

# INDEX

## Symbols

- < > (angle brackets), 31
- :
- ! (logical NOT operator), 31, 74
- ( ) (parentheses), 21, 69

## A

- Acar, Can Erkin, 115
- access points, 38–39
- ACK packets, 92–93
- adaptive.end value, 124
- adaptive.start value, 124
- address pools, 50–51
- address tables, 125
- addresses. *See also* IP addresses
  - CARP, 99, 100, 102
  - email, 85
  - inner, 3
  - MAC, 40
  - nonroutable, 3, 65–66
  - outer, 3
  - routable, 3, 26, 46–51
- ADSL connections, 21
- advbase parameter, 102, 103
- advskew parameter, 101–102
- ALTQ (ALTErnate Queuing). *See also* queues
  - allocation by percentage, 93
  - basic concepts, 88
  - directing traffic with, 87–97
  - example, 97
  - on FreeBSD, 90
  - handling unwanted traffic with, 96–97
  - integration with PF, 6

- on NetBSD, 90–91
- on OpenBSD, 89
- patch, 90
- percentage-wise bandwidth
  - allocation, 93
  - setting up, 89–91
  - undesired traffic, 97
- ALTQ option, 90
- ALTQ\_NOPCC option, 90
- anchors, 26, 27, 42
- angle brackets (< >), 31
- antispoof keyword, 19, 127, 128–129
- application-level filtering, 3
- ath0 interface, 37
- attacks
  - antispoof keyword, 19, 127, 128–129
  - brute force, 68–71, 122
  - Denial of Service, 65, 112
  - scrub keyword, 19, 127–128
  - spoofed packets, 127–129
  - SYN-flood, 47
  - wireless networks, 35–40
- authenticating gateway, 41–43
- authentication
  - authpf, 40–44
  - shared-secret, 82
  - ssh, 41
  - user, 40–44
- authoritative slave server, 46
- authpf anchors, 42
- authpf authentication, 40–44
- authpf.rules* file, 41–43

## B

- backup machines, 98, 102–103
- backup tables, 53, 54

- bandwidth
  - actual, 95
  - allocating with ALTQ, 87–97
  - available, 95
  - class-based allocation, 93–94
  - interface, 95
  - labels, 114
  - network bottlenecks and, 95
  - total, 91
  - usable, 91
- basic setups. *See also* PF configurations
  - bridge, 61–64
  - gateway, 19–23
  - network, xvi
  - redundancy, 97
- Beck, Bob, 80, 85
- Berkeley Software Distribution (BSD), 1–2, 136–137
  - clients, 40
  - license, 1–2
  - systems. *See also* FreeBSD; NetBSD; OpenBSD
    - defined, xvi
    - DragonFly, xvi, 3
    - vs. Linux systems, xvi–xvii
    - PF compatibility and, xvi
    - resources, 135–140
- best-effort services, 75
- blacklisting spammers, 72–74, 79–82, 84–85
- block all default, 42
- block all rule, 48
- block policies, 122
- block-policy option, 122
- boot-time system messages, 36
- brconfig command, 61–62, 64
- brconfig(8), 34
- bridge rule set, 64–65
- bridge(4) facility, 34
- bridges
  - Ethernet, 61
  - firewalls implemented as, 61–64
    - on FreeBSD, 62–63
    - on NetBSD, 63–64
    - on OpenBSD, 61–62
- bridging firewall, 61–64
- broadband connections, 21
- brute force attacks, 68–71, 122

- BSD. *See* Berkeley Software Distribution (BSD)
- bsnmpd, 119
- bulk SSH transfers, 93
- bytes, 4

## C

- CARP. *See* Common Address Redundancy Protocol (CARP)
- CARP-based failover, 55
- cbq option, 89, 93–94
- Cho, Kenjiro, 87
- class-based queues, 89, 93–94
- clients
  - BSD, 40
  - FTP, 26, 27
    - on local network, 46–48
  - OpenBSD, 40
- cloned pflog interfaces, 111
- colon (:), 73, 77
- Common Address Redundancy Protocol (CARP), 97–105.
  - See also* pfsync protocol.
  - addresses, 99, 100, 102
  - arp balancing, 101
  - backup machines, 98, 102–103
  - described, 97–98
  - FreeBSD users, 100
  - group, 101
  - high availability, 97
  - master machines, 98, 101–102
  - NetBSD users, 100
  - OpenBSD users, 100
  - redundant gateways, 98–100
  - security issues, 103–104
  - setting up, 100–103
  - traffic, 101, 103, 105
- configuration file. *See also* `/etc/pf.conf` file; `/etc/rc.conf` file
  - ftp-proxy, 25–26
  - included with system, 6
  - overview, 11–12
  - simple setup on FreeBSD, 9–10
  - simple setup on NetBSD, 10–11
  - simple setup on OpenBSD, 8–9
  - single, stand-alone machine, 11–12

- configurations. *See* basic setups; PF configurations
- connections
  - ADSL, 21
  - block policies, 122
  - broadband, 21
  - dial-up, 21
  - Internet, 21
  - monitoring, 115–119
  - new, 69, 70
  - PPP, 21
  - rate of, 69, 70
  - simultaneous, 69, 70
  - spamd, 110
  - ssh, 110
  - terminated (flushed), 69
- control messages, 28
- conversions
  - automating, xviii
  - from OtherProduct setups, xviii
  - from product rule sets, xviii
- cookie hash, 55
- Core Force product, 3
- cron jobs, 32

## D

- database synchronization, 82
- de Raadt, Theo, 2
- debug option, 126
- debugging. *See also* troubleshooting
  - considerations, 28–31
  - importance of log data, 119
  - options for, 126
  - rule sets, 131–133
- default deny rule set, 13
- default rule sets, 8, 9
- De-Militarized Zone (DMZ)
  - in NAT environments, 49–50, 56–57
  - servers in, 49–50, 94–96
- demotion counter, 102
- Denial of Service (DoS) attacks, 65, 112
- devices
  - CARP, 100
  - cloneable, 111
  - hardware, 125
  - pflog, 108, 113

- pfsync, 100
    - pseudo-devices, 21
    - wireless, 34, 36
- dhclient command, 40
- dhcpcd, 32, 38
- dial-up connections, 21
- dmesg command, 36
- DMZ. *See* De-Militarized Zone (DMZ)
- DNS (domain name service), 46, 84
- DNS query, 15
- DNS test, 15
- Dobbelaar, Camiel, 26
- domain name lookups, 110
- domain name service (DNS), 46, 84
- domain names, 14, 23
- DoS (Denial of Service) attacks, 65, 112
- DragonFly BSD, xvi, 3
- drop value, 122

## E

- email. *See also* mail servers; spam
  - as basic service, 71, 74
  - as best-effort service, 75–76
  - delay in sending, 83
  - harvesting addresses, 85
  - RFC 2821 standard, 75–76
  - sending outside local network, 47–48
  - SMTP, 71, 75, 85
  - tracking, 77–78
- encryption
  - data transfer, 24
  - link-level, 34
  - web traffic, 54, 56
  - WEP, 35, 37, 40
  - WPA, 35
- Engen, Vegard, 43
- errors. *See also* troubleshooting
  - correcting, 14
  - logic, 131–132
  - in rule sets, 14, 131–132
  - syntax, 8, 14
  - temporary, 75
- ESP protocol traffic, 39
  - `/etc/authpf/authpf.conf` file, 41
  - `/etc/defaults/rc.conf` file, xvii
  - `/etc/inetd.conf` entry, 25

- /etc/pf.conf* file
    - configuring access point as gateway, 38
    - creating authenticating gateway, 41–43
    - described, xvii
    - editing with `pfctl`, 7
    - ftp-proxy, 25–26
    - global settings, 122–127
    - included with system, 6
    - simple setup on FreeBSD, 9–10
    - simple setup on NetBSD, 10–11
    - simple setup on OpenBSD, 8–9
    - single, stand-alone machine, 11–12
  - /etc/rc.conf* file, xvii, 8–10, 27, 76
  - /etc/rc.conf.local* file, xvii
  - /etc/syslog.conf* file, 113
  - Ethernet bridge, 61
  - Ethernet interface, 21, 91
  - expire keyword, 71
  - expiretable utility, 71
  - expiring table entries, 70–71
  - explicit blocking, 65
- F**
- failover, 55, 97–105
  - FAQs, xvi–xviii
  - Fatal: timeout before authentication message, 69
  - fdescfs code, 76
  - FIFO (First In, First Out), 88, 92
  - file field, 73
  - file transfer, 24
  - File Transfer Protocol (FTP), 24–27
    - clients, 26, 27
    - described, 24
    - ftp-proxy (new), 26–27
    - ftp-proxy (old), 24, 25–26
    - ftpsesame daemon, 26
    - NAT mode, 25–26
    - pftpx program, 26
    - routable addresses, 26
    - security challenges of, 24
    - servers, 26, 27
    - TCP and, 24
  - fileservers, 46–51
  - filtering. *See also* PF (Packet Filter)
    - application-level, 3
    - ICMP, 28, 29
    - on interface groups, 59–60
    - on IPsec encapsulation interface, 39
    - on loopback interface, 123
    - MAC addresses, 34, 40
    - with traceroute command, 29
  - filtering rules. *See* rules
  - filtering services, 45–51
  - fingerprinting, OS, 97
  - firewalls
    - bridging, 61–64
    - described, 3, 17
    - NAT and, 4
    - nonroutable addresses, 65–66
  - First In, First Out (FIFO), 88, 92
  - floating state policy, 123
  - flush global option, 69
  - frag value, 124
  - fragmentation, 30, 124, 128
  - FreeBSD. *See also* Berkeley Software Distribution (BSD), systems
    - adoption of PF, 2–3
    - ALTQ on, 90
    - basic bridge setup on, 62–63
    - CARP setup, 100
    - enabling/disabling PF, 10
    - etc/rc.conf* file, 9–10
    - greylisting and, 76
    - PF compatibility and, xvi
    - PF-related settings in, 9–10
    - resources, 138
    - simple PF setup, 9–10
    - versions, xiii, 9
  - FTP. *See* File Transfer Protocol (FTP)
  - ftp-proxy program, 24, 25–27
  - ftpsesame daemon, 26
- G**
- gateways, 17–23
    - authenticating, 41–43
    - considerations, 18–19
    - pitfalls, 18–19
    - redundant, 98–100
    - setting up, 19–23
    - specific rules for, 18–19
    - specifying local network, 19
    - stopping probes at, 29
    - to keyword and, 18
    - wireless networks, 36–42
  - GENERIC kernel, 61, 89–90, 100

- GENERIC.MP* kernel, 89, 100
- global settings, 122–127
- global state policy, 123
- greyexp value, 77
- greylisting, 75–85
  - FreeBSD and, 76
  - incompatible sites, 83–84
  - mode, 76–77, 80, 84
  - overview, 75–76
  - resources, 139
  - turning off, 74
- greytrapping, 78, 80–83, 85
- groups
  - CARP, 101
  - failover, 103
  - interface, 59–60
  - redundancy, 103
  - user, 137
- GUI tools, xvii, xviii
- Gustafsson, Henrik, 71

## H

- hacking attacks
  - antispoof keyword, 19, 127, 128–129
  - brute force, 68–71, 122
  - Denial of Service, 65, 112
  - scrub keyword, 19, 127–128
  - spoofed packets, 127–129
  - SYN-flood, 47
  - wireless networks, 35–40
- haiku, PF, xix
- hardware
  - OpenBSD support for, 141–145
  - wireless networks, 35–36, 142–144
- hardware-support developers, 144
- Harris, Evan, 75
- Hartmeier, Daniel, 1, 2, 91, 116, 136
- header options, 55
- HFSC (Hierarchical Fair Service Curve) queues, 89, 90
- hfsc option, 89
- high availability (CARP), 97
- host names, 12, 14, 23
  - hostname.if* configuration file, 40, 59
  - hostname.pflog1* file, 77, 111
- hoststatedctl program, 53–54
- hoststated, load balancing with, 51–65
- HTTP relay, 54–55
- HTTPS relay, 54–55

## I

- ICMP (Internet Control Message Protocol), 28–31
- ICMP ECHO requests, 28, 30
- ICMP filtering, 28, 29
- icmp queue, 94
- ICMP traffic
  - bandwidth for, 94
  - blocking/filtering, 29
  - troubleshooting and, 28–31
- IEEE 802.11 standard, 33–36
- if-bound state policy, 123
- if\_bridge module, 62–63
- ifconfig commands
  - CARP setup, 100–103
  - displaying interface status, 20
  - wireless device setup, 34
  - wireless network setup, 36–40
- IKE/ISAKMP (IPsec with udp key exchange), 39
- in keyword, 18–19
- inner addresses, 3
- interface bandwidth, 95
- interface for PPPoE (PPP over Ethernet), 21
- interface groups, 59–60
- Internet
  - commercialization of, 4
  - connections, 21
  - nonroutable addresses to, 65
  - overview, 4
  - resources on, 135–140
- Internet Control Message Protocol (ICMP), 28–31
- Internet Protocol, version 6. *See* IPv6
- Internet protocols, 4, 6, 28, 30
- interval value, 124
- IP addresses. *See also* addresses
  - CARP and, 100
  - forwarding, 19–20
  - NAT and, 5
  - physical vs. virtual, 100
  - resolving, 14
  - rule sets and, 23
  - shortage of, 5
  - spoofed, 128–129
- IP masquerade. *See* Network Addressable Translation (NAT)
- ipconfig -a command, 20

- IPFilter, 1–2
- IPsec, 21, 39, 104
- IPsec with udp key exchange (IKE/ISAKMP), 39
- IPv6 (Internet Protocol, version 6), 4–5, 16
  - packets, 16
  - traffic, 19–20

## K

- KAME project, 5
- keep state rule, 11
- kern.debug log level, 126
- kernel
  - enabling PF in, 10–11
    - GENERIC*, 61, 89–90, 100
    - GENERIC.MP*, 89, 100
  - memory, 125
  - messages, 36
- key exchange, 39
- Knight, Joel, 119

## L

- labels, 113–115
- Layer 7 proxying, 54
- license audit, 2
- limit option, 124, 125
- Linux systems
  - vs. BSD systems, xvi–xvii
  - migrating to BSD from, xvi
  - PF and, xvi–xvii
  - traceroute command, 29
- lists, 13–15, 115
- load balancing, 51–65
  - via hostated redirection, 51–65
  - via HTTPS relay, 54–55
  - NAT and, 51, 57
  - redirection and, 50–51, 57
  - via round robin redirection, 50–51
- load sharing, 50–51
- local networks
  - clients in, 46–48
  - redirection and, 58–59
  - restricting services to, 46–48
  - security issues, 48
  - sending email outside, 47–48
  - servers in, 46–48
  - specifying for gateways, 19

- log all option, 110–111
- log files
  - debugging and, 119
  - /etc/syslog.conf* file, 113
  - hostname.pflog1*, 77, 111
  - kern.debug log level, 126
  - labels, 113–115
  - rule data in, 108–115
  - rule numbers in, 109
  - spamd, 74, 77–78
  - tcpdump tool for, 108–111, 132–133
  - /var/log/messages* file, 36
  - /var/log/pflog* file, 108
- log keyword, 108, 111
- logger, 112–113
- logging, 107–119
  - all packets, 110–111
  - basics, 108–115
  - example of, 108–109
  - live display of traffic, 109–110
  - local, 112–113
  - log all option, 110–111
  - log keyword, 108, 111
  - monitoring tools, 115–119
  - options for, 107
  - periodic data, 115
  - pfflowd tool, 118
  - pflog interfaces, 77–78, 111
  - pflogd, 108, 112
  - pfstat utility, 116–118
  - pftop tool, 115–116
  - remote, 112–113
  - rule statistics, 113–115
  - SNMP tools, 118–119
  - syslog, 112–113
  - tools for, 115–119
  - verbose, 14, 74, 78–79, 133
- logic errors, 131–132
- logical NOT operator (!), 31, 74
- logs. *See* log files
- loopback interface, 123

## M

- MAC address filtering, 34, 40
- machines
  - backup, 98, 102–103
  - load sharing, 50–51
  - master, 98, 101–102
  - stand-alone, 11–15

- macros, 13–15
    - assigning logical names to network interfaces, 20–21
    - described, 14
    - as interface groups, 60
    - rule set, 13–15, 21, 23, 115
  - mail servers, 46–51, 56–59. *See also* email
  - man 8 `pfctl` command, 16
  - man pages (manual pages), xviii, 134
  - Management Information Base (MIB), 118–119
  - manual pages (man pages), xviii, 134
  - master machines, 98, 101–102
  - master/slave servers, 46
  - Maximum Transmission Unit (MTU), 30–31
  - `max-src-conn` option, 69, 70
  - `max-src-conn-rate` option, 69
  - memory
    - kernel, 125
    - physical, 125
    - pools, 124–125
    - rule sets, 109
    - tables, 31, 32, 70
  - method field, 73
  - MIB (Management Information Base), 118–119
  - Microsoft Windows systems, 3, 30
  - migrating
    - to BSD from Linux, xvi
    - from previous ftp-proxy version, 27
    - rules, 104
  - Miller, Damien, 118
  - monitoring tools, 115–119
  - `msg` field, 73
  - MTU (Maximum Transmission Unit), 30–31
  - MX use, 83
- N**
- `-n` option, 14, 109
  - name resolution, 14, 15, 42, 44
  - name service, 23
  - nameservers, 46, 48
  - NAT. *See* Network Addressable Translation (NAT)
  - nat rules, 21, 42
  - NAT Traversal (NAT-T), 39
  - NetBSD. *See also* Berkeley Software Distribution (BSD), systems
    - ALTQ on, 90–91
    - basic bridge setup on, 63–64
    - CARP setup, 100
    - enabling PF, 10–11
    - minimal setup, 10
    - PF compatibility and, xvi
    - `pfsync` not supported on, 100, 103
    - resources, 138
    - simple PF setup, 10–11
    - version, xiii
  - NetFlow
    - data model, 118
    - tools, 118
  - `net-snmp` package, 118–119
  - Network Addressable Translation (NAT), 17–23
    - DMZ setup in, 49–50, 56–57
    - firewalls and, 4
    - ftp-proxy program, 25–27
    - IP addresses and, 5
    - load balancing and, 51, 57
    - overview, 3–6
    - packet filtering and, 6
    - redirection, 57
    - servers in local network, 56–59
    - single NATed network, 57–59
  - network flow, 118
  - network hygiene, 127
  - network interfaces, 20–21
  - Network Time Protocol (NTP), 23
  - network traffic. *See also* traffic
    - block policies, 122
    - cleaning up, 127–129
    - forwarding with `sysctl` command, 19–20
    - ICMP, 28–31, 94
    - interactive, 93
    - live display of, 109–110
    - monitoring, 115–119
    - normalization, 128
    - overload, 96–97
    - spoofed, 128–129
    - streamlining, 127–129
    - TCP, 133
    - UDP, 14

- networks
  - advanced techniques, 45–66
  - books about, 138
  - bottlenecks, 95
  - DMZ, 49–50
  - filtering services, 45–51
  - local. *See* local networks
  - resources, 136–137, 138
  - routable addresses, 46–51
  - subnets, 59
  - traffic on. *See* network traffic
  - TCP/IP. *See* TCP/IP, networks
- no rdr rule, 84
- nodelay parameter, 55
- no-df parameter, 128
- nohup command, 113
- nonroutable addresses, 3, 65–66
- no-sync option, 105
- NTP (Network Time Protocol), 23
- nwid parameter, 37
- nwkey parameter, 37

**O**

- octets, 4
- on keyword, 18–19
- OpenBSD. *See also* Berkeley Software Distribution (BSD), systems
  - ALTQ on, 89
  - basic bridge setup on, 61–62
  - CARP setup, 100
  - clients, 40
  - enabling PF, 8–9
  - hardware support, 141–145
  - license audit, 2
  - PF compatibility and, xvi
  - resources, 135–140
  - simple PF setup, 8–9
  - versions, xiii, xvi, 6
- OpenBSD Foundation, 140
- openbsd-misc* list, 30
- operating system (OS) fingerprint, 97
- optimization
  - PF performance, 92–93, 119, 124, 136
  - rule sets, 126–127
- optimization option, 127
- OS fingerprinting, 97
- out keyword, 18–19

- outer addresses, 3
- out-of-order MX use, 83
- overload <bruteforce> option, 69
- overload mechanism, 70
- overload rules, 70, 96
- overload traffic, 96–97
- overloaded tables, 69, 70

**P**

- Packet Filter. *See* PF (Packet Filter)
- packet normalization, 128
- packet tagging, 60
- packet-filtering gateways. *See* gateways
- packets
  - ACK, 92–93
  - fragmented, 30, 124, 128
  - IPv6, 16
  - matching to state tables, 123
  - optimal size of, 30
  - spoofed, 128–129
  - tagging, 60
  - TCP, 92
- parentheses (( )), 21, 69
- pass rules, 12, 19, 22, 94, 114
- passtime value, 77
- path filter configuration option, 55
- path MTU discovery, 30–31
- PCI cards, 36
- performance, 92–93, 119, 124, 136
- periodic data, 115
- persist keyword, 31
- PF (Packet Filter)
  - code, 2, 6, 9, 26
  - creation of, 1
  - current state of, 6
  - disabling, 10, 131
  - early performance benchmark, 2
  - enabling at startup, 8–9
  - enabling for debugging, 131
  - enabling in kernel configuration, 10–11
  - enabling on FreeBSD, 10
  - enabling on NetBSD, 10–11
  - enabling on OpenBSD, 8–9
  - FAQs, xvi–xviii
  - gateways. *See* gateways
  - haiku, xix
  - history, 1

- Linux and, xvi–xvii
- logs. *See* log files; logging
- man pages, xviii, 134
- NAT and, 6
- overview, 1–3
- performance, 92–93, 119, 124, 136
- processing
  - block policies, 122
  - excluding specific interfaces
    - from, 123
  - matching packets to state
    - table, 123
  - timeouts, 69, 123–124, 127
- resources for, xviii
- rule sets. *See* rule sets
- statistics about. *See* statistics
- web interfaces for, 7
- PF configurations, 121–134. *See also*
  - basic setups
    - ALTQ setup on FreeBSD, 90
    - ALTQ setup on NetBSD, 90–91
    - ALTQ setup on OpenBSD, 89
  - becoming familiar with, 133–134
  - bridge setup, 61–64
  - CARP setup, 100–103
  - converting OtherProduct
    - setups to, xviii
  - customizing, 121–127
  - debugging rule sets, 131–133
  - defaults, 9, 12, 122
  - global settings, 122–127
  - IP forwarding, 19–20
  - maintaining control of, 133–134
  - optimizing performance, 92–93, 119, 124, 136
  - sample, 137–138
  - simple setup on FreeBSD, 9–10
  - simple setup on NetBSD, 10–11
  - simple setup on OpenBSD, 8–9
  - streamlining traffic, 127–129
  - testing, 12, 129–131
- pf.conf* file. *See* */etc/pf.conf* file
- `pfctl -s all` command, 16
- `pfctl -s info` command, 15–16
- `pfctl` tool
  - command lines, 9
  - described, 7, 16
  - displaying statistics with, 15–16
  - tidying tables with, 70–71
- `pfcts -vs rules` command, 114
- `pfcts -vs1` command, 114–115
- `pfctl -vsz1` command, 115
- `pfflowd` tool, 118
- `pflog` devices, 108, 113
- `pflog` interfaces, 77–78, 111
- `pflogd` logging daemon, 108, 112
- pfsense* configuration, xvii
- `pfstat` utility, 116–118
- `pfsync` protocol, 97–105, 118. *See also*
  - Common Address Redundancy Protocol (CARP)
- `pftop` tool, 115–116
- `pftpx` program, 26
- `ping` command, 29
- ping of death bug, 28
- policies, 122, 123, 127
- Postma, Peter, 90
- PPPoE (PPP over Ethernet), 21
- priority, 88–89
- priority-based queues, 88–89, 91–92
- `priq` option, 88–89, 91–92
- privileges, 8, 59
- probes, 29
- problems. *See* troubleshooting
- proxies
  - FTP, 24–27
  - Layer 7, 54
  - SYN, 47, 56

## Q

- queue schedulers, 88–89
- queues, 87–105. *See also* ALTQ (ALTErnate Queuing)
  - based on OS fingerprint, 97
  - class-based, 89, 93–94
  - described, 88
  - disciplines, 88–89
  - DMZ servers, 94–96
  - HFSC, 89, 90
  - `icmp`, 94
  - options, 88–89
  - overloading, 96–97
  - priority-based, 88–89, 91–92
  - subqueues, 88, 89, 92, 93
- quick keyword, 22
- quick rules, 22–23, 127, 132

## R

- Raadt, Theo de, 2
- Random Early Detection (RED), 90
- Ranum, Marcus, 13
- rc scripts, 9–11, 20
- rc system, 8
- rdr rule, 25
- RED (Random Early Detection), 90
- redirection
  - address pools, 50–51
  - hoststated, 51–65
  - load balancing and, 50–51, 57
  - local networks and, 58–59
  - NAT, 57
  - round robin, 50–51
  - web traffic, 43–44
- redundancy, 97–105
- Reed, Darren, 1–2
- relay definition, 55
- resources, 135–140
- return value, 122
- reverse engineering, 144
- RFC 1067, 118
- RFC 1631, 5
- RFC 1918, 5
- RFC 2018, 55
- RFC 2821, 75–76
- round-robin option, 51
- routable addresses, 3, 26, 46–51
- rule editor, xvii, 7
- rule numbers, 109, 132
- rule sets
  - access points, 38–39
  - blocking incoming/outgoing traffic, 13–15
  - CARP traffic, 104–105
  - debugging, 131–133
  - default, 8, 9
  - default deny, 13
  - lists, 13–15, 115
  - loading, 14
  - logic errors, 131–132
  - macros, 13–15, 21, 23, 115
  - managing, xvi
  - minimal, 12, 110
  - optimizing, 126–127
  - pfsync traffic, 98, 104–105
  - putting together, 104
  - readability of, 19

- restrictive, 13–15
- sample, xvii
- services by name in, 13
- simple, 11–12
- single, stand-alone machine, 11–15
- syntax errors in, 14
- testing, 12, 129–131

rules

- editing, xvii, 7
- evaluation order, 11, 22, 127
- flushing, 14
- labels, 113–115
- log data for. *See* log files; logging
- merging into tables, 127
- specific rules for gateways, 18–19
- statistics for, 113–115
- subsets, 127
- tracking statistics for, 113–115

ruleset-optimization option, 126–127

## S

- scp tool, 24
- SCP transfers, 93–94
- scrub keyword, 19, 127–128
- Secure Shell protocol (SSH), 39, 68–70
  - traffic, 93
  - transfers, 93
- security
  - attacks on. *See* attacks
  - CARP and, 103–104
  - FTP and, 24
  - IPv6 and, 5
  - local networks and, 48
  - NAT and, 6
  - network services, 16
  - wireless networks, 34, 40–44
- servers
  - in DMZ, 49–50, 94–96
  - file servers, 46–51
  - FTP, 26, 27
  - load balancing, 50–51
  - on local network, 46–48
  - mail servers, 46–51, 56–59
  - master/slave, 46
  - nameservers, 46, 48
  - queuing for, 94–96
  - SMTP, 83–84
  - webservers, 46–51, 56–59

- services
  - best-effort, 75
  - filtering, 45–51
  - names, 13, 23
  - restricting to local access, 46–48
  - in rule sets, 13
  - TCP, 15
- setups. *See* basic setups; PF
  - configurations
- sftp tool, 24
- shared-secret authentication, 82
- Simple Network Management Protocol (SNMP), 118–119
  - email, 71, 75, 85
  - MIBs, 118–119
  - return codes, 75
  - servers, 83–84
  - tools, 118–119
- skip option, 123
- slave servers, 46
- SNMP. *See* Simple Network Management Protocol (SNMP)
- source-tracking data, 124
- spam. *See also* email
  - blacklists, 72–74, 79–82, 84–85
  - greylisting, 75–85
  - greytrapping, 78, 80–83, 85
  - harvesting email addresses, 85
  - overview, 71
  - SMTP email and, 71, 75, 85
  - whitelists, 73, 77, 78, 83–84
- SpamAssassin, 72
- spamd connections, 110
- spamd program (OpenBSD), 71–85
  - basic configuration file, 73–74
  - blacklists, 72–73
  - database synchronization, 82
  - example tasks, 78–83
  - greylists. *See* greylisting
  - greytrapping, 78, 80–83, 85
  - log files, 74, 77–78
  - manual intervention, 78
  - out-of-order MX use, 83
  - overview/conclusions, 71–72, 84–85
  - resources, 139
  - routine operations, 78–83
  - synchronization, 82, 110
  - tables, 71
  - tarpitting, 72
  - traplists, 81–82, 85
- spamd program (SpamAssassin), 72
- spamdb
  - database, 78
  - program, 74, 78, 80–82
- spamd.conf* file, 73–74, 81
- spamd-setup program, 73–74
- spamlogd program, 77–78
- SPF records, 84
- spoofed packets, 128–129
- src.track value, 124
- SSH. *See* Secure Shell protocol (SSH)
- ssh authentication, 41
- ssh connections, 110
- ssh sessions, 41
- ssl options, 55
- state information, 14
- state tables
  - described, 11–12
  - matching packets to, 123
  - memory pool size, 125
  - statistics, 117
  - synchronization, 98, 103–104, 105
  - timeout options, 123, 127
  - unmatched entries, 15
- state-policy option, 123
- state-tracking options, 69, 96–97
- statistics
  - displaying with *pfctl*, 15–16
  - graphing with *pfstat*, 116–118
  - monitoring with *pftop*, 115–116
- sticky-address option, 51
- stuttering, 72
- subnet traffic, 59
- subnets, 59
- sudo, 8–15
- SYN packets, 97
- SYN proxying, 47, 56
- sync listener, 82
- sync target, 82
- synchronization
  - spamd, 82, 110
  - state tables, 98, 103–104, 105
  - time, 23, 110
- SYN-flood attacks, 47
- synproxy flag, 56
- synproxy state option, 47

- sysctl command
  - access point setup, 38
  - bridge setup, 63
  - CARP setup, 100–101
  - forwarding network traffic, 19–20
- syslog system log facility, 112–113
- system fingerprinting, 97

## T

- tables, 31–32
  - address, 125
  - backup, 53, 54
  - described, 31
  - expired entries, 70–71
  - initializing, 31
  - loading from files, 31
  - memory, 31, 32, 70
  - merging rules into, 127
  - names, 31
  - overloaded, 69, 70
  - removing entries, 70–71
  - replacing contents of, 32
  - size of, 70
  - state. *See* state tables
- tag keyword, 60
- tagged keyword, 60, 62
- tagging packets, 60
- tags, 60, 62
- tail -f command, 36
- tarpitting, 72
- tcp options, 55
- TCP packets, 92
- TCP services, 15
- TCP traffic, 133
- tcpdump tool, 108–111, 132–133

- TCP/IP
  - networks
    - bandwidth overhead, 91
    - FTP and, 24
    - wireless networks, 36–37
  - stacks, 16, 88
- testing
  - PF configurations, 129–131
  - rule sets, 12, 129–131
- text editors, 7
- time synchronization, 23, 110
- timeout option, 123–124
- timeouts, 69, 123–124, 127
- to keyword, 18
- ToS (type of service) field, 92
- ToS Delay bit, 92
- ToS flag, 93
- traceroute command, 29–30
- TRACERT.EXE* program, 30
- traffic. *See also* network traffic
  - block policies, 122
  - CARP, 101, 103, 105
  - ESP, 39
  - ICMP, 28–31, 94
  - interactive, 93
  - IPv6, 19–20
  - live display of, 109–110
  - overload, 96–97
  - pfsync, 98, 104–105
  - spoofed, 128–129
  - SSH, 93
  - subnet, 59
  - TCP, 133
  - UDP, 14
  - web, 43–44
- traplists, 81–82, 85. *See also* spam
- trapped entries, 82

troubleshooting. *See also* debugging;  
errors  
considerations, 28–31  
ICMP traffic and, 28–31  
path MTU discovery, 28, 30–31  
ping command, 29  
traceroute command, 29–30  
-ttt option, 109  
TXT records, 84  
type of service (ToS) field, 92

## U

UDP traffic, 14  
Unix systems, 29–30, 68, 107, 115  
url hash, 55  
user groups, 137  
users  
authentication, 40–44  
FreeBSD, 100  
local networks, 93  
NetBSD, 100  
OpenBSD, 100

## V

-v option, 14, 74, 78–79  
*/var/log/messages* file, 36  
*/var/log/pflog* file, 108  
*/var/run/dmesg.boot* file, 36  
verbose logging, 14, 74, 78–79, 133  
Virtual Private Networks (VPNs), 39  
-wv flag, 132

## W

web interfaces, PF, 7  
web traffic, 43–44

webservers, 46–51, 56–59  
websites  
book-related, 139–140  
incompatible with greylisting,  
83–84  
resources on, 135–140  
WEP (Wired Equivalent Privacy), 35,  
37, 40  
key, 37  
whiteexp value, 77  
whitelists, 73, 77, 78, 83–84  
*whitelist.txt* file, 84  
Wi-Fi Net News site, 34  
Wi-Fi Protected Access (WPA), 35  
Windows systems, 3, 30  
Wired Equivalent Privacy (WEP), 35,  
37, 40  
key, 37  
wireless access points, 38–39  
wireless gateways, 41  
wireless networks, 33–44  
access point, 38–39  
attacks on, 35–40  
case study, 142–143  
configuring for TCP/IP, 36–37  
gateways for, 36–42  
hardware for, 35–36, 142–144  
IEEE 802.11 standard, 33–36  
protecting with authpf, 40–44  
resources, 139  
security, 34, 40–44  
setting up simple network, 36–40  
VPNs, 39  
WEP encryption, 35, 37, 40  
WPA encryption, 35  
WPA (Wi-Fi Protected Access), 35