
- single-firewall, 211
 - Internet firewall with multiple DMZs, 211–212*
 - Internet firewall with single DMZ, 211*
 - Internet-screening firewall, 212 layers, 215–216*

ARO (annual rate of occurrence), 22

ARP (Address Resolution Protocol), 75

ASA (Cisco Adaptive Security Algorithm), 133

- anti-X, 127
- configuring, 137

ASA 5510, 129

ASA 5510 Security Plus, 129

ASA 5520, 129

ASA 5540, 129

ASDM/PDM remote access, configuring on PIX/ASA firewall, 143

assigning

- ACLs to interfaces, 151
- IP addresses to firewall interfaces, 138–140

attacks

- motives for, 19–20
- targeted, 13
- untargeted, 13

auditing policies, 237

authentication, 9–10

- certificates, 9
- xauth, 9

autonomous systems, 80

B

Basic Setup screen (BEFSR41v4 Setup tab), 116

best-effort delivery, 52

BGP (Border Gateway Protocol), 80

bidirectional NAT, 73

binary notation, 67

bridging firewalls. *See* transparent firewalls

broadband routers

- Linksys BEFSR41v4, 109
 - configuring, 115–121*
 - management and administration features, 110*
 - miscellaneous features, 111*
 - routing features, 110*
 - VPN passthrough, 110*

- NAT-based, 108

broadcast traffic, 74

building NetFilter-based firewalls, checklist, 174–175

built-in chains. *See* chains

C

caching, enabling on ISA server, 205

central office implementation, 209–210

certificates, authentication, 9

chains (Netfilter), 163

- user-defined, 166
- within filter table, 163
- within mangle table, 166
- within NAT table, 165

change control, 267

- as part of troubleshooting methodology, 306

change control system

- setting up, 267, 270–271
- logging, 271–272

checklist

- for building Netfilter-based firewalls, 174–175
- for Linksys router configuration, 123
- for Trend Micro's PC-cillin firewall feature configuration, 103–104
- for Windows Firewall configuration, 94–95
- of troubleshooting procedures, developing, 301–310

choosing between ASA and PIX, 127**CIDR (classless interdomain routing), 69****circuit-level firewalls, 37****Cisco PIX Firewall. *See* PIX Firewall****classes of IP addresses, 68–69****classifications of routing protocols, 79****CLI (command-line interface), firewall management, 255–256****closed source firewalls, 40****closed-source vendor software, availability of patches, 254****combining VLANs and firewalls on a network, 219****commands**

- enable, 137
- fixup, 38, 134
- interface, 138
- logging, 153
- logging permit-hostdown, 250

comparing

- deep packet inspection and application layer filtering, 178
- HTTP and HTTPS, 262
- known good and current configuration, 308

configuration files

- controlling access to, 267
- RCS log, viewing, 271–272

configuring

- ACLs, 147–151
 - parameters, 148–150*
- ASA, 137
- default gateway, 263–264
- interfaces, 262
- Linksys routers, 115
 - administration, 121*
 - basic setup procedures, 116*
 - checklist, 123*
 - gaming application support, 119–121*
 - security, 117*

NAT

- on PIX 6.x, 145–146*
- on PIX 7.x, 146–147*

Netfilter, 166–168

- with Firestarter, 170–171*
- with Firewall Builder, 169*
- with iptables, 168*
- with Webmin, 171*

PIX/ASA firewall, 137

- remote management access, 141–143*
- URL filtering, 324–325*

syslog, 264–266**Trend Micro's PC-cillin firewall feature, 97–98, 101–102**

- checklist, 103–104*
- profiles, 98*
- security level, 101*

Windows Firewall, 89–93

- checklist, 94–95*

connection teardowns (TCP), reasons for, 288–289**connectionless protocols**

- sessions, 7
- UDP, 61
 - header fields, 62*
 - messages, 62*

connection-oriented protocols,**TCP, 7, 57**

- port numbers, 58
- segments, 58
- sliding windows, 58
- SYN flood, 60

connectivity

- requirements for Linksys routers, 112
- testing, 303–305
- through firewall, troubleshooting, 310, 313–315
- to firewall, troubleshooting, 316

console notification, 11**controlling**

- access to configuration files, 267
- management interface access, 260
 - in-band management, 260*
 - out-of-band management, 260*
- SSH, 261
- Telnet, 261

corner cases, 273**corrupt IP packets, 56–57****creating**

- access rules, 195
- effective security policies, 20
- NetFilter-based firewalls, checklist, 174–175
- publishing rules, 198
- security policies, 230

CS-MARS (Cisco Security Monitoring, Analysis and Response System), 282

D

- data link layer, 48**
- DDNS screen (BEFSR41v4 Setup tab), 117**
- DDoS (distributed DoS) attacks, 15**
- deep packet inspection, 127, 178**
- default firewall passwords, 253–254**
- default gateway, configuring, 263–264**
- deficiencies in syslog security, 282–283**
- defining**
 - DMZ policy standards, 235–236
 - rulesets for firewall security policy, 241
 - egress filtering, 245, 247*
 - ingress filtering, 240–245*
 - management access, 247–250*
- de-perimeterization of the network, 217**
- desktop firewalls, 27, 217**
 - implementing, 217–218
- developing checklist of troubleshooting procedures, 301–310**
- DHCP (Dynamic Host Configuration Protocol), 75**
- displaying RCS log, 271–272**
- distance vector routing protocols, 79**
- “DMZ-on-a-stick” architecture, 211**
- DMZ**
 - on Linksys routers, 110
 - policies, 235
- DMZ forwarding, 114**
- DNAT target, 168**
- DNS (domain naming system), 75**
- DoD Model, 51**
- DoS (denial of service) attacks, 15–16, 63**
- dotted-decimal notation, 68**
- DROP target, 168**
- dropped traffic, identifying in firewall logs, 287**
- dual-firewall architectures, 213–214**
 - layers of, 216–217
- dynamic NAT, 73**
- dynamic routing, 77**

E

- ego as motivation for attacks, 19**
- egress filters**
 - firewall security policy ruleset, defining, 245–247

- for DMZs, applying, 247
 - for internal traffic, applying, 246
- email, SMTP anti-spam software, 330**
- e-mail notification, 12**
- enable command, 137**
- enable password, 140**
- encapsulation process, 49–50**
- encryption policies, 237**
- end-user services, 44**
- ensuring legal admissibility of firewall logs, 285**
- enterprise office solutions, ASA and PIX models designed for, 129**
- ESP (Encapsulated Security Payload), 334**
- estimating**
 - ALE, 22–24
 - SLE, 22–24
- events**
 - recording and reporting with firewalls, 11
 - syslog, 290–295
- evolution of Linux firewall capabilities, 161**
- example of troubleshooting firewall configuration, 316, 319–320**
- examples of security policies, 20**
- exceptions for Windows Firewall, 88**
- extended ACLs, parameters, 148–150**
- exterior gateway routing protocols, 80**

F

- failed authentication, identifying in firewall logs, 289**
- failover, active/active, 224–225**
- features**
 - of Microsoft ISA Server 2004, 182–184
 - of Trend Micro firewall, 103
 - of Windows Firewall, 94
- fields**
 - of IP packet header, 54, 56
 - of TCP segment header, 59–60
 - of UDP header, 62
- Filter screen (BEFSR41v4 Security tab), 118**
- filter table (Netfilter), 163**
- filtering decision process on PIX Firewall, 130–132**
- filtering policies, 233**
- filtering systems, maintaining, 254**

Firestarter, configuring Netfilter, 170–171**Firewall Builder, configuring Netfilter, 169****firewall client, 185**

- configuring on ISA server, 204

firewall dynamic configuration layer, 230, 238–239**firewall logs**

- forensics analysis

- performing, 295–296*

- port numbers, accessing from*

- IANA, 298

- spoofed IP addresses, identifying, 296–298*

- importance of, 284–285

- legal admissibility of, ensuring, 285

- reviewing, 286, 307

- spoofed IP addresses, identifying, 296–298

- suspicious events, identifying, 287–290

firewall management

- change control system

- configuring, 267, 270–271*

- logging, 271–272*

- configuration files, controlling

- access to, 267

- default gateway, configuring, 263–264

- default passwords, 253–254

- interfaces, configuring, 262

- operating system maintenance, 254–255

- physical failure, checking for, 306

- software

- defects, tracking, 274–275*

- updating, 273–275*

- vulnerabilities, 274*

- syslog, configuring, 264–266

- with CLI, 255–256

- with GUI, 256

firewall physical integrity layer, 238**firewall security layer, 230****firewall security policies. *See* security policies,****firewall static configuration layer, 230, 238****firewalls**

- functions performed by, 6

- access authentication, 9–10*

- connection monitoring, 7–8*

- event reporting and recording, 11*

- packet inspection, 6*

- proxy, 10*

- resource protection, 10–11*

- stateful packet inspection, 8*

- host-based, 5

- trust, 21–22

fixup command, 38, 134**forensic analysis**

- incorporating findings in security

- policies, 298

- performing, 295–296

- port numbers, accessing from IANA, 298

- spoofed IP addresses, identifying, 296–298

FORWARD chain (filter table), 164**fragrouter utility, 57****freeware, syslog server products, 281****FTP, 82**

- remote firewall management, 250

functionality

- of firewalls, 6

- access authentication, 9–10*

- connection monitoring, 7–8*

- event recording and reporting, 11*

- packet inspection, 6*

- proxy, 10*

- resource protection, 10–11*

- stateful packet inspection, 8*

- of Microsoft ISA Server 2004, 192

- application filtering, 200*

- caching web data, 205*

- client access method configuration, 203–205*

- outbound access filtering, 195–198*

- publishing internal resources, 198–199*

- system policy rule configuration, 201–202*

- of proxy servers, 179–180

G

gaming application support, configuring on

- Linksys BEFSR41v4, 119, 121

guidelines, 231

H

HA (high availability), active/active failover, 224–225**header fields**

- of IP packets, 53–56

- of TCP packets, 59–60

- of UDP packets, 62

hexadecimal notation, 68
 HIPAA (Health Insurance Portability and Accountability Act of 1996), 16
 host ID, 67
 host-based firewalls, 5
 host-to-host layer (DoD model), 51
 HTTP
 remote firewall management, 250
 versus HTTPS, 262
 HTTPS, remote firewall management, 250
 hybrid routing protocols, 79

I

IANA (Internet Assigned Numbers Authority), 61
 port numbers, accessing, 298
 ICMP (Internet Control Message Protocol), 63
 connectionless sessions, 7
 messages, 64–66
 identifying
 spoofed IP addresses in firewall logs, 296–298
 suspicious events in firewall logs, 287–290
 IDS (intrusion detection systems), 96, 331
 implementing
 effective security policies, 20
 internal firewalls, 223–224
 personal/desktop firewalls, 217–218
 in-band management, 260
 incorporating forensic analysis findings into security policies, 298
 ingress filtering
 applying
 from DMZ segment to internal segment, 244
 from Internet to DMZ segment, 242–244
 from Internet to internal segment, 245
 firewall security policy ruleset, defining, 240–245
 INPUT chain (filter table), 163
 inside interfaces, configuring, 263
 integrated firewalls, 32
 interface command, 138
 interfaces, configuring, 262

internal firewalls, implementing, 223–224
 internal networks, segmenting/protecting, 222
 internal resources, protecting, 222–223
 Internet firewall architectures
 with multiple DMZs, 211–212
 with single DMZ, 211
 Internet layer (DoD model), 51
 Internet-screening firewalls, 212
 investigating suspicious activity, 287–290
 IP (Internet Protocol), 52–53
 less common applications, 81
 most common applications, 81
 packets, 53
 corrupt, 56–57
 header, 53–56
 routing process, 77–78
 IP addresses
 address classes, 68–69
 address display formats, 67–68
 assigning to firewall interfaces, 138–140
 CIDR, 69
 logical addresses, 67
 NAT, 71–73
 dynamic NAT, 73
 static NAT, 73
 physical addresses, 66–67
 subnets, 70
 IP services
 ARP, 75
 DHCP, 75
 DNS, 75
 NTP, 76
 ipchains filter, 161
 ipfw code, 161
 ipfwadm utility, 161
 IPS (intrusion prevention system)
 deep packet inspection, 127
 firewall as, 332
 IPsec, 83
 AH, 333
 ESP, 334
 transport mode, 335
 tunnel mode, 336
 iptables command utility, configuring
 Netfilter, 166
 targets, 168
 IPv6, 71

K–L

- Kiwi Syslog Daemon, 281**
- known good configuration, comparing to current configuration, 308**
- layers of firewall security policies, 237–239**
- legal admissibility of firewall logs, ensuring, 285**
- limitations of application proxy firewalls, 180**
- link-state routing protocols, 79–80**
- Linksys routers/firewalls, 109**
 - administration, configuring, 121
 - basic setup procedures, 116
 - BEFSR41v4, 109
 - management and administration features, 110*
 - miscellaneous features, 111*
 - routing features, 110*
 - configuring, 115
 - connectivity, requirements, 112
 - gaming application support, configuring, 119–121
 - Log Viewer, 111
 - security model, 111
 - security, configuring, 117
 - SPI support, 109
 - traffic filtering, 112
 - DMZ forwarding, 114*
 - from internal sources, 114*
 - port triggering, 113*
 - port-range forwarding, 112*
 - UPnP, 111
 - VPN passthrough, 110
- Linux-based firewalls, 161**
 - ipfw code, 161
 - Linux kernel 2.2, ipchains filter, 161
 - Netfilter, 162
 - chains, 163*
 - configuring, 166–171*
 - filter table, 163*
 - mangle table, 166*
 - NAT table, 164*
 - requirements for operation, 162*
 - tables, 163*
 - website, 162*
- Liu, Cricket, 76**
- load balancing, 165**
- log files. *See* firewall logs**

- Log screen (BEFSR41v4 Administration tab), 122**
- LOG target, 168**
- Log Viewer (Linksys), 111**
- logging**
 - monitoring/logging policies, 235
 - syslog
 - configuring, 264–266*
 - events, 290–295*
- logging command, 153**
- logging facilities (syslog), 278–279**
- logging methods, proprietary, 283**
- logging permit-hostdown command, 250**
- logical addresses, 67**
- login passwords, 140**

M

- MAC address, 66**
- MAC Address Clone screen (BEFSR41v4 Setup tab), 117**
- malicious content, 14**
- malware, 15**
- management access, defining firewall security policy ruleset, 247–250**
- management console (Microsoft ISA Server 2004), 187, 192**
- management interface**
 - accessing, 260
 - via SSH, 261*
 - via Telnet, 261*
 - in-band management, 260
 - out-of-band management, 260
- Management screen (BEFSR41v4 Administration tab), 121**
- management-access policies, 233**
- managing firewalls. *See* firewall management**
- mangle table (Netfilter), 166**
- manipulation utility. *See* Netfilter**
- MASQUERADE target, 168**
- masquerading, 165**
- medium-to-large office solutions, ASA and PIX models designed for, 128**
- message facility (syslog), 264**
- messages**
 - ICMP, 64, 66
 - syslog, 278–279
 - UDP, 62

Microsoft ISA Server 2004, 180
 access rule management, 187–188
 features, 182–183
 filtering functions, 183–184
 firewall client, 185
 functionality of, 192
 application filtering, 200
 caching web data, 205
 client access method configuration, 203–205
 outbound access filtering, 195–198
 publishing internal resources, 198–199
 system policy rule configuration, 201–202
 management console, 187, 192
 misconceptions about, 181–182
 monitoring and reporting, 188
 publishing rules, 186
 remote administration, 193
 SecureNAT client, 184
 securing, 181
 service requirements, 191–192
 supported networks, 189
 system requirements, 189
 VPN functionality, 186
 VPN Quarantine Control, 189
 web caching server functionality, 185
 web proxy client, 185
misconceptions about Microsoft ISA Server 2004, 181–182
monitoring network traffic, 309
monitoring/logging policies, 235
motives for attacks, 19–20
multicast traffic, 74

N

NAT (Network Address Translation), 71–73
 configuring on PIX 6.x, 145–146
 configuring on PIX/ASA 7.x, 146–147
 dynamic NAT, 73
 firewalls, 35–36
 static NAT, 73
NAT-based routers, 108
NAT-T (NAT Traversal), 73, 336
Netfilter, 162
 chains, 163
 configuring, 166–168
 with Firestarter, 170–171

with Firewall Builder, 169
 with iptables, 168
 with Webmin, 171
 NAT table, 164
 requirements for operation, 162
 tables, 163
 filter table, 163
 mangle table, 166
 NAT table, 164
 website, 162
NetIQ Security Manager, 281
network access layer (DoD model), 51
network communication models
 DoD model, 51
 OSI model, 45
 application layer, 46
 data link layer, 48
 encapsulation process, 49–50
 network layer, 47–48
 physical layer, 48
 presentation layer, 46–47
 session layer, 47
 transport layer, 47
network firewalls, 29
network ID, 67
network layer, 47–48
network traffic, monitoring, 309
Network Translations, 125
Network Virus Emergency Center (Trend Micro firewall), 102
NIX syslogd, 281
non-firewall specific systems, troubleshooting, 309
normalization policies, deriving from firewall log analysis, 286
NTP (Network Time Protocol), 76

O

open source firewalls, 40
operating systems
 filtering systems, 254
 maintaining, 254–255
OPSEC LEA (Open Platform for Security - Logging Export API), 283
OSI model, 45
 application layer, 46
 data link layer, 48
 encapsulation process, 49–50

- network layer, 47–48
- physical layer, 48
- presentation layer, 46–47
- session layer, 47
- transport layer, 47

OSPF (Open Shortest Path First), 80

OUI (organizationally unique identifier), 66

outbound access filtering on ISA Server, 195, 198

out-of-band management, 260

OUTPUT chain

- filter table, 164
- NAT table, 165

outside interfaces, configuring, 263

P

packet filters, 34–35

packet inspection, 6

- versus stateful packet inspection, 8

packet-filtering, NAT-based, 108

packets, IP, 53

- corrupt, 56–57
- header, 53–56

paging notification, 12

parameters for extended ACLs, 148–150

password policies, 237

PAT (Port Address Translation), 73

patches, availability of for closed-source vendor software, 254

PDM (PIX Device Manager), 143

personal firewalls, 27–28, 33, 217

- implementing, 217–218

- Trend Micro's PC-cillin firewall feature, 96

- checklist, 103–104*

- configuring, 97–102*

- system requirements, 96*

- Windows Firewall, 87

- checklist, 94–95*

- configuring, 89–93*

- exceptions, 88*

- features, 94*

physical addresses, 66–67

physical firewall failure, checking for, 306

physical integrity layer, 230

physical layer, 48

ping, 63

- connectivity, testing, 303–305

PIX/ASA firewalls

- configuring, 137

- filtering decision process, 130–132

- PIX 501, 128

- PIX 506E, 128

- PIX 515E, 128

- PIX 525, 129

- PIX 535, 129

- remote management access, configuring, 141–143

- URL filtering, 324–325

- version 6.x

- IP addresses, assigning, 138–140*

- NAT, configuring, 145–146*

- version 7.x software, 127

- IP addresses, assigning, 139–140*

- NAT, configuring, 146–147*

- transparent mode, 133*

policies, 231. See also security policies

port forwarding, 165

port numbers, 58

- accessing from IANA, 298

- UDP, 61

Port Range Forwarding screen (BEFSR41v4

Applications and Gaming tab), 119

port triggering, 113

Port Triggering screen (BEFSR41v4

Applications and Gaming tab), 120

port-range forwarding, 112

POSTROUTING chain (NAT table), 165

predicting ALE and SLE, 22–24

PREROUTING chain (NAT table), 165

presentation layer, 46–47

procedures, 231

profiles, configuring on Trend Micro

firewall, 98

proprietary firewall management

methods, 250

proprietary logging, 283

protecting internal resources, 222–223

protocols supported for application inspection, 135–136

proxies for applications, 18

proxy firewalls, 37

proxy servers, functionality, 179–180

PSKs (preshared keys), 9

publishing rules, 186

- creating, 198

Q–R

QoS screen (BEFSR41v4 Applications and Gaming tab), 121

QUEUE target, 168

RCS (revision control system)

log file, viewing, 271–272

repository, modifying, 270–271

recent changes, reviewing as part of troubleshooting methodology, 306

reconnaissance attacks, 296

redundancy, active/active failover, 224–225

REJECT target, 168

release notes, reading, 274

remote administration of Microsoft ISA Server 2004, 193

remote management access, configuring on PIX/ASA firewall, 141–143

remote office implementation, 210

remote-access/VPN policies, 234

requirements for Linksys router connectivity, 112

restricting access to configuration files, 267

RETURN target, 168

reviewing firewall logs, 286, 307
suspicious events, 287–290

revision control systems, 267

RIP (Routing Information Protocol), 79

risk-assessment policies, 237

routed mode, 133

routing policies, 234

routing protocols

BGP, 80

classifications of, 79

OSPF, 80

RIP, 79

routing tables, contents of, 76

rulesets

defining for firewall security, 241

egress filters, 245–247

ingress filters, 240–245

management access, 247–250

verifying, 308

S

SecureNAT client, 184

security contexts, 221

security layers

firewall static configuration layer, 230

physical integrity layer, 230

security level of Trend Micro firewall, configuring, 101

security policies, 20, 229, 237

creating, 230

DMZ policies, 235

egress filtering rulesets, defining, 245–247

examples of, 20

filtering policies, 233

firewall security layers, 230–231

format, 232

incorporating forensic analysis findings, 298

ingress filtering rulesets, defining, 240–245

layers, 237–239

management-access policies, 233

rulesets, defining, 247–250

monitoring/logging policies, 235

remote-access/VPN policies, 234

routing policies, 234

rulesets, defining, 241

Security tab (Linksys BEFSR41v4 router), 117

segmenting internal networks, 222

segments (TCP), 58

header fields, 59–60

selecting

between ASA and PIX, 127

software version, 273

service provider solutions, ASA and PIX models designed for, 129

service requirements for Microsoft ISA Server 2004, 191–192

session layer, 47

Setup tab (Linksys BEFSR41v4 router), 116

severity levels (syslog messages), 264–266, 279

Shorewall firewall, 41 172

single-firewall architectures, 211

Internet firewall with multiple DMZs, 211–212

Internet firewall with single DMZ, 211

Internet-screening firewall, 212

layers, 215–216

SLE (single loss expectancy), predicting, 22–24

sliding windows, 58

SMTP (Simple Mail Transport Protocol), anti-spam software, 330

- SNAT (source NAT), masquerading, 165
- SNAT target, 168
- SNMP (Simple Network Management Protocol), remote firewall management, 249
- SNMP notification, 11
- social engineering, 17
- software
 - defects, tracking, 274–275
 - PIX version 7.x, 127
 - updating, 273–275
 - vulnerabilities, 274
- software firewalls, 30–31
- SOHO solutions, PIX models designed for, 128
- spam, anti-spam software, 330
- SPI (stateful packet inspection), support on Linksys routers, 109
- spoofed IP addresses, identifying in firewall logs, 296–298
- SSH (Secure Shell) remote access, 82
 - accessing management interface, 261
 - configuring on PIX/ASA firewall, 142–143
- SSL VPNs, 336
- standards, 231
 - for DMZ policies, defining, 235–236
- stateful firewalls, 38–39, 97
- stateful inspection, 8, 133
- stateful packet inspection versus packet inspection, 8
- static NAT, 73
- static routing, 77
- subnets, 70
- suspicious events, identifying in firewall logs, 286–290
- SYN (synchronize) segment, 57
- SYN floods, 15, 60
- syslog, 82, 278
 - client configuration, 280
 - configuring, 264–266
 - events, 290–291, 293–295
 - messages, 278–279
 - logging facilities, 278–279
 - remote firewall management, 249–250
 - security deficiencies, 282–283
 - server configuration, 281
 - TCP-based, 250
- system policy rules, configuring on ISA server, 201
- system requirements for Trend Micro's PC-cillin firewall feature, 96

T

- tables (Netfilter)
 - filter table, 163
 - mangle table, 166
 - NAT table, 164
- targeted attacks, 13
- targets (iptables), 168
- TCP (Transmission Control Protocol), 57
 - connection teardowns, reasons for, 288–289
 - connections, 7
 - port numbers, 58
 - segments, 58
 - header fields, 59–60
 - sliding windows, 58
 - SYN floods, 60
- TCP-based syslog, 250
- Telnet, 81
 - accessing management interface, 261
 - configuring on PIX/ASA firewall, 141–142
 - connectivity, testing, 305
 - remote firewall management, 248
- testing connectivity, 303–305
- TFTP, 82
 - remote firewall management, 250
- threats to security
 - compromise of personal information, 16–17
 - DoS attacks, 15
 - malware, 15
 - poorly designed applications, 18
 - social engineering, 17
 - targeted attacks, 13
 - trojans, 13
 - untargeted attacks, 13
 - viruses, 13
 - worms, 13
 - zero-day attacks, 18
 - zombies, 16
- three-way handshake, 57
- tracking firewall defects, 274–275
- traffic filtering on Linksys routers/firewalls
 - DMZ forwarding, 114
 - from internal sources, 114
 - port triggering, 113
 - port-range forwarding, 112
- traffic going through firewall, troubleshooting, 310, 313–315
- traffic going to firewall, troubleshooting, 316
- transparent firewalls, 39–40
- transparent mode, 133

- transparent proxying, 165**
- transport layer, 47**
- transport mode (IPsec), 335**
- Trend Micro's PC-cillin firewall**
 - feature, 96**
 - checklist, 103–104
 - configuring, 97–102
 - profiles, 98
 - system requirements, 96
- trojans, 14**
- troubleshooting**
 - advanced features, 316
 - checklist of procedures, developing, 301–310
 - firewall configuration, example of, 316, 319–320
 - need for, verifying, 302–303
 - non-firewall specific systems, 309
 - traffic going through firewall, 310, 313–315
 - traffic going to firewall, 316
- trust, 21–22**
- tunnel mode (IPsec), 336**

U

- UDP (User Datagram Protocol), 61**
 - connectionless sessions, 7
 - header fields, 62
 - messages, 62
- ULOG target, 168**
- untargeted attacks, 13**
- updating firewall software, 273–275**
- UPnP (Universal Plug-and-Play), Linksys routers, 111**
- UPnP Forwarding screen (BEFSR41v4 Applications and Gaming tab), 120**
- URL filters, 323**
 - maintenance, 326
 - on Cisco PIX Firewall, configuring, 324–325
- user-defined chains (mangle table), 166**
- utilities, fragrouter, 57**

V

- verifying**
 - firewall configuration, 308
 - firewall rulesets, 308
 - need for troubleshooting, 302–303

- viewing**
 - ACEs, 151
 - RCS log, 271–272
- virtual firewalls, 40, 221**
- viruses, 13**
- VLANs**
 - interaction with firewalls, 219
 - virtual firewalls, 221
- VPN passthrough on Linksys routers, 110**
- VPN Passthrough screen (BEFSR41v4 Security tab), 119**
- VPN Quarantine Control (ISA Server 2004), 189**
- VPNs, 332**
 - IPsec-based, 333
 - AH*, 333
 - ESP*, 334
 - transport mode*, 335
 - tunnel mode*, 336
 - remote-access/VPN policies, 234
 - SSL VPNs, 336
- vulnerabilities, 274**

W

- web applications, application filtering, 327–330**
- web proxy client, 185**
 - configuring on ISA server, 203
- Webmin, configuring Netfilter, 171**
- websites, Netfilter, 162**
- Windows Firewall, 87**
 - checklist, 94–95
 - configuring, 89–93
 - exceptions, 88
 - features, 94
- worms, 14**

X–Y–Z

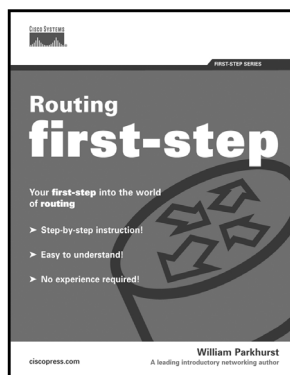
- xauth (extended authentication), 9**
- XDMCP (X Display Management Control Protocol), 61**
- zero-day attacks, 18**



Cisco Press

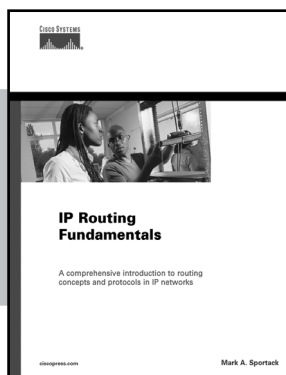
3 STEPS TO LEARNING

STEP 1



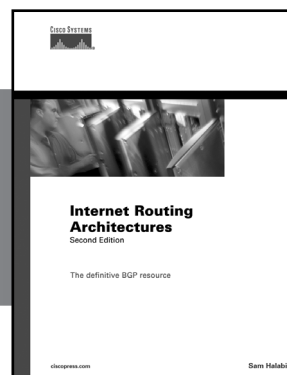
First-Step

STEP 2



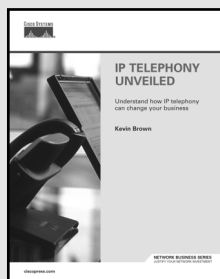
Fundamentals

STEP 3



Networking Technology Guides

- STEP 1 First-Step**—Benefit from easy-to-grasp explanations. No experience required!
- STEP 2 Fundamentals**—Understand the purpose, application, and management of technology.
- STEP 3 Networking Technology Guides**—Gain the knowledge to master the challenge of the network.



NETWORK BUSINESS SERIES

The Network Business series helps professionals tackle the business issues surrounding the network. Whether you are a seasoned IT professional or a business manager with minimal technical expertise, this series will help you understand the business case for technologies.

Justify Your Network Investment.

Look for Cisco Press titles at your favorite bookseller today.

Visit www.ciscopress.com/series for details on each of these book series.



**Cisco Press**

Your first-step to networking starts here

Are you new to the world of networking? Whether you are beginning your networking career or simply need a better understanding of a specific technology to have more meaningful discussions with networking experts, Cisco Press First-Step books are right for you.

- **No experience required**
- **Includes clear and easily understood explanations**
- **Makes learning easy**

Check out each of these First-Step books that cover key networking topics



Computer Networking First-Step
ISBN: 1-58720-101-1

LAN Switching First-Step
ISBN: 1-58720-100-3



Network Security First-Step
ISBN: 1-58720-099-6

TCP/IP First-Step
ISBN: 1-58720-108-9



Voice over IP First-Step
ISBN: 1-58720-156-9

Routing First-Step
ISBN: 1-58720-122-4



Wireless Networks First-Step
ISBN: 1-58720-111-9

Visit www.ciscopress.com/firststep to learn more.

What's your next step?

Eager to dig deeper into networking technology? Cisco Press has the books that will help you move to the next level. Learn more at www.ciscopress.com/series.

ciscopress.com

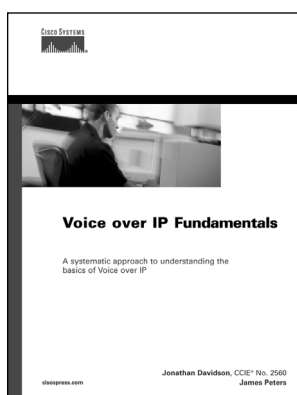
Learning begins with a first step.

**Cisco Press**

FUNDAMENTALS SERIES

ESSENTIAL EXPLANATIONS AND SOLUTIONS

1-57870-168-6



When you need an authoritative introduction to a key networking topic, **reach for a Cisco Press Fundamentals book**. Learn about network topologies, deployment concepts, protocols, and management techniques and **master essential networking concepts and solutions**.

Look for Fundamentals titles at your favorite bookseller

802.11 Wireless LAN Fundamentals

ISBN: 1-58705-077-3

**Cisco CallManager Fundamentals:
A Cisco AVVID Solution**

ISBN: 1-58705-008-0

Cisco LAN Switching Fundamentals

ISBN: 1-58705-089-7

Cisco Unity Fundamentals

ISBN: 1-58705-098-6

Data Center Fundamentals

ISBN: 1-58705-023-4

IP Addressing Fundamentals

ISBN: 1-58705-067-6

IP Routing Fundamentals

ISBN: 1-57870-071-X

Network Security Fundamentals

ISBN: 1-58705-167-2

Storage Networking Fundamentals

ISBN: 1-58705-162-1

Voice over IP Fundamentals

ISBN: 1-57870-168-6

Coming in Fall 2005**Cisco CallManager Fundamentals:
A Cisco AVVID Solution, Second Edition**

ISBN: 1-58705-192-3

Visit www.ciscopress.com/series for details about the Fundamentals series and a complete list of titles.



Cisco Press

NETWORKING TECHNOLOGY GUIDES

MASTER THE NETWORK

Turn to Networking Technology Guides whenever you need **in-depth knowledge of complex networking technologies**. Written by leading networking authorities, these guides offer theoretical and practical knowledge for **real-world networking applications and solutions**.

Look for Networking Technology Guides at your favorite bookseller

**Cisco CallManager Best Practices:
A Cisco AVVID Solution**

ISBN: 1-58705-139-7

**Cisco IP Telephony: Planning, Design,
Implementation, Operation, and Optimization**

ISBN: 1-58705-157-5

Cisco PIX Firewall and ASA Handbook

ISBN: 1-58705-158-3

Cisco Wireless LAN Security

ISBN: 1-58705-154-0

**End-to-End QoS Network Design:
Quality of Service in LANs, WANs, and VPNs**

ISBN: 1-58705-176-1

Network Security Architectures

ISBN: 1-58705-115-X

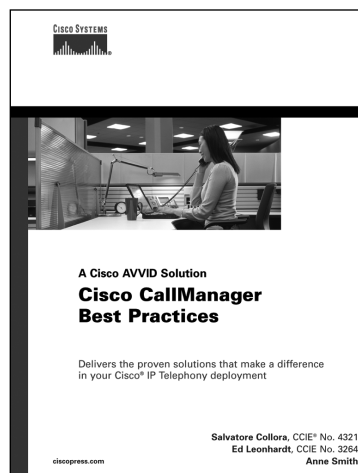
Optimal Routing Design

ISBN: 1-58705-187-7

Top-Down Network Design, Second Edition

ISBN: 1-58705-152-4

Visit www.ciscopress.com/series for details about Networking Technology Guides and a complete list of titles.



1-58705-139-7



Learning is serious business.
Invest wisely.

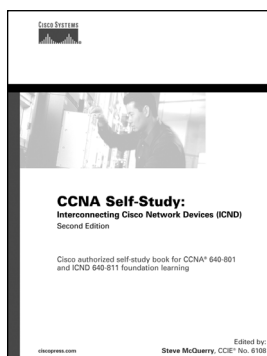


Cisco Press

CISCO CERTIFICATION SELF-STUDY

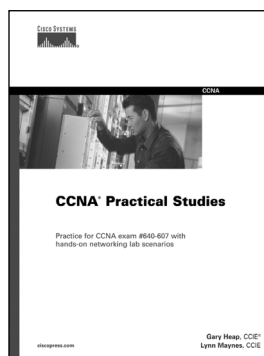
#1 BEST-SELLING TITLES FROM CCNA® TO CCIE®

Look for Cisco Press Certification Self-Study resources at your favorite bookseller



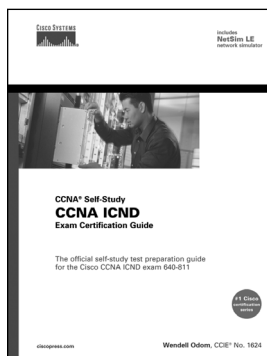
Learn the test topics with **Self-Study Guides**

1-58705-142-7



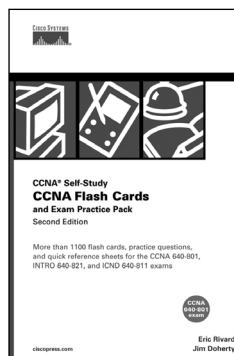
Gain hands-on experience with **Practical Studies** books

1-58720-046-5



Prepare for the exam with **Exam Certification Guides**

1-58720-083-X



Practice testing skills and build confidence with **Flash Cards and Exam Practice Packs**

1-58720-079-1

Visit www.ciscopress.com/series to learn more about the Certification Self-Study product family and associated series.



Learning is serious business.
Invest wisely.

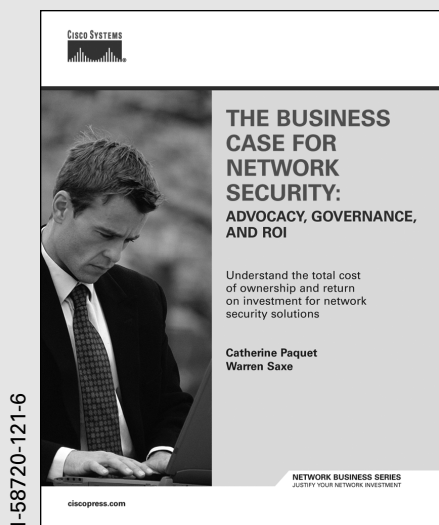


Cisco Press

NETWORK BUSINESS SERIES

JUSTIFY YOUR NETWORK INVESTMENT

Understand the business case for technologies with Network Business books from Cisco Press. Designed to support anyone **searching for optimal network systems**, Network Business titles help you justify your network investments.



Look for Network Business titles at your favorite bookseller

The Business Case for E-Learning

Kelly / Nanjiani • ISBN: 1-58720-086-4

The Business Case for Network Security

Paquet / Saxe • ISBN: 1-58720-121-6

The Business Case for Storage Networks

Williams • ISBN: 1-58720-118-6

The Case for Virtual Business Processes

Young / Jude • ISBN: 1-58720-087-2

IP Telephony Unveiled

Brown • ISBN: 1-58720-075-9

Power Up Your Small-Medium Business

Aber • ISBN: 1-58705-135-4

The Road to IP Telephony

Carhee • ISBN: 1-58720-088-0

Taking Charge of Your VoIP Project

Walker / Hicks • ISBN: 1-58720-092-9

Coming in Fall 2005

The Business Case for Enterprise-Class Wireless LANs

Castaneda / Alasdair / Vinckier • ISBN: 1-58720-125-9

MPLS for Decision Makers

Sayeed / Morrow • ISBN: 1-58720-120-8

Network Business Series. **Justify Your Network Investment.**

Visit www.ciscopress.com/netbus for details about the Network Business series and a complete list of titles.



Cisco Press

SAVE UP TO 30%

Become a member and save at **ciscopress.com!**



Complete a **user profile** at ciscopress.com today to become a member and benefit from **discounts up to 30% on every purchase** at ciscopress.com, as well as a more customized user experience. Your membership will also allow you access to the entire Informit network of sites.

Don't forget to subscribe to the monthly Cisco Press newsletter to be the first to learn about new releases and special promotions. You can also sign up to get your first **30 days FREE on Safari Bookshelf** and preview Cisco Press content. Safari Bookshelf lets you access Cisco Press books online and build your own customized, searchable electronic reference library.

Visit www.ciscopress.com/register to sign up and start saving today!

The profile information we collect is used in aggregate to provide us with better insight into your technology interests and to create a better user experience for you. You must be logged into ciscopress.com to receive your discount. Discount is on Cisco Press products only; shipping and handling are not included.



Learning is serious business.

Invest wisely.



THIS BOOK IS SAFARI ENABLED

INCLUDES FREE 45-DAY ACCESS TO THE ONLINE EDITION

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

TO GAIN 45-DAY SAFARI ENABLED ACCESS TO THIS BOOK:

- Go to <http://www.ciscopress.com/safarienabled>
- Complete the brief registration form
- Enter the coupon code found in the front of this book before the "Contents at a Glance" page

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.