

# CONTENTS IN DETAIL

<b>FOREWORD by Bob Beck (from the first edition)</b>	<b>xv</b>
--	-----------

<b>ACKNOWLEDGMENTS</b>	<b>xvii</b>
------------------------	-------------

<b>INTRODUCTION</b>	<b>xix</b>
---------------------	------------

This Is Not a HOWTO	xx
What This Book Covers	xx

<b>1</b>	
<b>BUILDING THE NETWORK YOU NEED</b>	<b>1</b>

Your Network: High Performance, Low Maintenance, and Secure	1
Where the Packet Filter Fits In	3
The Rise of PF	3
If You Came from Elsewhere	6
Pointers for Linux Users	6
Frequently Answered Questions About PF	7
A Little Encouragement: A PF Haiku	9

<b>2</b>	
<b>PF CONFIGURATION BASICS</b>	<b>11</b>

The First Step: Enabling PF	12
Setting Up PF on OpenBSD	12
Setting Up PF on FreeBSD	13
Setting Up PF on NetBSD	15
A Simple PF Rule Set: A Single, Stand-Alone Machine	16
A Minimal Rule Set	16
Testing the Rule Set	18
Slightly Stricter: Using Lists and Macros for Readability	18
A Stricter Baseline Rule Set	19
Reloading the Rule Set and Looking for Errors	20
Checking Your Rules	21
Testing the Changed Rule Set	22
Displaying Information About Your System	22
Looking Ahead	24

<b>3</b>	
<b>INTO THE REAL WORLD</b>	<b>25</b>

A Simple Gateway	25
Keep It Simple: Avoid the Pitfalls of in, out, and on	26
Network Address Translation vs. IPv6	27
Final Preparations: Defining Your Local Network	29
Setting Up a Gateway	29
Testing Your Rule Set	34

That Sad Old FTP Thing . . . . .	35
If We Must: ftp-proxy with Divert or Redirect . . . . .	36
Variations on the ftp-proxy Setup . . . . .	37
Making Your Network Troubleshooting-Friendly . . . . .	37
Do We Let It All Through? . . . . .	38
The Easy Way Out: The Buck Stops Here . . . . .	39
Letting ping Through . . . . .	39
Helping traceroute . . . . .	40
Path MTU Discovery . . . . .	40
Tables Make Your Life Easier . . . . .	42

## **4 WIRELESS NETWORKS MADE EASY 45**

A Little IEEE 802.11 Background . . . . .	46
MAC Address Filtering . . . . .	46
WEP . . . . .	47
WPA . . . . .	47
The Right Hardware for the Task . . . . .	48
Setting Up a Simple Wireless Network . . . . .	48
An OpenBSD WPA Access Point . . . . .	51
A FreeBSD WPA Access Point . . . . .	52
The Access Point's PF Rule Set . . . . .	53
Access Points with Three or More Interfaces . . . . .	54
Handling IPSec, VPN Solutions . . . . .	55
The Client Side . . . . .	55
OpenBSD Setup . . . . .	56
FreeBSD Setup . . . . .	58
Guarding Your Wireless Network with authpf . . . . .	59
A Basic Authenticating Gateway . . . . .	60
Wide Open but Actually Shut . . . . .	62

## **5 BIGGER OR TRICKIER NETWORKS 65**

A Web Server and Mail Server on the Inside: Routable IPv4 Addresses . . . . .	66
A Degree of Separation: Introducing the DMZ . . . . .	70
Sharing the Load: Redirecting to a Pool of Addresses . . . . .	72
Getting Load Balancing Right with relayd . . . . .	73
A Web Server and Mail Server on the Inside—The NAT Version . . . . .	79
DMZ with NAT . . . . .	80
Redirection for Load Balancing . . . . .	81
Back to the Single NATed Network . . . . .	81
Filtering on Interface Groups . . . . .	84
The Power of Tags . . . . .	85
The Bridging Firewall . . . . .	86
Basic Bridge Setup on OpenBSD . . . . .	87
Basic Bridge Setup on FreeBSD . . . . .	88
Basic Bridge Setup on NetBSD . . . . .	89
The Bridge Rule Set . . . . .	90

Handling Nonroutable IPv4 Addresses from Elsewhere . . . . .	91
Establishing Global Rules . . . . .	91
Restructuring Your Rule Set with Anchors . . . . .	91
How Complicated Is Your Network?—Revisited . . . . .	94

## **6 TURNING THE TABLES FOR PROACTIVE DEFENSE 95**

Turning Away the Brutes . . . . .	96
SSH Brute-Force Attacks . . . . .	96
Setting Up an Adaptive Firewall . . . . .	97
Tidying Your Tables with pftcl . . . . .	99
Giving Spammers a Hard Time with spamd . . . . .	100
Network-Level Behavior Analysis and Blacklisting . . . . .	100
Greylisting: My Admin Told Me Not to Talk to Strangers . . . . .	104
Tracking Your Real Mail Connections: spamlogd . . . . .	108
Greytrapping . . . . .	109
Managing Lists with spamdb . . . . .	111
Detecting Out-of-Order MX Use . . . . .	113
Handling Sites That Do Not Play Well with Greylisting . . . . .	113
Spam-Fighting Tips . . . . .	115

## **7 TRAFFIC SHAPING WITH QUEUES AND PRIORITIES 117**

Always-On Priority and Queues for Traffic Shaping . . . . .	118
Shaping by Setting Traffic Priorities . . . . .	119
Introducing Queues for Bandwidth Allocation . . . . .	121
Using Queues to Handle Unwanted Traffic . . . . .	130
Transitioning from ALTQ to Priorities and Queues . . . . .	131
Directing Traffic with ALTQ . . . . .	133
Basic ALTQ Concepts . . . . .	134
Queue Schedulers, aka Queue Disciplines . . . . .	134
Setting Up ALTQ . . . . .	135
Priority-Based Queues . . . . .	136
Using ALTQ Priority Queues to Improve Performance . . . . .	136
Using a match Rule for Queue Assignment . . . . .	137
Class-Based Bandwidth Allocation for Small Networks . . . . .	139
A Basic HFSC Traffic Shaper . . . . .	140
Queuing for Servers in a DMZ . . . . .	142
Using ALTQ to Handle Unwanted Traffic . . . . .	144
Conclusion: Traffic Shaping for Fun, and Perhaps Even Profit . . . . .	145

## **8 REDUNDANCY AND RESOURCE AVAILABILITY 147**

Redundancy and Failover: CARP and pfsync . . . . .	148
The Project Specification: A Redundant Pair of Gateways . . . . .	148
Setting Up CARP . . . . .	150
Keeping States Synchronized: Adding pfsync . . . . .	154
Putting Together a Rule Set . . . . .	155
CARP for Load Balancing . . . . .	157

## **9 LOGGING, MONITORING, AND STATISTICS** **161**

PF Logs: The Basics . . . . .	162
Logging the Packet's Path Through Your Rule Set: log (matches) . . . . .	164
Logging All Packets: log (all). . . . .	165
Logging to Several pflog Interfaces . . . . .	167
Logging to syslog, Local or Remote . . . . .	167
Tracking Statistics for Each Rule with Labels . . . . .	169
Additional Tools for PF Logs and Statistics . . . . .	171
Keeping an Eye on Things with systat . . . . .	171
Keeping an Eye on Things with pftop . . . . .	173
Graphing Your Traffic with pfstat . . . . .	173
Collecting NetFlow Data with pflow(4). . . . .	176
Collecting NetFlow Data with pfflowd . . . . .	182
SNMP Tools and PF-Related SNMP MIBs . . . . .	182
Log Data as the Basis for Effective Debugging . . . . .	183

## **10 GETTING YOUR SETUP JUST RIGHT** **185**

Things You Can Tweak and What You Probably Should Leave Alone . . . . .	185
Block Policy . . . . .	186
Skip Interfaces . . . . .	187
State Policy . . . . .	187
State Defaults . . . . .	188
Timeouts . . . . .	188
Limits . . . . .	189
Debug . . . . .	190
Rule Set Optimization . . . . .	191
Optimization . . . . .	192
Fragment Reassembly . . . . .	192
Cleaning Up Your Traffic . . . . .	193
Packet Normalization with scrub: OpenBSD 4.5 and Earlier . . . . .	193
Packet Normalization with scrub: OpenBSD 4.6 Onward . . . . .	193
Protecting Against Spoofing with antispoof. . . . .	194
Testing Your Setup . . . . .	195
Debugging Your Rule Set . . . . .	197
Know Your Network and Stay in Control. . . . .	199

## **A RESOURCES** **201**

General Networking and BSD Resources on the Internet . . . . .	201
Sample Configurations and Related Musings . . . . .	203
PF on Other BSD Systems . . . . .	204
BSD and Networking Books . . . . .	204
Wireless Networking Resources . . . . .	205
spamd and Greylisting-Related Resources . . . . .	205
Book-Related Web Resources. . . . .	206
Buy OpenBSD CDs and Donate! . . . . .	206

<b>B</b>	
<b>A NOTE ON HARDWARE SUPPORT</b>	<b>207</b>
Getting the Right Hardware. . . . .	208
Issues Facing Hardware Support Developers . . . . .	209
How to Help the Hardware Support Efforts . . . . .	210
<b>INDEX</b>	<b>211</b>