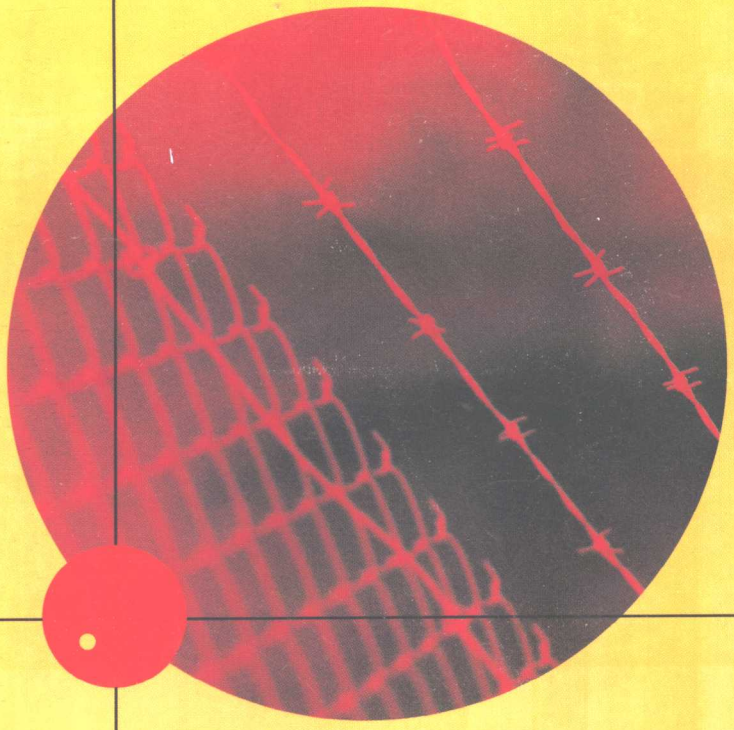
THOMSON
COURSE TECHNOLOGY

GUIDE TO FIREWALLS AND NETWORK SECURITY

INTRUSION DETECTION AND VPNs

GREG HOLDEN



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Guide to

Firewalls and Network Security: with Intrusion Detection and VPNs

Greg Holden

THOMSON
COURSE TECHNOLOGY

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

Guide to Firewalls and Network Security: with Intrusion Detection and VPNs

By Greg Holden

Senior Editor:
William Pitkin III

Senior Product Manager:
Laura Hildebrand

Production Editor:
Brooke Booth

Development Editor:
Jill Batistick

Technical Reviewers:
Eileen Vidrine, Dave DiFabio, Rob Andrews, Gary Sparks, Jeffrey Monts

Quality Assurance Manager:
John Bosco

MQA Project Leader:
Nicole Ashton

Associate Product Manager:
Tim Gleeson

Editorial Assistant:
Nick Lombardi

Marketing Manager:
Jason Sakos

Text Designer:
GEX Publishing Services

Compositor:
GEX Publishing Services

Cover Design:
Julie Malone

Printed in Canada

1 2 3 4 5 6 7 8 9 WC 07 06 05 04

For more information, contact Course Technology, 25 Thomson Place, Boston, Massachusetts, 02210.

Or find us on the World Wide Web at: www.course.com

ISBN 0-619-13039-3

Introduction

This book is intended to provide an introduction to firewalls and other network security components that can work together to create an in-depth defensive perimeter around a Local Area Network (LAN). Firewalls are among the best-known security tools in use today, and they are growing in popularity among the general public as well as Information Technology professionals. However, firewalls work most effectively when they are backed by a security policy and when they work in consort with anti-virus software, intrusion detection systems, and other tools.

Accordingly, this book examines firewalls in context with the other elements needed for effective perimeter security as well as security within a network. These include packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems.

Where Should You Start?

This book is not intended to be read in sequence, from beginning to end. The first three chapters, however, do provide you with a solid introduction to firewalls and where they fit in a network security program, so it's highly recommended that you start with them. The chapters are as follows:

Chapter 1, "Firewall Planning and Design," provides you with an overview of the different kinds of firewalls and their primary functions, so you can choose the right one to meet your needs.

Chapter 2, "Developing a Security Policy," helps you coordinate the goals of a firewall with the goals of an organization's overall security policy. You also learn how to work with administration in a step-by-step way to make sure your security policy works. **Chapter 3**, "Firewall Configuration Strategies," introduces you to the different approaches you can take to locating one or more firewalls on your network perimeter and coordinating them to work with other components such as DMZs, routers, and VPNs.

The next several chapters discuss specific topics important to firewalls and network security. You are encouraged to read the chapters that have the most immediate interest to you rather than feeling you have to read them in a linear fashion. **Chapter 4**, "Packet

Filtering," explores the first, and in some ways, the most fundamental activities of firewalls. Both stateless and stateful packet filtering are examined, as well as the establishment of a packet filtering rule base for common protocols such as ICMP, TCP, and UDP. **Chapter 5**, "Working with Proxy Servers and Application-Level Firewalls," discusses how proxy servers work to shield individual hosts on the internal network by acting on their behalf. **Chapter 6**, "Authenticating Users," describes why firewalls do authentication and how they are able to identify authorized individuals through user, client, and session authentication, as well as through centralized authentication systems and one-time password systems. **Chapter 7**, "Encryption and Firewalls," focuses on the role encryption plays in firewall architecture, and the establishment of a Public Key Infrastructure (PKI) for a network. **Chapter 8**, "Choosing a Bastion Host," explains how to secure the host computers that run firewall or intrusion detection software or that provide public services on the DMZ.

The book's last three chapters delve into more advanced topics and focus on a survey of popular firewall and VPN options. **Chapter 9**, "Setting Up a Virtual Private Network," discusses the establishment of VPNs, which provide corporations with a cost-effective means for conducting secure communications over the public Internet. Because VPNs use encryption and authentication, it's a good idea to read Chapters 6 and 7 before you get to this chapter. **Chapter 10**, "Building Your Own Firewall," teaches you about the two categories of firewalls and explains how desktop and enterprise firewalls work. **Chapter 11**, "Ongoing Administration," talks about the various periodic maintenance tasks you need to perform when administering a firewall, including log file rotation and examination. It also delves into the integration of anti-virus and intrusion detection systems with firewalls.

Readers are also encouraged to investigate the many pointers to online and printed sources of additional information that are cited throughout this book.

Features

To aid you in fully understanding networking concepts, there are many features in this book designed to improve its pedagogical value.

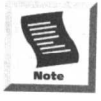
- **Chapter Objectives:** Each chapter in this book begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with a quick reference to the contents of that chapter, as well as a useful study aid.
- **Illustrations, Tables, and Screenshots:** Numerous illustrations of networking configurations aid you in the visualization of common firewall setups and architectures. In addition, many tables provide details and comparisons using both practical

and theoretical information. Some tables provide specific examples of packet filtering rules you can use to build a firewall rule base. Because most campus laboratories use Microsoft operating systems, we use their products for screen shots and Hands-on Projects for this book.

- **Chapter Summaries**: Each chapter's text is followed by a summary of the concepts it has introduced. These summaries provide a helpful way to recap and revisit the ideas covered in each chapter.
- **Key Terms**: Following the Chapter Summary, a list of new networking terms and their definitions encourages proper understanding of the chapter's key concepts and provides a useful reference.
- **Review Questions**: End-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions ensure that you have mastered the concepts.
- **Hands-on Projects**: Although it is important to understand the theory behind networking technology, nothing can improve upon real-world experience. With the exceptions of those chapters that are purely theoretical, each chapter provides a series of exercises aimed at providing students with hands-on implementation experience.
- **Case Projects**: Finally, each chapter closes with a section that proposes certain firewall and security-related situations. You are asked to evaluate the situation and decide upon the course of action to be taken to remedy the problems described. This valuable tool will help you to sharpen decision-making and troubleshooting skills—important aspects of firewall and security systems administration.

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below.



Notes present additional helpful material related to the subject being described.

Tips highlight suggestions on ways to attack problems you may encounter in a real-world situation. As an experienced network administrator, the author has practical experience with how networks work in real business situations.

Hands-on Project icons precede each hands-on activity in this book.

Case Project icons are located at the end of each chapter. They mark more involved, scenario-based projects. In this extensive case example, you are asked to independently implement what you have learned.

Endmatter

In addition to its core materials, this book includes several appendices.

- **Appendix A**: **Security Resources:** This appendix provides suggestions of places you can go online to find the latest security-related information. You get descriptions of well-known and highly regarded Web sites that provide background information on network security as well as virus alerts, port scanners that can test your existing security configuration, and places where you can go to obtain certifications that can help you find employment in a network security field.
- **Glossary**: This is a complete compendium of all of the acronyms and technical terms used in this book, with definitions.

Instructor's Materials

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM.

Electronic Instructor's Manual. The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

Solution Files. The Solution Files include answers to all end-of-chapter materials, including the Review Questions, and when applicable, Hands-on Projects, and Case Projects.

ExamView®. This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

PowerPoint presentations. This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Figure Files. All of the figures in the book are reproduced on the Instructor's Resource CD in bit-mapped format. Similar to the PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

Coping with Change on the Web

Sooner or later, all the specific Web-based resources mentioned throughout the rest of this book will go stale or be replaced by newer information. In some cases, the URLs you find here may lead you to their replacements; in other cases, the URLs will lead nowhere, leaving you with the dreaded 404 error message, "File not found."

When that happens, please don't give up! There's always a way to find what you want on the Web, if you're willing to invest some time and energy. To begin with, most large or complex Web sites offer a search engine. As long as you can get to the site itself, you can use this tool to help you find what you need.

Don't be afraid to use general search tools like *http://www.google.com*, *http://www.hotbot.com*, or *http://www.excite.com* to find related information. Although certain standards bodies may offer the most precise and specific information about their standards online, there are plenty of third-party sources of information, training, and assistance in this area as well. The bottom line is: if you can't find something where the book says it lives, start looking around. It's got to be around there, somewhere!

Visit our World Wide Web Site

Additional materials designed especially for you might be available for your course on the World Wide Web. Go to *www.course.com* and search for this book title periodically for more details.

Acknowledgments

I would like to thank the team at Course Technology for the opportunity to write this book on a topic of such value and interest. This team includes but is not limited to Laura Hildebrand, Product Manager, Brooke Booth, Production Editor, and the excellent work of the copy editors and quality assurance folks. Thanks also to Jill Batistick, Development Editor, for her always-excellent edits, her words of encouragement, and her periodic reminders that kept me on track. I would also like to thank the reviewers, who guided me with excellent and helpful feedback on each chapter. I would also like to thank Mark Ciampa, who is a great author, for helping us make changes to the book in the final stages of production. A special thanks goes to my best friend Ann Lindner and to my daughters Lucy and Zosia, whose patience and support made this project successful.

Read This Before You Begin

This book contains more than 70 hands-on projects, many of which require you to install and use different security-related software programs. You need to have access to a computer that is connected to the Internet and that can run those programs. The suggested hardware and software requirements are described below.

Hardware Requirements

Your computer's CPU should be at least a Pentium II and running at 300MHz or faster. To run Web browsers, word processing programs, and other applications at the same time, you should have at least 192MB of RAM (ideally, 256MB or more of RAM) and a minimum of 75MB of available hard disk space.

Software Requirements

Most of the projects in this book can be completed using a computer that runs Windows 2000 or XP or Red Hat Linux 7.3 or later.

Many of the programs used for the Hands-on Projects require you to download and install software. At the very least, your computer should be equipped with a Web browser and the archiving utility WinZip (available at *www.winzip.com*). You'll also need a word processing program or text editor to record answers from the Hands-on Projects. An e-mail application such as Outlook Express or Netscape Messenger is used in several of the projects as well.

Special Requirements

In this book, you will find references to Check Point NG. If you have the software, note that you will need to have a minimum of 128 MB of RAM on your system to run it. Note also that Check Point NG is designed to run on Windows 2000; it will run with limited functionality on Windows XP.

Free Downloadable Software Is Required in the Following Chapters:

Chapter 3:

- Sygate Personal Firewall, *www.sygate.com*

Chapter 4:

- Tiny Personal Firewall, *www.tinysoftware.com*

Chapter 5:

- NetProxy, *www.grok.co.uk*
- SOCKS, *www.socks.nec.com*

Chapter 7:

- PGP (Pretty Good Privacy), *http://web.mit.edu/network/pgp.html*

Chapter 8:

- NetScan Tools 4, *www.netscantools.com*
- IP Sentry, *www.ipsentry.com*

Chapter 9:

- Symantec Enterprise Virtual Private Network 7.0, *www.symantec.com/downloads*

Chapter 10:

- ZoneAlarm Pro, *www.zonelabs.com*

In Chapter 10, you learn about Linksys (*www.linksys.com*), which offers a wide variety of routers, hubs, wireless access points, firewalls, and other hardware. The image of the Linksys product in the chapter is courtesy of Linksys.

BRIEF

Contents

TABLE OF

Contents