to understand, choose, install, maintain, and foresee future needs involving firewalls and security at a very informal level. It has a conversational style with practical information, tips, and cautions to help the Internet, network, and security administrator to cope, and "survive" their tasks and responsibilities.

As important as implementing firewalls at your site, you first need a security policy that takes into consideration services to be blocked and allowed. It should also consider implementation of authentication and encryption devices and the level of risks you are willing to undertake in order to be connected to the Internet. This book will discuss all of these topics and the issues that arise when dealing with site security and administration. It will go over all the services, such as Telnet, FTP, Web, e-mail, news, and so on.

How This Book Is Organized

This book is organized in three parts:

Part 1, "Introducing TCP/IP and the Need for Security: Firewalls," is a *reference* section covering all the rationales for having security at a site, the Internet threats, the security concepts, and firewall fundamentals.

Chapter 1, "Internetworking Protocols and Standards: An Overview," covers all the major standards used on the Internet. It discusses TCP/IP, ICMP, IGMP, routing (including super routers and terabit ones), bridging, gateways, IPv6, BGP-4, BOOTP, NTP/SNTP, DHCP, WINS, DNS, and more.

Chapter 2, "Basic Connectivity," discusses the protocols and standards that enable Internet connectivity such as TTYs, UUCP, SLIP, PPP, Rlogin, Telnet, RAS, and more.

Chapter 3, "Cryptography: Is It Enough?," is a natural result of what is discussed in Chapters 1 and 2 in light of the insecurity of these protocols and standards. It provides an introduction to one of the most efficient techniques to enhance security on the Internet: cryptography. It provides an introduction to the subject, as well as covering symmetric encryption techniques, such as DES, IDEA, CAST, Skipjack, and RC2/RC4. It also discusses asymmetric key encryption and public key encryption schemes such as RSA, PKCS, DSS, and much more.

Chapter 4, "Firewalling Challenges: The Basic Web," marks the beginning of the discussion of how the insecurity and weakness of the IP technologies covered earlier and the many attempts to increase its security affect services provided on the Internet. This chapter concentrates specifically on issues related to the basic Web technologies, such as HTML, URL/URI, HTTP, CGI, and more.

Chapter 5, "Firewalling Challenges: The Advanced Web," digs much deeper into the issues discussed in Chapter 4, which directly affect the Web and its level of security. This chapter discusses the concepts and security of advanced technologies behind the Web, such as ISAPI, NSAPI, Servlets, plug-ins, ActiveX, JavaScript, Shockwave, and more.

Chapter 6, "The APIs Security Holes and Its Firewall Interactions," discusses the influence of APIs on network environments connecting to the Internet and its effect due to lack of security. It covers sockets, Java APIs, Perl modules, W3C www-lib, and more.

Part 2, "Firewall Implementations and Limitations," is a more practical section covering all aspects involving firewall implementations, the security limitations and the advantages of plugging in security as discussed in Part I, in light of the multitude of protocols and standards. It discusses how to use the various types of firewalls for the many different environments, what to use where and how, and so on.

Chapter 7, "What Is an Internet/Intranet Firewall After All?," discusses the basic components and technology behind firewalls and cyberwalls, extending the discussion to the advantages and disadvantages of using firewalls, security policies, and types of firewalls.

Chapter 8, "How Vulnerable Are Internet Services?," lists all the major Internet services' weaknesses and what can be done to minimize the risks they generate for users and corporations attached to the Internet. This chapter discusses how to protect and configure electronic mail, SMTP, POP, MIME, FTP, TFTP, FSP, UUCP, News, and much more.

Chapter 9, "Setting Up a Firewall Security Policy," peels another layer off the Internet security onion by discussing how to set up a firewall policy, what to look for, and when enough security is really enough!

Chapter 10, "Putting It Together: Firewall Design and Implementation," begins to put everything discussed so far into action. It discusses planning, choosing the right firewall according to your environment and needs, and implementing it.

Chapter 11, "Proxy Servers," is vital for the success of firewall implementation as discussed in the previous chapter. It brings security a step further by showing how proxy servers can significantly enhance the level of security offered by a firewall. This chapter defines a proxy, shows how to implement it, and introduces the concept of SOCKS and how to implement it with your proxy server.

Chapter 12, "Firewall Maintenance," adds naturally to the two previous chapters. Once you set up your firewall and add a proxy server, you know you will need to get ready to maintaining your firewall. This chapter will help you keep your firewall in tune, monitor your systems, and perform preventive and curative maintenance.

Chapter 13, "Firewall Toolkits and Case Studies," complements this section of the book by providing you with supplementary information and case studies on the subject.

Part 3, "Firewall Resource Guide," expands the information contained in Chapter 13 by providing an extensive resource guide on firewalls. It discusses the major firewall technologies and brands, their advantages and disadvantages, what to watch for, and what to avoid, as well as what to look for in a firewall product.

Chapter 14, "Types of Firewalls and Products on the Market," provides you with a technical overview of the main firewall products available on the market as of the summer of 1999. It's an extensive selection of all the major vendors and their firewall technologies, so you can have a chance to evaluate each one of them before deciding which firewall best suits your needs.

Appendix A, "List of Firewall Resellers and Products," provides you with a list of firewall vendors and their product descriptions. Most of them have a demo or evaluation copy included in the CD that accompanies this book.

The Glossary provides you with a comprehensive list of terms generally used in the firewall/Internet environment.

The Bibliography provides you with a list of URL links to sites offering white papers, general and more technical information on firewalls, and proxy servers.

Who Should Read This Book?

The professionals most likely to take advantage of this book are

- Computer-literate professionals who graduated a few or more years ago and are concerned with security
- Programmers/Analysts/Software Developers, Engineers/Test Engineer Programmers, and Project Managers
- MIS and IS&T (Information Systems and Technology) professionals
- Professionals involved with setting up, implementing, and managing Intranets and the Internet
- Webmasters
- Entry-level (in terms of computer literacy) professionals who want to understand how the Internet works rather than how to use the Internet
- Advanced computer-literate people who would use this book as a quick reference

ACKNOWLEDGMENTS

Many are the friends and professionals that contributed directly or indirectly to this book. To name all of them would be practically impossible, as there are so many. But I would like to acknowledge those that went an extra mile to help me make this book possible, starting with the great professionals who are making a difference in the world of Internet security and who helped me with inputs, suggestions, technical knowledge, and support. They are Alec Muffett of COAST, Marcus Ranum of Network Flight Recorder, Inc., Peter Trei of Process Software Corporation, Anders Wahlin and Paul Hoffman of the Internet Mail Consortium, Scott Schnell of RSA, Frank da Cruz of Columbia University, Serge Hallyn of the College of William and Mary, and Andrea Dixon.

I thank my acquisition editor at McGraw-Hill, Steven Elliott, for the opportunity he extended to me with this book and Jennifer Perillo for her hard work in making this book a reality.

As always, I would like to thank my beautiful wife Carla, for her understanding when I had to break my bedtime schedule so that this book could be finished! I'll be eternally thankful to God, for all the above, and for allowing me to reach out to people this way. I thank Him for giving me the strength I needed to finish this task.

Marcus Gonçalves—goncalves@arcweb.com

ABOUT THE AUTHOR

Marcus Gonçalves, MS in CIS, has several years of internetworking and security consulting in the IS&T arena. He lives in Hopkinton, Massachusetts with his wife and kids. He's a Senior IT/Enterprise Applications Analyst for ARC Advisory Group, one of the leaders in global market research and advisory services firms in the greater Boston area.

He has taught several workshops and seminars on IS and Internet security in the U.S. and internationally. He's a member of the International Computer Security Association (ICSA), the Internet Society, the Association for Information Systems (AIS), and the New York Academy of Sciences (NYAS). He also serves as the Editor in Chief for the *Journal for Internet Security* (JISec) of Canada.

He is the author of *Protecting Your Web Site with Firewalls* (PRT), the *Internet Privacy Kit* (Que), and *Web Security with Firewalls* (Axcel Books). He co-authored the *Web Site Administrator's Survival Guide* (Sams.Net) and *Windows NT Server 4.0: Management and Control* (PTR). He is also a regular contributor for *BackOffice Magazine*, *WEBster Magazine*, *WebWeek*, and *Developer's Magazine*.

If you're interested in his articles, check the URL `http://members.aol.com/goncalvesv/private/writer.htm`. For complete background information, go to `http://members.aol.com/goncalvesv`. To contact the author, please send e-mail to `goncalves@arcweb.com`.

SOFTWARE AND INFORMATION LICENSE

The software and information on this diskette (collectively referred to as the "Product") are the property of The McGraw-Hill Companies, Inc. ("McGraw-Hill") and are protected by both United States copyright law and international copyright treaty provision. You must treat this Product just like a book, except that you may copy it into a computer to be used and you may make archival copies of the Products for the sole purpose of backing up our software and protecting your investment from loss.

By saying "just like a book," McGraw-Hill means, for example, that the Product may be used by any number of people and may be freely moved from one computer location to another, so long as there is no possibility of the Product (or any part of the Product) being used at one location or on one computer while it is being used at another. Just a book cannot be read by two different people in two different places at the same time, neither can the Product be used by two different people in two different places at the same time (unless, of course, McGraw-Hill's rights are being violated).

McGraw-Hill reserves the right to alter or modify the contents of the Product at any time.

This agreement is effective until terminated. The Agreement will terminate automatically without notice if you fail to comply with any provisions of this Agreement. In the event of termination by reason of your breach, you will destroy or erase all copies of the Product installed on any computer system or made for backup purposes and shall expunge the Product from your data storage facilities.

LIMITED WARRANTY

McGraw-Hill warrants the physical diskette(s) enclosed herein to be free of defects in materials and workmanship for a period of sixty days from the purchase date. If McGraw-Hill receives written notification within the warranty period of defects in materials or workmanship, and such notification is determined by McGraw-Hill to be correct, McGraw-Hill will replace the defective diskette(s). Send request to:

Customer Service
McGraw-Hill
Gahanna Industrial Park
860 Taylor Station Road
Blacklick, OH 43004-9615

The entire and exclusive liability and remedy for breach of this Limited Warranty shall be limited to replacement of defective diskette(s) and shall not include or extend any claim for or right to cover any other damages, including but not limited to, loss of profit, data, or use of the software, or special, incidental, or consequential damages or other similar claims, even if McGraw-Hill has been specifically advised as to the possibility of such damages. In no event will McGraw-Hill's liability for any damages to you or any other person ever exceed the lower of suggested list price or actual price paid for the license to use the Product, regardless of any form of the claim.

THE McGRAW-HILL COMPANIES, INC. SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Specifically, McGraw-Hill makes no representation or warranty that the Product is fit for any particular purpose and any implied warranty of merchantability is limited to the sixty day duration of the Limited Warranty covering the physical diskette(s) only (and not the software or information) and is otherwise expressly and specifically disclaimed.

This Limited Warranty gives you specific legal rights; you may have others which may vary from state to state. Some states do not allow the exclusion of incidental or consequential damages, or the limitation on how long an implied warranty lasts, so some of the above may not apply to you.

This Agreement constitutes the entire agreement between the parties relating to use of the Product. The terms of any purchase order shall have no effect on the terms of this Agreement. Failure of McGraw-Hill to insist at any time on strict compliance with this Agreement shall not constitute a waiver of any rights under this Agreement. This Agreement shall be construed and governed in accordance with the laws of New York. If any provision of this Agreement is held to be contrary to law, that provision will be enforced to the maximum extent permissible and the remaining provisions will remain in force and effect.

CONTENTS