## Index

### Numerics
- 1GE-66 Gigabit interface, 49
- 3DES (Triple Data Encryption Standard), 334
- 4FE-66 interface card, 48

### A
- AAA (authentication, authorization, and accounting), 12, 517, 520
  - configuring, 542
  - cut-through proxies, 573
  - Do I Know This Already? quiz, 537–539
  - defined, 517
  - Do I Know This Already? quiz, 513
  - PIX Firewalls supported AAA server technologies, 520
  - servers
    - identifying, 542, 545
    - specifying, 541
    - support, 45
    - troubleshooting, 577, 581
- aaa accounting command, 543
- aaa authentication command, 543, 546
- aaa authentication console command, 548
- aaa authorization command, 543
- aaa-server command, 542
- aaa-server local command, 543
- access, 9
  - AAA, 517, 520
  - networks
    - security, 7
    - threats, 8
    - types of attacks, 8, 11
    - vulnerabilities, 8
- access attacks, 9–11
- access VPNs, 331
  - Do I Know This Already? quiz, 395
- access-group command, 631
- accessing
  - ASDM
    - from browser, requirements, 459
    - from Windows 2000/XP OS, requirements, 460
  - Cisco Security Appliance, 79
    - with SSH, 80–82
    - with Telnet, 79–80
  - security contexts, 234
- accounting, 518
  - configuring, 567–569
  - troubleshooting, 579
- ACEs (access list entries), 185
  - managing, 188–189
- ACLs (access control lists), 27
  - ACEs, managing, 188–189
  - configuring on WebVPNs, 371
  - downloadable, configuring, 573–576
  - inbound access, configuring on Cisco Security Appliance, 185–187
  - line numbers, 188
  - logging feature, 192–193
  - remarks, removing, 189
- ACS (Cisco Secure Access Control Server), 45, 537
- activation keys, upgrading, 88–89
- active units, 307
- active-active failover, 313
  - failover groups, 314–316
- ActiveX objects, filtering, 501–503
Adaptive Security Algorithm (ASA), 32, 41–43
address command, 91
addresses
  IP
    global, 629–630
    mapping, 627
translation, 46, 118, 126
  bidirectional, 126
  commands, 119–120
  configuring multiple, 124, 126
  NAT, 120–121
  PAT, 122
  static, 119, 123
  troubleshooting, 126, 130
admin contexts, 227–228
  converting to security contexts, 229
admin-context command, 229
administrative access modes, transparent mode
  configuring, 165–167
  traffic management, 168–169
AES (Advanced Encryption Standard), 334
  aggressive mode key exchanges, 335–337
AH (Authentication Header), 332
AIP-SSM (ATM Interface Processor-SSM), 49
AIP-SSM (Advanced Inspection and Protection Security Service Module), 610
  installing, 611–613
  setup process, 613–615
algorithms, ASA, 32, 41–43
allocate-interface command, 230
applets (Java), filtering, 502
application inspection, 193
  of DNS, 194, 605–606
  of FTP, 194, 601–602
  of HTTP, 602–605
  of rsh, 608
  of RTSP, 591
  of SMTP, 195, 606–607
  of SNMP, 608
  of SQL*NET, 609
  of VoIP protocols/applications, 592
    H.323, 593, 595
    MGCP, 596–597
    QTIQBE, 593
    SCCP, 597–598
    SIP, 598
  ports, reassigning, 600
applications
  AVVID, 14–15, 19
  threats, 8
applying multiple service policies to traffic, 216–217
Architecture for Voice, Video, and Integrated Data. See AVVID, 14, 19–20
area command, parameters, 285
arp-inspection ethertype command, 169
ASA (Adaptive Security Algorithm), 32, 41–43
ASA Security Appliance
  password recovery procedures, 96–97
ASBRs (Autonomous System Boundary Routers), 282, 286
ASDM (Adaptive Security Device Manager), 453, 457
  accessing from browser, requirements, 459
  Building Blocks tab, 476
Device Administration tab, 477
GUI, 457
installing, 461–463
Interfaces tab, 465
IPS, configuring, 615–616
IPS tab, 474
minimum hardware/software requirements, 458–459
Monitoring tab, 479–481
NAT tab, 472
Properties tab, 477–479
remote access VPNs, creating, 486, 489, 493
Routing tab, 474
running with Linux, requirements, 460
running with SPARC, 460
Security Policies tab, 467, 471–472
site-to-site VPNs, creating, 482–486
VPN tab, 473–474
assigning
access to WebVPN users, 364–365, 367
actions to traffic classes, 207–209, 211–213
connection policies, 213
interfaces to contexts, 230–232
match parameters to class maps, 206
policies to interface, 214–216
policies to traffic classes, 208–209
connection policy, 213
inspect policy, 211–212
IPS policy, 212–213
police policy, 209–210
priority policy, 210
shell authorization sets to NDGs, 562
users to groups, 555
virtual contexts to failover groups, 316
attacks, 9, 18
access, 10–11
DoS, 11
reconnaissance, 9–10
Syslog, 251
threats, 8
authentication, 281, 517
Cisco VPN Software Client, 420
configuring, 545–546, 554
authentication timeout, 553
console access authentication, 548
designating parameters, 547
services, 549
cut-through proxy, 32, 43
Easy VPN Remote, 422
IUA, Cisco VPN Client configuration, 434–435
prompts, 552
services, 549
SU, Cisco VPN Client configuration, 433–434
timeout, 553
troubleshooting, 578
VPDN group, 438
X.509 certificate support, 45, 67
XAUTH, configuring, 409–416
authentication telnet console command, 80
authorization, 517
command-level, 82–85
configuring, 554
Cisco Secure ACS, 555, 558–565
cut-through proxy, 32, 43
troubleshooting, 579
auth-prompt command, 552–553
AVVID (Architecture for Voice, Video, and Integrated Data), 14–15, 19

B

bandwidth, restricting on traffic flows, 209
banner command, 164–165
banner messages, configuring on Cisco Security Appliance, 163–165
basic AIP-SSM settings, configuring, 613–615
debug command, 645
bidirectional network address translation, 126
bidirectional service policies, 215
block scans, 10
blocking applets, 502
boothelper disks, creating, 92–93
Building Blocks tab (ASDM), 476

caches
no url-cache command, 506
show url-cache command, 508

call-agent command, 596
capabilities of specific PIX Firewall models, 49, 61
CAs (certificate authorities), 338, 421

case studies
DUKEM, 623
  authentication, 632
  basic Cisco Security Appliance
  configuration, 625–630
  configuring access rules, 631
  failover, 646, 648
  growth expectation, 624
  VPNs, 633–645
  troubleshooting PIX Firewall
  implementation, 649–658
causes of failover events, 307
certificates, X.509, 45
cgi-truncate parameter, 507
changelog command, 234
changing context mode of operation, 228
CIFS (Common Internet File System), 117
cipher block chains, 334
Cisco ASA 5510 Security Appliance
  configuring, 235–240
  features and capabilities, 62–63
Cisco ASA 5520 Security Appliance, features
  and capabilities, 63–64
Cisco ASA 5540 Security Appliance, features
  and capabilities, 64–65
Cisco ASA Security Appliance, AIP-SSM
  module, 610–611
Cisco ASA Security Appliance 5510, 44
Cisco ASA Security Appliance 5520, 44
Cisco ASA Security Appliance 5540, 44
Cisco Easy VPN Remote Router clients, 407
Cisco FWSM (Firewall Service Module), 44
Cisco PIX 501 Firewall, 49–50
Cisco PIX 501 VPN Client, 406
Cisco PIX 506 VPN Client, 406
Cisco PIX 506E Firewall, 51–53
Cisco PIX 515E Firewall, 55, 53–56
Cisco PIX 525 Firewall, 56–58
Cisco PIX 535 Firewall, 58–61
Cisco PIX Firewall FastEthernet Interface
  Card (PIX-1FE), 48
Cisco Secure ACS (Access Control Server), 537
  configuring, 531
downloadable PIX ACLs, 576
  configuring, 573–576
logging targets and options, 570
users, configuring, 555
  verifying, 581
version 3.3, new features, 521
  Windows server installation, 523–533
Cisco Secure Intrusion Detection
Sensor, 44, 67
Cisco Secure PIX 506, 44
Cisco Secure PIX 515, 44
Cisco Secure PIX 525, 44
Cisco Secure PIX 535, 44
Cisco Secure Scanner, 13
Cisco Security Appliance
  AAA, supported server technologies, 520
  accessing, 79
    with SSH, 80–82
    with Telnet, 79–80
  Cisco VPN Client, configuring, 432–435
    configuring, 464
      as VPN gateway, 343–355
cut-through proxy feature, 43, 519
DHCP, enabling, 445
DHCP client, configuring, 159
DHCP server
  auto configuration, 445
  configuring, 156–159, 443–444
  debugging, 445–446
DNS message support, 154
Easy VPN Remote, configuring, 431–432
failover
  active-active, 313–316
  configuring, 316–321
  LAN-based, 312–313
  monitoring, 309–310
  stateful, 311–312
MAC address table, 169
MPFs, 46
multimedia support, 591
NTP, configuring, 160–162
OS, upgrading, 89–92
PPPoE client
  configuring, 437–438
  enabling, 439
  monitoring, 439–441
running on PPPoE network, 435–436
security contexts, 47
shell configuration, 465
SNMP, configuring, 98
system clock, configuring, 162–163
transparent mode
  configuring, 165–167
  traffic management, 168–169
troubleshooting-related commands, 98–103
Cisco VPN 3002 Hardware Client, 405–406
Cisco VPN Client
   client device mode, configuring, 432
   IUA, configuring, 434–435
   SUA, configuring, 433–434
Cisco VPN Software Client, 405, 418
   authentication and encryption, 420
   digital certificates, 421
   features, 419
   installing, 423–425
   key management techniques, 420
   manual configuration, 422–430
      modifying VPN Client options, 426–428
   specifications, 419
   tunneling protocols, 420
CiscoWorks Management Center for Firewalls (PIX MC), 47
class maps
   creating, 203–205
   match criteria, viewing, 207
   match parameters, assigning, 206
   matches, defining, 206
clear command, 358
clear rip command, 282
clear route command, 280
clear uauth command, 554
clear xlate command, 127
clearing multicast routes, 291
CLI (command-line interface), 46, 68, 80
client device mode, Cisco VPN Client configuration, 432
client mode (Easy VPN Remote), 417
clients, Easy VPN Remote, 405–407
clock timezone command, 163
command-level authorization, 82–85
command-line interface (CLI), 46, 68, 80
commands
   aaa accounting, 543
   aaa authentication console, 548
   aaa authentication, 543, 546
   aaa authorization, 543
   aaa-server command, 542
   access-group command, 631
   address, 91
   admin-context, 229
   allocate-interface, 230
   area, parameters, 285
   arp-inspection ethertype, 169
   authentication telnet, 80
   auth-prompt, 552–553
   banner, 164–165
   call-agent, 596
   changeto, 234
   clear, 358
   clear route, 280
   clear uauth, 554
   clear xlate, 127
   clock timezone, 163
   config-url, 232
   content-type-verification, 604
   copy tftp flash, 90
   crypto ipsec transform-set, 412
   debug, 645
      VPs, troubleshooting, 358–360
   debug aaa accounting, 579
   debug aaa authentication, 578
   debug aaa authorization, 579
   debug igmp, 297
   debug radius, 580
   debug tacacs, 580
   default-inspection-traffic, 206
dhcpd address, 443
duplex, 148
enable password, 80
failover poll, 309
file, 91
filter activex, 503
filter java, 501
filter url, 504
global, 149–150
icmp, 152
igmp access-group, 292
igmp forward, 291
igmp join-group, 291
igmp query-interval, 292
igmp query-max-response-time, 293
igmp version, 292
inspect, 211, 600
inspect dns, 606
inspect ftp, 194
inspect h323, 595
inspect rtsp, 592
inspect smtp, 607
interface, 91, 142–143
ip address, 145
ip local pool, 411
ips, 212
logging (syslog), 253
logging facility facility, 252
logging on, 260
max-header-length, 604
mroute, 290
multicast interface, 290
nameif, 113, 131, 144, 277
nat, 146–147
nat 0, 183
nat-control, 149
no aaa-server, 544
no url-cache, 506
object-group
  icmp-type object type parameter, 191
  network object type parameter, 190
  protocol object type parameter, 191
  service object type parameter, 191
OSPF-related, 282, 288
  network command, 284
  prefix-list command, 285
  redistribute ospf command, 286
  router ospf command, 283
passwd, 80
pim, 292
pim dr-priority, 293
pim rp-address, 293
ping, 91, 152
police, 209
port-misuse, 605
priority, 210
redistribute ospf, 286
rip, 151–152
rip command, 281
route, 150, 278
router ospf, 286
server, 91
set connection, 214
show, 645
  VPNs, troubleshooting, 356, 358
show aaa-server, 578
show accounting, 579
show activation-key, 88
show command, 578
show conn, 128
show context, 235
show mac-address-table, 169
show mode, 228
show perfmon, 509
show route, 280
show run policy-map, 214
show running-config service policy, 217
show service-policy, 217–218
show tech-support, 99
show url-cache, 508
show url-server stats, 508
show version, 86
show vpdn, 439, 441
show vpdn pppinterface, 440
show xlate, 127
speed, 148
ssh command, 81
static, 124, 180
sysopt uauth allow-http-cache, 548
telnet, 79
tftp flash, performing OS upgrades, 89–90
timeout uauth, 553
translation, 119–120
troubleshooting, 100–103
troubleshooting-related, 98–99, 101–103
url-cache, 505
url-server, 503
virtual telnet, 549
vpnclyent server, 432
vpnclyent vpngroup, 432
write memory, 80, 154, 311
xlate, 120
Common Internet File System (CIFS), 117
components of AAA, 517, 520, 541
configuration administrative access mode, 141
configuration files, uploading to contexts, 232
configuration replication, 310–311
configuring. See also example configurations
AAA, 542
cut-through proxies, 573
Do I Know This Already? quiz, 537–539
accounting, 567–569
authentication, 545–546, 554
  authentication timeout, 553
  console access authentication, 548
  designating parameters, 547
  services, 549
authentication timeout, 554
authorization, 554
Cisco Secure ACS, 555, 558–565
per group command authorization, 563
shell command authorization, 561
Cisco Security Appliance, 464
as DHCP client, 159
as DHCP server, 156–159, 443–444
as VPN gateway, 343–355
DUKEM case study, 625–632
failover, 316–321
login banners, 163–165
NTP, 160–162
PPPoE client, 437–438
system clock, 162–163
Cisco VPN Client
client device mode, 432
manual configuration, 422–430
modifying VPN Client options, 426–428
IUA, 434–435
SUA, 433–434
CSACS, 531, 555
cut-through proxy, 573
DHCP server, 441–442
DNS support, 130
downloadable PIX ACLs, 573–576
Easy VPN Remote, 431–432
PIX Firewalls, 433
failover
   DUKEM case study, 646, 648
   requirements, 308–309
failover groups, 315
filters, 508
inbound access on Cisco Security Appliance, 180–187
interfaces, 628–630
IPS through ASDM, 615–616
multiple translation types, 124–126
NAT, 415
   on Security Appliance interfaces, 232
OSPF, 286–288
PAT, 147
per user command authorization, 564
redundancy, 33–34
RIP, 151–152, 281–282
routing, 628–630
security contexts, 235, 237–240
SNMP on Cisco Security Appliance, 98
static routes, 279–280
syslog, 47, 68, 255
messages at the console, 258
sending messages to a log server, 259–261
SNMP traps and SNMP requests, 261
syslog servers, 262–263
transparent mode, 165–167
traffic management, 168–169
URL-filtering policy, 504
virtual HTTP inbound connections, 552
virtual Telnet, outbound connections, 550
VPDN group, 438
VPNs, 645
   DUKEM case study, 633–635, 638, 641–645
WebVPNs
   content filtering, 371
e-mail proxies, 369–371
gateways, 361–364
port forwarding, 367–368
user access, 364–365, 367
XAUTH, 409–416
config-url command, 232
connection policies, assigning, 212–213
connection process for Easy VPN Remote, 407–409
connectionless protocols, UDP, 114–117
connections
   Cisco Secure PIX 501, 50
   Cisco Secure PIX 515E, 55
   Cisco Secure PIX 535, 60
cut-through proxy, 32, 519
embryonic (half-open), 116
filters, Java applets, 502
flags, 129
security, 7
telnet, 79
threats, 8
troubleshooting, 126
types of attacks, 8, 11
vulnerabilities, 8
connectivity of Security Appliance, testing, 152–153
console access authentication, 548
content filtering
   "Do I Know This Already?" quiz, 498
   configuring on WebVPN, 371
content-type-verification command, 604
context administrators, 229
contexts
  admin context, 227
  administration context, 228
  assigning to failover groups, 316
  configuration files, uploading, 232
deleting, 234
  interfaces, allocating, 230–232
  modes of operation, changing, 228
  status, displaying, 235
  switching between, 234
controlling HTTP message header size, 604
deleting contexts, 234
converting admin contexts to security contexts, 229
copy tftp flash command, 90
crypto maps, arguments and options, 354
creating
  boothelper disks, 92–93
class maps, 203–205
downloadable ACLs, 576
object groups, 189
policy maps, 207–208
remote access VPNs with ASDM VPN Wizard, 486, 489, 493
security contexts, 230
site-to-site VPNs with ASDM VPN Wizard, 482–483, 485–486
crypto ipsec transform-set command, 412
crypto maps
  arguments and options, 354
dynamic, 414
CSACS. See Cisco Secure ACS (Access Control Server)
cut-through proxy, 32, 43, 519, 573
data compression, Easy VPN Remote, 421
DDoS (distributed denial of service) attacks, 11
debug aaa accounting command, 579
debug aaa authentication command, 578
debug aaa authorization command, 579
debug command, troubleshooting VPNs, 358–360
debug igmp command, 297
debug radius command, 580
debug tacacs command, 580
dehacking
  DHCP server on Cisco Security Appliance, 445–446
  multicast configuration, 296
default routes, 279
default-inspection-traffic command, 206
defense in depth, 14
defining class map matches, 206
deleting contexts, 234
demilitarized zone (DMZ) segment, 125
denial of service (DoS) attacks, 11
devices (Data Encryption Standard), 334
Device Administration tab (ASDM), 477
DHCP (Dynamic Host Configuration Protocol), 442
DHCP client, Cisco Security Appliance configuration, 159
DHCP server
  auto configuration, 445
  Cisco Security Appliance configuration, 156–159, 443–444
  configuring, 441–442
  debugging commands, 445–446
dhcpd address command, 443
dhcpd auto-config command, 437
Diffie-Hellman, 336
digital certificates
  Cisco VPN Software Client functionality, 421
  X.509, 45
disabling Syslog messages, 264
displaying
  class map match criteria, 207
  context information, 235
  policy map configurations, 214
  service policy configurations, 217
distributed denial of service (DDoS) attacks, 11
DMZ (demilitarized zone) segment, 125
DN (distinguished name), 408
DNS (Domain Name Service)
  application inspection, 194, 605–606
  message support on Security Appliance, 154
  queries, 9
  support, configuring, 130
dNS doctoring, 155
dNS inspection, 605
Do I Know This Already? quizzes
AAA, 513, 537, 539
access VPNs, 395
content filtering, 498
network security, 4–6
PIX Firewalls, 25, 38–40
Syslog, 247
system maintenance, 75
domains, 207
connection policy, 213
inspect policy, 211–212
IPS policy, 212
police policy, 209
priority policy, 210
DoS (denial of service) attacks, 9–11
downloadable PIX ACLs, 576
configuring, 573–576
DPD (dead peer detection), 402, 416
duplex command, 148
dynamic address translation, 119
dynamic crypto maps, 414
dynamic routes, 280
OSPFW
commands, 282–286
configuring, 286–288
RIP, configuring , 282

E
Easy VPN Remote, 400
authentication, 422
configuring, 431–432
connection process, 407–409
modes of operation, 416
client mode, 417
overview, 404
PIX Firewall configuration, SUA, 433
supported clients, 405–406
supported servers, 404
Easy VPN Server, 400
IPSec options, 403
overview, 402
e-mail proxies, configuring on WebVPN, 369–371
EMBLEM format, 261
embryonic connections, 116
enable password command, 80
enabling
DHCP on Cisco Security Appliance, 445
IUA, 435
PPPoE client on Cisco Security Appliance, 439
transparent mode, 167
encapsulation of upper-level data, 114
encryption, 334
Cisco VPN Software Client, 420
hash algorithms, 413
enrollment mechanisms, 421
environments, ROBO, 51
Ethernet VLAN tagging, 273
logical interfaces, 274–276
managing VLANs, 276–277
event reporting (syslog), 47, 68
example configurations
of routed mode Security Appliance, 170–172
of transparent mode Security Appliance, 172–173
external threats, 9
extranet VPNs, 331

F
failover
active-active, 313
failover groups, 314–316
causes of, 307
configuring, 316–317, 319–321
DUKEM case study, 646–648
requirements, 308–309
LAN-based, 312–313
monitoring on Cisco Security Appliance, 309–310
redundancy, 33–34
stateful, 311–312
failover groups
assigning virtual contexts to, 316
configuring, 315
failover poll command, 309
feature domains, 207
file command, 91
filter activex command, 503
filter java command, 501
filter url command, 504
filtering, 501
  ActiveX objects, 503
  FTP, 506
  FTP sites, 505
  HTTPS, 505–506
  Java applets, 501–502
  URLs, 503, 505
    configuring URL-filtering policy, 504
    identifying servers, 503
  viewing, 508
firewalls, 27, 31
  managing, 46–47, 68
  packet filtering, 27, 29
  PIX, 31, 33–34
    ASA, 32, 41–43
    Cisco 501, 50
    Cisco 515E, 55
    Cisco 535, 60
  proxy servers, 29
  stateful packet inspection, 30–31
first-match classification policy, 217
first-match rule, 216
fixup protocols, 333
Flash memory, saving Security Appliance configuration, 154
floating routes, 279
formatting boothelper disk, 93
frames, 114
FTP (File Transfer Protocol)
  application inspection, 194, 601–602
  filtering, 506
FWSM (Cisco Firewall Service Module), 44

G
  gateways, 91
    VPNs, 48, 69
  global addresses, 118
  global attributes (WebVPNs), configuring, 361–364
  global command, 149–150
  global information, recording, 626
  global IP addresses, 629–630
  global_policy policy maps, 208
  grouping objects, 189
  groups, assigning users to, 555

H
  H.323, application inspection, 593, 595
  hardware requirements
    for ASDM, 458–459
    for CSACS, 522
  hash algorithms, 334
  HMAC (Keyed-Hash Message Authentication Code), 335
  horizontal scans, 9
  HTTP
    application inspection, 602–605
    message header size, controlling, 604
    OS upgrades, performing on client, 92
  HTTPS filtering, 506
I
  IANA (Internet Assigned Numbers Authority), reserved private address space, 118
  icmp command, 152
  icmp-type object type parameter (object-group command), 191
  identifying servers, 503, 542, 545
  IGMP (Internet Group Management), 289
  igmp access-group command, 292
  igmp forward command, 291
  igmp join-group command, 291
  igmp query-interval command, 293
  igmp query-max-response-time command, 293
  igmp version command, 292
  IKE (internet Key Exchange), 335
    phase 1 negotiation, 337
  inactivity timer, 554
  inbound access, configuring on Cisco Security Appliance, 180–187
  inbound connections, cut-through proxy, 32
  inbound multicast traffic, 294–295
  Individual User Authentication (IUA), 434
  information security, 7
  Initial Contact, 403
  inline mode (AIP-SSM), 610
  Inline mode (IPS), 212
  input service policies, 215
  inspect command, 211, 600
  inspect dns command, 606
  inspect ftp command, 194
inspect h323 command, 595
inspect policy, 211–212
inspect rtsp command, 592
inspect smtp command, 607
installing
AIP-SSM module, 611–613
ASDM, 461–463
Cisco VPN Software Client, 423–425
CSACS 3.3 on Windows server, 523–533
operating systems, 85–87
integrity, X.509 certificate support, 45, 67
interception, 10
interface command, 91, 142–143
interfaces
assigning to contexts, 230–232
CLI, 46, 68, 80
configuring, 628–630
NAT translation, configuring, 232
security levels, 41, 143
Interfaces tab (ASDM), 465
interface-specific service policies, 216
first-match classification policy, 217
matching logic, 216
multimatch classification policy, 216
intranet VPNs, 331
intrusion detection, 44, 67
optimizing, 13
IP addresses
address pools, 411
global, 629–630
mapping, 627
ip address command, 145
ip local pool command, 411
IP routing, 277
dynamic routes, 280
RIP, configuring, 282
OSPF, 282, 284–286, 288
multicast, 289
commands, 290–293
debugging, 296
inbound traffic, 294–295
outbound traffic, 295–296
static routes, 277
configuring, 279–280
IP subnets, performing address translation, 181
IPS, configuring through ASDM, 615–616
IPS policy, 212
IPS tab (ASDM), 474
IPSec
AH, 332
CA server enrollment process, 338
Easy VPN Server, 403
IKE, 335
options and attributes, 403
PFS, 338
phase 1 negotiation, 337
phase 2 negotiation, 337
isakmp keepalive command, 416
isakmp policy command, 410
IUA (Individual User Authentication), 434
Cisco VPN Client configuration, 434–435
Java applets, filtering, 501–502
joining multicast groups, 291
LAN-based failover, 312–313
levels of syslog security, 252
licenses, Security Plus Software, 64
Linux, requirements for running ASDM, 460
listening ports, 8
local addresses, 118
logging ACLs, 192–193
logging commands (syslog), 253
logging facilities, 2520
logical interfaces, 274–276
login banners, configuring, 163–165
logs, viewing, 256
longurl-truncate parameter, 507
lost passwords, recovering on ASA Security Appliance, 96–97
LSAs (link-state advertisements, 282
MAC address table, 169
mac-learn command, 170
mail inspection, 606–607
main mode key exchanges, 335
managing
ACEs, 188–189
firewalls, 46–47, 68
VLANs, 276–277
manual configuration, Cisco VPN Software Client, 422, 426–430
mapping static IP addresses, 627
MARs (Machine Access Restrictions) on Cisco Secure ACS 3.3, 521
matching logic of service policies, 216
max-header-length command, 604
MD5 (Message Digest 5), 335
MDIX (Medium Dependent Interface Crossover), 406
memory
Flash memory, saving Security Appliance configuration, 154
requirements, 85
message digest, 335
messages, syslog
changing levels, 253
disabling, 264
organizing, 254
reading, 254
sending to a Telnet session, 259
MGCP (Message Group Configuration Protocol), application inspection, 596–597
MIBs (Message Information Bases), 97
Microsoft NetMeeting, 549
minimum hardware/OS requirements for Cisco Secure ACS, 522
modes of context operation, verifying, 228
modification
access attacks, 10
activation keys, 89
monitor mode, performing OS upgrades, 90–91
monitoring
Cisco Security Appliance failover, 309–310
PPPoE client, 439
on Cisco Security Appliance, 439–441
Monitoring tab (ASDM), 479, 481
MPFs (Modular Policy Frameworks), 46
policies, assigning to interface, 214–216
policy maps
creating, 207–208
viewing, 214
traffic classes
assigning actions to, 207–213
assigning policies to, 208–213
traffic flow matching
class map criteria, viewing, 207
class map matches, defining, 206
class maps, creating, 203–205
mroute command, 290
MTU (maximum transmission unit), 423
multicast groups, joining, 291
multicast interface command, 290
multicast routing, 289
commands
igmp access-group command, 292
igmp forward command, 291
igmp join-group command, 291
igmp query-interval command, 292
igmp query-max-response-time command, 293
igmp version command, 292
mroute command, 290
multicast interface command, 290
debugging, 296
inbound traffic, 294–295
outbound traffic, 295–296
multimatch classification policy, 216
multimedia application protocols, support for on Cisco Security Appliance, 591
multiple-context mode, creating security contexts, 230
N
NAC (Network Admission Control) feature, Cisco Secure ACS 3.3, 521
NAFs (Network Access Filters), 521
nameif command, 113, 131, 144, 277
NAS (Network Access Server), 518, 541
identifying, 542, 545
NAT (Network Address Translation), 118–121
bidirectional, 126
configuring, 415
inbound access, configuring on Cisco Security Appliance, 180–181, 184–185
policy NAT, 184
static NAT, 180
translated addresses, viewing, 150
nat 0 access-list address translation rule, 180
nat 0 command, 183
configuring inbound access on Cisco Security Appliance, 183
nat command, 146–147
NAT tab (ASDM), 472
NAT Traversal, 334
nat/global command, 113
nat-control command, 149
NDG (Network Device Group), assigning shell authorization sets, 562
nesting object groups, 192
NetBIOS Domain Name System, 117
NetMeeting, 549
network command, 284
Network Device Group (NDG), assigning shell authorization sets, 562
network extension mode (Easy VPN Remote), 418
network object type parameter (object-group command), 190
network of networks, 14
network security
as a “legal issue,” 13
defense in depth, 14
Do I Know This Already? quiz, 4–6
network security policies, MPF
policies, assigning to interface, 214, 216
policy maps
creating, 207–208
viewing, 214
traffic classes
assigning actions to, 207–209, 211–213
assigning policies to, 208–213
traffic flow matching, 203–207
no aaa-server command, 544
no url-cache command, 506
nodes, communication, 115
NTP (Network Time Protocol), configuring on Cisco Security Appliance, 160–162

object-group command
icmp-type object type parameter, 191
network object type parameter, 190
protocol object type parameter, 191
service object type parameter, 191
Open System Interconnection (OSI), 27
optimizing security, 13
organizing ACEs, 188–189
OSs (operating systems)
activation key, upgrading, 88–89
CSACS minimum requirements, 522
installing, 85–87
upgrading
with HTTP client, 92
with monitor mode, 90–91
with ftp/flash command, 89–90
OSI (Open System Interconnection) reference model, 27–29
OSPF (Open Shortest Path First)
ASBRs, 286
commands, 282
network command, 284
prefix-list command, 285
redistribute ospf command, 286
show ospf command, 288
configuring, 286–288
overview, 282
OU (Organizational Unit), 408
outbound multicast traffic, 295–296
output service policies, 215

P
packets, 113
parameters
for AAA authentication, 547
for access-list command, 185
for allocate-interface command, 230
for area command, 285
for arp-inspection ethertype, 169
for banner command, 164–165
for cgi-truncate command, 507

O
object groups
creating, 189
nesting within other object groups, 192
for class map match criteria, assigning, 206
for duplex command, 148
for filter command, 145
for global command, 149–150
for interface command, 142
for ip address command, 145
for nameif command, 144
for nat command, 146–147
for police command, 209
for rip command, 151–152
for route command, 150
for service-policy command, 215
for set connection command, 214
for show service-policy command, 218
for speed command, 148
for syslog command, 255
for username command, 84
passwd command, 80
password recovery procedures
  on ASA Security Appliance, 96–97
  on diskless PIX Firewall, 95
  on PIX Firewall 520, 94–95
PAT (Port Address Translation), 46, 118–119, 122
  configuring, 147
  inbound access, configuring on Cisco Security Appliance, 182
  translated addresses, viewing, 150
patches, 8
PDM Log panel, 256
per group command authorization, configuring, 563
per user command authorization, configuring, 564
perimeter security, firewalls, 27, 31
  packet filtering, 27, 29
  PIX, 31, 33–34
  proxy servers, 29
  stateful inspection, 30–31
PFS (Perfect Forward Secrecy), 338
PFSS (PIX Firewall Syslog Server), 251
  phase 1 negotiation (IPSec), 332, 337
  phase 2 negotiations (IPSec), 332, 337
physical security
  AAA, 517, 520
  security policies, 11
PIDs (process IDs), 286
pim command, 292
pim dr-priority command, 293
pim rp-address command, 293
ping command, 91, 152
ping sweeps, 9
pipes, 252
PIX Firewalls, 33
  ASA, 41–43
  characteristics, 31
  Easy VPN Remote configuration, SUA, 433
  IP routing, 277
    dynamic routes, 280–288
    static routes, 277–280
  logical interfaces, 274–276
  lost passwords, recovering, 94–95
  optional components, 48–49
  PPPoE
    enabling PPPoE client, 439
    monitoring PPPoE client, 439
  secure real-time embedded system, 32
  specific model capabilities, 49–61
syslog
  configuring, 255, 258
  logging facilities, 252
  organizing messages, 254
  PFSS, 263
  reading messages, 254
  sending messages to a log server, 259–261
  sending messages to a Telnet session, 259
  severity levels, 253
  SNMP traps and SNMP requests, 261
troubleshooting, 649–658
virtual interfaces, 54
PIX Firewall Syslog Server (PFSS), 251
PIX MC (CiscoWorks Management Center for Firewalls), 47
PIX-1FE (Cisco PIX Firewall FastEthernet Interface Card), 48
police command, 209
policies, 18
  assigning to interface, 214–216
  security, 11
policy maps
  configurations, displaying, 214
  creating, 207–208
  global_policy, 208
policy NAT, configuring inbound access on Cisco Security Appliance, 184–185

Port Fast, 309

port forwarding, 342
  configuring on WebVPN, 367–368

portal interface (WebVPNs), 340

port-misuse command, 605

ports. See also PAT
  listening, 8
  reassigning for application inspection, 600
  redirection, 124

PPP (Point-to-Point Protocol), 436

PPPoE (Point-to-Point Protocol over Ethernet), 435–436
  enabling PPPoE client, 439
  monitoring PPPoE client, 439

PPPoE client
  configuring on Cisco Security Appliance, 437–438
  enabling on Cisco Security Appliance, 439
  monitoring on Cisco Security Appliance, 439–441

prefix-list command, 285

principle of least privilege, 600

priority policy, 210

privileged administrative access mode, 141

processes, security, 12

promiscuous mode (IPS), 212

prompts, authentication, 552

Properties tab (ASDM), 477, 479

protocol object type parameter (object-group command), 191

proxy firewalls, 29

public address translation, 46

recovering lost passwords, 93–94
  on ASA Security Appliance, 96–97
  on diskless PIX Firewalls, 95
  on PIX Firewall 520, 94–95

redirection, 124

redistribute ospf command, 286

redundancy, 33–34

remarks, removing from ACLs, 189

remote access VPNs, 331
  creating with ASDM VPN Wizard, 486, 489, 493

remote office/branch office (ROBO), 51

remote-procedure call (RPC), 117

removing
  contexts from running configuration, 234
  NTP configuration from Cisco Security Appliance, 162
  remarks from ACLs, 189

replication, 310–311

reports, viewing, 570

requests, SNMP, 261

requirements
  for failover configuration, 308–309
  memory, 85

reserved private address space, 118

resources, unauthorized access to, 10

Restricted Bundle, 61

restricting bandwidth on traffic flows, 209

RIP (Routing Information Protocol), configuring, 151–152, 281–282

rip command, 151–152, 281

ROBO (remote office/branch office), 51

route command, 150, 278

routed mode (Security Appliance), example configuration, 170–172

router ospf command, 283, 286

routing, 269, 281
  authentication, 281
  configuring, 626–630
  IP routing, 277
    dynamic routes, 280–288
    static routes, 277–280
  multicast routing, 289, 292
  commands, 290–293
  debugging, 296
  inbound traffic, 294–295
  outbound traffic, 295–296
  principles, 273

Routing tab (ASDM), 474

Q-R

QTIQBE, application inspection, 593

queries, DNS, 9

RADIUS (Remote Authentication Dial-In User Service), 520

reassigning monitored ports (application inspection), 600

reconnaissance attacks, 9–10

recording global information, 626

reconnaissance attacks, 9–10

recording global information, 626
RPC (remote-procedure call), 117
rsh, application inspection, 608
RTSP (Real-Time Streaming Protocol), application inspection, 591
running configuration, removing security contexts from, 234

saving Security Appliance configuration to Flash memory, 154
scalability of AVVID, 15
scanning
Cisco Secure Scanner, 13
horizontal, 9
vertical, 9
SCCP (Skinny Client Control Protocol), application inspection, 597–598
SCEP (Simple Certificate Enrollment Protocol), 45, 68
Secure Intrusion Detection Sensor, 44, 67
security
ASA, 32, 41–43
firewalls, 27, 31
packet filtering, 27–29
PIX, 31–34
proxy servers, 29
stateful inspection, 30–31
network security, 7
as “legal issue,” 13
optimizing, 13
policies, 11, 18
testing, 13
threats, 8, 17
traffic, transport protocols, 113, 118
types of attacks, 8, 11
vulnerabilities, 8

Security Appliance. See Cisco Security Appliance
security contexts, 47, 226
accessing, 234
configuring, 235–240
creating, 230
deleting, 234
interfaces, allocating, 230–232
status, displaying, 235
switching between, 234
unsupported features, 227
security levels of interfaces, 143
Security Plus Software License, 64
Security Policies tab (ASDM), 467, 471–472
segments, 113
DMZ, 125
server command, 91
servers
AAA
configuring, 542, 573
identifying, 542, 545
specifying, 541
CSACS, 45, 521, 537
installing, 533
users, 555
verifying, 581
filters, identifying, 503
NAS, 518, 541
identifying, 542, 545
NetMeeting, 550
PFSS, 251
Syslog, 251, 262–263
service object type parameter (object-group command), 191
service policies, 46
configurations, viewing, 217
first-match classification policy, 217
interface-specific, 216
matching logic, 216
multimatch classification policy, 216
statistics, viewing, 217
services, authentication, 549
sessions, 440
set connection command, 214
setting up AIP-SSM module, 613–615
severity levels (syslog), 253
SHA-1 (Secure Hash Algorithm 1), 335
shell authorization sets, assigning to NDGs, 562
shell command authorization, configuring, 561, 565
shell configuration, 465
show aaa-server command, 578
show accounting command, 579
show activation-key command, 88
show command, 578, 645
VPNs, troubleshooting, 356–358
show conn command, 128
show context command, 235
show mac-address-table command, 169
show mode command, 228
show object-group command, 190
show ospf command, 288
show perfmon command, 509
show route command, 280
show run policy-map command, 214
show running-config service policy command, 217
show service-policy command, 217–218
show tech-support command, 99
show url-cache command, 508
show url-server stats command, 508
show version command, 86
show vpdn command, 439, 441
show vpdn ppinterface command, 440
show xlate command, 127
single context mode, 227
    changing to multiple-mode, 228
SIP (Session Initiation Protocol), application inspection, 598
site-to-site VPNs, 331
    creating with ASDM VPN Wizard, 482–486
SMTP, application inspection, 195, 606–607
SNMP (Simple Network Management Protocol), 47, 68
    application inspection, 608
    configuring on Cisco Security Appliance, 98
    MIBs, 97
    requests, 261
    system maintenance, 97
    traps, 261
software requirements for ASDM, 458–459
SPARC, requirements for running ASDM, 460
specifying AAA servers, 541
speed command, 148
SPIs (Security Parameter Indexes), 334
spoofing, 28
SQL*NET, application inspection, 609
SSH, accessing Cisco Security Appliance, 80–82
SSM (Service Security Module), 49
standby unit, 307
    configuration replication, 310–311
Startup Wizard (Cisco Security Appliance Adaptive Security Device Manager), 464
state tables, 30, 42
stateful failover, 311–312
    redundancy, 33–34
static command, 123–124, 180
static crypto maps, 414
static IP address mapping, 627
static NAT, 180
static PAT, configuring inbound access on Cisco Security Appliance, 182
static routes, 277
    configuring, 279–280
static translation, 119, 123
statistics, viewing filters, 508
structured threats, 8
SUA (Secure Unit Authentication), 433–434
switch ports, Port Fast, 309
switching between contexts, 234
syslog, 251
    changing message levels, 253
    configuring, 255
        messages at the console, 258
        sending messages to a log server, 259–261
        SNMP traps and SNMP requests, 261
        syslogd servers, 262–263
    "Do I Know This Already?" quiz, 247
    event reporting, 47
    logging facilities, 252
    messages
        disabling, 264
        EMBLEM format, 261
        organizing, 254
        reading, 254
        sending to a Telnet session, 259
    severity levels, 252–253
    support, 47, 68
    viewing logging with PDM, 256
syslogd servers, 262–263
sysopt uauth allow-http-cache command, 548
system clock, configuring on Cisco Security Appliance, 162–163
system maintenance
    activation keys, upgrading, 88–89
    "Do I Know This Already?" quiz, 75
    command-level authorization, 82–85
    creating boothelper disks, 92–93
    OS, installing, 85–87
password recovery, 93–94
  on diskless PIX Firewalls, 95
  on PIX Firewall 520, 94–95
SNMP, 97
system requirements, CSACS, 522

T
TACACS+ (Terminal Access Controller Access Control System Plus), 520
  reports, viewing, 571–572
  shell command authorization, configuring, 561
tagging. See Ethernet VLAN tagging, 273
TCP
  three-way handshake, 115
  virtual circuits, 114
TCP intercept, configuring inbound access on Cisco Security Appliance, 182
Telnet
  Cisco Security Appliance, accessing, 79–80
  Virtual Telnet, 549
telnet command, 79
testing
  security, 13
  Security Appliance connectivity, 152–153

tftp flash command, performing OS upgrades, 89–90
threats, 8, 17
three-way handshake (TCP), 115
throughput, 49, 61
time settings, configuring NTP on Cisco Security Appliance, 160–162
timeout uauth command, 553
timeouts, authentication, 553
tokens, X.509 certificate support, 45, 67
traffic, 31
  cut-through proxy, 519
  routing, 269
  principles, 273
  stateful inspection, 30
traffic classes
  assigning matches to, 207–213
  assigning policies to, 208–209
    connection policy, 213
    inspect policy, 211–212
    IPS policy, 212–213
  police policy, 209–210
  priority policy, 210
traffic flow matching, class maps
  creating, 203–205
  matches
    criteria, viewing, 207
    defining, 206
traffic management in transparent mode, 168–169
transform sets, 350
  creating, 412
translation. See also address translation
  bidirectional, 126
  flags, 128
  multiple, configuring, 124–126
translation slots, 116
transparent firewalls, 48
transparent mode
  configuring, 165–167
  example configuration, 172–173
  traffic management, 168–169
transparent tunneling, 425
transport protocols, 113, 118
  TCP, 114–118
  UDP, 114–117
traps (SNMP), 97, 261
Trojan horses, 10
troubleshooting. See also debugging; system maintenance
  AAA, 577, 581
  accounting, 579
  address translation, 126, 130
  authentication, 578
  authorization, 579
  boothelper disk, 93
  commands, 100–103
  password recovery, 93–95
  PIX Firewall implementation, 649–658
  security, 13
  Syslog, 251
  VPNs, 356, 644
    clear command, 358
    debug command, 358–360
    show command, 356, 358
troubleshooting-related commands, 98–99, 101–103
trunk ports, 274
tunneling protocols
Cisco VPN Software Client, 420
transparent, 425
types of attacks, 8
access, 10–11
DoS, 11
reconnaissance, 9–10

UDP (User Datagram Protocol), 114–117
unauthorized access, 10
unprivileged administrative access mode, 141
unstructured threats, 8
unsupported security context features, 227
upgrading
activation keys, 88–89
operating system
with copy tftp flash command, 89
with HTTP client, 92
with monitor mode, 90–91
with tftp flash command, 89–90
uploading configuration files to contexts, 232
upper-level data encapsulation, 114
url-cache command, 505
URL filtering, 503–505
configuring URL-filtering policy, 504
identifying servers, 503
url-server command, 503
User Datagram Protocol (UDP), 114

VAC (VPM Accelerator Card), 48
VAC+ (VPN Accelerator Card Plus), 48
verifying
AIP-SSM initialization, 613
context mode of operation, 228
CSACS, 581
Security Appliance connectivity, 152–153
X.509, 45
vertical scans, 9
viewing
class map match criteria, 207
filters, 508
logging, 256
policy map configurations, 214
reports, 570–572

service policy configurations, 217
service policy statistics, 217
status of security contexts, 235
virtual circuits, 114
virtual HTTP, configuring inbound connections, 552
virtual interfaces, 54
virtual services, authentication, 549
virtual Telnet, configuring outbound connections, 550
virtual telnet command, 549
viruses, 10
Virtual Telnet, 549
VLANs
managing, 276–277
trunk ports, 274
VoIP, application inspection, 592
H.323, 593–595
MGCP, 596–597
QTIQBE, 593
SCCP, 597–598
SIP. 598
VPDN (Virtual Private Dial-Up Networking)
group, 438
VPN Accelerator Card Plus (VAC+), 48
VPN tab (ASDM), 473–474
vpnclient server command, 432
vpnclient vpgroup command, 432
VPNs (virtual private networks)
access VPNs, 395
certificates, 45
configuring, DUKEM case study, 635, 638, 641–644
gateways, 48, 69
Cisco Security Appliance
colfiguration, 343–355
IPsec, 332–338
remote access, DUKEM case study, 645
troubleshooting, 356, 358, 360, 645
WebVPNs, 339
port forwarding, 342
portal interface, 340
vulnerabilities, 8
W
WebVPN gateways, 339
  ACLs, configuring, 371
  configuring, 361–364
  content filtering, 371
  e-mail proxies, configuring, 369–371
  port forwarding, configuring, 342, 367–368
  portal interface, 340
  user access, assigning, 364–365, 367

Windows 2000/XP OS
  accessing from browser, requirements, 460
  CSACS, 533
  CSACS 3.3, installing, 523–533

Windows NT
  CSACS, 533
  CSACS 3.3, installing, 523–533

worms, 10
write memory command, 80, 154, 311

X-Y-Z
X.509 certificates, 45
XAUTH (extended authentication)
  configuring, 409–412, 414–416
  defining group policy for mode
  configuration push, 412
  transform sets, 413
xlate command, 120