

# **Building Firewalls with OpenBSD and PF**

# **Building Firewalls with OpenBSD and PF**

**Jacek Artymiak**

**Second Edition**

**Lublin**

# Table of Contents

Preface ..... 1

0.1 Acknowledgments ..... 3

Chapter 1: Introduction ..... 5

1.1 Why Do We Need to Secure Our Networks ..... 5

1.2 Why Do We Need Firewalls ..... 7

1.3 Why Open Source Software ..... 7

1.4 Why OpenBSD and pf ..... 9

1.5 Cryptography and Law ..... 11

1.6 How This Book Is Organized ..... 12

1.7 Typographic Conventions Used in This Book ..... 14

1.8 Staying in Touch with the OpenBSD Community ..... 14

1.9 Getting in Touch with the Author ..... 15

Chapter 2: Firewall Designs ..... 17

2.1 Define Your Local Packet Filtering Policy ..... 17

2.2 What Is a ‘Firewall’? ..... 18

2.3 What Firewalls Are Not ..... 19

2.4 Hardware vs. Software Firewalls ..... 19

2.5 Firewalls Great and Small ..... 20

2.5.1 Screened Host ..... 20

2.5.2 Screened LAN or Screened LAN Segment ..... 22

2.5.3 Bastion Host ..... 24

2.5.4 Demilitarized Zone (DMZ) ..... 25

2.5.5 Large-Scale LANs ..... 27

2.6 Invisible Hosts and Firewalls ..... 27

2.6.1 Filtering Bridge ..... 28

2.6.2 Network Address Translation (NAT) ..... 30

2.7 Additional Functionality ..... 30

---

Chapter 3: Installing OpenBSD .....	33
3.1 Software Requirements .....	33
3.1.1 Buy Official OpenBSD CD-ROM Sets .....	34
3.1.2 Additional Software Requirements .....	35
3.2 Hardware Requirements .....	36
3.2.1 Which Hardware Platform Should You Choose? .....	36
3.2.2 Motherboard .....	38
3.2.3 BIOS .....	39
3.2.4 Processor .....	39
3.2.5 Memory .....	41
3.2.6 Disk Space .....	42
3.2.7 Network Interfaces .....	43
3.2.8 Communicating with Your Computer During Installation .....	46
3.2.9 How Are You Going to Install OpenBSD? .....	48
3.2.10 Tape Drives .....	49
3.2.11 Debugging Hardware .....	49
3.2.12 Other Requirements .....	49
3.2.13 When in Trouble, Use the Manual .....	50
3.3 Downloading OpenBSD .....	50
3.4 Preparing Installation Media .....	51
3.5 Installing OpenBSD .....	52
3.6 Securing Your Firewall Hardware .....	65
Chapter 4: Configuring OpenBSD .....	67
4.1 User Management .....	67
4.1.1 Adding Users .....	67
4.1.2 Letting Users Do As Root Does (su) .....	68
4.1.3 Changing the User Password .....	69
4.1.4 Giving Users Limited Access to Root Privileges (sudo) .....	69
4.1.5 Removing Users .....	70
4.2 Hardening OpenBSD .....	70
4.2.1 Disabling Non-Essential Services .....	70
4.2.2 Patching .....	71
4.2.3 When a Patch Is Not Enough .....	76
4.3 Configuring Networking .....	76
4.3.1 More Than One Address on a Single Interface (Aliases) .....	78
4.3.2 Pf Configuration Options .....	80
4.3.3 Bridge Configuration Options .....	81

4.3.4 IP Forwarding .....	84
4.3.5 Fixing FTP .....	85
4.3.6 Taking Control of ARP .....	89
4.4 Automated System Reboot .....	95
4.5 Swap Encryption .....	95
4.6 Working with Securelevels .....	96
4.7 Setting Time and Date .....	97
4.8 Configuring the Kernel to Solve Hardware Problems .....	97
4.8.1 Make a Copy of the Old Kernel .....	98
4.8.2 User Kernel Config (UKC) .....	98
4.8.3 Brain Transplants for OpenBSD .....	101
4.9 Adding and Compiling Software .....	101
4.10 Configuring Disks .....	102
4.10.1 RAID .....	102

## Chapter 5: /etc/pf.conf .....

5.1 Inside pf.conf .....	103
5.1.1 Changing the pf.conf Section Order .....	105
5.1.2 Breaking Long Lines into Smaller Pieces .....	105
5.1.3 Grouping Rule Elements into Lists ({} ) .....	105
5.2 Macros .....	106
5.3 Tables (table) .....	107
5.4 Anchors (anchor, nat-anchor, rdr-anchor, binat-anchor) .....	109
5.5 Common Components Found in pf Rules .....	110
5.5.1 Directions (in, out) .....	110
5.5.2 Interfaces (on) .....	110
5.5.3 Address Families (inet, inet6) .....	111
5.5.4 Protocols (proto) .....	111
5.5.5 Addresses (from, to, any, all) .....	112
5.5.6 Dynamic Assignment of Addresses .....	115
5.5.7 Ports (port) .....	116
5.5.8 Ports (port) .....	118
5.6 Tools for Writing and Editing pf.conf .....	119
5.6.1 Why Not Edit pf.conf on Another Machine? .....	119
5.6.2 Syntax Highlighting .....	119
5.6.3 GUI Tools for Writing Rulesets with a Mouse .....	120
5.6.4 Scripting pf.conf .....	120
5.7 Managing pf.conf Versions with CVS .....	120

---

**Chapter 6: Packet Normalization ... 125**

- 6.1 Implementing Packet Normalization (scrub) ..... 125
  - 6.1.1 Scrub Rule Syntax ..... 125
  - 6.2 Fine-Tuning Scrub Rules ..... 127
    - 6.2.1 Pf Options (limit frags, timeout frags) ..... 128
    - 6.2.2 Scrub Rule Options ..... 128
  - 6.3 Who's Sending All Those Malformed Packets? ..... 131

**Chapter 7: Packet Redirection .... 133**

- 7.1 Security Applications ..... 133
- 7.2 Expanding the IPv4 Address Space ..... 134
  - 7.2.1 Does IPv6 Make NAT redundant? ..... 136
  - 7.2.2 What Problems Does NAT Cause? ..... 136
- 7.3 NAT Rules ..... 137
  - 7.3.1 Hiding Hosts Behind a Single Address with nat Rules ..... 138
  - 7.3.2 Redirecting Packets to Other Addresses and Ports (rdr) ..... 145
  - 7.3.3 Forcing Everyone to Use a Web Cache ..... 150
  - 7.3.4 Other Uses of rdr Rules ..... 150
  - 7.3.5 binat ..... 150
- 7.4 Proxy ARP ..... 153

**Chapter 8: Packet Filtering ... 155**

- 8.1 The Anatomy of a Filtering Rule ..... 155
  - 8.1.1 What Is pf Supposed to Do (block, pass)? ..... 156
  - 8.1.2 Return to Sender (return-icmp, return-rst) ..... 157
  - 8.1.3 Inbound or Outbound (in, out)? ..... 160
  - 8.1.4 To Log or Not to Log (log, log-all)? ..... 160
  - 8.1.5 Finishing Early (quick) ..... 161
  - 8.1.6 Network Interface Names (on)? ..... 162
  - 8.1.7 Routing Options (fastroute, reply-to, route-to, dup-to) ..... 162
  - 8.1.8 IP Addressing Families: IPv4 (inet) or IPv6 (inet6)? ..... 164
  - 8.1.9 Protocols (proto)? ..... 165
  - 8.1.10 Source Address (from, any, all)? ..... 165
  - 8.1.11 Source Port (port)? ..... 166
  - 8.1.12 Sender's Operating System (os)? ..... 168
  - 8.1.13 Destination IP address (to, any, all) ..... 169
  - 8.1.14 Destination Port (port) ..... 170

8.1.15 User and Group Access Control (user, group) .....	170
8.1.16 TCP Flags (flags) .....	171
8.1.17 ICMP Packets .....	172
8.1.18 Stateful Filtering (keep state, modulate state, synproxy state) ...	173
8.1.19 IP Options (allow-opts) .....	179
8.1.20 Labels (label) .....	180
8.2 Antispoof Rules .....	180
8.3 Filtering Rules for Redirected Packets .....	181
Chaper 9: Dynamic Rulesets .....	185
9.1 Designig an Automated Firewall .....	185
Chaper 10: Bandwidth Shaping and Load Balancing .....	191
10.1 Load Balancing .....	191
10.1.1 Implementing Load Balancing .....	193
10.2 Bandwidth Shaping .....	195
10.2.1 The Anatomy of a Scheduler Rule .....	196
10.2.2 The Anatomy of a Queue Rule .....	197
10.2.3 Assigning Queues to Packet Filtering Rules .....	199
10.2.4 Priority Queuing (PRIQ) .....	199
10.2.5 Class-Based Queuing (CBQ) .....	206
10.2.6 Hierarchical Fair Service Curve (HFSC) .....	213
10.2.7 Queuing Incoming Packets .....	218
10.2.8 Which Scheduler is Best? .....	218
Chapter 11: Logging and Log Analysis .....	221
11.1 Enabling Packet Logging .....	222
11.2 Log Analysis .....	222
11.3 Which Packets Do You Want to Capture? .....	224
11.4 The Secret Life of Logs .....	226
11.5 Bandwidth and Disk Space Requirements .....	229
11.6 Logging on a Bridge (Span Ports) .....	232
Chapter 12: Using authpf .....	233
12.1 Configuring authpf .....	233
12.2 Configuring sshd .....	234

---

12.3 Configuring Login Shell .....	234
12.4 Writing pf Rules for authpf .....	235
12.i5 Authenticating User Joe .....	235
 Chapter 13: Using spamd .....	 239
13.1 Configuring spamd .....	239
 Chapter 14: Ruleset Optimization .....	 245
14.1 The pf Optimization Checklist .....	245
14.2 Pf Optimization Options .....	246
 Chapter 15: Testing Your Firewall .....	 249
15.1 Pencil Test .....	249
15.2 Checking Host Availability .....	250
15.2.1 When Ping Cannot Help .....	252
15.3 Discovering Open Ports on Remote Hosts .....	253
15.4 Testing Network Performance .....	253
15.5 Are packets passing through pf? .....	256
15.6 Additional tools .....	258
 Chapter 16: Firewall Management .....	 259
16.1 General Operations .....	259
16.2 Pftcl Output Control Options .....	259
16.3 Managing Rulesets .....	260
16.4 Managing Macros .....	260
16.5 Managing Tables .....	260
16.6 Managing pf Options .....	262
16.7 Managing Queues .....	262
16.8 Managing Packet Redirection Rules .....	262
16.9 Managing Packet Filtering Rules .....	263
16.10 Managing Anchors .....	263
16.11 Managing States .....	264
16.12 Managing Operating System Fingerprints .....	265
16.13 Statistics .....	265
16.14 Additional Tools for Managing pf .....	266

Appendix A: Manual Pages ...	267
A.1 Using the OpenBSD Manual .....	267
A.1.1 Reading the OpenBSD Manual Pages on the Web .....	268
A.2 Pages Related to pf .....	268
A.3 Other Pages of Interest .....	269
Appendix B: Rules for Poplar (and Less Popular) Services .....	271
B.1 Dealing with ICMP .....	273
B.2 Fixing FTP .....	276
B.3 Template Rules for Services Using TCP and UDP .....	276
B.4 Adapting the Template for Other Services .....	283
Appendix C: Rule Templates for Typical Firewall Configurations .....	287
C.1 Bastion Host .....	287
C.2 Bastion Host II (Some Access Allowed) .....	288
C.3 Screened Host/LAN (Public IP Addresses) .....	289
C.4 Screened LAN (Some Access Allowed) .....	290
C.5 NAT + Screened LAN .....	292
C.6 NAT + Screened LAN + DMZ .....	293
C.7 Invisible Bridge .....	295
Appendix D: Helping OpenBSD and PF .....	297
D.1 Buy Official CD-ROMs, T-Shirts, and Posters .....	297
D.2 Make Small, but Regular Donations .....	298
D.3 Hire Developers of OpenBSD and Pf .....	299
D.4 Donate Hardware .....	300
D.5 Spare Some of Your Precious Time .....	300
D.6 Spread the Word .....	301
D.7 Attend Training Seminars .....	301
D.8 Encourage People to Buy this Book .....	301
Bibliography .....	303
Index .....	307
About this Book .....	322