INDEX

Symbols & Numerics

 # (pound sign), 29
(*,G) multicast flows, 131
? (question mark), context-based help, 31
4GE (4-port Gigabit Ethernet) SSM, 725

A

AAA, configuring
command accounting, 286–287
command authorization, 283–285
AAA servers, user management, 272–280
administrative users, 280–287
end-user cut-through proxy, 287–301
abbreviating
commands, 30
contiguous 0s on IPv6 addresses, 61
ABRs (Area Border Routers), 101
absolute uauth timer, 9
access control, 323
accessing
ASA Flash memory partitions, 194–195
firewall user interface
with console connection, 232–233
with PDM/ASDM, 238–242
with SSH session, 235, 237
with Telnet, 234
FWSM on Catalyst 6500 switch, 28
specific privilege levels, 263
accounting
local user activity, 272
of generic users on Cisco firewalls, 263–264
ACEs (access control entries)
adding to ACLs, 353–355
logging activity, 379–380
removing from ACLs, 358–359
time range, applying, 360–362
time-based, 356
ACLs (access control lists)
ACEs
adding, 353
logging activity, 379–380
removing, 358–359
time range, applying, 360–362
time-based, 356
applying
to lower-security interfaces, 351
to outbound direction, 8
compiling, 352
configuring, 348–349, 353
descriptions, adding, 359–360
downloadable, verifying, 299
examples of, 362–363
extended, 356–357
hit counters, resetting, 382
hit counts, displaying, 707–708
logging activity, 617–619
manipulating, 357–358
monitoring, 380–382
object groups, 352
applying, 373–379
defining, 363–373
enhanced service object groups, defining, 370–373
ICMP type, defining, 367–369
network object groups, defining, 364–365
protocol object groups, defining, 365–367
service object groups, defining, 369–370
recompiling, 353
renaming, 359
verifying firewall connectivity, 705–707
wildcards, specifying, 355
activating debug packet sessions, 690–691
activation keys
unlocking firewall features, 39
upgrading, 40–41
active firewall process, checking, 629–632
active shuns, verifying connectivity, 718–720
active-active failover pair, 474–477
configuration example, 501–508
requirements, 482–484
active-standby failover pair, 474–475
configuration example, 498–501
manually upgrading, 520–524
AD (Anomaly Detection) policies, configuring on AIP SSM, 778–780
adding
ACEs to ACLs, 354–355
descriptions to ACLs, 359–360

address spoofing on outside interface, 5–6
address translation, 323
conn entries, 326
connection limits, configuring, 328–330
dynamic NAT, configuring, 341–346
dynamic PAT, configuring, 342–346
embryonic connections, limiting, 330–331
identity NAT, configuring, 338–340
inbound access, defining, 324
NAT exemption, 327
configuring, 340–341
outbound access, defining, 323–324
outside NAT, 328
PAT, 326
policy NAT, configuring, 335–338
same-security access, 324–325
static NAT, 326, 331–334
types of supported on Cisco firewalls, 326–327
verifying, 709–714
xlate entries, 325
xlate table entries
clearing, 717
table timeout values, adjusting, 717–718
addressing, multicast, 127
adjacency logging (OSPF), disabling, 106
adjusting
fragment cache size, 72
interface MTU, 70–71
resource limits to security contexts, 186
terminal screen width, 34
xlate table timeout values, 717–718
admin context, 169, 173–175
administration of ASA Flash memory, 196–200
administrative context, 158
administrative distance, 83–84
administrative sessions, monitoring, 244–245
administrative users, 261
managing with AAA servers, 280–287
administratively scoped addresses, 127, 142
advertising default routes, 96
AIP (Advanced Inspection and Prevention) SSM, 725
configuring, 769–772
IPS policies, configuring, 777–780
IPS sensors, configuring, 780–781
IPS virtual sensors, configuring, 781–785
license, updating, 773–774
managing, 773
signature database file, updating, 774–776
alerts (syslog), 799-802
alias keyword, 319
allocating
firewall resources to contexts, 185–191
resources in multiple-context mode, 185–186
analyzing firewall logs, 619–623
application inspection, 423, 426
configuring, 426–432
DCERPC inspection, configuring, 437–438
DNS inspection, configuring, 438–440
ESMTP inspection, configuring, 441–443
FTP inspection, configuring, 443–446
GTP inspection, configuring, 446–448
H.323 inspection, configuring, 449–451
HTTP inspection, configuring, 452–460
ICMP inspection, configuring, 460–462
IM inspection, configuring, 462, 464
IPSec Passthru inspection, configuring, 465
matching text with regular expressions, 433–437
MGCP inspection, configuring, 465, 467
MGCP map, configuring, 467
NetBIOS inspection, configuring, 468
RADIUS accounting inspection, configuring, 468–469
SNMP accounting inspection, configuring, 470–471
application partition passwords, resetting, 308
applications
for optimizing Syslog servers, 590–591
logging analysis, 620
applying
ACLs to lower-security interfaces, 351
object groups to access lists, 373–379
policy maps to interface, 406–420
default policies, 421–423
time ranges to ACEs, 360–362
area 0, 107
areas (OSPF), subnet notation, 107
ARP (Address Resolution Protocol)
configuring, 68–69
static entries, clearing, 319
ARP cache, clearing, 69
arp command, alias keyword, 319
ARP inspection, 314
configuring, 320

arp timeout command, 699
arrow keys, recalling commands, 32
ASA (Adaptive Security Algorithm), 4
ASA (Adaptive Security Appliance)
4GE SSM, 725
AIP SSM, 725, 769–780
classifiers, 166
configuring as Auto Update Server, 228–232
CSC SSM, 725
automatic updates, configuring, 741–743
configuring, 729–738
connecting to management interface, 740–741
inspection policy configuration, 744–769
repairing initial configuration, 738–740
failover pair capabilities, 39
Flash memory
administration, 194–200
partitions, accessing, 194–195
MAC address allocation, 165
Packet Tracer feature, verifying firewall connectivity, 692–694
Passwords, recovering, 302–305
SSM modules, initial configuration, 726–729
traceroute, performing, 703–705
ASA 7.2, WCCPv2, 396–397
ASA 7.3, configuring redundant interfaces, 48–49
ASA 8.0, configuring EIGRP, 97–101
ASBRs (Autonomous System Boundary Routers), 101
ASDM (Adaptive Security Device Manager)
accessing firewall user interface, 238–242
ACL hit counts, displaying, 707–708
firewall throughput, checking, 638–639
image file, copying into Flash memory, 238–239
packet capture sessions, configuring with Packet Capture Wizard, 683–685
assigning
IP address to interfaces, 54–58
privilege levels
to commands, 268–271
to users, 265
security level to interfaces, 54
unique MAC addresses to ASA physical addresses, 167–168
VLAN number to logical interface, 52–53
attributes of trunk links, 46
audit trails, generating, 245
AUS (Automatic Upgrade Server), automatically upgrading failover pair, 524
authentication
of generic users on Cisco firewalls, 262–263
of local users, 265–267
uauth, absolute uauth timer, 9
authorization, local user configuration, 268–272
authorizing
firewall command access, 267–272
user activity with TACACS+ servers, 291–293
Auto Update client
configuring firewall as, 221–227
verifying operation, 227
Auto Update Server, configuring firewall as, 228–232
automatic CSC SSM updates, configuring, 741– 743
automatically upgrading image files, 211
Auto-RP, 136–137

B

banners, configuring on user interface, 243–244
Base license, failover support, 39
BEQ (best-effort queuing), 73–74, 663
configuring, 75–77
displaying information, 77
best practices
for firewall configuration, 21–23
for security policy maintenance, 21–23
bidirectional mode (PIM), 135
configuring, 138
neighbor filtering, 143–144
Bidirectional NAT, 328
boot image setting, displaying, 201
bootstrap router method, 136
bridge mode (CSM), 550
broadcast traffic, 126
BSRs (bootstrap routers), 136
buffered logging, enabling, 626
buffered messages, viewing, 597
bump-in-the-wire, 312
bypass links, 81–83

C

calculating runtime differences on processes, 630–632
candidate RPs, 136
capture sessions
controlling, 680–681
copying buffer contents
to TFTP server, 676
to web browser, 677–680
displaying trunk contents, 675–676
example, 682
monitoring, 673–674
verifying packets passing through interfaces, 666–673
capturing traffic
with Packet Capture Wizard, 683–685
on VLANs inside switch chassis, 686–689
Catalyst 6500 switch, FWSM, 20
accessing, 28
changeto command, 185
changeto system command, 584
changing message severity levels, 616
characteristics of context configuration files, 168–169
checking system resources, 627
failover performance, 646–655
firewall CPU load, 627–632
firewall interface throughput, 655–665
firewall memory usage, 633–636
firewall throughput, 638–645
inspection engine activity, 645–646
stateful inspection resources, 636–638
circular logging buffer, 597
Cisco firewalls
clock management, 581
setting clock manually, 582–583
setting clock with NTP, 584–586
message logging, configuring, 591–613
specifications, 20–21
supported translation types, 326–327
user management
accounting local user activity, 272
generic users, 262–264
with AAA servers, 272–301
with local database, 264–272
CiscoACS servers, configuring command authorization, 283–285
class maps, configuring, 398–406
classifiers, 160, 166
classifying traffic, 398–406
clear ip verify statistics command, 86
clear traffic command, 514
clearing
ARP cache, 69
internal logging buffer, 615
static ARP entries, 319
xlate table entries, 717
CLI, initial firewall configuration, 41–42
clock management, 581
setting clock manually, 582–583
setting clock with NTP, 584–586
clock summer-time command, recurring keyword, 583
collecting Syslog firewall logs, 21–23
combining load balancing techniques, 530
command accounting, configuring, 286–287
command authorization, configuring, 283–285
command history, 32
commands
abbreviating, 30
active, viewing, 29
arp, alias keyword, 319
arp timeout, 699
changeto, 185
changeto system, 584
clear ip verify statistics, 86
clear traffic, 514
configure terminal, 41–42
debug icmp trace, 10–11
debug ntp authentication, 586
debug track, 94
editing, 30
entering, 29
executing on failover peer, 517–519
failover active, 516
failover exec, 519
failover mac address, 490
failover poll, 492
failover preempt, 486
failover reload-standby, 517
filtering output, 32–33
fragment chain, 72

inspect, 432
mac-address auto, 167
mode multiple, 172
operators, 356
ping
example, 696
permitting on ASA and PIX platforms, 696
preempt, 489
privilege levels, 262
assigning, 268–271
regular expressions
operators, 33
searching, 32–33
same-security-traffic, 323
show activation-key, 170, 518
show admin-context, 191
show arp, 68–69
show arp-inspection, 320
show blocks, 516, 634
show conn, 326, 713
show dhcprelay statistics, 125
show failover, 497, 508–513, 521
show firewall, 312
show flash, 200
show interface, 176, 515
show ipv6 interface, 67
show local-host, 715
show logging, 614, 622
show memory detail, 634
show mode, 171
show pim topology, 153
show processes, 629
show resource allocation, 189
show rip, 96–97
show running-config all, 30
show service-policy, 427, 645
show shun statistics, 383
show tech-support, 692
show traffic, 514
show version, 34–36
show xlate, 709–714
static, 327
syntax errors, 31
terminal width, 34
write mem, 42
community string (SNMP), defining, 257–258
compiling access lists, 352
conditional NAT
configuring, 335–338
static NAT, 335
configuration commands, entering manually, 218
configuration examples
of active-active failover, 501–508
with FWSM, 500– 501
with PIX firewalls, 498–501
of active-standby failover, 474–475
configuration files
of contexts, characteristics, 168–169
running configuration
copying across failover pair, 217–218
displaying, 214
saving to Flash memory, 214–215
saving to TFTP server, 216–217
startup configuration
displaying, 213–214
erasing configuration commands, 218
managing, 211–213
selecting, 212–213
configuration mode, 29
configure terminal command, 41–42
configuring
ACLs, 348–349, 353
address translation
connection limits, 328–330
dynamic NAT, 341–346
dynamic PAT, 342–346
identity NAT, 338–340
NAT exemption, 340–341
policy NAT, 335–338
static NAT, 331–334
AIP SSM, 769–772
IPS policies, 777–780
IPS sensors, 780–781
IPS virtual sensors, 781–785
application inspection, 426–432
DCERPC inspection, 437–438
DNS inspection, 438–440
ESMTP inspection, 441–443
FTP inspection, 443–446
GTP inspection, 446–449
H.323 inspection, 449–451
HTTP inspection, 452–460
ICMP inspection, 460–462
IM inspection, 462, 464

IPSec Passthru inspection, 465
matching text with regular expressions, 433–437
MGCP inspection, 465, 467
MGCP map, 467
NetBIOS inspection, 468
RADIUS accounting inspection, 468–469
SNMP accounting inspection, 470–471
ARP, 68–69
banners on user interface, 243–244
bidirectional PIM neighbor filtering, 144
class maps, 398–406
command accounting, 286–287
command authorization, 283–285
content filters, 390–395
contexts, 174–180
CSC SSM, 729
automatic updates, 741–743
FTP inspection policies, 753–755
initial settings, 733–738
inspection policies, 744–753
POP3 inspection policies, 765–769
SMTP inspection policies, 755–764
traffic inspection, 730–733
CSM FWLB, 552–561
CSS FWLB, 571–574
DDNS, 121–123
verifying configuration, 123–124
DHCP relay, 124–125
DHCP server functions, 116–120
EIGRP, 97–101
failover, 484, 495
contexts, 495
health monitoring policy, 490–492
interface failure policy, 492
primary unit, 485–488
stateful, 492–497
firewalls
as Auto Update client, 221–227
as Auto Update Server, 228–232
best practices, 21–23
FragGuard, 71–73
identity NAT for exclusive outbound use, 340
IGMP, 147–149
interfaces, 50, 52–60
examples, 58–60
IP address assignment, 54–58
MTU, 70–71
IOS FWLB, 531–540
IPv6, 61–63
neighbor advertisements, 65–66
neighbor discovery, 64–65
prefix advertisements, 66–67
IPv6 addresses, 60–61
local user authorization, 268–272
medium-security interfaces, inbound access, 350–352
message logging, 591–613
multicast boundaries, 142–143
multiple-context mode, 170–173
navigating multiple security contexts, 173–174
OSPF, 105–112
example configuration, 115–116
on firewall, 101–104
on both sides of firewall, 104–105
prefix lists, 108
redistribution, 112–115
PIM, 137–141
neighbor filtering, 143–144
priority queuing, 75–77
RADIUS user authorization, 294–295
redundant interfaces, 48–49
RIP on firewall, 95–97
verifying configuration, 96–97
shuns, 382–384
example, 384–386
SLA monitor process, 89–92
SMR, 145–147
example, 150
SNMP, 256–259
SSM modules
AIP SSM, 769–772
CSC SSM, 729-733
initial configuration, 726–729
static routes, 86–87, 89
switch ports, 485
transparent firewall, 314–317
access lists, 321
ARP inspection, 319–321
interface speed, 315
MAC address learning process, 318–319
management address, 317–319
non-IP protocol forwarding policy, 321– 322

conn table, 7
entries, 7–8
size, checking, 637–638
connecting to CSC SSM management interface, 740–741
connection limits
configuring for address translation, 328–329
outbound, configuring on UDP/TCP, 329–330
connectionless protocols, 9
ICMP, stateful inspection, 10–13
UDP, 13–15
connection-oriented protocols, 9
TCP, 15–19
connections
embryonic, 16–17
limiting, 330–331
maximum limit of, defining, 18
TCP intercept, 18
half-closed, 18
inbound access, 324
xlate lookup, 7
maximum number supported on Cisco firewalls, 37–39
outbound access, 323–324
shunning, 382–384
example, 384–386
stateful inspection, 7
verifying, 711–716
connectivity
active shuns, verifying, 718–720
IPv6, testing, 67–68
of failover pairs, 481–482
verifying, 691–722
with ACLs, 705–707
console connection, accessing firewall user interface, 232–233
console logging, 595–596
content filtering, 19
configuring, 390–395
examples, 396
WCCPv2, 396–397
context mode, displaying, 171
context-based help, 31
contexts, 158
admin contexts, 173–175
allocating firewall resources, 185–191
assigning to failover groups, 495
classifiers, 166
configuration files, characteristics, 168–169
configuring, 174–180
CPU usage, displaying, 192
example definition, 180–185
inside context interfaces, sharing, 161–164
labeling, 175
multiple-context mode
configuring, 170–173
navigating multiple security contexts, 173–174
resource allocation, 185–186
physical interfaces, mapping to logical interfaces, 178
system execution space, features, 169–170
system name, viewing, 176
controlling
capture sessions, 680–681
traffic
ACLs, configuring, 348–349
to/from medium-security interfaces, 349–352
copying
ASDM image into Flash memory, 238–239
capture buffer contents
to TFTP server, 676
to web browser, 677–680
files to/from Flash memory, 196–197
PDM image into Flash memory, 238–239
running configuration across failover pair, 217–218
CPU utilization
checking, 627–632
of contexts, displaying, 192
crashes
forcing, 250
information, saving, 248–249
crashinfo files
deleting, 251
generating, 249
viewing, 250–251
creating
directories
in Flash memory, 198
in PIX 7.x Flash memory, 198–199
test crashinfo files, 249

critical messages (syslog), 802-803
CSC (Content Security and Control) SSM, 725
automatic updates, configuring, 741–743
configuring, 729
initial configuration, repairing, 738–740
initial settings, configuring, 733–738
inspection policies
configuring, 744–753
FTP, configuring, 753–755
POP3, configuring, 765–769
SMTP, configuring, 755–764
management interface, connecting to, 740–741
traffic inspection, configuring, 730–733
CSM (Content Switching Module) FWLB, 549–552
configuring, 552–561
displaying information, 569–571
example configuration, 561–569
CSS (Cisco Content Services Switch), 529
CSS FWLB
configuring, 571–574
displaying information, 579
example configuration, 574–579
Ctrl-I command, displaying typed commands, 30

D

DCERPC (Distributed Computing Environment Remote Procedure Call), 437
DCERPC inspection, configuring, 437–438
DDNS (Dynamic DNS), 120
configuring, 121–123
database, updating, 121
verifying configuration, 123–124
debug icmp trace command, 10–11
debug ntp authentication command, 586
debug packet sessions, enabling, 689–691
debug track command, 94
debugging
failover activity, 513–516
ICMP debugging, enabling, 697–698
debugging messages (syslog), 837-845
default behavior of firewalls, 4
default policies, defining, 421–423
default routes, 84
advertising, 96
defining
logging policies, 594–595
object groups, 363–364
enhanced service object groups, 370–373
ICMP type object groups, 367–369
network object groups, 364–365
protocol object groups, 365–367
service object groups, 369–370
policy maps, 406–420
default policies, 421–423
security policies in MPF, 397–398
server reactivation policies, 274
SNMP community string, 257–258
deleting
crashinfo files, 251
files from Flash memory, 197
depletion mode, 274
descriptions, adding to ACLs, 359–360
detecting
firewall failures, 480
spam
in POP3 e-mail, 767–768
in SMTP e-mail, 759–762
DHCP (Dynamic Host Configuration Protocol), 19
DDNS, configuring, 121–124
DHCP relay, configuring, 124–125
DHCP server, configuring, 116–120
directories
creating in Flash memory, 198–199
removing from Flash memory, 199
disabling
active commands, 29
OSPF adjacency logging, 106
screen paging, 34
disconnecting from active PDM sessions, 245
displaying
ACL hit counts, 707–708
active PDM/ASDM management application sessions, 245
ARP inspection status, 320
available firewall interfaces, 46–47
boot image setting, 201
buffered messages, 597
configured contexts, 174
context information, 191
context mode, 171

contexts, 174, 191
system name, 176
CPU usage for contexts, 192
CSM FWLB information, 569–571
CSS FWLB information, 579
failover statistics, 508–513
firewall crash information, 250–251
firewall features, 34
IOS FWLB information, 546–549
monitoring status of interfaces, 497
PIX 6.3 flash files, 200
priority queuing information, 77
redundant interface status, 49–50
running configuration, 214
startup configuration, 213–214
startup configuration environment variable, 212
trunk contents, 675–676
typed commands, Ctrl-I, 30
disrupting
ping process, 697
traceroute process, 705
DMZ (demilitarized zone) networks, 349–352
protecting, 22
DNS Guard, 15
DNS inspection, configuring, 438–440
DNS resolution, configuring on firewall interface, 197
DoS attacks, preventing IP address spoofing, 84–86
downloadable ACLs
enabling on firewall, 298
verifying, 299
downloading operating system image from monitor prompt, 202–206
DUAL (Diffusing Update Algorithm), 97
dynamic NAT
configuring, 341–346
examples, 346–348
dynamic PAT
configuring, 342–346
examples, 346–348

E

editing commands, 30
EIGRP (Enhanced Interior Gateway Routing Protocol)
configuring, 97–101
DUAL, 97
EMBLEM format (system messages), 588
embryonic connections, 16–17
limiting, 330–331
maximum limit of, defining, 18
TCP intercept, 18
enabling
buffered logging, 626
debug packet sessions, 689–691
ICMP debugging, 697–698
ICMP inspection, 703
RPF, 85
end users, 261
end-user cut-through proxy
configuration examples, 300–301
configuring on AAA servers, 287–300
enhanced service object groups, defining, 370–373
entering commands, 29
environment variable for startup configuration, displaying, 212
erasing
configuration commands from startup configuration, 218
Flash memory, 199–200
error messages (syslog), 804-815
ESMTP inspection, configuring, 441–443
examining firewall crash information, 248–249
example configurations
CSM FWLB, 561–569
CSS FWLB, 574–579
interfaces, 58–60
OSPF, 115–116
examples
of ACLs, 362–363
of capture session, 681–682
of content filters, 396
of context definition, 180–185
of dynamic NAT, 346–348
of dynamic PAT, 346–348

of firewall failover configuration
active-active, 501–508
active-standby with FWSM, 500–501
active-standby with PIX firewalls, 498– 500
of IOS FWLB, 540–546
of ping command, 696
of SMR configuration, 150
exec banners, configuring on user interface, 243–244
executing commands
on failover peer, 517–519
remotely, 519
exploits, VLAN hopping, 79–80
preventing, 80–81
extended access lists, 356–357
extended pings
disrupting, 697
sending, 696–697

F

failover, 19
active-active failover pair, 474–477
configuration example, 501–508
requirements, 482–484
active-standby failover pair, 474–475
configuration example, 498–501
manually upgrading, 520–524
cause of, determining, 652–655
configuring, 484, 495
contexts, configuring, 495
debugging, 513–516
displaying statistics, 508–513
health monitoring policy, configuring, 490–492
interfaces
failure policy, configuring, 492
"testing" mode, 480–481
LAN-based, 479
manually forcing role change, 516
primary unit, configuring, 485–488
required licenses, 475
resetting failed firewall unit, 517
stateful
configuring, 492–497
monitoring, 514–516
toggling roles, 655
verifying
communication, 647–650
unit roles, 646–647
failover active command, 516
failover cable, 479
failover exec command, 519
failover groups, 482–484
failover hello messages, 492
failover mac address command, 490
failover pairs
connectivity, 481–482
copying running configuration across, 217–218
failover poll command, 492
failover preempt command, 486
failover reload-standby command, 517
failures, detecting, 480
feasible successors, 97
features of firewalls
displaying, 34
unlocking, 39
fields of system messages, 588
file blocking (HTTP), configuring on CSC SSM, 751
files
copying to/from Flash memory, 196–197
deleting from Flash, 197
renaming in Flash, 198
filtering. *See also* content filtering
command output, 32–33
POP3 content, 768–769
SMTP content, 758–759
fine-tuning logging message generation, 615–616
firewall farms, 527
firewall masks, 355
firewalls
configuring
as Auto Update client, 221–227
as Auto Update Server, 228–232
crashes, forcing, 250
interface throughput, checking, 655–665
first-hop routers, 128
fixed-group addresses, 127
fixup. *See* application inspection
flash files, displaying in PIX 6.3, 200

Flash memory
ASA
administration, 196–200
managing, 194
copying files to/from, 196–197
creating new directories, 198
deleting files from, 197
erasing, 200
formatting, 199
FWSM, managing, 194–196
hierarchical structure, 195–196
managing, 192–193
operating system image
downloading from monitor prompt, 202–206
identifying, 200–201
upgrading, 205–210
PIX 7.x, creating directories, 198–199
removing directories, 199
renaming files, 198
running configuration, saving, 214–215
system integrity, verifying, 199
FO (Failover) license, 39
FO-AA (Failover-Active/Active) license, 39
forcing
failover role change, 516
firewall crashes, 250
foreign addresses, 6
formatting Flash memory, 199
FragGuard, configuring, 71–73
fragment cache, adjusting size of, 72
fragment chain command, 72
FTP, uploading logging buffer contents, 598
FTP inspection
configuring, 443–446
policies, configuring on CSC SSM, 753–755
FWLB (Firewall Load Balancing), 527–528
CSM FWLB, 549–552
configuring, 552–561
displaying information, 569–571
example configuration, 561–569
CSS FWLB
configuring, 571–574
displaying information, 579
example configuration, 574–579
IOS FWLB, 530–531
configuring, 531–540
displaying information, 546–549
example, 540–546
methods of, 529
FWSM (Firewall Services Module), 20
accessing on Catalyst 6500 switch, 28
failover pairs, 477
capabilities, 39
Flash memory management, 194–196
logical interfaces, 47
NTP support, 584
passwords, recovering, 307–308
security levels, 316
VLAN groups, defining, 47

G

General Queries (IGMPv2), 130
generating
audit trails, 245
test crashinfo files, 249
generic users
accounting, 263–264
authentication, 262–263
managing on Cisco firewalls, 262
global addresses, 6, 61
global configuration mode, 29
globally scoped addresses, 127
GMT (Greenwich Mean Time), 581
Group-Specific Queries (IGMPv2), 130
GTP inspection, configuring, 446–449

H

H.323 inspection, configuring, 449–451
half-closed connections, 18
half-open connections, 17
hardware load balancing, CSM FWLB, 549–552
configuring, 552–561
displaying information, 569–571
example configuration, 561–569
help system, context-based help, 31
hierarchical structure of flash file system, 195–196

history of failover state changes, displaying, 513
hit counter (ACL), resetting, 382
hitless upgrade, 479, 519
holdtime timer, setting, 491
HTTP inspection
configuring, 452–460
policies, configuring on CSC SSM, 751
file blocking, 751
HTTP scanning, 751–753
URL blocking, 745–746
URL filtering, 746–750
HTTP scanning, configuring on CSC SSM, 751–753

I

ICMP (Internet Control Message Protocol)
ACLs operation, 8
debugging, enabling, 697–698
message types, 788–790
object groups, defining, 367–369
ping, 481
restricting traffic, 23
stateful inspection, 10–11
case study, 12–13
time-exceeded messages, permitting, 704
ICMP inspection
configuring, 460–462
enabling, 703
identifying operating system image in Flash memory, 200–201
identity NAT, configuring, 338–340
idle uauth timer, 9
IEEE 802.1Q trunks, attributes, 46
IGMP (Internet Group Message Protocol)
configuring, 147–149
SMR, configuring, 145–147
verifying operation, 151–152
IGMP proxy agent, 126
IM inspection, configuring, 462–464
image files, automatically upgrading, 211
inbound access, 324
configuring on medium-security interfaces, 350–352
inbound connections, 4
xlate lookup, 7
informational messages (syslog), 827-837
initial firewall configuration, 41–42
initial settings, configuring on CSC SSM, 733–738
initiating
firewall reload, 246–247
after specific time interval, 247–248
multiple context mode, 172–173
inline interface configuration, 781
inside context interfaces, sharing, 161–164
inside interfaces, 2–3
inspect command, 432
inspection engines, 9. *See also* application inspection
activity, checking, 645–646
ICMP stateful inspection, 10–13
TCP stateful inspection, 15–19
UDP stateful inspection, 13–15
inspection policies (CSC SSM), 744– 753
FTP, configuring, 753–755
HTTP, configuring, 745–753
interface polltime, 492
POP3, configuring, 765–769
SMTP, configuring, 755–764
interface priority queues, 73–74
interfaces
ASA, assigning unique MAC addresses, 167– 168
configuring, 50, 52–60
connectivity
checking ARP cache, 698–700
checking routing table, 700
testing with ping packets, 695–696
verifying, 691–692, 720–722
verifying with ACLs, 705–707
verifying with traceroute, 700–703
DNS resolution, configuring, 197
example configurations, 58–60
inbound access, 324
inside context interfaces, sharing, 161–164
IP addresses
assigning, 54–58
IPv6 addresses, configuring, 60–61
logical, assigning VLAN number, 52–53
lower-security, applying ACLs, 351

medium-security
inbound access, 350, 352
traffic, controlling, 349–352
monitoring status, displaying, 497
MTU, configuring, 70–71
outbound access, 323–324
physical, mapping to contexts, 158, 160–161
policy maps, applying, 406–423
redundant interface groups, 474
same-security access, 324–325
security level, assigning, 54
testing mode, 480–481
verifying packets passing through via capture sessions, 666–676
internal clock
setting manually, 582–583
setting with NTP, 584–586
internal logging buffer, clearing, 615
invoking
context-based help, 31
Packet Tracer tool, 694
IOS FWLB, 530–531
configuring, 531–540
displaying information, 546–549
example, 540–546
IP address spoofing, preventing, 84–86
IP addresses, assigning to interfaces, 54–58
IP multicast, 127
addressing, 127
administratively scoped addresses, 142
bidirectional PIM neighbor filtering, configuring, 144
IGMP
configuring, 147–149
verifying operation, 151–152
multicast boundaries, configuring, 142–143
multicast trees, 128
PIM, 130–131
configuring, 137–141
Sparse Mode, 131–134
verifying operation, 152–155
Version 1, 136
PIM neighbor filtering, configuring, 143–144
PIM-SM, RP designation, 136–137
RPF, 128–129
SMR
configuring, 145–147
example configuration, 150
IP port numbers, 790–791
corresponding Cisco firewall keywords, 791– 794
ip verify reverse-path interface, 85
IPS (Intrusion Prevention Systems), configuring on AIP SSM, 778–780
policies, 777–779
sensors, 780–781
virtual sensors, 781–785
IPSec Passthru inspection, configuring, 465
IPv6
configuring, 60–63
connectivity, testing, 67–68
neighbor advertisements, configuring, 65–66
neighbor discovery, configuring, 64–65
prefix advertisements, configuring, 66–67
ISNs (initial sequence numbers), 8, 331

J-K-L

knowledge base, 779

labeling contexts, 175
LAN-based failover, 479–481
last-hop routers, 128
Layer 2 firewalls, 312
Layer 3 traffic
classifying, 398–406
policy maps, defining, 406–420
Layer 4 traffic
classifying, 398–406
policy maps, defining, 406–420
Leave Group messages (IGMPv2), 130
length of terminal screen, adjusting, 34
level 0 passwords, resetting, 263
license, registering, 39
licenses
activation keys, 39
upgrading, 40–41
Base license, failover support, 39
FO-AA, 39
required for failover, 475
upgrading, 39

limitations on outbound UDP/TCP connections, 329–330
limiting
embryonic connections, 330–331
resource allocation on security contexts, 186–188
resources allocated to contexts, 185–189
TCP MSS size, 71
link-local addresses, 61, 127
links, bypass links, 81–83
link-state protocols, OSPF configuration, 105–112
listing available firewall interfaces, 46–47
LLQ (low-latency queue), 74, 663
configuring, 75–77
displaying information, 77
load balancing
CSM FWLB, 549–552
configuring, 552–561
displaying information, 569–571
example configuration, 561–569
FWLB, 528–529
IOS FWLB, 530–531
configuring, 531–540
displaying information, 546–549
example, 540–546
local addresses, 6
local database, user management, 264–265
accounting local user activity, 272
firewall command access, authorizing, 267–272
local user authentication, 265–267
local user authorization, configuring, 268–272
logging
ACE activity, 379–380
ACL activity, 617–619
logging messages, 587
analyzing firewall logs, 619–623
clearing internal logging buffer, 615
configuring, 591–613
destinations, verifying, 614
logging to secure Syslog server with SSL, 604–611
manually testing message generation, 615
pruning messages, 615–616
sending messages
to ASDM management application, 613
to email address, 611–613
severity levels
changing, 616
setting, 587
time stamp synchronization, 588
logging timestamp message, 604
logical interfaces, 35, 47
mapping to physical interfaces, 178
subinterface number, 51–52
VLAN number, assigning, 52–53
logical VLAN interfaces, 51–52
login banner, configuring on user interface, 243–244
lookups (xlate table), 7
lower-security interfaces, applying ACLs, 351
LSAs (link-state advertisements), 101

M

MAC addresses
of ASA physical interfaces, displaying, 165
learning process, configuring on transparent firewalls, 318–319
mac-address auto command, 167
management traffic, restricting access to, 23
managing
AIP SSM, 773
Flash memory, 192–193
ASA, 194
FWSM, 194–196
startup configuration, 211–213
manipulating ACLs, 357–358
manually forcing failover role change, 516
manually resetting failed firewall units, 517
manually setting internal clock, 582–583
manually testing logging message generation, 615
manually upgrading active-standby pair, 520– 524
mapping
to contexts, 158, 160–161
to logical interfaces (contexts), 178
mapping agents, 136
medium-security interfaces
inbound access, configuring, 350, 352
traffic, controlling, 349–352
Membership Report messages, 129

memory
Flash
copying files to/from, 196–197
creating directories in, 198
deleting files from, 197
downloading operating system image, 202–206
formatting, 199
identifying operating system image, 200–201
managing, 192–196
removing directories from, 199
renaming files in, 198
upgrading operating system image, 205–210
usage, checking, 633–636
merging startup and running configuration commands, 219–221
messages
ICMP, 788–790
IGMP Membership Report, 129
logging, 587
analyzing firewall logs, 619–623
buffered messages, displaying, 597
destinations, verifying, 614
logging ACL activity, 617–619
logging to secure Syslog server with SSL, 604–611
manually testing, 615
pruning messages, 615–616
sending messages to ASDM management application, 613
sending messages to email address, 611–613
setting severity levels, 587
time stamp synchronization, 588
logging timestamp, 604
severity levels, changing, 616
syslog
severity level 1 alerts, 799-802
severity level 2 critical messages, 802-803
severity level 3 error messages, 804-815
severity level 4 warning messages, 815-821
severity level 5 notifications, 821-822
severity level 6 informational messages, 827-832
severity level 7 debugging messages, 831-845
system messages, format, 588
MGCP inspection, configuring, 465, 467
MGCP map, configuring, 467
MIBs, 252, 255
monitoring firewall activity, 251–252
objects, 253
mode multiple command, 172
modifying message severity levels, 616
monitor screen length/width, changing, 34
monitoring
ACLs, 380–382
active shun activity, 383
address translations, 709–714
administrative sessions, 244–245
capture sessions, 673–674
connections, 711–716
firewall activity with SNMP, 251–252
traps, 255
firewall configuration changes, 722–723
stateful failover, 514–516
xlate entries based on local address, 710
MOTD banners, configuring on user interface, 243–244
MPF (Modular Policy Framework), defining security policies, 397–398
mroutes, 142
MSS (maximum segment size), configuring, 71
MTU (maximum transmission unit), interface configuration, 70–71
multicast, 126–127
boundaries, configuring, 142–143
IGMP
configuring, 147–149
verifying operation, 151–152
OUI values, 127
PIM, 130–131, 136
configuring, 137–141
verifying operation, 152–155
PIM-SM, 131–134
RP designation, 136–137
routing
multicast trees, 128
RPF, 128–129

SMR
configuring, 145–147
example configuration, 150
multicast groups, 126
multicast trees, 128
multiple-context mode, 158, 313
classifiers, 160
configuring, 170–173
initiating, 172–173
navigating multiple security contexts, 173–174
resource allocation, 185–186

N

naming format for downloadable ACLs, 299
NAT
Bidirectional, 328
identity NAT, configuring, 338–340
policy NAT, configuring, 335–338
NAT exemption, 327
configuring, 340–341
navigating multiple security contexts, 173–174
NBNS (NetBIOS Name Service), configuring NetBIOS inspection, 468
neighbor advertisements, IPv6 configuration, 65–66
neighbor discovery, IPv6 configuration, 64–65
NetBIOS inspection, configuring, 468
network object groups, defining, 364–365
non-IP protocol forwarding policy, configuring on transparent firewall, 321–322
notifications (syslog), 821-827
NTP (Network Time Protocol), setting internal clock, 584–586

O

object groups, 352
applying to ACLs, 373–379
defining, 363–364
enhanced service object groups, defining, 370–373
ICMP type, defining, 367–369
network object groups, defining, 364–365
protocol object groups, defining, 365–367
service object groups, defining, 369–370
operating system
of active-standby failover pair, upgrading, 520–524
downloading image from monitor prompt, 202–206
identifying image in Flash memory, 200–201
upgrading image, 205–210
operators, 356
optimizing Syslog servers, 589
options (commands), entering, 29
OSPF (Open Shortest Path First)
Areas, subnet notation, 107
configuring, 105–112
example configuration, 115–116
prefix lists, configuring, 108
redistribution, configuring, 112–115
static route redistribution, configuring, 114
virtual links, 109
OUI (Organizationally Unique Identifier) values, 127, 168
outbound access, 323–324
outbound connections, 4
UDP/TCP limitations, 329–330
xlate lookup, 7
output interface queues, 73–74
outside interfaces, 2–3
address spoofing, 5–6
Outside NAT, 328

P

packet capture, 19
Packet Capture Wizard, enabling packet capture sessions in ASDM, 683–685
packet classifiers, 160
Packet Tracer feature, verifying firewall connectivity, 692–694
Packet Tracer tool, invoking, 694
packets
fragments, handling, 71–73
ICMP, stateful inspection of, 10–13
IPv4, Protocol field, 787–788
TCP, stateful inspection of, 15–19
UDP, stateful inspection of, 13–15

parameters
of conn table entries, 7–8
for xlate table entries, 6
partitions, accessing ASA Flash memory, 194–195
passwords, recovering
ASA, 302–305
FWSM, 307–308
PIX, 303–307
PAT (Port Address Translation), 326
dynamic PAT, configuring, 342–346
PDM (PIX Device Manager)
accessing firewall user interface, 238–242
image file, copying into Flash memory, 238–239
perfmon counters, checking firewall throughput, 643–645
permitting ICMP time-exceeded messages, 704
physical interfaces, mapping
to contexts, 158–161
to logical interfaces, 178
PIM (Protocol Independent Multicast), 130–131
bidirectional mode, 135
configuring, 137–141
neighbor filtering, configuring, 143–144
bidirectional configuring, 144
shared trees, 132
Sparse Mode, 131–134
verifying operation, 152–155
Version 1, 136
PIM-SM, RP designation, 136–137
ping command, 481
example, 696
permitting on ASA and PIX platforms, 696
PIX
failover pair capabilities, 39
passwords, recovering, 306–307
PIX 6.3, displaying flash files, 200
policy maps
default policies, defining, 421–423
defining, 406–420
policy NAT, configuring, 335–338
POP3 inspection policies, configuring on CSC SSM, 765–766
content filtering, 768–769
spam detection, 767–768
port numbers, 790–791
corresponding Cisco firewall keywords, 791–794
predefined logging messages, 591–592
preempt command, 489
prefix advertisements (IPv6), configuring, 66–67
preventing
IP address spoofing, 84–86
VLAN hopping, 80–81
primary failover unit, configuring, 485–488
priority queuing
configuring, 75–77
displaying information, 77
privilege levels, 262
accessing, 263
assigning
to commands, 268–271
to users, 265
privileged EXEC mode, 28
processes, calculating runtime differences, 630–632
promiscuous monitoring, 780
protecting DMZ, 22
Protocol field, 787
corresponding Cisco firewall keywords, 788
protocol object groups, defining, 365–367
pruning messages, 615–616

Q-R

queuing
priority queuing
configuring, 75–77
displaying information, 77
transmit ring, 7

R (Restricted) license, 39
RADIUS
accounting inspection, configuring, 468–469
user authorization, configuring, 294–295
rate-limiting logging messages, 593
reachability, testing, 91–95
recalling commands, 32
recompiling access lists, 353

recovering passwords
ASA, 302–305
FWSM, 307–308
PIX, 303–307
recurring keyword (clock summer-time command), 583
redistribution, configuring OSPF, 112–115
redundant interface groups, 474
redundant interfaces, configuring, 48–49
registering firewall licenses, 39
regular expressions
regular expressions
application inspection, text matching, 433–437
operators, 33
performing searches on, 32–33
reloading firewalls, 246–247
after specific time interval, 247–248
remark ACEs, adding to ACLs, 359–360
remote command execution, 519
removing
ACEs from ACLs, 358–359
directories in Flash memory, 199
static routes, 88
renaming
ACLs, 359
files in Flash memory, 198
repairing CSC SSM initial configuration, 738–740
requirements for active-active failover, 482–484
resetting
ACL hit counters, 382
application partition passwords, 308
failed firewall unit, 517
level 0 passwords, 263
resources, allocating to contexts, 185–191
restricting
access to management traffic, 23
ICMP traffic, 23
RFC 2827, 5
RFC Sourcebook, 787
RIP (Routing Information Protocol)
configuring on firewall, 95–97
verifying configuration, 96–97
route lookups, 531
route maps (OSPF), configuring, 112–115
routed firewall mode, 311
router mode (CSM), 550
routing information sources, 83
routing IP multicast, 128–129
routing tables, checking connectivity, 700
RP (Rendezvous Point), 131
RPF (Reverse Path Forwarding), 84, 128–129
enabling, 85
preventing IP address spoofing, 85–86
running configuration, 478
configuration commands, entering manually, 218
copying across failover pair, 217–218
displaying, 214
merging configuration commands with startup configuration, 219–221
saving to Flash memory, 214–215
saving to TFTP server, 216–217
runtime differences, calculating on processes, 630–632

S

same-security access, 324–325
same-security-traffic command, 323
saving
firewall crash information, 248–249
running configuration to Flash memory, 214– 215
running configuration to TFTP server, 216–217
scheduling firewall reloads, 247
screen paging, disabling, 34
searching for regular expressions, 32–33
security contexts, 158
security levels
assigning to interfaces, 54
on FWSM, 316
security policies
best practices, 21–23
defining in MPF, 397–398
"security wheel", 23
selecting startup configuration, 212–213
sending Syslog messages with TCP, 602
server reactivation policies, defining, 274
service contact port, 791
service object groups, defining, 369–370

setting system clock
manually, 582–583
with NTP, 584–586
severity levels, 587
changing, 616
setting for message logging, 587
severity level 1 alerts, 799-802
severity level 2 critical messages, 802-803
severity level 3 error messages, 804-815
severity level 4 warning messages, 815-821
severity level 5 notifications, 821-827
severity level 6 informational messages, 827-837
severity level 7 debugging messages, 832-845
shared trees, 131-132
sharing inside context interfaces, 161–164
show activation-key command, 170, 518
show admin-context command, 191
show arp command, 68–69
show arp-inspection command, 320
show blocks command, 516, 634
show conn command, 326, 713
show dhcprelay statistics command, 125
show failover command, 497, 508–513, 521
show firewall command, 312
show flash command, 200
show interface command, 176, 515
show ipv6 interface command, 67
show local-host command, 715
show logging command, 614, 622
show memory detail command, 634
show mode command, 171
show pim topology command, 153
show processes command, 629
show resource allocation command, 189
show rip command, 96–97
show running-config all command, 30
show service-policy command, 427, 645
show shun statistics command, 383
show tech-support command, 692
show traffic command, 514
show version command, 34–36
show xlate command, 709–714
shunning traffic, 382–384
example, 384–386
shuns
configuring, 382–384
verifying connectivity, 718–720
signature database file (AIP SSM), updating, 774–776
single-context mode, 158
site-local addresses, 61
SLA (service level agreement) monitor process, configuring, 89–92
SMR (stub multicast router), 128
configuring, 145–147
example configuration, 150
SMTP inspection policies, configuring on CSC SSM, 755–758
mail handling, 763–765
SMTP filtering, 758–759
spam detection, 759–762
SNMP (Simple Network Management Protocol)
accounting inspection, configuring, 470–471
configuring, 256–259
MIBs, 253, 255
monitoring firewall activity, 251–252
traps, 255–256
software load balancing, IOS FWLB, 530–531
configuring, 531–540
displaying information, 546–549
example, 540–546
source address, spoofing, 5
spam
detecting in POP3 e-mail, 767–768
SMTP inspection, configuring, 759–762
SPAN (switch port analyzer), configuring traffic capture sessions, 687
Sparse Mode (PIM), 131
sparse mode (PIM)
shared trees, 132
specifications of Cisco firewalls, 20–21
spoofed IP addresses, preventing, 84–86
SPT (shortest path tree), 135
SSH (Secure Shell), accessing firewall user interface, 235–237
SSL (Secure Sockets Layer), secure Syslog server logging, 604–611

SSM modules
4GE SSM, 725
AIP SSM, 725
configuring, 769–772
IPS policies, configuring, 777–780
license, updating, 773–774
managing, 773
signature database file, updating, 774–776
CSC SSM, 725
automatic updates, configuring, 741–743
configuring, 729–738
FTP inspection policies, configuring, 753–755
initial configuration, repairing, 738–740
inspection policies, configuring, 744–753
management interface, connecting to, 740–741
POP3 inspection policies, configuring, 765–769
SMTP inspection policies, configuring, 755–764
initial configuration, 726–729
startup configuration, 478
configuration commands, merging with running configuration commands, 219–221
displaying, 213–214
environment variable, displaying, 212
erasing configuration commands from, 218
managing, 211–213
selecting, 212–213
stateful backup, 531
stateful failover, 481
configuring, 492–497
monitoring, 514–516
stateful inspection, 7, 9
of ICMP, 10–11
case study, 12–13
packet classifiers, 160
resources, checking, 636–638
of TCP, 15–18
TCP normalization, 18–19
of UDP, 13–15
stateless backup, 531
stateless failover, 481
static ARP entries, clearing, 319
static command, 327
static NAT, 326, 331–334
static routes
configuring, 86–89
reachability, testing, 93–95
redistributing into OSPF, 114
removing, 88
SLA monitor process, configuring, 89–92
stealth firewalls, 312
sticky connections, 532
stratum, 581
structure of flash file system hierarchy, 195–196
stub routers, 126
subinterface number, 51–52
supported translation types on Cisco firewalls, 326–327
switch ports, configuring, 485
synchronizing time stamps on logging messages, 588
syntax errors, 31
Syslog, 19
firewall logs, collecting, 21–23
firewall throughput, checking, 639
messages
sending with TCP, 602
severity level 1 alerts, 799-802
severity level 2 critical messages, 802-803
severity level 3 error messages, 804-815
severity level 4 warning messages, 815-821
severity level 5 notifications, 821-827
severity level 6 informational messages, 827-837
severity level 7 debugging messages, 831-845
secure logging with SSL, 604–611
servers, optimizing, 589
viewing recent messages, 626–627
system execution space, 158, 169
features, 169–170
system messages, EMBLEM format, 588
system name (contexts), displaying, 176
system resources, checking, 627
failover performance, 646–655
firewall CPU load, 627–632
firewall interface throughput, 655–665
firewall memory usage, 633–636

firewall throughput, 638–645
inspection engine activity, 645–646
stateful inspection resources, 636–638

T

TACACS+ servers
authorizing user activity, 291–293
enable authentication support, 281
TCP
connections
monitoring, 711–716
embryonic connections, 18, 330–331
half-closed connections, 18
half-open connections, 17
ISNs, 331
MSS, configuring, 71
sending Syslog messages, 602
stateful inspection, 15–18
TCP normalization, 18–19
TCP intercept, 18
TCP normalization, 18
Telnet, accessing firewall user interface, 234
terminal screen width, adjusting, 34
terminal width command, 34
termination of TCP connections, 17
test crashinfo files, generating, 249
testing
address reachability, 91
connectivity
with ARP cache, 698–700
with ping packets, 695–696
IPv6 connectivity, 67–68
logging message generation, 615
reachability, 93–95
"testing mode", 480–481
TFTP server, saving running configuration to, 216–217
three-way handshakes, 15
throughput, checking, 638–645
time stamps, synchronizing on logging messages, 588
timed reactivation, 274
time-based ACEs, 356
time-exceeded messages (ICMP), permitting, 704
timers
CPU utilization, 629
Holdtime, setting, 491
idle uauth timer, 9
toggling failover roles, 655
topologies, 77–79
bypass links, 81–83
traceroute
disrupting, 705
performing on ASA, 703–705
verifying firewall connectivity, 700–703
traffic
capture sessions, enabling on VLAN inside switch chassis, 686– 689
classifying, 398–406
controlling
to/from medium-security interfaces, 349– 352
with ACLs, 348–349
shunning, 382–384
example, 384–386
traffic counters, checking firewall throughput, 640–643
traffic inspection, configuring on CSC SSM, 730–733
translation table size, checking, 636–637
translations
conditional, 335
dynamic NAT, configuring, 341–346
dynamic PAT, configuring, 342–346
identity NAT, configuring, 338–340
NAT exemption, configuring, 340–341
policy NAT, configuring, 335–338
static NAT, 331–334
xlate table entries
clearing, 717
timeout values, adjusting, 717–718
transmit ring, 76
transparent firewall mode, 312–314
ARP inspection, 314
interface support, 312
transparent firewalls
access lists, configuring, 321
ARP inspection, configuring, 319–321
configuring, 314–317
interface speed, configuring, 315
MAC address learning process, configuring, 318–319

management address, configuring, 317–319
non-IP protocol forwarding policy, configuring, 321–322
traps (SNMP), 255–256
triggering a firewall reload, 246–247
after specific time interval, 247–248
troubleshooting logging buffer content uploads to FTP server, 598
trunk link attributes, 46
trunks, displaying contents, 675–676
tuning OSPF, 110
Turbo ACLs
compiling, 352
recompiling, 353

U

uauth
absolute uauth timer, 9
verifying firewall connectivity, 720–722
UDP
Connections, monitoring, 711–716
stateful inspection, 13–15
unicast traffic, 126
unique MAC addresses, assigning to physical interfaces, 167–168
unlocking firewall features, 39
updating
AIP SSM license, 773–774
AIP SSM signature database file, 774–776
DDNS database, 121
upgrading
active-standby failover pair, 520–524
failover pair with AUS, 524
image files, 211
licenses, 39
activation keys, 40–41
operating system image, 205–210
uploading logging buffer contents to FTP, 598
UR (Unrestricted) license, 39
URL blocking, configuring on CSC SSM, 745–746
URL filtering, configuring on CSC SSM, 746–750
URLs, RFC Sourcebook, 787
user activity, generating audit trails, 245
user activity accounting, configuring, 300
user authentication. *See* uauth
user contexts, 158
user EXEC mode, 28
user interface
accessing
with console connection, 232–233
with SSH, 235, 237
with Telnet, 234
administrative sessions, monitoring, 244–245
command history, 32
commands
abbreviating, 30
editing, 30
entering, 29
context-based help, 31
regular expressions
operators, 33
searching for, 32–33
user interface modes, 28
configuration mode, 29
privileged EXEC mode, 28
user EXEC mode, 28
user management (Cisco firewalls)
with AAA servers, 272–280
administrative users, 280–287
end-user cut-through proxy, 287–301
generic users, 262
accounting, 263–264
authentication, 262–263
with local database, 264–265
accounting local user activity, 272
firewall command access, authorizing, 267–272
local user authentication, 265–267

V

VACL (VLAN ACLs), enabling traffic capture sessions, 688–689
verifying
address translation, 709–714
based on local addresses, 710
Auto Update client operation, 227
connections, 711–716
DDNS configuring, 123–124
downloadable ACLs, 299

failover communication, 647–650
failover roles, 646–647
firewall connectivity, 691–692
ACLs, 705–707
checking ARP cache, 698–700
checking routing table, 700
checking Uauth, 720–722
with Packet Tracer feature, 692–694
testing with ping packets, 695–696
with traceroute, 700–703
Flash memory system integrity, 199
IGMP multicast operation, 151–152
message logging activity, 614
packets passing through interfaces via capture sessions, 666–676
PIM multicast routing, 152–155
rip configuration, 96–97
viewing
active commands, 29
boot image setting, 201
buffered messages, 597
configured contexts, 174
context information, 191
context mode, 171
failover statistics, 508–513
firewall crash information, 250–251
list of firewall features, 34
priority queuing information, 77
running configuration, 214
startup configuration, 213–214
Syslog information, 626–627
virtual links, 109
virtual sensors, configuring on AIP SSM, 781–785
VLAN groups, defining on FWSM, 47
VLAN hopping, 79–80
preventing, 80–81
VLAN inline pair configuration, 781
VLAN number, assigning to logical interface, 52–53
VLANs
logical interfaces, 51–52
traffic, capturing inside switch chassis, 686–689
VPN users, 261

W

warning messages (syslog), 815-821
WCCPv2, 396–397
weighted least connections algorithm, 557
weighted round robin algorithm, 557
well-known port numbers, service contact port, 791
wildcards, specifying for ACLs, 355
write mem command, 42

X-Y-Z

xlate table, 6
entries, 325
clearing, 717
locating based on local addresses, 710
parameters, 6
verifying, 709–714
lookups, 7
size, checking, 636–637
timeout values, adjusting, 717–718

zero downtime upgrade, 479, 519