



Numerics

3DES (triple Data Encryption Standard), 199

A

AAA (Authentication, Authorization, and Accounting), 111–114, 236

configuring, 114, 144–145

CSACS, 116–122

floodguard, 168–169

servers, 115

configuring, 275–278

specifying groups, 124

aaa accounting command, 140–145

aaa authentication command, 125

aaa authentication command, 124–125, 145

aaa authentication console command, 130–131

aaa authentication login global configuration command, 276

aaa authorization auth-proxy command, 276

aaa authorization auth-proxy global configuration command, 276

aaa authorization command, 134–136, 145

aaa new-model global configuration command, 275

aaa-server command, 122–123

aaa-server radius protocol radius command, 122

aaa-server tacacs+protocol tacacs+ command, 122

access, 31–32

ACEs, 270

attacks, 8–9

configuring, 81–82

connections, 83–88

console authentication, 130–131

lists

command, 82

crypto, 208–211

multimedia, 94–95

SSH, 306–307

unauthorized, 9

access-group command, 208

access-list command, 82, 207

access-list deny command, 168

access-list permit command, 168

accounting, configuring, 140–143. *See also* AAA

ACEs (access control entries), 270

ACK (acknowledgement), 177

ACLs (Access Control Lists) . *See also* access

CBAC, 243–246

router interfaces, 260–262

ACS (Access Control Sever), 236

adding

four-port expansion cards, 24

users (CSACS-NT), 119–122

addresses

dynamic

PIX 506 DHCP server, 302

translations, 74–76

mapping, 83

NAT, 89–90

PAT, 89–91

port translation, 76

static

PIX 506 DHCP server, 301

translations, 72–73

administration, command-line interface, 31–32

advanced protocol handling, 149

fixup protocol ftp command, 153–154

passive mode FTP, 151–153

rsh, 154

SQL*Net, 156–158

standard mode FTP, 150–151

AH (Authentication Header), 198

alerts. *See also* security

configuring, 247

syslog messages, 101

algorithms

ASA, 19, 53

D-H, 199

applications

IOS Firewall

Authentication Proxy, 236

CBAC, 235

IDS, 237–243

mapping, 252

multimedia

H.323, 163–164

RTSP, 159–163

support, 94–95

upgrading, 42–44

applying

crypto maps, 219

Java filtering, 256–257

arguments, 205

access-list command, 208

ACL, 275

crypto ipsec transform-set command, 212

crypto map command, 216

failover command, 184

ip inspect command, 261

ip inspect name, 258

ip inspect name command, 255

- ip port-map, 253
- show ip inspect, 265
- show ip inspect name command, 266
- unlisted, 140
- ARP (Address Resolution Protocol), 179
- ASA (Adaptive Security Algorithm), 19, 53
- ASN.1 (Abstract Syntax Notation), 163
- assembly, FragGuard, 167
- associations, professional development security, 317
- Attack Guards, 165
 - AAA Floodguard, 168–169
 - DNS Guard, 166
 - Fragmentation Guard, 166–168
 - MailGuard, 165–166
 - SYN Floodguard, 169–173
- attacks
 - DoS, 236, 259
 - network security, 7–9
- audits
 - policies
 - configuring, 286
 - disabling IDS signatures, 288
 - trails, 247
- authentication. *See also* AAA
 - configuring, 122–125
 - console access, 130–131
 - customizing services, 126
 - prompts, 133–134
 - timeouts, 132–133
 - virtual Telnet, 126–129
 - virtual HTTP, 129–130
 - Identification Authentication Systems, 11
 - IOS Authentication Proxy, 269, 271–283
- Authentication Header (AH), 198
- Authentication Proxy, IOS Firewall, 236
- authentication proxy name command, 280
- authorization, configuring, 134–140. *See also* AAA
- auth-prompt command, 133–134, 145

B

- backup gateways, 216
- bastion hosts, 4
- benefits of firewalls, 19–20
- block-time settings, 251
- Boothelper diskette, 45–46

C

- cables, failover, 176–177
- caches, 127

- CAs (Certificate Authorities), 200
- categorizing network security threats, 6–7
- CBAC (Context-Based Access Control), 235
 - ACLs, 243–246
 - configuring, 247–254
 - debugging, 266
 - firewalls, 262–264
 - monitoring, 265–266
 - protocols, 254–259
 - PKI resources, 321
 - router interfaces, 260–262
 - IOS Firewall, 235
- channels
 - control, 150
 - data, 150
- Cisco
 - IOS Firewall. *See* IOS Firewall
 - web site, 321
 - PIX Firewall models, 20. *See also* PIX Firewall
 - Model 506, 21
 - Model 515, 22–23
 - Model 520, 24–25
 - Model 525, 26
 - Model 535, 26–27
 - Cisco Secure Access Control Server (CSACS), 112
 - classic mode FTP. *See* standard mode FTP
 - clean fixup protocol rsh command, 156
 - clear access-list command, 208
 - clear fixup protocol ftp command, 154
 - clear fixup protocol h323 command, 164
 - clear fixup protocol rstp command, 163
 - clear fixup protocol smtp command, 166
 - clear fixup protocol sqlnet command, 158
 - clear ip auth-proxy cache command, 281
 - clear logging command, 102, 109
 - clear logging disabled command, 104
 - clear passwd command, 34
 - clear telnet command, 41
 - clear uauth command, 132
 - clear xlate command, 77
- clients
 - DHCP, 300
 - multimedia, 158–159
 - H.323, 163–164
 - RTSP, 159–163
 - SSH
 - downloading, 314
 - troubleshooting, 312–314
- command-line interfaces, 31–32
- commands, 145, 248–250
 - aaa accounting, 140–142, 145
 - aaa authentication, 124–125, 145

- aaa authentication console, 130–131
- aaa authentication login global configuration, 276
- aaa authorization, 134–136, 145
- aaa authorization auth-proxy, 276
- aaa authorization auth-proxy global configuration, 276
- aaa new-model global configuration command, 275
- aaa-server, 122–123
- aaa-server radius protocol radius, 122
- aaa-server tacacs+protocol tacacs+, 122
- access-group, 208
- access-list, 82, 207
- access-list deny, 168
- access-list permit, 168
- authentication proxy name, 280
- auth-prompt, 133–134, 145
- clear fixup protocol rsh, 156
- clear access-list, 208
- clear fixup protocol h323, 164
- clear fixup protocol ftp, 154
- clear fixup protocol rstp, 163
- clear fixup protocol smtp, 166
- clear fixup protocol sqlnet, 158
- clear ip auth-proxy cache, 281
- clear logging, 102, 109
- clear logging disabled, 104
- clear passwd, 34
- clear telnet, 41
- clear uauth, 132
- clear xlate, 77
- conduit, 73, 82–88
- configure memory, 35
- configure net, 35
- configure terminal, 33
- copy tftp flash, 42
- crypto ipsec security-association lifetime, 207, 214
- crypto ipsec transform-set, 207, 212
- crypto map map-name interface, 207
- debug dhcp, 300
- debug icmp trace, 41
- debug ip auth-proxy, 281
- debug ip inspect, 265
- debug ssh, 312
- dhcp address, 301
- dhcpcd, 299
- disable, 33
- enable, 33
- enable password password, 33
- exit, 33
- failover, 184
- failover active, 182
- failover poll, 178
- failover reset, 179
- File menu, Save Settings, 309
- fixup protocol 66, 156
- fixup protocol ftp, 21, 151, 153–154
- fixup protocol ftp port-number, 153
- fixup protocol h323, 164
- fixup protocol protocol, 150
- fixup protocol rsh, 154–155
- fixup protocol rstp, 162–163
- fixup protocol smtp, 165
- fixup protocol sqlnet, 156–158
- floodguard, 168
- global, 59–61, 300
- hostname, 40
- HTTP GET, 130
- interface, 36, 57–58
- IOS, 136
- ip address, 58
- ip audit, 286
- ip audit attack, 286–287
- ip audit info, 286
- ip audit interface, 288
- ip audit name, 286–287
- ip audit name inbound, 289
- ip audit name info, 287
- ip audit name outbound, 289
- ip audit signature, 288
- ip audit signature disable, 288
- ip authentication aaa, 278
- ip auth-proxy auth-cache-time, 279
- ip auth-proxy auth-cache-time global configuration, 278
- ip auth-proxy interface configuration, 280
- ip auth-proxy name global configuration, 279
- ip http authentication aaa, 269
- ip http server, 278
- ip inspect, 260–261
- ip inspect audit-trail, 247
- ip inspect dns-timeout command, 249
- ip inspect max-incomplete high, 249
- ip inspect name, 255, 257–258
- ip inspect name inspection-name http, 256
- ip inspect one-minute high, 250
- ip inspect tcp finwait-time, 248
- ip inspect tcp idle-time, 248
- ip inspect tcp max-incomplete host, 251
- ip port-map, 253, 256
- isakmp enable, 202
- isakmp identity, 205
- isakmp key, 205
- isakmp policy, 203
- kill, 41
- kill -HUP process_id, 45

- logging buffered, 104, 106
 - logging console, 106
 - logging facility, 106
 - logging history, 105, 295
 - logging host, 103, 105
 - logging message, 108
 - logging monitor, 107
 - logging on, 101–102, 104
 - logging standby, 107
 - logging timestamps, 107
 - logging trap, 105
 - name, 98
 - nameif, 56–57, 83
 - nat, 59, 75, 172
 - nat 0, 92
 - nat(DMZ)0, 92
 - no aaa accounting, 145
 - no aaa authentication, 145
 - no aaa authorization, 145
 - no failover, 185
 - no failover active, 182
 - no fixup protocol smtp 25, 165
 - no ip audit interface, 288
 - no ip audit name, 286
 - no ip audit signature, 288
 - no ip inspect, 266
 - no ip inspect alert-off, 247
 - no isakmp policy 100 encryption, 204
 - no logging message, 104
 - no logging message 101001, 108
 - no logging on, 295
 - no logging standby, 104, 107
 - no names, 98
 - no telnet, 41
 - passwd, 34
 - ping, 41, 179, 201
 - ps aux | grep inetd, 45
 - quit, 33
 - radius-server host global configuration, 277
 - radius-server key global configuration, 277
 - reload, 40
 - route, 61–63, 300
 - show aaa, 144–145
 - show access-list, 220
 - show auth-prompt, 145
 - show clock, 107
 - show conduit, 89
 - show config, 108
 - show configure, 34
 - show conn, 78
 - show crypto map, 201
 - show enable, 33
 - show failover, 179, 183, 185
 - show history show interface command, 35
 - show interface, 35
 - show ip address, 38
 - show ip audit signature, 288
 - show ip auth-proxy, 280
 - show ip inspect, 265
 - show ip inspect name, 266
 - show ip port-map, 254
 - show isakmp, 201
 - show isakmp identity, 202
 - show isakmp policy, 201
 - show local-host, 171
 - show logging, 102, 104, 108
 - show logging queue, 104
 - show memory, 39
 - show message disabled, 104
 - show static, 83
 - show telnet, 41
 - show timeout auth, 145
 - show version, 39
 - show xlate, 40, 77
 - snmp-server enable traps, 295
 - snmp-server host, 295
 - spantree portfast, 181
 - Start>Run, 45
 - static, 73, 82–83, 170–171
 - sysopt security fragguard, 166
 - tacacs-server host, 276
 - tacacs-server key global, 277
 - tcp max-incomplete host, 250
 - telnet, 41, 131
 - timeout uauth, 132–133
 - virtual http, 130
 - virtual telnet, 127
 - who, 41
 - write erase, 34
 - write floppy, 34
 - write memory, 34, 178
 - write net, 34
 - write standby, 34, 178
 - write terminal, 34, 103, 108, 201
 - xlate, 77
- compatibility with IPSec, 196
- conduit command, 73, 82–88
- configuration
- AAA, 114
 - servers, 273–278
 - viewing, 144–145
 - access, 81–82
 - accounting, 140–142
 - customizing services, 143
 - viewing records, 142
 - alerts, 247

- audit policies, 286
 - authentication, 122–125
 - console access, 130–131
 - customizing services, 126
 - prompts, 133–134
 - timeouts, 132–133
 - virtual HTTP, 129–130
 - virtual Telnet, 126–127, 129
 - authorization, 134–140
 - block-time, 251
 - CBAC, 243–254
 - defining protocols, 254–259
 - router interfaces, 260–262
 - commands, 56
 - global, 59–61
 - interface, 57–58
 - ip address, 58
 - nameif, 56–57
 - nat, 59
 - route, 61–63
 - crypto maps, 216–219
 - DHCP, 299, 301–302
 - clients, 300
 - servers, 299
 - elements, 286–290
 - Failover Operation, 182–191
 - failover replication, 177
 - FIXUP protocol, 93–94
 - global IPsec SA lifetimes, 214
 - identity modes, 205
 - IOS Authentication Proxy, 272–283
 - IPsec, 200, 207–208, 210–219
 - preparing, 201
 - pre-shared keys, 202–207
 - testing, 221–223
 - verifying, 220–223
 - MIB browsing, 294
 - multiple interfaces, 95–98
 - nat 0, 92
 - parameters, 114
 - routers, 262–264
 - SSH, 305–309
 - syslog, 101–109, 294
 - thresholds, 248–251
 - transform sets, 211–213
- Configuration Mode, 31
- configure memory command, 35
 - configure net command, 35
 - configure terminal command, 33
- connections
- access, 83–88
 - failover cables, 176–177
 - inbound, 150–151
 - RDT mode, 161
 - rsh, 154
 - RTSP, 161
 - SQL*Net, 157
 - inbound PASV, 153
 - multimedia, 94–95
 - OSI. *See* OSI
 - outbound, 151
 - RDT mode, 161
 - rsh, 154
 - RTSP, 161
 - SQL*Net, 157
 - outbound PASV, 152
 - slots, 68
 - SSH, 307, 309
 - configuring, 306–307
 - downloading clients, 314
 - troubleshooting clients, 312–314
 - stateful packet filters, 18
 - translations, 77–78
- consoles, authenticating, 130–131
- control channels, 150
- copy tftp flash command, 42
- CPU usage, CBAC, 236
- cracking tools, 320
- crypto access lists, creating, 208–211. *See also* ACLs
- crypto ipsec security-association lifetime command, 207, 214
- crypto ipsec transform-set command, 207, 212
- crypto map map-name interface command, 207
- crypto maps
- applying, 219
 - configuring, 216–219
 - creating, 215
- CSACS (Cisco Secure Access Control Server), 11, 112
- AAA, 116–122
 - Windows NT
 - adding authorization rules, 136
 - viewing records, 142
- CSI (Computer Security Institute), 3
- CSIDS (Cisco Secure Intrusion Detection System), 11
- CSPM (Cisco Secure Policy Manager), 291
- customization
- AAA services, 126
 - accounting services, 143
 - authorization services, 138–140
 - virtual HTTP, 129–130
 - virtual Telnet, 126–129
- cut-through proxies, 19, 114. *See also* AAA

D

- data channels, 150
- DDoS attacks, 9
- debug dhcp command, 300
- debug icmp trace, 41
- debug ip auth-proxy command, 281
- debug ip inspect command, 265
- debug ssh command, 312
- debugging CBAC, 266
- defining
 - inspection rules, 255
 - PAM, 251–254
 - protocols, 254–259
- delays, forwarding, 181
- demilitarized zone (DMZ), 95
- depleting syslog messages, 101
- DES (Data Encryption Standard), 199
- design, network security, 3–5. *See also* configuration
- detection, interface failures, 181. *See also* IDS
- D-H (Diffie-Helman) algorithm, 199
- DHCP (Dynamic Host Configuration Protocol)
 - clients, 300
 - configuring, 299, 301–302
 - resources, 302
 - servers, 299
- dhcp address command, 301
- dhcpcd command, 299
- disable command, 33
- disabling
 - IDS signatures, 288
 - IKE, 202
- diskettes
 - creating, 45
 - installing, 46
- DMZ (Demilitarized Zone), 4, 95, 364
- DNS (Domain Name System), 248
- DNS Guard, 166
- DoS (Denial of Service) attacks, 8, 236, 259
- downloading SSH clients, 314
- dynamic address translations, 74–76
- dynamically acquired outside addresses, 302

E

- EDI (Electronic Data Interchange), 95
- Electronic Data Interchange (EDI), 95
- elements, configuring IDS, 286–290
- e-mail, MailGuard, 165–166
- enable command, 33

- enable password command, 33
- enable password password command, 33
- enabling
 - IKE, 202
 - VPN, 195
- Encapsulating Security Payload (ESP), 198
- encryption, 11
- enrollment of CAs, 223
- escalation, unauthorized privilege, 9
- ESP (Encapsulating Security Payload), 198
- events, syslog messages, 101
- exclude parameter, 134
- exit command, 33
- expansion, adding four-port expansion cards, 24
- exploits, OS, 319
- external interfaces, configuring, 261–262
- external threats, 7

F

- fail back, 182
- Failover Operation, 176
 - command, 182
 - configuration replication, 177
 - configuring, 182–191
 - fail back, 182
 - failover cable, 176–177
 - monitoring, 178–181
- failovers
 - poll command, 178
 - reset command, 179
 - stateful, 19
- FAQs (frequently asked questions), IDS, 291
- features of firewalls, 19–20
- File menu commands, Save Settings, 309
- filters
 - Java, 256–257
 - packets, 16–18
 - proxy, 17
- firewalls, 3, 11. *See also* PIX Firewall; security
 - benefits and features, 19–20
 - configuration commands, 56
 - global, 59–61
 - interface, 57–58
 - ip address, 58
 - nameif, 56–57
 - nat, 59
 - route, 61–63
 - configuring, 262–264
 - interfacing, 4

- IOS Firewall, 235
 - ACLs, 243–246
 - Authentication Proxy, 236
 - CBAC, 235
 - IDS, 237–243
 - monitoring CBAC, 265–266
- maintaining, 33–41
- models (PIX Firewall), 20
 - 506, 21
 - 515, 22–23
 - 520, 24–25
 - 525, 26
 - 535, 26–27
- testing, 33–41
- three interface, 263
- translations, 71–72
 - connections, 77–78
 - dynamic addresses, 74–76
 - static addresses, 72–73
- types of, 15–16
 - packet filters, 16–17
 - proxy filters, 17
 - stateful packet filters, 18
- upgrading, 42–44
- FIXUP protocol, configuring, 93–94
- fixup protocol 66 command, 156
- fixup protocol ftp 21 command, 153
- fixup protocol ftp command, 151, 153–154
- fixup protocol ftp port-number command, 153
- fixup protocol h323 command, 164
- fixup protocol protocol commands, 150
- fixup protocol rsh command, 154–155
- fixup protocol rstp command, 162–163
- fixup protocol smtp command, 165
- fixup protocol sqlnet command, 156–158
- floodguard command, 168
- floppy drives
 - Boothelper, 46
 - password recovery, 47–48
- formatting. *See also* configuration
 - Boothelper diskette, 45–46
 - crypto access lists, 208, 210–211
 - crypto maps, 215
 - IKE policies, 202–204
- forwarding delays, 181
- four-port expansion cards, adding, 24
- Fragmentation Guard, 166–168, 259
- FTP (File Transfer Protocol), 150
 - AAA, 112
 - passive mode, 151, 153
 - standard mode, 150–151

G

- gateways, backup, 216
- global audit policies, 287
- global command, 59–61, 75, 300
- global IP addresses, mapping, 83
- global IPSec SA lifetimes, configuring, 214
- global timeouts, 248–251
- Greenwich Mean Time, 107
- Group Setup window, 136
- groups, specifying AAA servers, 124

H

- H.225-RAS (Registration, Admission, and Status), 163
- H.323 multimedia support, 163–164
- handling
 - fixup protocol ftp command, 153–154
 - passive mode FTP, 151
 - rsh, 154
 - SQL*Net, 156
 - standard mode FTP, 150–151
- hardware
 - failover cables, 176–177
 - firewalls, 15–16
 - packet filters, 16–17
 - proxy filters, 17
 - stateful packet filters, 18
- hello messages, 179
- hostname command, 40
- hosts
 - bastion, 4
 - IDS, 319
- hot standbys, 19
- HTTP (Hypertext Transfer Protocol), 236
 - AAA, 113
 - virtual, 129–130
 - show virtual, 145
- HTTP GET command, 130

I

- IANA (Internet Assigned Numbers Authority), 71, 156
- Identification Authentication Systems, 11
- identities, configuring, 205
- IDS (Intrusion Detection System), 285
 - configuration elements, 286–290
 - FAQs, 291
 - hosts, 319
 - IOS Firewall, 237–243
 - networks, 318
 - signatures, 290
- IETF (Internet Engineering Task Force), 197

- IKE (Internet Key Exchange)
 - configuring, 206–207
 - disabling, 202
 - enabling, 202
 - policies, 202–204
- inbound connections, 150–151
 - RDT mode, 161
 - rsh, 154
 - RTSP, 161
 - SQL*Net, 157
- inbound PASV connections, 153
- inbound traffic, 264
- information gathering, 8
- input, AAA, 112
- inspection
 - RPC, 257–258
 - rules
 - defining, 255
 - router interfaces, 260–262
- installation, 44
 - CSACS, 116–122
 - OS, 42
 - creating Boothelper diskette, 45
 - installing Boothelper diskette, 46
 - PIX 5.0 and earlier, 44
 - PIX 5.1 and later, 44
 - upgrading PIX software, 42–44
- interfaces, 31–32
 - audit policies, 286
 - command, 36, 57–58
 - crypto maps, 219
 - failures, 181
 - firewalls, 4
 - internal interfaces, 262
 - MIB, 294
 - multiple, 95–98
 - routers, 260–262
 - three-interface firewalls, 263
- internal threats, 7
- Internet Assigned Numbers Authority (IANA), 71
- Internet Engineering Task Force (IETF), 197
- internetworks, 3
- inventories, SNMP v1 MIB-11, 295
- IOS Authentication Proxy, 269–281
- IOS commands, 136. *See also* commands
- IOS Firewall, 235
 - Authentication Proxy, 236
 - CBAC, 235
 - ACLs, 243–246
 - configuring, 247, 262–264
 - configuration
 - audit trails, 247
 - global timeouts, 248–251
 - PAM, 251–254
 - defining protocols, 254–259
 - router interfaces, 260–262
 - IDS, 237–243
 - monitoring, 265–266
- IP (Internet Protocol)
 - address mapping, 83
 - name command, 98
 - traffic, 255
- ip address command, 58
- ip adit info command, 286
- ip audit attack command, 286–287
- ip audit command, 286
- ip audit interface command, 288
- ip audit name command, 286–287
- ip audit name inbound command, 289
- ip audit name info command, 287
- ip audit name outbound command, 289
- ip audit signature command, 288
- ip audit signature disable command, 288
- ip authentication aaa command, 278
- ip auth-proxy auth-cache-time command, 279
- ip auth-proxy auth-cache-time global configuration command, 278
- ip auth-proxy interface configuration command, 280
- ip auth-proxy name global configuration command, 279
- ip http authentication aaa command, 269
- ip http server command, 278
- ip inspect max-incomplete high command, 249
- ip inspect max-incomplete low command, 249
- ip inspect one-minute high command, 250
- ip inspect audit-trail command, 247
- ip inspect command, 260
- ip inspect dns-timeout command, 249
- ip inspect max-incomplete low command, 249
- ip inspect name command, 255, 257–258
- ip inspect name inspection-name http command, 256
- ip inspect one-minute low command, 250
- ip inspect tcp finwait-time command, 248
- ip inspect tcp idle-time command, 248
- ip inspect tcp max-incomplete host command, 251
- ip inspect tcp synwait-time command, 248
- ip port-map command, 253, 256
- IPSec (IP Security), 197–198, 236
 - compatibility, 196
 - configuring, 200, 207–219
 - preparing, 201
 - pre-shared keys, 202–207
 - testing, 221–223
 - verifying, 220–223
 - VPN, 197–198

isakmp enable command, 202
 isakmp identity command, 205
 isakmp key command, 205
 isakmp policy command, 203

J–L

Java, filtering, 256–257

kill command, 41
 kill -HUP process_id command, 45

L2TP (Layer 2 Tunneling Protocol), 235

legal resources, 318

levels

ASA security, 53, 55

logging, 102

lifetimes, configuring global IPSec SAs, 214

limitations of ACLs, 243–246

Linux, creating Boothelper diskettes, 45

lists, ACL. *See* ACL

local IP addresses, mapping, 83

logging buffered command, 104, 106

logging console command, 106

logging facility command, 106

logging history command, 105, 295

logging host command, 103, 105

logging message command, 108

logging monitor command, 107

logging on command, 101–102, 104

logging standby command, 107

logging timestamps command, 107

logging trap command, 105

logic, firewalls, 19–20

M

magazines, 321

Mail Guard, CBAC, 258–259. *See also* e-mail

maintenance, 33–41. *See also* troubleshooting

mapping

crypto

applying, 219

configuring, 216–219

creating, 215

IP addresses, 83

name command, 98

system-defined ports, 252–254

MD5 (Message Digest 5), 199

memory, CBAC, 236

messages

ACK, 177

hello, 179

Sync Completed, 178

Sync Started, 178

syslog, 101, 109

MIB (Management Information Base)

browsing, 294

SNMP v1 MIB-II inventory, 295

minimum system requirements, OS installation, 42

models (PIX Firewall), 20

506, 21

515, 22–23

520, 24–25

525, 26

535, 26–27

modes

command-line interface, 31

identities, 205

RDT, 161

RTP, 160–161, 163

modification

prompts, 133–134

timeouts, 132–133

Monitor Mode, 31

monitoring

CBAC, 265–266

Failover Operation, 178–181

networks, 11

PAM, 254

multimedia support, 94–95, 158–159

H.323, 163–164

RTSP, 159–163

multiple interfaces, configuring, 95–98

N

name command, 98

nameif command, 56–57, 83

nat (DMZ)0 command, 92

NAT (Network Address Translation), 89–90, 149, 236

nat 0 command, 92

nat command, 59, 75, 172

NetBIOS, 72

Network Address Translation (NAT), 89–90

networks

activity, 179

IDS, 318

monitoring, 11

security, 3
 categorizing threats, 6–7
 design, 3–5
 policies/Security Wheel, 10–11
 types of attacks, 7–9

SNMP
 resources, 296
 retrieving data, 294–295
 support, 293
 v1 MIB-II inventory, 295

VPN
 3DES, 199
 CAs, 200, 223
 DES, 199
 D-H, 199
 enabling, 195
 IPSec, 197–198
 MD5, 199
 RSA signatures, 200
 SA, 198
 scaling, 223
 SHA-1, 199

NIC (network information card), 179

no aaa accounting command, 145

no aaa authentication command, 145

no aaa authorization command, 145

no failover active command, 182

no failover command, 185

no fixup protocol smtp 25 command, 165

no ip audit interface command, 288

no ip audit name command, 286

no ip audit signature command, 288

no ip inspect alert-off command, 247

no ip inspect command, 266

no isakmp policy 100 encryption command, 204

no logging message 101001 command, 108

no logging message command, 104, 108

no logging on command, 295

no logging standby command, 104, 107

no names command, 98

no telnet command, 41

non-standard port mappings, 252

NTP (Network Time Protocol), 107

NVRAM (non-volatile RAM), 246

O

OID (object ID), 294

operations
 cut-through proxy, 114
 Failover Operation, 176
 configuration replication, 177
 configuring, 182–191

fail back, 182

failover cable, 176–177

monitoring, 178–181

options. *See also* customization
 access-list command, 208
 ACL, 275
 clear ip auth-proxy cache command, 281
 crypto map command, 216
 debug ip auth-proxy command, 281
 failover command, 184
 isakmp key command, 205

OS (operating system)
 Boothelper diskette
 creating, 45
 installing, 46
 exploits, 319
 installing, 42, 42–44
 PIX 5.0 and earlier, 44
 PIX 5.1 and later, 44

OSI (Open System Interconnection), 17

OTP (One-Time Passwords), 11

outbound connections, 151
 RDT mode, 161
 rsh, 154
 RTSP, 161
 SQL*Net, 157

outbound PASV connections, 152

outbound traffic, 263

outbound traffic policies, 262

output of show logging command, 108

P

packets
 filters, 16–18
 proxy filters, 17
 testing, 16

PAM (Port-to-Application Mapping), 247
 defining, 251–254
 monitoring, 254

parameters
 crypto maps, 215
 exclude, 134
 IPSec, 207–219
 isakmp policy command, 203
 logging, 102
 timeout uauth, 114

passive mode FTP, 151, 153

passwd command, 34

passwords
 OTP (One-Time Passwords), 11
 recovery, 47–49

PAT (Port Address Translation), 89–91, 150

- periodicals, 321
 - PFSS (PIX Firewall Syslog Server), 105
 - physical security, 11
 - ping command, 41, 179, 201
 - ping sweeps, 8
 - PIX 506, DHCP server, 301–302
 - PIX Firewall
 - configuration commands, 56
 - global, 59–61
 - interface, 57–58
 - ip address, 58
 - nameif, 56–57
 - nat, 59
 - route, 61–63
 - maintaining, 33–41
 - models, 20
 - 506, 21
 - 515, 22–23
 - 520, 24–25
 - 525, 26
 - 535, 26–27
 - testing, 33–41
 - translations, 71–72
 - connections, 77–78
 - dynamic addresses, 74–76
 - static addresses, 72–73
 - upgrading, 42–44
 - policies
 - audit
 - configuring, 286
 - disabling IDS signatures, 288
 - global audit, 287
 - IKE, 202–204
 - inbound traffic, 263
 - outbound traffic, 262
 - security, 10–11, 202, 206
 - show isakmp command, 202, 206
 - Port Address Translation (PAT), 89–91
 - portals, security, 320
 - ports. *See also* PAM
 - addresses, 76
 - expansion cards, 24
 - Privileged Mode, 31
 - professional development security associations, 317
 - prompts
 - AAA
 - authentication, 145
 - authorization, 145
 - Administrative Modes, 32
 - modifying, 133–134
 - protocols
 - advanced protocol handling, 149
 - fixup protocol ftp command, 153–154
 - passive mode FTP, 151–153
 - rsh, 154
 - SQL*Net, 156–158
 - standard mode FTP, 150–151
 - CBAC (Context-Based Access Control), 254–259
 - DHCP (Dynamic Host Control Protocol)
 - clients, 300
 - configuring, 299–302
 - resources, 302
 - servers, 299
 - FIXUP, 93–94
 - fixup protocol protocols, 150
 - FTP (File Transfer Protocol), 150
 - HTTP (Hypertext Transfer Protocol), 236
 - NTP (Network Time Protocol), 107
 - RDT (Real Data Transport Protocol), 159
 - RTCP (RTP Control Protocol), 159
 - RTP (Real-Time Transport Protocol), 159
 - RTSP (Real Time Streaming Protocol), 159–161, 163
 - SNMP (Simple Network Management Protocol)
 - resources, 296
 - retrieving data, 294–295
 - support, 293
 - v1 MIB-II inventory, 295
 - transport, 67
 - TCP, 68–69
 - UDP, 70
 - proxy filters, 17
 - ps aux | grep inetd command, 45
- ## Q–R
-
- QoS (Quality of Service), 235
 - quad cards, 25
 - quit command, 33
 - RADIUS (Remote Authentication Dial-In User Service), 20, 236
 - radius-server host global configuration command, 277
 - radius-server key global configuration command, 277
 - RAM (random-access memory), 246
 - rawrite.exe, 45
 - RDT (Real Data Transport Protocol), 159
 - RealNetworks, 161
 - recommended reading, 321
 - reconnaissance attacks, 8

- reconnaissance tools
 - UNIX, 319
 - Windows, 319
- records, 142
- recovery of passwords, 47–49
- reload command, 40, 43
- replication of failover configuration, 177
- requirements, OS installation, 42
- resources
 - certificate authority (PKI), 321
 - DHCP, 302
 - legal, 318
 - security, 317–322
 - SNMP, 296
 - SSH, 320
 - syslog messages, 101
- retrieval
 - data, 294–295
 - unauthorized data, 8
- route command, 61–63, 300
- routers
 - firewalls, 262–264
 - interfaces, 260–262
- RPC (Remote Procedure Call), 257–258
- RSA signatures, VPN, 200
- rsh (Remote Shell), 150, 154
- RTCP (RTP Control Protocol), 159
- RTP (Real-Time Transport Protocol), 159
- RTSP (Real Time Streaming Protocol), 159–163
- Run command, 45

S

- SA (Security Authority)
 - global IPsec SA lifetimes, 214
 - VPN, 198
- Save Settings command (File menu), 309
- scaling VPNs, 223
- script kiddies, 6
- secure, real-time, embedded systems, 19
- security
 - AAA, 111–114
 - ASA levels, 53, 55
 - Attack Guards, 165
 - AAA Floodguard, 168–169
 - DNS Guard, 166
 - Fragmentation Guard, 166–168
 - MailGuard, 165–166
 - SYN Floodguard, 169, 171, 173
 - configuring, 81–82
 - IDS, 285
 - configuration elements, 286–290
 - signatures, 290

- IPsec, 200–207
- networks, 3
 - categorizing threats, 6–7
 - design, 3–5
 - policies/Security Wheel, 10–11
 - types of attacks, 7–9
- portals, 320
- resources, 317–322
- SNMP, 293
 - resources, 296
 - retrieving data, 294–295
 - v1 MIB-II inventory, 295
- SSH
 - clients, 307, 309
 - configuring, 305–307
 - downloading clients, 314
 - troubleshooting clients, 312–314
- VPN
 - 3DES, 199
 - CAs, 200
 - DES, 199
 - D-H, 199
 - IPsec, 197–198
 - MD5, 199
 - RSA signatures, 200
 - SA, 198
 - SHA-1, 199
- security parameter index (SPI), 198
- Security Wheel, 10–11
- sending syslog traps, 294
- servers
 - AAA, 115
 - configuring, 273–278
 - Floodguard, 168–169
 - specifying groups, 124
 - ACS, 236
 - CSACS, 11
 - DHCP, 299
 - DNS Guard, 166
 - Fragmentation Guard, 166–168
 - MailGuard, 165–166
 - PFSS, 105
 - SYN Floodguard, 169–173
 - syslog messages, 101
 - TFTP password recovery, 48–49
- services
 - AAA, 126
 - accounting, 143
 - authorization, 138–140
 - IOS Authentication Proxy, 269, 271–281
- SHA-1, VPN, 199
- show aaa commands, 144–145
- show access-list command, 220

- show auth-prompt command, 145
 - show clock command, 107
 - show conduit command, 89
 - show config command, 108
 - show configure command, 34
 - show conn command, 78
 - show crypto map command, 201
 - show enable command, 33
 - show failover command, 179, 183, 185
 - show history command, 35
 - show ip address command, 38
 - show ip audit signature command, 288
 - show ip auth-proxy command, 280
 - show ip inspect command, 265
 - show ip inspect name command, 266
 - show ip port-map command, 254
 - show isakmp command, 201
 - show isakmp identity command, 202
 - show isakmp policy command, 201
 - show local-host command, 171
 - show logging command, 102, 104, 108
 - show logging queue command, 104
 - show memory command, 39
 - show message disabled command, 104
 - show static command, 83
 - show telnet command, 41
 - show timeout uauth command, 145
 - show version command, 39
 - show xlate command, 40, 77
 - signatures, IDS, 288–290
 - SMTP (Simple Mail Transfer Protocol)
 - CBAC, 258–259
 - MailGuard, 165–166
 - SNMP (Simple Network Management Protocol)
 - discovery tools (Windows), 319
 - resources, 296
 - retrieving data, 294–295
 - support, 293
 - v1 MIB-II inventory, 295
 - snmp-server enable traps command, 295
 - snmp-server host command, 295
 - software, upgrading, 42–44
 - SOHO (small office/home office), 299
 - Solaris, creating Bootheper diskettes, 45
 - spantree portfast command, 181
 - specifying AAA server groups, 124
 - SPI (security parameter index), 198
 - SQL*Net, 156, 158
 - SSH (Secure Shell)
 - clients
 - configuring, 307–309
 - downloading, 314
 - troubleshooting, 312–314
 - configuring, 305–307
 - resources, 320
 - standard mode FTP, 150–151
 - Start command, 45
 - stateful, packet filters, 18
 - stateful failover, 189. *See also* Failover Operation
 - stateful failovers, 19
 - states, waiting, 181
 - static address translations, 72–73
 - static command, 73, 82–83, 170–171
 - static outside addresses, 301
 - structured threats, 7
 - support
 - AAA servers, 115
 - multimedia, 94–95, 158–159
 - H.323, 163–164
 - RTSP, 159–163
 - SNMP, 293
 - SYN Floodguard, 169–173
 - Sync Completed message, 178
 - Sync Started message, 178
 - synchronization of failover configuration replication, 177
 - syslog
 - configuring, 101–109
 - messages, 101, 109
 - traps, 294
 - sysopt security fragguard command, 166–168
 - SystemAccess attackers, 9
 - system-defined port mapping, 252–254
-
- ## T
-
- TACACS+ (Terminal Access Controller Access Control System), 20, 236
 - tacacs-server host commands, 276
 - tacacs-server key global configuration command, 277
 - TCP (Transmission Control Protocol), 68–69
 - tcp max-incomplete hosts command, 250
 - TCP/IP (Transmission Control Protocol/Internet Protocol), 16–17
 - Telnet
 - AAA, 112
 - command, 41, 131
 - virtual, 126–129
 - testing, 179, 280–281
 - CBAC, 265–266
 - failover operations, 179
 - firewalls, 33–41
 - IPSec, 221–223
 - packets, 16
 - ping, 179
 - TFTP (Trivial File Transfer Protocol) servers, 48–49
 - threats, categorizing, 6–7

- three-interface firewalls, 263
- thresholds, configuring, 248–251
- time, block-time settings, 251
- timeout uauth command, 132–133
- timeout uauth configuration parameter, 114
- timeouts
 - configuring, 248–251
 - modifying, 132–133
- tools
 - cracking, 320
 - UNIX reconnaissance, 319
 - Windows
 - reconnaissance, 319
 - SNMP discovery, 319
- topologies, VPN, 195
- traffic
 - DMZ-bound, 264
 - inbound, 263–264
 - IP, 255
 - outbound, 263
 - RTP, 161
 - RTSP, 161
 - TCP/IP packet filters, 16–17
- trails, configuring, 247
- transactions
 - advanced protocol handling, 149
 - fixup protocol ftp command, 153–154
 - passive mode FTP, 151–153
 - rsh, 154
 - SQL*Net, 156–158
 - standard mode FTP, 150–151
 - RTP, 160
- transform sets, configuring, 211–213
- translations, 71–72
 - connections, 77–78
 - dynamic addresses, 74–76
 - NAT, 89–90
 - PAT, 89–91
 - port addresses, 76
 - slots, 68
 - static addresses, 72–73
- transport protocols, 67
 - TCP, 68–69
 - UDP, 70
- traps
 - SNMP, 294
 - syslog, 294
- Trojan horses, 6

- troubleshooting
 - CBAC, 265–266
 - interfaces, 181
 - passwords, 47–49
 - SSH clients, 312–314
- trusted areas, 4
- types
 - of attacks, 7–9
 - of firewalls, 15–16
 - packet filters, 16–17
 - proxy filters, 17
 - stateful packet filters, 18

U–V

- uauth caches, 127
- UDP (User Datagram Protocol), 18, 70
- unauthorized data retrieval, 8
- unauthorized privileges, 9
- unauthorized system access, 9
- UNIX
 - Boothelper diskettes, 45
 - reconnaissance tools, 319
- unlisted arguments, 140
- Unprivileged Mode, 31
- unstructured threats, 6
- untrusted areas, 4
- upgrading PIX software, 42–44
- user-based authentication, 111. *See also* AAA
- users, adding, 119–122
- UTC (Coordinated Universal Time), 107

- verification, 145
 - CBAC, 265–266
 - IKE, 206–207
 - IOS Authentication Proxy, 280–281
 - IPSec, 220–223
- versions
 - PIX 5.0 and earlier, 44
 - PIX 5.1 and later, 44
 - syslog messages, 109
- viewing
 - AAA configuration, 144–145
 - records, 142
- virtual HTTP, 129–130
- virtual http command, 130
- virtual private network. *See* VPN, 195
- virtual reassembly, FragGuard, 167

- virtual Telnet, 126–127, 129
- virtual telnet command, 127
- viruses, 6
- VPN (virtual private network), 223, 235
 - 3DES, 199
 - CAs, 200
 - DES, 199
 - D-H, 199
 - enabling, 195
 - IPSec, 197–198
 - MD5, 199
 - RSA signatures, 200
 - SA, 198
 - SHA-1, 199
- vulnerability patching, 11

W–X

- waiting states, 181
- web sites, Cisco, 321
- who command, 41
- Windows
 - Group Setup, 136
 - reconnaissance tools, 319
 - SNMP discovery tools, 319
- Windows NT
 - adding authorization rules, 136
 - adding users, 119–122
 - installing, 116–117, 119
 - viewing records, 142
- write erase command, 34
- write floppy command, 34
- write memory command, 34, 178
- write net command, 34
- write standby command, 34, 178
- write terminal command, 34, 103, 108, 201, 206

xlate command, 77