

Symbols

- # (pound sign), 28
- (*G) multicast flows, 110
- /tftpboot directory, 265
- ? (question mark), context-based help, 31

A

- AAA
 - command accounting, configuring, 248–249
 - command authorization, configuring, 245–248
 - AAA servers, user management, 236–242
 - administrative users, 242–249
 - end-user cut-through proxy, 249–263
 - abbreviating
 - commands, 30
 - contiguous 0s on IPv6 addresses, 55
 - absolute uauth timer, 9
 - access control, 281
 - accessing
 - firewall user interface
 - with console connection, 196
 - with PDM/ASDM, 201–205
 - with SSH session, 197–200
 - with Telnet, 196–197
 - PIX 7.x Flash memory partitions, 169–170
 - specific privilege levels, 227
 - accounting
 - local user activity, 235
 - generic users on Cisco firewalls, 227–228
 - ACEs (access control entries)
 - adding to ACLs, 325–328
 - logging activity, 333–334
 - removing from ACLs, 322
 - time range, applying, 323–325
 - ACLs (access control lists)
 - ACEs
 - adding, 325–328
 - removing, 322
 - time range, applying, 323–325
 - applying
 - to lower-security interfaces, 311
 - to outbound direction, 8
 - to signature IDs, 708
 - compiling, 313
 - configuring, 307–309, 320–321
 - descriptions, adding, 322–323
 - downloadable, verifying, 261
 - examples of, 329–332
 - Firewall ACL Bypass, 647, 655
 - logging activity, 533–535
 - manipulating, 321
 - monitoring, 334–335
 - NAT exemption, 299–300
 - object groups, 312
 - defining, 314
 - ICMP type, defining, 315–316
 - protocol object groups, defining, 317–318
 - service object groups, defining, 319–320
 - recompiling, 313
 - removing from running configuration, 322
 - Syslog messages, 683
 - verifying firewall connectivity, 607–609
- activating debug packet sessions, 598–599
- activation keys
 - unlocking firewall features, 38
 - upgrading, 38–39
- active firewall process, checking, 545–548
- active shuns, verifying connectivity, 618–619
- active-active failover, 394–397
 - configuration example, 422–427
 - requirements, 403
- active-standby failover, 394
 - configuration example, 419–422
- ActiveX content, filtering, 340–341
- adding
 - ACEs to ACLs, 325–328
 - descriptions to ACLs, 322–323
 - IDS sensors to CiscoWorks VMS, 715–716
- address spoofing on outside interface, 5–6
- address translation, 281
 - dynamic, 638–639
 - configuring, 639–644
 - example of, 644–645
 - inside source address translation, 630
 - NAT, configuring, 629–630

- policy NAT, 293
- static, 633–634
- static NAT, 289–292
- verifying, 609–613
- xlate table entries
 - clearing, 616–617
 - timeout values, adjusting, 617–618
- addressing, multicast, 106
- adjacency logging (OSPF), disabling, 89
- adjusting
 - fragment cache size, 66
 - interface MTU, 64–65
 - logging buffer size, 677
 - resource limits on security contexts, 161–162
 - terminal screen width, 34
 - xlate table timeout values, 617–618
- admin context, 144, 148–150
- administration of PIX 7.x Flash memory, 171–175
- administrative context, 136
- administrative sessions, monitoring, 207–208
- administrative users, 225
 - managing with AAA servers, 242–249
- alarms
 - on IDS sensors, 694
 - sending to Post Office, 695
- alerts (syslog), 747–749
 - enabling, 705
- allocating resources
 - in multiple-context mode, 160–161
 - to contexts, 160–166
- analyzing firewall logs, 535–538
- application inspection, 365–367
 - configuring, 368–373
 - ARP inspection, 278
 - FTP inspection, 381–382
 - GTP inspection, 385–386
 - HTTP inspection, 376–381
 - ICMP inspection, 373–376
 - MGCP map, 383–384
 - SNMP inspection, 383
 - submitting traffic for, 352–354
- application partition, 266
- applications
 - for optimizing Syslog servers, 511–512
 - logging analysis, 536
- applying
 - ACLs
 - to lower-security interfaces, 311
 - to signature IDs, 708
 - audit policies to interfaces, 710
 - policy maps to interfaces, 350–352, 355–364
 - default policies, 364–365
 - signature updates, 698–699
 - time ranges to ACEs, 323–325
- areas, subnet notation, 90
- ARP (Address Resolution Protocol)
 - cache, clearing, 63
 - configuring, 62–64
 - static ARP entries, configuring, 64
- ARP inspection, configuring, 278
- arrow keys, recalling commands, 32
- ASA (Adaptive Security Algorithm), 4
 - passwords, recovering, 264–265
- ASDM
 - accessing firewall user interface, 201–205
 - image file, copying into Flash memory, 201–202
- assigning
 - IP address to interfaces, 49–53
 - privilege levels
 - to commands, 232–234
 - to users, 229
 - security level to interfaces, 49
 - VLAN number to logical interface, 48
- atomic signatures, 693
- attack signatures, 693
- attributes of trunk links, 44
- audit policies, applying to interfaces, 710
- audit trails, generating, 208
- authentication
 - of generic users on Cisco firewalls, 226–227
 - of local users, 229–231
 - uauth, absolute uauth timer, 9
- authentication proxy
 - configuring, 685–690
 - example, 690–691
- authorization, local user configuration, 232–235
- authorizing
 - firewall command access, 231–235
 - user activity with TACACS+ servers, 253–255
- Auto-RP, 115–116
- availability of embedded IDS sensors on Cisco Firewalls, 694

B

- banners, configuring on user interface, 206–207
- BEQ (best-effort queuing), 67–68
 - configuring, 69–71
 - displaying information, 71
- best practices, firewall configuration, 22–24
- blocked traffic (CBAC), monitoring, 660–661
- boot image setting (PIX 7.x), displaying, 175–176
- bootstrap routers, 115
- bridge mode (CSM), 472
- broadcast traffic, 105
- buffered messages, viewing, 519
- bump in the wire, 269
- bypass links, 76–77

C

- calculating runtime differences on processes, 545–548
- candidate RPs, 115
- capture sessions
 - controlling, 594–595
 - copying buffer contents
 - to TFTP server, 591
 - to web browser, 591–594
 - displaying trunk contents, 590–591
 - example, 595–597
 - monitoring, 588–589
 - verifying packets passing through interfaces, 581–587
- CBAC (Content-Based Access Control), 645–648
 - blocked traffic, monitoring, 660–661
 - configuring, 649–658
 - example of, 658–659
 - Syslog messages, 681–682
 - tearing down connections, monitoring, 659
- changeto command, 160
- changeto system command, 444, 505
- changing message severity levels, 532
- characteristics of context configuration files, 144
- checking system resources, 543
 - failover performance, 561–570
 - firewall CPU load, 543–548
 - firewall interface throughput, 571–580

- firewall memory usage, 548–551
- firewall throughput, 554–560
- inspection engine activity, 560–561
- stateful inspection resources, 552–553
- circular logging buffer, 519
- Cisco firewalls
 - clock management, 503, 669
 - setting clock manually, 504–505, 670–672
 - setting clock with NTP, 505–508, 672–674
 - logging messages, severity levels, 680–681
 - message logging, configuring, 512–529, 677–680
 - sensors, supported signatures, 724–735
 - specifications, 20–21
 - user management
 - accounting local user activity, 235
 - generic users, 226–228
 - with AAA servers, 236–263
 - with local database, 228–235
- Cisco IDS signature ID numbers, 722–724
- CiscoACS servers, configuring command authorization, 245–248
- CiscoWorks VMS
 - IDS sensors, adding, 715–716
 - Network Security Database URL, 725
- class maps, configuring, 345–349
- classifiers, 138
- classifying traffic, 345–349
- clear configure all command, 192
- clear traffic command, 435
- clearing
 - ARP cache, 63
 - internal logging buffer, 531, 680
 - static ARP entries, 277
 - xlate table entries, 616–617
- CLI, initial firewall configuration, 40–41
- clock management, 503, 669
 - setting clock manually, 504–505, 670–672
 - setting clock with NTP, 505–508, 672–674
- collecting Syslog firewall logs, 22
- combining load balancing techniques, 452
- command accounting, configuring, 248–249
- command authorization, configuring, 245–248
- command history, 32
- commands
 - abbreviating, 30
 - active, viewing, 29

- changeto, 160
 - changeto system, 444, 505
 - clear configure all, 192
 - configure terminal, 40–41
 - debug icmp trace, 10–11
 - editing, 30
 - entering, 29
 - failover active, 437
 - failover mac address, 410–411
 - filtering output, 32–33
 - fragment chain, 66
 - igmp join-group, 128
 - ip audit notify, 705
 - ip ips sdf location, 698
 - mode multiple, 147
 - more, 171
 - preempt, 409
 - privilege levels, 226
 - assigning, 232–234
 - regular expressions
 - operators, 33
 - searching, 32–33
 - reload, 445
 - show admin-context, 166–167
 - show arp, 63
 - show blocks, 549
 - show failover, 429–434
 - show flash, 175
 - show fragment, 67
 - show interface, 45
 - show ip audit statistics, 720–721
 - show ip ips signature, 706
 - show ip urlfilter config, 665–666
 - show logging, 529, 677, 714
 - show memory detail, 549
 - show mode, 146
 - show priority-queue statistics, 580
 - show resource allocation, 164
 - show route, 82
 - show service-policy, 354
 - show version, 34–37
 - show xlate, 609–613
 - syntax errors, 31
 - terminal width, 34
 - write standby, 398
- community strings (SNMP), defining, 221–222
 - compiling ACLs, 313
 - compound signatures, 693
 - conditional NAT, 295
 - configuring, 293
 - static NAT translations, 294
 - configuration commands, entering manually, 191
 - configuration examples
 - of active-active failover, 422–427
 - of active-standby failover
 - with FWSM, 421–422
 - with PIX firewalls, 419–421
 - configuration files
 - of contexts, characteristics, 144
 - running configuration
 - copying across failover pair, 189–190
 - displaying, 187
 - erasing, 192
 - saving to Flash memory, 187–188
 - saving to TFTP server, 188–189
 - startup configuration
 - displaying, 186
 - erasing configuration commands, 190
 - managing, 184
 - selecting, 184–186
 - configuration mode, 28–29
 - configure terminal command, 40–41
 - configuring
 - ACLs, 307–309, 320–321
 - application inspection, 368–373
 - ARP inspection, 278
 - FTP inspection, 381–382
 - GTP map, 385–386
 - HTTP inspection, 376–381
 - ICMP inspection, 373–376
 - MGCP map, 383–384
 - SNMP inspection, 383
 - ARP, 62–64
 - authentication proxy, 685–690
 - banners on user interface, 206–207
 - CBAC, 649–658
 - class maps, 345–349
 - command accounting, 248–249
 - command authorization, 245–248
 - content filters, 336–342
 - filtering policies, 338–339
 - contexts, 149–155
 - CSM FWLB, 474–483
 - CSS FWLB, 493–496

- DHCP relay, 103–104
- DHCP server functions, 100–103
- dynamic address translation, 639–644
- embedded sensors, 697, 701–704, 707, 710
- failover, 404–405, 409–411, 416
 - contexts, 416
 - health monitoring policy, 411–412
 - interface failure policy, 413
 - primary unit, 406–408
 - stateful, 413–415
- firewalls, best practices, 22–24
- FragGuard, 65–66
- identity NAT, 297
 - for exclusive outbound use, 298
- IGMP, 125–128
- interfaces, 44–48
 - examples, 53–55
 - IP address assignment, 49–53
 - MTU, 64–65
- IOS firewall
 - as transparent firewall, 625–629
 - for web protocol inspection, 661–662
- IOS FWLB, 453–462
- IPv6, 55–58
 - neighbor advertisements, 59
 - neighbor discovery, 58
 - prefix advertisements, 60–61
- local user authorization, 232–235
- medium-security interfaces, inbound access, 310–311
- message logging, 512–529, 677–680
 - PIX 7.0 logging filters, 513–514
- multiple-context mode, 145–148
 - navigating multiple security contexts, 148–149
- NAT, 629–630
- NAT exemption, 299–300
- OSPF, 88–95
 - example configuration, 98–99
 - on firewall, 85–88
 - prefix lists, 91
 - redistribution, 96–98
- outbound access, 282
- PIM, 116–122
- PIX 7.0 logging filters, 513–514
- policy NAT, 293
- port static translations on IOS firewall, 638
 - priority queuing, 69–71
 - RADIUS user authorization, 256–257
 - RIP on firewall, 83–84
 - shuns, 386–390
 - SMR, 122–124
 - example, 128
 - SNMP, 220–223
 - static NAT entries, 291–292
 - on IOS firewall, 634–636
 - static routes, 80–82
 - translations, 294–295
 - transparent firewall, 272–276
 - interface speed, 273
- conn table, 7
 - entries, 284
 - parameters, 7–8
 - size, checking, 552
- connection limits, setting on matched traffic (policy maps), 355
- connectionless protocols, 9
 - ICMP, stateful inspection, 10–13
 - UDP, 13–15
- connection-oriented protocols, 9
 - TCP, 15–19
- connections
 - embryonic, 16
 - limiting, 288
 - TCP intercept, 18
 - half-closed, 18
 - inbound access, 282
 - xlate lookup, 7
 - outbound access, 281
 - limitations on UDP/TCP, 287
 - shunning, 386–389
 - example, 389–390
 - stateful inspection, 7
 - verifying, 611–616
- connectivity
 - active shuns, verifying, 618–619
 - IPv6, testing, 61–62
 - of failover pairs, 401
 - verifying, 599–607, 620–622
 - with ACLs, 607–609
- console connection, accessing firewall user interface, 196
- console logging, 517
- content filters, 19

- configuring, 336–342
- examples of, 342–343
- filtering policies, configuring, 338–339
- context mode, displaying, 146
- context-based help, 31
- contexts, 136
 - admin contexts, 148
 - allocating firewall resources, 160–166
 - assigning to failover groups, 416
 - configuration files, characteristics, 144
 - configuring, 149–155
 - CPU usage, displaying, 167
 - displaying statistics, 166–167
 - example definition, 155–160
 - inside context interfaces, sharing, 140–142
 - labeling, 150
 - multiple-context mode
 - configuring, 145–148
 - navigating multiple security contexts, 148–149
 - resource allocation, 160–161
 - physical interfaces, mapping to logical interfaces, 153
 - system execution space, features of, 144–145
 - system name, viewing, 151
- controlling
 - capture sessions, 594–595
 - traffic, ACL configuration, 307–309
- copy running-config tftp command, 440
- copying
 - ASDM image into Flash memory, 201–202
 - capture buffer contents
 - to TFTP server, 591
 - to web browser, 591–594
 - files to/from Flash memory, 172
 - PDM image into Flash memory, 201–202
 - running configuration across failover pair, 189–190
- CPU utilization
 - checking, 543–548
 - of contexts, displaying, 167
- crashes
 - forcing, 213
 - information, saving, 212
- crashinfo files
 - deleting, 214–215
 - generating, 213
 - viewing, 214

- creating
 - directories in PIX 7.x Flash memory, 173
 - test crashinfo files, 213
- critical messages (syslog), 750–751
- CSM FWLB, 472–474
 - configuring, 474–483
 - displaying information, 491–493
 - example configuration, 483–491
- CSS (Cisco Content Services Switch), 451
- CSS FWLB
 - configuring, 493–496
 - displaying information, 501
 - example configuration, 496–501
- Ctrl-I command, displaying typed commands, 30

D

- debug icmp trace command, 10–11
- debug packet sessions, enabling, 597–599
- debugging
 - failover activity, 434–437
 - messages (syslog), 781–789
- default behavior of firewalls, 4
- default policies, defining, 364–365
- defining
 - object groups, 314
 - ICMP type, 315–316
 - network object groups, 314
 - protocol object groups, 317–318
 - service object groups, 319–320
 - policies for signatures, 709
 - policy maps, 350–352
 - adjusting TCP options on matched traffic, 356–358
 - assigning matched traffic priority service, 363–364
 - default policies, 364–365
 - policing matched traffic, 360–363
 - sending matched traffic to IPS module, 359
 - setting connection limits on matched traffic, 355
 - security policies in MPF, 343–344
 - server reactivation policies, 237
 - SNMP community string, 221–222

- deleting
 - crashinfo files, 214–215
 - files from Flash memory, 172
 - depletion mode, 237
 - descriptions, adding to ACLs, 322–323
 - detecting firewall failures, 400
 - DHCP (Dynamic Host Configuration Protocol), 19
 - DHCP relay, configuring, 103–104
 - DHCP server functions, 100
 - configuring, 100–103
 - directories
 - creating in PIX 7.x Flash memory, 173
 - removing from Flash memory, 174
 - disabling
 - active commands, 29
 - OSPF adjacency logging, 89
 - screen paging, 34
 - signatures, 707
 - disconnecting from active PDM sessions, 208
 - displaying
 - active PDM/ASDM management application sessions, 208
 - ARP status, 278
 - buffered messages, 519
 - configured contexts, 149
 - context information, 166–167
 - context mode, 146
 - contexts, system name, 151
 - CPU usage for contexts, 167
 - CSM FWLB information, 491–493
 - CSS FWLB information, 501
 - failover statistics, 429–434
 - firewall crash information, 214
 - firewall features, 34
 - firewall license type, 36–37
 - IDS sensor audit statistics, 720–721
 - internal logging buffer, 680
 - IOS FWLB information, 468–471
 - logging buffer size, 677
 - monitoring status of interfaces, 418
 - PIX 7.x boot image setting, 175–176
 - priority queuing information, 71
 - running configuration, 187
 - service policies, 354
 - signature details, 718
 - startup configuration, 186
 - environment variable, 185
 - total IDS activity on Firewall sensors, 721–722
 - trunk contents, 590–591
 - typed commands, Ctrl-I, 30
 - DMZ (demilitarized zone) networks, 309
 - protecting, 22–23
 - DNS Guard, 15
 - DoS attacks, preventing IP address spoofing, 78–80
 - downloadable ACLs
 - enabling on firewall, 260
 - verifying, 261
 - downloading operating system image from monitor prompt, 176–179
 - dynamic address translation, 300, 638–639
 - configuring, 639–644
 - dynamic NAT, 300–307
 - dynamic PAT, 300–307
 - examples of, 644–645
 - dynamic NAT, 300–303
 - examples of, 306–307
 - mapped addresses, configuring, 302–303
 - translation policies, 304–305
 - dynamic PAT, 300–303
 - examples of, 306–307
 - mapped addresses, configuring, 302–303
 - translation policies, 304–305
- ## E
-
- editing commands, 30
 - embedded IDS sensors, 696
 - availability on Cisco Firewalls, 694
 - configuring, 697, 701–704, 707, 710
 - examples, 711–713
 - logging, verifying, 714–715
 - monitoring, 713
 - EMBLEM format (system messages), 511
 - embryonic connections, 16
 - limiting, 288
 - TCP intercept, 18
 - enabling
 - debug packet sessions, 597–599
 - RPF, 78
 - end users, 225
 - end-user cut-through proxy, configuring
 - examples, 262–263
 - on AAA servers, 249–262

entering commands, 29
 environment variables for startup configuration,
 displaying, 185
 erasing
 configuration commands from startup
 configuration, 190
 Flash memory, 174
 PIX 7.x, 175
 running configuration, 192
 error messages (syslog), 751–762
 examining firewall crash information, 212
 examples
 of ACLs, 329–332
 of authentication proxy, 690–691
 of capture session, 595–597
 of CBAC, 658–659
 of content filters, 342–343
 of context definition, 155–160
 of CSM FWLB configuration, 483–491
 of CSS FWLB configuration, 496–501
 of DHCP relay configuration, 104
 of dynamic address translation, 644–645
 of dynamic NAT, 306–307
 of firewall failover configuration
 active-active, 422–427
 active-standby with FWSM, 421–422
 active-standby with PIX firewalls,
 419–421
 of IDS sensors, 711–713
 of interface configuration, 53–55
 of IOS FWLB, 462–468
 of OSPF configuration, 98–99
 of SMR configuration, 128
 of static NAT, 636–638
 exec banners, configuring on user interface, 206–207
 exploits, VLAN hopping, 74
 preventing, 75–76
 extended translation, 631–632

F

failover, 19
 active-active, 396
 configuration example, 422–427
 requirements, 403
 upgrading operating system, 444–446

 active-standby
 configuration example, 419–422
 upgrading operating system, 439–444
 cause of, determining, 567–570
 communication, verifying, 563–567
 configuring, 404–405, 409–411, 416
 contexts, configuring, 416
 debugging, 434–437
 health monitoring policy, configuring, 411–412
 interfaces
 failure policy, configuring, 413
 “testing” mode, 400
 LAN-based, 399
 manually forcing role change, 437
 performance, checking, 561–570
 primary unit, configuring, 406–408
 required licenses, 394
 resetting failed firewall unit, 438
 stateful
 configuring, 413–415
 monitoring, 435–437
 statistics, displaying, 429–434
 toggling roles, 570
 unit roles, verifying, 561–562
 failover active command, 437
 failover cables, 399
 failover groups, 403
 failover hello messages, 412
 failover mac address command, 410–411
 failover pairs
 connectivity, 401
 copying running configuration across, 189–190
 failover poll command, 412
 failover reload-standby command, 438
 features of firewall
 displaying, 34
 unlocking, 38
 fields (system messages), 510–511
 files
 copying to/from Flash memory, 172
 deleting from Flash memory, 172
 renaming in Flash memory, 173
 filtering
 content, 336
 ActiveX, 340–341
 command output, 32–33
 Java applets, 341
 policies, defining, 338–339

fine-tuning logging message generation, 531–532
 Firewall ACL Bypass, 647, 655
 firewall crashes, forcing, 213–214
 firewall farms, 449
 firewall IDS sensors, verifying activity, 721–722
 firewall interface throughput, checking, 571–580
 firewall masks, 328
 firewalls, routed, 625
 first-hop routers, 107
 fixup. *See* application inspection
 Flash memory

- checking system integrity, 174
- copying files to/from, 172
- creating new directories, 173
- deleting files from, 172
- formatting, 174
- FWSM, managing, 169–171
- managing, 167–168
- operating system image
 - downloading from monitor prompt, 176–179
 - identifying, 175–176
 - upgrading, 179–183
- PIX 6.x, managing, 168–169
- PIX 7.x
 - administration, 171–175
 - directories, creating, 173
 - erasing, 175
 - hierarchical structure, 170–171
 - managing, 169–171
 - system integrity, verifying, 174
- removing directories, 174
- renaming files, 173
- running configuration, saving, 187–188

- FO (failover) licenses, 37
- forcing
- firewall crashes, 213–214
- failover role change, 437
- foreign addresses, 6
- formatting Flash memory, 174
- FragGuard, configuring, 65–66
- fragment cache, adjusting size of, 66
- fragment chain command, 66
- fragmentation inspection, 650
- FTP inspection, configuring, 381–382

FWLB (Firewall Load Balancing), 449–450

- CSM FWLB, 472–474
 - configuring, 474–483
 - displaying information, 491–493
 - example configuration, 483–491
- CSS FWLB
 - configuring, 493–496
 - displaying information, 501
 - example configuration, 496–501
- IOS FWLB, 452–453
 - configuring, 453–462
 - displaying information, 468–471
 - example, 462–468
 - methods of, 451

- FWSMs (Firewall Services Module), 505
- failover pairs, 398
- Flash memory management, 169–171
- passwords, recovering, 265

G

gb-ethernet interfaces, 34
 General Queries (IGMPv2), 109
 generating

- audit trails, 208
- test crashinfo files, 213

- generic users
- accounting, 227–228
- authentication, 226–227
- managing on Cisco firewalls, 226
- global addresses, 6, 56, 630
- global configuration mode, 28–29
- GMT (Greenwich Mean Time), 503, 669
- Group-Specific Queries (IGMPv2), 109
- GTP (GPRS Tunneling Protocol), 385
- GTP map, configuring, 385–386

H

half-closed connections, 18
 hardware load balancing, CSM FWLB, 472–474

- configuring, 474–483
- displaying information, 491–493
- example configuration, 483–491

- heartbeat messages, 702

help system, context-based help, 31
 history of failover state changes, displaying, 434
 hitless upgrade, 399, 439

HTTP

port cloaking, 378–379
 transfer encoding types, 380

HTTP inspection engine

configuring, 376–381
 on IOS firewall, 661
 content filtering
 configuring, 336–342
 examples of, 342–343

ICMP (Internet Control Message Protocol), 401

ACLs operation, 8
 message types, 738–740
 object groups, defining, 315–316
 restricting traffic, 23
 stateful inspection, 10–11
 case study, 12–13

ICMP inspection, configuring, 373–376

identifying operating system image in Flash
 memory, 175–176

identity NAT, configuring, 297

for exclusive outbound use, 298

idle uauth timer, 9

IDSs

sensors, 696
 adding to CiscoWorks VMS, 715–716
 alarms, 694–695
 displaying audit statistics, 720–721
 embedded, 697, 701–713
 signatures, 693
 definitions, locating, 697

IEEE 802.1Q trunks, attributes, 44

IGMP (Internet Group Message Protocol), 108

configuring, 125–128
 SMR, configuring, 122–124
 verifying operation, 129

igmp join-group command, 128

IGMP proxy agent, 105

inactivity timer, 253

inbound access, 282

configuring on medium-security interfaces,
 310–311

inbound connections, 4

xlate lookup, 7

info signatures, 693

informational messages (syslog), 773–781

initial firewall configuration, 40–41

initiating

firewall reload, 209–210
 after specific time interval, 210–211
 multiple context mode, 147–148

inside context interfaces, sharing, 140–142

inside interfaces, 2–3

inside NAT, 630

interfaces, 643

inside source address translation, 630

inspection engines, 9. *See also*

application inspection

activity, checking, 560–561
 HTTP, transfer encoding types, 380
 ICMP stateful inspection, 10–11
 case study, 12–13
 TCP stateful inspection, 15–18
 TCP normalization, 18–19
 UDP stateful inspection, 13–15

installing signature update files, 699

interface polltime, 412

interface priority queues, 67–68

interfaces

audit policies, applying, 710
 configuring, 44–48
 connectivity
 checking ARP cache, 602–604
 checking routing table, 604
 testing with ping packets, 600–602
 verifying, 599, 620–622
 verifying with ACLs, 607–609
 verifying with traceroute, 604–607

example configurations, 53–55

gb-ethernet, 34

hardware ID names, 45

inbound access, 282

inside context interfaces, sharing, 140–142

IP address, assigning, 49, 52–53

IPv6 addresses, configuring, 55

line protocol state, 45

- logical VLAN number, assigning, 48
 - lower-security, applying ACLs, 311
 - medium-security, 309
 - inbound access, 310–311
 - monitoring status, displaying, 418
 - MTU, configuring, 64–65
 - outbound access, 281
 - physical, mapping to contexts, 137–139
 - policy maps, applying, 350–352, 355–365
 - same-security access, 282–283
 - security level, assigning, 49
 - testing mode, 400
 - verifying packets passing through via
 - capture sessions, 581–591
 - internal clock
 - setting manually, 504–505, 670–672
 - setting with NTP, 505–508, 672–674
 - internal logging buffer, clearing, 531, 680
 - IOS firewalls
 - CBAC inspection, 646–648
 - configuring, 649–658
 - transparent firewall configuration, 625–629
 - URL filtering
 - generating logging messages, 663
 - tuning, 664
 - IOS FWLB (Firewall Load Balancing), 452–453
 - configuring, 453–462
 - displaying information, 468–471
 - example, 462–468
 - IOS IPS
 - signature definitions, locating, 697
 - signature updates, 698–699
 - IP addresses
 - assigning to interfaces, 49–53
 - spoofing, preventing, 78–80
 - ip audit notify command, 705
 - ip ips sdf location command, 698
 - IP multicast, 106
 - addressing, 106
 - IGMP, 108
 - configuring, 125–128
 - verifying operation, 129
 - multicast trees, 107
 - PIM, 109
 - configuring, 116–122
 - Sparse Mode, 110–114
 - verifying operation, 130–133
 - Version 1, 115
 - PIM-SM, RP designation, 115–116
 - RPF, 108
 - SMR
 - configuring, 122–124
 - example configuration, 128
 - IP port numbers, 740–741
 - corresponding Cisco firewall keywords, 741–743
 - IPv6
 - configuring, 55–58
 - connectivity, testing, 61–62
 - neighbor advertisements, configuring, 59
 - neighbor discovery, configuring, 58
 - prefix advertisements, configuring, 60–61
 - ISNs (initial sequence numbers), 8, 289
- ## J-K-L
-
- Java applets, filtering, 341
 - labeling contexts, 150
 - LAN-based failover, 399–401
 - last-hop routers, 107
 - Leave Group messages (IGMPv2), 109
 - length of terminal screen, adjusting, 34
 - licenses
 - activation keys, 38
 - upgrading, 38–39
 - listing, 36–37
 - required for failover, 394
 - limitations on outbound UDP/TCP connections, 287
 - limiting
 - embryonic connections, 288
 - resources allocated to contexts, 161–164
 - TCP MSS size, 65
 - line protocol state (interfaces), 45
 - link-local addresses, 55
 - links, bypass links, 76–77
 - LLQ (low-latency queueing), 67–68
 - configuring, 69–71
 - displaying information, 71
 - load balancing
 - CSM FWLB, 472–474

- configuring, 474–483
 - displaying information, 491–493
 - example configuration, 483–491
- FWLB, 450–451
- IOS FWLB, 452–453
 - configuring, 453–462
 - displaying information, 468–471
 - example, 462–468
- local addresses, 6, 630
- local database, user management, 228–229
 - accounting local user activity, 235
 - firewall command access, authorizing, 231–235
 - local user authentication, 229–231
- local user authorization, configuring, 232–235
- locating signature definitions, 697
- logging
 - ACE activity, 333–334
 - ACL activity, 533–535
 - buffer size, adjusting, 677
 - messages, 508, 674
 - ACL-related Syslog messages, 683
 - analyzing firewall logs, 535–538
 - CBAC-related Syslog messages, 681–682
 - clearing internal logging buffer, 531
 - configuring, 512–529, 677–680
 - destinations, verifying, 529–530
 - manually testing message generation, 530–531
 - PIX 7.0 logging filters, configuring, 513–514
 - pruning messages, 531–532
 - severity levels, setting, 509, 532, 675, 680–681
 - time stamp synchronization, 509
 - URL filtering Syslog messages, 683–684
- logical interfaces, 35
 - mapping to physical interfaces, 153
 - subinterface number, 47
 - VLAN number, assigning, 48
- login banner, configuring on user interface, 206–207
- lookups (xlate table), 7
- lower-security interfaces, applying ACLs, 311

M

- maintenance partition, 266
- managing
 - Flash memory, 167–168
 - FWSM, 169–171
 - PIX 6.x, 168–169
 - PIX 7.x, 169–171
 - startup configuration, 184
- manipulating ACLs, 321
- manually forcing failover role change, 437
- manually resetting failed firewall units, 438
- manually setting internal clock, 504–505, 670–672
- manually testing logging message generation, 530–531
- mapping
 - physical interfaces to contexts, 137–139
 - physical interfaces to logical interfaces, 153
- mapping agents, 115
- medium-security interfaces, 309
 - inbound access, configuring, 310–311
- Membership Report messages, 108
- memory
 - Flash
 - checking system integrity, 174
 - copying files to/from, 172
 - deleting files from, 172
 - downloading operating system image, 176–179
 - creating directories in, 173
 - formatting, 174
 - identifying operating system image, 175–176
 - managing, 167–171
 - removing directories from, 174
 - renaming files in, 173
 - upgrading operating system image, 179–183
 - usage, checking, 548–551
- merging startup and running configuration commands, 191–195
- messages
 - heartbeat, 702
 - ICMP, 738–740
 - IGMP Membership Report, 108

- logging, 508, 674, 680–681
 - ACL-related Syslog messages, 683
 - analyzing firewall logs, 535–538
 - CBAC-related Syslog messages, 681–682
 - destinations, verifying, 529–530
 - logging ACL activity, 533–535
 - manually testing, 530–531
 - pruning messages, 531–532
 - severity levels, setting, 509, 532, 675
 - time stamp synchronization, 509
 - URL filtering Syslog messages, 683–684
 - syslog
 - severity level 1 alerts, 747–749
 - severity level 2 critical messages, 750–751
 - severity level 3 error messages, 751–762
 - severity level 4 warning messages, 762–767
 - severity level 5 notifications, 767–772
 - severity level 6 informational messages, 773–781
 - severity level 7 debugging messages, 781–789
 - system messages, format, 510–511
 - MGCP map, configuring, 383–384
 - MIBs, 216, 219
 - monitoring firewall activity, 215
 - objects, 218
 - mode multiple command, 147
 - modifying message severity levels, 532
 - monitor screen dimensions, changing, 34
 - monitoring
 - ACLs, 334–335
 - active shun activity, 388
 - address translations, 609–613
 - administrative sessions, 207–208
 - capture sessions, 588–589
 - CBAC operation, 659
 - blocked traffic, 660–661
 - connections, 611–616
 - embedded IDS sensors, 713
 - firewall activity with SNMP, 215
 - traps, 219
 - firewall configuration changes, 622–623
 - stateful failover, 435–437
 - URL filtering, 665–666
 - xlate entries based on local address, 610
 - more command, 171
 - MOTD banners, configuring on user interface, 206–207
 - MPF (Modular Policy Framework), defining security policies, 343–344
 - MSS (maximum segment size), configuring, 65
 - MTU (maximum transmission unit), interface configuration, 64–65
 - multicast, 105
 - IGMP
 - configuring, 125–128
 - verifying operation, 129
 - PIM, 109, 115
 - configuring, 116–122
 - verifying operation, 130–133
 - PIM-SM, 110–114
 - RP designation, 115–116
 - routing
 - IGMP, 108
 - multicast trees, 107
 - RPF, 108
 - SMR
 - configuring, 122–124
 - example configuration, 128
 - multicast addressing, 106
 - OUI values, 106
 - multicast groups, 106
 - multicast trees, 107
 - multiple-context mode, 136
 - classifiers, 138
 - configuring, 145–148
 - initiating, 147–148
 - navigating multiple security contexts, 148–149
 - resource allocation, 160–161
-
- ## N
-
- naming format for downloadable ACLs, 261
 - NAT (Network Address Translation)
 - configuring, 629–630
 - dynamic address translations, 638–639
 - configuring, 639–644
 - example of, 644–645
 - extended translation entries, 631–632
 - identity NAT, configuring, 297
 - inside interfaces, 643

- inside NAT, 630
- outside interfaces, 643
- outside NAT, 630
- port static translations, configuring on IOS
 - firewall, 638
- simple translation entries, 631–632
- static address translation, 633–634
- static NAT
 - configuring on IOS firewall, 634–636
 - example of, 636–638
- NAT exemption, configuring, 299–300
- navigating multiple security contexts, 148–149
- neighbor advertisements, IPv6 configuration, 59
- neighbor discovery, IPv6 configuration, 58
- network object groups, defining, 314
- Network Security Database, URL, 725
- notifications (syslog), 767–772
- NTP, setting internal clock, 505–508, 672–674

O

- object groups, 312–313
 - ICMP type, defining, 315–316
 - network object groups, defining, 314
 - protocol object groups, defining, 317–318
 - service object groups, defining, 319–320
- operating system
 - downloading image from monitor
 - prompt, 176–179
 - identifying image in Flash memory, 175–176
 - image, upgrading, 179–183
 - of active-active failover pair, upgrading, 444–446
 - of active-standby failover pair, upgrading, 439–444
- optimizing Syslog servers, 511–512, 676
- options (commands), entering, 29
- OSPF (Open Shortest Path First)
 - areas, subnet notation, 90
 - configuring, 88–95
 - example configuration, 98–99
 - on both sides of firewall, 88
 - on firewall, 85–88
 - prefix lists, configuring, 91
 - redistribution, configuring, 96–98

- OUI (Organizationally Unique Identifier)
 - values, 106
- outbound access, 281–282
- outbound connections, 4
 - UDP/TCP limitations, 287
 - xlate lookup, 7
- output interface queues, 67–68
- outside interfaces, 2–3
 - address spoofing, 5–6
- outside NAT, 630
 - interfaces, 643

P

- packet classifiers, 138
- packets
 - capturing, 19
 - fragments, handling, 65–66
 - ICMP, stateful inspection of, 10–13
 - IPv4, Protocol field, 737–738
 - TCP, stateful inspection of, 15–19
 - UDP, stateful inspection of, 13–15
- parameters
 - of conn table entries, 7–8
 - of xlate table entries, 6
- partitions on PIX 7.x Flash memory,
 - accessing, 169–170
- passwords, recovering
 - ASA, 264–265
 - FWSM, 265
 - PIX, 264–265
- PDM
 - accessing firewall user interface, 201–205
 - firewall throughput, checking, 554
 - image file, copying into Flash memory, 201–202
- perfmon counters, checking firewall
 - throughput, 558–560
- PFSS (Cisco PIX Firewall Syslog Server), 676
- physical interfaces
 - mapping to contexts, 137–139
 - mapping to logical interfaces, 153
- PIM (Protocol Independent Multicast), 109
 - configuring, 116–122
 - shared trees, 112

- verifying operation, 130–133
 - Version 1, 115
- PIM-SM (PIM Sparse Mode), 110–114
 - RP designation, 115–116
- PIX 6.x, Flash memory management, 168–169
- PIX 7.x
 - boot image setting, displaying, 175–176
 - Flash memory
 - administration, 171–175
 - erasing, 175
 - managing, 169–171
 - partitions, accessing, 169–170
 - system integrity, verifying, 174
 - logging filters, 513–514
- policies, defining for signatures, 709
- policy maps
 - default policies, defining, 364–365
 - defining, 350–352
 - matched packets
 - adjusting TCP options, 356–358
 - assigning priority service, 363–364
 - policing, 360–363
 - sending to IPS module, 359
 - setting connection limits, 355
- policy NAT, 295
 - configuring, 293
- port cloaking, 378–379
- port numbers, 740–741
 - corresponding Cisco firewall keywords, 741–743
- port static translations, configuring on IOS
 - firewall, 638
- Post Office
 - changing attributes of routers, 701
 - sending IDS sensor alarms, 695
- preempt command, 409
- prefix advertisements, configuring IPv6, 60–61
- preventing
 - IP address spoofing, 78–80
 - VLAN hopping, 75–76
- primary failover unit, configuring, 406–408
- priority queuing
 - configuring, 69–71
 - displaying information, 71
- privilege levels
 - accessing, 227

- assigning
 - to commands, 232–234
 - to users, 229
 - privileged EXEC mode, 28
 - processes, calculating runtime differences, 545–548
 - protecting DMZ, 22–23
 - Protocol field, 737
 - corresponding Cisco firewall keywords, 738
 - protocol object groups, defining, 317–318
 - pruning messages, 531–532

Q-R

- queuing
 - priority queuing
 - configuring, 69–71
 - displaying information, 71
 - transmit ring, 70
- R (restricted) licenses, 37
- RADIUS, configuring user authorization, 256–257
- recalling commands, 32
- recompiling ACLs, 313
- recovering passwords
 - ASA, 264–265
 - FWSM, 265
 - PIX, 264–265
- redistribution, OSPF configuration, 96–98
- regular expressions
 - operators, 33
 - performing searches on, 32–33
- reload command, 445
- reloading firewalls, 209–210
 - after specific time interval, 210–211
- remark ACEs, adding to ACLs, 322–323
- removing
 - ACEs from ACLs, 322
 - ACLs from running configuration, 322
 - active shuns, 388
 - directories in Flash memory, 174
 - static routes, 81
- renaming files in Flash memory, 173
- requirements for active-active failover, 403
- resetting
 - failed firewall unit, 438
 - level 0 passwords, 227
- resources, allocating to contexts, 160–166

- restricting ICMP traffic, 23
- RFC 2827, 5
- RFC Sourcebook, 737
- RIP (Routing Information Protocol),
 - configuring on firewall, 83–84
- route lookups, 452
- routed firewall mode, 280
- routed firewalls, 625
- router IDS sensors, supported signatures,
 - 724–735
- router mode (CSM), 472
- routing
 - IP multicast, 108
 - multicast, 107
- routing tables, checking connectivity, 604
- RP (Rendezvous Point), 110
- RPF, 108
 - enabling, 78
 - preventing IP address spoofing, 78–80
- running configuration, 399
 - ACLs, removing, 322
 - configuration commands, entering
 - manually, 191
 - copying across failover pair, 189–190
 - displaying, 187
 - erasing, 192
 - merging configuration commands with startup configuration, 191–195
 - saving
 - to Flash memory, 187–188
 - to TFTP server, 188–189
- runtime differences, calculating on processes,
 - 545–548

S

- SDM (Security Device Manager), 699
 - searching for regular expressions, 32–33
- security contexts, 136
- security levels, assigning to interfaces, 49
- security policies, defining in MPF, 343–344
- “security wheel”, 24
- selecting startup configuration, 184–186
- sending Syslog messages with TCP, 524
- sensors, 696
 - adding to CiscoWorks VMS, 715–716
 - Cisco Firewall, supported signatures, 724–735
 - displaying audit statistics, 720–721
 - displaying total IDS activity, 721–722
 - embedded
 - configuring, 697, 701–704, 707, 710
 - examples of, 711–713
 - monitoring, 713
 - router IDS, supported signatures, 724–735
- server reactivation policies, defining, 237
- service contact port, 741
- service object groups, defining, 319–320
- service policies, displaying, 354
- setting system clock
 - manually, 504–505, 670–672
 - with NTP, 505–508, 672–674
- severity levels, 508, 674, 680–681
 - changing, 532
 - setting for message logging, 509, 675
 - severity level 1 alerts, 747–749
 - severity level 2 critical messages, 750–751
 - severity level 3 error messages, 751–762
 - severity level 4 warning messages, 762–767
 - severity level 5 notifications, 767–772
 - severity level 6 informational messages,
 - 773–781
 - severity level 7 debugging messages, 781–789
- shared trees, 110
 - PIM shared trees, 112
- sharing inside context interfaces, 140–142
- show admin-context command, 166–167
- show arp command, 63
- show blocks command, 437, 549
- show failover command, 429–434, 439
- show flash command, 175
- show fragment command, 67
- show interface command, 45, 436
- show ip audit statistics command, 720–721

- show ip ips signature command, 706
- show ip urlfilter config command, 665–666
- show logging command, 529, 677, 714
- show memory detail command, 549
- show mode command, 146
- show priority-queue statistics command, 580
- show resource allocation command, 164
- show route command, 82
- show service-policy command, 354
- show traffic command, 435–436
- show version command, 34–37
- show xlate command, 609–613
- shuns, 386–389
 - example of, 389–390
 - removing from firewall, 388
 - verifying connectivity, 618–619
- signatures, 693
 - definitions, locating, 697
 - details, displaying, 718
 - disabling, 707
 - for Cisco Firewall sensors, 724–735
 - for router IDS sensors, 724–735
 - policies, defining, 709
 - signature ID numbers, 722–724
 - updates, applying, 698–699
- simple translation, 631
- simple translation entries, 632
- SIMS (Security Information Management Solution), 696
- single-context mode, 136
- site-local addresses, 55
- SMR (stub multicast router), 107
 - example configuration, 128
- SNMP (Simple Network Management Protocol)
 - configuring, 220–223
 - MIBs, 218–219
 - monitoring firewall activity, 215
 - traps, 219–220
- SNMP inspection, configuring, 383
- software load balancing, IOS FWLB, 452–453
 - configuring, 453–462
 - displaying information, 468–471
 - example, 462–468
- source address spoofing, 5
- Sparse Mode (PIM), 110
- specifications of Cisco firewalls, 20–21
- spoofed IP addresses, preventing, 78–80
- SPT (shortest path tree), 114
- SPT switchover, 114
- SSH (Secure Shell), accessing firewall user interface, 197–200
- startup configuration, 399
 - configuration commands, merging with running configuration commands, 191–195
 - displaying, 186
 - environment variable, displaying, 185
 - erasing configuration commands from, 190
 - managing, 184
 - selecting, 184–186
- stateful failover, 401
 - configuring, 413–415
 - monitoring, 435–437
- stateful inspection, 7–9
 - CBAC, 645–648
 - configuring, 649–658
 - example of, 658–659
 - monitoring blocked traffic, 660–661
 - monitoring connection tear down, 659
 - of ICMP, 10–11
 - case study, 12–13
 - of TCP, 15–18
 - TCP normalization, 18–19
 - of UDP, 13–15
 - packet classifiers, 138
 - resources, checking, 552–553
- stateless backup, 453
- stateless failover, 401
- static address translation, 633–634
- static ARP entries
 - clearing, 277
 - configuring, 64
- static NAT, 289–291
 - configuring on IOS firewall, 634–636
 - entries, configuring, 291–292
 - example of, 636–638
- static routes
 - configuring, 80–82
 - removing, 81
- sticky connections, 454
- stratum, 503, 669
- structure of Flash memory hierarchy
 - PIX 6.x, 169
 - PIX 7.x, 170–171
- stub routers, 105

subinterface number, 47
 submitting traffic for application inspection,
 352–354
 supported translation types, 284–285
 synchronizing time stamps on logging
 messages, 509
 syntax errors, 31
 Syslog, 19
 ACL-related messages, 683
 alerts, enabling, 705
 CBAC-related messages, 681–682
 firewall logs, collecting, 22
 firewall throughput, checking, 555
 messages
 recent messages, viewing, 542–543
 sending with TCP, 524
 severity level 1 alerts, 747–749
 severity level 2 critical messages, 750–751
 severity level 3 error messages, 751–762
 severity level 4 warning messages,
 762–767
 severity level 5 notifications, 767–772
 severity level 6 informational messages,
 773–781
 severity level 7 debugging messages,
 781–789
 PFSS, 676
 servers, optimizing, 511–512, 676
 URL filtering messages, 683–684
 verifying logging on embedded IDS sensors,
 714–715
 system execution space, 136, 144
 features, 144–145
 system messages, 510
 EMBLEM format, 511
 system name (contexts), displaying, 151
 system resources, checking, 543
 failover performance, 561–570
 firewall CPU load, 543–548
 firewall interface throughput, 571–580
 firewall memory usage, 548–551
 firewall throughput, 554–560
 inspection engine activity, 560–561
 stateful inspection resources, 552–553

T

TACACS+ servers
 authorizing user activity, 253–255
 enable authentication support, 243
 TCP
 connections
 embryonic connections, limiting, 288
 half-closed connections, 18
 monitoring, 611–616
 ISNs, 289
 MSS, configuring, 65
 options, setting on matched traffic (policy
 maps), 356–358
 sending Syslog messages, 524
 stateful inspection, 15–18
 TCP normalization, 18–19
 TCP intercept, 18
 TCP normalization, 18
 tearing down connections (CBAC), monitoring, 659
 Telnet, accessing firewall user interface, 196–197
 terminal screen width, adjusting, 34
 terminal width command, 34
 termination of TCP connections, 17
 test crashinfo files, generating, 213
 testing
 connectivity
 of IPv6, 61–62
 with ARP cache, 602–604
 with ping packets, 600–602
 logging message generation, 530–531
 “testing mode”, 400
 TFTP server, saving running configuration to,
 188–189
 three-way handshakes, 15
 throughput, checking, 554–560
 time stamps, synchronizing on logging
 messages, 509
 timed reactivation, 237
 timers
 CPU utilization, 545
 idle uauth timer, 9
 toggling failover roles, 570
 topologies, 72–73
 bypass links, 76–77
 traceroute, verifying firewall connectivity, 604–607

- traffic
 - classifying, 345–349
 - controlling with ACLs, 307–309
 - shunning, 386–389
 - example, 389–390
 - submitting for application inspection, 352–354
 - traffic counters, checking firewall throughput, 555–558
 - traffic policers, 360–64
 - transfer encoding types (HTTP), 380
 - translations
 - conditional, 294
 - configuring, 294–295
 - policies, 304–305
 - policy NAT, 293
 - static NAT, 289–291
 - entries, configuring, 291–292
 - xlate table
 - entries, clearing, 616–617
 - size, checking, 552
 - timeout values, adjusting, 617–618
 - transmit ring, 70
 - transparent firewalls
 - configuring, 272–276
 - on IOS firewall, 625–629
 - interface speed, configuring, 273
 - traps (SNMP), 219–220
 - triggering a firewall reload, 209–210
 - after specific time interval, 210–211
 - trunk links, attributes, 44
 - trunks, displaying contents, 590–591
 - tuning
 - OSPF, 93–94
 - URL filtering on IOS firewall, 664
 - TurboACLs, 313
- U**
-
- uauth
 - absolute uauth timer, 9
 - verifying firewall connectivity, 620–622
 - UDP
 - connections, monitoring, 611–616
 - stateful inspection, 13–15
 - unicast traffic, 105
 - unlocking firewall features, 38
 - upgrading
 - active-active failover pair, 444–446
 - active-standby failover pair, 439–444
 - licenses, 38
 - activation keys, 38–39
 - operating system image, 179–183
 - uploading signature update files, 699
 - UR (unrestricted) licenses, 36
 - URL filtering
 - configuring on IOS firewall, 662
 - generating logging messages, 663
 - monitoring, 665–666
 - Syslog messages, 683–684
 - tuning on IOS firewall, 664
 - URLs
 - Network Security Database, 725
 - RFC Sourcebook, 737
 - user activity, generating audit trails, 208
 - user authentication. *See* uauth
 - user contexts, 136
 - user EXEC mode, 28
 - user interface
 - accessing
 - with console connection, 196
 - with SSH, 197–200
 - with Telnet, 196–197
 - administrative sessions, monitoring, 207–208
 - command history, 32
 - commands
 - abbreviating, 30
 - editing, 30
 - entering, 29
 - configuration mode, 28–29
 - context-based help, 31
 - privileged EXEC mode, 28
 - regular expressions
 - operators, 33
 - searching for, 32–33
 - user EXEC mode, 28
 - user management
 - generic users, 226
 - accounting, 227–228
 - authentication, 226–227
 - of Cisco firewalls, configuring authentication
 - proxy, 684–690
 - with AAA servers, 236–242

- administrative users, 242–249
- end-user cut-through proxy, 249–263
- with local database, 228–229
 - accounting local user activity, 235
 - firewall command access, authorizing, 231–235
 - local user authentication, 229–231

- signature details, 718
- startup configuration, 186
- Syslog information, 542–543
- VLAN hopping, 73–74
 - preventing, 75–76
- VLAN number, assigning to logical interface, 48
- VLANs, logical interfaces, 47
- VPN users, 225

V

verifying

- address translation, 609–613
 - based on local addresses, 610
 - connections, 611–616
 - downloadable ACLs, 261
 - failover communication, 563–567
 - failover roles, 561–562
 - firewall connectivity, 599
 - ACLs, 607–609
 - checking ARP cache, 602–604
 - checking routing table, 604
 - checking Uauth, 620–622
 - testing with ping packets, 600–602
 - with traceroute, 604–607
 - IGMP multicast operation, 129
 - message logging activity, 529–530
 - packets passing through interfaces via capture sessions, 581–591
 - PIM multicast routing, 130–133
 - PIX 7.x Flash memory system integrity, 174
 - Sylog server operation, 714–715
- ### viewing
- active commands, 29
 - buffered messages, 519
 - configured contexts, 149
 - context information, 166–167
 - context mode, 146
 - failover statistics, 429–434
 - firewall crash information, 214
 - firewall license type, 36–37
 - list of firewall features, 34
 - PIX 7.x boot image setting, 175–176
 - priority queuing information, 71
 - running configuration, 187
 - service policies, 354

W

- warning messages (syslog), 762–767
- web protocol inspection, configuring on IOS
 - firewall, 661–662
- weighted least connections algorithm, 479
- weighted round robin algorithm, 479
- well-known port numbers, service contact port, 741
- write standby command, 398

X-Y-Z

- xlate table, 6
 - entries, 283
 - clearing, 616–617
 - parameters, 6
 - lookups, 7
 - size, checking, 552
 - timeout values, adjusting, 617–618
- xlates
 - locating based on local addresses, 610
 - verifying, 609–613
- zero downtime upgrade, 399