INDEX

Numerics

3DES, 484
500 series PIX Firewall, 27
PIX Firewall 501, 29–32
PIX Firewall 506E, 32
PIX Firewall 515E, 33–36
PIX Firewall 525, 37–39
PIX Firewall 535, 40–43

AAA (authentication, authorization, and accounting), 391–392
accounting
  configuring, 428–431
  viewing information, 431–432
authentication
  with FTP, 393
  with HTTP, 393
  with Telnet, 393
authorization
  adding rules, 421, 423
  configuring, 419–420
server groups, 409, 681–683
supported protocols, 395
AAA Flood Guard, 370
ABRs (Area Border Routers), 308
access attacks
  unauthorized data retrieval, 7
  unauthorized privilege escalation, 8
  unauthorized system access, 7
access modes (CLI), 85
access rules (Firewall MC), configuring, 710–716
Access Rules tab (PDM 3.0 configuration screen), 162–164
access-group command, 243, 248–249, 506
accessing Firewall MC console, 651
  from CiscoWorks, 648–649
access-list command, 244, 504
  arguments, 246–248
accounting, 391
  configuring, 428–431
  viewing information, 431–432
ACLs (access control lists), 17
  applying to interfaces, 243
  inside interfaces, 256–257
  combining with conduit configuration, 254
  creating from conduits, 255–256
  downloadable, 423–424
  configuring, 426–427
  editing, 245
  filtering inbound traffic, 248–249
  filtering malicious active codes
  ActiveX controls, 263–264
  Java applets, 263
  guidelines for implementing, 244
  misconfiguration, 254–255
  object groups, 281–282
  configuring, 284–288
  nested, 288–292
  removing, 291
  permitting web access to DMZ, 258–259
  Turbo ACLs, 250–251
  versus conduits, 252–253
activating AUS, 757
activation keys, 48, 616–617
troubleshooting upgrades, 618–619
ActiveX control filtering, 263–264
activities, 656
  committed, 659
  submitting for approval, 720
Activity Management Interface, 657
adding
  authorization rules, 421–423
  users to CSACS, 404–407
adding cryptographic services to PIX Firewall, 48
Address Translation Pool, 683–684
adjusting failover poll time, 463
administration of Firewall MC
  maintenance, 733–734
  workflow setup, 731–732
advanced protocols, 333
AES, 484
agents, 608
alias command
  DNAT, 220–222
  DNS doctoring, 218–220
  translating embedded IP addresses, 217–218
antispoofing, 375
any keyword, caveat against using, 507
application inspection
configuring, 334–337
FTP, 340–341
H.323, 350–352
rsh, 341–343
RTSP, 350
SCCP, 345
SIP, 345
SQL*Net, 343–344
applications, multimedia, 346–347
RealNetworks RDT mode, 349–350
RTSP, 348
applying ACLs to interfaces, 243
inside interfaces, 256–257
approval process for Firewall MC tasks, 654, 720
A-records, embedded IP addresses, translating
with alias command, 217–218
with expanded NAT, 222–223
arguments
access-group command, 248–249
clear object group, 291
clock command, 101
conduit command, 215–216
extended static command, 207
filter url | ftp | https command, 267
fixup command, 334–337
for access-list command, 246–248
for failover command, 456
icmp command
type literals, 262
interface command, 107–109
ip address command, 110
logging command, 117–119
mroute command, 325
nat access-list command, 249
nat command, 198–200
object-group command, 283
of enable command, 86
port-object command, 286
prefix-list command, 317–318
RIP command, 307
route command, 114
route-map command, 318–320
router ospf command, 312–315
routing interface command, 316–317
show aaa-server command, 432–433
show auth-prompt command, 433
show conn command, 213
show object-group command, 290
static command, 203
tftp-server command, 90
url-server command, 266
ASA (Adaptive Security Algorithm), 21, 334
application inspection, 334
configuring, 334–337
security levels, 103, 105
ASBRs (Autonomous System Boundary
Routers), 308
assembling fragments, 367–370
assigning
IP address to interface, 109–110
names to interfaces, 106–107
public IP addresses to internal hosts, 112–113
static IP address to inside interface, 125
Assignments tab (AUS), 768, 771–772
associations, professional development security, 837
attack guards
AAA Flood Guard, 370
antispoofing, 375
DNS Guard, 365–366
FragGuard, 367–370
Mail Guard, 363–365
SYN Flood Guard, 370–375
Virtual Re-assembly, 367–370
attack-class signatures, 377
attacks
access, 7
unauthorized data retrieval, 7
unauthorized privilege escalation, 8
unauthorized system access, 7
reconnaissance, 7
shunning, 381, 383
augmenting global pools with PAT, 227
AUS, 753
activating, 757
Assignments tab, 768, 771–772
deployment feature, 762–763
Devices tab, 765–767
enabling communication with PIX Firewall,
758–760
features, 753
Files tab, 767–768
installing, 754–756
verifying client access requirements, 755
verifying server requirements, 754
interaction with Firewall MC, 754
interface elements, 763–765
launching, 763
reporting and administration feature, 772–774
changing database passwords, 777–778
event reports, 774–776
NAT settings, 776
unique identity feature, 760–761
authentication
challenge prompts, changing, 418–419
configuring on CSACS, 407–411
cut-through proxy, 21–22, 394–395
of console access, 415–416
on Virtual Telnet, 412–413
with FTP, 393
with HTTP, 393
with Telnet, 393
with Virtual HTTP, 413–415
authorization, 391–392. See also command authorization
adding rules, 421–423
configuring, 419–420
downloadable ACLs, 423–424
configuring, 426–427
auth-prompt command, 418–419
available memory, displaying, 93
AVVID. See Cisco AVVID

B
backing up PAT addresses, 227
backup gateways, 513
bootstrapping PIX Firewall with Firewall MC, 645–648
broadband connections, PPPoE, 128–129
configuring on PIX Firewall, 130–133
monitoring sessions, 133–134
building blocks (Firewall MC)
AAA server groups, 681–683
Address Translation Pool, 683–684
network objects, 672, 675
service definitions, 676–678
service groups, 678–680

cable-based failover, configuring, 454–461
CAs, 485–486
available resources on Internet, 841
peer enrollment, 487–488
command authorization, 845
case studies, three-site full-mesh IPSec tunnels
using preshared keys, 540–542
Catalyst 6500 Series switch
 FWSM, 44–46
requirements, 793
Switch Fabric Module, 45–47
CBAC (Context-Based Access Control), 18
certificate authority, PKI resources, 841
challenge text, changing authentication prompts, 418–419
changing authentication timeouts, 417
characteristics of UDP, 195–197
Cisco website, 840
Cisco 7600 series Internet router, FWSM, 44–46
Switch Fabric Module, 45–47
Cisco AVVID, architectural components, 12–13
Cisco PIX 501, notebook-locking slot, 808
Cisco PIX Firewall
 DMZ support, 54
selecting appropriate model, 55–56
Cisco PIX Firewall 500 series, 27
 PIX Firewall 501, 29–30, 32
 PIX Firewall 506E, 32
 PIX Firewall 515E, 33–36
 PIX Firewall 525, 37–39
 PIX Firewall 535, 40–43
Cisco SAFE Blueprint, 13–14
benefits of implementing, 14–15
CiscoWorks
 accessing Firewall MC, 648–649
Firewall MC, user management, 649–650
CiscoWorks Common Services, 641
clear access-list command, 245, 506
clear command, 92
clear fragment command, 370
clear object-group command, 291
clearing
 DHCP default routes, 305
 Flash memory configuration, 89
CLI (command-line interface)
 access modes, 85
 obtaining help, 85
clock command, 99–101
command authorization, 599
 CSACS, 604–606
 enable level passwords, 599–601
 local user database, 602–604
 TACACS, 392
 viewing configuration, 606–607
command channel (standard mode FTP), 337–338
commands
  access-group, 243, 248–249, 506
  access-list, 244, 504
  arguments, 246–248
  alias
    DNAT, 220–222
    DNS doctoring, 218–220
  assigning privilege levels, 600
  auth-prompt, 418–419
  ca, options, 489–491
  clear, 92
  clear access-list, 245, 506
  clear fragment, 370
  clear object-group, 291
  clock, 99–101
  conduit, 215–216
  configure net, 90
  configure terminal, 87
  crypto ipsec security-association lifetime,
    504, 511
  crypto ipsec transform-set, 504, 509
  crypto map map-name interface, 505
dhcpd, 122
  enable, 86
  failover, 456
  fixup, 334–337
  fixup protocol skinny, 346
  fragment, 368–369
  global, 112–113
  hostname, 87
  icmp, 261
    arguments, 262
  igmp forward command, 322
  igmp join-group, 323
  interface, 107–109
  ip address, 109–110
  ip audit, 378–380
  logging, 117–119
  logging console, 115
  logging message, 116
  mroute, 325
  multicast interface, 322–324
  name, 91–92
  nameif, 106–107
  nat, 110, 112
  nat access-list, 249
  ntp server, 102–103

object-group, 283–284
  arguments, 283
  PDM support, 151
  ping, 98–99
  port-object, 286
  prefix-list, arguments, 317–318
  reload, 92
  rip, 307
  route, 114–115, 303
  route-map, 318–320
  routing interface, 316
  arguments, 316–317
  show aaa-server, arguments, 432–433
  show access-list, 244–245
  show auth-prompt, arguments, 433
  show conn, 212–213
  show cpu usage, 98
  show flashfs, 152
  show fragments, 370
  show history, 89
  show interface, 94–98
  show ip address, 94
  show local-host, 372
  show memory, 93
  show object-group, 290
  show running-config, 89
  show version, 93–94
  shun, 381, 383
  static, 203, 372
  port redirection, 228
tftp-server, 89
timeout uauth, 417
url-server, 266
vpngroup, 556
write erase, 89, 646
write memory, 89, 450
write net, 90–91
write term, 291
write terminal, 89
xlate, 212
committed activities, 659
communication, enabling between AUS and PIX
Firewall, 758–760
communities, 608
comparing
  Cisco PIX Firewall models, 56
  conduits and ACLs, 253
components of Cisco AVVID framework, 12–13
conduit command, 215–216
conduits, 214
  combining with ACL configuration, 254
  converting to ACLs, 251–253
ICMP, 216
configurable proxy pinging, 261
configuration elements (Firewall MC), 640–641
configuration files
  deploying in AUS, 762–763
  IPSec, 508, 511, 513–518
    pre-shared keys, 501
    verifying, 518–519
  reloading, 92
storing on TFTP server, 90–91
configuration replication, 450–451
configuration screen (PDM)
  Access Rules tab, 162–164
  Hosts/Networks tab, 169–171
  System Properties tab, 171–174
  Translations Rules tab, 165–167
  VPN tab, 167
configure net command, 90
configure terminal command, 87
configuring
  AAA
    accounting, 428–432
    authorization, 419–423
  ACLs and conduits in same configuration, 254
  application inspection, 334–337
  authentication on CSACS, 407–411
  crypto maps, 512
  DHCP client, 812
  DHCP relay agent, 126–127
  DHCP server, 120–126
  downloadable ACLs, 426–427
failover
  cable-based, 454–461
  LAN-based, 461–466
Firewall MC
  access rules, 709–716
  building blocks, 672–684
  Easy VPN Remote, 700–702
  Firewall Device Contact Information feature, 705–707
  import device setting, 704–705
  logging, 695–700
  management features, 702–704
  settings, 684–694
  translation rules, 716–720
FragGuard, 368
FWSM, 797
  initialization, 798–800
  interface configuration, 802
  VLAN switch configuration, 800–801
  with PDM, 803
IDSs, 378–380
IGMP, 326–327
IP multicast
  multicast transmission forwarding, 325–326
  multicast transmission reception, 322–325
multiple interfaces, security levels, 229–232
name-to-IP address mappings, 91–92
NAT, conduits, 214–216
nested object groups, 289–292
object groups, 283–284
  ICMP-type object groups, 287–288
  network object groups, 285–286
  protocol object groups, 287
  service object groups, 286–287
OSPF, 311–312
  router ospf command arguments, 312–320
PIX Firewall, responding to prompts, 87–88
PPPoE on PIX Firewall, 130–133
protocol fixup, FTP, 340–341
remote access
  with SSH, 594–598
  with Telnet, 591, 593–594
remote access VPNs, 555
  groups, 556–558
  PPTP client configuration, 565
  preshared keys for ISAKMP authentication, 558–564
RIP, 305–307
site-to-site VPNs, 495–499
  IKE parameters, 500–504
  IPSec parameters, 504–509
  verifying configuration, 519
  with Easy VPN technology, 520–526
  with PDM, 526–531
SNMP, 611–613
  static IP addresses, 125
  system clock, daylight savings time, 100–101
  transform sets, 509–511
connections
  conduits, 214
  embryonic, 194
  translations, 212–213
connectivity, ping command, 98–99
console (PIX Firewall), requiring authentication, 415–416
converting conduits to ACLs, 251–256
cracking tools, 840
creating, 501
crypto maps, 531
Firewall MC job tasks, 723, 726
IPSec rules, 533
new activities in Firewall MC, 6557–660
new device groups in Firewall MC, 661–662
object groups, 283–284
ICMP-type object groups, 287–288
nested, 289–292
network object groups, 285–286
protocol object groups, 287
service object groups, 286–287
privileged mode passwords, 86
crypto access lists, 508
crypto ipsec security-association lifetime command, 504, 511
crypto ipsec transform-set command, 504, 509
crypto map map-name interface command, 505
crypto maps, 513–518
configuring, 512
creating, 531
cryptographic services, adding to PIX Firewall, 48
CSACS
accounting, viewing information, 431–432
adding users, 404–407
authentication, configuring, 407–411
command authorization, 604–606
downloadable ACLs, 423–424
configuring, 426–427
installing on Windows NT, 396–403
CSI (Computer Security Institute), 5
CSPM, 614–616
cut-through proxy, 21–22
cut-through proxy operation, 394–395

D

data channel (standard mode FTP), 337–338
daylight savings time, configuring on system clock, 100–101
DDoS attacks, 8
default access rules (Firewall MC), 709
default routes, 303
configuring on interface, 114–115
defining IKE policies, 486
deleting PIX configuration files, 768
deploying
Firewall MC job tasks, 727–728
network security, 8–9
improving security, 11
monitoring the network, 11
securing the system, 10
deployment feature (AUS), 762–763
DES (Data Encryption Standard), 483–484
DES Cracker, 484
designing secure networks
DMZs, 54
enterprise network scenario, 57–66
large company network scenario, 66–71
medium business network scenario, 72–76
small business network scenario, 72–76
SOHO network scenario, 76–80
device groups, creating in Firewall MC, 661–662
devices
assigning to images, 768, 771–772
importing in Firewall MC, 663–669
managing in Firewall MC, 670–672
supported by Firewall MC, 641
Devices tab (AUS), 765, 767
D-H, 484
DHCP (Dynamic Host Configuration Protocol)
configuring, 120–126
default routes, clearing, 305
lease information, viewing, 109
server functionality, 810–811
DHCP client
configuring, 812
functionality, 811
DHCP relay agent
configuring, 126–127
functionality, 811
dhcpd address command, 122
disabling
HTTP fixup, 337
pinging to PIX Firewall interface, 261
displaying
command history, 89
configured object groups, 290
failover protection

33

CPU usage, 98
failover status, 466
IP address of network interface, 94
memory statistics, 93
network interface, statistics, 94–98
PIX Firewall software version, 93–94
distance-vector routing protocols, 308
DMZs, 54
partner web access, configuring, 259
permitting web access, ACL configuration, 258–259
DNAT (destination NAT), 217–222
DNS
A-records, translating embedded IP addresses, 217–218, 222–223
doctoring, 218, 220
DNS Guard, 365–366
downloadable ACLs, 423–424
configuring, 426–427
downloading PDM, 150
dynamic inside translations, 198–202
dynamic outside translations, 205–206
dynamic routing, 305
OSPF, 307
ABRs, 308
ASBRs, 308
configuring, 311–320
LSAs, 308
security considerations, 309
supported features on PIX
Firewall 6.3, 310
unsupported features on PIX
Firewall 6.3, 311
RIP, 305–307
dynamic translation rules, configuring, 718, 720

E

Easy VPN
configuring site-to-site VPNs, 520–526
remote configuration, 537
Easy VPN Remote
configuring, 700–702
functionality in SOHO devices, 809–810
editing
ACLs, 245
service groups, 680

elements of Firewall MC interface, 652–653
e-mail, Mail Guard, 363–365
embryonic connections (TCP), 194
enable command, 86
enable level passwords, command authorization, 599–601
enabling
interface, 107–109
IPSec encryption, 482
NAT on PIX Firewall, 110–112
encryption, IPSec
3DES, 484
AES, 484
DES, 483
D-H, 484
enabling, 482
MD5, 484
SAs, 482
SHA-1, 484
enrollment process (CAs), 487–488
entering commands in CLI, 85
enterprise networks, implementing network security, 57–63, 66
event reports, 774–776
expanded NAT, translating embedded IP addresses, 222–223
expanded static command, 207
exploits, OS, 839
external threats, 6
extranet VPNs, 480

F

failover, 23
viewing status, 466
failover command, arguments, 456
failover licensing, 48
failover protection, 449
cable-based, configuring, 454–461
configuration replication, 450–451
failover interface tests, 452
hardware requirements, 453
IP addresses, 450
LAN-based, configuring, 461–466
licensing requirements, 454
stateful failover, 451–452
features

of AUS, 753
  reporting and administration, 772–774
  changing database passwords, 777–778
  event reports, 774–776
  NAT settings, 776
of Firewall MC, 640
  configuration elements, 640–641
  Report feature, 729
  Support page, 730–731
of FWSM, 791–792
  versus PIX Firewall features, 792–793
of IKE, 485–486
of PIX Firewall for SOHO deployments, 808
  DHCP client functionality, 811
  DHCP relay functionality, 811
  DHCP server functionality, 810–811
  Easy VPN Remote functionality, 809–810
  PDM, 809
  PPPoE client functionality, 810
of VPN client, 553–554
Files tab (AUS), 767–768
filtering
  malicious active codes
    ActiveX controls, 263–264
    Java applets, 263
    URLs, 265–267
    long URLs, 268–269
Finesse operating system, 20
Firewall MC, 639
  accessing from CiscoWorks, 648–649
  user management, 649–650
administration
  maintenance, 733–734
  workflow, 731–732
bootstrapping a PIX Firewall, 645–648
features, 640
  configuration elements, 640–641
  Report feature, 729
  Support page, 730–731
GUI, 652–653
installing, 641–645
  system requirements, 642–643
interaction with AUS, 756
launching, 651
supported devices, 641
task workflow, 653–654
  configuring access, 709–710
  configuring access rules, 710–716
  configuring building blocks, 672, 675–684
  configuring Firewall Device Contact Information, 705–707
  configuring import device setting, 704–705
  configuring management features, 702–704
  configuring settings, 684–702
  configuring translation rules, 716–720
  creating device groups, 661–662
  creating job task, 723, 726
  creating new activities, 655–660
  deploying jobs, 727–728
  importing devices, 663–669
  managing devices, 670–672
  viewing configuration, 720
firewalls
  packet filtering, 17–18
  proxy servers, 19
  stateful packet filters, 19
  translations, 197
  connections, 212–213
fixing up
  FTP, 340–341
  H.323, 350–352
  rsh, 341–343
  RTSP, 350
  SCCP, 345
  SIP, 345
  SQL*Net, 343–344
fixup command, 334–337
fixup protocol skinny command, 346
Flash memory, clearing, 89
forcing reauthentication, 417
formatting IKE policies, 501
forwarding IP multicast transmissions, configuring, 325
Franguard, 367–370
  configuring, 368
fragment command, 368–369
free memory, displaying, 93
FTP (File Transfer Protocol)
  authentication, 393
  fixup configuration, 340–341
  passive mode, 338–339
  standard mode, 337–338
full memory test, conducting on FWSM, 804
FWSM (Firewall Services Module), 20, 44–46, 791
  characteristics, 793
  configuring, 797
    initialization, 798–800
    interface configuration, 802
    VLAN switch configuration, 800–801
    with PDM, 803
  features, 791–792
  versus PIX Firewall features, 792–793
memory test, conducting, 804
packet flow, 795–797
rebooting, 804
Switch Fabric Module, 45–47
troubleshooting, 803–804

G
gateways, backup, 513
generating syslog messages, 115–119
global command, 112–113
global IPSec SA lifetimes, 511–512
GRE (Generic Route Encapsulation) tunnels, 322
groups
  AAA servers, specifying, 409
  configuring for remote access VPNs, 556–558
GUI (Firewall MC), 652–653

H
H.323, application inspection, 350–352
half-open connections attacks, SYN Flood Guard, 370–375
hardware requirements for failover, 453
hashing algorithms, SHA-1, 484
help system (CLI), 85
hierarchical object grouping, 288
  configuring, 289–292
history (commands), displaying, 89
host-based IDSs, websites, 838
hostname command, 87
hosts, IDS, 838
Hosts/Networks tab (PDM 3.0 configuration screen), 169–171
HTTP
  authentication, 393
  fixup, disabling, 337
HTTPS, configuring, 692–694

I
IANA (Internet Assigned Numbers Authority), 197
icmp command, 261
  arguments, type literals, 262
ICMP-type object groups, configuring, 287–288
Identity NAT, 210
IDSs, 376–377
  configuring, 378–380
  hosts, 838
  networks, 838
IGMP (Internet Group Management Protocol)
  configuring, 326–327
  IP multicasting, 321
  Leave Group message, 326
  messages
    configuring host forwarding, 325–326
    configuring host reception, 322–325
igmp forward command, 322
igmp join-group command, 323
IKE, 483–486
  policies, 501
  policy parameters, 497–499
    configuring, 500–504
  RSA signatures, 485
IKE Phase 1 policy, 555
images
  deleting, 768
  managing from AUS, 767–768
  upgrading, 621
implementing
  ACLs, guidelines, 244
  Cisco SAFE Blueprint, benefits of, 14–15
  network security, 8–9
    enterprise network scenario, 57–66
    improving security, 11
    large company network scenario, 66–71
    medium business network scenario, 72–76
    monitoring the network, 11
    securing the system, 10
security policies, 53–54
small business network scenario, 72–76
SOHO network scenario, 76–80
importing devices in Firewall MC, 663–669, 704–705
improving network security, 11
inactivity timers, changing authentication timeouts, 417
inbound packets, 252
inbound traffic, filtering with ACLs, 248–249
information-class signatures, 377
initializing FWSM, 798, 800
installing
activation keys, 616–617
AUS, 754–756
verifying client access requirements, 755
verifying server requirements, 754
CSACS on Windows NT, 396–399, 402–403
Firewall MC, 641–645
system requirements, 642–643
interaction of Firewall MC and AUS, 756
interactive setup dialog, PDM preconfiguration process, 157–158
interface command, 107–109
interfaces
applying ACLs, 243
AUS, 763–765
configuring multiple, 229–232
default routes, configuring, 114–115
FWSM, configuring, 802
settings, configuring, 687–689
internal threats, 6
Internet, available security resources, 837–838
Internet Assigned Numbers Authority (IANA), 197
intranet VPNs, 480
intrusion detection, 376–377
intrusion protection, 376
ip address command, 109–110
IP addresses
DHCP, configuring, 120–126
DHCP relay agent, configuring, 126–127
for failover, 450
NAT
Identity NAT, 210
Policy NAT, 211
translations, 110, 112
DNAT, 220–222
DNS doctoring, 218–220
dynamic inside translations, 198–202
dynamic outside translations, 205–206
NAT, 197–198
PAT, 223–228
static inside translations, 203–204
static outside translations, 206–209
ip audit command, 378–380
IP multicasting, 321
configuring host forwarding of multicast transmissions, 325–326
configuring host reception of multicast transmissions, 322–325
GRE tunnels, 322
IGMP, configuring, 326–327
SMR, 322
viewing configurations, 327
IP spoofing, antispoofing, 375
IPSec, 481
3DES, 484
AES, 484
attributes of VPN client, 554–555
CAs, 485–486
peer enrollment, 487–488
configuring, 508, 511–518
preshared keys, 501
verifying, 518–519
DES, 483
D-H, 484
enabling encryption, 482
IKE, 483–486
MD5, 484
NAT-T, 485
parameters, configuring, 504–509
rules, creating, 533
SAs, 482, 485
SHA-1, 484
site-to-site VPNs, configuring, 495–509
supported standards, 483
tunnel mode, 482
tunnel mode, 482
VPN features, 481–482
J-K

Java applet filtering, 263
joining multicast groups, 323
keywords, any, 507

L

LAN-based failover, configuring, 461–466
large company networks, implementing network security, 66–71
launching
   AUS, 763
   Firewall MC, 651
lease information (DHCP), viewing, 109
Leave Group message, 326
legal resources on Internet, 838
licensing options
   for failover, 454
   for PIX Firewall, 47
   for VPNs, 48
link-state protocols, OSPF, 308
   configuring, 311–320
Linux, PDM support, 155
load balancing on PIX Firewall Easy VPN Remote devices, 809
local user database, command authorization,
   602–604
logging, configuring, 695–700
logging command, 117–119
logging message command, 116
long URL filtering, 268–269
lost passwords, recovering, 619–620
LSAs (link-state advertisements), 308

M

magazines, 841
Mail Guard, 363–365
malicious active codes
   ActiveX controls, filtering, 263–264
   Java applets, filtering, 263
managed devices, 608
managed objects, 608
management features, configuring, 702–704
management tools, 614
CSPM, 614, 616
PDM, 150–151, 614
   Access Rules tab (configuration screen), 162–164
   as command-learning tool, 151
   Hosts/Networks tab (configuration screen), 169–171
   monitoring screen, 175
   operational requirements, 151–155
   Options menu, 175
   preconfiguration process, 156–158
   Startup Wizard, 155, 159
   System Properties tab (configuration screen), 171–174
   Tools menu, 175
   Translations Rules tab (configuration screen), 165–167
   VPN tab (configuration screen), 167
managing devices in Firewall MC, 670–672
mandatory access rules (Firewall MC), 709
mapping subnets to PAT addresses, 226
MD5, 484
medium business networks, implementing network security, 72–76
memory
   displaying statistics, 93
   requirements for Turbo ACLs, 250–251
   testing on FWSM, 804
messages
   DHCP, 120
   syslog, generating, 115–119
MIBs, 608–611
misconfiguring ACLs, 254–255
monitoring
   network activity, 11
   PPPoE on PIX Firewall, 133–134
Monitoring screen (PDM), 175
mroute command, 325
multicast groups, joining, 323
multicast interface command, 322–324
multicasting, 321
   configuring host forwarding of multicast transmissions, 325–326
   configuring host reception of multicast transmissions, 322–325
   GRE tunnels, 322
multimedia application support, 346–347
H.323 fixup, 350–352
RealNetworks RDT mode, 349–350
RTSP
fixup, 350
standard RTP mode, 348
multiple interfaces, configuring, 229–232

name command, 91–92
nameif command, 106–107
names, assigning to PIX Firewall interfaces, 106–107
name-to-IP address mappings, configuring, 91–92
NAT (Network Address Translation)
conduits, 214
ICMP, 216
DNAT, 220–222
dynamic inside translations, 198–202
dynamic outside translations, 205–206
enabling on two interfaces, 201
Identity NAT, 210
Policy NAT, 211
static inside translations, 203–204
static outside translations, 206–209
supported address translations, 197–198
nat access-list command, 249
nat command, 110–112
NAT-T, 485
need for network security, 5
negotiation (transform sets), configuring, 511
nested object groups, 288
configuring, 289–292
network interface
IP address, viewing, 94
statistics, displaying, 94–98
network objects 672, 675
groups, configuring, 285–286
NMSs, 608
notebook-locking slot (PIX 501), 808
ntp server command, 102–103

O
object groups, 281–282
configuring, 283–284
ICMP-type object groups, configuring, 287–288
nested, 288–292
network object groups, configuring, 285–286
protocol object groups, configuring, 287
removing, 291
service object groups, configuring, 286–287
object-group command, 283–284
operating systems
exploits, 839
Finesse, 20
PDM support
Linux, 155
Sun Solaris, 154
Windows, 153–154
Windows NT, installing CSACS, 396–403
operational requirements, PDM, 151–155
Linux, 155
Sun Solaris, 154
Windows, 153–154
options, ca command, 489–491
Options menu (PDM 3.0 configuration screen), 175
OSPF (Open Shortest Path First), 307
ABRs, 308
ASBRs, 308
configuring, 311–320
LSAs, 308
security considerations, 309
supported features on PIX Firewall 6.3, 310
unsupported features on PIX Firewall 6.3, 311
OSs. See operating systems

P
packet filtering, 17–18
stateful, 19, 22
packet flow through FWSM, 795–797
packets, inbound, 252
parameters
ca command, 489–491
crypto maps, 513
IPSec, configuring, 504–518
passwords
  configuring, 691
  enable level, command authorization, 599–601
  privileged mode, setting, 86
  recovering, 619–620
PAT (port address translation), 223–224
  augmenting global pools, 227
  backing up PAT addresses, 227
  mapping subnets to PAT addresses, 226
  static PAT, port redirection, 227–228
  using outside interface address, 225
PDM (PIX Device Manager), 149–151, 614, 809
  as command-learning tool, 151
  Configuration screen
    Access Rules tab, 162–164
    Hosts/Networks tab, 169–171
    System Properties tab, 171–174
    Translations Rules tab, 165–167
    VPN tab, 167
downloading, 150
FWSM configuration, 803
Monitoring screen, 175
  operational requirements, 151–155
    Linux, 155
    Sun Solaris, 154
    Windows, 153–154
Options menu, 175
PIX Firewall CLI command handling, 157
preconfiguration process, 156–157
  interactive setup dialog, 157–158
remote access VPN configuration, 568, 573
Startup Wizard, 155, 159
  supported commands, 151
  Tools menu, 175
  versions, 150
VPNs, configuring, 526–531
peer enrollment, CAs, 487–488
periodicals, 841
permitting web access to DMZ, ACL configuration, 258–259
PFTP (passive mode FTP), 338–339
ping command, 98–99
pinging PIX Firewall interfaces, 261
PIX Firewall version, configuring, 686–687
PIX VPN topologies, 480–481
PLI, certificate authority resources, 841

policies, IKE, 497–499
  configuring, 500–504
  creating, 501
  parameters, 486
Policy NAT, 211
port numbers, PAT, 223–224
port redirection, 227–228
portals, security, 839
port-object command, 286
PPPoE client, 128–129
  configuring on PIX Firewall, 130–133
  functionality in PIX Firewall 6.2, 810
  monitoring, 133–134
PPTP, configuring remote access VPNs, 565
pre-authentication with Virtual Telnet, 412–413
preconfiguration process, PDM, 156–157
  interactive setup dialog, 157–158
prefix-list command, arguments, 317–318
preshared keys, 555
primary PIX Firewall, failover protection
  cable-based configuration, 454–461
  configuration replication, 450–451
  failover interface tests, 452
  hardware requirements, 453
  IP addresses, 450
  LAN-based configuration, 461–466
  licensing requirements, 454
  stateful failover, 451–452
privilege levels, assigning commands, 600
privileged mode password, setting, 86
professional development associations, web sites, 837–838
prompts (configuration), responding to, 87–88
protocol fixup
  configuring on FTP, 340–341
    H.323, 350–352
    rsh, 341–343
    RTSP, 350
    SCCP, 345
    SIP, 345
    SQL*Net, 343–344
protocol object groups, configuring, 287
proxy servers, 19
public IP addresses, assigning to internal hosts, 112–113
public-key cryptography, RSA signatures, 485
R

RDT mode (RealNetworks), 349–350
RealNetworks RDT mode, 349–350
rebooting FWSM, 804
recommended reading, 841
reconnaissance attacks, 7
reconnaissance tools
UNIX, 838
Windows, 839
recovering lost passwords, 619–620
redundancy. See failover protection
reload command, 92
remote access
with SSH, 594–598
with Telnet, 591–594
remote access VPNs
configuring, 555
configuring with PDM, 568, 573
groups, configuring, 556–558
IKE Phase 1 policy
presheared keys for ISAKMP
authentication, configuring, 558–564
PPTP client configuration, 565
remote configuration, Easy VPN, 537
remote users of VPN client, 552
removing object groups, 291
Report feature (Firewall MC), 729
reporting and administration feature of AUS,
772–774
changing database passwords, 777–778
event reports, 774–776
NAT settings, 776
requirements for failover support, 453–454
requiring authentication of console access, 415–416
resetting FWSM, 804
resources
certificate authority (PKI), 841
legal, 838
security, 837, 841
SSH, 840
responding to PIX Firewall configuration
prompts, 87–88
restricted licensing for PIX Firewall, 47
RIP (Routing Information Protocol), configuring,
305–307
rip command, 307
route command, 114–115, 303
route-map command, 318–320
router ospf command, arguments, 312–315
routing
dynamic, 305
OSPF, 307–320
RIP, 305–307
static, 303
routing interface command, 316
arguments, 316–317
RSA signatures, 485
rsh (remote shell), application inspection, 341–343
RTSP, 347
application inspection, 350
S

SA, 482, 485
crypto maps, configuring, 513–518
SCCP, application inspection, 345
script kiddies, 6
secondary PIX Firewall, failover protection, 450
security, 482, 501
AAA, 391–392
Attack Guards, SYN floodguard, 372–374
portals, 839
resources, 837, 841
VPN, DES, 484
security levels (ASA), 103–105
security wheel, 53
selecting appropriate PIX Firewall model, 55–56
servers
AAA, 392
specifying groups, 409
SYN floodguard, 372–374
service definitions, 676–678
service groups, 678–680
service object groups, configuring, 286–287
session establishment, TCP, 194
setup dialog, responding to configuration prompts,
87–88
SH-1, 484
show aaa-server command, arguments, 432–433
show access-list command, 244–245
show auth-prompt command, arguments, 433
show conn command, 212–213
show cpu usage command, 98
show flashfs command, 152
show fragment command, 370
show history command, 89
show interface command, 94–98
show ip address command, 94
show local-host command, 372
show memory command, 93
show object-group command, 290
show running-config command, 89
show version command, 93–94
shun command, 381–383
signatures, 376
attack-class, 377
information-class, 377
SIP (Session Initiation Protocol), application inspection, 345
site-to-site VPNs
configuring, 495–499
with Easy VPN technology, 520–526
with PDM, 526–531
with VPN Wizard, 533–536
crypto maps, creating, 531
IKE parameters, configuring, 500, 502–504
IPSec
parameters, configuring, 504–509
rules, creating, 533
verifying configuration, 519
small business networks, implementing network security, 72–76
SMR (Stub Multicast Routing), 322
viewing configurations, 327
SMTP fix up, 337
SNMP (Simple Network Management Protocol), 607
configuring, 611–613
discovery tools, 839
MIBs, 609–611
operations, 608–609
software images
managing from AUS, 767–768
upgrading, 621
software version (PIX Firewall), displaying, 93–94
SOHO (small office home office)
implementing network security, 76–80
PIX Firewall models, 807–808
PIX Firewall features, 808
DHCP client functionality, 811
DHCP relay functionality, 811
DHCP server functionality, 810–811
Easy VPN Remote functionality, 809–810
PDM, 809
PPPoE client functionality, 810
specifying AAA server groups, 409
SQL*Net, application inspection, 343–344
SSH
available Internet resources, 840
configuring, 694
remote access, 594–598
resources, 840
SSL configuring, 692, 694
standard mode FTP, 337–338
standard RTP mode (RTSP), 348
Startup Wizard (PDM), 155, 159
stateful failover, 451–452
adjusting failover poll time, 463
stateful packet filters, 19, 22
static command, 203, 372
port redirection, 228
static inside translations, 203–204
static IP addresses, configuring, 125
static mappings, creating between inside IP address and global IP address, 214
static outside translations, 206–209
static PAT, port redirection, 227–228
static routes, configuring, 114–115, 690–691
static translation rules, configuring, 716, 718
storing configuration files on TFTP servers, 90–91
structured threats, 6
Stub Multicast Routing (SMR), 322, 327
subcommand mode (object-group command), 283–284
submitting Firewall MC activities for approval, 720
Sun Solaris, PDM support, 154
Support page (Firewall MC), 730–731
supported AAA protocols, 395
supported address translations (NAT), 197–198
dynamic inside translations, 198–202
dynamic outside translations, 205–206
static inside translations, 203–204
static outside translations, 206–209
supported IPSec standards, 483
Switch Fabric Module, 45–47
SYN Flood Guard, 370–375
SYN floodguard, 372–374
synchronizing PIX Firewall with network time server, 102–103
syslog
configuring, 696–700
messages, generating, 115–119
system clock, configuring daylight savings time, 100–101
system maintenance. See also management tools
remote access
with SSH, 594–598
with Telnet, 591–594
SNMP, 607
  configuring, 611–613
  MBs, 609–611
  operations, 608–609
System Properties tab (PDM 3.0 configuration screen), 171–174
system requirements
  for Firewall MC installation, 642–643
  for failover, 453–454
  for PDM, 151–155
    Linux, 155
    Sun Solaris, 154
    Windows, 153–154

T
TACACS+ authorization, 392
task workflow, Firewall MC, 653–654
  configuring access, 709–710
  configuring access rules, 710–716
  configuring building blocks, 672–684
  configuring Firewall Device Contact Information, 705, 707
  configuring import device setting, 704–705
  configuring management features, 702–704
  configuring settings, 684–702
  configuring translation rules, 716–720
  creating device groups, 661–662
  creating job task, 723, 726
  creating new activities, 655–660
  deploying jobs, 727–728
  importing devices, 663–669
  managing devices, 670–672
  viewing configuration, 720
TCP (Transport Control Protocol), 193–194
  Telnet
    authentication, 393
    remote access, 591–594
    testing
      connectivity with ping command, 98–99
      for failover, 452
    tftp-server command, 89
threats to security, 6
  three-site full-mesh IPSec tunnels using preshared keys, case study, 540–542
time zones, configuring on system clock, 100–101
timeout uauth command, 417
tools
  cracking, 840
  UNIX, reconnaissance, 838
  Windows, 839
Tools menu (PDM 3.0 configuration screen), 175
topologies (VPNs), 480–481
transform sets, 511
  configuring, 509–511
  negotiation, 511
translating IP addresses embedded in DNS A-records
  alias command, 217–218
  expanded NAT, 222–223
  translation
  translations, 197
    connections, 212–213
    DNAT, 220–222
    DNS doctoring, 218–220
    PAT, 223–224
      augmenting global pools, 227
      backing up PAT addresses, 227
      mapping subnets to PAT addresses, 226
      port redirection, 227–228
      using outside interface address, 225
      rules (Firewall MC), configuring, 716–720
Translations Rules tab (PDM 3.0 configuration screen), 165–167
transport mode (IPSec), 482
transport protocols
  TCP, 193–194
  UDP, characteristics, 195, 197
traps, 608
troubleshooting
  activation keys upgrades, 618–619
  FWSM, 803–804
tunnel mode (IPSec), 482
tunnel policies, creating crypto maps, 531
Turbo ACLs, 250–251
  memory requirements, 250–251
  viewing configuration, 251
type literals, icmp command arguments, 262
UDP (User Datagram Protocol), characteristics, 195–197
unauthorized data retrieval, 7
unauthorized privilege escalation, 8
unauthorized system access, 7
unified client framework, VPN client, 552
unique identity feature (AUS), 760–761
UNIX
  reconnaissance tool web sites, 838
  reconnaissance tools, 838
unrestricted licensing for PIX Firewall, 47
unstructured threats, 6
upgrading images, 621
URL filtering, 265–267
  long URL filtering, 268–269
url-server command, 266
user management of Firewall MC, 649–650

verifying
  AUS installation
    client access requirements, 755
    server requirements, 754
  failover status, 452
  site-to-site VPN configuration, 519
versions of PDM, 150
viewing
  accounting information, 431–432
  command authorization configuration, 606–607
  DHCP lease information, 109
  failover status, 466
  Firewall MC configuration, 720
  IGMP configurations, 327
  IP address of network interface, 94
  network interface statistics, 94–98
  Turbo ACL configuration, 251
Virtual HTTP, authentication, 413–415
virtual MAC address feature, 450
Virtual Re-assembly, 367–370
Virtual Telnet, preauthentication, 412–413
VLANs, configuring on MSFC, 800–801
VPN client, 551–552
  features, 553–554
  IPSec attributes, 554–555
  remote users, 551–552
VPN tab (PDM 3.0 configuration screen), 167
VPN Wizard, creating site-to-site VPNs, 533, 536
vpngroup command, 556
VPNs (virtual private networks), 479–491
  DES, 483–484
  Easy VPN, remote configuration, 537
  IPSec, 481–482
  remote access
    configuring, 555–558
    configuring with PDM, 568, 573
  PPTP client configuration, 565
  preshared keys for ISAKMP
    authentication, configuring, 558–564
SAs, 483
site-to-site
  configuring, 495–509
  configuring with Easy VPN technology, 520–526
  configuring with PDM, 526–531
  creating with VPN Wizard, 533, 536
  verifying configuration, 519
topologies, 480–481

websites
  CA resources, 841
  Cisco links, 840
  cracking tools, 840
  host-based IDSs, 838
  professional security associations, 837
    legal, 838
  security portals, 839
  SNMP discovery tools, 839
  SSH-related, 840
  UNIX reconnaissance tools, 838
  Windows reconnaissance tools, 839
Windows operating system
  PDM support, 153–154
  reconnaissance tool web sites, 839
  reconnaissance tools, 839
  SNMP discovery tools, 839
Windows NT, installing CSACS, 396–403
work flow of Firewall MC common tasks, 653–654
  configuring access, 709–710
  configuring access rules, 710–716
  configuring building blocks, 672–684
configuring Firewall Device Contact Info, 705–707
configuring import devices, 704–705
configuring management features, 702–704
configuring settings, 684–702
configuring translation rules, 716–720
creating device groups, 661–662
creating jobs, 723–727
creating new activities, 655–660
deploying jobs, 727–728
importing devices, 663–669
managing devices, 670–672
submitting activities for approval, 720–722
submitting jobs for approval, 723–727
viewing configurations, 720
write erase command, 89, 646
write memory command, 89, 450
write net command, 90–91
write term command, 291
write terminal command, 89

X-Y-Z

xlate command, 212

zombies, 8