

Building Firewalls with OpenBSD and PF

Building Firewalls with OpenBSD and PF

Jacek Artymiak

Second Edition

Lublin

Index

Symbols

!=, 117
", 103-104
#, 67
\$, 67
%, 198
(), 115
->, 139, 146, 152
/, 54-58
<, 117
<=, 117
<>, 117
<spamd>, 240
=, 117
>, 117
><, 117
>=, 117
\, 105
{}, 103-104

Label macros

\$dstaddr, 180
\$dstport, 180
\$if, 180
\$nr, 180
\$proto, 180
\$srcaddr, 180

\$srcport, 180
\$user_id, 235
\$user_ip, 235

Files

/bin/sh, 235
/bsd, 67, 98
/dev/kmem, 54
/etc/adduser.conf, 68
/etc/authpf/authpf.allow,
234, 236
/etc/authpf/authpf.conf,
234-235
/etc/authpf/authpf.message,
234
/etc/authpf/authpf.problem,
234
/etc/authpf/authpf.rules, 235
/etc/authpf/banned, 234
/etc/authpf/users, 235
/etc/bridgename, 81-84, 92,
94, 232
/etc/fstab, 55, 102
/etc/group, 68
/etc/hostname, 61, 78, 84, 94,
143
/etc/hosts, 60-61, 77
/etc/inetd.conf, 71, 86

- `/etc/login.conf`, 235
 - `/etc/mygate`, 62
 - `/etc/myname`, 76
 - `/etc/netstart`, 84, 91
 - `/etc/networks`, 77
 - `/etc/newsyslog`, 227
 - `/etc/newsyslog.conf`, 228
 - `/etc/pf.conf`, 12, 61, 77, 86, 96, **103-123**, 121, 123, 127-128, 139-140, 146, 152, 187, 194, 222-223, 235-237, 246, 250, 252, 269
 - `/etc/pf.conf`, changing order of sections, 105
 - `/etc/pf.conf`, editing, 119-120
 - `/etc/pf.conf`, rule evaluation order, 104
 - `/etc/pf.os`, 168-169, 269
 - `/etc/protocols`, 111, 165
 - `/etc/rc.conf`, 80-81, 96, 104
 - `/etc/rc.local`, 240
 - `/etc/rc.securelevel`, 96
 - `/etc/resolv.conf`, 61, 78
 - `/etc/services`, 117, 168, 252, 271
 - `/etc/spamd.conf`, 269
 - `/etc/ssh/sshd_config`, 68, 234
 - `/etc/sudo`, 69
 - `/etc/sudoers`, 69
 - `/etc/sysctl.conf`, 84
 - `/usr/sbin/authpf`, 235
 - `/var/log/authlog`, 226
 - `/var/log/daemon`, 226
 - `/var/log/maillog`, 226
 - `/var/log/messages`, 226
 - `/var/log/pflog`, 224-227
 - `/var/log/secure`, 226
 - `/var/log/wtmp`, 226
- Address wildcards
 - `:broadcast`, 115
 - `:network`, 115
 - Numbers
 - 4.2BSD, 58
 - 802.11, 303-304
 - A
 - `adaptive.end`, 177
 - `adaptive.start`, 177
 - `add` (in `brconfig`), 82-83
 - address redirection, *see* trans-
lation, packet
 - Addison-Wesley, 120, 303-305
 - address families, 103, **111**, 164-165
 - Address Resolution Protocol (APR) broadcast, 89
 - Address Resolution Protocol (APR) cache, 89-90, 93, 154
 - Address Resolution Protocol (APR) proxy, 153-154
 - Address Resolution Protocol (APR), 84
 - Address Resolution Protocol (APR), static, 93, 154
 - Address Resolution Protocol (ARP), 89-95
 - addresses, 103-104
 - dynamic assignment of, 115-116

- IP, **112-114**
- addspan, 232
- adduser, 68
- afterboot, 269
- AIX, 48
- alias, 78, 84, 142, 194, 253
- all, 114, 165-166, 169-170
- allow-opts, 179
- Alternative Queueing (ALTQ), 10,
13, 104, 191, **195-219**, 240,
246, 254
performance 218-219
- anchor, 103, **109-110**, 162,
187-189, 235-236
- announcements, security, 71
- antispoof, **181**, 155
- any, 115-117, 165-166, 169-170
- Apache, 133
- apdm, 49
- apm, 49
- Apple Macintosh, 37
- AppleTalk, 83
- apropos, 162, **167-268**
- arp, 93
- ascii, 103
- ASCII, 103, 107
- ATA, 38, 41-42, 48
- attacks, 1
- attacks, motives of, 6
- auth, 157
- authentication, 10, 13, 31, **233-238**
- authpf, 13, 31, 46, 83, 145, 186,
233-238, 268
sshd configuration, 234
- AWK, 120
- B
- balance, 30
- bandwidth shaping, 13, 31,
40, 104, **195-219**
- bandwidth, 196-197
- base34.tgz, 63-64
- bastion host, 24, 287-288
- Bellovin, Steven M., 27, 135,
303
- binat, 151-153
- binat-anchor, 109, 235-236
- BIOS, 39, 42, 46-48, 52, 65
- bitmask, 164, 194
- block (in brconfig), 92
- block, 156-157
- block-policy, 159
- blocknoip, 83
- boot floppies, 35, 51, 52, 60
- boot, 96, 98
- booting, 52
- borrow, 198
- bpf, 269
- brconfig, 82, 84, 92, 232
- bridge, 84, 232
configuration, 81-84
interaction with NAT,
136
incompatibility with
drop return, 160
invisible, 21, 81-84,
27-28, 252, 295-296
learning, 94
visible, 82-82
- bridgename, *see* /etc/bridge-
name
- BSD web sites, 3

-
- bsd, 63
 - bsd.rd, 63
 - C
 - cables, 50
 - CardBus, 51
 - cbq, 196
 - CBQ, 196, 198, **206-213**, 219
 - cd, 72, 75, 88, 121-122
 - CD-ROM, 34-65
 - CERT, 303
 - Chapman, D. Brent, 305
 - Cheswick, William R., 27, 135, 303
 - chflags, 96
 - chgrp, 81
 - chmod, 54, 81, 103, 121, 123
 - chown, 81, 103
 - chromatic, 3
 - Classless Inter-Domain Routing (CIDR), 112
 - ClientAliveCountMax, 234
 - ClientAliveInterval, 234
 - code, 173
 - Coleman, Chris, 3
 - Colls, 256
 - COM1, 47
 - COM2, 47
 - community, 3, 14-15
 - comp34.tgz, 63-64
 - comp34.tgz, 71-72
 - Computer Shop of Calgary, The, 4
 - comsat, 70
 - config, 98
 - configuring OpenBSD, 12, 67-102
 - console, 47
 - console, serial, 46-47
 - const, 108
 - Cooper, Simon, 305
 - cp, 88, 101, 122, 237
 - cron, 185, 226, 228
 - crontab, 185, 226-228
 - Crypto Law Survey, 11
 - cryptography, 11
 - CURRENT, 72
 - CVS tutorial, 12, 103-123
 - CVS, 12, 72, 76, 121-123, 305
 - cvs, 88, 120-123, 250
 - CVSROOT, 121
 - D
 - DaemonNews, 3
 - date, 97
 - daytime, 70-71
 - ddb.panic, 95
 - DDoS, *see* Denial of Service
 - de Raadt, Theo, 3, 299-300
 - debarriage, 71
 - default, 198
 - delete (in brconfig), 82-83
 - Dell, 42
 - Demilitarized Zone (DMZ), 193, 208, 216, 254
 - Demilitarized Zone (DMZ), 37, **25-27**, 61-61, 77, 87, 134, 138, 146-148, 229, 251, 284
 - Denial of Service (DoS), 125, 251
 - Destination Unavailable, 274
 - destination-unreachable, 157
 - DF, 129
 - DHCP, 186

- dhcp, 61, 62
- diagnostics, network, 273
- Digital Alpha, 37-38, 46
- Digital VAX, 38
- DIN, 46
- directions, packet, 110
- disk space calculations, 54-58
- disklabel, 102
- disks, configuring, 102
- Distributed Denial of Service (DDoS), 6, 8
- dmesg, 102, 111, 162
- Dooley, Kevin, 27, 46, 303
- DOS, 35
- down (in brconfig), 82-83
- downloading OpenBSD, 34, 50
- drop, 157-160
- DSL, 43-44, 115, 130, 134, 138, 246, 287
- dst (in brconfig), 92
- du, 58
- dup-to, 162-164
- E
- eBay, 47
- Echo Reply, 273-274
- Echo Request, 273-274
- echo, 236
- echoreq, 175
- ecn, 198
- ed, 62
- ee, 119
- Emacs, 119
- Enidan Technologies, 47
- EPROM, 19
- etc34.tgz, 63-64
- ethereal, 257
- Ethernet address, 84, 89-95
- Ethernet, 304
- evangelists, 4
- exit, 69, 101, 121
- export, 121
- F
- failover, 31
- Farrow, Rich, 175, 303
- fastroute, 162, 164
- fdisk, 102
- FDISK, 54
- file (in table definitions), 108
- File Transfer Protocol (FTP)
 - active, 85
 - interaction with pf, 276
 - br Microsoft IIS, 276
 - mirrors, 34, 36, 51, 72
 - passive, 85, 87
 - problems, 85-89
 - proxy, 151, 273, 276
 - Trivial, 285
- ftp, 72
- ftp-proxy, 86-89, 171, 276
 - reverse, 87, 89, 276
- filtering policy, 17-18
- filtering rules for translated packets, 181-183
- filtering rules, order of evaluation, 161
- filtering, packet, 7, 10, 12-13, 104, **155-183**, 271-272
- fingerprinting, 157
- fingerprints, 169
- firewall
 - a definition, 18-19
 - designs, 12, 17-31
 - hardware, 19, 30

- reasons for using, 7
 - software, 19
- flags, 171-172
- Fleck, Bob, 46, 304
- floppy34.fs, 51
- floppyB34.fs, 51
- floppyC34.fs, 51
- fragment crop, 131
- fragment drop-ovl, 129, 131
- fragment reassemble, 128-129, 131
- fragmentation, packet, 12
- fragmnet crop, 129
- FreeBSD pf port, 33
- FreeBSD, 1, 10, 33-35
- FreeDOS, 36
- Frish, Aileen, 5, 27, 303
- from, 115-117, 165-166
- fsck, 102
- fstab, 55
- Fujitsu, 42
- fwanalog, 266

- G

- game34.tgz, 63-64
- Gast, Matthew, 46, 303
- gcc, 91
- Grabowski, Artur, 3
- grep, 84, 91, 180, 238
- group, 170-171
- gzip, 227

- H

- halt, 65
- Handley, Mark, 132, 304
- hard disks, 42-43
- hardening OpenBSD, 12, 70
- hardware platforms, 10, 36-38, 72
- hardware requirements, 36-50
- Hartmeier, Daniel, 2-3, 5, 9, 300
- HDPCP, 61, 62
- helping the OpenBSD project, 297-302
- Hewlett-Packard (HP), 48
- Hewlett-Packard HP 9000, 38
- Hewlett-Packard PA-RISC, 38
- Hewlett-Packard, 42
- hfsc, 196, 213
- Hierarchical Fair Service Curve, 196, 198, 206, **213-218**, 219
- Hogan, Christine, 18, 27, 46, 304
- Holland, Nick, 3
- Hook, Austin, 4
- hops, 129
- hostname, 76-77
- Howell, Paul, 132, 304
- HP-UX, 48
- HTTP proxy, 63
- HTTP, 61-63
- HTTPS, 284

- I

- i386, 35, 37-38, 50, 72,
- IBM, 42, 48
- ICMP packets, 157-159, 172-175, 178, 271, 273
- icmp-type, 173, 175

-
- icmp.error, 178
 - icmp.first, 178
 - ICMPv4, 172-173
 - ICMPv6, 172-173
 - icmpv6, 173
 - ident, 70
 - IDS, *see* NIDS
 - Ierrs, 256
 - ifconfig 78-80, 84, 89-91, 93, 111, 129, 135, 153, 194, 253
 - IMAP, 284
 - import, 121
 - in, 110, 160
 - inet (in ifconfig), 79
 - inet, 111, 164-165
 - inet6 (in ifconfig), 79
 - inet6, 111, 164-165
 - inetd, 87
 - installing OpenBSD, 12, 33-65
 - installing over FTP, 35, 59
 - installing over HTTP, 35, 59
 - installing over NFS, 35, 59
 - interface, 162
 - interface, network, 43-46
 - interfaces, 110-111
 - Internet Assigned Numbers Authority, 112, 117, 165, 168, 271
 - interval, 178
 - intro, 269
 - IP forwarding, 84, 137
 - IP networking, 12
 - IP options, 179
 - IPng, 135
 - IPSec, 10
 - IPv4, 10, 24, 27-28, 83, 104, 111-114, 126, 133-136, 142, 151, 164, 272, 284
 - IPv4 private addresses, 21-22
 - IPv4 public addresses, 22-22
 - IPv6, 10, 24, 27-28, 83, 85, 111, 113-114, 116, 126, 131, 133, 135-136, 142, 164, 173, 284
 - ipv6-icmp-type, 173
 - IPX, 83
 - IRC, 284
 - IRIX, 48
 - ISA, 38
 - ISDN, 43-44, 246
- J
- J1, 47
 - Jaap-Koops, Bert, 11
 - Jacobs, Leonard, 3
 - Jahanian, Farnam, 132, 304
 - jed, 119
 - jftpgw, 30
 - joe, 119
- K
- KAME, 195
 - kd85.com, 4, 33, 298, 302
 - keep state, 173-179
 - kern.securelevel, 96
 - kernel configuration, 97-101
 - kernel, 12, 137, 198
 - keyboard, 46
 - kill, 75, 87
 - Koch, Christian, 9
 - Kreibich, Christian, 132, 304

L

label, 180
labels, 180
Lamb, Linda, 119, 304
large-scale networks, 27, 303
LDAP, 284
less, 72, 162, 268
licence, 10
limit frags, 128, 130
Limoncelli, Thomas A., 18, 27, 46, 304
linkshare, 213,
Linux, 1, 10, 34, 47-48, 51
load balancing, 10, 13, 31, 40, 104, **191-195**
log (in cvs), 121
log, 160-161
log-all, 160-161
logging, packet, 7, 13, 30, 40, 49, 126, 164, 221-232
 bandwidth and disk space requirements, 229-232
 enabling, 222
 log analysis, 222
 policy, 221-222
 selecting packets, 224-226
 bridge, on a, 232
 log file size, 228
 log configuration, 226
long-lines, breaking, 105
LPD, 284
ls, 227, 267
lynx, 91

M

MAC address, 84

MAC address, changing, 81
MAC filtering, 91
MAC, 84
macros, 12, 75, 88, 103-104, **106-107**, 187
make, 88
Malan, G. Robert, 132, 304
malformed packets, *see* normalization, packet
man, 14, 226, 228, 229-230, 267
man34.tgz, 63-64
management, firewall, 259-266
 additional tools, 266
 anchors, 263
 disabling, 259
 enabling, 259
 flushing rules, 260
 loading rules, 259
 macros, 260
 operating system fingerprints, 265
 options, 262
 packet filtering rules, 262
 packet translation rules, 262
 queues, 262
 states, 264
 statistics, 265-266
 tables, 260
 testing rules, 260
manual, 13-14, 50, **267-269**
masquerading, *see* translation, packet
max, 179
max-mss, 129, 131

-
- Maxtor, 42
 - Media Access Control (MAC),
 - 89-95
 - memory, 41, 246
 - mg, 119
 - Microsoft Global Catalog, 284
 - Microsoft Windows, 35-36, 43,
 - 47, 51
 - Middle Digital, 47
 - min-ttl, 129, 131
 - mkdir, 120-121, 236
 - modem, 43-46, 115
 - modulate state, 173-179
 - monitor, 46
 - motherboard, 38
 - Motorola 680x0, 37, 39
 - Mototrola VME 680x0, 38
 - mount point, 58
 - mount, 54, 102
 - MP3, 13
 - mrtg, 256
 - MS-DOS, 51, 54
 - MSS, 129
 - mtr, 252
 - MTU, 129
 - mv, 72, 101
 - MySQL, 284

 - N

 - named, 191
 - nano, 119
 - nat 138-145
 - nat-anchor, 109, 235-236
 - Nazario, Jose, 3
 - ncftp, 50
 - net.inet.ip.forwarding, 84
 - net.inet6.ip.forwarding, 85

 - NetBIOS, 48
 - NetBSD pf port, 33
 - NetBSD, 1, 10, 33-35, 49
 - netstat, 255-256
 - Network Address Translation (NAT), 10, 12, 22, 27, 30-31, 44, 84, 87, 96, 104, 117, 128, 130, 133-136, 138, 140-146, 151, 153-155, 160-161, 171, 181, 187, 191, 203, 218, 245-246, 249, 252, 292-295. (*See also* translation, packet.
 - bidirectional, *see* binat
 - problems with, 142
 - proxy, 144
 - network configuration, 59-62, 76
 - Network File System (NFS), 61-62, 129
 - Network Intrusion Detection System (NIDS), 12, 30, 42, 125, 129, 186, 230, 251
 - Network Time Protocol (NTP), 97, 284
 - networking, 269
 - newfs, 102
 - newsyslog, 226, 228-229
 - nmap, 102, 253, 273, 71
 - Network News Transfer Protocol (NNTP), 284, 305
 - no, 138, 145, 151-152
 - no-df, 129, 131
 - no-route, 114
 - nodev, 54-56
 - nomatch, 169

- Non-Disclosure Agreement (NDA), 43
- normalization, packet, 7, 10, 12, 104, 125-132, 104, 304
 - fine-tuning, 127-131
- nosuid, 54-56
- Novell, 36
- O
- O'Reilly & Associates Network, 2-3
- O'Reilly & Associates, 3, 120, 303-305
- O'Reilly, Tim, 3
- Oerrs, 256
- official CD-ROM set, 33-34, 297-298
- on (in brconfig), 92
- ONLamp.com, 2
- Open Source, reasons for using, 7-9
- OpenBSD 3.3, 3, 4
- OpenBSD 3.4, 63
- OpenBSD developers, 3-4, 297, 299-300
- OpenBSD Gazetteer, The, 3, 303
- OpenBSD Journal, The, 3
- OPENBSD, 72
- OpenBSD, reasons for using, 9-11
- OpenBSD, release schedule, 9
- OPENBSD_3_4, 88
- OpenSSH, 4, 10, 29
- operating system fingerprints, 168-169
- optical link, 49
- optimization, 13, 245-247
 - aggressive, 247
 - conservative, 247
 - default, 247
 - high-latency, 247
 - normal, 247
 - satellite, 247
 - timeout options, 247
- os, 168-169
- other, 178
- other.first, 178
- other.multiple, 178
- other.single, 178
- out, 110, 160
- P
- packet fragmentation, *see* normalization packet
- Parameter Problem, 275
- partitions, disk, 54-59
- pass (in binat rules), 152
- pass (in brconfig), 92
- pass (in nat rules), 138
- pass (in rdr rules), 149
- pass, 156-157
- password, 62, 67, 69
- patch, 74, 88
- patching, 12, 70-76
- Paxson, Vern, 132, 304
- PC Weasel 2000, 47
- PC Weasel, 47
- PC-DOS, 36
- PC/104, 46
- PC/104-Plus, 46
- PCI, 38
- PCMCIA, 46, 51, 53, 60
- performance, 39-41
- Perl, 120
- PermitRootLogin, 68

-
- persist, 107-108
 - pf options, 104
 - pf, reasons for using, 9-11
 - pf.conf, *see* /etc/pf.conf
 - pf configuration file, *see*
 /etc/pf.conf
 - pfctl, 69, 81, 87, 96, 103-105,
 108-109, 112, 116, 126, 128,
 149, 160, 167-169, 174, 180,
 187, 224, 235-236, 250,
 259-266, 269
 - pflog, writing rules for, 235
 - pflog, *see* /var/log/pflog
 - pflog0, 223
 - pflogd, 81, 269
 - pfstat, 266, 269
 - pftcl output options, 259
 - pftop, 266
 - pico, 119
 - ping, 84, 175, 187, 250-252, 256,
 273
 - pkg_add, 102
 - pool options, 140
 - POP, 284
 - port numbers, 165, 271
 - port redirection, *see* translation,
 packet
 - port, 116-117, 166-168, 170
 - ports (TCP and UDP), 103,
 116-117
 - higher, 271
 - lower, 271
 - ports.tar.gz, 72
 - PostgreSQL, 284
 - Potter, Bruce, 46, 304
 - Prentice-Hall, 120
 - priority 198
 - Priority Queueing (PRIQ),
 199-206
 - priority, 198
 - priq, 196
 - processor (CPU), 39. *See also*
 hardware platforms.
 - PROM, 89
 - propolice, 10
 - proto, 111-112
 - Protocol, 234
 - protocols, 103, **111-112**, 165
 - PROT_, 10
 - proxy, 30, 273
 - proxy-suite, 30
 - ps, 233
 - PS/2, 46
 - PuTTY, 47
 - Python, 120
- Q
- qlimit, 196
 - QoS, 31, 40, 104
 - queue, 199
 - queue, child, 197-198
 - queue, parent, 196-197
 - queueing, packet, 104
 - queues, 195-199
 - quick, 161
 - quick, anchors and, 162
 - QuickTime, 284
- R
- Rahn, Dale, 3
 - raid, 102
 - RAID, 42, 35, 51, 102, 230,
 255
 - raidctl, 102, 230

- random, 164, 194-195
- random-id, 130, 131
- rdr, 145-151
- rdr-anchor, 109, 235-236
- Real Audio, 284
- realtime, 213
- reassemble tcp, 128, 130
- reboot, 75, 91, 101
- reboot, automatic, 95
- Recv-Q, 255
- RED IN/OUT (RIO), 198
- RED, 198
- red, 198
- redirection, packet, *see* translation, packet
- Reed, Darren, 2
- reply-to, 162-164, 195
- require-order, 105
- return, 157-160
- return-icmp, 157-160, 164
- return-icmp6, 157-160
- return-rst, 157-160
- RFC Editor, 303
- rio, 198
- rm, 234
- rmuser, 70
- Robbins, Arnold, 119, 304
- root, 62, 67-70, 80-81, 133-134, 171, 226-228
 - dangers of being, 67
- Rosenthal, Morris, 49, 304
- round-robin, 164, 191, 193-194
- route, 84, 162, 187
- route-to, 162-164
- routing options, 162-164
- routing, 12, 84, 114, 195, 252
- RS232, 47
- RSVP, 271
- Rubin, Aviel D., 27, 135, 303
- rylesets, **103-123**
- rulesets, dynamic, 7, 13, **185-189**
- S
- Samsung, 42
- sappend, 96
- scaling factor, 177
- scanning, 157, 273
- scheduler choices, 218-219
- schg, 96
- SCI, 53
- scp, 75, 119, 121-122
- screened host, 20
- screened LAN, 22
- scrub options, 127
- scrub rules, 104
- scrub, 126
- scrubbing, *see* translation, packet
- SCSI, 38-39, 42, 48-49
- sea, 91
- sea.c, 91
- Seagate, 42
- securelevel, 96
- Securing Small Networks
 - with OpenBSD, 2
- Send-Q, 255
- sendmail, 133, 157
- sequence number attacks, 303
- sequence numbers, 175
- serial, 47
- services, non-essential, 70
- setenv, 88

-
- setgid, 171
 - setuid, 171
 - SGI, 48
 - sgid, 54
 - Single Board Computer (SBC), 46
 - sleep, 250
 - Symmetric Multi-Processing (SMP), 38, 41
 - Simple Mail Transfer Protocol (SMTP), 239, 284, 285
 - snort, 30, 186
 - software commoditization, 8
 - software requirements, 33-36
 - software, additional, 101-102
 - Solaris, 48
 - Source Quench, 275
 - source-hash, 164, 194-194
 - spam filtering, 10, 239-243
 - spamd, 153, 239-243, 269
 - spamd-setup, 269
 - span port, 232
 - Spurgeon, Charles, 46, 304
 - Squid, 30
 - src (in brconfig), 92
 - src.tar.gz, 72, 88
 - sreened host/LAN, 289-293
 - SSH, 47, 67, 164, 233, 237, 276, 299
 - rules for, 277, 283
 - SSH1, 10
 - SSH2, 10
 - sshd, 68, 236
 - SSL, 19, 284
 - stateful filtering, 10, **173-179**
 - static-port, 164, 195
 - Stevens, W. Richard, 5, 129-130, 132, 172, 178-179, 269, 304-305
 - Strayer, W. Timothy, 27, 135, 303
 - streamer, 231
 - su, 68-68, 70, 75, 88, 121-122
 - sudo, 69-70, 116, 128, 149, 180, 187
 - sudoer, 70
 - suid, 54
 - Sun SPARC, 38, 46
 - Sun UltraSPARC, 38
 - SVGA, 46
 - swap partition, 56-58
 - encryption, 98
 - swapping, 42
 - SYN floods, 175
 - synproxy state, 173-179
 - sysctl, 84, 95-96
 - syslog, 227
 - syslogd, 226
 - systat, 255
 - system administration, 303
 - system statup, 12
 - systrace, 10

 - T

 - table, 107-108
 - tables, 103-104, **107-109**, 187
 - tag, 118-119
 - tagged, 118-119
 - tagging, packet, 118-119
 - tape drive, 49
 - tar, 72-73, 88
 - Tatham, Simon, 47
 - tbrsize, 197

- Tcl, 120
- TCP flags, 171-172
 - ACK, 171
 - CWR, 172
 - ECN-Echo, 172
 - FIN, 172
 - PUSH, 172
 - RST, 171
 - SYN, 171, 174
 - URG, 171
 - TCP services, 283-285
- TCP state transition cycle, 178
- TCP, 43, 125, 130, 133, 135, 151, 159, 165, 167, 171, 173, 175, 177-178, 271, 276, 284, 304-305
- tcp.established, 177
- tcp.closed, 177
- tcp.closing, 177
- tcp.finwait, 177
- tcp.first, 177
- tcp.opening, 177
- TCP/IP networking, 5
- tcpdump, 22, 225, 226, 256, 257, 273, 90
 - expressions, 225, 257
- tcpreplay, 257
- tcpshow, 257
- tcpslice, 257
- tcpstat, 257
- tcptrace, 257
- telnet, 252, 256
- template, 14, 105, 271-273, 287
- terminal emulator, 47
- terminal, 47, 63
- testing, firewall, 249-258
 - additional tools, 258
 - host availability, 250-252
 - pencil test, 249
 - scanning, 253
- threats, 5-7
- Time Exceeded, 275
- time, 70-71, 97
- timeout frags, 128, 178
- timeout interval, 178
- timeout, 177, 179
- timezone, 64
- tinyproxy, 30
- to, 115-117, 169-170
- Token Bucket Regulator (TBR), 197
- top, 255
- Toshiba, 42
- totd, 30
- touch, 234-235
- traceroute, 131-132, 252, 256
- traceroute6, 131-132, 256
- translation, packet, 7, 10, 104, 133-154, 272-273
 - rule evaluation order, 137
- TTL, 129-130, 158
- tun0, 225
- U
 - UDP services, 284-285
 - UDP, 111, 133, 159, 165, 167, 171, 174, 178, 271, 276, 284
 - udp.first, 178
 - udp.multiple, 178
 - udp.single, 178
 - UKC, 98, 101
 - Uninterruptible Power Supply (UPS), 49

Unix Domain Protocols, 305
Unix, 5, 35, 43, 97, 118, 186, 299
unknown, 171
up (in brconfig), 82-83
upperlimit, 213
uptime, 254
user management, 12, 67
user mode, single, 96
user, 170-171
users, adding new, 67-68
users, removing, 70

V

Vallat, Miod, 3
Vandeputte, Wim, 3-4
Vesperman, Jennifer, 305
VGA, 46
vi, 68, 79, 119, 228 237, 304
video card, 36
vim, 119
vipw, 234-235
visudo, 69-70
vm.swapencrypt.enable, 95
vmstat, 254
VPN, 12, 135-136, 140, 151, 305
vt220, 53

W

Watson, David, 132, 304
web cache, 150-151, 304
Wessels, Duane, 150, 304
wget, 50-51
wheel, 68, 80
WHOIS, 284
WiFi, 46
wily, 119

winmodems, 43
wireless networks, 31
Wright, Gary R., 5, 129-130,
132, 172, 178-179, 304
Wright, Jason L., 3
W^X, 10

X

X Display Management Con-
trol Protocol, 285
X Font Service, 284
X Window System, 64, 284
XEmacs, 119
XF4.tar.gz, 72

Y

Yuan, Ruixi, 27, 135, 303

Z

ZIP, 48-49
Zwicky, Elizabeth D., 305