

# CONTENTS IN DETAIL

<b>FOREWORD by Bob Beck</b>	<b>xi</b>
-----------------------------	-----------

<b>PREFACE</b>	<b>xiii</b>
----------------	-------------

About the Book and Thanks .....	xiv
If You Came from Elsewhere .....	xvi
PF looks really cool. Can I run PF on my Linux machine? .....	xvi
I know some Linux, but I need to learn some BSD. Any pointers? .....	xvi
Can you recommend a GUI tool for managing my PF rule set? .....	xvii
Is there a tool I can use to convert my OtherProduct® setup to a PF configuration? .....	xviii
Where can I find out more? .....	xviii
A Little Encouragement: A PF Haiku .....	xix

<b>1</b>	
<b>WHAT PF IS</b>	<b>1</b>

Packet Filter? Firewall? A Few Important Terms Explained .....	3
Network Address Translation .....	3
Why the Internet Lives on a Few White Lies .....	4
Internet Protocol, Version 6 on the Far Horizon .....	4
The Temporary Masquerade Solution Called NAT .....	5
PF Today .....	6

<b>2</b>	
<b>LET'S GET ON WITH IT</b>	<b>7</b>

Simplest Possible PF Setup on OpenBSD .....	8
Simplest Possible PF Setup on FreeBSD .....	9
Simplest Possible PF Setup on NetBSD .....	10
First Rule Set—A Single, Stand-Alone Machine .....	11
Slightly Stricter, with Lists and Macros .....	13
Statistics from pfctl .....	15

<b>3</b>	
<b>INTO THE REAL WORLD</b>	<b>17</b>

A Simple Gateway, NAT If You Need It .....	17
Gateways and the Pitfalls of in, out, and on .....	18
What Is Your Local Network, Anyway? .....	19
Setting Up .....	19
Testing Your Rule Set .....	23
That Sad Old FTP Thing .....	24
FTP Through NAT: ftp-proxy .....	25
FTP, PF, and Routable Addresses: ftpsesame, pftpx, and ftp-proxy .....	26
New-Style FTP: ftp-proxy .....	26

Making Your Network Troubleshooting Friendly .....	28
Then, Do We Let It All Through? .....	28
The Easy Way Out: The Buck Stops Here .....	29
Letting ping Through .....	29
Helping traceroute .....	29
Path MTU Discovery .....	30
Tables Make Your Life Easier .....	31

## **4 WIRELESS NETWORKS MADE EASY 33**

A Little IEEE 802.11 Background .....	33
MAC Address Filtering .....	34
WEP .....	35
WPA .....	35
Picking the Right Hardware for the Task .....	35
Setting Up a Simple Wireless Network .....	36
The Access Point's PF Rule Set .....	38
If Your Access Point Has Three or More Interfaces .....	38
Handling IPsec, VPN Solutions .....	39
The Client Side .....	40
Guarding Your Wireless Network with authpf .....	40
A Basic Authenticating Gateway .....	41
Wide Open but Actually Shut .....	43

## **5 BIGGER OR TRICKIER NETWORKS 45**

When Others Need Something in Your Network: Filtering Services .....	45
A Webserver and a Mail Server on the Inside—Routable Addresses .....	46
Getting Load Balancing Right with hoststated .....	51
A Webserver and a Mail Server on the Inside—The NAT Version .....	56
Back to the Single NATed Network .....	57
Filtering on Interface Groups .....	59
The Power of Tags .....	60
The Bridging Firewall .....	61
Basic Bridge Setup on OpenBSD.....	61
Basic Bridge Setup on FreeBSD.....	62
Basic Bridge Setup on NetBSD.....	63
The Bridge Rule Set .....	64
Handling Nonroutable Addresses from Elsewhere .....	65

## **6 TURNING THE TABLES FOR PROACTIVE DEFENSE 67**

Turning Away the Brutes .....	68
You May Not Need to Block All of Your Overloaders .....	70
Tidying Your Tables with pfctl .....	70
The Forerunner: expiretable .....	71

Giving Spammers a Hard Time with spamd .....	71
Remember, You Are Not Alone: Blacklisting .....	72
Greylisting: My Admin Told Me Not to Talk to Strangers .....	75
Some Highlights of Day-to-Day spamd Use .....	78
Handling Sites That Do Not Play Well with Greylisting .....	83
Conclusions from Our spamd Experience .....	84

## **7** **QUEUES, SHAPING, AND REDUNDANCY** **87**

Directing Traffic with ALTQ .....	87
Basic ALTQ Concepts .....	88
Queue Schedulers, aka Queue Disciplines .....	88
Setting Up ALTQ .....	89
Understanding Priority-Based Queues (priq) .....	91
Class-Based Bandwidth Allocation for Small Networks (cbq) .....	93
Queuing for Servers in a DMZ .....	94
Using ALTQ to Handle Unwanted Traffic .....	96
Redundancy and Failover: CARP and pfsync .....	97
The Project Specification: A Redundant Pair of Gateways .....	98
Setting Up CARP: Kernel Options, sysctl, and ifconfig Commands .....	100
Keeping States Synced: Adding pfsync .....	103
Putting Together a Rule Set .....	104

## **8** **LOGGING, MONITORING, AND STATISTICS** **107**

PF Logs: The Basics .....	108
Logging All Packets: log (all) .....	110
Logging to Several pflag Interfaces .....	111
Logging to syslog, Local or Remote .....	112
Tracking Statistics for Each Rule with Labels .....	113
Some Additional Tools for PF Logs and Statistics .....	115
Keeping an Eye on Things with pftop .....	115
Graphing Your Traffic with pfstat .....	116
Collecting NetFlow Data with pfflowd .....	118
SNMP Tools and PF-Related SNMP MIBs .....	118
Remember, Useful Log Data Is the Basis for Effective Debugging .....	119

## **9** **GETTING YOUR SETUP JUST RIGHT** **121**

The Things You Can Tweak and What You Probably Should Leave Alone .....	121
block-policy .....	122
skip .....	123
state-policy .....	123
timeout .....	123
limit .....	125
debug .....	126
ruleset-optimization .....	126
optimization .....	127