

Index

Numerics

3DES (Triple Data Encryption Standard),
265

A

AAA (authentication, authorization, and
accounting), 12, 511, 515
 configuring, 538
 cut-through proxies, 569
 “Do I Know This Already?” quiz,
 533–536
 defined, 511
 “Do I Know This Already?” quiz,
 507–510
 Floodguard, 597
 PIX Firewalls supported AAA server
 technologies, 515
 servers
 identifying, 538, 541
 specifying, 537
 support, 44
 troubleshooting, 573, 577
aaa accounting command, 539
aaa authentication command, 539, 542
aaa authentication console command, 544
aaa authorization command, 539
aaa-server command, 538
AAA server groups, 446
aaa-server local command, 539
AAA servers, 383
access, 9
 AAA, 511, 515
 ACL, 26
 configuring inbound access, 159–168
 “Do I Know This Already?” quiz,
 155–158

 lists, 164
 modes, 129
 NAS, 512
 networks
 security, 7
 threats, 8
 types of attacks, 8, 11
 vulnerabilities, 8
 object grouping, 169, 172
 PDM requirements, 376
 remote, 71, 74
 SSH, 72–74
 Telnet, 71–72
 rules, configuring, 642
access attacks, 9, 10–11
Access Control Server (ACS), 44
access list entries (ACEs), 164
access lists, managing access control entries,
 167
access rules, 387–389
access VPNs, 261, 311
access-group command, 280, 641
access-list command, 164, 275
accounting, 512
 configuring, 563–565
 troubleshooting, 575
 viewing, 565
ACEs (access list entries), 164
ACLs (access control lists), 26
 downloading, 569, 572
 logging, 172
 TurboACL, 168–169
ACS (Access Control Server), 44
activating AUS, 464
 auto update server contact information,
 469
 PIX Firewall configuration deployment,
 470

PIX Firewall unique identification
parameters, 467

activation keys
license, 265
upgrading, 79–80

ActiveX objects, filtering, 495–497

Activity bar (Firewall MC user interface),
428

Activity Report (Firewall MC), 455

Adaptive Security Algorithm (ASA), 31,
41–43

address command, 82

address translation pools, 447

addresses
IP
 global, 639–640
 mapping, 637
translation, 45, 106, 114
 bidirectional, 114
 commands, 107–108
 configuring multiple, 112, 114
 NAT, 108–109
 PAT, 110
 static, 111
 static port translation, 161
 troubleshooting, 114, 118

administration tasks (Firewall MC), 458
maintenance, 461
support, 462
workflow setup, 458–460

advanced protocol handling, 175–177

aggressive mode (IKE), 266

AH (Authentication Header), 263

algorithms
ASA, 31, 41–43
SHA-1, 265
transform sets, 276

alias command, 596

applets, 496

applications
advanced protocol handling, 175
AVVID, 14–15, 19
multimedia
 H.323, 591
 RTSP, 588
 support, 587–593
threats, 8

arc, 15

Architecture for Voice, Video, and Integrated
Data. *See* AVVID

ASA (Adaptive Security Algorithm), 31,
41–43

ASBRs (Autonomous System Boundary
Routers), 216, 220

assigning users to groups, 551

Association, 643

attack guards, 594, 598
AAA Floodguard, 597
DNS, 595
“Do I Know This Already?” quiz,
583–586
Flood Defender, 597
fragmentation, 594
mail guard, 596–597

attacks, 9, 18
reconnaissance, 9
SYN flooding, 597
Syslog, 185
threats, 8
types of
 access, 10–11
 DoS, 11
 reconnaissance, 9–10

audit policy, 599

AUS (Auto Update Server), 409, 462
 activation, 464
 auto update server contact information, 469
 PIX Firewall configuration deployment, 470
 PIX Firewall unique identification parameters, 467
 administrative tasks, 483
 assignment configuration, 477
 device configuration, 474
 image configuration, 475
 installing, 463
 reports, 479–481
 supported devices, 463
 user interface, 471–473

authentication, 215
 CAs, 268–269
 configuring, 541–542, 550
 authentication timeout, 549
 console access authentication, 544
 designating parameters, 543
 services, 545
 cut-through proxy, 31, 43
 Easy VPN Remote, 336–338
 HMAC, 265
 prompts, 548
 services, 545
 timeout, 549
 troubleshooting, 574
 VPDN group, 354
 X.509 certificate support, 44, 61

Authentication Header (AH), 263

authentication telnet console command, 72

authentication, authorization, and accounting. See AAA

authorization
 command-level, 74–76
 configuring, 550–561
 Cisco Secure ACS, 551
 cut-through proxy, 31, 43
 rules, 555
 troubleshooting, 575

auth-prompt command, 548–549

Autonomous System Boundary Routers (ASBRs), 216, 220

Auto Update Server. See AUS

AVVID (Architecture for Voice, Video, and Integrated Data), 14–15, 19

B

back user task flow (Firewall MC), 428

banner command, 147

basic configuration, 641

bidirectional network address translation, 114

block scans, 10

blocking applets, 496

boothelper disks, 84

bootstrap commands (Firewall MC), 418

browsers, PDM requirements, 376

C

cables (Crossover Ethernet), 246

caches
 no url-cache command, 500
 show url-cache command, 502

cannot, 497

CAs (Certification Authorities), 337
 VPN, 268–269

case studies
 DUKEM, 633
 authentication, 642
 basic PIX Firewall configuration, 635–640
 configuring access rules, 641
 failover, 655–656
 growth expectation, 634
 logging, 642
 VPNs, 643–654
 troubleshooting implementation, 657–665

certificate revocation lists (CRLs), 144

certificates (X.509), support, 44

cgi-truncate parameter, 501

chapter, 288

CIFS (Common Internet File System), 105

Cisco, 139

Cisco AVVID. See AVVID

Cisco Easy VPN Remote Router clients, 323

Cisco Firewall Services Module. See FWSM

Cisco PIX 501 Firewall, 48

Cisco PIX 501 VPN Client, 322

Cisco PIX 506 Firewall, 49

Cisco PIX 506 VPN Client, 322

Cisco PIX 515E Firewall, 51–53

Cisco PIX 525 Firewall, 54–56

- Cisco PIX 535 Firewall, 56–58
- Cisco PIX Firewall. *See* PIX Firewall
- Cisco PIX Firewall FastEthernet Interface Card (PIX-1FE), 47
- Cisco Secure ACS (Access Control Server), 515, 533, 566
- Cisco Secure Intrusion Detection Sensor, 44, 61
- 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 VPN 3002 Hardware Client, 321–322
- Cisco VPN Software Client, 321, 334
 - features, 335
 - manual configuration, 338–344
 - specifications, 335
- CiscoWorks
 - Firewall MC, 46, 419
 - adding users*, 421
 - login process*, 419
 - user authorization roles*, 421
- clear command, 285
- clear ntp command, 145
- clear rip command, 216
- clear route command, 214
- clear uauth command, 550
- clear xlate command, 115, 593
- CLI (command-line interface), 45, 62, 72
- Click, 568
- client mode (Easy VPN Remote), 333
- clients
 - Cisco Easy VPN Remote Router clients, 323
 - DHCP, 143
 - Easy VPN Remote, 321–322
 - HTTP, upgrading OS, 83
- clock summer-time command, 147
- clocks (system), 146–147
- command-level authorization, 74–76
- command-line interface (CLI), 45, 62, 72
- commands, 111, 143, 216, 227, 277, 285, 326, 332, 353, 539, 615–616, 625
 - aaa accounting command, 539
 - aaa authentication command, 539, 542
 - aaa authentication console command, 544
 - aaa authorization command, 539
 - aaa-server local command, 539
 - aaa-server command, 538
 - access modes command, 129
 - access-group command, 280, 641
 - access-list command, 164, 275
 - address command, 82
 - alias command, 596
 - authentication telnet command, 72
 - auth-prompt command, 548–549
 - banner command, 147
 - clear command, 285
 - clear ntp command, 145
 - clear rip command, 216
 - clear route command, 214
 - clear uauth command, 550
 - clear xlate command, 115, 593
 - clock command, 146
 - clock summer-time command, 147
 - configuration, 129, 151
 - global command*, 135–136
 - interface command*, 130
 - ip address command*, 133
 - nameif commands*, 131
 - nat command*, 133–134
 - rip command*, 137
 - route command*, 136–137
 - configure terminal command, 129
 - copy tftp flash command, 81
 - crypto ipsec transform-set command, 280, 328
 - crypto map command, 278
 - debug aaa accounting command, 575
 - debug aaa authentication command, 574
 - debug aaa authorization command, 575
 - debug command, 138, 286, 653
 - debug crypto isakmp command, 286
 - debug igmp command, 231
 - debug radius command, 576
 - debug tacacs command, 576
 - dhcpcd address command, 359
 - dhcpcd command, 140
 - enable command, 129
 - enable password command, 72
 - file command, 82
 - filter activex command, 497
 - filter java command, 495
 - filter url command, 498
 - fixup command, 174–175
 - fixup protocol command, 587

commands (*continued*)

- fixup protocol h323 command, 591
 - floodguard disable command, 598
 - fragment command, 594
 - hw-module command, 625
 - igmp access-group command, 227
 - igmp forward command, 226
 - igmp join-group command, 226
 - igmp query-interval command, 227
 - igmp query-max-response-time command, 227
 - igmp version command, 227
 - interface command, 82, 210
 - ip address command, 133
 - ip address dhcp command, 143
 - ip audit command, 599
 - ip local pool command, 327
 - ip verify reverse-path command, 602–603
 - isakmp keepalive command, 332
 - isakmp policy command, 271
 - logging command (syslog), 187
 - logging facility command, 186
 - logging on command, 194
 - match address command, 280
 - mroute command, 225
 - multicast interface command, 224
 - nameif command, 101, 119, 211
 - nameif interface commands, 619
 - nat command, 162
 - nat 0 command, 162
 - no aaa-server command, 540
 - no fixup protocol ftp command, 176
 - no url-cache command, 500
 - ntp authenticate command, 145
 - ntp authentication-key command, 145
 - ntp trusted-key command, 145
 - OSPF, 216, 222
 - network command*, 218
 - prefix-list command*, 219
 - redistribute ospf command*, 220
 - router ospf command*, 217
 - show ospf command*, 222
 - passwd command, 72
 - permit ip any command, 275
 - ping command, 82, 138
 - PIX bootstrap commands, 418
 - prefix-list command, 219
 - rip command, 215
 - route command, 213
 - server command, 82
 - setup command, 619
 - show aaa-server command, 574
 - show accounting command, 575
 - show activation-key command, 79
 - show command, 273, 284, 574, 653
 - show conn commands, 116
 - show crypto ispec sa command, 285
 - show failover command, 251
 - show isakmp policy command, 274
 - show module command, 624
 - show perfmon command, 503
 - show route command, 214
 - show url-cache command, 502
 - show url-server stats command, 502
 - show version command, 78
 - show vpdn pppinterface command, 356
 - show xlate command, 115
 - shun command, 601
 - ssh command, 73
 - static command, 112
 - sysopt connection permit-ipsec command, 283
 - sysopt uauth allow-http-cache command, 544
 - telnet command, 71
 - timeout uauth command, 549
 - transform-set command, 277
 - translation, 107–108
 - troubleshooting, 88–93
 - url-cache command, 499
 - url-server command, 497
 - virtual telnet command, 545
 - vpnclient server command, 348
 - vpnclient vpngroup command, 348
 - write memory command, 72, 139
 - write standby command, 244
 - xlate command, 108
- Common Internet File System (CIFS), 105**
- communications**
- VPN, 261
 - CAs, 268–269
 - configuring, 269
 - IKE, 265, 268
 - IPSEC, 262, 265
 - troubleshoot, 288
- components (AAA), 511, 515, 537**

- Computer Telephony Interface Quick Buffer Encoding (CTIQBE), 589
- Configuration Differences report (Firewall MC), 456
- configuration replication (failover), 244
- configuration tasks
 - Firewall MC, 435
 - creating building blocks*, 440, 443, 447
 - defining access rules*, 436
 - defining translation rules*, 438
 - generating and viewing configuration information*, 448
 - MC settings*, 449
- configure terminal command, 129
- configuring, 139, 617
 - AAA, 538
 - cut-through proxies*, 569
 - “Do I Know This Already?” quiz*, 533–536
 - access
 - access rules*, 642
 - inbound*, 159–168
 - accounting, 563–565
 - assignments (Firewall MC), 477
 - authentication, 541–542, 550
 - authentication timeout*, 549
 - console access authentication*, 544
 - designating parameters*, 543
 - services*, 545
 - authorization, 550–561
 - basic configuration, 641
 - Cisco Secure ACS, 525, 551
 - Cisco VPN Software Client
 - manually*, 338–342, 345
 - modifying VPN Client options*, 342–344
 - commands, 129
 - global command*, 135–136
 - interface command*, 130
 - ip address command*, 133
 - nameif command*, 131
 - nat command*, 133–134
 - rip command*, 137
 - route command*, 136–137
 - crypto maps, 278–280
 - cut-through proxy, 569
 - DHCP, 140, 143
 - clients*, 143
 - servers*, 140–142
 - DHCP options, 360
 - DHCP server, 357–358
 - DNS support, 118
 - downloadable PIX ACLs, 569, 572
 - Easy VPN Remotes, 347–350
 - failover, 242, 246–247, 251, 657
 - configuration replication*, 244
 - DUKEM case study*, 655–656
 - filters, viewing, 502
 - FWSM, 618
 - access lists*, 620
 - interfaces*, 619
 - running setup command*, 619
 - IKE, 270, 274
 - images (Firewall MC), 475
 - interfaces, 638–640
 - intrusion detection, 599–600
 - IPSec, 274, 283
 - login banners, 147–148
 - multiple translation types, 112–114
 - NAT, 331
 - object group, 170
 - OSPF, 220–222
 - PAT, 134
 - PIX Firewall, 129
 - DUKEM case study*, 635–642
 - interface command*, 130
 - nameif command*, 131
 - nat command*, 133
 - PDM*, 379–380, 383
 - route command*, 136
 - sample configuration*, 149
 - saving configuration*, 139
 - time settings*, 144
 - verification*, 132
 - preshared keys, 272
 - redundancy, 32–33
 - replication, 244
 - RIP, 215–216
 - routing, 638, 640
 - SA lifetimes, 278
 - servers, 384
 - SNMP, 88
 - static routes, 213

configuring (*continued*)

- switches (FWSM), 615–616
- syslog, 46, 62, 189
 - messages at the console*, 192
 - sending messages to a log server*, 193–194
 - SNMP traps and SNMP requests*, 195
 - syslogd servers*, 195–197
- testing configuration, 138
- time settings, 147
- transform sets, 276
- TurboACL, 169
- URL-filtering policy, 498
- virtual HTTP inbound connections, 548
- VPDN group, 354
- VPNs, 269, 292, 647
 - DUKEM case study*, 643–654
 - PDM*, 392–404
 - troubleshooting*, 654
 - tunneling*, 653
 - verifying configuration*, 273
- XAUTH, 325–331

connections

- Cisco Secure PIX 501, 48
- Cisco Secure PIX 506, 49
- Cisco Secure PIX 515E, 51–53
- Cisco Secure PIX 525, 54–56
- Cisco Secure PIX 535, 56–58
- cut-through proxy, 31, 43, 513
- “Do I Know This Already?” quiz, 97–100
- Easy VPN Remote, 323–324
- embryonic (half-open), 104
- failover (LAN-based), 245–246
- filters (Java applets), 496
- flags, 117
- security, 7
- stateful failover, 244–245
- Telnet, 71
- threats, 8
- troubleshooting, 114, 118
- types of attacks, 8, 11
- VPNs, troubleshooting, 283–286
- vulnerabilities, 8

console access authentication, 544

content area (Firewall MC user interface), 426

content filtering, 492

- copy tftp flash command**, 81
- creating boothelper disks**, 84
- CRLs** (certificate revocation lists), 144
- Crossover Ethernet cables**, 246
- crypto access lists**, 275–276
- crypto IPSec SA lifetime**, 278
- crypto ipsec transform-set command**, 280, 328
- crypto map command**, 278–280
- crypto maps**
 - commands, 280
 - configuring, 278
 - dynamic, 330
- Cisco Secure ACS** (Cisco Secure Access Control Server), 533
 - authorization, 551
 - configuring, 525
 - downloadable PIX ACLs, 569, 572
 - users, configuring, 551
 - verifying, 577
- CTIQBE** (Computer Telephony Interface Quick Buffer Encoding), 589
- cut-through proxy**, 31, 43, 513
- cut-through proxy configuration**, 569

D**data**

- compression, 337
- frames, 102
- segments, 101
- Data Encryption Standard (DES)**, 265, 375
- DDoS** (distributed denial of service) attacks, 11
- dead peer detection (DPD)**, 318, 337
- debug aaa accounting command**, 575
- debug aaa authentication command**, 574
- debug aaa authorization command**, 575
- debug command**, 138, 286, 653
- debug crypto isakmp command**, 286
- debug igmp command**, 231
- debug radius command**, 576
- debug tacacs command**, 576
- debugging**
 - DHCP server, 361–362
 - multicast configuration, 230
 - VPN connectivity, 286
- default routes**, 213

- default security policies, 101
 - defense in depth, 14
 - defining, 616
 - access rules (Firewall MC), 436
 - multiple transform sets, 276
 - translation rules (Firewall MC), 438
 - demilitarized zone (DMZ) segment, 113
 - denial of service (DoS) attacks, 11
 - deny keyword, 275
 - deploying FWSM, 612–613
 - deployment tasks
 - Deploy Saved Changes, 450–451
 - Status Summary, 454
 - DES (Data Encryption Standard), 265, 375
 - device management (Firewall MC), 429, 434
 - importing devices, 431
 - managing groups, 429
 - Device Setting Report, 457
 - devices
 - Firewall MC support, 416
 - supported by AUS, 463
 - DHCP (Dynamic Host Configuration Protocol), 358
 - configuration, 140–143
 - lease length, 360
 - overview, 358
 - DHCP servers
 - auto configuration, 361
 - configuring, 357–358
 - debugging, 362
 - PIX Firewall, 359–360
 - dhcpcd address command, 359
 - dhcpcd auto-config command, 353
 - dhcpcd command, 140–141
 - disabling Syslog messages, 198
 - distinguished name (DN), 324
 - distributed denial of service (DDoS) attacks, 11
 - DMZ (demilitarized zone) segment, 113
 - DN (distinguished name), 324
 - DNS (Domain Name Service), 176, 596
 - DNA guard, 595
 - support
 - configuring, 118
 - in PIX Firewall, 139
 - queries, 9
 - “Do I Know This Already?” quizzes
 - AAA, 507–510
 - AAA configuration, 533–536
 - access, 155–158
 - access VPNs, 311–315
 - attack guards and multimedia support, 583–586
 - content filtering, 491–494
 - failover, 238–240
 - Firewall MC, 409–413
 - FWSM, 607–610
 - network security, 3–6
 - PDM, 369–372
 - PIX Firewalls, 23–25, 37–40, 125–128
 - Syslog, 181–184
 - system maintenance, 67–70
 - translation and connection, 97–100
 - DoS (denial of service) attacks, 9–11
 - downloadable PIX ACLs, 569, 572
 - DPD (dead peer detection), 318, 332
 - dynamic address translation, 107
 - dynamic crypto maps, 330
 - Dynamic Host Configuration Protocol. *See* DHCP
 - dynamic routes, 214
 - configuring RIP, 216
 - OSPF
 - commands, 216–220
 - configuring, 220
 - viewing configuration, 222
 - dynamic shunning, 601
- ## E
- Easy VPN Remote
 - authentication, 338
 - connection process, 323–324
 - modes of operation, 332–333
 - overview, 320
 - PIX Firewall configuration, 347–348
 - client device mode, 348
 - IUA, 350
 - SUA, 349
 - supported clients, 321–322
 - supported servers, 320
 - tunneling protocols, 336
 - Easy VPN Server, 316
 - IPSec options, 319
 - overview, 318
 - embedding, secure real-time embedded systems, 31

- embryonic (half-open) connections, 104
- enable command, 129
- enable password command, 72
- enabling
 - DHCP on PIX Firewall, 361
 - IUA, 351
 - PPPoE client, 355
 - RIP, 137
- Encapsulating Security Payload (ESP), 262
- encapsulation (upper-level data), 102
- encryption
 - 3DES, 265
 - crypto access lists, 275
 - DES, 265, 375
 - Easy VPN Remote, 336
 - hash algorithms, 329
- enrollment mechanisms, 337
- ESP (Encapsulating Security Payload), 262
- Ethernet VLAN tagging, 208
 - logical interfaces, 209–210
 - managing VLANs, 211
- Event Report (AUS), 481
- events
 - failover, 241–243
 - Syslog, 46, 62
- external threats, 9

F

- fabrication, access attacks, 10
- failover
 - configuring, 242, 246–247, 251, 657
 - configuration replication*, 244
 - DUKEM case study*, 655–656
 - “Do I Know This Already?” quiz, 238–240
 - events, 241–243
 - LAN-based, 245–246
 - PIX Firewall, 248–251
 - redundancy, 32–33
 - stateful, 244–245
- file command, 82
- File Transfer Protocol (FTP), 176
- filter activex command, 497
- filter java command, 495
- filter url command, 498
- filtering, 495
 - ActiveX objects, 497

- FTP, 500
- FTP sites, 499
- HTTPS, 500
- HTTPS sites, 499
- Java applets, 495
- URLs, 497–499
 - configuring URL-filtering policy*, 498
 - identifying servers*, 497
 - long URLs, 501–502

filters

- Java applets, 496
- viewing, 502

Firewall MC

- administration tasks, 458
 - maintenance*, 461
 - support*, 462
 - workflow setup*, 458–460
- AUS, 462
 - activation*, 464, 467–470
 - administrative tasks*, 483
 - assignment configuration*, 477
 - device configuration*, 474
 - image configuration*, 475
 - installing*, 463
 - reports*, 479–481
 - supported devices*, 463
 - user interface*, 471–473
- back user task flow, 428
- CiscoWorks, 419
 - adding users*, 421
 - login process*, 419
 - user authorization roles*, 421
- configuration hierarchy, 415
- configuration tasks, 435
 - creating building blocks*, 440, 443, 447
 - defining access rules*, 436
 - defining translation rules*, 438
 - generating and viewing configuration information*, 448
 - MC settings*, 449
- deployment tasks
 - Deploy Saved Changes*, 450–451
 - Status Summary*, 454
- device management, 429, 434
 - importing devices*, 431
 - managing groups*, 429

- “Do I Know This Already?” quiz, 409–413
- installing, 416
 - client requirements*, 418
 - server requirements*, 417
- key concepts, 414
- PIX bootstrap commands, 418
- reports, 454–457
- supported devices, 416
- user interface, 423
 - Activity bar*, 428
 - configuration tabs*, 425
 - Object Selector*, 427
 - options bar*, 425
 - path bar*, 426
 - TOC*, 425
 - Tools bar*, 427
- firewall module switch command, 616
- firewall vlan-group command, 616
- firewalls, 26, 30
 - basic configuration, 641
 - managing, 45, 62
 - packet filtering, 26–28
 - PIX, 30–33
 - ASA*, 31, 41–43
 - Cisco 501*, 48
 - Cisco 506*, 49
 - Cisco 515E*, 51–53
 - Cisco 525*, 54–56
 - Cisco 535*, 56–58
 - models*, 44
 - proxy, 28
 - proxy servers, 28
 - stateful inspection, 29–30
- fixup command, 174–175
- fixup protocol command, 587
- fixup protocol h323 command, 591
- Flood Defender, 597
- Floodguard, 597
- floodguard disable command, 598
- formatting
 - boothelper disk, 84
 - crypto access lists, 275
- fragment command, 594
- fragmentation guard, 594
- frames, 102
- FTP (File Transfer Protocol), 176, 500

- FWSM (Cisco Firewall Services Module), 44, 607
 - configuring, 618–619
 - access lists*, 620
 - interfaces*, 619
 - deployment scenarios, 612–613
 - “Do I Know This Already?” quiz, 607–610
 - initializing, 615–616
 - overview, 611
 - PIX Firewall, 622
 - status LED, 625
 - troubleshooting, 623
 - resetting and rebooting*, 625
 - switch commands*, 623

G

- gateways, 46, 62, 82, 269
- gigabits per second (Gbps), 611
- global command, 135–136
- global information, recording, 636
- global IP addresses, 639–640
- groups
 - rules, 555
 - users, 551
- guards, 596
 - attack, 598
 - DNS, 595–596
 - mail, 596–597

H

- H.323, 589–591
- H.323 collection of protocols, 591
- handling protocols, 175, 177
- hardware (Cisco Secure ACS), 515
- headers (AH), 263
- HMAC (Keyed-Hash Message Authentication Code), 265
- horizontal scans, 9
- Hosts/Networks tab (Startup Wizard), 385
- HTTP
 - clients, upgrading OS, 83
 - virtual, 548
- HTTPS filtering, 500
- hw-module command, 625

ICMP object groups, 172

identifying

filtering servers, 497

servers, 538, 541

IGMP (Internet Group Management Protocol), 224

igmp access-group command, 227

igmp forward command, 226

igmp join-group command, 226

igmp query-interval command, 227

igmp query-max-response-time command, 227

igmp version command, 227

IKE (Internet Key Exchange)

configuring, 270, 274

VPN, 265, 268

implementation of security designs, 12

importing devices (Firewall MC), 431

inbound access, 159–162

access lists, 164–166

inbound connections, 43

cut-through proxy, 31

Individual User Authentication (IUA), 350

information security, 7

Initial Contact, 319

initializing

FWSM, 615–616

PDM, 623

inspection

advanced protocol handling, 175–177

FTP, 176

installing

AUS, 463

Cisco VPN Software Client, 339

Cisco Secure ACS, 516–518, 527

Firewall MC, 416

client requirements, 418

server requirements, 417

operating systems, 77

PDM, 378

Instructions box (Firewall MC user

interface), 426

integrated data (AVVID), 14–15, 19

integrity, X.509 certificate support, 44, 61

Intel Internet Video Phone, 177

interception, 10

intercepts (TCP), 161–162

interface command, 82, 130, 210

interfaces, 641. *See also* access

CLI, 45, 62, 72

configuring, 638–640

static NAT, 159

Internet Group Management Protocol (IGMP), 224

Intranet VPNs, 261

intrusion detection, 44, 61, 598, 601

configuring, 599–600

dynamic shunning, 601

optimizing, 13

IP

address pool, 327

addresses

global, 639–640

mapping, 637

fragmentation, 594

ip address command, 133

ip address dhcp command, 143

ip audit command, 599

ip local pool command, 327

IP routing, 212

dynamic routes, 214

configuring RIP, 216

OSPF, 216–222

multicasting, 224

commands, 224–227

debugging, 230

inbound traffic, 228–229

outbound traffic, 230

static routes, 212–213

ip verify reverse-path command, 602–603

IPSec (Internet Protocol Security)

configuring, 274, 283

Easy VPN Server, 319

sysopt connection permit-ipsec command, 283

VPN, 262, 265

IPSec Traffic Selector Panel, 396

isakmp keepalive command, 332

isakmp policy command, 271, 326

IUA (Individual User Authentication), 350

J–K

Java applets, 495–496

Keyed-Hash Message Authentication Code (HMAC), 265
keywords, 275

L

LAN-based failover, 245–246
levels of security, 101, 186
link-state advertisements (LSAs), 216
Linux, PDM requirements, 377
listening (ports), 8
lists
 access, 164
 CRLs, 144
logging
 ACLs, 172
 configuring, 642
logging commands (syslog), 187
logging facilities, 186
logging on command, 194
logical interfaces, 209–210
login banners, configuring, 147–148
logs, viewing, 190
longurl-truncate parameter, 501
LSAs (link-state advertisements), 216

M

mail guard, 596–597
main mode (IKE), 266
managing
 firewalls, 45, 62
 VLANs, 211
mapping
 static IP addresses, 637
 static NAT, 159
match address command, 280
MD5 (Message Digest 5), 265
MDIX (Medium Dependent Interface Crossover), 322
Media Gateway Control Package (MGCP), 591–592

Medium Dependent Interface Crossover (MDIX), 322

memory requirements, 77

Message Digest 5 (MD5), 265

messages

 digest, 265

 HMAC, 265

 Syslog

changing levels, 187

disabling, 198

organizing, 188

reading, 189

sending to a Telnet session, 193

MGCP (Media Gateway Control Package), 591–592

Microsoft NetMeeting, 177, 545

Microsoft Netshow, 177

models (PIX Firewalls), 44

modes

 access, 129

 monitor, 82

 stateful failover, 244

modification

 access attacks, 10

 activation keys, 80

monitor mode, 82

monitoring

 failover events, 243

 networks, 13

 PPPoE client, 355–356

Monitoring button (PDM), 389–391

monitoring PIX Firewall, 389–391

mroute command, 225

MSFC (Multilayer Switch Feature Card), 613

 configuring on the inside interface, 617

 as inside router, 613

MTU (maximum transmission unit), 339

multicast interface command, 224

multicast routing, 224

 commands

igmp access-group command, 227

igmp forward command, 226

igmp join-group command, 226

igmp query-interval command, 227

igmp query-max-response-time command, 227

igmp version command, 227

mroute command, 225

multicast interface command, 224

- multicast routing** (*continued*)
 - debugging, 230
 - inbound traffic, 228–229
 - outbound traffic, 230
- multimedia**
 - H.323, 591
 - RTSP, 588
 - support, 177, 587, 591
 - “Do I Know This Already?” quiz, 583–586
 - H.323, 589–591
 - MGCP, 591–592
 - SCCP, 592
 - SiP, 593
 - VoIP, 588–589

N

- name, 324
- nameif command, 101, 119, 131, 211
- nameif interface commands, 619
- NAS (Network Access Server), 512, 537–538, 541
- NAT (Network Address Translation), 106–109
 - bidirectional, 114
 - configuring, 331
 - policy NAT, 162
 - static, 159
 - static NAT, 159
- nat 0 access-list address translation rule, 159
- nat 0 command, 162
- nat command, 133–134
- nat/global command, 101
- NDG (Network Device Group), 558
- negotiation
 - IKE, 265, 268
- nesting object groups, 172
- NetBIOS Domain Name System, 105
- NetMeeting, 545
- Network Access Server (NAS), 512
- Network Address Translation. *See* NAT
- network command, 218
- Network Device Group (NDG), 558
- network object group, 170
- network of networks, 14
- network security
 - defense in depth, 14

- “Do I Know This Already?” quiz, 3–6
 - as a “legal issue”, 13
- Network Time Protocol (NTP), 144–145
- networks
 - addresses, translation, 45
 - firewalls, 26, 30–33
 - monitoring, 13
 - SAFE, 16, 20
 - security, 7, 11
 - threats, 8
 - types of attacks, 8, 11
 - VPN, 261
 - CAs, 268–269
 - certificates, 45
 - configuring, 269, 647
 - gateways, 46, 62
 - IKE, 265, 268
 - IPSec, 262, 265
 - scalability, 288
 - troubleshooting, 288, 654
 - tunneling, 653
 - vulnerabilities, 8
 - no aaa-server command, 540
 - no fixup protocol ftp command, 176
 - no url-cache command, 500
 - nodes (communication), 103
 - nonce values, 267
 - NTP (Network Time Protocol), 144–145
 - ntp authenticate command, 145
 - ntp authentication-key command, 145
 - ntp trusted-key command, 145
 - null rules, 389

O

- object grouping, 169, 172
- Object Selector (Firewall MC user interface), 427
- Open System Interconnection (OSI), 26
- operating systems (Cisco Secure ACS), 515
- optimization (security), 13
- Organizational Unit (OU), 324
- OS (operating system)
 - installing, 77
 - upgrading, 80
 - copy tftp flash command, 81
 - HTTP client, 83
 - monitor mode, 82

OSI (Open System Interconnection), 26
 OSI reference model, 28
 OSPF (Open Shortest Path First)
 commands, 216
 network command, 218
 prefix-list command, 219
 redistribute ospf command, 220
 router ospf command, 217
 show ospf command, 222
 configuring, 220
 overview, 216
 viewing configuration, 222
 OU (Organizational Unit), 324

P

packets, 101
 parameters

 AAA authentication, 543
 access-list command, 164
 banner command, 148
 cgi-truncate command, 501
 clock command, 146
 dhcpcd command, 141
 filter command, 496
 global command, 135
 interface command, 130
 isakmp policy command, 271
 longurl-truncate command, 501
 nameif command, 132
 nat command, 134
 ntp command, 144
 rip command, 137
 static command, 159
 syslog command, 189
 username command, 76

passwd command, 72

password recovery, 85–87
 diskless PIX Firewall, 86
 floppy drives, 86

PAT (Port Address Translation), 45,
 106–107, 110, 134

patches, 8. *See also* vulnerabilities

path bar, Firewall MC user interface, 426

PDM

 access rules, 387
 configuring PIX Firewall, 379–380,
 383

 defining hosts and networks, 385
 “Do I Know This Already?” quiz,
 369–372
 GUI, 374
 installing, 378
 monitoring capability, 389–391
 overview, 373
 requirements to run on PIX Firewall,
 375
 Linux requirements, 377
 SUN Solaris, 377
 Windows, 377
 workstation, 376
 translation rules, 386–387
 versions, 375
 VPN configuration, 392–394
 remote-access, 397–404
 Site to Site VPNs, 395

PDM (PIX Device Manager), 46, 62, 544,
 601

PDM (PIX Device Manager) Image, 622

PDM Log panel, 190

per user command authorization, 560

performance, 15

perimeter security

 firewalls, 26, 30
 packet filtering, 26–28
 PIX, 30–33
 proxy servers, 28
 stateful inspection, 29–30

permit ip any command, 275

permit keyword, 275

PFSS (PIX Firewall Syslog Server), 185,
 196

phase 1 negotiation, 266

physical interfaces, 211

physical security

 AAA, 511, 515
 security policies, 11

PIDs (process identifications), 220

ping command, 82, 138

ping sweeps, 9

pipes, 186

PIX 515E Firewall, 52

PIX Device Manager (PDM), 46, 62, 544,
 601, 622

PIX DHCP, 360

- PIX Firewall, 32**
 - AAA, 512
 - supported server technologies, 515*
 - ASA, 41–43
 - characteristics, 30
 - Cisco 501, 48
 - Cisco 506, 49
 - Cisco 515E, 51–53
 - Cisco 525, 54–56
 - Cisco 535, 56–58
 - configuring, 129
 - DHCP, 140–143
 - inbound access, 159–166*
 - PDM, 379–380, 383
 - sample configuration, 149*
 - cut-through proxy, 513
 - DHCP server, 359–360
 - auto configuration, 361*
 - debugging, 362*
 - DNS support, 139
 - “Do I Know This Already?” quiz, 23–25, 37–40, 125–128
 - dynamic shunning, 601
 - Easy VPN Remote configuration, 347–348
 - client device mode, 348*
 - IUA, 350
 - SUA, 349
 - failover
 - configuring, 242*
 - events, 241*
 - sample configuration, 248–249, 251*
 - Flood Defender, 597
 - FWSM, installing PDM, 622
 - intrusion detection, 598
 - IP routing, 212
 - dynamic routes, 214–222*
 - static routes, 212–213*
 - logical interfaces, 209–210
 - login banners, 147–148
 - models, 44
 - monitoring, 389–391
 - multimedia support, 587
 - H.323, 589–591
 - MGCP, 591–592
 - SCCP, 592
 - SiP, 593
 - VoIP, 588–589
 - optional components, 47
 - OSPF, 216
 - PDM, requirements to run, 375–377
 - PPPoE, 351–352
 - enabling PPPoE client, 355*
 - monitoring PPPoE client, 355–356*
 - RIP, 215
 - scalable VPNs, 288
 - secure real-time embedded system, 31
 - syslog
 - configuring, 189, 192*
 - logging facilities, 186*
 - organizing messages, 188*
 - PFSS, 197
 - reading messages, 189*
 - sending messages to a log server, 193–194*
 - sending messages to a Telnet session, 193*
 - severity levels, 187*
 - SNMP traps and SNMP requests, 195*
 - time settings, 144
 - troubleshooting, 574
 - implementation, 657–665*
 - upgrading OS, 80
- PIX Firewall Syslog Server (PFSS), 185, 196
- PIX MC (CiscoWorks Management Center for Firewalls), 46
- PIX-1FE (Cisco PIX Firewall FastEthernet Interface Card), 47
- point-to-point architecture, 12, 42–58, 102–104, 112–114, 120–121, 191, 248, 261–267, 292, 308, 374, 380–390, 393–405, 514, 519, 521–522, 527–528, 538–541, 546, 552–573, 590
- policies, 18
 - ISAKMP, 272
 - security, 11, 101
- policy, 647
- policy NAT, 162
- Port Address Translation (PAT), 45, 107
- Port Fast, 242
- ports
 - address translation, 45
 - fixup command, 174–175
 - listening, 8
 - redirection, 112
 - static address translation, 161

PPP (Point-to-Point Protocol), 352
 PPPoE (Point-to-Point Protocol over Ethernet), 351–352

- enabling PPPoE client, 355
- monitoring PPPoE client, 355–356

 prefix-list command, 219
 preshared keys, 267

- configuring, 272

 process identifications (PIDs), 220
 processes (security), 12
 prompts (authentication), 548
 protocol object-type, 171
 protocols

- advanced handling, 175–177
- FTP, 176
- H.323 collection, 591
- NTP, 144–145
- PPP, 352
- SCEP, 45, 61
- SNMP, 46, 62
- TCP, 102
 - intercepts*, 161–162
- transport, 101, 106
- UDP, 102

 proxy firewalls, 28
 public address translation, 45

Q–R

queries (DNS), 9

RADIUS (Remote Authentication Dial-In User Service), 515
 RealNetworks RealAudio and RealVideo, 177
 Real-Time Streaming Protocol (RTSP), 588
 reconnaissance attacks, 9–10
 recording global information, 636
 recovery, passwords, 87
 redirection (ports), 112
 redistribute ospf command, 220
 redundancy, 32–33
 remote access, 71, 74

- DUKEM case study, 654
- SSH, 72–74
- Telnet, 71–72

Remote Authentication Dial-In User Service (RADIUS), 515
 remote office/branch office (ROBO), 49
 remote-access VPNs, 261, 397–400, 402, 404
 remote-procedure call (RPC), 105
 replication, configuration, 244
 reports

- AUS, 479
 - Event Report*, 481
 - System Info Report*, 480
- Firewall MC, 454, 457

 requests (SNMP), 195
 requirements (memory), 77
 resources, 10
 Restricted Bundle, 59
 reverse path forwarding, 602–603
 RIP (Routing Information Protocol), 137

- configuring, 216
- enabling, 137

 rip command, 137, 215
 ROBO (remote office/branch office), 49
 route command, 136–137, 213
 router ospf command, 217
 routing, 203, 215

- authentication, 215
- configuring, 636–640
- IP routing, 212
 - dynamic routes*, 214–222
 - static routes*, 212–213
- multicast routing, 224, 227
 - commands*, 224–227
 - debugging*, 230
 - inbound traffic*, 228–229
 - outbound traffic*, 230
- principles, 208

 Routing Information Protocol. *See* RIP
 RPC (remote-procedure call), 105
 RTSP (Real-Time Streaming Protocol), 588
 rules

- access, configuring, 642
- groups, authorization, 555

 running setup command, 619

S

SA (security association), 262, 278

- SAFE (Secure Blueprint for Enterprise Networks), 16, 20
- saving configuration, 139
- scalability
 - AVVID, 15
 - VPN, 288
- scanning
 - block, 10
 - Cisco Secure Scanner, 13
 - horizontal, 9
 - vertical scans, 9
- SCCP (Skinny Client Control Protocol), 592
- SCEP (Simple Certificate Enrollment Protocol), 45, 61
- Scope bar (Firewall MC user interface), 426
- Secure Hash Algorithm 1 (SHA-1), 265
- Secure Intrusion Detection Sensor, 44, 61
- secure real-time embedded systems, 31
- Secure Shell (SSH), 72–74
- Secure Unit Authentication (SUA), 349
- security, 262, 265
 - AAA, 511, 515
 - access rules (PDM), 387
 - ASA, 31, 41–43
 - attack guards, 594, 598
 - AAA Floodguard, 597
 - DNS, 595
 - Flood Defender, 597
 - fragmentation, 594
 - mail guard, 596
 - attacks, 18
 - design, implementing, 12
 - firewalls, 26, 30
 - packet filtering, 26–28
 - PIX, 30, 32–33
 - proxy servers, 28
 - stateful inspection, 29–30
 - intrusion detection, 598, 601
 - configuring, 599–600
 - dynamic shunning, 601
 - levels (Syslog), 186
 - network, 7, 13
 - optimizing, 13
 - policies, 11, 18, 101
 - process, 12
 - static NAT, 159
 - testing, 13
 - threats, 8, 17
 - traffic
 - levels, 101
 - transport protocols, 101, 106
 - types of attacks, 8, 11
 - vulnerabilities, 8
- security association (SA), 262
- segments, 101, 113
- selecting VPN configuration, 269–270
- sends, 187
- server, 642
- server command, 82
- servers
 - AAA
 - configuring, 538, 569
 - identifying, 538, 541
 - specifying, 537
 - ACS, 44
 - configuring, 384
 - Cisco Secure ACS, 515, 527, 533
 - authorization, 551
 - installing, 516–518, 527
 - users, 551
 - verifying, 577
 - DHCP, 140–143
 - filters, identifying, 497
 - NAS, 512, 537–538, 541
 - NetMeeting, 546
 - PFSS, 185, 196
 - Syslog, 185
 - syslogd servers, 195–197
- service definitions, 443
- service groups, 445
- service object-type, 171
- services
 - authentication, 545
 - fixup command, 174–175
- session command, 625
- Session Initiation Protocol (SIP), 593
- setup command, 619
- severity levels (syslog), 187
- SHA-1 (Secure Hash Algorithm), 265
- shell command authorization sets, 561
- show aaa-server command, 574
- show accounting command, 575
- show activation-key command, 79
- show command, 273, 284, 574, 653
- show conn command, 116
- show crypto ipsec sa command, 285
- show failover command, 251

- show isakmp policy command, 274
- show module command, 624
- show ospf command, 222
- show perfmon command, 503
- show route command, 214
- show url-cache command, 502
- show url-server stats command, 502
- show version command, 78
- show vpdn pppinterface command, 356
- show xlate command, 115
- shun command, 601
- Simple Certificate Enrollment Protocol (SCEP), 45, 61
- SIP (Session Initiation Protocol), 593
- Site to Site VPNs, 261, 392–395
- Skinny Client Control Protocol (SCCP), 592
- SMTP, 177
- SNMP (Simple Network Management Protocol), 46, 62
 - configuring, 88
 - requests, 195
 - system maintenance, 87
 - traps, 195
- specifying AAA servers, 537
- split tunneling, 404
- spoofing, 28
- SSH (Secure Shell), remote access, 72–74
- standby unit, 244
- state tables, 29
- stateful failover, 244–245
 - redundancy, 32–33
- static command, 111–112
- static crypto maps, 330
- static IP address mapping, 637
- static NAT, 159
- static port address translation (static PAT), 161
- static routes, 212–213
- static translation, 107, 111
- statistics
 - show url-server stats command, 502
 - viewing filters, 502
- structured threats, 8
- SUA (Secure Unit Authentication), 349
- Sun Solaris, PDM requirements, 377
- support
 - DNS, configuring, 118
 - multimedia, 177, 591
 - H.323, 591
 - RTSP, 588
 - Syslog, 46, 62
 - X.509 certificates, 44
- SYN flooding, 597
- Syslog, 185
 - changing message levels, 187
 - configuring, 189
 - messages at the console, 192
 - sending messages to a log server, 193–194
 - SNMP traps and SNMP requests, 195
 - syslogd servers, 195–197
 - “Do I Know This Already?” quiz, 181–184
 - logging facilities, 186
 - messages
 - disabling, 198
 - organizing, 188
 - reading, 189
 - sending to a Telnet session, 193
 - security levels, 186
 - severity levels, 187
 - support, 46, 62
 - viewing logging with PDM, 190
- syslogd servers, 195, 197
- sysopt connection permit-ipsec command, 283
- sysopt uauth allow-http-cache command, 544
- system clock, 146–147
- System Info Report (AUS), 480
- system maintenance. *See also* troubleshooting
 - command-level authorization, 74–76
 - creating boothelper disks, 84
 - “Do I Know This Already?” quiz, 67–70
 - installing OS, 77
 - object grouping, 169, 172
 - password recovery, 85
 - diskless PIX Firewall, 86
 - floppy drives, 86
 - SNMP, 87
 - TurboACL, 168
 - upgrading activation keys, 79
- System Properties tab (Startup Wizard), 381
- system requirements (Cisco Secure ACS), 515

T

TACACS+ (Terminal Access Controller Access Control System Plus), 515

tagging. See Ethernet VLAN tagging

TCP

- intercepts, 161–162
- three-way handshake, 103
- virtual circuits, 102

technologies (VPN), 261

Telnet, 71

- starting sessions, 72
- virtual Telnet, 545

telnet command, 71

Terminal Access Controller Access Control System Plus (TACACS+), 515

testing

- configuration, 138
- security, 13

TFTP (Trivial File Transfer Protocol), 374

threats, 8, 17

three-way handshake (TCP), 103

time settings

- configuration, 147
- configuring, 144
- NTP, 144–145
- system clock, 146–147

timeout uauth command, 549

timeouts (authentication), 549

tokens, X.509 certificate support, 44, 61

Tools bar (Firewall MC user interface), 427

traffic, 30

- cut-through proxy, 513
- firewalls, 26, 28, 30
 - PIX, 30–33
 - proxy servers, 28
- routing, 203, 208
- security
 - levels, 101
 - transport protocols, 101, 106
- stateful inspection, 29

Transform Set Panel, 395

transform sets

- configuring, 276
- creating, 328
- crypto ipsec transform-set command, 280
- defining multiple, 276

transform-set command, 277

translation

- addresses, 45, 106, 114
 - commands, 107–108
 - NAT, 108–109
 - PAT, 110
 - static, 111
 - troubleshooting, 114, 118
- bidirectional, 114
- “Do I Know This Already?” quiz, 97–100
- dynamic address translation, 107
- flags, 116
- multiple, configuring, 112, 114
- rules, 386, 438
- static port add, 161

translation rules, 387

translation slots, 104

transparent tunneling, 341

transport protocols, 101, 106

traps (SNMP), 195

Triple Data Encryption Standard (3DES), 265

Trivial File Transfer Protocol (TFTP), 374

Trojan horses, 10

troubleshooting, 67, 654. See also system maintenance

- AAA, 573, 577
- accounting, 575
- address translation, 114, 118
- authentication, 574
- authorization, 575
- boothelper disk, 84
- commands, 88–93
- FWSM, 623
 - resetting and rebooting, 625
 - switch commands, 623
- password recovery, 85–86
- PIX Firewall implementation, 657–665
- security, 13
- Syslog, 185
- VPN, 288, 653
- VPN connections, 283–286

trunk ports, 209

tunneling

- transparent, 341
- VPN, 653

tunneling protocols, 336

TurboACL, 168–169

U

- UDP (User Datagram Protocol), 102
- unauthorized access, 10
- Unicast RPF (Unicast Reverse Path Forwarding), 602–603
- unstructured threats, 8
- upgrading
 - activation keys, 79–80
 - operating systems, 80
 - copy tftp flash command*, 81
 - HTTP client*, 83
 - monitor mode*, 82
- upper-level data, 102
- url-cache command, 499
- URLs
 - filtering, 497–499
 - configuring URL-filtering policy*, 498
 - identifying servers*, 497
 - long (filtering), 501–502
- url-server command, 497
- User Datagram Protocol (UDP), 102
- users
 - accounting, 563–565
 - authentication, 541–545, 549–550
 - authorization, 550–561

V

- VAC (VPM Accelerator Card), 47
- VAC+ (VPN Accelerator Card Plus), 47
- VDOnet VDOLive, 177
- verification
 - Cisco Secure ACS, 577
 - IKE configuration, 273
 - X.5, 61
 - X.509, 44
- vertical scans, 9
- video (AVVID), 14–15, 19
- viewing
 - accounting, 565
 - filters, 502
 - logging, 190
- virtual circuits, 102
- virtual HTTP, 548
- virtual interfaces, 52
- virtual private networks. *See* VPNs

- virtual services, authentication, 545
- virtual telnet command, 545
- virtual Telnet, 545
- viruses, 10
- vlan command, 615
- VLANs (Virtual LANs), 615
 - creating, 615
 - managing, 211
 - physical interfaces, 211
- VocalTech, 177
- voice (AVVID), 14–15, 19
- VoIP, 588–589
- VPDN (Virtual Private Dial-Up Networking)
 - group, 354
- VPN Accelerator Card (VAC), 47
- VPN Accelerator Card Plus (VAC+), 47
- vpnclient server command, 348
- vpnclient vpngroup command, 348
- VPNs (Virtual Private Networks)
 - access VPNs, 261, 311
 - CAs, 268–269
 - certificates, 45
 - configuring, 269, 292, 647
 - DUKEM case study*, 645–653
 - ISAKMP policies*, 272
 - troubleshooting*, 654
 - tunneling*, 653
 - verifying configuration*, 273
 - connections, troubleshooting, 283–286
 - gateways, 46, 62
 - IKE, 265, 268
 - IPSec, 262, 265
 - PDM
 - configuration*, 392–404
 - remote access
 - DUKEM case study*, 654
 - remote-access, 397–404
 - scalability, 288
 - Site to Site VPNs, 392–395
 - technologies, 261
 - troubleshooting, 288
- vulnerabilities, 8
- VXtreme WebTheatre, 177

W

- White Pine CuSeeMe, 177

- White Pine Meeting Point, 177
- Windows 2000
 - Cisco Secure ACS, 516–518, 527
 - PDM requirements, 377
- Windows Internet Naming Service (WINS), 142
- Windows NT
 - Cisco Secure ACS, 516–518, 527
 - PDM requirements, 377
- WINS (Windows Internet Naming Service), 142
- worms, 10
- write memory command, 72, 139

- write standby command, 244

X

- X.509 certificates, support, 44
- XAUTH (extended authentication), 325
 - configuring, 326, 330–331
 - defining group policy for mode
 - configuration push, 328
 - transform sets, 329
- Xing StreamWorks, 177
- xlate command, 108