

Table of Contents

Introduction 1

About This Book	2
How to Use This Book	2
What You Don't Need to Read	2
Foolish Assumptions	2
How This Book Is Organized	3
Part I: Introducing Firewall Basics	3
Part II: Establishing Rules	3
Part III: Designing Network Configurations	4
Part IV: Deploying Solutions Using Firewall Products	4
Part V: The Part of Tens	4
Icons Used in This Book	5
Where to Go from Here	5

Part 1: Introducing Firewall Basics 7

Chapter 1: Why Do You Need a Firewall? 9

Defining a Firewall	9
The Value of Your Network	11
Get Yourself Connected	12
Modem dial-up connections	13
ISDN connections	14
DSL connections	14
Cable modems	15
T1 and T3	16
Address types	17
The need for speed and security	17
TCP/IP Basics	18
What Firewalls Do	19
What Firewalls Look Like	20
A firewall that fits	20
Network router	21
Appliance	21
Software-only firewalls	21
All-in-one tools	21
Rules, Rules, Everywhere Rules	22

Chapter 2: IP Addressing and Other TCP/IP Basics 23

How Suite It Is: The TCP/IP Suite of Protocols	24
Sizing up the competition	24
Networking for the Cold War: A very short history of TCP/IP	25



Peeling Away the Protocol Layers	26
The Numbers Game: Address Basics	28
URLs: How to Reference Resources	32
Understanding IP Addresses	33
1 and 1 is 10	33
What IP addresses mean	34
Private IP Addresses	36
Dissecting Network Traffic: The Anatomy of an IP Packet	37
Source address	37
Destination address	38
Transport layer protocol	38
Other stuff	38
The other Internet layer protocol: ICMP	38
Transport Layer Protocols	39
Staying connected: UDP and TCP	39
Ports are not only for sailors	40
Some ports are well known	41
Application Layer Protocols	42
HTTP	42
SMTP	43
POP3	43
DNS	43
Telnet	43
Complex protocols	44
FTP	44
Future protocols	45
The Keeper of the Protocols	45
Putting It All Together: How a Request Is Processed	46
Chapter 3: Understanding Firewall Basics	47
What Firewalls Do (And Where's the Fire, Anyway?)	48
Basic functions of a firewall	48
What a firewall can't do	50
General Strategy: Allow-All or Deny-All	51
Packet Filtering	54
Filtering IP data	55
Stateful packet filtering	60
Network Address Translation (NAT)	62
Security aspects of NAT	63
Consequences of NAT	64
Application Proxy	65
Monitoring and Logging	68
Chapter 4: Understanding Firewall Not-So-Basics	71
Making Internal Servers Available: Static Address Mapping	73
Static IP address assignment	74
Static inbound translation	75
Filtering Content and More	76

Detecting Intrusion	79
Detecting an intrusion in progress	80
Responding to an intrusion	81
Reacting to a security incident	82
Improving Performance by Caching and Load Balancing	83
Caching Web results	84
United we stand, dividing the load	86
Using Encryption to Prevent Modification or Inspection	88
Encryption and firewalls	88
Who are you: Authentication protocols	89
The S in HTTPS	90
IP and security: IPSec	91
Virtual Private Networks (VPNs)	92

Chapter 5: “The Key Is under the Mat” and Other Common Attacks 97

Intrusion Attacks: A Stranger in the House	97
Denial-of-service Attacks	99
When everyone is out to get you: Distributed DoS attacks	100
How Hackers Get In	101
The key is under the mat: Insecure passwords	100
Default configurations	101
Bugs	102
Back doors	104
It’s a zoo: Viruses, worms, and Trojan horses	105
Who are you? Man-in-the-middle attacks	106
Impersonation	107
Eavesdropping	107
Inside jobs	108
Other techniques	108
Can a Firewall Really Protect Me?	109
Are You Scared Yet?	110

Part II: Establishing Rules 111

Chapter 6: Developing Policies 113

Defining an Internet Acceptable Use Policy	114
Defining a Security Policy	118
Setting a Security policy	118

Chapter 7: Establishing Rules for Simple Protocols 121

For Starters, Some Default Rules	123
Allowing Web Access	123
Configuring inbound firewall rules	125
Configuring outbound firewall rules	126

Finding Internet Resources	126
Providing name resolution to Internet-based clients	127
Providing Internet name resolution to internal clients	128
File Transfer Protocol (FTP)	131
Messaging and Conferencing	133
America Online (AOL) Messaging	133
MSN Messenger and Windows Messenger	134
NetMeeting	135
Thin Client Solutions	137
Citrix Metaframe	137
Windows Terminal Services	138
Internet Control Message Protocol (ICMP)	139

Chapter 8: Designing Advanced Protocol Rules143

Rain, Sleet, Snow, and Firewalls: Getting the E-Mail Through	144
Answering the right questions	146
Allowing access to external mail services	147
Allowing access to internal mail services	148
Knock, Knock: Who Goes There?	149
RADIUS functionality	150
Configuring inbound RADIUS firewall rules	151
IPSec Encryption	152
When does IPSec fail?	154
What will the future bring?	155
Configuring a firewall to pass IPSec data	157
Let Me In: Tunneling through the Internet	158
Selecting a tunneling protocol	158
Using PPTP firewall rules	159
Using L2TP/IPSec firewall rules	160

Chapter 9: Configuring “Employees Only” and Other Specific Rules163

Limiting Access by Users: Not All Are Chosen	163
Filtering Types of Content	165
Filtering Other Content	166
Preventing access to known “bad” sites	166
Implementing Content Rating	167
Setting the Clock: Filtering on Date/Time	168

Part III: Designing Network Configurations 169

Chapter 10: Setting Up Firewalls for SOHO or Personal Use171

No-Box Solution: ISP Firewall Service	171
Single-Box Solution: Dual-Homed Firewall	172
Screened Host	173
Bypassing the screened host	174

Deployment Scenario	175
Allowing internal network users to access the Internet	175
Chapter 11: Creating Demilitarized Zones with a Single Firewall	179
Looking at the Demilitarized Zone: No-Man's Land	179
Examining Typical DMZ Configurations	180
Designing Three-Pronged Firewalls	182
Pros and cons	182
Addressing decisions	183
Deploying a Three-Pronged Firewall	186
Deploying a tunnel solution using PPTP	186
Deploying a tunnel solution using L2TP	189
Deploying a Web server with a SQL back end	193
Building a Case for Multi-Pronged Firewalls	195
Chapter 12: Designing Demilitarized Zones with Multiple Firewalls	197
When Two Firewalls Are Better than One	197
DMZs with Two Firewalls	200
Deploying a tunnel solution using PPTP	200
Deploying a tunnel solution using L2TP	203
Deploying a Web server with a SQL back end	206
Allowing private network users to access the Internet	208
<i>Part IV: Deploying Solutions Using Firewall Products</i>	211
Chapter 13: Using Windows as a Firewall	213
Firewall Functions in Windows	214
Windows 98 and Windows Me	216
File and printer sharing	216
PPTP client	217
Internet Connection Sharing: NAT for Dummies	218
Windows NT 4.0	221
Packet filtering	222
PPTP server	223
Windows 2000	224
Packet filtering	224
Network Address Translation (NAT)	227
L2TP and IPSec	229
Windows XP	230
Internet Connection Firewall (ICF)	231
Windows Server 2003	232

Chapter 14: Configuring Linux as a Firewall233

Making Installation Choices	233
Introducing iptables	235
Using iptables Commands	237
iptables commands	238
iptables targets	238
Order matters	240
iptables options and conditions	241
Putting it all together: Building a simple Linux firewall	243
Masquerading and NAT	244
Simplifying Things: Firewall GUIs	246
Adding Proxy Functionality	247
Put your SOCKS on	248
Squid anyone?	248

**Chapter 15: Configuring Personal Firewalls: ZoneAlarm,
BlackICE, and Norton Personal Firewall249**

Home Computers at Risk	250
Home computers have changed	250
Hackers have changed	251
You have changed	252
Features of Personal Firewalls	253
Enterprise firewalls versus personal firewalls	254
How to Be Safe on the Internet	258
Personal Firewall: ZoneAlarm	259
ZoneAlarm features	259
ZoneAlarm user interface	263
ZoneAlarm installation	266
ZoneAlarm configuration tasks	268
Personal Firewall: BlackICE	269
BlackICE features	269
BlackICE user interface	275
BlackICE installation	279
BlackICE configuration tasks	281
Norton Personal Firewall	283
Norton Personal Firewall features	283
Norton Personal Firewall interface	288
Norton Personal Firewall installation	291
Norton Personal Firewall configuration tasks	293

**Chapter 16: Microsoft's Firewall: Internet Security
and Acceleration Server295**

Making Internet Access Faster and More Secure	296
Looking under the Hood: How ISA Works	297
Choosing between the Two Editions	301
Preparing for Installation	302

Installing ISA Server	305
Gathering information	305
Connecting by telephone	310
Examining the Three Clients	312
SecureNAT client	312
Firewall Client	314
Web proxy client	315
The best client for you	316
Following the Rules: The Two Types	317
Putting the two types together	318
Creating a protocol rule	319
Letting the Good Guys In	320
Publishing a Web server	321
Publishing a non-Web server	321
Creating Packet Filters	322
Designing Your Network with ISA Server	326
A simple network	326
A network with a three-pronged DMZ	327
A network with a back-to-back DMZ	328
Taking the Next Step	329

Chapter 17: The Champ: Check Point FireWall-1

Next Generation331

FireWall-1 Features	331
Access control	332
Tracking access: advanced logging, reporting, and alerting	334
Protection against commonly used attacks	335
Content security	335
Intrusion detection	336
Network Address Translation (NAT)	337
VPN-1	338
Performance	338
FireWall-1 Components	339
Standalone deployments	340
Client/Server deployment	341
FireWall-1 Next Generation Installation	342
Installing and Configuring FireWall-1 NG	342
FireWall-1 NG Configuration Tasks	347
Starting the SmartDashboard client	348
Defining a computer object	349
Defining a firewall object	350
Defining a network segment	352
Creating a user account	352
Creating a group account	353
Defining a rule base	353
Installing the Security policy	355

Chapter 18: Choosing a Firewall That Meets Your Needs	357
How Do You Decide?	357
What to Compare?	358
What Are Some of the Choices?	363
 Part V: The Part of Tens	 365
Chapter 19: Ten Tools You Can't Do Without	367
Sam Spade	368
Nmap	369
Netstat	369
TCPView	370
TDIMon	370
FPort	371
Snort	371
Internet Scanner	372
Nessus	373
Network Monitor	373
Ethereal	373
NetCat	374
 Chapter 20: Ten Web Sites to Visit	 375
www.sans.org	375
www.cert.org	376
www.infosyssec.org	377
www.microsoft.com/security	378
www.icsalabs.com	379
www.securityfocus.com	380
www.gocsi.com	380
www.isaserver.org	381
www.interhack.net/pubs/fwfaq	381
Firewall Lists	382
 Appendix: Protocol Listings and More	 383
IP Protocol Numbers	383
ICMP Type Numbers	384
TCP and UDP Port Listing	384
 Index	 393