Index

/etc/authpf/authpf.allow, 128
/etc/authpf/authpf.conf, 126
/etc/authpf/authpf.message, 129
/etc/authpf/authpf.rules, 127, 131
/etc/authpf/banned/, 128
/etc/inetd.conf, 62
/etc/login.conf, 129, 130
/etc/pf.boot.conf, 8
/etc/pf.conf, 10, 11, 15, 131
/etc/pf.os, 44, 66
/etc/protocols, 18
/etc/rc.conf, 10, 11
/etc/rc.conf.local, 5
/etc/rc.d/pf, 9, 11
/etc/rc.d/pf_boot, 8
/etc/services, 17
/etc/sysctl.conf, 51
/etc/syslog.conf, 115
/var/log/pflog, 111, 113
3-way handshake, 37

ACK flag, 31
action, 29
activating PF, 5
address alias, 17
address family, 30, 41
address pool, 99
addresses, 16, 27
addresses, dynamic, 16, 53
ADSL, 87, 88
af (address family), 30
alias, 17
all, 17
allow-opts, 45
allowing traffic, 31
Alternate Queueing (ALTQ), 82
ALTQ, 82, 83
altq, 83, 86
anchor, 125, 127
anchors, 73, 74
anchors, loading, 74
angle brackets, 26
antispoof, 40–42
any, 17
ARP requests, 149
asymmetric connections, 87
Auth, 160
authenticating PF, 125–130, 132

authpf, 125–130, 132
authpf configuration, 126
authpf login message, 129
authpf_users table, 128

backup firewalls, 149
backups, 149
balancing load, 99
bandwidth, 84, 85
banned users, 128
benchmarking, 118
BGP, 101
bidirectional mapping, 54
binat, 54
binat-anchor, 73
block, 29
block-policy, 30
blocking packets, 31
blocking spoofed packets, 40
borrow, 85
brconfig(8), 110
bridge, 7, 35, 110
broadcast address, 17

CARP, 149, 157, 158
carp, 158
CARP and pfsync, 155
carp password, 151
CBQ, 78, 80, 82, 84
cbq, 83
CIDR, 16, 17, 100
Class Based Queueing (CBQ), 78
classes, 78
classifying packets, 108
commas, 20
comments, 16
configuration file, 15
congestion, 81
connection limiting, 37
connection redirection, 57
connections, asymmetric, 87
const, 25
controlling PF, 12
cron, 115
crossover cable, 155

debugging, 65
default deny, 31, 42
default filter, 31
defragment, 15
Demilitarized Zone, 60
destination address, 30
destination port, 30
DHCP, 16
dial-up, 16
direction, packet, 30
DMZ, 60, 92
DNS, 16, 61
DNS, split-horizon, 61
DragonFly, 2, 3, 10–12, 51, 83, 122, 137
drop, 65
dynamic addresses, 16, 53
dynamically assigned address, 160

ECE, 39
ECN, 82, 83, 85, 86
enabling PF, 5

ethernet frames, 110
expansion, 23
Explicit Congestion Notification (ECN), 82

failover, 157, 158
fdescfs, 127, 136
features, 15
FIFO queue, 78
filtering, 107
fingerprinting, passive OS, 66
flags, 39
flags, packet, 31, 38, 82
floating, 67
flush, 38
flushing rules, 76
forwarding, 51
fragment crop, 71
fragment drop-ovl, 71
fragment reassemble, 70
fragment, don't, 70
fragment, unassembled timeout, 68
fragmented packets, 69
fragments, duplicate, 71
fragments, overlapping, 71
FreeBSD, 2, 3, 9, 10, 51, 83, 122, 127, 136, 137, 151
FTP, 120, 122, 163
FTP proxy, 120
ftp-proxy, 120, 163

gateway, 50, 58, 88
gateway, authenticating, 125
global synchronization, 81
grammar, 19, 42
greylist, 143
greylisting, 140, 141
greytrapping, 142

handshake proxy, 35
hardware, 117
Hartmeier, Daniel, 1
HFSC (Hierarchical Fair Service Curve), 83
high availability, 149
hostname, 27
Hot Standby Router Protocol (HSPR), 149
HSRP, 149

ICMP, 34, 50, 160, 165
icmp, 18
icmp6, 18
Ident, 160
ifconfig, 150, 153, 154, 156
IGMP, 45
in, 30
inet, 30
inet6, 30
inetd, 62
Initial Sequence Number, 31, 34
interface group, 30
interface, network, 16, 21, 30
inverse matching, 107

IP forwarding, 5, 51
IP options, 45
IPF, 1
ipsec, 154
IPv4, 30
IPv6, 27, 30
ISN, 31, 34

KAME, 82
keep state, 30, 31, 33, 39
kldload, 9

list, 17, 19
lists, 22, 23
lists, negated, 20
LKM, 6
load balancing, 99, 101, 102, 152
loading rules, 12
log, 30, 40, 52
log analysis, 112
log-all, 111
logging, 111, 115
logging packets, 111
logging, statistics, 162
login, 125
long lines, 16
loopback, 41, 62, 67, 162
low-delay TOS, 87

MAC address, 110
macro, 105
macros, 20–23, 27, 106, 161, 165
macros and quotes, 21
macros in anchors, 75
macros, predefined, 105, 128
macros, recursive, 21
managing PF, 12
marking packets, 105
master, 149, 158
max-mss, 70
Maximum Segment Size (MSS), 70
memory, 25, 26, 67, 68, 70, 113
memory pool, 66
min-ttl, 70
modload, 6
modulate state, 30, 31, 34
MSS, 70
multi-path routing protocol, 101

named rulesets, 73
NAT, 100, 122, 162
nat, 52, 100
NAT and redirection, 62
NAT and state, 34
NAT exceptions, 54
NAT gateway, 50
NAT status, 54
nat-anchor, 73, 127
negated, 28
negated address, 17
negation, 26
NetBSD, 3, 6–8, 83, 110, 122, 137
netmask, 16
network, 16

Network Address Translation, 162
network block, 17
network interface card (NIC), 117
nmap, 45
no rdr, 146
no-df, 70
normalization, 15, 40, 69, 71

OpenBSD, 1, 5, 51, 82, 110, 122, 137, 157, 173
operating system detection, 44
optimization, 32, 66
options, 30, 36, 37, 65–67, 69, 70, 162
ordering of pf.conf, 15
OSFP, 44, 45
out, 30

packet logging, 111
packet normalization, 69
packet payloads, 112
packet tagging, 105
packets, malformed, 69
parentheses, 16, 17, 53
parenthesis, 111, 163
pass, 29, 32
passing traffic, 31
Passive OS Fingerprinting, 44
peer, 17
persist, 26
pf.conf, 15, 83
pf.conf sections, 15
pf_rules, 7, 10, 11
pfctl, 12, 13, 15, 19, 26, 44, 54, 55, 74, 76
pfctl(8), 5
pfil(9), 7, 110
pflkm, 6
pflog0 interface, 111, 112
pflogd, 7, 30, 52, 111, 113
pfsync, 153, 154
pfsync0 device, 154
physical interface, 158
ping, 160
pkgsrc, 6, 9, 12
point-to-point link, 17
policy filtering, 107
policy-based filtering, 105, 107, 108
pool, 99
port, 52
port forwarding, 57
port range, inclusive, 18
port range, inverse, 18
ports, 17
ports, FreeBSD, 9, 10
ppp, 30
PPPoE, 161
prioritization, 15
priority level, 79
Priority Queueing, 80
PRIQ, 80–82
priq, 83
Private Service Network, 60
protocols, 18, 30
proxy, 120

PSN, 60

qlimit, 84
Quality of Service, 85
queue, 78, 83, 84, 87, 88
queue and keep state, 88
queue name, 84
queue priority, 79, 85
queue, assigning traffic to, 83
queueing, 78, 87, 88
queueing, configuring, 83
queues, 79, 81
quick, 30, 32, 33, 41

Random Early Detection, 81
random-id, 70
rate limiting, 37
rdr, 57, 59, 60, 101, 120, 121, 163
rdr-anchor, 73
reassemble tcp, 71
RED, 81–83, 85, 86
redirection, 57, 60, 120, 121, 163
redundancy, 149
redundancy group, 149
redundant firewalls, 149
reload, 10, 11
reserved words, 20
restart, 10, 11
resync, 10, 11
return, 43, 65
return-icmp, 43
return-rst, 43
RFC 1323, 71, 113
RFC 1631, 49
RFC 1918, 22, 49
RFC 2281, 149
RFC 3168, 82
RFC 3768, 149
RIO, 83, 85
round-robin, 80, 99–102
route-to, 101, 102
routing, 5, 51
RST flag, 38
rule, last, 29
ruleset, 5, 19, 20, 29, 31, 41, 74, 128, 132
ruleset processing, 74
ruleset, simplifying, 43
ruleset, viewing, 13
rulesets, sub, 73

scheduler, 83, 85
scheduler, queueing, 83
schedulers, 78, 83
scrub, 40, 66, 69, 71, 162
scrubbing, 40, 69, 162
securelevel, 25
self, 27
set block-policy, 65, 162
set debug, 65
set fingerprints, 66
set limit, 66
set loginterface, 66, 162
set optimization, 66
set skip, 162
set skip on, 67
set state-policy, 67
set timeout, 68
shortcuts, 42

SMTP, 143
source address, 30
source port, 30
source-hash, 100
source-quench, 34
source-track, 36
spam, 26
spam trap, 143
SpamAssassin, 135
spamd, 9, 10, 12, 107, 135, 141–143, 146, 172, 173
spamd, installing, 136
spamd-setup, 144, 145
spamd.conf, 144
spamdb, 141, 143
spamlogd, 146, 147
spoofed TCP SYN floods, 31, 35
spoofing, 40
SSH, 160
sshd, 129
state, 31, 33, 67
state and queue, 88
state limits, 66
state lookups, 33
state table, 153
stateful connections, 125
stateful inspection, 33
statistics, 27, 66, 162
sticky connection, 101
sticky-address, 100
substitution of variables, 20
SYN flag, 31
synproxy state, 30, 31, 35
syntax highlighting, 15
sysctl, 51, 152, 161
syslog, 114, 126

table, 20, 25, 26, 28, 127, 128
table file, 26
tables, 142, 146
tables, manipulating, 26
tagged, 107
tagging, 106, 110
tagging packets, 105
tags, 106
tail-drop, 78
tarpit, 135
tbrsize, 84
TCP, 33
tcp, 18
TCP flags, 31, 38, 40
TCP packet headers, 70
TCP proxy, 62
TCP Syn Proxy, 165
tcpdump, 44, 112–114, 153
Time to Live (TTL), 70
timeout, 35
timeouts, 68
token bucket regulator, 84
ToS, 87
translation, 59
TTL, 70, 71
Type of Service (ToS), 87

UDP, 34
udp, 18
UDP and state, 35
uptime, 71

user logins, 125, 130

variables, 20
variables substitution, 20
viewing ruleset, 13
Virtual Router Redundancy Protocol (VRRP), 149
VRRP, 149

Zalewski, Michal, 45