



Guide to Firewalls and VPNs

Third Edition

Michael E. Whitman
Herbert J. Mattord
Andrew Green



Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

Brief Contents

INTRODUCTION	XV
PART 1	
Introduction to Information Security	
CHAPTER 1	
Introduction to Information Security	1
CHAPTER 2	
Security Policies and Standards	33
CHAPTER 3	
Authenticating Users	67
PART 2	
Firewalls	
CHAPTER 4	
Introduction to Firewalls	97
CHAPTER 5	
Packet Filtering	143
CHAPTER 6	
Firewall Configuration and Administration	179
CHAPTER 7	
Working with Proxy Servers and Application-Level Firewalls	209
CHAPTER 8	
Implementing the Bastion Host	237
PART 3	
VPNs	
CHAPTER 9	
Encryption—The Foundation for the Virtual Private Network	261
CHAPTER 10	
Setting Up a Virtual Private Network	293
APPENDIX A	
Setting Up and Operating a Software Firewall	323
GLOSSARY	329
INDEX	337

Table of Contents

INTRODUCTION	xv
PART 1	
Introduction to Information Security	
CHAPTER 1	
Introduction to Information Security	1
Running Case: You Must Be Joking	2
Introduction	2
What Is Information Security?	3
Critical Characteristics of Information	3
CNSS Security Model.	4
Balancing Information Security and Access	5
Business Needs First.	6
Security Professionals and the Organization.	6
Data Management.	7
Key Information Security Terminology.	8
Threats and Attacks.	8
Vulnerabilities and Exploits	9
Risk.	9
Security Perimeter and Defense in Depth.	10
Threats to Information Security	12
The TVA Triple	14
Other Ways to View Threats	16
Attacks on Information Assets	17
Malicious Code	18
Compromising Passwords	18
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS).	19
Spoofing	20
Man-in-the-Middle	20
E-Mail Attacks	21
Sniffers	21
Social Engineering	22
Buffer Overflow	22
Running Case: Connecting the Dots	23
Chapter Summary	23
Review Questions	24
Real World Exercises	25
Hands-On Projects	26
Project 1-1 Getting to Know Your Web Browser: Internet Explorer.	26
Project 1-2 Getting to Know Your Web Browser: Firefox.	27
Running Case Projects	28
Student Tasks.	30
Endnotes	30
CHAPTER 2	
Security Policies and Standards	33
Running Case: Why Would We Need a Policy?	34

Introduction 34

Information Security Policy, Standards, and Practices 35

 Enterprise Information Security Policy (EISP) 37

 Issue-Specific Security Policy (ISSP) 37

 Systems-Specific Policy (SysSP) 40

Frameworks and Industry Standards 41

 The ISO 27000 Series 41

 NIST Security Models 42

 IETF Security Architecture 47

 Benchmarking and Best Practices 47

Security Education, Training, and Awareness Program 49

 Security Education 49

 Security Training 50

 Security Awareness 50

Continuity Strategies 51

 Business Impact Analysis 53

 Incident Response Planning 56

 Disaster Recovery Planning 57

 Business Continuity Planning 58

 Crisis Management 59

Running Case: For Business Use Only 60

Chapter Summary 60

Review Questions 61

Real World Exercises 62

Hands-On Projects 63

 Project 2-1: Identifying Local Computer Security Policies 63

 Project 2-2: Incident Handling Form 64

Running Case Projects 65

 Student Tasks 65

Endnotes 65

CHAPTER 3

Authenticating Users 67

Running Case: Getting Them to Drink 68

Introduction 69

Access Controls 69

 Mandatory Access Control (MAC) 70

 Nondiscretionary Access Controls 72

 Discretionary Access Controls (DACs) 72

 Centralized vs. Decentralized Access Controls 73

The Authentication Process 73

How Firewalls Implement the Authentication Process 75

 Firewall Authentication Methods 75

Centralized Authentication 78

 Kerberos 79

 TACACS+ 80

 RADIUS 81

 TACACS+ and RADIUS Compared 81

Password Security Issues 83

 Preventing Passwords from Being Cracked 83

One-Time Password Software	84
Other Authentication Systems	84
Certificate-Based Authentication	84
802.1x Wi-Fi Authentication	84
Running Case: Start at the Beginning	85
Chapter Summary	86
Review Questions	86
Real World Exercises	87
Hands-On Projects	88
Project 3-1: The Microsoft Security Compliance Manager	88
Project 3-2: Microsoft Baseline Security Analyzer	92
Running Case Projects	94
Student Tasks	94
Endnotes	95

PART 2

Firewalls

CHAPTER 4

Introduction to Firewalls	97
Running Case: A \$50 Router	98
Introduction	98
Firewalls Explained	99
Misconceptions about Firewalls	100
An Analogy: Office Tower Security Guard	100
Firewall Security Features	101
Firewall Network Perimeter Security	101
Firewall Components	102
Firewall Security Tasks	103
Types of Firewall Protection	106
Packet Filtering	107
PAT and NAT	112
Application Layer Gateways	114
Firewall Categories	117
Processing Mode	117
Firewall Generations	119
Firewall Structures	119
Firewall Architectures	127
Limitations Of Firewalls	130
Running Case: Apology Accepted	130
Chapter Summary	131
Review Questions	132
Real World Exercises	133
Hands-On Projects	133
Project 4-1: View Active Connections	133
Project 4-2: Do Your Own Manual “Port Scanning” at the Internet Assigned Numbers Authority (IANA) Web Site	134
Project 4-3: Determine Your Computer’s IP Address	134

Running Case Projects **135**
 Student Tasks 135
Endnotes **141**

CHAPTER 5

Packet Filtering **143**
 Running Case: Not My Job **144**
 Introduction **144**
 Understanding Packets and Packet Filtering **145**
 Packet-Filtering Devices 145
 Anatomy of a Packet 145
 Packet-Filtering Rules 148
 Packet-Filtering Methods **150**
 Stateless Packet Filtering 151
 Stateful Packet Filtering 156
 Filtering Based on Packet Content 157
 Setting Specific Packet Filter Rules **158**
 Best Practices for Firewall Rules 158
 Rules That Cover Multiple Variations 159
 Rules for ICMP Packets 159
 Rules That Enable Web Access 161
 Rules That Enable DNS 162
 Rules That Enable FTP 162
 Rules That Enable E-Mail 164
 Running Case: Unauthorized Personnel **165**
 Chapter Summary **165**
 Review Questions **165**
 Real World Exercises **166**
 Hands-On Projects **167**
 Project 5-1: Explore and Configure Windows Firewall (Vista or XP SP3) 167
 Project 5-2: Set Up Windows Packet Filtering 168
 Project 5-3: Use Windows IPSec Packet Filtering 169
 Project 5-4: Install and Configure ZoneAlarm Basic Firewall 170
 Running Case Projects **171**
 Student Tasks 172

CHAPTER 6

Firewall Configuration and Administration **179**
 Running Case: The Prohibition Era **180**
 Introduction **180**
 Establishing Firewall Rules and Restrictions **181**
 The Importance of the Rule Set 181
 Restrictive Firewalls 181
 Connectivity-Based Firewalls 182
 Firewall Configuration Strategies: A High-Level Overview **183**
 Scalability 183
 Productivity 183
 Dealing with IP Address Issues 184
 Approaches That Add Functionality to the Firewall **185**
 NAT/PAT 185

Encryption	186
Application Proxies	186
VPNs	186
Intrusion Detection and Prevention Systems	187
Enabling a Firewall to Meet New Needs	189
Verifying Resources Needed by the Firewall	190
Identifying New Risks	191
Adding Software Updates and Patches	192
Adding Hardware	192
Dealing with Complexity on the Network	193
Adhering to Proven Security Principles	194
Environmental Management	195
BIOS, Boot, and Screen Locks and Passwords	195
Remote Management Interface	196
Why Remote Management Tools Are Important	196
Security Concerns	197
Basic Features of Remote Management Tools	197
Automating Security Checks	197
Configuring Advanced Firewall Functions	198
Data Caching	198
Hot Standby Redundancy	199
Load Balancing	200
Filtering Content	200
Running Case: Actually, We Have Had a Problem	202
Chapter Summary	203
Review Questions	204
Real World Exercises	205
Hands-On Projects	206
Project 6-1: Draw a Simple Packet-Filtering Design	206
Project 6-2: Drawing a DMZ	206
Running Case Projects	207
Student Tasks	207
Endnotes	208

CHAPTER 7

Working with Proxy Servers and Application-Level Firewalls	209
Running Case: Gambling with the Company's Future	210
Introduction	210
Overview of Proxy Servers	211
How Proxy Servers Work	211
How Proxy Servers Differ from Packet Filters	213
Sample Proxy Server Configurations	213
Benefits of Proxy Servers	214
Concealing Internal Clients	214
Blocking URLs	215
Blocking and Filtering Content	216
E-Mail Proxy Protection	217
Improving Performance	217
Ensuring Security	217
Providing User Authentication	219
Redirecting URLs	219

Configuring Proxy Servers	219
Providing for Scalability	220
Working with Client Configurations	220
Working with Service Configurations	221
Creating Filter Rules	221
Recognizing the Single Point of Failure	222
Recognizing Buffer Overflow Vulnerabilities	223
Choosing a Proxy Server	223
Transparent Proxies	223
Nontransparent Proxies	223
SOCKS-Based Proxies	224
SocksCap	224
Proxy Server-Based Firewalls Compared	224
Squid	225
WinGate	225
Norton from Symantec	225
Microsoft Internet Security & Acceleration Server	226
Reverse Proxies	226
When a Proxy Server Isn't the Correct Choice	227
Running Case: Busted	228
Chapter Summary	228
Review Questions	229
Real World Exercises	230
Hands-On Projects	231
Project 7-1: Install and Configure NetProxy	231
Project 7-2: Configure a Client to Work with a Proxy	232
Project 7-3: Test Proxy Server Network Address Translation (NAT)	233
Running Case Projects	234
Student Tasks	234
CHAPTER 8	
Implementing the Bastion Host	237
Running Case: Dealing with Intruders	238
Introduction	238
Installing a Bastion Host: General Requirements	239
Selecting the Host Machine	240
Do You Need More Than One Machine?	240
Memory Considerations	240
Processor Speed	241
Choosing the Operating System	241
UNIX and Linux Hosts	242
Windows Hosts	242
Keep Your Operating System Updated	242
Positioning the Bastion Host	243
Physical Location	244
Network Location	245
Securing the Machine Itself	246
Selecting a Secure Location	246
Installing the Operating System Securely	247
Documenting Your Work	247
Configuring Your Bastion Host	248
Making the Host Defend Itself	248
Selecting Services to Be Provided	248

Special Considerations for UNIX Systems	249
Special Considerations for Windows Systems	249
Disabling Accounts	250
Disabling Unnecessary Services	250
Limiting Ports	251
Handling Backups	251
Auditing the Bastion Host	252
Connecting the Bastion Host	252
Running Case: Able to Hack It	253
Chapter Summary	253
Review Questions	254
Real World Exercises	255
Hands-On Projects	256
Project 8-1: Port Scanning with SuperScan for Windows	256
Project 8-2: Active Stack Fingerprinting Using Nmap	256
Project 8-3: Determining Which Services Are Functioning in a Windows System	257
Project 8-4: Microsoft Baseline Security Analyzer	258
Running Case Projects	258
Endnotes	259

PART 3

VPNs

CHAPTER 9

Encryption—The Foundation for the Virtual Private Network	261
Running Case: Secret Codes	262
Introduction	262
Encryption Overview	262
Principles of Cryptography	264
Encryption Definitions	264
Cryptographic Notation	265
Encryption Operations	265
Using Cryptographic Controls	273
E-Mail Security	274
Securing the Web	275
Securing Authentication	276
Attacks on Cryptosystems	277
Man-in-the-Middle	279
Correlation Attacks	279
Dictionary Attacks	279
Timing Attacks	280
Defending From Attacks	280
Running Case: I'll Take One of Those VPN Servers, Too	280
Chapter Summary	281
Review Questions	281
Real World Exercises	282
Hands-On Projects	283
Project 9-1: Using Truecrypt Encryption to Protect Files	283
Project 9-2: Sending Encrypted E-Mail with iSafeguard	285

Running Case Projects 290
 Student Tasks 290
Endnotes 292

CHAPTER 10

Setting Up a Virtual Private Network **293**
 Running Case: Second Time’s a Charm 294
 Introduction 294
 VPN Components and Operations 295
 VPN Components 295
 Essential Activities of VPNs 298
 Benefits and Drawbacks of VPNs 300
 VPNs Extend Network Boundaries 300
 Types of VPNs 301
 VPN Appliances 301
 Software VPN Systems 302
 VPN Combinations of Hardware and Software 303
 Mixed Vendor VPNs 303
 VPN Setups 303
 Mesh Configuration 303
 Hub-and-Spoke Configuration 304
 Hybrid Configuration 305
 Configurations and Extranet and Intranet Access 306
 Tunneling Protocols Used with VPNs 306
 IPSec/IKE 306
 PPTP 308
 L2TP 308
 PPP Over SSL and PPP Over SSH 308
 Enabling Remote Access Connections Within VPNs 309
 Configuring the Server 309
 Configuring Clients 311
 VPN Best Practices 311
 The Need for a VPN Policy 311
 Connecting from Personal Computers 312
 Packet Filtering and VPNs 312
 Auditing and Testing the VPN 315
 Running Case: Thinking Ahead 316
 Chapter Summary 317
 Review Questions 318
 Real World Exercises 319
 Hands-On Projects 319
 Project 10-1: A VPN Connection with Microsoft VPN Client 320
 Project 10-2: Remote Access with Microsoft Remote Desktop Protocol 321
 Endnotes 322

APPENDIX A

Setting Up and Operating a Software Firewall **323**

GLOSSARY **329**

INDEX **337**