

---

# Index

---

## A

- A switch (iptables), 111-112
- ACCEPT rules, 106, 149-150
- accepting only SMTP connections from specific hosts, 262-263
- access
  - filtering to forwarded servers, 278
  - restricting with firewall rules (FTP), 291-292
- action plans, creating, 67
- adding rules, 112
- AIDE (Advanced Intrusion Detection Environment), 60
- AIM (AOL Instant Messenger), 314-317
- ALLOW policy, 164
- allowing MySQL connections, 253-255
- analyzing
  - risk management, 26-29
  - solutions, 68
  - traffic utilization, 157-158
- AOL Instant Messenger (AIM), 314-317
- application layers, troubleshooting OSI model, 91
- application proxies, 17
- apt-get, 49
- arp cache, network diagnostics, 173-174
- assets
  - isolating, 36-37
  - quantifying value of, 28
- AUTH connections, TCP reset for, 146

## B

- bad flag rules (example firewall), 134-135
- bad IP options rules (example firewall), 135
- basic masquerading firewalls, 224-226
- basic SNAT firewalls, 226-228

## blocking

- AIM traffic, 315-317
- clients from accessing websites, 279
- ICQ, 318
- internal users from sending mail through firewalls, 261-262
- MSN messenger traffic at firewalls, 310
- outbound DHCP, 328-329
- outbound NetMeeting/GnomeMeeting traffic, 308
- Yahoo Messenger traffic, 311-314

## bridging, 203

- building inline transparent bridging firewalls with ebtables, 207-210
- common questions, 205-206

## C

- catch all rule, diagnostic logging, 172

## chains

- creating, 112
- default policy, 113
- deleting, 113
- order of rules, 121-122
- renaming, 113
- user-defined chains, 241

- chkrootkit, 59

- chroots, 56

- CIA (confidentiality, integrity, and/or availability), 24

- clients, blocking from accessing websites, 279

- closing connections with TCP, 86

- comparing solutions, 68

- compatibility issues, IPSEC, 336

- computer security, 12-14, 24

- configuring software correctly, 60

## INDEX

congestion control, TCP, 84  
 connection tracking, 340  
   engine, memory load diagnostics, 182-185  
   fields, 102  
 connections  
   accepting SMTP connections from specific hosts, 262-263  
   to AIM, 315  
   closing with TCP, 86  
   connections timeout, SSH, 253  
   establishing with TCP, 84  
   forwarding from firewalls to internal web servers, 272-273  
   FTP, troubleshooting, 299-300  
   to ICQ, 317  
   MySQL, allowing, 253-255  
   to other MSN users, 309-310  
   redirecting FTP connections to other ports on the server, 293  
   to remote NetMeeting/GnomeMeeting clients, 304-307  
   telnet, forwarding to other systems, 253  
   to Yahoo Messenger, 311  
 control tools  
   cutter, 160-161  
   network probes, 161-162  
 counter measures, securing the enterprise, 35  
 countertrace, 146  
 cronjobs, 45, 49  
 cutter, 160-161

## D

-D switch (iptables), 112  
 Debian, apt-get, 49  
 default policy, chains, 113  
 defense in depth (DID), 21, 31  
 defragmentation, 101  
 deleting  
   chains, 113  
   rules, 112, 119  
 denying large e-mails, 265  
 deploying security technology and counter measures, 35  
 DHCPClient, 327  
 DHCP  
   blocking outbound, 328-329  
   dynamically updating firewall rules with IP changes, 327-328  
   filtering with ebtables, 214-215  
   redirecting requests to DMZ, 330-332  
   two addresses on one external interfaces, 329-330  
 DHCPd, 327  
 DHCPRelay, 322, 331  
 diagnostics  
   logging, 169-173, 219-220  
   memory load, 182-185  
   network problems, 173-179  
   sniffers, 179-182

DID (defense in depth), 21, 31  
 disabling  
   ICMP echo response, 126-127  
   ICMP redirection, 124-125  
   ip forwarding, 123  
   proxyarp, 125  
   source routing, 124  
 DMZ (DeMilitarized Zones), 217, 228-230  
   cannot be reached from the outside, 236-239  
   segments, forwarding to FTP servers, 293-296  
   web servers, 245, 267  
 DNAT rules, PPTP connections, 347  
 DNS  
   forwarding queries to upstream/remote DNS servers, 322-324  
   lookups fail, 324-326  
   rDNS, misleading, 326-327  
 DNSMasq, 322-324  
 documentation  
   iptables, 109-111  
   risk management, 29-30  
   creating plans, 30-32  
   creating security policies, 33  
   creating security procedures, 34  
   holistic approach, 32-33  
 domains, 36  
 down stream liability, 29  
 drivers, troubleshooting OSI model, 89  
 dropping packets (example firewall), 143-144  
 dsniiff, 202

## E

-E switch (iptables), 113  
 ebtables, 206, 331  
   building inline transparent bridging firewalls, 207-210  
   filtering, 211, 214-215  
 ECN (Explicit Congestion Notification), 128, 278  
 ECN flag, diagnostics, 180-181  
 effective security, 9  
 egress filtering  
   example firewall, 145  
   securing the enterprise, 39  
 email. *See also* SMTP  
   blocking internal users from sending mail through firewalls, 261-262  
   large e-mail, deny, 265  
   small e-mail, send/receive correctly, 265  
   SMTP server timeouts/failures/numerous processes, 264-265  
 emerge, 47-49  
 enabling  
   ip dynaddr, 124  
   ip forwarding, 150  
 enclaves, 36  
 end state, defining, 67  
 enforcement rules (example firewall), 144

- ESTABLISHED (netfilter), 100
- establishing connections with TCP, 84
- eth0, 242
- eth1, 242
- etherape, 157-158
- ethereal, 155, 304, 338
- example firewall, 122-123
  - ACCEPT rules, 149-150
  - bad flag rules, 134-135
  - bad IP options rules, 135
  - egress filtering rules, 145
  - enforcement rules, 144
  - firewall rules, 130
  - fragments rules, 140
  - invalid packets rules, 139
  - IP spoofing rules, 145
  - iptables modules, loading, 129-130
  - kernal options, 123-129
  - odd port detection rules, 142-143
  - polite rules, 142
  - port scan rules, 132-134
  - quality of service rules, 130-132
  - shunning packets rules, 148-149
  - silently dropping packets, 143-144
  - small packets rules, 135-136
  - state tracking rules, 147
  - STEALTH rules, 147-148
  - string-matching rules, 136-139
  - SYN floods rules, 140-142
  - TCP reset for AUTH connections, 146
  - TTL values rules, 146-147
- Explicit Congestion Notification (ECN), 128, 278
- Explicit Congestion Notification (ECN) flag, diagnostics, 180-181
- external IPSEC servers, connections from internal systems, 338-340
- F**
- F switch (iptables), 119
- facts, gathering, 66-67
- failures, SMTP, 264-265
- file services, 283. *See also* FTP; NFS
- file systems, restricting, 56-57
- File Transfer Protocol. *See* FTP
- file transfers, troubleshooting, 240
- filtering
  - access to forwarded servers, 278
  - DHCP with ebtables, 214-215
  - incoming web servers to specific hosts, 270-271
  - MAC addresses, 211-214
  - port 80, 267
  - securing the enterprise, 39
  - specific ports with ebtables, 211
- filtering tools, ebtables, 206
- FIN scan, 198-199
- Firewall Builder (fwbuilder), 165
- firewall rules
  - example firewall, 130
  - protecting services, 51-55
- firewalls, 189. *See also* example firewall; iptables firewalls
  - DMZ, 228-230
  - forwarding connections from firewalls to internal web servers, 272-273
  - IP forwarding firewalls, 284-290
  - local firewall security. *See* local firewall security
  - managing building rules, 163-166
  - masquerading firewalls, 224-226
  - NAT, 284-290
  - packet filtering firewalls, 190
  - reasons for having, 16-17
  - recommendations for, 15-16
  - securing the enterprise, 36
  - SMTP, allowing through firewalls, 258
  - SNAT firewalls, 226-228
  - stealth firewalls, 207-210
  - testing, 190
  - with three interfaces and corresponding devices, 242
  - transparent firewalls, 203-204
  - types of, 17-19
- flow control, TCP, 83
- forcing mail server traffic to use specific IP address with SNAT rule, 260
- FORWARD, 98
- forwarded servers
  - filtering access to, 278
  - restricting FTP access to, 298-299
- forwarding
  - connections from firewalls to internal web servers, 272-273
  - DNS queries to upstream/remote DNS servers, 322-324
  - filtering access to forwarded servers, 278
  - FTP servers
    - behind firewalls on DMZ segments, 293-295
    - from one Internet server to another Internet server, 297-298
  - local port 80 to local port 8080, 271-272
  - to multiple FTP servers behind firewalls on DMZ segments, 295-296
  - to multiple internal servers, 273-275
  - packets from some other host to some other host, 96
  - to remote servers on the Internet, 275-277
  - restricting FTP access to forwarded servers, 298-299
  - SMTP to internal mail servers, 258-260
  - SSH to another system, 248-253
  - telnet connections to other systems, 253
- fragment reassembly, memory load diagnostics, 185
- fragmentation, 101-102
- fragments rules (example firewall), 140
- fragrouter, testing firewalls, 200-201

## INDEX

- FTP (File Transfer Protocol), 283
  - forwarding
    - from one Internet server to another Internet server, 297-298
    - FTP servers behind firewalls on DMZ segments, 293-295
    - to multiple FTP servers behind firewalls on DMZ segments, 295-296
    - restricting FTP access to forwarded servers, 298-299
  - redirecting connections to other ports on the server, 293
  - restricting access with firewall rules, 291-292
  - running local FTP servers (basic rules), 290-291
  - troubleshooting, 299-300
- full duplex, TCP, 83
- fwbuilder (Firewall Builder), 165
- fwsnort, 138
- G**
  - gathering facts, 66-67
  - Gentoo, emerge, 47-49
  - glibc, 45
  - GnomeMeeting, 304-308
  - GNU Gatekeeper, 304
  - grsecurity, 61
- H**
  - h switch (iptables), 109-111
  - hardened kernels, 61
  - hardening, 62
  - highly structured threats, 10
  - holistic approach, documenting risk management, 32-33
  - host intrusion detection, 58-60
  - hostnames versus IP addresses, 321
  - hosts, filtering incoming web servers to specific hosts, 270-271
  - hosts.allow, 52-53
  - hosts.deny, 52
  - hybrids, 18
- I**
  - I switch (iptables), 111-112
  - ICMP (Internet Control Message Protocol), 79-80
    - echo response, disabling, 126-127
    - redirection, disabling, 124-125
  - ICQ, 317-318
  - identd, 264
  - iftop, 158
  - IM (Instant Messaging), 303
    - AIM, 314-317
    - GnomeMeeting, 304-308
    - ICQ, 317-318
    - MSN, 309-310
    - NetMeeting, 304-308
    - questions/problems, 303
    - Yahoo Messenger, 311-314
  - improving risk management, 41
  - inaccessible websites, 278
  - inbound
    - creating rules for new TCP services, 243-246
    - filtering incoming web servers to specific hosts, 270-271
    - running local web servers, 269
    - SSH as a local system, 246-248
  - incoming web servers, filtering to specific hosts, 270-271
  - ingress filtering, securing the enterprise, 39
  - inline transparent bridging firewalls
    - building with iptables, 211-213
    - creating with ebtables, 207-210
  - INPUT, 98
  - INSIDE-OUT test, 190
    - interpreting from output, 194-195
    - testing with nmap and iplog, 190-193
  - installing DNSMasq, 324
  - Instant Messaging. *See* IM
  - Integrated Secure Communications System (ISCS), 163
  - integration, risk management, 41
  - internal mail servers, forwarding SMTP, 258-260
  - internal systems
    - communication with external systems, 236-240
    - connections to external IPSEC servers, 338-340
  - internal users, blocking from sending mail through firewalls, 261-262
  - internal VPN routing, 342-344, 348-351
  - Internet, forwarding to remote servers on, 275-277
  - Internet Control Message Protocol. *See* ICMP
  - Internet protocol. *See* IP
  - interpreting output from INSIDE-OUT tests, 194-195
  - intrusion detection, snort signatures, 138
  - INVALID (netfilter), 100
  - invalid packets rules (example firewall), 139
  - inventory, analyzing risk management, 26-27
  - IP (Internet Protocol), 77. *See also* ICMP; TCP; UDP
    - addresses, 211, 321
    - packets, 78
    - spoofing rules (example firewall), 145
  - ip dynaddr, enabling, 124
  - ip forwarding
    - disabling, 123
    - enabling, 150
    - firewalls, troubleshooting, 284-290
  - iplog, testing, 190-193
  - IPSEC, 335-336
    - common problems, 336-338
    - connections to external IPSEC servers, 338-340
    - internal VPN routing, 342-344
    - NAT/MASQ firewall connections, 340-342
    - securing wireless networks, 351-358
  - \$IPTABLES, 241
  - iptables, 93, 241. *See also* rules
    - building inline transparent bridging firewalls, 211-213
    - filtering MAC addresses, 213-214

- fragmentation, 101-102
- listing current NAT entries, 221-222
- syntax, 109-120
- TRACE patch, 173
- iptables firewalls, connecting to remote
  - NetMeeting/GnomeMeeting clients, 304
- iptables modules, loading (example firewall), 129-130
- iptables policies, order of rules, 121-122
- ip\_conntrack, memory load diagnostics, 183-184
- ip\_conntrack\_max, memory load diagnostics, 184
- ISCS (Integrated Secure Communications System), 163-165
- isolating assets, securing the enterprise, 36-37

## J-K-L

- j switch (iptables), 119-120
- kernel options (example firewall), 123-129
- kernels, 61, 294, 300
- L switch (iptables), 113-119
- Layer 2 transparent firewalls. *See* transparent firewalls
- length of names, DNS lookups, 325
- liability, down stream liability, 29
- libpcap library, 155
- Linux, ECN, 278
- loading iptables modules (example firewall), 129-130
- local firewall security, 43-44
- local systems, SSH, 246-248
- local web servers, running, 269
- log monitoring tools, 57-58
- logcheck, 58
- logging, diagnostic logging, 169-173, 219-220
- logwatch, 58
- lookup failures, DNS, 324-326

## M

- MAC addresses, filtering with iptables, 213-214
- mail server traffic, forcing to use a specific IP address with
  - SNAT rule, 260
- managing firewalls, building rules, 163-166
- martian addresses, detecting, 126
- masquerading firewalls, 224-226
- Maximum Transmission Unit. *See* MTU
- memory load diagnostics, 182-183, 185
- methodologies, 6-8, 64-66. *See also* troubleshooting, methodologies
- misleading rDNS, 326-327
- models. *See* OSI model
- monitoring, implementing, 40
- MSN, 309-310
- MTU (Maximum Transmission Unit), 77
  - path discovery and VPNs, 337
  - settings
    - IPSEC, 336, 340
    - PPTP, 346

- multiplexing, TCP, 83
- MySQL, allowing connections, 253-255
- myths, trustworthy or secure software, 19-20

## N

- N switch (iptables), 112, 115
- name length, DNS lookups, 325
- name servers, running, 325-326
- NAT (Network Address Translation), 217-218
  - common questions about, 218-219
  - connections, viewing with netstat-nat, 220-221
  - current NAT and rule packet counters, listing, 222-224
  - current NAT entries with iptables, listing, 221-222
  - firewalls, troubleshooting, 284-290
  - and IPSEC, 336
  - rules, 340-342, 348-351
- NAT Traversal Mode, 339
- NAT/MASQ firewalls
  - connections between internal systems and external
    - IPSEC servers, 338-340
  - IPSEC VPN connections, 340-342
  - PPTP VPN connections, 347-348
- netfilter, 93, 268
  - firewalls, connecting to remote
    - NetMeeting/GnomeMeeting clients, 305-307
  - fragmentation, 101-102
  - how it works, 93-94
  - iptables. *See* iptables
  - packets
    - forwarding for some other host to some other host (FORWARD), 96
    - sent by firewall from a local process to a remote system (OUTPUT), 96
    - sent to service running on firewall from remote host (INPUT), 94
  - parsing rules, 94-100
  - states, 100-101
  - TCP connections, 121
  - UDP connections, 120
  - website, 110
- NetMeeting, 304-308
- netstat-nat, viewing NAT connections, 220-221
- Network Address Translation. *See* NAT
- network diagnostics, 173-179
- network performance settings (kernel options), 127-129
- network traffic analyzers, 159-160
- NEW, netfilter, 100
- NFS (Network File System), 283-290
- ngrep, 155
- NIDS (Network Intrusion Detection System), 58
- nmap, 162-163
  - network diagnostics, 175-176
  - reading output from, 197-198
  - testing, INSIDE-OUT, 190-193

## INDEX

### O

odd port detection rules (example firewall), 142-143  
 Open System Interconnection. *See* OSI model  
 openswan, 336-338, 351-358  
 order of rules, 121-122  
 OSI (Open System Interconnection) model, 75-76, 89-91  
 outbound  
   blocking clients from accessing websites, 279  
   blocking DHCP, 328-329  
   FTP, troubleshooting, 299-300  
   inaccessibility of websites, 278  
   web traffic, transparent proxy servers, 279-281  
 OUTSIDE-IN tests, 190, 195-198

### P

-P switch (iptables), 113  
 package management tools, 45-49  
 packet filtering, 17  
 packet filtering firewalls, 189-190  
 packet sniffers. *See* sniffers  
 packets  
   forwarding for some other host to some other host (FORWARD), 96  
   invalid packets rules (example firewall), 139  
   IP packets, 78  
   sent by firewall from a local process to a remote system (OUTPUT), 96  
   sent to service running on firewall from remote host (INPUT), 94  
   shunning (example firewall), 148-149  
   silently dropping packets (example firewall), 143-144  
   small packets rules (example firewall), 135-136  
   string-matching rules (example firewall), 136-139  
   TCP, 82  
   troubleshooting packets that do not pass in or out of a firewall, 230-235  
 parsing rules, netfilter, 94-100  
 patch maintenance, 45  
 patching  
   iptables, TRACE patch, 173  
   reliance on, 50  
 physical connectivity, troubleshooting OSI model, 89  
 ping, 152-154, 174-175  
 PKI (Public Key Infrastructure), 163  
 plans, documenting risk management, 30-32  
 Point to Point Tunneling Protocol. *See* PPTP  
 policies, implementing, 35  
 polite rules (example firewall), 142  
 port 80, filtering out, 267  
 port scan rules (example firewall), 132-134  
 PORT STATE SERVICE, 199-200  
 POSTROUTING chains, 222  
 PPTP (Point to Point Tunneling Protocol), 345  
   connections through firewall, 345-347  
   internal VPN routing, 348-351  
   NAT/MASQ firewall connections, 347-348

pttpclient, 346  
 PREROUTING, 98, 101  
 presentation layers, troubleshooting OSI model, 91  
 preventing networks from being added to routes, 243  
 privilege, running services with least privilege, 55-56  
 probing tools, 162-163  
 problem solving methodology, 64-65  
 /proc, 102  
 procedures, implementing, 35  
 processes, SMTP, 264-265  
 protecting services with TCP wrappers and firewall rules, 51-55  
 protocols. *See* ICMP; IP; TCP; UDP  
 proxyarp, disabling, 125  
 proxys, 304, 307-308  
 Public Key Infrastructure (PKI), 163

### Q-R

quality of service rules (example firewall), 130-132  
 quantifying value of assets, analyzing risk management, 28  
 -R switch  
   iptables, 112  
   ping, 174  
 Rash, Michael, 138  
 rDNS, misleading, 326-327  
 reading output from nmap, 197-198  
 ReAIM, 304  
 recognizing, defining, and isolating the problem, 65-66  
 red carpet, 46-47  
 redirecting  
   DHCP requests to DMZ, 330-332  
   disabling ICMP redirection, 124-125  
   FTP connections to other ports on the server, 293  
   local port 80 to local port 8080, 271-272  
 RELATED, netfilter, 100  
 reliability, TCP, 83  
 reliance on patching, 50  
 remote DNS servers, forwarding DNS queries to, 322-324  
 remote logging, 60  
 remote servers, forwarding to remote servers on the Internet, 275-277  
 renaming chains, 113  
 replacing rules, 112  
 restricting  
   access with firewall rules (FTP), 291-292  
   file systems, 56-57  
   FTP access to forwarded servers, 298-299  
 risk, 8  
 risk management, 9-12, 23-24  
   computer security, 12-14, 24  
   elements of, 24-25  
   steps for, 25  
   analyze, 26-29  
   documentation, 29-34  
   implementing monitoring, 40

- improving, 41
- integration, 41
- securing the enterprise, 34-39
- testing, 40
- rkhunter, 59
- routers, 189
- routing, internal VPN routing, 342-344, 348-351
- Rowland, Craig, 58
- RPC Bind, 197
- rsync, 50
- rule packet counters, listing, 222-224
- rules. *See also* example firewall; iptables
  - adding, 112
  - building, 163-166
  - catch all, diagnostic logging, 172
  - creating for new TCP services, 243-246
  - deleting, 112, 119
  - internal VPN routing, 344, 349-351
  - IPSEC connections, 340-342
  - order of, 121-122
  - parsing with netfilter, 94-100
  - PPTP connections, 346-347
  - PPTP VPN connections, 348
  - replacing, 112
  - wireless network security, 355-357
- running
  - local FTP servers (basic rules), 290-291
  - local web servers, 269
  - services with least privilege, 55-56
- S**
- s switch (ping), 175
- samhain, 59
- scripts, diagnostic logging, 170-172
- search engines, troubleshooting methodologies, 69
- Secondary Exploitation, 37
- Secure Shell. *See* SSH
- securing
  - enterprise, risk management, 34-39
  - wireless networks with openswan VPN, 351-358
- security, 8-9, 17
  - computer security, 12-14
  - effective security, 9
- security policies, 21, 33
- security procedures, 34
- security technology, securing the enterprise, 35
- security tools, 57-60
- selecting solutions, 68
- SELinux, 45, 61
- server timeouts, SMTP, 264-265
- servers
  - DNS servers. *See* DNS
  - forwarded servers, filtering access to, 278
  - FTP servers, running local FTP servers (basic rules), 290-291
  - remote servers. *See* remote servers
  - transparent proxy servers, squid, 279-281
- services
  - protecting with TCP wrappers and firewall rules, 51-55
  - running with least privilege, 55-56
  - turning off, 50
- session layers, troubleshooting OSI model, 91
- shunning packets rules (example firewall), 148-149
- silently dropping packets (example firewall), 143-144
- slabinfo, memory load diagnostics, 182-183
- Small Office/Home Office (SOHO), 217
- small packets rules (example firewall), 135-136
- SMTP, 257
  - accepting SMTP connections from specific hosts, 262-263
  - allowing through firewalls, 258
  - forwarding to internal mail servers, 258-260
  - large email, deny, 265
  - questions about, 257
  - server timeouts/failures/numerous processes, 264-265
  - small e-mail send/receive correctly, 265
- smurf attacks, detecting, 126-127
- SNAT firewalls, 226-228
- SNAT rule, forcing mail server traffic to use specific IP address, 260
- sniffers, 155-156, 179-182, 304, 338
- Snort, 258, 313
- snort signatures, 138
- software
  - configuring correctly, 60
  - importance of updating, 44-45
  - myths of trustworthy or secure software, 19-20
- SOHO (Small Office/Home Office), 217
- solutions
  - analyzing and comparing, 68
  - developing, 67
  - selecting and implementing, 68
- source routing, disabling, 124
- sP switches (nmap), 175
- spoof protection, 125
- spoofing rules (example firewall), 145
- squid, 268-269, 279-281
- SSH (Secure Shell), 246
  - connections timeout, 253
  - forwarding to another system, 248-253
  - as local system, 246-248
- ssh service, protecting, 54
- SSLDump, 156
- state engine, 102-106
- state tracking rules (example firewall), 147
- stateful inspection, 18
- states of netfilter, 100-101
- stealth firewalls, 207-210
- STEALTH rules (example firewall), 147-148
- steps for risk management. *See* risk management, steps for
- Stevens, W. Richard, 76
- string-matching rules (example firewall), 136-139

## INDEX

structured threats, 10

SYN cookies, 128

SYN flood attacks

example firewall, 140-142

preventing, 128

SYN scan, 198

syntax, iptables, 109-120

## T

TCP (Transmission Control Protocol), 82-83

closing connections, 86

congestion control, 84

creating rules for new TCP services, 243-246

establishing connections, 84

flow control, 83

full duplex and multiplexing, 83

reliability, 83

TCP ABORT, 87-88

TCP CLOSE, 86

TCP connections, netfilter engine, 121

TCP FIN timeout network setting, 127

TCP layers, troubleshooting OSI model, 90

TCP packets, 82

tcp ping, 176

TCP reset for AUTH connections (example firewall), 146

TCP wrappers, protecting services, 51-55

tcp-window-tracking modification, 106

tcpdump, 155-156, 179

tcptraceroute, 161-162, 178-179

telnet, 151, 253, 267

testing

application layers, OSI model, 91

drivers, OSI model, 89

firewalls, 190-201

presentation layers, OSI model, 91

risk management, 40

session layers, OSI model, 91

TCP layers, OSI model, 90

tetheral, diagnostics, 179-180

threat analysis, analyzing risk management, 29

threats, 10

Three-Way Handshake (TWH), 85

TIGER, 59

TIME WAIT state, 104

timeouts, UDP connection timeout setting, 128

TITAN, 59

tools

cutter, 160-161

dsniff, 202

ebtables, 206

etherape, 157

iftop, 158

network traffic analyzers, 159-160

nmap, 162-163

package management tools, 45-49

ping, 152-154

probing tools, 162-163

security tools, 57-60

sniffers, 155-156, 338

tcpdump, 158

tcptraceroute, 161-162

telnet, 151

top, 158

vnstat, 159

top, 158

TRACE patch (iptables), 173

traceroute, 146-147, 154, 161-162, 176-179

traffic, analyzing utilization, 157-158

training, 21

Transmission Control Protocol. *See* TCP

transparent firewalls, 203-204

transparent proxy servers, 279-281

tripwire, 59

troubleshooting. *See also* diagnostics

internal and external systems communication, 230-240

large file transfer failures, 240

methodologies, 63-64, 69

analyzing and comparing solutions, 68

defining end state, 67

developing solutions and creating action plans, 67

gathering facts, 66-67

implementing solutions, 68

problem solving methodology, 64-65

recognizing, defining, and isolating the problem, 65-66

websites for, 69-70

with search engines, 69

OSI model, 89-91

TTL values rules (example firewall), 146-147

tunneling. *See* VPNs

turning off services, 50

TWH (Three-Way Handshake), 85

## U

UDP (User Datagram Protocol), 88

UDP connections, 120, 128

unstructured threats, 10

up2date, 47

updating

firewall rules with IP changes, 327-328

software, importance of, 44-45

upstream DNS servers, forwarding DNS queries to, 322-324

User Datagram Protocol. *See* UDP

user-defined chains, 241

## V

-v switch (iptables), 116

viewing NAT connections with netstat-nat, 220-221

VLANs, 201-202

vnstat, 159

VPNs (virtual private networks), 335



---

**INDEX**

---

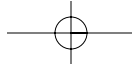
- common problems, 336-338
- IPSEC, 335-344
- NAT/MASQ firewall connections, 340-342, 351-358
- PPTP, 345-351
- sniffers, 338
- vulnerabilities, 20
- vv switch (iptables), 117

**W**

- web servers
  - DMZ, 267
  - filtering incoming web servers to specific hosts, 270-271
  - forwarding connections from firewalls to internal web servers, 272-273
  - forwarding to multiple internal servers, 273-275
  - local web servers, running, 269
  - redirecting local port 80 to local port 8080, 271-272
- web services, squid. *See* squid
- websites
  - blocking clients from accessing, 279
  - inaccessibility of, 278
  - for troubleshooting methodologies, 69-70
- wireless networks, securing with openswan VPN, 351-358
- wrenchin', 7
- Wright, Gary R., 76

**X-Z**

- X switch (iptables), 113
- xinetd, 51
- Yahoo Messenger, 311-314
- yum, 45-46
- Z switch (iptables), 113
- Zeroconf route, 243



# informIT

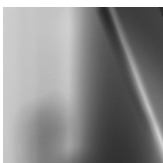
[www.informit.com](http://www.informit.com)

## YOUR GUIDE TO IT REFERENCE



### Articles

Keep your edge with thousands of free articles, in-depth features, interviews, and IT reference recommendations – all written by experts you know and trust.



### Online Books

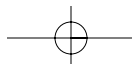
Answers in an instant from **InformIT Online Book's** 600+ fully searchable on line books. For a limited time, you can get your first 14 days **free**.

POWERED BY  
**Safari**  
TECH BOOKS ONLINE™



### Catalog

Review online sample chapters, author biographies and customer rankings and choose exactly the right book from a selection of over 5,000 titles.



# Wouldn't it be great

if the world's leading technical publishers joined forces to deliver their best tech books in a common digital reference platform?

They have. Introducing  
**InformIT Online Books**  
powered by Safari.

## ■ Specific answers to specific questions.

InformIT Online Books' powerful search engine gives you relevance-ranked results in a matter of seconds.

## ■ Immediate results.

With InformIT Online Books, you can select the book you want and view the chapter or section you need immediately.

## ■ Cut, paste and annotate.

Paste code to save time and eliminate typographical errors. Make notes on the material you find useful and choose whether or not to share them with your work group.

## ■ Customized for your enterprise.

Customize a library for you, your department or your entire organization. You only pay for what you need.

## Get your first 14 days FREE!

For a limited time, InformIT Online Books is offering its members a 10 book subscription risk-free for 14 days. Visit <http://www.informit.com/online-books> for details.

POWERED BY  
**Safari**  
TECH BOOKS ONLINE

**informIT**  
**Online Books**

**informit.com/onlinebooks**



# Register Your Book

at [www.awprofessional.com/register](http://www.awprofessional.com/register)

You may be eligible to receive:

- Advance notice of forthcoming editions of the book
- Related book recommendations
- Chapter excerpts and supplements of forthcoming titles
- Information about special contests and promotions throughout the year
- Notices and reminders about author appearances, tradeshows, and online chats with special guests



## Contact us

If you are interested in writing a book or reviewing manuscripts prior to publication, please write to us at:

Editorial Department  
Addison-Wesley Professional  
75 Arlington Street, Suite 300  
Boston, MA 02116 USA  
Email: [AWPro@aw.com](mailto:AWPro@aw.com)

Visit us on the Web: <http://www.awprofessional.com>

