



John R. Vacca
Scott R. Ellis

Firewalls

Jumpstart for

Network and

Systems

Administrators

Contents

Foreword	xvii
Introduction	xix
Acknowledgments	xxix
 Section I—Overview of Firewall Technology	 I
 I Firewalls: What Are They?	 3
1.1 Chapter objectives	3
1.2 Firewall defined	7
1.3 Why firewalls?	8
1.3.1 The need for firewalls	9
1.4 Benefits of firewalls	12
1.4.1 Protection from vulnerable services	13
1.4.2 Controlled access to site systems	13
1.4.3 Concentrated security	14
1.5 Enhanced privacy	15
1.5.1 Logging and statistics on network use and misuse	15
1.5.2 Policy enforcement	15
1.6 Limitations of firewalls	16
1.6.1 What about viruses?	18
1.7 Summary	19
1.8 References	21
 2 Type of Firewall Security Policy	 23
2.1 Chapter objectives	23
2.2 Firewall protection	24

2.3	Firewall architectures	25
2.3.1	Multi-homed host	25
2.3.2	Screened host	26
2.3.3	Screened subnet	26
2.4	Types of firewalls	26
2.4.1	Packet-filtering gateways	27
2.4.2	Application gateways	28
2.4.3	Hybrid or complex gateways	29
2.5	Issues	29
2.5.1	Authentication	30
2.5.2	Routing versus forwarding	30
2.5.3	Source routing	30
2.5.4	IP spoofing	31
2.5.5	DNS and mail resolution	31
2.6	Intranet	32
2.7	Network trust relationships	33
2.7.1	High	33
2.7.2	Low to medium	33
2.8	Virtual private networks	34
2.9	Firewall administration	34
2.9.1	Qualification of the firewall administrator	35
2.9.2	Remote firewall administration	35
2.9.3	User accounts	36
2.9.4	Firewall backup	37
2.9.5	System integrity	37
2.9.6	Documentation	38
2.9.7	Physical firewall security	38
2.9.8	Firewall incident handling	39
2.9.9	Restoration of services	39
2.9.10	Upgrading the firewall	40
2.9.11	Logs and audit trails: audit/event reporting and summaries	40
2.10	Revision/update of firewall policy	41
2.11	Examples of service-specific policies	44
2.12	Summary	48
2.13	References	48

3 Firewall Types 49

3.1	Chapter objectives	49
3.2	Types of firewalls	50
3.2.1	Simple packet filtering: IP or filtering firewalls	50

3.2.2	Application-layer firewalls: proxy servers	53
3.2.3	Stateful multilayer-inspection firewalls	54
3.3	Understanding firewall types	55
3.4	Firewall types drawbacks	55
3.5	Summary	56
3.6	References	57

Section II—Firewall Topologies 59

4 Choosing the Right Firewall 61

4.1	Chapter objectives	61
4.2	Convergence	63
4.2.1	The criminal meagermind	63
4.2.2	Considerations	65
4.2.3	Products	70
4.3	About packet inspection	72
4.3.1	Selecting a firewall	72
4.3.2	Firewall solutions	75
4.4	Summary	90

5 Defense in Depth: Firewall Topologies 93

5.1	Chapter objectives	93
5.2	Virtual private network	94
5.2.1	Remote office VPN	96
5.2.2	Remote user VPN	96
5.2.3	Point-to-point tunneling protocol VPN	97
5.2.4	Authenticating with a remote access dial-in user service server	97
5.3	Firewall policies	97
5.3.1	How secure is VPN technology?	98
5.3.2	Document access	99
5.4	Setting up a demilitarized zone: A VPN alternative?	100
5.4.1	Uses	100
5.4.2	Theory of operation	100
5.4.3	Managing ports in a DMZ	103
5.4.4	DMZ topology	106
5.5	Summary	110

Section III—Firewall Installation and Configuration **111**

6 Installation Preparation **113**

6.1	Chapter objectives	113
6.2	Unbreakable walls	114
6.3	Selecting an operating system	115
6.3.1	Microsoft	115
6.3.2	UNIX	121
6.4	Scanning for vulnerabilities	124
6.4.1	Searching for weaknesses	124
6.5	Summary	129

7 Firewall Configuration **131**

7.1	Chapter objectives	131
7.2	Defining firewall security objects	131
7.2.1	Object discovery process	132
7.2.2	Post object discovery evaluation	134
7.3	Scanning the firewall and fixing vulnerabilities	135
7.3.1	Tracing the routes	135
7.3.2	Perimeter packet analysis	140
7.4	Identifying trusted and untrusted networks	142
7.4.1	The firewall stops here	142
7.4.2	Creating trusted networks	144
7.5	Summary	145

Section IV—Supporting Outgoing Services Through Firewall Configuration **147**

8 Simple Policy Implementation **149**

8.1	Chapter objectives	149
8.2	Policy configuration	150
8.2.1	Interface	150
8.2.2	Source	151
8.2.3	Destination	151
8.2.4	Services	152
8.3	Supporting HTTP	153
8.3.1	Web access control	154
8.3.2	HTTP as a policy	155

8.4	Dynamic content	156
8.5	Summary	157

9 Complex Web Services Management 159

9.1	Chapter objectives	159
9.2	Telnet	161
9.3	FTP	161
9.3.1	The role of FTP	162
9.3.2	FTP access	163
9.3.3	FTP sessions	163
9.3.4	FTP and firewalls	164
9.3.5	Netstat	164
9.3.6	FTP security	164
9.3.7	Alternatives	164
9.4	Handling port numbers	165
9.5	Deploying Real Audio	170
9.5.1	Outgoing versus incoming	170
9.5.2	Flexibility	171
9.6	Summary	172

10 Content Filtering 175

10.1	Chapter objectives	175
10.2	Filtering out dangerous content	175
10.2.1	Scanning e-mail	177
10.2.2	Web filtering	178
10.2.3	Application filtering	182
10.3	Summary	184

Section V—Secure External Services Provision 185

11 Publicly Accessible Servers Implementation 187

11.1	Chapter objectives	187
11.2	Securing your organization's Internet site	187
11.2.1	Pros and cons	188
11.2.2	Special concerns	193
11.3	Separating your Internet site from your intranet	197
11.4	Supporting SMTP mail architectures	199
11.4.1	Internal e-mail	201
11.5	Summary	201

12 Architecture Selection **203**

12.1	Chapter objectives	203
12.2	Types of screened subnet architectures	203
12.2.1	The perimeter	205
12.2.2	Two routers	207
12.2.3	Single router	208
12.2.4	Multiple screened subnet architecture	208
12.2.5	Screened host	210
12.2.6	Dual-homed host	210
12.3	Single-box architecture	213
12.4	Summary	215

13 External Servers Protection **217**

13.1	Chapter objectives	217
13.2	Siting external servers on a perimeter net	217
13.2.1	Security of SQL and web servers	219
13.2.2	Search engines	222
13.2.3	SQL server security	224
13.3	Deploying packet filtering to control access to your servers	225
13.4	Router packet filtering	226
13.5	Using router access control lists	227
13.6	Summary	227

Section VI—Internal IP Services Protection **229**

14 Internal IP Security Threats: Beyond the Firewall **231**

14.1	Chapter objectives	231
14.2	Network threats	232
14.2.1	Behavior of employees	232
14.2.2	E-mail	234
14.2.3	Viruses	234
14.2.4	Spyware	235
14.2.5	Hackers	236
14.3	Organization risk assessment	236
14.4	Examining inside attacks	238
14.4.1	Saboteurs	238
14.4.2	Leaky e-mail	239
14.5	Handling new threats	239
14.6	Antivirus software technology: Beyond the firewall	240
14.6.1	Layered approach	241

14.6.2	Intrusion detection tools	242
14.6.3	Public key infrastructure	243
14.6.4	Security content	244
14.7	Summary	247
14.8	References	247

15 Network Address Translation Deployment 249

15.1	Chapter objectives	249
15.2	Person-to-person communication	249
15.3	Internet protocol telephony	250
15.4	Routers, firewalls, and NATs	251
15.5	Handling SIP	251
15.6	Firewall traversal/SIP NAT	252
15.7	Employing a Linux-based SOHO firewall solution with NAT technology	253
15.7.1	Realities of securing SOHOs with firewall protection	257
15.7.2	Hardware and software solutions options	260
15.7.3	Employing a Linux-based SOHO firewall solution	263
15.7.4	Plugging the SOHO firewall leaks	265
15.8	Summary	267
15.9	References	268

Section VII—Firewall Remote Access Configuration 269

16 Privacy and Authentication Technology 271

16.1	Chapter objectives	271
16.2	Selecting cryptographic algorithms through encryption	273
16.2.1	Data Encryption Standard	273
16.2.2	3DES	273
16.2.3	Advanced Encryption Standard	273
16.2.4	RC4	273
16.2.5	Message Digest and Secure Hash Algorithm	274
16.2.6	Asymmetric Key Algorithms	274
16.2.7	Additional cryptographic options: modes and initialization vectors	274
16.2.8	Options in padding	274
16.3	Key management	275
16.3.1	Administration and storage centralization	275
16.3.2	Specialized hardware	275
16.3.3	Importing a key	275

16.3.4	Exporting a key	276
16.3.5	Rotating keys	276
16.4	Auditing, authentication, and authorization	276
16.4.1	Authentication	276
16.4.2	Authorization	277
16.4.3	Auditing	277
16.4.4	Secure the credentials	277
16.4.5	Disaster recovery, backup, and restore	278
16.5	High availability and load balancing	278
16.5.1	Key replication services	278
16.6	Transport and network	278
16.6.1	Firewalls	279
16.7	Encryption of multiple columns: database considerations	279
16.7.1	Creating indexes	279
16.7.2	Primary key encryption	279
16.7.3	Foreign key constraint	280
16.7.4	Randomly generated initialization vectors	280
16.7.5	Exact match searching	281
16.7.6	Encrypted data encoding	281
16.7.7	Additional space	281
16.7.8	Backups during pre-migration	282
16.8	Summary	282
16.9	References	283

17	Tunneling: Firewall-to-Firewall	285
17.1	Chapter objectives	285
17.2	Increasing risk on extranets and intranets	286
17.3	Openness with protection of firewall tunneling and Internet security solutions	286
17.4	Firewall tunneling and Internet security architecture technologies	287
17.4.1	Protection solutions for the intranet	287
17.4.2	Protection solutions for the extranet and Internet	289
17.5	Firewall tunneling technologies	289
17.5.1	Application proxies	289
17.5.2	Encryption with virtual private network	290
17.5.3	Management center	290
17.5.4	Stateful IP filtering	290
17.5.5	Static IP filtering	291
17.6	Demilitarized zone focus	291
17.6.1	Isolating the machine	291

17.6.2	Controlling the flow	291
17.6.3	Controlling remote access	291
17.6.4	Authentication mechanisms	292
17.7	Keeping the firewall tunneling security rules up-to-date through enterprise intranets	292
17.8	Summary	293
17.8.1	A high level of trust	293
17.8.2	Centralized security management	293
17.8.3	Enterprise-class scalability	294
17.8.4	High-end firewall tunneling protection	294
17.9	References	295

Section VIII—Firewall Management 297

18 Auditing and Logging 299

18.1	Chapter objectives	299
18.2	Auditing your firewall	299
18.2.1	Methodology	300
18.3	Logging	302
18.3.1	Configuration of firewall logging	303
18.3.2	Firewall monitoring	307
18.4	Summary	308
18.5	References	309

19 Firewall Administration 311

19.1	Chapter objectives	311
19.2	System administration	312
19.3	Managing your firewall remotely	312
19.3.1	Achieving high uptime	313
19.3.2	External and internal solution monitors	316
19.4	Maintenance of a firewall	317
19.4.1	Performing firewall maintenance	318
19.5	Managing firewall security	321
19.5.1	Firewall products common functionality	321
19.5.2	Analysis and activity reporting of firewalls	323
19.5.3	Enterprise firewalls: automated event response and Real-Time monitoring	323
19.6	Summary	326
19.7	References	327

20 Summary, Conclusions, and Recommendations	329
20.1 Chapter objectives	329
20.2 Summary	330
20.3 Conclusions	331
20.4 Recommendations	332
20.4.1 Purchasing, learning, configuring, and maintaining	335
20.4.2 Effective firewall security: baseline design principles	336
20.4.3 Final recommendation: purchase a high-speed firewall	338
20.5 References	339

Section IX—Appendixes	341
------------------------------	------------

A Contributors of Firewall Software	343
B Worldwide Survey of Firewall Products	349
C Firewall Companies	353
D Commercial Products or Consultants Who Sell or Service Firewalls	357
E Establishing Your Organization's Security	363
E.1 Firewalls	364
F Network Interconnections: A Major Point of Vulnerability	367
G Deterring Masqueraders and Ensuring Authenticity	371
G.1 Boundary Protection: firewalls	372
H Preventing Eavesdropping to Protect Your Privacy	381
I Thwarting Counterfeiters and Forgery to Retain Integrity Through a Reverse Firewall	385
J Avoiding Disruption of Service to Maintain Availability	391
K Developing Your Firewall Security Policy	393

Glossary	397
-----------------	------------

Index	407
--------------	------------