Table of Contents

Preface .... *xiii*

I. Network Security *1*

1. Why Internet Firewalls? *3*
What Are You Trying to Protect? *4*
What Are You Trying to Protect Against? *7*
Who Do You Trust? *16*
How Can You Protect Your Site? *17*
What Is an Internet Firewall? *21*
Religious Arguments *28*

2. Internet Services *33*
Secure Services and Safe Services *35*
The World Wide Web *35*
Electronic Mail and News *40*
File Transfer, File Sharing, and Printing *43*
Remote Access *48*
Real-Time Conferencing Services *51*
Naming and Directory Services *52*
Authentication and Auditing Services *54*
Administrative Services *55*
Databases *58*
Games *58*

3. *Security Strategies* 59
Least Privilege 59
Defense in Depth 61
Choke Point 62
Weakest Link 63
Fail-Safe Stance 64
Universal Participation 67
Diversity of Defense 68
Simplicity 70
Security Through Obscurity 71

II. *Building Firewalls* 73

4. *Packets and Protocols* 75
What Does a Packet Look Like? 75
IP 79
Protocols Above IP 85
Protocols Below IP 93
Application Layer Protocols 94
IP Version 6 94
Non-IP Protocols 96
Attacks Based on Low-Level Protocol Details 97

5. *Firewall Technologies* 102
Some Firewall Definitions 102
Packet Filtering 104
Proxy Services 110
Network Address Translation 114
Virtual Private Networks 119

6. *Firewall Architectures* 122
Single-Box Architectures 122
Screened Host Architectures 126
Screened Subnet Architectures 128
Architectures with Multiple Screened Subnets 133
Variations on Firewall Architectures 137
Terminal Servers and Modem Pools 148
Internal Firewalls 149

7. *Firewall Design* 157
Define Your Needs 157
Evaluate the Available Products 159
Put Everything Together 162

8. *Packet Filtering* 165
What Can You Do with Packet Filtering? 166
Configuring a Packet Filtering Router 171
What Does the Router Do with Packets? 173
Packet Filtering Tips and Tricks 178
Conventions for Packet Filtering Rules 180
Filtering by Address 183
Filtering by Service 185
Choosing a Packet Filtering Router 190
Packet Filtering Implementations for General-Purpose Computers 203
Where to Do Packet Filtering 214
What Rules Should You Use? 216
Putting It All Together 216

9. *Proxy Systems* 224
Why Proxying? 225
How Proxying Works 226
Proxy Server Terminology 231
Proxying Without a Proxy Server 232
Using SOCKS for Proxying 233
Using the TIS Internet Firewall Toolkit for Proxying 237
Using Microsoft Proxy Server 238
What If You Can't Proxy? 239

10. *Bastion Hosts* 241
General Principles 242
Special Kinds of Bastion Hosts 243
Choosing a Machine 244
Choosing a Physical Location 248
Locating Bastion Hosts on the Network 249
Selecting Services Provided by a Bastion Host 250
Disabling User Accounts on Bastion Hosts 253
Building a Bastion Host 255
Securing the Machine 256
Disabling Nonrequired Services 259

Operating the Bastion Host ... 269
Protecting the Machine and Backups ... 270

11. *Unix and Linux Bastion Hosts* ... 273
Which Version of Unix? ... 273
Securing Unix ... 275
Disabling Nonrequired Services ... 278
Installing and Modifying Services ... 288
Reconfiguring for Production ... 291
Running a Security Audit ... 295

12. *Windows NT and Windows 2000 Bastion Hosts* ... 297
Approaches to Building Windows NT Bastion Hosts ... 297
Which Version of Windows NT? ... 298
Securing Windows NT ... 299
Disabling Nonrequired Services ... 301
Installing and Modifying Services ... 313

III. *Internet Services* ... 315

13. *Internet Services and Firewalls* ... 317
Attacks Against Internet Services ... 319
Evaluating the Risks of a Service ... 327
Analyzing Other Protocols ... 334
What Makes a Good Firewalled Service? ... 336
Choosing Security-Critical Programs ... 339
Controlling Unsafe Configurations ... 347

14. *Intermediary Protocols* ... 349
Remote Procedure Call (RPC) ... 349
Distributed Component Object Model (DCOM) ... 358
NetBIOS over TCP/IP (NetBT) ... 359
Common Internet File System (CIFS) and Server Message Block (SMB) ... 361
Common Object Request Broker Architecture (CORBA) and Internet Inter-Orb Protocol (IIOP) ... 365
ToolTalk ... 367
Transport Layer Security (TLS) and Secure Socket Layer (SSL) ... 368
The Generic Security Services API (GSSAPI) ... 373
IPsec ... 373

Remote Access Service (RAS) ... 377
Point-to-Point Tunneling Protocol (PPTP) ... 378
Layer 2 Transport Protocol (L2TP) ... 381

15. *The World Wide Web* ... 384
HTTP Server Security ... 385
HTTP Client Security ... 390
HTTP ... 397
Mobile Code and Web-Related Languages ... 406
Cache Communication Protocols ... 412
Push Technologies ... 415
RealAudio and RealVideo ... 417
Gopher and WAIS ... 419

16. *Electronic Mail and News* ... 423
Electronic Mail ... 423
Simple Mail Transfer Protocol (SMTP) ... 430
Other Mail Transfer Protocols ... 441
Microsoft Exchange ... 442
Lotus Notes and Domino ... 443
Post Office Protocol (POP) ... 445
Internet Message Access Protocol (IMAP) ... 448
Microsoft Messaging API (MAPI) ... 450
Network News Transfer Protocol (NNTP) ... 450

17. *File Transfer, File Sharing, and Printing* ... 454
File Transfer Protocol (FTP) ... 455
Trivial File Transfer Protocol (TFTP) ... 468
Network File System (NFS) ... 470
File Sharing for Microsoft Networks ... 479
Summary of Recommendations for File Sharing ... 482
Printing Protocols ... 483
Related Protocols ... 487

18. *Remote Access to Hosts* ... 488
Terminal Access (Telnet) ... 488
Remote Command Execution ... 491
Remote Graphical Interfaces ... 507

19. *Real-Time Conferencing Services* ... 520
Internet Relay Chat (IRC) ... 520
ICQ ... 523
talk ... 525
Multimedia Protocols ... 528
NetMeeting ... 533
Multicast and the Multicast Backbone (MBONE) ... 535

20. *Naming and Directory Services* ... 539
Domain Name System (DNS) ... 539
Network Information Service (NIS) ... 563
NetBIOS for TCP/IP Name Service and Windows Internet Name Service ... 565
The Windows Browser ... 576
Lightweight Directory Access Protocol (LDAP) ... 583
Active Directory ... 585
Information Lookup Services ... 586

21. *Authentication and Auditing Services* ... 591
What Is Authentication? ... 592
Passwords ... 596
Authentication Mechanisms ... 600
Modular Authentication for Unix ... 604
Kerberos ... 609
NTLM Domains ... 615
Remote Authentication Dial-in User Service (RADIUS) ... 622
TACACS and Friends ... 625
Auth and identd ... 627

22. *Administrative Services* ... 630
System Management Protocols ... 630
Routing Protocols ... 637
Protocols for Booting and Boot-Time Configuration ... 644
ICMP and Network Diagnostics ... 647
Network Time Protocol (NTP) ... 654
File Synchronization ... 658
Mostly Harmless Protocols ... 661

23. Databases and Games 664
Databases 664
Games 678

24. Two Sample Firewalls 681
Screened Subnet Architecture 681
Merged Routers and Bastion Host Using General-Purpose Hardware 704

IV. Keeping Your Site Secure 721

25. Security Policies 723
Your Security Policy 724
Putting Together a Security Policy 731
Getting Strategic and Policy Decisions Made 734
What If You Can't Get a Security Policy? 741

26. Maintaining Firewalls 742
Housekeeping 742
Monitoring Your System 746
Keeping up to Date 758
How Long Does It Take? 762
When Should You Start Over? 762

27. Responding to Security Incidents 764
Responding to an Incident 764
What to Do After an Incident 774
Pursuing and Capturing the Intruder 775
Planning Your Response 778
Being Prepared 787

V. Appendixes 795

A. Resources 797

B. Tools 813

C. Cryptography 823

Index 849