



Symbols & Numerics

? (question mark), displaying command help, 428

3-way handshakes, embryonic connections, 158

A

AAA (Authentication, Authorization, and Accounting)

- Cisco ASDM connections, configuring, 227
- external authentication server, configuring, 657–660
- serial console connections, configuring, 227
- server groups, specifying, 220–222
- server reactivation policies, 221
- supported protocols, 213–215
 - Active Directory*, 219
 - Kerberos*, 219
 - LDAP*, 219–220
 - Microsoft Windows NT*, 219
 - RADIUS*, 215–217
 - RSA SecurID*, 218–219
 - TACACS+*, 217–218

aaa accounting command, 235

abbreviating commands, 54

ABRs (Area Border Routers), 184

absolute time restrictions, 134–135

accessing

- ASDM, 613–614
- LogApp, 426

accounting

- configuring, 235
- RADIUS, configuring, 236–237
- TACACS+, configuring, 237

ACEs (access control entries), 117

- arguments, 121–123
- object groups, 127
 - defining*, 131–133
 - ICMP-type*, 130
 - network-based*, 129
 - protocol-based*, 128–129
 - service-based*, 129–130

ACLs (access control lists), 6, 117, 388, 645–646

- ACEs, 117
 - arguments*, 121–123
 - object groups*, 127–133
- advanced features, 126
- applying to interfaces, 124–125
- configuring, 121–124
- crypto ACLs, creating, 474
- downloadable, 136
- EtherType, 119
- extended, 119
- features of, comparing, 120
- inbound/outbound traffic filtering, 145–147
- inheritance rule, 484
- IPv6, 119
 - arguments*, 126
 - configuring*, 125–126
- monitoring, 149–152
- object groups, 127
 - defining*, 647–649
 - ICMP-type*, 130
 - network-based*, 129
 - protocol-based*, 128–129
 - service-based*, 129–130
- outbound, 118
- remarks, adding, 124
- standard, 119
- traffic filtering across site-to-site VPNs, 477–478
- WebVPN ACLs, 120, 561–564

active Cisco ASA, 347

Active Directory, 219

Active/Active failover, 352–353, 667

- active unit failover, specifying MAC address, 365
- asymmetric routing, 353–355
- configuring, 359–364
- multiple security context deployment, 371–374
- verifying operation, 376

Active/Standby failover, 351–352

- configuring, 355–359
- single mode deployment, 369–371

ActiveX content filtering, 137–138

adding

- remarks to ACLs, 124
- trusted hosts to AIP-SSM, 436–437
- user accounts to AIP-SSM, 434–435

address translation, 153, 649

- bypassing, 165
 - with Identity NAT, 166*
 - with NAT exemption, 166–167*
- dynamic NAT, configuring, 160–161
- dynamic PAT, configuring, 163–164
- exemption rules, 652–653
- monitoring, 172–173
- NAT, 154–155
 - order of operation, 167–168*
- packet flow sequence, 156–157
- PAT, 155–156
- policies, defining, 650
- policy NAT/PAT, configuring, 164–165
- static NAT, configuring, 157–159
- static PAT, configuring, 161–163
- static translation, 651

adjacencies, troubleshooting, 200–201**adjusting system clock**

- automatically, 73–74
- manually, 72

admin contexts, 293–294, 305–306**administrative distance, 177****administrative sessions**

- ASDM connections, authenticating, 227
- serial console connections, authenticating, 227
- SSH, authenticating, 225–227
- Telnet, authenticating, 224
- troubleshooting, 242–245

administratively down interfaces as failover trigger, 349**adminstrator account (AIP-SSM), 433–434****advanced features, 126**

- of ACLs, 127
 - ICMP-type object groups, 130*
 - network-based object groups, 129*
 - protocol-based object groups, 128–129*
 - service-based object groups, 129–130*
- of CIPS 5.x
 - custom signatures, 453–457*
 - IP logging, 457–460*
 - IPS tuning, 450–453*
 - shunning, 460–462*

of Cisco WebVPNs, 548

- ACLs, 561–564*
- e-mail proxy, 554–559*
- port forwarding, 549–551*
- URL mangling, 551–553*
- Windows file sharing, 559–561*

of remote-access VPNs

- client auto-update, 525–527*
- client firewalling, 527–528*
- hardware client NEM, 531*
- Individual User Authentication, 529–530*
- interactive hardware client authentication, 529*
- IP phone bypass, 530*
- IPSec hairpinning, 521–522*
- Leap bypass, 530*
- transparent tunneling, 519–521*
- VPN load balancing, 522–525*

AES (Advanced Encryption Standard), 469**AF (Assured Forwarding) DSCP, 387****aggressive mode (IPSec), 20, 483****AH (Authentication Header), 24–26****AIP-SSM (Adaptive Inspection and Prevention Security Services Module), 407, 421**

- administrator account, 433–434
- initializing, 429–433
- LED indicators, 408
- logging into via CIPS 5.x CLI, 427–428
- management interface port, 408–409
- operator account, 434
- promiscuous mode, traffic flow, 411–412
- recovery parameters, configuring, 414–415
- service account, 434
- trusted hosts, adding, 436–437
- user accounts, adding/deleting, 434–435
- viewer account, 434

alarms, false positives, 12, 417**algorithms, heuristic 12****allocating interfaces for security contexts, 304–305****Analysis Engine Configuration Module, 424****anomaly-based analysis, 13****application inspection**

- case study, 767–768
- configuring, 660–664
- CTIQBE, 252–253
- deployment scenarios, 285
- DNS inspection, 253–254

- ESMTP inspection, 254–256, 286
- FTP inspection, 256–258, 288–289
- GTP inspection, configuring, 262–263
- H.323 inspection, 263–266
 - control-signaling methods*, 267–268
 - enabling*, 267
- HTTP inspection, 268–275, 287–288
 - enabling*, 269–271
- ICMP inspection, 276
- ILS inspection, 276
- MGCP inspection, 277–279
- NetBIOS inspection, 279
- policies, provisioning, 248–249
- PPTP inspection, 279
- RPC inspection, 280
- RSH inspection, 280
- RTSP inspection, 280–281
- selecting traffic for inspection, 250–252
- SIP inspection, 281–282
- Skinny inspection, 282–284
- SNMP inspection, 284
- SQL*Net inspection, 284
- TFTP inspection, 284
- XDMCP inspection, 285
- application layer, content filtering, 137**
 - ActiveX filtering, 138
 - configuring, 138–139
 - Java filtering, 138
- application proxies, 7–8**
- applying**
 - ACLs to interfaces, 124–125
 - crypto maps to interfaces, 476–477
 - policy maps to interface, 394
 - service packs/signature updates to CIPS 5.x, 437–441
- architectural overview of CIPS 5.x**
 - AuthenticationApp, 425
 - cipsWebserver, 425
 - EventStore, 426–427
 - LogApp, 426
 - MainApp, 422–423
 - NAC, 424
 - SensorApp, 423–424
 - TransactionSource, 427
- areas, 184**
 - stub areas, configuring, 192–193
- arguments, ntp command, 74**
- ARP (Address Resolution Protocol)**
 - gratuitous ARP, 364
 - testing, 349
- ASBRs (Autonomous System Boundary Routers), 185**
 - configuring Cisco ASA as, 191–192
- ASDM (Adaptive Security Device Manager), 611**
 - accessing, 613–614
 - Configuration screen, 622–623
 - connections, authenticating, 227
 - file management, 634
 - File menu options, 629
 - image, loading, 612
 - initial setup, 615–616
 - interface management, 625–626
 - logging, 107
 - Monitoring screen, 624–625
 - remote management
 - via SSH*, 631–632
 - via SSL*, 632–633
 - via Telnet*, 630–631
 - running configuration, 628–629
 - setting up, 611
 - SNMP, configuring, 641–643
 - Startup Wizard, 616
 - launching*, 617
 - sub-interfaces, creating, 626
 - system clock, configuring, 627–628
 - system image files, installing, 633–634
 - system logging, 635–641
 - uploading software, 611–612
- VPNs**
 - monitoring*, 745–746, 748
 - remote-access IPSec VPNs, configuring*, 721–731
 - site-to-site VPNs using PKI, configuring*, 713–720
 - site-to-site VPNs using preshared keys, configuring*, 706–713
 - statistics, displaying*, 746–747
 - WebVPN, configuring*, 731–745
- assigning**
 - device names, 58–59
 - IPv6 addresses, 70–71
 - auto-configuration addresses*, 72
 - global addresses*, 70
 - link-local addresses*, 71
- asymmetric routing, 353–355**

attributes

- of mode-config user policies, 504–505
- of security contexts, 292

authentication

- cut-through proxy authentication, deploying, 240–242
- of ASDM administrative sessions, 227
- of firewall sessions, 227–229
 - exceptions, configuring, 230–231*
- of serial console connections, 227
- of SSH administrative sessions, 225–227
- of Telnet administrative sessions, 224
- OSPF configuration, 189–190
- prompts, customizing, 231–232
- RIP, configuring, 180–181
- timeouts, customizing, 231

authentication servers, defining, 220–224**AuthenticationApp, 425****authorization**

- command authorization, configuring, 233–234
- downloadable ACLs, configuring, 234–235

auth-prompt command, 231–232**auto-configuration IPv6 addresses, assigning, 72****automatic IP logging, 457****automatically adjusting system clock, 73–74****AYT (“Are you there”) messages, 527****B****backup configuration files, creating for CIPS 5.x, 444–445****blind hijacking, 18****blocked multicast/broadcast packets, troubleshooting RIP, 182–183****blocking, 460–462****branch office deployment, case study, 751–755****broadcast ping tests, 349****buffer block sizes, 114****buffer overflows, 13****buffered logging, 104–106****burst size, configuring, 393****bypassing**

- address translation, 165
 - Identity NAT, 166*
 - NAT exemption, 166–167*
- CRL checking, 589

C**cached credentials, deleting, 231****captured packets, displaying, 151****CAs (certificate authorities), 577–578**

- manual enrollment, 585–588

case studies

- application inspection, 767–768
- branch office deployment, 751–755
- data center security, 769–775
- large enterprise network deployment, 757–758
 - DMZ, 759–762*
 - Internet edge, 759–762*
- remote-access VPN clusters, 763–764
 - master ASA, 765–767*
- small business deployment, 755–757
- URL filtering, Websense servers, 762–763

certificates, 22, 576

- CAs, 577–578
 - manual enrollment, 585–588*
- Cisco VPN client IPSec connection
 - termination, configuring, 596–602
- CRLs, 578–579
 - configuring, 588–591*
- enrolling Cisco ASA to CA server, 579–580
 - trustpoints, 580–585*
- IPSec site-to-site VPNs, configuring, 591–595
- SCEP, 579

CIPS (Cisco Intrusion Prevention Software) 5.x

- backup configuration files, creating, 444–445
- CLI
 - configuration mode, 428*
 - logging into AIP-SSM, 427–428*
- components of, 421
 - AuthenticationApp, 425*
 - cipsWebserver, 425*
 - EventStore, 426–427*
 - LogApp, 426*
 - MainApp, 422–423*
 - NAC, 424*
 - SensorApp, 423–424*
 - TransactionSource, 427*

- configuration information, displaying, 442–443
- custom signatures, 453–457
- IP logging, 457–460
- IPS tuning, 450–453
- service packs, applying, 437–441
- shunning, 460–462
- software version, displaying, 441
- statistics, displaying, 446–449
- cipsWebserver, 425**
- Cisco 4200 Series Sensors, 32**
- Cisco all-in-one solution, 33–34**
 - firewall services, 34
 - IPS services, 34–35
 - VPN services, 35
- Cisco ASDM. *See* ASDM (Adaptive Security Device Manager)**
- Cisco Easy VPN Client, configuring, 513**
 - hardware-based, 517–519
 - software-based, 514–516
- Cisco firewall products**
 - Cisco FWSM, 32
 - Cisco IOS Firewalls, 32
 - Cisco PIX Firewalls, 31–32
- Cisco IDS products, 32–33**
- Cisco IPSec remote-access VPN solutions**
 - bypass NAT, 511–512
 - CiscoEasy VPN Client configuration, 513
 - hardware-based, 517–519*
 - software-based, 514–516*
 - configuring, 500
 - dynamic crypto maps, configuring, 509–510
 - IP addresses, assigning, 507–508
 - IPSec policy, defining, 509
 - ISAKMP policy, creating, 502
 - ISAKMP preshared keys, configuring, 506
 - ISAKMP, enabling, 501
 - remote-access attributes, configuring, 502–505
 - split tunneling, 512–513
 - traffic filtering, configuring, 510–511
 - tunnel default gateway, 511
 - tunnel type, defining, 505–506
 - user authentication, configuring, 506–507
- Cisco PIX Firewalls, 31–32**
- Cisco VPN products, 33**
- Cisco WebVPN, 541**
 - advanced features, 548
 - ACLs, 561–564*
 - e-mail proxy, 554–559*
 - port forwarding, 549–551*
 - URL mangling, 551–553*
 - Windows file sharing, 559–561*
 - configuring, 543–548
 - deployment scenarios, 564
 - group attributes, configuring, 546–548
 - monitoring, 569–570
 - troubleshooting, 570–573
 - user authentication, configuring, 548
 - versus Cisco VPN client solution, 542–543
 - with e-mail proxy, deployment scenario, 567–568
 - with external authentication, deployment scenario, 565–566
- class map command, 413**
- class maps, 249**
 - QoS configuration, 390–393
- class selector DSCP, 387**
- class-default command, 393**
- classifying traffic. *See* traffic classification**
- class-map command, 390**
- clear aaa-server statistics command, 224**
- clear configure aaa-server command, 224**
- clear configure all command, 81**
- clear configure context command, 307**
- clear configure isakmp command, 80**
- clear configure rip command, 179**
- clear uauth command, 231**
- clearing**
 - CIPS 5.x statistics, 446–449
 - events, 445–446
- CLI (command-line interface), 52–54**
 - configuration mode, 428
 - logging into AIP-SSM, 427–428
- client auto-update, 525–527**
- client firewalling, 527–528**
- clock set command, 72**
- clock summer-time command, 75**
- clock timezone command, 74**
- colon-hexadecimal notation, 69**
- command authorization, configuring, 233–234**
- commands**
 - aaa accounting, 235
 - abbreviating, 54

- auth-prompt, 231–232
- class map, 413
- class-default, 393
- class-map, 390
- clear aaa-server statistics, 224
- clear configure aaa-server, 224
- clear configure all, 81
- clear configure context, 307
- clear configure isakmp, 80
- clear configure rip, 179
- clear uauth, 231
- clock set, 72
- clock summer-time, 75
- clock timezone, 74
- configure terminal, 53
- content-length, 270
- content-type-verification, 271
- debug ospf, 200
- failover interface-policy, 365
- failover lan interface, 358
- filter, 143
- help mode, invoking, 428
- hw-module module, 414
- inspect dns, 254
- inspect esmtp, 255
- inspect skinny, 283
- ip audit, 416
- ip audit signature, 417
- management-only, 330
- max-header-length, 271–272
- max-uri-length, 272
- mode multiple, 299
- nat-control, 165–166
- neighbor, 195
- NTP, arguments, 74
- police, 393
- policy-map, 413
- port-misuse, 272
- request-method, 273–275
- route, 175
- set, 93
- setup, 429–433
- show aaa-server, 244
- show aaa-server protocol, 222
- show access-list, 149–152
- show capture, 151
- show clock, 73
- show configuration, 442–443

- show conn, 150, 418
- show events, 445–446
- show failover, 374
- show firewall, 330
- show local-host, 173
- show logging, 378–379
- show module, 409, 415
- show ntp status, 74
- show ospf, 196
- show ospf interface, 197
- show route, 176, 199
- show running-config aaa-server, 223
- show running-config command, 76–79
- show service-policy, 251, 401
- show shun, 418
- show snmp-server statistics, 112
- show ssh sessions, 87–88
- show startup-config, 79–80
- show statistics, 446
- show uauth, 245
- show url-server statistics, 152–153
- show version, 441
- shun, 418
- strict-http, 270
- telnet, 82–83
- timeout uauth, 231
- transfer-encoding type, 275
- url-server, 141
- username attributes, 504
- write memory, 80

comparing

- ACL features, 120
- CIPS 5.x and CIDS 4.x, 421
- IPSec security protocols, 26
- routed and transparent firewalls, 322–323

configuration files

- running configuration, 76–79
 - managing on ASDM*, 628–629
- startup configuration, 79–81

configuration mode (CIPS 5.x CLI), 53, 428**Configuration screen (ASDM), 622–623****configuration URL (security contexts),
specifying, 302–304****configure terminal command, 53****configuring**

- AAA server groups, 220–222
- accounting, 235

- ACLs
 - standard*, 133
 - time-based*, 133–135
- address translation
 - dynamic NAT*, 160–161
 - dynamic PAT*, 163–164
 - policy NAT/PAT*, 164–165
 - static NAT*, 157–159
 - static PAT*, 161–163
- AIP-SSM recovery parameters, 414–415
- application inspection, 660–664
- ASDM
 - system clock*, 627–628
 - system logging*, 635–641
- Cisco IPSec remote-access VPN solutions
 - CiscoEasy VPN Client*, 500, 513–519
 - bypass NAT*, 511–512
 - dynamic crypto maps*, 509–510
 - IP addresses, assigning*, 507–508
 - IPSec policy, defining*, 509
 - ISAKMP policy, creating*, 502
 - ISAKMP preshared keys*, 506
 - ISAKMP, enabling*, 501
 - remote-access attributes*, 502–505
 - split tunneling*, 512–513
 - traffic filtering*, 510–511
 - tunnel default gateway*, 511
 - tunnel type, defining*, 505–506
 - user authentication*, 506–507
- Cisco WebVPN, 543–548
 - group attributes*, 546–548
 - user authentication*, 548
- command authorization, 233–234
- content filtering, 138–139
- CRLs, 588–591
- DNS doctoring, 170–172
- downloadable ACLs, 234–235
- external authentication server, 657–660
- failover
 - Active/Active*, 359–364
 - Active/Standby*, 355–359
 - groups*, 361
 - interface policy*, 365
 - interface polltime*, 366
- firewall session authentication exceptions, 230–231
- GTP inspection, 262–263
- interfaces during initial setup, 59–62
- IP multicast, 204–207
 - static multicast routes*, 207
- IPv6, 70
 - auto-configuration addresses*, 72
 - global addresses*, 70–71
 - link-local addresses*, 71
- multicast routing, 656
- OSPF, 185–187, 654–655
 - ASBRs*, 191–192
 - authentication*, 189–190
 - neighbors*, 195–196
 - stub areas*, 192–193
 - type 3 LSA filtering*, 193–194
 - virtual links*, 187–189
- packet filtering, ACLs, 120–126
- policy maps, burst size, 393
- QoS, 389, 671–674
 - class maps*, 390–393
 - DSCP-based policy*, 674–676
 - policy maps*, 393–395
- RADIUS, accounting, 236–237
- RIP, 179–180, 654
 - authentication*, 180–181
- security contexts, 299–301
 - admin context*, 305–306
 - configuration URL*, 302–304
 - customer context*, 306–307
 - interface allocation*, 304–305
 - system execution space*, 301–302
- SNMP, 110–112
- SSH, 85–89
- static routes, 175–178
- subinterface during initial setup, 63–64
- system clock
 - automatic clock adjustment*, 73–74
 - DST*, 75
 - manual clock adjustment*, 72
 - time zone*, 74–75
- TACACS+, accounting, 237
- transparent firewalls, 328–330
 - ARP inspection*, 333–334
 - interface ACLs*, 331–332
 - IP address*, 330–331
 - L2F table parameters*, 334
- trustpoints, 580–585

- URL filtering, 141–143
 - filtering servers, 142–144*
 - long URL support, 144–145*
- VPNs
 - remote-access IPSec VPNs, 721–731*
 - site-to-site VPNs using PKI, 713–720*
 - site-to-site VPNs using preshared keys, 706–713*
 - WebVPN, 731–745*
- connection entries, displaying, 150**
- connections**
 - setting maximum limits, 159
 - shunning, 417–418
- console logging, 104**
- console port, 49**
 - connecting to PC, 50
 - HyperTerminal connection, establishing, 50–52
- content filtering, 137, 649. *See also* URL filtering**
 - ActiveX filtering, 138
 - configuring, 138–139
 - Java filtering, 138
 - monitoring, 152–153
 - Websense servers, deploying, 147–148
- content-length command, 270**
- content-type-verification command, 271**
- control signaling methods for H.323, 267–268**
- CoS (class of service), 383–384**
- CPP (Centralized Protection Policy), 528**
- CPU utilization, 113–115**
- creating**
 - CIPS 5.x backup configuration files, 444–445
 - custom signatures, 453–457
 - ISAKMP policy, 471
 - security contexts, 665
 - subinterfaces on ASDM, 626
 - traffic classes, 390
 - user accounts on AIP-SSM, 435
- CRL checking, bypassing, 589**
- CRLs (certificate revocation lists), 578–579**
 - configuring, 588–591
 - troubleshooting retrieval problems, 606
- crypto access lists, creating, 474**
- crypto maps**
 - applying to interface, 476–477
 - configuring, 475–476
- CSA (Cisco Security Agent), 32**
- CS-MARS (Cisco Security Monitoring, Analysis and Response System), 769**

- CTIQBE inspection, 252–253**
- custom signatures, creating, 453–457**
- customer contexts, 294–295, 306–307**
- customizing**
 - authentication prompts, 231–232
 - authentication timeouts, 231
- cut-and-paste CA enrollment, 585–588**
- cut-through proxy authentication, deploying, 240–242**

D

- Daemen, Joan, 469**
- data center security, case study, 769–775**
- data rule inheritance, 484**
- DDoS attacks, 17–18**
- debug failover messages, enabling, 377**
- debug ospf command, 200**
- debugging IP multicast, 208–209**
- defining**
 - ACEs, object groups, 131–133
 - ACLs, 122–123
 - authentication servers, 220–224
 - interesting traffic for IPSec site-to-site VPNs, 474–475
 - NAT/PAT policies, 650
 - static translation, 651*
 - object groups, 647
 - OSPF neighbors, 195–196
- deleting**
 - cached credentials, 231
 - user accounts on AIP-SSM, 434–435
- dense mode (PIM), 203**
- depletion mode, AAA server reactivation, 221**
- deploying**
 - ACLs for inbound/outbound traffic filtering, 145–147
 - cut-through proxy authentication, 240–242
 - IP multicast, 211
 - OSPF, 209–210
 - QoS
 - for remote-access VPN tunnels, 398–401*
 - for VoIP traffic, 395–398*
 - site-to-site VPNs
 - fully-meshed topology with RRI, 488–492*
 - single tunnel configuration using NAT-T, 485–487*

- TACACS+ for administrative sessions, 238–240
- transparent firewalls, 334
 - MMTF with security contexts*, 336–341
 - SMTF*, 335–336
- virtual firewalls
 - with shared interface*, 312–316
 - with two customer contexts*, 308–312
- Websense servers for content filtering, 147–148
- device names, assigning, 58–59**
- deviceInfo.cfg file, 615**
- DHCP services, configuring during initial setup, 65–67**
- digital certificates, 576**
 - CAs, 577–578
 - CRLs, 578–579
 - enrolling Cisco ASA to CA server, 579–580
 - manual enrollment*, 585–588
 - trustpoints*, 580–585
 - SCEP, 579
- Dijkstra algorithm, 183**
- disabling**
 - IPS signatures, 452–453
 - ISAKMP aggressive mode, 483
 - password recovery process, 97–100
- displaying**
 - AAA server running configuration, 223
 - captured packets, 151
 - CIPS 5.x configuration information, 442–443
 - CIPS 5.x software version, 441
 - CIPS 5.x statistics, 446–449
 - connection entries, 150
 - events, 445–446
 - IP logger statistics, 449
 - IP multicast configuration information, 208
 - OSPF database information, 199
 - OSPF neighbor information, 197
 - running configuration, 77–79
 - startup configuration, 79–80
 - stateful failover statistics, 375
 - VPN statistics on ASDM GUI, 746–747
- distance-vector routing protocols, RIP, 178**
 - blocked multicast/broadcast packets, troubleshooting, 182–183
 - configuring, 179–181
 - mismatched authentication, troubleshooting, 182
 - mismatched version, troubleshooting, 181–182
 - verifying configuration, 181
- DIT (Directory Information Tree), 220**
- DMZs (demilitarized zones), 9**
- DNs (distinguished names), 220**
- DNS doctoring, 169–172**
- DNS inspection, 253–254**
- DoS attacks, 14**
 - Land.c attacks, 16
 - smurf attacks, 16
 - TCP SYN flood attacks, 15
- double colon notation, 69**
- downloadable ACLs, 136**
 - configuring, 234–235
- DSCP (Differentiated Services Code Point), 386–388**
- DSCP-based QoS policy, configuring, 674–676**
- DST (daylight savings time), system clock configuration, 75**
- dynamic NAT, configuring, 160–161**
- dynamic PAT, configuring, 163–164**

E

- EF (Expedited Forwarding) DSCP, 387**
- e-mail logging, 107**
- e-mail proxy, 554–559**
- embryonic connections, 158**
- enabling**
 - debug failover messages, 377
 - event logging, 102–103
 - ASDM logging*, 107
 - buffered logging*, 104–106
 - console logging*, 104
 - e-mail logging*, 107
 - syslog server logging*, 108
 - terminal logging*, 104
 - failover logging, 378
 - H.323 inspection, 267
 - HTTP inspection, 269–271
 - security context, 299–301
- enrolling Cisco ASA to CA server, 579–580**
 - manual enrollment*, 585–588
 - trustpoints*, 580–585
- erasing startup configuration, 81**

ESMTP (Extended SMTP) inspection, 254–256, 286

ESP (Encapsulation Security Payload), 25–26

**establishing HyperTerminal connection to
console port, 50–52**

EtherType ACLs, 119

event logging, 101. *See also* events

- ASDM logging, 107
- buffered logging, 104–106
- console logging, 104
- e-mail logging, 107
- enabling, 102–103
- severity levels, 101–102
- syslog server logging, 108
- terminal logging, 104

events

- displaying, 445–446
- failover triggers, 348–349

EventStore, 426–427

**exemption rules for address translation,
652–653**

extended ACLs, 119

**external authentication servers,
configuring, 657–660**

external filtering servers, 140

external groups, 503

F

fail-open, 768

failover, 667

- Active/Active, 352–353
 - asymmetric routing, 353–355*
 - configuring, 359–364*
 - multiple security context deployment,
371–374*
- Active/Standby, 351–352
 - configuring, 355–359*
 - single mode deployment, 369–371*
- debug messages, enabling, 377
- detection, testing, 349
- groups
 - configuring, 361*
 - mapping to security contexts, 362*
- hardware/software requirements, 351
- implementing, 668–670
- interface policy, configuring
- interfaces, 365–366

- logging, enabling, 378

- monitoring, 374–377

- specifying standby/active unit MAC addresses,
364–365

- stateful, 350

 - replicated traffic, 350–351*

- timing issues, troubleshooting, 378

- triggers, 348–349

- troubleshooting, 377

- zero-downtime software upgrades, performing,
367–369

failover control link, 347

failover interface-policy command, 365

failover lan interface command, 358

false positives, 12, 417

FastConnect H.323 feature, 264

features of ACLs, comparing, 120

fields of IPv6 header, 68–69

File menu options (ASDM), 629

filter command, 143

filtering type 3 LSAs, 193–194

filtering servers, configuring, 142–144

firewall session authentication, 227–229

- exceptions, configuring, 230–231

firewalls

- network-based, 5–6

- packet filtering, 6

- personal firewalls, 5, 10

- routed, 321

- stateful inspection, 9

- transparent

 - and VPNs, 327–328*

 - comparing with routed firewalls,
322–323*

 - configuring, 328–334*

 - deployment scenarios, 334–341*

 - MMTF, 326–327, 336–341*

 - monitoring, 341–342*

 - single-mode, 323*

 - SMTF, 336*

 - troubleshooting, 342–344*

FoIP (Fax over IP), 268

FTP filtering, configuring, 143

FTP inspection, 256–258, 288–289

G

gatekeepers, 263
gateways, 263
GET-NEXT messages (SNMP), 109
global configuration mode (CIPS 5.x), 428
global IPv6 addresses, configuring, 70–71
GPRS (General Packet Radio Service), 258.
 See also GTP
gratuitous ARP, 364
group attributes, 503
GTP (GPRS Tunneling Protocol), 258–259
 application inspection, 262–263
 GTPv0, 259–260
 GTPv1, 260–261

H

H.323 protocol suite, 263–265
 application inspection, 263–266
 control-signaling methods, 267–268
 enabling, 267
 FastConnect H.323 feature, 264
 FoIP, 268
hairpinning, Easy VPN and firewalling
 deployment scenario, 531–534
hardware client NEM, 531
hardware requirements for failover, 351
hardware-based VPN clients, configuring,
 517–519
header fields (IPv6), 68–69
heuristic scanning, 12
hop count, 178
host-based intrusion detection systems, 13–14
HTTP filtering, configuring, 143
HTTP inspection, 268, 287–288
 enabling, 269–275
hw-module module command, 414
HyperTerminal, establishing connection with
 console port, 50–52

I

ICMP filtering, 136–137
ICMP inspection, 276

ICMP-type object groups, 130
IDCONF (Intrusion Detection Configuration)
 protocol, 424
Identity NAT, 166
IDSM-2 (IDS Services Module-2), 33
IDSs (intrusion detection systems), 10–11
 host-based, 13–14
 network-based, 11
 anomaly-based analysis, 13
 heuristic-based analysis, 12
 pattern-matching, 11
 protocol analysis, 12
 stateful pattern-matching, 12
 NIDS, protocol analysis, 12
IGMP (Internet Group Multicast Protocol), 203
 configuration information, displaying, 208
 query timeouts, configuring, 205
IKE (Internet Key Exchange), 20
 Phase 1, 20–22
 Phase 2, 22–24
ILS (Internet Locator Service) inspection, 276
image upgrades. performing zero-downtime
 software upgrades, 367–369
images, upgrading via Cisco ASA CLI, 89–92
implementing failover, 668–670
inbound NAT, TCP intercept, 159
inbound/outbound traffic filtering, ACLs,
 145–147
Individual User Authentication feature, 529–530
inheritance, 484, 502
initial setup
 of ASDM, 615–616
 of ASA, 56
 device name, 58–59
 DHCP services, configuring, 65–67
 interface configuration, 59–62
 management interfaces, configuring, 65
 parameters, 57–58
 subinterface configuration, 63–64
initializing AIP-SSM, 429–433
Inline IPS mode, 410
inside NAT, 154
inspect dns command, 254
inspect esmtp command, 255
inspect skinny command, 283
inspection policies, provisioning, 248–249
installing ASDM system image files, 633–634
interactive hardware client authentication, 529

interesting traffic, defining, 474–475**interface polltime, failover configuration, 366****interfaces**

- ACLs, applying, 124–125
- administratively down, as failover trigger, 349
- allocating for security contexts, 304–305
- configuring, 59–62
- failover detection, testing, 349
- managing on ASDM, 625–626
- monitoring during failover, 366
- policies, failover configuration, 365

internal groups, 503**invoking command help, 428****IP address notation, 69****ip audit command, 416****IP audit feature, 416–417****ip audit signature command, 417****IP flow-based packet classification, 388****IP logging, 457–460**

- statistics, displaying, 449

IP multicast

- configuration information, displaying, 208
- configuring, 204–207
- debugging, 208–209
- deploying, 211
- IGMP, 203
- troubleshooting, 207

IP phone bypass feature, 530**IP precedence field, 385–386****IP routing**

- RIP, 178–181
- static routes
 - configuring, 175–178*
 - redistribution, 178*

IPSec, 19–20

- AH, 24–26
- ESP, 25
- hairpinning, 521–522
- IKE, 20
 - Phase 1, 20–22*
 - Phase 2, 22–24*
- over TCP, 520–521
- over UDP, 521
- quick mode, 23

remote-access VPNs

- deployment scenarios, 531–537*
- monitoring, 537–539*
- troubleshooting, 539–541*

site-to-site VPNs

- advanced Cisco ASA features, 479–482*
- configuring with certificates, 591–595*
- crypto maps, applying to interface, 476–477*
- crypto maps, configuring, 475–476*
- fully-meshed topology with RRI, 488–492*
- interesting traffic, defining, 474–475*
- ISAKMP attributes, 468*
- ISAKMP keepalives, 484–485*
- ISAKMP policies, defining, 471–473*
- ISAKMP preshared keys, configuring, 472*
- ISAKMP, enabling, 470*
- mismatched preshared keys, troubleshooting, 496*
- monitoring, 492–494*
- NAT, bypassing, 478*
- PFS, 482*
- preconfiguration checklist, 467–469*
- SA lifetimes, 483*
- single tunnel configuration using NAT-T, 485–487*
- traffic filtering, 477–478*
- troubleshooting, 494–496*
- tunnel type, setting, 471–472*

transform sets, 473**transport mode, 27****tunnel mode, 28****IPSs (intrusion prevention systems)****features**

- IP audit, 416–417*
- shunning, 417–418*
- inline IPS mode, traffic flow, 410
- management, 769
- signatures
 - disabling, 452–453*
 - retiring, 452–453*
- tuning, 450–453

IPv6, 68**ACLs, 119**

- arguments, 126*
- configuring, 125–126*

address assignment, 70–71

- auto-configuration addresses, assigning, 72
- configuring, 70
- global addresses, configuring, 70–71
- header fields, 68–69
- link-local addresses, configuring, 71

ISAKMP

- aggressive mode, disabling, 483
- enabling, 470
- keepalives, 484–485
- policies, creating, 471

J-K-L

Java filtering, 137–138

Kerberos, 219

Land.c attacks, 16

large enterprise network deployment case study, 757–758

- DMZ, 759–762

- Internet edge, 759–762

launching ASDM Startup Wizard, 617

LDAP (Lightweight Directory Access Protocol), 219–220

Leap bypass feature, 530

licenses, managing, 54–56

link up/down tests, 349

link-local IPv6 addresses, configuring, 71

link-state routing protocols, OSPF, 183

- ABRs, 184
- adjacencies, troubleshooting, 200–201
- configuring, 185–193
- deploying, 209–210
- mismatched areas, troubleshooting, 202
- mismatched authentication, troubleshooting, 202
- neighbors, configuring, 195–196
- type 3 LSA filtering, 193–194
- virtual links, troubleshooting, 202

LLQ (low-latency queuing), 383–384

load balancing and site-to-site integration, remote-access VPN deployment scenario, 534–537

loading ASDM image, 612

LogApp, 426

logging, 101

- ASDM logging, 107
- buffered logging, 104–106
- console logging, 104
- e-mail logging, 107
- failover messages, 378
- enabling, 102–103
- SNMP, ASDM configuration, 641–643
- syslog, 108
 - ASDM configuration, 635–641*
 - parameters, 108*
- terminal logging, 104

logging into AIP-SSM, 427–428

long URL support, configuring, 144–145

lost passwords

- disabling ability to recover, 97–100
- recovering, 93–96

LSAs (link-state advertisements), 183

- type 3, filtering, 184, 193–194
- type 7, 193

M

MAC addresses of active/standby failover units, specifying, 364–365

main mode (IPSec), 20

MainAPP, 422–423

management interface port (AIP-SSM), 408–409

management interfaces, configuring during initial setup, 65

management-only command, 330

managing

- licenses, 54–56
- security contexts, 307

man-in-the-middle attacks, 18

manual IP logging, 458

manually adjusting system clock, 72

manually enrolling Cisco ASA to CA server, 585–588

mapping failover groups to security contexts, 362

master blocking sensors, 424

max-header-length command, 271–272

maximum limits on connections, setting, 159

max-uri-length command, 272

MBZ (must be zero), 385

MCUs (multipoint control units), 263

MD5 authentication, OSPF configuration, 189–190**memory**

- buffer block sizes, 114
- usage, monitoring, 113–115

messages, SNMP PDUs, 109**MGCP inspection, 277–279****Microsoft Windows NT, 219****mismatched proxy identities, troubleshooting on****IPSec site-to-site VPNs, 497****mismatched RIP authentication, troubleshooting, 182****mismatched RIP version, troubleshooting, 181–182****mismatched time and date on PKI, troubleshooting, 602–605****MMTF (multi-mode transparent firewalls)**

- deploying, 336–341
- packet flow, 326–327

mode multiple command, 299**mode-config, 500**

- configurable attributes, 504–505

monitoring, 113–115

- ACLs, 149–152
- address translation, 172–173
- ASDM system logs, 639
- Cisco remote-access IPSec VPNs, 537–539
- content filtering, 152–153
- CPU utilization, 113–115
- failover, 366, 374–377
- memory usage, 113–115
- QoS, 401–403
- security contexts, 316–317
- site-to-site VPNs, 492–494
- transparent firewalls, 341–342
- VPNs on ASDM, 745–748
- WebVPN, 569–570

Monitoring screen (ASDM), 624–625**multicast groups, statically assigning, 204****multicast routing**

- configuring, 204–207, 656
- RPs, specifying, 657
- troubleshooting, 207

multimode virtual firewall topology, deploying, 308–312**multiple security context Active/Active failover deployment, 371–374****multiple security context mode, 292**

- admin context, 293–294
- converting to single mode, 301
- customer context, 294–295
- packet classification, 295–296
- packet flow, 295
- packet forwarding, 296
 - with shared interface, 298–299*
 - without shared interface, 297–298*
- system execution space, 292–293

N

N2H2 servers, 140**NAC (Network Access Controller), 424****NASs (network access servers), 215****NAT (Network Address Translation), 7, 154–155**

- dynamic NAT, configuring, 160–161
- exempting site-to-site VPN traffic, 478
- order of operation, 167–168
- policies, defining, 650–651
- policy NAT, configuring, 164–165
- static NAT, 8–9
 - configuring, 157–160*

NAT exemption, 166

- exemption rules, 652–653

NAT-T (NAT Traversal), 481, 519**nat-control command, 165–167****neighbor command, 195****neighbors (OSPF), defining, 195–196****NEM (Network Extension Mode), 518**

- hardware-client NEM, 531

NetBIOS inspection, 279**network activity tests, 349****network-based attacks**

- DDoS attacks, 17–18
- DoS attacks, 14
 - Land.c attacks, 16*
 - smurf attacks, 16*
 - TCP SYN flood attacks, 15*
- session hijacking, 18

network-based firewalls, 5–6

network-based IDSs, 11
 anomaly-based analysis, 13
 heuristic-based analysis, 12
 pattern-matching, 11
 protocol analysis, 12
 stateful pattern-matching, 12
network-based object groups, 129
new pin mode, 218
NIDS (network-based intrusion detection systems), protocol analysis, 12
NSSAs (not-so-stubby areas), 193
NTP (Network Time Protocol), configuring system clock, 73–74
ntp command arguments, 74

O

object groups, 127
 defining, 647
 ICMP-type, 130
 network-based, 129
 protocol-based, 128–129
 service-based, 129–130
one-time upgrades, performing on CIPS 5.x, 438–439
operator account (AIP-SSM), 434
OSPF (Open Shortest Path First), 183
 ABRs, 184
 adjacencies, troubleshooting, 200–201
 ASBRs, configuring, 191–192
 authentication, configuring, 189–190
 configuring, 185–187, 654–655
 deploying, 209–210
 LSAs
 type 3 filtering, 184, 193–194
 type 7, 193
 mismatched areas, troubleshooting, 202
 neighbors, defining, 195–196
 stub areas, configuring, 192–193
 troubleshooting, 196–199
 virtual links, configuring, 187–189
OTPs (one-time passwords), RSA SecureID, 218
outbound ACLs, 118
outside NAT, 155
outside static NAT entries, configuring, 160

P

packet classification, 385
 ACLs, 388
 DSCP, 386–388
 in multiple context mode, 295–296
 IP flow-based, 388
 IP precedence field, 385–386
 VPN tunnel groups, 388–389
packet filtering. *See also* content filtering; URL filtering
 ACLs, 6, 117, 645–646
 advanced features, 126
 applying to interfaces, 124–125
 configuring, 121, 123–126
 downloadable, 136
 EtherType, 119
 extended, 119
 features of, comparing, 120
 IPv6, 119
 monitoring, 149–152
 object grouping, 127–130, 647–649
 on outbound traffic, 118
 remarks, adding, 124
 standard, 119, 133
 time-based, 133–135
 WebVPN, 120
 configuring, 120
 ICMP filtering, 136–137
packet flow
 during address translation, 156–157
 in multiple context mode, 295
 through QoS-configured security appliance, 384–385
packet forwarding in multiple context mode, 296
 with shared interface, 298–299
 without shared interface, 297–298
parameters for initial Cisco ASA setup, 57–58
passwords
 changing, 435–436
 disabling recovery ability, 97–100
 recovering, 93–96
PAT (Port Address Translation), 7–8, 155–156
 dynamic PAT, configuring, 163–164
 exemption rules, 652–653
 policies, defining, 650–651
 policy PAT, configuring, 164–165
 static PAT, configuring, 161–163

- pattern matching, 11
- PCs, connecting to console port, 50
- PDU (protocol data units), 109
- performing zero-downtime software upgrades, 367–369
- periodic time restrictions, 135
- personal firewalls, 5, 10
- PFS (Perfect Forward Secrecy), 482
- piggyback HTTPS, 555
- PIM (Protocol Independent Multicast), 203
 - configuration information, displaying, 208
 - dense mode, 203
 - sparse mode, 204, 656
- PIX Firewalls, 31–32
- PKI (public key encryption)
 - CAs, 577–578
 - enrolling Cisco ASA to CA server*, 579–585
 - manual enrollment*, 585–588
 - certificates, 576
 - CRLs*, 578–579
 - SCEP*, 579
 - CRL retrieval problems, troubleshooting, 606
 - SCEP enrollment issues, troubleshooting, 605–606
 - time and date mismatches, troubleshooting, 602–605
- police command, 393
- policy maps, 249
 - applying to interface, 394
 - burst size, configuring, 393
 - priority queue, tuning, 394–395
 - QoS configuration, 393–394
- policy NAT/PAT, configuring, 164–165
- policy-map command, 413
- port forwarding, 549–551
- port redirection. *See* static NAT
- port-misuse command, 272
- PPTP inspection, 279
- preconfiguration checklist for site-to-site IPSec VPNs, 467–469
- preserved keys, 22
 - configuring, 472
- primary Cisco ASA, designating, 357
- priority queues, tuning, 394–395
- privileged mode (CLI), 52
- profile-based detection, 13

- promiscuous mode (AIP-SSM), traffic flow, 411–412
- protocol analysis, 12
- protocol-based detection, 13
- protocol-based object groups, 128–129
- provisioning inspection policies, 248–249
- proxy servers, 7–8

Q

- QoS (quality of service)
 - class maps, configuring, 390–393
 - configuring, 389, 671–674
 - deploying on remote-access VPN tunnels, 398–401
 - deploying on VoIP traffic, 395–398
 - DSCP-based policy, configuring, 674–676
 - monitoring, 401–403
 - on VPN tunnels, 389
 - packet classification, 385
 - ACLs*, 388
 - DSCP*, 386–388
 - IP flow-based*, 388
 - IP precedence field*, 385–386
 - VPN tunnel groups*, 388–389
 - packet flow sequences, 384–385
 - policy maps
 - applying to interface*, 394
 - configuring*, 393–394
 - priority queue, tuning*, 394–395
 - traffic policing, 382–383
 - traffic prioritization, 383–384
- quick mode (IPSec), 23

R

- RADIUS (Remote-Access Dial-In User Service), 215–217
 - accounting, 236–237
- rate limiting, 382–384
- recovering
 - lost passwords, 93–96
 - disabling recovery ability*, 97–100
 - system image with ROMMON, 92–93
- recovery parameters for AIP-SSM, configuring, 414–415

redistribution,
 of static routes, 178
 OSPF configuration, 191–192

redundancy. *See* failover

remarks, adding to ACLs, 124

remote management (ASDM)
 via SSH, 631–632
 via SSL, 632–633
 via Telnet, 630–631

remote-access IPsec VPNs, 19
 advanced features
 client auto-update, 525–527
 client firewalling, 527–528
 hardware client NEM, 531
 Individual User Authentication,
 529–530
 interactive hardware client
 authentication, 529
 IP phone bypass, 530
 IPsec hairpinning, 521–522
 Leap bypass, 530
 transparent tunneling, 519–521
 VPN load balancing, 522–525
 clusters, case study, 763–764
 master ASA, 765–767
 configuring, 500–513
 on ASDM, 721–731
 connection termination with certificates,
 configuring, 596–602
 deployment scenarios
 IPsec hairpinning with Easy VPN and
 firewalling, 531–534
 load balancing and site-to-site
 integration, 534–537
 monitoring, 537–539
 QoS, deploying, 389, 398–401
 troubleshooting, 539–541

remote-management protocols
 SSH, 84–89
 Telnet, 82–83
 user access mode password, changing, 84

removing ISAKMP policy commands from
 running configuration, 81

removing users from AIP-SSM, 435

replicated traffic during stateful failover, 350–351

request-method command, 273–275

retiring IPS signatures, 452–453

Rijmen, Vincent, 469

RIP (Routing Information Protocol), 178
 authentication
 configuring, 180–181
 mismatches, troubleshooting, 182
 blocked multicast/broadcast packets,
 troubleshooting, 182–183
 configuring, 179–180, 654
 verifying configuration, 181
 version mismatches, troubleshooting, 181–182

ROMMON, recovering system image, 92–93

route command, 175

routed firewalls, 321
 comparing with transparent firewalls, 322–323

routing protocols
 distance-vector. *See* RIP
 link-state. *See* OSPF

RPC inspection, 280

RPs (rendezvous points)
 configuring, 205
 specifying for multicast routing, 657

RRI (reverse route injection), 196, 479–480

RSA SecurID, 218–219

RSH inspection, 280

RTSP inspection, 280–281

running configuration, 76–79
 ISAKMP policy commands, removing, 81
 managing on ASDM, 628–629
 on AAA server, viewing, 223

S

SAs (security associations), 468
 lifetimes, 483

SCEP (Simple Certificate Enrollment Protocol), 579, 715
 enrolling Cisco ASA to CA server, 579–580
 manual enrollment, 585–588
 trustpoints, configuring, 580–585
 troubleshooting, 605–606

scheduled upgrades, performing on CIPS 5.x, 439–441

secondary Cisco ASA, configuring for Active/Active failover, 364

security contexts, 291
 admin context, configuring, 305–306
 configuration URL, 302–304
 configuring, 299–301

- creating, 665
- customer context, configuring, 306–307
- enabling, 299–301
- interfaces, allocating, 304–305
- managing, 307
- monitoring, 316–317
- multiple security context mode, 292
 - admin contexts*, 293–294
 - converting to single mode*, 301
 - customer contexts*, 294–295
 - packet classification*, 295–296
 - packet flow*, 295
 - packet forwarding*, 296–299
- system execution space, 292–293
 - configuring*, 301–302
- troubleshooting, 317–319
- selecting traffic for application inspection, 250–252**
- SensorApp, 423–424**
- serial console connections, authenticating, 227**
- server delimiters, 558**
- server reactivation policies, AAA, 221**
- service account (AIP-SSM), 434**
- service packs, applying to CIPS 5.x, 437–441**
- service-based object groups, 129–130**
- session hijacking, 18**
- set command, 93**
- setup command, 429–433**
- setup process, 56**
 - assigning device name, 58–59
 - DHCP services, configuring, 65–67
 - interface configuration, 59–62
 - management interfaces, configuring, 65
 - parameters, 57–58
 - subinterface configuration, 63–64
- severity levels of events, 101–102**
- show aaa-server command, 244**
- show aaa-server protocol command, 222**
- show access-list command, 149–152**
- show capture command, 151**
- show clock command, 73**
- show configuration command, 442–443**
- show conn command, 150, 418**
- show events command, 445–446**
- show failover command, 374**
- show firewall command, 330**
- show local-host command, 173**
- show logging command, 378–379**
- show module command, 409, 415**
- show ntp status command, 74**
- show ospf command, 196**
- show ospf interface command, 197**
- show route command, 176, 199**
- show running-config aaa-server command, 223**
- show running-config command, 76–79**
- show service-policy command, 251, 401**
- show shun command, 418**
- show snmp-server statistics command, 112**
- show ssh sessions command, 87–88**
- show startup-config command, 79–80**
- show statistics command, 446**
- show uauth command, 245**
- show url-server statistics command, 152–153**
- show version command, 441**
- shun command, 418**
- shunning, 417–418, 460–462**
- signatures, 11**
 - customizing, 453–457
 - disabling, 452–453
 - updates, applying to CIPS 5.x, 438–441
- single mode Active/Standby failover, 369–371**
- single-mode transparent firewalls, 323**
 - packet flow, 323–326
- SIP inspection, 281–282**
- site-to-site IPSec VPNs, 19**
 - advanced Cisco ASA features, 479
 - NAT -T*, 481
 - OSPF updates over IPSec*, 479
 - RRI*, 479–480
 - tunnel default gateway*, 481–482
 - connection type, specifying, 483–484
 - crypto maps, applying to interface, 476–477
 - crypto maps, configuring, 475–476
 - fully-meshed topology with RRI, 488–492
 - interesting traffic, defining, 474–475
- ISAKMP**
 - attributes*, 468
 - enabling*, 470
 - keepalives*, 484–485
 - policies, creating*, 471
 - presheared keys, configuring*, 472
- mismatched presheared keys,
 - troubleshooting, 496
- monitoring, 492–494
- NAT, bypassing, 478
- PFS, 482

- preconfiguration checklist, 467–469
- QoS, 389
- SA lifetimes, 483
- single tunnel configuration using NAT-T, 485–487
- traffic filtering, 477–478
- troubleshooting, 494–496
- tunnel type, setting, 471–472
- unacceptable ISAKMP proposals, troubleshooting, 496
- using PKI, configuring on ASDM, 713–720
- using preshared keys, configuring on ASDM, 706–713
- Skinny inspection, 282–284**
- small business deployment, case study, 755–757**
- SMTF (single-mode transparent firewalls), deploying, 335–336**
- smurf attacks, 16**
- SNMP (Simple Network Management Protocol), 109–112**
 - application inspection, 284
- software**
 - ASDM image file, uploading, 611–612
 - failover requirements, 351
 - recovery parameters, configuring on AIP-SSM, 414–415
- software-based VPN clients, configuring, 514–516**
- source routing, 18**
- sparse mode (PIM), 204**
- specifying**
 - AAA server groups, 220–222
 - connection type on site-to-site VPNs, 483–484
 - RPs for multicast routing, 657
- split tunneling, 512–513**
- spoofing, 15**
- SQL*Net inspection, 284**
- SSH (Secure Shell), 84–89**
 - ASDM, remote management, 631–632
 - connections, authenticating, 225–227
- SSL, ASDM remote management, 632–633**
- standard ACLs, 119, 133**
- standby unit**
 - failover MAC address, specifying, 365
 - role during Active/Standby failover, 351–352
- startup configuration, 79–81**
- Startup Wizard (ASDM), 616–617**
- state table, 9**
- stateful failover, 350**
 - replicated traffic, 350–351
 - statistics, displaying, 375
- stateful inspection firewalls, 9**
- stateful pattern matching, 11–12**
- static address translation, 651**
- static multicast routes, configuring, 207**
- static NAT, 8–9**
 - configuring, 157–159, 650
 - outside entries, configuring, 160
- static PAT, configuring, 161–163**
- static routes**
 - configuring, 175–178
 - redistribution, 178
- statically assigning multicast groups, 204**
- stealth firewalls. *See* transparent firewalls**
- strict-http command, 270**
- stub areas, 192**
 - OSPF configuration, 192–193
- sub-configuration mode (CLI), 53**
- subinterface configuration, 63–64**
- subinterfaces, creating on ASDM, 626**
- supported AAA protocols, 213–215**
 - Active Directory, 219
 - Kerberos, 219
 - LDAP, 219–220
 - Microsoft Windows NT, 219
 - RADIUS, 215–217
 - RSA SecurID, 218–219
 - TACACS+, 217–218
- synchronization of NTP server and system clock, verifying, 74**
- syntax, clock set command, 72–73**
- syslog**
 - enabling on ASDM, 635–641
 - parameters, 108
 - server logging, 108
- system clock**
 - automatic adjustment, 73–74
 - ASDM configuration, 627–628
 - DST, setting, 75
 - manual adjustment, 72
 - time zone, configuring, 74–75
- system execution space, 292–293**
 - security context configuration, 301–302
- system images**
 - recovering with ROMMON, 92–93
 - upgrading via Cisco ASA CLI, 89–92

system logging

event logging

*ASDM logging, 107**buffered logging, 104–106**console logging, 104**e-mail logging, 107**enabling, 102–103**syslog server logging, 108**terminal logging, 104*

SNMP, 109–112

*configuring on ASDM, 641–643***system monitoring, 100–101****system time. *See* system clock****T****TACACS+ (Terminal Access Controller Access Control System), 217–218**

accounting, 237

administrative connections, troubleshooting,
243–245

deploying for administrative sessions, 238–240

TCP (Transmission Control Protocol)

3-way handshakes, embryonic connections, 158

custom signatures, creating, 453–457

SYN flood attacks, 15

TCP interception, 159**Telnet, 82–83**

ASDM, remote management, 630–631

authentication, 224

user access mode password, changing, 84

telnet command, 82–83**Telnet connections****terminal logging, 104****terminals, 263****terminating Cisco VPN client IPSec connections**

using certificates, 596–602

testing interface failover detection, 349**TFTP inspection, 284****three-way handshake, 15****time and date mismatches on PKI,**

troubleshooting, 602–605

time zone, configuring, 74–75**time-based ACLs**

absolute time restrictions, 134–135

configuring, 133–134

periodic time restrictions, 135

timed mode, AAA server reactivation, 221**timeout uauth command, 231****timing-related failover issues,**

troubleshooting, 378

TLS trusted host, adding to AIP-SSM, 437**TOS (Type Of Service) bits, 385****traffic**

prioritization, 383–384

selecting for application inspection, 250–252

traffic classes, creating, 390**traffic policing, 382–383****TransactionSource, 427****transfer-encoding type command, 275****transform sets, 473**

troubleshooting on IPSec site-to-site VPNs, 496

transmission ring, 382**transparent firewalls, 666**

and VPNs, 327–328

ARP inspection, configuring, 333–334

comparing with routed firewalls, 322–323

configuring, 328–330

deploying, 334

interface ACLs, configuring, 331–332

IP address, configuring, 330–331

L2F table parameters, configuring, 334

MMTF

*packet flow, 326–327**with security contexts, deploying, 336–341*

monitoring, 341–342

single-mode, 323

packet flow, 323–326

SMTF, deploying, 335–336

troubleshooting, 342–344

transparent tunneling, 519–521**transport mode (IPSec), 27****troubleshooting**

administrative connections, 242–245

Cisco remote-access IPSec VPNs, 539–541

failover, 377

timing issues, 378

IP multicast, 207

OSPF, 196–199

*adjacencies, 200–201**mismatched areas, 202**mismatched authentication, 202**virtual links, 202*

PKI

retrieval problems, 606
SCEP enrollment issues, 605–606
time and date mismatches, 602–605

RIP

authentication mismatches, 182
blocked multicast/broadcast packets, 182–183
version mismatches, 181–182
 security contexts, 317–319
 site-to-site VPNs, 494–496
 transparent firewalls, 342–344
 WebVPN, 570–573

trusted hosts, adding to AIP-SSM, 436–437

trustpoints, configuring, 580–585

tunnel default gateway, 481–482, 511

tunnel mode (IPSec), 28

type 3 LSA filtering, 193–194

U

upgrading images via Cisco ASA CLI, 89–92

uploading ASDM image file, 611–612

URL filtering, 139

configuring, 141–143
 external filtering servers, 140
 filtering servers, configuring, 142–144
 long URL support, configuring, 144–145
 Websense servers, case study, 762–763

URL mangling, 551–553

url-server command, 141

user accounts (AIP-SSM)

adding/deleting, 434–435
 administrator account, 433–434
 operator account, 434
 passwords, changing, 435–436
 service account, 434
 viewer account, 434

user group-policy, 503

user mode (CLI), 52

user policies, configuring, 504

username attributes command, 504

username delimiters, 557

UTC (Universal Time, Coordinated), 74

V

vendors of CAs, 577

verifying

NTP server synchronization with system clock, 74
 operation of primary Cisco ASA failover, 374–377
 RIP configuration, 181

viewer account (AIP-SSM), 434

viewing

AAA server running configuration, 223
 ASA connections, 418
 module statistics, 409

Virtual Alarm, 424

virtual firewalls. *See also* security contexts

multimode topology, 308–312
 with shared interface, deploying, 312–316

virtual links

configuring, 187–189
 troubleshooting, 202

VoIP (Voice over IP), deploying QoS, 395–398

VPNs, 18–19

and transparent firewalls, 327–328
 Cisco IPSec remote-access VPN solution
 advanced features, 519–531
 bypass NAT, 511–512
 CiscoEasy VPN Client, configuring, 513–519
 configuring, 500, 721–731
 connection termination with certificates, configuring, 596–602
 dynamic crypto maps, configuring, 509–510
 hairpinning with Easy VPN and firewalling, 531–534
 IP addresses, assigning, 507–508
 IPSec policy, defining, 509
 ISAKMP, enabling, 501
 ISAKMP policy, creating, 502
 ISAKMP preshared keys, configuring, 506
 load balancing and site-to-site integration, 534–537
 remote-access attributes, configuring, 502–505
 split tunneling, 512–513
 traffic filtering, configuring, 510–511

- tunnel default gateway, 511*
- tunnel type, defining, 505–506*
- user authentication, configuring, 506–507*
- Cisco WebVPN, 541
 - advanced features, 548–564*
 - configuring, 543–548, 731–745*
 - deployment scenarios, 564*
 - monitoring, 537–539, 569–570*
 - troubleshooting, 539–541, 570–573*
 - versus Cisco VPN client solution, 542–543*
 - with e-mail proxy deployment scenario, 567–568*
 - with external authentication deployment scenario, 565–566*
- IPSec, 19–20
 - AH, 24–25*
 - ESP, 25*
 - IKE, 20–24*
 - transport mode, 27*
 - tunnel mode, 28*
- load balancing, 522–525
- monitoring on ASDM, 745–746, 748
- QoS, 389
- site-to-site
 - advanced Cisco ASA features, 479–482*
 - configuring with certificates, 591–595*
 - connection type, specifying, 483–484*
 - crypto maps, applying to interface, 476–477*
 - crypto maps, configuring, 475–476*
 - fully-meshed topology with RRI, 488–492*
 - ISAKMP attributes, 468*
 - ISAKMP keepalives, 484–485*
 - ISAKMP policy, creating, 471*
 - ISAKMP preshared keys, configuring, 472*
 - ISAKMP, enabling, 470*
 - mismatched preshared keys, troubleshooting, 496*
 - monitoring, 492–494*
 - NAT, bypassing, 478*
 - PFS, 482*
 - preconfiguration checklist, 467–469*
 - SA lifetimes, 483*
 - single tunnel configuration using NAT-T, 485–487*
 - traffic filtering, 477–478*
 - troubleshooting, 494–496*

- tunnel type, setting, 471–472*
- unacceptable ISAKMP proposals, troubleshooting, 496*
- using PKI, configuring on ASDM, 713–720*
- using preshared keys, configuring on ASDM, 706–713*
- tunnel groups, packet classification, 388–389

W

Websense servers, 140

- content filtering, 147–148

WebVPN, 541

- ACLs, 120
- advanced features, 548
 - ACLs, 561–564*
 - e-mail proxy, 554–559*
 - port forwarding, 549–551*
 - URL mangling, 551–553*
 - Windows file sharing, 559–561*
- configuring, 543–548, 731–745
- data capture tool, 571
- deployment scenarios, 564
- group attributes, configuring, 546–548
- monitoring, 569–570
- troubleshooting, 570–573
- user authentication, configuring, 548
- versus Cisco VPN client solution, 542–543
- with e-mail proxy deployment scenario, 567–568
- with external authentication deployment scenario, 565–566

Windows file sharing, 559–561

Windows operating system, ASDM support, 614

Wizards, 616

write memory command, 80

X-Y-Z

X.509 certificates, 576

XDMCP (X Display Manager Control Protocol) inspection, 285

zero-downtime software upgrades, 351

- performing, 367–369