

# INDEX

## Numbers

- 10.0.0.1 IP address, 27
- 192.168.0.1 IP address, 27
- 802.11
  - hardware, 44
  - MAC address filtering, 42–43
  - WEP (Wired Equivalent Privacy), 43
  - WPA (Wi-Fi Protected Access), 43

## Symbols

- < > (angle brackets), 39
- :
- ! (exclamation mark), 39, 58
- () (parentheses), 31, 154, 159

## A

- Absolute OpenBSD* (Lucas), 170
- Acar, Can Erkin, 141
- access points
  - FreeBSD WPA, 48–49
  - with multiple interfaces, 50
  - OpenBSD WPA, 47–48
  - PF rule set, 49–50
- adaptive firewall. *See also* firewall
  - max, 88
  - overload, 88
  - setting up, 86–88
- address-allocation process, 27–28
- addresses
  - IP version 4, 27
  - IP version 6, 27

- nonroutable, 83–84
- routable, 60, 72
- alert syslog level, 156
- (all) logging option, 134–135
- ALTQ (ALTErnate Queueing). *See also* network traffic; traffic
- ACK packets, 110
- cbq (class-based queues), 107, 112–113
- concepts, 106
- determining bandwidth, 109
- features of, 105–106
- on FreeBSD, 107–108
- handling unwanted traffic, 117–118
- HFSC (Hierarchical Fair Service Curve)
  - algorithm, 107
  - traffic shaper, 113–115
- match rules for assignment, 110–111
- on NetBSD, 108
- on OpenBSD, 107
- priq queues, 106–107, 108–111
- queue concept, 106
- queue disciplines, 106
- queue schedulers, 106
- real-world example, 109–110
- rule sets, 113
- for servers in DMZ, 115–117
- setting up, 107–108
- syntax for, 108
- ToS (type of service) fields, 110
- using to handle traffic, 117–118

ancontrol program, 42  
angle brackets (< >), 39  
antispoof, 159–160  
ARPANET, 27  
ARP balancing, 128  
Artymiak, Jacek, 170  
attack techniques, 159  
authpf program, 55–57. *See also*  
    security  
    macros and redirection, 57–58  
    special-case rules, 57  
    user\_ip macro, 57  
auth\_web macro, 58

## B

baseline filtering rule, 19  
Beck, Bob, 104, 168, 171  
Berkeley Software Distribution  
    (BSD) systems, 3, 5  
    vs. Linux, 6  
    reading configurations, 6  
blacklisting mode, setting up  
    spamd in, 91–92  
blacklists, 97, 104  
block in all rule, 17  
block-policy option  
    drop value, 152  
    return value, 152  
Brauer, Henning, 2, 5, 106,  
    144, 168  
bridge, defined, 78  
bridge setup. *See also* firewall  
    on FreeBSD, 80–81  
    on NetBSD, 81–82  
    on OpenBSD, 79–80  
brute-force attacks, 86–88  
bruteforce table entries,  
    removing, 89  
BSD (Berkeley Software  
    Distribution) systems, 3, 5  
    vs. Linux, 6  
    reading configurations, 6  
Buechler, Christopher M., 171  
*Building Firewalls with OpenBSD and  
    PF, 2nd Edition*  
    (Artymiak), 170  
bytes in and out, showing, 23

## C

CARP (Common Address  
    Redundancy Protocol).  
    *See also* gateways  
    advskew parameter, 123, 129  
    checking configurations, 123  
    checking kernel options, 121  
    demotion counter, 124  
    gateways, 119–121  
GENERIC kernel  
    configurations, 121  
ifconfig for interfaces, 122–124  
ifstated daemon, 127  
kernel options, 121  
    for load balancing, 128–131  
    network interfaces, 122–124  
    passphrase, 124  
    setting sysctl values, 121–122  
    setting up, 121–124  
    sysstat states, 130  
    traffic, handling, 126  
    using for load balancing,  
        128–130  
    vhid (virtual host ID), 121  
Cho, Kenjiro, 170  
Christmas Tree EXEC worm, 2  
Cisco's PIX firewall series  
    exploit, 159  
colon (:), 91  
Common Address Redundancy  
    Protocol (CARP). *See*  
    CARP (Common Address  
    Redundancy Protocol)  
configuration files  
    placement of, 11, 13  
    as program output, 8  
    reading, 6  
configuration tools, 11  
connection information. *See* state  
    table  
content filtering, 90  
control messages. *See* ICMP  
    (Internet Control  
    Message Protocol)  
Core Force firewall product, 5. *See*  
    also firewall  
crit syslog level, 156  
cron job, creating for spamd-setup, 92

## D

debugging. *See also* logging;  
PF (Packet Filter)  
    subsystem: logs  
    rule sets, 162–164  
    using log data for, 150  
debug option, 156–157  
debug syslog level, 156  
deep packet inspection, 2  
Dehmlow, Sven, 2  
demilitarized zone (DMZ), 63–64  
    with NAT, 73  
    queueing for servers in, 115–117  
    testing, 161  
    total\_ext bandwidth, 117  
denial-of-service (DoS) attacks,  
    83, 159  
de Raadt, Theo, 2, 4, 170  
“Design and Performance of the  
    OpenBSD Stateful Packet  
    Filter (pf)” (Hartmeier),  
    168  
dhclient command, 53  
divert(4) sockets, 2  
Dixon, Jason, 9, 170  
DMZ (demilitarized zone), 63–64  
    with NAT, 73  
    queueing for servers in, 115–117  
    testing, 161  
    total\_ext bandwidth, 117  
DNS, running, 60  
domain name resolution,  
    performing, 18  
domain names vs. IP addresses, 33  
DoS (denial-of-service) attacks,  
    83, 159  
DragonFly BSD, 3, 5

## E

email setups, dealing with, 102–103  
email transmissions, RFC for, 95  
error information, generating,  
    156–157  
ESP protocol traffic, 51  
*Essential SNMP, 2nd Edition* (Mauro  
    and Schmidt), 171

*/etc/pf.conf* file, 6, 18  
*/etc/rc.conf* file, 6, 13  
*example.com* network, 60  
exclamation mark (!), 39, 58  
“Exploit Mitigation Techniques”  
    (de Raadt), 2

## F

failover and redundancy. *See* CARP  
    (Common Address  
    Redundancy Protocol)  
“Failover Firewalls with OpenBSD  
    and CARP” (Dixon), 170  
FAQs (frequently answered  
    questions), 7–8  
File Transfer Protocol (FTP), 34  
    proxying configuration, 34–36  
    security issues, 34  
file transfers, options for, 34  
filtering on interface groups, 76–77  
filtering rules, testing, 23  
firewall, 3. *See also* adaptive firewall;  
    bridge setup; Core Force  
    firewall product  
    configuration  
        mistakes in, 26  
        to keyword, 26  
    guides, applying to rule sets, 21  
    implementing as bridges, 78–79.  
Floeter, Reyk, 66  
flowd package  
    configuration, 146  
    described, 145–146  
    filtering features, 147–149  
    flows, 146–147  
    gateway field, 147  
    internalnet macro, 148  
    limiting data stored, 148  
    protocols, 146  
    setting up daemon, 146  
    storage of fields in flow  
        records, 148  
    unwired macro, 148  
    verbose output, 147–148  
fragments  
    handling, bugs in, 159  
    reassembly options, 158

- FreeBSD, 3–4
    - ALTQ (ALternate Queueing)
      - on, 107–108
    - bridge setup on, 80–81
    - connecting to WEP access point, 53–54
    - default values for PF-related settings, 14
    - /etc/rc.d/pf* script, 15
    - GENERIC kernel, 14
    - IP forwarding, 29
    - kernel options, 121–122
    - packet filter (pf) home page, 170
    - pfSense build, 7
    - rc* scripts, 15
    - setting up PF on, 13–15
    - spamd in greylisting mode, 96
    - versions of, 14
    - wireless network configuration, 46, 48
  - frequently answered questions (FAQs), 7–8
  - FTP (File Transfer Protocol), 34
    - proxying configuration, 34–36
    - security issues, 34
  - ftp-proxy with redirection, 34–36
- G**
- gateways, 160–161. *See also* CARP (Common Address Redundancy Protocol)
    - allowing name service for clients, 32
    - authenticating, setting up, 55–57
    - diagram, 120
    - rule sets, 31
    - setting up, 26, 29–33
    - using pass rule with, 32
  - GENERIC kernel, using with FreeBSD, 14
  - global settings
    - block-policy, 152
    - debug option, 156–157
    - fragment reassembly, 158
    - limit option, 155–156
    - optimization option, 158
    - reassemble option, 158
    - ruleset-optimization option, 157–158
    - skip option, 152–153
    - state-defaults option, 153–154
    - state-policy, 153
    - timeout option, 154–155
  - greylisting, 93–98
    - keeping in sync, 101–102
    - mode
      - managing, 102–103
      - setting up spamd in, 94–96
      - web resources, 171
  - greytrapping, 98–99, 104
  - GUI tool, using with PF rule set, 7
- H**
- haiku, 8
  - hardware support
    - developers, 175
    - efforts, 175–176
    - getting, 174–175
  - Harris, Evan, 93–94, 171
  - Hartmeier, Daniel, 4, 109–110, 141, 168
  - Hole, Kjell Jørgen, 42, 171
  - hostnames vs. IP addresses, 33
  - hosts, providing feedback to, 152
- I**
- IBM Christmas Tree EXEC worm, 2
  - ICMP (Internet Control Message Protocol), 36–37, 39
    - codes, 38, 39
    - packet types, 38–39
  - IEEE 802.11
    - hardware, 44
    - MAC address filtering, 42–43
    - WEP (Wired Equivalent Privacy), 43
    - WPA (Wi-Fi Protected Access), 43
  - ifconfig command, 45
    - a output of, 30
    - bridge configuration, 79–80

- CARP configuration, 124
  - interface groups, 45, 47, 51, 52, 71, 76–77, 123
- ifstated daemon, 127
- ILOVEYOU worm, 2
- in and out rules, 26–27
- information technology (IT), 2
- info syslog level, 156
- inserts counter, 23
- interface groups, filtering on, 76–77
- interface:network notation, 28–29
- interfaces, testing running
  - status of, 30
- interface state daemon, 127
- Internet Control Message Protocol (ICMP), 36–37, 39
  - codes, 38, 39
  - packet types, 38–39
- IP addresses
  - vs. domain names, 33
  - vs. hostnames, 33
  - IPv4 vs IPv6, 27
  - lists of, 39–40
- IPFilter
  - compatibility with, 4
  - copyright infringement
    - episode, 4
- IPSec VPN solutions, 50–51
- iptables vs. PF, 8
- IPv6
  - ICMP updates for, 39
  - vs. NAT (Network Address Translation), 27–28
  - packets, blocking, 23
  - traffic, forwarding, 29
- IT (information technology), 2

## K

- KAME project, 28
- keep state, 17
- kern.debug* log level, 156–157
- kernel
  - hacking, 4
  - memory space, 155
  - PF loadable module, 14, 15, 108
- Knight, Joel, 150
- Kozierok, Charles M., 169

## L

- labels, using for traffic statistics, 138–139
- Lehey, Greg, 3
- limit option, 155–156
- links, establishing in wireless networks, 42
- Linux
  - vs. BSD, 6
  - naming conventions, 6
  - possibility of running PF on, 7
- lists
  - defined, 18
  - of IP addresses, 39–40
  - maintaining for services, 20
  - managing with spamdb, 100–101
  - updating, 101
  - using for readability, 18–22
- load balancing, 66–71, 73–74, 128–131
- local network, defining, 28–29
- logging. *See also* debugging; monitoring tools; PF (Packet Filter) subsystem: logs
  - (all) option, 134–135
  - basics, 132–133
  - data, using for debugging, 150
  - files, rule numbers in, 133
  - legal implications of, 134
  - with pflogd daemon, 132
  - to pflog interfaces, 135
  - syslog, 135–137
  - using tcdump program for, 133
- logical NOT operator (!), 39, 58
- loopback interface, preventing
  - filtering of, 13
- Lucas, Michael W., 170

## M

- MAC address filtering, 42–43
- macros
  - using for readability, 18–22, 28–29, 31
  - using with authpf program, 57–58
- mail connections, tracking, 98
- mail-in and mail-out labels, 138

- mail server, 61, 71–72
- malicious software, 2
- Management Information Base (MIB), 150
- “Managing Traffic with ALTQ” (Cho), 170
- man pages (manuals)
  - consulting, 8
  - looking up, 44
  - listing, 44
- martians macro, 83–84
- match rule, using with nat-to, 31
- Mauro, Douglas R., 171
- maximum transmission unit (MTU), 38
- Mazzocchio, Daniele, 169
- McBride, Ryan, 5
- memory pools, setting size of, 155–156
- MIB (Management Information Base), 150
- Miller, Damien, 2, 145, 150
- monitoring tools. *See also* logging; NetFlow; PF (Packet Filter) subsystem: logs; pflow(4) pseudo-interface
  - flowd, 145–149
  - flow-tools, 145
  - nfdump, 145
  - pfflowd, 149
  - pftop, 141
  - pstat, 141–143
  - systat, 139–141
- Morris worm, 2
- MTU (maximum transmission unit), 38

## N

- name resolution
  - handling, 20, 60
  - testing, 21–22
- naming network interfaces, 6
- NAT (Network Address Translation)
  - DMZ with, 73
  - handling for gateways, 31
  - vs. IPv6, 27–28

- Nazario, Jose, 171
- NetBSD, 3, 5
  - ALTQ (ALTErnate Queueing) on, 108
  - bridge setup on, 81–82
  - /etc/defaults/pf.boot.conf* file, 16
  - /etc/pf.conf* file, 16
  - IP forwarding, 29
  - kernel options, 121
  - PF pages, 170
  - setting up PF on, 15–16
- NetFlow, 143–144. *See also* monitoring tools; pflow(4) pseudo-interface
  - analysis, 145–149
  - choosing collectors, 145
  - collector and analysis packages, 145
  - data collecting, 145–149, 149–150
  - flowd package, 145–149
  - flow-tools package, 145
  - nfdump package, 145
  - reporting, 145–149
  - sensor, setting up, 144–145
  - network, diagram of, 60, 64, 82, 116, 120, 161
- Network Address Translation (NAT)
  - DMZ with, 73
  - handling for gateways, 31
  - vs. IPv6, 27–28
- Network Flow Analysis* (Lucas), 170
- network interfaces
  - excluding from PF processing, 152–153
  - naming, 6, 31
- networks
  - with gateways, 120
  - setting up, 74–76
- network traffic. *See also* ALTQ (ALTErnate Queueing); traffic
  - catching via filtering rules, 23
  - cleaning up, 158–160
  - diagram of, 142, 143
  - directing with ALTQ, 105–108
  - IPSec VPN solutions, 50–51

- limiting, 3
- logging, 133
- seeing snapshots of, 139–141
- viewing on interfaces, 164

network troubleshooting, 36–39

nixspam blacklist, 104

nonroutable addresses, 83–84

notice syslog level, 156

## O

### OpenBSD

- 3.0 base system, 4
- 3.1, PF performance, 4
- ALTQ (ALternate Queueing)
  - on, 107
- approach toward design, 2
- approach toward security, 2
- benefits of, 5
- bridge setup on, 79–80
- connecting to WEP access point,
  - 51–53
- default *pf.conf* file, 13
- encapsulation interface, 51
- /etc/rc* script, 13
- ifstated daemon, 127
- IP forwarding, 29
- kernel options, 121
- papers by developers, 168
- pass rules, 17
- presentations by developers, 168
- setting up PF on, 12–13
- version of IPFilter, 4
- website, 168

*OpenBSD Journal*, 167

optimization option

- aggressive setting, 158
- conservative setting, 158
- high-latency value, 158
- satellite value, 158

out-of-memory conditions, 159

out-of-order MX use, detecting, 102

## P

Packet Filter (PF) subsystem. *See* PF (Packet Filter) subsystem

### packets

- displaying live view of, 140
- filtering, 3–4, 18, 76–77
- forwarding, turning on for
  - gateways, 29
- getting information about, 23
- logging, 134–135
- matching to state table, 153
- movement, tracking, 137
- normalization, 158–159
- tagging, 77–78
- tracking paths of, 164

Palmer, Brandon, 171

parentheses (), 31, 154, 159

pass rule, using with gateways, 32

path MTU discovery, 36, 38–39

Pentium III machine, 5

permissive rule sets, 19–20

*pf.conf* file, 13

pfctl program, 11–12

- d option, 12, 162
- sm option, 155
- s timeouts option, 154–155
- using to extract information,
  - 22–23
  - using with tables, 89

pfflowd package, 149–150

#*pf*IRC channel wiki, 169

pflog interfaces

- cloning, 135
- disabling data accumulation, 136
- logging to, 135
- pflogd logging daemon, 132

pflog(4) pseudo-interface, 143–144.

*See also* monitoring tools; NetFlow

pflog device, enabling, 144–145

pflog state option, 143

PF (Packet Filter) subsystem, 1

- code, finding, 5
- configuration
  - converting other products to,
    - 7–8
  - debugging, 162
- confirming running status of, 22
- data, graphing, 141–143
- disabling, 12

- PF (Packet Filter) subsystem,
    - continued*
    - enabling, 12–13, 162–163
    - haiku, 8
    - vs. iptables, 8
    - logs, 132–133. *See also*
      - debugging; logging;
      - monitoring tools; syslog
    - collecting data for, 132
    - storage of data, 132
    - tracking statistics for rules, 137–139
    - using labels with, 137–139
  - operating system fingerprinting, 118
  - releases 4.4 through 4.8, 5
  - requirements for, 5
  - rise of, 3–5
  - rules, changes to syntax, 8
  - rule set, managing, 7
  - running on Linux, 7
  - setting up on FreeBSD, 13–15
  - setting up on NetBSD, 15–16
  - setting up on OpenBSD, 12–13
  - user guide, 75
  - version in OpenBSD 4.8, 5
  - pf\_rules= setting, 13
  - pfSense build of FreeBSD, 7
  - pfSense: The Definitive Guide* (Buechler and Pingle), 171
  - pfstat utility
    - collect statements, 142
    - color values in graphs, 142
    - described, 141
    - home page, 143
    - image definition, 142
    - setting up, 142
    - specifying graph size, 142
  - pfsync interfaces, configuring, 125
  - pfsync protocol, 119
    - adding, 125–126
    - rule sets, 126–127
    - sysat states, 126
  - pftop tool, 141
  - ping command, 37
  - Pingle, Jim, 171
  - ping of death, 36
  - PIX firewall series exploit, 159
  - pool memory, availability of, 155
  - PPP connection, using with
    - gateways, 30
  - PPPoE, using with gateways, 30
  - pstat tool, 141–143
  - “Puffy at Work—Getting Code Right and Secure, the OpenBSD Way” (Brauer and Dehmlow), 2
- Q**
- queues. *See* ALTQ (ALTErnate Queueing)
  - quick keyword, 32–33
- R**
- Ranum, Marcus, 2, 18, 169
  - readability, using lists and macros for, 18–22
  - Realtek Ethernet cards, 31
  - reassemble option, 158
  - redirection
    - for load balancing, 73–74
    - to pool of addresses, 65–66
    - using with authpf program, 57–58
    - using with auth\_web macro, 58
    - using with ftp-proxy, 34–36
  - re driver, 26–27
  - redundancy and failover. *See* CARP (Common Address Redundancy Protocol)
  - Reed, Darren, 4
  - Reed, Jeremy C., 171
  - relayd daemon
    - CARP-based failover, 71
    - enabling at startup, 69
    - redirects and relays, 66
    - ssl options, 70–71
    - starting, 68
    - sticky-address option, 68
    - tcp options, 71
    - using for load balancing, 128
    - webpool table, 68



- remote X11 traffic, blocking, 13
- removals counter, 23
- resource exhaustion, 159
- RFCs
  - 114 (FTP), 34
  - 765 and 775 (TCP/IP), 34
  - 792, 39
  - 950, 39
  - 1067 (SNMP), 150
  - 1191, 39
  - 1256, 39
  - 1631 (IP NAT), 168
  - 1631 (NAT), 28
  - 1885 (ICMP updates for IPv6), 39
  - 1918 (address allocation), 28, 60, 169
  - 2018, 71
  - 2281 (VRRP), 119
  - 2460 (IPv6), 28
  - 2463 (ICMP updates for IPv6), 39
  - 2466 (ICMP updates for IPv6), 39
  - 2521, 39
  - 2765, 39
  - 2821, 95
  - 3330, 60
  - 3411 through 3418 (SNMP), 150
  - 3768 (VRRP), 119
  - 5321, 95
- Ritschard, Pierre-Yves, 66
- round-robin option, 65
- routable addresses, 60, 72
- rule numbers, displaying for debugging, 163
- rules
  - changing order of, 157
  - evaluating for gateways, 32
  - expansion of, 138–139
  - getting log data for, 132
  - merging into tables, 157
  - parsing without loading, 21
  - reading, 21
  - removing duplicates, 157
  - removing subsets of, 157
  - tracking statistics for, 137–139

- ruleset-optimization option, 157–158
- rule sets
  - bridge, 82–83
  - building, 16–17
  - checking changes to, 21
  - debugging, 162–164
  - escapes from sequences, 32–33
  - examining, 13
  - firewall considerations, 21
  - keep state part, 17
  - loading, 12, 162–163
  - logic errors, 163–164
  - permissive, 19–20
  - quick keyword, 32–33
  - storage of, 11
  - test case sequence, 162
  - testing, 18
    - after changing, 21–22
    - for gateways, 33
- Russian name server example, 134

## S

- Schmidt, Kevin J., 171
- Schwartz, Randal L., 169, 170
- scrub feature, 158–159
- Secure Architectures with OpenBSD* (Palmer and Nazario), 171
- Secure Shell (SSH) service, 86
- security. *See also* authpf program
  - OpenBSD's approach to, 2
  - in wireless networks, 42
- “Security Measures in OpenSSH” (Damien Miller), 2
- Sender Policy Framework (SPF) records, storage of, 103
- services
  - maintaining lists of, 20
  - running, 65
  - segregating, 63–65
- set options, 152
- setup, testing, 160–162
- Simple Network Management Protocol (SNMP), 150
- skip option, 152–153

- SMTP
    - servers, outgoing, 103
    - standards, interpreting, 93–97
    - traffic, initiating, 61–62
  - SNMP (Simple Network Management Protocol), 150
  - software, malicious, 2
  - spam, fighting, 104
  - SpamAssassin, 90
  - spamdb, using to manage lists, 100–101
  - spamd daemon
    - features of, 89–90
    - keeping greylists in sync, 101–102
    - logging, 93
    - running, 104
    - setting up in blacklisting mode, 91–92
    - setting up in greylisting mode, 94–96
  - spamlogd whitelist updater, 98
  - SPF (Sender Policy Framework)
    - records, storage of, 103
  - spoofing, protecting against, 159–160
  - SSH brute-force attacks, 86
  - SSH (Secure Shell) service, 86
  - state-defaults option, 153–154
  - state information, keeping, 17
  - state-policy option
    - floating value, 153
    - if-bound value, 153
  - state table, 17, 153
    - graphing, 142, 143
    - statistics, interpreting, 23
    - viewing, 139–140
  - state-timeout handling, 158. *See also* timeout option
  - state-tracking options, 87–88
  - statistics, displaying live view of, 140
  - sticky-address option, 65–66
  - stuttering, 90
  - SYN-flood attacks, 62
  - synproxy state option, 62
  - sysctl command, using with IPv6 traffic, 29
  - syslog
    - levels, 156
    - logging to, 135–137. *See also* PF (Packet Filter) subsystem: logs
  - sysstat program, 111
    - bytes view, 140
    - cyclng through views, 141
    - iostat view, 141
    - netstat view, 141
    - packets view, 140
    - pf view, 140
    - rules output, 140
    - states output, 139–140
    - vmstat view, 141
  - system information, displaying, 22–23
  - system status. *See* monitoring tools
- ## T
- tables
    - entries, expiring, 89
    - tidying with pfctl, 89
    - using as lists of IP addresses, 39–40
  - tags, 77–78
  - tarpitng, 90
  - tcdump program, 133
    - nohup command, 137
    - using to view traffic, 164
    - using with syslog, 136–137
  - TCP/IP
    - configuring client for, 53
    - packet filtering, 30–31, 34, 38, 169
  - TCP traffic, viewing, 164
  - TCP vs. UDP services, 20
  - testing setups, 160–162
  - “The Next Step in the Spam Control War: Greylisting” (Harris), 93–94, 171
  - The OpenBSD PF Packet Filter Book* (Reed), 171
  - “The Six Dumbest Ideas in Computer Security” (Ranum), 2, 18, 169
  - The TCP/IP Guide* (Kozierok), 169

- timeout option. *See also* state-timeout handling
  - adaptive values, 154
  - frag value, 154
  - inspecting settings for
    - parameters, 154–155
  - interval value, 154
  - src.track value, 154
- to keyword, with firewalls, 26
- traceroute command, 37–38
- traffic. *See also* ALTQ (ALternate Queueing); network traffic
  - catching via filtering rules, 23
  - cleaning up, 158–160
  - diagnostic, permitting, 37
  - directing with ALTQ, 105–108
  - displaying live view of, 140
  - graphing with pfstat, 142, 143
  - limiting, 3
  - logging, 133
  - seeing snapshots of, 139–141
  - shaping
    - cbq (class-based queues), 107, 112–113
    - concepts, 106
    - features of, 105–106
    - HFSC (Hierarchical Fair Service Curve), 107
    - queue concept, 106
    - queue disciplines, 106
    - queue schedulers, 106
    - real-world example, 109–110
    - setting up, 107–108
    - ToS (type of service)
      - fields, 110
    - using to handle traffic, 117–118
  - showing snapshots of, 141
  - totals, 137
  - viewing on interfaces, 164
- triplist, setting up, 99–100
- trojans, 2
- troubleshooting networks
  - ICMP protocol, 36–37
  - path MTU discovery, 38–39
  - ping command, 37
  - traceroute command, 37–38

## U

- UDP vs. TCP services, 20
- Unix.se user group, 169
- `/usr/share/examples/pf/pf.conf` file, 15

## V

- verbose mode, 20
- virtual local area network (VLAN), 63
- virtual private networks (VPNs),
  - setting up, 50–51
- Virtual Router Redundancy Protocol (VRRP), 119
- viruses, 2
- VLAN (virtual local area network), 63
- VPNs (virtual private networks),
  - setting up, 50–51
- VRRP (Virtual Router Redundancy Protocol), 119

## W

- warning syslog level, 156
- webpool table, creating, 68
- web server, running, 71–72
- websites
  - Cisco's PIX firewall series
    - exploit, 159
  - "Explaining BSD," 3
  - flow-tools package, 145
  - FreeBSD packet filter (pf) home page, 170
  - greylisting.org, 171
  - Hartmeier, Daniel, 4
  - network security, 42
  - nfdump package, 145
  - OpenBSD, 168
  - OpenBSD security, 2
  - pfSense (FreeBSD build), 7
  - security, 42
  - SpamAssassin, 90
  - Wi-Fi Net News, 42
- WEP (Wired Equivalent Privacy),
  - 43, 45
- wicontrol program, 42
- Wi-Fi Net News website, 42

- Wi-Fi Protected Access (WPA), 43, 47–48
- Wired Equivalent Privacy (WEP), 43, 45
- wireless networks
  - access points
    - FreeBSD WPA, 48–49
    - with multiple interfaces, 50
    - OpenBSD WPA, 47–48
    - PF rule set, 49–50
  - client side, 51
  - establishing links in, 42
  - FreeBSD WEP setup, 46
  - FreeBSD WPA access point, 48–49
  - IPSec VPN solutions, 50–51
  - OpenBSD WEP setup, 44
  - OpenBSD WPA access point, 47–48
  - security in, 42
  - setting up, 44–46
  - viewing kernel messages, 44
- worms, 2
- wpa-psk utility, running, 47
- wpa\_supplicant, setting up, 54
- WPA (Wi-Fi Protected Access), 43, 47–48