

Contents

Forward	ix
1 Introduction	1
1.1 Background	1
1.2 Versions	1
2 Getting Started	5
2.1 Activating PF	5
2.2 OpenBSD	5
2.3 NetBSD	6
2.4 FreeBSD	9
2.5 DragonFly	10
2.6 Controlling PF	12
3 Configuration Basics	15
3.1 pf.conf Configuration File	15
3.2 Addresses	16
3.3 Ports	17
3.4 Protocols	18
4 Lists and Macros	19
4.1 Overview	19
4.2 Lists	19
4.3 Macros	20
4.4 Using Macros	21
4.5 More Examples	22
5 Tables	25

5.1	Overview	25
5.2	Configuration	25
5.3	Manipulating Tables with pfctl	26
5.4	Specifying Addresses	27
5.5	Address Matching	28
6	Packet Filtering	29
6.1	Overview	29
6.2	Rule Syntax	29
6.3	Default Deny	31
6.4	Passing Traffic	31
6.5	The quick Keyword	32
6.6	Keeping State	33
6.7	Keeping State for UDP	34
6.8	TCP SYN Proxy	35
6.9	Stateful Tracking Options	35
6.10	TCP Flags	38
6.11	Blocking Spoofed Packets	40
6.12	Shortcuts for Creating Rulesets	42
6.13	Passive Operating System Fingerprinting	44
6.14	IP Options	45
6.15	Filtering Ruleset Example	46
7	Network Address Translation	49
7.1	Overview	49
7.2	How NAT Works	49
7.3	NAT and Packet Filtering	51
7.4	IP Forwarding	51
7.5	Configuring NAT	52
7.6	Bidirectional Mapping (1:1 mapping)	54
7.7	Translation Rule Exceptions	54
7.8	Checking NAT Status	54
8	Traffic Redirection (Port Forwarding)	57
8.1	Overview	57
8.2	Redirection Example	57
8.3	Redirection and Packet Filtering	58

8.4	Security Implications	60
8.5	Redirection and Reflection	60
9	Runtime Options	65
9.1	Overview	65
9.2	The set Command	65
9.3	Examples	68
10	Scrub (Packet Normalization)	69
10.1	Overview	69
10.2	Scrubbing packets	69
10.3	scrub Options	70
10.4	Examples	71
11	Anchors	73
11.1	Overview	73
11.2	Anchors	73
11.3	Anchor Options	75
11.4	Manipulating Anchors	76
12	Packet Queueing and Prioritization	77
12.1	Queueing	77
12.2	Schedulers	78
12.3	Configuring Queueing	82
12.4	Example #1: Small, Home Network	88
12.5	Example #2: Company Network	92
13	Address Pools and Load Balancing	99
13.1	Overview	99
13.2	NAT Address Pool	100
13.3	Load Balance Incoming Connections	101
13.4	Load Balance Outgoing Traffic	101
14	Packet Tagging (Policy Filtering)	105
14.1	Overview	105
14.2	Assigning Tags to Packets	105
14.3	Checking for Applied Tags	107
14.4	Policy Filtering	107

14.5	Tagging Ethernet Frames	110
15	Logging	111
15.1	Overview	111
15.2	Logging Packets	111
15.3	Reading a Log File	112
15.4	Filtering Log Output	112
15.5	Packet Logging Through Syslog	114
16	Performance	117
17	Issues with FTP	119
17.1	FTP Modes	119
17.2	FTP Client Behind the Firewall	120
17.3	PF “Self-Protecting” an FTP Server	122
17.4	Server Protected by External Firewall Running NAT	122
18	Authpf: User Shell for Authenticating Gateways	125
18.1	Overview	125
18.2	Configuring authpf	126
18.3	Creating an authpf Login Class	129
18.4	Seeing Who is Logged In	130
18.5	Example	131
19	Limiting spam with spamd	135
19.1	Overview	135
19.2	Enabling spamd	136
19.3	spamd and PF	137
19.4	Example SMTP Session	138
19.5	Greylisting with spamd	140
19.6	Maintaining the spamd Database	141
19.7	Greytrapping	142
19.8	The spamd configuration	143
19.9	Bypassing spamd	145
19.10	Auto whitelists with spamlogd	146
20	Firewall Redundancy with CARP and pfsync	149
20.1	Introduction to CARP	149

20.2	CARP Operation	150
20.3	Configuring CARP on FreeBSD and OpenBSD . .	150
20.4	carp(4) Example	152
20.5	Introduction to pfsync	153
20.6	pfsync Operation	153
20.7	Configuring pfsync	154
20.8	pfsync Example	155
20.9	Combining CARP and pfsync For Failover	155
20.10	Operational Issues	157
21	Example Ruleset: Firewall for Home or Small Office	159
21.1	The Scenario	159
21.2	The Network	159
21.3	The Objective	160
21.4	The Ruleset	161
21.5	The Complete Ruleset	165
A	Other Tools	167
	Index	175
	Colophon	183