Index

Numerics

- 3DES (triple Data Encryption Standard), 9
  - cryptography, 10
  - encryption algorithm, 549
- 5-GHz spectrum, power restrictions, 159
- 10BASE-T Ethernet switches, packet snooping, 245
- 10-Mbps/100-Mbps Ethernet, MTUs, 266
- 16MB IBM Token Ring, MTUs, 266
- 802.11
  - MAC packet format, 162
  - physical layer standards, 160
  - spread-spectrum radio technology, 156
    - DSSS, 156–157
    - FHSS, 157
    - media access controls, 160–162
    - OFDM, 158–160
    - wireless roaming, 163–164
- 802.11a standard, 152
- 802.11b standard, 152, 278
- 802.11g standard, 152
- 802.1X, network port authentication, 173–175
  - EAP-TLS, 175
  - EAP-TTLS, 175
  - LEAP, 176
  - packet snooping, 245
  - PEAP, 176–177

A

- AAA
  - accounting
    - event types, 522
    - keywords, 523
    - methods, 523
  - authentication methods, 399
    - commands, 386
    - privilege access mode, 385–386
  - authorization mechanisms, 388
  - dial-in access
    - double authentication, 532, 539
    - lock and key, 526, 532
- aaa commands, 405, 513
  - aaa-server commands, 402
  - authentication enable default method 1 commands, 386
  - authentication local-override commands, 513
  - authentication login commands, 399
  - authorization commands, default method lists, 518
  - new-model commands, 386, 398
  - TACACS+ authorization, 388
- acceptable-use policies, incident violation, 370–371
- access
  - controls. *See* access controls
  - corporate network privilege levels, 379–395
  - dial-in
    - AAA, 525, 539
    - accounting, 522–525
    - authentication, 503, 515
    - authorization, 515, 521
    - billing, 522–525
  - security concerns, 502–503
  - line controls, 395–396
    - Cisco IOS auxiliary ports, 400–401
    - Cisco IOS console ports, 396–400
    - Cisco IOS virtual terminal ports, 401
    - Cisco PIX firewall, 402–405
    - Cisco switches, 401–402
    - HTTP security, 406–408
    - SNMP security, 405–406
  - logical control, 330–331
    - authentication, 331–333
    - greeting messages, 333
    - passwords, 331
    - users, 333
  - physical device security, 320–321
  - virtual dial-in encryption, 539, 572
- access control lists (ACLs). *See* ACLs
- Access Control Server, 593
- access controls, 20
  - 802.11, 160–162
  - definition, 37
  - gatekeeper services, 181
  - identity, 37
  - physical, 379
  - VoIP network, 599–601
    - MGCP, 602
    - SIP, firewall , 601–602
    - tokenless call authorization, 602
  - VPNs
    - how provided, 587–588
    - resources protected, 586–587
  - wireless network, 593–594
- access lists, tracing DDoS attacks, 647–648. *See also* ACLs
  - logging, 650–651
  - log-input, 648
  - Smurf attack, 649
  - SYN flood, 648–649
  - without log-input, 650
- access points (APs), 248
  - WLANs component, 153
- access servers, authorization configuration, 518
- Access VPNs, 136, 149–150
- access-enable commands
  - Cisco IOS basic access, 379
  - Cisco IOS privilege access, 381
- access-list commands, 449, 487, 529

access-list compiled commands, 455, 487
access-profile commands, 533
  Cisco IOS basic access, 379
  Cisco IOS privilege access, 381
access-template commands, Cisco IOS privilege access, 381
accounting
  dial-access, TACACS+, 522–523
  RADIUS protocol, 61
  site security policies, 344
  TACACS+ protocol, 58
ACK (Acknowledgment field), 261
  flag, TCP, 260
  SIP signaling message type, 189
acknowledgement packets, 222
ACLs (access control lists), 69, 448. *See also* access lists
  Cisco IOS filters, 448–449
    extended, 451, 455
    named, 456
    reflexive, 456, 459
    standard IP, 449–450
    Turbo, 455
  Java inspections, 478
acquisition data, data classification, 297
ACS (Access Control Server), 593
active audit devices, 446–447
active states, EIGRP routing concepts, 223
ad hoc wireless LAN, 278
Adaptive Security Algorithm, 485
address of record, 286
Address Resolution Protocol (ARP), 364
addresses
  illegal, 342
  IP. *See* IP addresses
  RIP routing database, 214
  translation, gatekeeper service, 181
  unicast, 324
  VPN device authentication, 582
administrative data, asset value, 296
administrators
  security policy and procedures
    audits, 348–350
    backups, 347–348
    equipment certification, 348
  site security policy and procedures
    portable tools, 348
    sample policy, 350–351
admissions
  gatekeeper services, 181
  request, 598
advanced distance vector protocol, 221
Advanced Encryption Standard, 9, 282
advanced filtering, 639–640
  branch routers, 640–641
  Internet router, 643
  NAS router, 641–642
AES (Advanced Encryption Standard), 9–11, 282
agents, DDoS, 254
AH (Authentication Header), 86, 139
Airsnort website, 281
alarms, false positives, 345
alerts
  incident handling, 367–369
  protocol, SSL, 79
algorithms
  Caesar Cipher, 7
  cryptography, 6
  Diffie–Hellman, 11
    key distribution, 24
    secret keys, 25–27
  El Gamal, 15
  Message Digest 4, 17
  Message Digest 5, 17
  Rijndael, 10
  RSA, 15
  Secure Hash Algorithm, 17
alps commands, Cisco IOS privilege access, 381
amplifiers, WLANs component, 153
antennas, WLANs component, 153
anti-spam methods, 196
Anti-Spam website, 272
AOR (address of record), 286
applets (Java)
  application content filtering, 461–462
  block encapsulated, 462
application-level proxy, 84
applications
  authentication, VPNs, 578, 584–585
  content filtering
    Java applets, 461–462
    World Wide Web, 461
  firewalls, 337
    authentication, 466–467
    authorization, 466–467
  gateways, 336
  layer, security protocols, 73
    S/MIME, 74, 77
    SHTTP, 73–74
  protocols, SSL, 79
application-specific integrated circuit, 455
apply commands, 488
APs (access points), 248
arap service, AAA authentication, 511
Archie protocol, 463
architectures
  advanced firewalls, 459
    application content filtering, 461–462
    authentication, 466–467
    authorization, 466–467
    common application protocols, 462, 466
    e-mail, 462
    encryption, 467, 471
    NAT, 472, 475
    packet session filtering, 460–461
    SMTP, 462
    URL-blocking, 462
    URL-filtering, 462

external screening router, 447–448, 459
Internet access, 445, 447
point-to-point architecture, 243–273, 280–283
security, 306
audit, 308–309
availability, 308
confidentiality, 308
identity, 306–307
integrity, 307
archive commands, Cisco IOS privilege access, 381
areas, 224
ARP (Address Resolution Protocol), 364
ARQ (admission request), 598
ASA (Adaptive Security Algorithm), 485
ASIC (application-specific integrated circuit), 455
assessments
procedures, risks, 342
security vulnerability, 343
assets
replacement values, 296
risk assessment, 295
evaluations, 299–302
network assets, 295–296
threats, 297–299
value of assets, 296–297
vulnerability, 297–299
asymmetric encryption, 11, 15
Asynchronous Transfer Mode, 526
ATM (Asynchronous Transfer Mode), 526
attacks
collecting information, 434–435
common deterrents
exposed services, 340
internal client hosts, 341
random host attacks behind firewalls, 340
spoofing, 341
corporate networks, 423
broadcast attacks, 425
fragmentation attacks, 424
spoofed packets, 423–424
TCP SYN attacks, 425–426
DDoS
filtering, 633–634
mitigating steps, 646, 651
preventive measures, 635, 646
rate limiting, 633–634
denial of service (DoS), 253–254
distributed denial-of-service (DDoS), 254, 257
DoS, basics, 633
examples, 625–626
FMS, 281
impersonation, 250–253
incidents
detection, 359–365
handling, 365–369
recovery, 372
responding to, 369–372
response team, 358–359
land.c, 253, 264
man-in-the-middle, 17, 26, 278
motivation for, 257–258
Ping of Death, 253, 266–267
protocol vulnerabilities, 258
DNS, 268–271
FTP, 272–273
ICMP, 265–268
NFS service, 275
NIS service, 275
NNTP, 271
SMTP, 271–272
TCP/IP, 258, 264
UDP, 264–265
X Window System, 275
Replay, 39, 250, 340
response guidelines, 615
documents, 621
employees, 619–620
investigations, 616, 622–623
legal processes, 618
managers, 622
networks, 618–619
protecting materials, 620–622
reporting, 622
reports, 616
security policies, 617–618
routing protocols, 287–288
Smurf, 253
ICMP, 267
tracing DDoS attacks, 649
social engineering, 288
spam, SMTP, 272
spoofing, 250, 258
TCP SYN, 253, 263–264
teardrop.c, 253, 267–268
unauthorized access, 242
Internet, 242–244
packet snooping, 244–245
remote dial-in access, 246–247
wireless access, 248–249
VoIP, 283
denial of service (DoS), 284
impersonation, 284
SIP-based networks, 284–287
unauthorized access, 283
VPN, 276
denial of service (DoS), 277
impersonation, 277
unauthorized access, 276
wireless networks, 278
denial of service (DoS), 279
impersonation, 279
unauthorized access, 278–279
WEP, 280–282
audio codecs, H.323 standard component, 183
audio streaming, protocol, 463
audio-prompt commands, Cisco IOS privilege access, 381

audits
  corporate networks, 427
    collecting attack information, 434–435
    configuration verification, 427
    intrusion detection, 431–434
    logging, 427–431
    monitoring, 427–431
  network administrator security policy, 348
    data storage, 349–350
    information to collect, 349
    legal considerations, 350
  security architecture, 308–309
  tracking incidents, 360
  VoIP networks, 605
  VPNs, 590
  wireless network, 595–596
authentication, 5, 20
  802.1X, 173–175
    EAP-TLS, 175
    EAP-TTLS, 175
    LEAP, 176
    PEAP, 176–177
  algorithm, OSPF, 229
  asymmetric encryption, 14–15
  BGP-4, 234–235
  Cisco IOS Software, lock ad key feature, 526
  corporate network, 378–379
    access privileges, 379–395
    line access controls, 395–408
  cryptography, impersonation, 250
  data
    CMS, 76
    integrity, 339
    routing updates, 339–340
  definition, 37
  dial-in access, 503
    complex corporate environment, 510–515
    simple corporate environments, 504, 510
  double, 532–536, 539
  EIGRP, 224
  firewalls, 337, 466–467
  FORTEZZA protocol, 71
  identity, 37
  identity technologies, 38–39
    passwords, 39, 44
    PPP, 45, 54
  image, 408–409
  IPsec protocol suite, 86, 91, 468
  IS-IS, 231–232
    cryptographic, 232–233
    simple password, 232
  Kerberos, 580
  key (shared secret), 210
  logical security controls, 331–333
  methods, 21
  object identifiers, 22–23
  OSPF, 225
    cryptographic, 226–228
    IPv6, 228
    null, 226
    simple password, 226
  password protocol enforcement, 333
  protocol, 463–464
  RIP, 216
    cryptographic, 217–220
    plaintext, 216–217
  routing, 210, 410–412
  routing protocols, 210
    MD5, 211–213
    plaintext, 211
  S/MIME, 198
  security architecture, 306
  server, 63
  shared key, 170
  subscription-based, 194
  symmetric encryption-based, 193
  trust model, 21–22
  value, 232
  verification mechanisms, 55
    DCE, 69
    FORTEZZA protocol, 69–71
    IEEE 802.1x standard, 71–72
    Kerberos protocol, 63, 68
    RADIUS protocol, 60–62
    TACACS+ protocol, 55, 59
  VoIP network, 597–599
  VPNs
    application authentication methods, 584– 585
    device authentication methods, 579–582
    identity, 577
    security, 147–148
    user authentication methods, 583–584
    various methods, 585–586
  wireless network, 593
  WLANs, 169–170
Authentication Header. *See* AH
auth-guest methods
  AAA authentication, 512
  services, 513
authorization, 20
  corporate network, 378–379
    access privileges, 379–395
    line access controls, 395–408
  definition, 37
  dial-in access, 515–516
    RADIUS, 516, 521
    TACACS+, 516, 521
  double, 532, 536
  firewalls, 466–467
  identity, 37
  methods, 21
  RADIUS protocol, 61
  security architecture, 306
  session, 57
  TACACS+ protocol, 57
  trust model, 21–22
auth-proxy events, AAA accounting, 522

auto commands, 530
automated attack-mitigations, 346
automated double authentication, 536–539
automatic risk analysis tools, 300
autonomous systems, 208
auxiliary ports, 400–401
availability
  corporate networks, 415–416
    attack deterrents, 423–426
    redundancy, 416–423
  security architecture, 308
  VoIP networks, 604–605
  VPNs, 589
  wireless network, 594–595

B

BackboneFast Convergence feature, 421
backups, network administrator security policy, 347–348
bandwidth management, gatekeeper services, 181
banner messages, logical security controls, 333
baseline signal levels, cable, 316
basic access modes (login mode), 379
  Cisco IOS devices, 379–383
  Cisco PIX firewall, 393–395
  Cisco switches, 389–392
Bellovin, Steven
  Firewalls and Internet Security, 258
  TCP fix, 262
Bernard Aboba website, 177
bfe commands, Cisco IOS privilege access, 381
BGP (Border Gateway Protocol), 411
BGP-4 (Border Gateway Protocol version 4), 209, 234
  authentication, 234–235
  security future, 235–236
billing
  dial-access, TACACS+, 524–525
  dial-in access, 522
Blaze, Matt, Clipper chip, 31
blocking, URL, 462
Bluetooth, 152
bombing, e-mail, 272
Border Gateway Protocol (BGP), 411
Border Gateway Protocol version 4 (BGP-4), 209
boundaries
  routing, 327, 329
  subnet, logical security controls, 324, 330
  VLAN, logical security controls, 329–330
BPDUs, 419–420 (bridge protocol data units), 419
branch routers, 510
  advance filtering, 640–641
  listing configuration, 508–509
  lock and key feature (Cisco IOS Software), 530–532
  simple filtering policy, 636–637
breaking, 6
bridge protocol data units (BPDUs), 419
bridges, WLANs component, 153
Bro, "A System for Detecting Network Intruders in Real-Time," 364
broadcast attacks, corporate networks, 425
broadcast keyword, AAA accounting, 523
brute-force attacks, 6
BYE, SIP signaling message type, 189

C

CA (certificate authorities), 29
cable tap, intrusion detection system, 362
cables
  baseline signal level, 316
  selection, physical security controls, 314–318
cache, 129, 270
Caesar Cipher algorithm, 7
California state laws, 624–625
call commands, Cisco IOS privilege access, 381
callback mechanisms, centralized billing, 524–525
call-processing manager, 178
campus networks, routing, 328
CANCEL, SIP signaling message type, 189
capabilities, 20
CAR (committed access rate), 644
carrier sense multiple access/collision detect architecture (CSMA/CD), 160
CAT (Cisco access token), 599
CAUCE website, 272
CBAC (Content-Based Access Control), 476
  Cisco IOS firewall, 476–479
  default threshold values, 478–479
  default timeout, 478–479
CBC (Cipher Block Chaining), 7
CCC (Chaos Computer Club), 356
CCIPS (Computer Crime and Intellectual Property Section), website, 369
ccm-manager commands, Cisco IOS privilege access, 381
CCO (Cisco Connection Online), 408
CCP (Compression Control Protocol), 143
cd commands, Cisco IOS privilege access, 381
CEF (Cisco Express Forwarding), 644, 657
CEK (content encryption key), 75
centralized billing, TACACS+, 524–525
CERT (Computer Emergency Response Team), filtering recommendations, 338
certificate authorities (CAs), 28–31
certificate revocation list (CRL), 127, 580
certificates
  authentication, VPNs security, 147–148
  format, S/MIME communication, 76
  PKI, 124–125, 128–129
  selection, SHTTP protocol, 73
certification, PKI function, 122
CET, virtual dial-in access, 540, 548

CFB (Cipher FeedBack), 7
chaining mechanisms, 7
Challenge Handshake Authentication Protocol *See* Chap
challenge-response approach, token authentication, 42
change cipher spec protocol, SSL, 79
Chaos Computer Club (CCC), 356
CHAP (Challenge Handshake Authentication Protocol), 45, 144, 277, 504, 580
  PPP protocol, 48–51
  simple corporate environment authentication, 504
  strengths, 54
  weaknesses, 54
Chapman, David W. Jr., *Cisco Secure PIX Firewalls,* 490
Chargen protocol, 464
checksums
  computation, 142
  packets, 340
  routing updates, 340
Cheswick, William, *Firewalls and Internet Security,* 258
CIAC website, 369
Cipher Block Chaining, 7
Cipher FeedBack, 7
circuits
  filtering, 336
  metro Ethernet, configuring, 243–273, 280–283, 315–328, 335–336, 378, 403, 409–418, 426, 501
Cisco. *See also* Cisco IOS Software
  access token, 599
  PIX firewall
    access modes, 393–395
    basic access commands, 393
    HTTP security, 408
    line access controls, 402–405
    network availability, 421–423
    privilege access commands, 393–394
  switches
    basic access commands, 389
    basic access mode, 389–392
    line access controls, 401–402
    network availability, 418–421
    privilege access commands, 390
    privilege access mode, 389–392
  website, 613
Cisco Connection Online (CCO), 408
Cisco Express Forwarding (CEF), 644, 657
Cisco IOS Software. *See also* Cisco
  authentication, 511
  auxiliary ports, 400–401
  basic access commands, 379–380
  CET, 540, 548
  control ports, 396–400
  devices
    access modes, 379–389
    HTTP security, 406–408
  filters, 448–449
    extended IP ACLs, 451–455
    named ACLs, 456
    reflexive ACLs, 456–459
    standard IP ACLs, 449–450
    Turbo ACLs, 455
  firewall
    CBAC, 476–479
    sample configuration, 480, 485
  intrusion detection, 432–433
  IPsec, configuring, 548, 554
  keyword group, 512
  lock and key feature, 526
    access operation, 526–528
    authentication, 526
    branch router access, 530–532
    multiple access privileges, 532
    telecommuter access, 528–530
  network availability, 416–417
  privilege access commands, 381–383
  virtual terminal ports, 401
Cisco Secure Intrusion Detection Systems, 432
Cisco Secure PIX Firewalls, 490
Cisco Secure server syntax, 520–521
clear commands
  Cisco IOS basic access, 379
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  clear help commands, 390
  clear ip cache, 650
CLI (command-line interface), 401
client data, asset value, 297
client-to-site VPNs, 138–139
clinical trial results, data classification, 297
Clipper chips, 31
CLNS (Connectionless Network Service), 209
clock commands, Cisco IOS privilege access, 381
CMS (Cryptographic Message Syntax), 75
cns commands, Cisco IOS privilege access, 381
coax cables, 314
Code Red II virus, 357
Code Red virus, 357
coded messages, 5
collision attacks
  IVs, 281
  Web IVs, 282
command-line interface (CLI), 401
commands, 405, 513
  aaa-server, 402
  AAA authentication, 386
  access-enable
    Cisco IOS basic access, 379
    Cisco IOS privilege access, 381
  access-list, 449, 487, 529
  access-list compiled, 455, 487
  access-profile, 533
    Cisco IOS basic access, 379
    Cisco IOS privilege access, 381

access-template commands, Cisco IOS privilege access, 381
authentication enable default method 1 commands, 386
authentication local-override, 513
authentication login, 399
authorization, default method lists, 518
Cisco IOS basic access, 379–380
Cisco IOS privilege access, 381–383
Cisco PIX firewall
  basic access commands, 393
  privilege access commands, 393–394
Cisco switch basic access, 389
Cisco switch privilege, 390
clear
  Cisco IOS basic access, 379
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  clear help commands, 390
  clear ip cache, 650
conduit, 487
configure
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  PIX firewall privilege access, 393
connect
  Cisco IOS basic access, 379
  Cisco IOS privilege access, 381
console, 402
copy, Cisco IOS privilege access, 381
crypto, TACACS+ authorization, 388
crypto map, 550
debug
  Cisco IOS privilege access, 381
  PIX firewall privilege access, 393
disable
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  PIX firewall privilege access, 393
disconnect
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
disengage request, 598
distance, 414
distribute list, 414
enable, 379
  AAA authorization, 387, 399, 512
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  enable password, 384–387, 394
  enable secret, 384–387
  PIX firewall basic access, 393
  PIX firewall privilege access, 393
  services, 512–513
events, AAA accounting, 522
help
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
history
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
http, 393
if-authenticated, 391
if-con, VIP console, 652
if-quit, VIP console, 653
illegal, 462
keyinit, 41
lock, 381
login
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
  lock and key authentication, 526
log-input commands, 424
logout
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
look, 380
kill, 393
microcode, 382
modemui, 380–382
monitor, 382
more, 382
mpoa, 382
mrinfo
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
mrm, 382
mstat
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
mtrace
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
name-connection
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
nat, 487
ncia, 382
new-model, 386, 398
no access-list , 450
no, 382
no exec, 400
no failover active, 422
no failover, 422
no ip directed-broadcast, 425
none, 391
outbound, 488
pad, Cisco IOS basic access, 380
passive interface, 414

passwords, 39, 393, 403, 526
  CEK encryption, 75
  Cisco IOS privilege access mode, 384–385
  logical security controls, 331–333
  protocol enforcement, 333
  S/Key One-Time Password System, 39–41
  security architecture, 307
  selection guidelines, 332
  statically configured, 579
  token authentication systems, 42–44
ping commands, 242
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  PIX firewall privilege access, 393
ppp
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
privilege level, 387
pwd, 382
quit
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  PIX firewall basic access, 393
  PIX firewall privilege access, 393
radio
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
radius-server, 393
reconfirm, 390
reload
  Cisco IOS privilege access, 382
  PIX firewall privilege access, 393
restart, 382
resume
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
rlogin
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
Router#?, 381
Router>?, 379
rsh, 382
sdlc, 382
session
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  PIX firewall privilege access, 393
set
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  set authentication login, 401
  set enable, 439
  set enablepass, 391
  set help, 389
  set ip permit, 402
  set password, 439
  set spantree root, 421
setup, 382
show, 387, 434
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  show config, 388
  show failover, 422
  show failover lan, 422
  show help, 389–390
  show interfaces rate-limit, 645
  show ip arp mac-address, 648
  show ip cache flow, VIP console, 654
  show line vty, 401
  show privilege all, 393
  show proc cpu, VIP console, 654
  show running-config, 387
  show startup-config, 388
slip
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
  Cisco switch privilege access, 390
standby, 390
start-chat, 383
switch, 390
Switch> (enable) ?, 390
syslog, 393
systat
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
TACACS+ authorization, 388
upload, 390
uptime
  PIX firewall basic access, 393
  PIX firewall privilege access, 394
username, 518, 526
virtual telnet commands, 585
voice commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
wait
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
where
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
who
  PIX firewall basic access, 393
  PIX firewall privilege access, 394
write, 403
  Cisco IOS privilege access, 383
  Cisco switch privilege access, 390
  PIX firewall privilege access, 394
write memory, 388, 423
write terminal, 387
Commands service type, AAA authorization, 516
commercial off-the-shelf (COTS), 70
committed access rate (CAR), 644
community strings, 406

Compression Control Protocol (CCP), 143
compulsory tunnels, 150
Computer Crime and Intellectual Property Section (CCIPS), 369
Computer Emergency Response Team, 338
Comsat protocol, 464
conduit commands, 487
confidentiality, 5
  data, 37
    asymmetric encryption, 13
    corporate networks, 414–415
  OSPF and IPv6, 228
  security architecture, 308
  standard of conduct sample, 293
  VoIP networks, 603
  VPNs, 589
  wireless network, 594
configurations, corporate networks, 427
configure commands
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  PIX firewall privilege access, 393
conflicts of interest, standard of conduct sample, 293
connect commands
  Cisco IOS basic access, 379
  Cisco IOS privilege access, 381
connection events, AAA accounting, 522
Connectionless Network Service, 209
connections, TCP/IP, three-way handshake, 260–261
console commands, 402
content encryption key, 75
Content-Based Access Control, 476
control connections
  L2TP protocol link-layer security, 116–117
  PPTP link-layer security, 112
control ports, 396–400
copy commands, Cisco IOS privilege access, 381
core teams
  incident response team, 359
  qualifications, 359
corporate memos, data classification, 297
corporate networks
  audit, 427
    collecting attack information, 434–435
    configuration verification, 427
    intrusion detection, 431–434
    logging, 427–431
    monitoring, 427–431
  availability, 415–416
    attack deterrents, 423–426
    redundancy, 416–423
  data confidentiality, 414–415
  identity
    authentication, 378–408
    authorization, 378–408
  infrastructure, 378
  integrity, 408
    image authentication, 408–409
    routing authentication, 410–412
    routing filters, 412–414
    workgroups, 409–410
  security implementation examples, 435–442
  VPNs, 136
corporate standard of conduct sample, 292–294
costs, security, 302–304
COTS (commercial off-the-shelf), 70
cracking passwords, 331
CRC (cyclic redundancy check), 117, 282
credentials, Kerberos protocol, 63, 67
CRL (certificate revocation list), 127, 580
cross-certification, PKI function, 123
crypto commands, TACACS+ authorization, 388
crypto map commands, 550
cryptographic algorithms, SHTTP protocol, 73
cryptographic authentication
  IS-IS, 232–233
  OSPF, 226–228
  RIP, 217–220
cryptographic checksum, 410
cryptographic keys, IPsec protocol suite, 92, 97–102, 106
Cryptographic Message Syntax (CMS), 75
Cryptographic Sequence Number, 227
cryptography, 5–6
  asymmetric encryption, 11, 15
  authentication, 20
    impersonation attacks, 250
    methods, 21
    object identifier, 22–23
    trust model, 21–22
  authorization, 20
    methods, 21
    object identifier, 22–23
    trust model, 21–22
  digital signatures, 17–20
  fata confidentiality, 342–343
  hash function, 16–17
  keys, 5
  escrow, 23, 31–32
  published resources, 611
  symmetric encryption, 6–9
    3DES, 10
    AES, 10–11
    DES, 9
    IDEA, 10
    RC-4, 10
  WLANs authentication, 169–170
CSMA/CD (carrier sense multiple access/collision detect architecture), 160
The Cuckoo's Egg, 348
CUseeMe protocol, CBAC inspection, 463, 477
Cut-Thur-Proxy, PIX firewall, 488–490
cyber crimes, 369
cyclic redundancy check (CRC), 117, 282

D

Daemen, Dr. Joan (Rijndael algorithm developer), 10
damage incident, 366
data
  asset value, 296–297
  channels, L2TP protocol link-layer security, 117–118
  classifications, 297
  confidentiality, 37, 342
    asymmetric encryption, 13
    corporate networks, 414–415
    sample policy, 343
  content type, CMS, 75
  integrity, 16–17, 37
    asymmetric encryption, 13
    site security policies, 335, 342
  log files, 309
  network assets, 296
  risk assessment
    compromises, 298
    integrity, 298–299
  storage audits, 349–350
Data Encryption Standard (DES), 9, 63, 540
databases
  link-state, 224, 229
  protocol, 464
datagrams, 207, 267
Daytime protocol, 464
DCE (Distributed Computing Environment), 55, 69
dCEF, 657
DDoS (distributed denial-of-service), 254–257
  attacks. *See also* DoS attacks
    filtering, 633–634
    mitigating steps, 646–651
    preventive measures, 635–646
    rate limiting, 633–634
    website links for blocking, 657
  automated attacks, 255
  clients, 254
  valid addresses, 634
  attacks. *See also* DoS attacks
    filtering, 633–634
    mitigating steps, 646–651
    preventive measures, 635–646
    rate limiting, 633–634
    website links for blocking, 657
DDR (dial-on-demand routing), 526
debug commands
  Cisco IOS privilege access, 381
  PIX firewall privilege access, 393
debug ip packet details, 650
decision support, 343
decryptions
  Caesar Cipher algorithm, 8
  WEP, 168
defaults
  method list, 513
  passwords, 331
  routing, 208
Defense Information Infrastructure (DII), 69
delegation of trust, 22
delete commands, Cisco IOS privilege access, 381
demilitarized zone, 601
  networks, 340
denial of service (DoS), 253–254. *See also* DoS
  VoIP vulnerabilities, 284
  VPN vulnerabilities, 277
  wireless networks, 279
deny all commands, 450
DES (Data Encryption Standard), 9, 63, 540
des option, encryption algorithm, 549
destination addresses, NAT, 475
destination port numbers, 453
detective controls, logical security, 330
devices
  authentication, VPNs, 577–582
  Cisco IOS
    access modes, 379–389
    HTTP security, 406–408
  security
    access, 320–321
    environmental safeguards, 321–322
    location, 319–320
DHCP (Dynamic Host Configuration Protocol), 145, 252, 582
dial-in access
  AAA
    double authentication, 532, 539
    lock and key, 526, 532
  accounting, TACACS+, 522–523
  authentication, 503
    complex corporate environment, 510, 515
    simple corporate environments, 504, 510
  authorization, 515–516
    RADIUS, 516, 521
    TACACS+, 516, 521
  billing, 522–525
  environment, 501
  Internet use, 502
  PPP authentication protocols, 45–46
    CHAP, 48–51
    EAP, 51–54
    PAP, 47–48
    summary, 54
  security concerns, 502–503
  unauthorized, 246–247
  virtual encryption, 539, 572
dial-on-demand routing, 526
Diffie-Hellman (DH) public-key algorithms, 11, 540
  agreement protocol, 229
  key distribution, 24
  secret keys, 25–27
diffusing computations, 222

Diffusing Update algorithm, 221
digest data content type, CMS, 75

digital certificates, 20, 39
    obtaining through certificate authority, 30
    public keys, 28–29
digital rights management, 355
Digital Signature Standard (DSS), 20, 540
digital signatures, 579
    creating, 18
    cryptography, 17–20
    impersonation, 253
    verification, 19
Digital Subscriber Line, 371, 576
DII (Defense Information Infrastructure), 69
dir commands, Cisco IOS privilege access, 381
direct connections, router mechanism, 208
Direct Sequencing Spread Spectrum. *See* DSSS
Directory Information Tree (DIT), 129
disable commands
    AAA authorization, 387
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 381
    Cisco switch privilege access, 390
    PIX firewall privilege access, 393
Discard protocol, 464
disconnect commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 381
    Cisco switch privilege access, 390
disengage request, 598
distance commands, 414
distribute list commands, 414
Distributed Computing Environment, 55
distributed denial-of-service. *See* DDoS
DIT (Directory Information Tree), 129
DMZ networks (demilitarized zone networks), 340
DNS (Domain Name System), 268, 446
    cache poisoning, 270
    hierarchy, 268
    protocol, 464
    resolving queries, 269
    vulnerabilities, 268
DNSSEC (DNS Security), 270
documentation
    incidents, 369–370, 621
    network assets, 296
    policies on network security, 612
Domain Name System. *See* DNS
DoS (denial of service), 253–254
    attacks. *See also* DDoS attacks
        basics, 633
        monitoring, 651–565
        resources, 662
    VoIP vulnerabilities, 284
    VPN vulnerabilities, 277
    wireless networks, 279
double authentication, 532–539
double authorization, 532–536
download commands, Cisco switch privilege access, 390
DRQ (disengage request), 598
DSL (Digital Subscriber Line), 371, 576
DSS (Digital Signature Standard), 20, 540
DSSS (Direct Sequencing Spread Spectrum), 156–157
DUAL (Diffusing Update algorithm), 221
Dynamic Host Configuration Protocol (DHCP), 145, 252, 582
dynamic ports, NAT, 475
dynamic source addresses, NAT, 475

E

EAP (Extensible Authentication Protocol), 45–51
    packet format, 51
    PPP protocol, 51–54
    RADIUS, 54
    strengths, 54
    weaknesses, 54
EAP over LANs (EAPOL), 72
EAP-Cisco Wireless. *See* LEAP
EAPOL (EAP over LANs), 72
EAP-TLS (EAP-Transport Layer Security), 802.1X network port authentication, 175
EAP-Transport Layer Security (EAP-TLS), 175
EAP-TTLS (EAP-Tunneled TLS), 802.1X network port authentication, 175
EAP-Tunneled TLS (EAP-TTLS), 175
eavesdropping, 244
ECB (Electronic CodeBook), 7
echo request packets, ICMP, 266
ECP (Encryption Control Protocol), 86, 143
EGP (Exterior Gateway Protocol), 208–209
egress
    Internet, 272
    filtering, DDoS attacks, 635
        advanced filtering, 639–643
        simple filtering policy, 636–639
    points, 341
EIGRP (Enhanced Interior Gateway Routing Protocol), 209, 221, 411, 548
    authentication, 224
    packet types, 223–224
    routing concepts, 222
        active state, 223
        neighbor table, 222
        passive state, 223
        tagging, 223
        topology table, 222
    technologies, 221–222
El Gamal algorithm, 15
Electronic CodeBook, 7
electronic messaging, FORTEZZA protocol, 71
e-mail
    advanced firewall architecture, 462
    bombing, 272

  protocol, 464
  spamming, 272
employees
  incidents, 619–620
  locator files, data classification, 297
  salaries, data classification, 297
  security policies, 309–310
    audits, 348–350
    backups, 347–348
    equipment certification, 348
    portable tools, 348
  site security policies and procedures samples, 350–351
enable commands, 379
  AAA authorization, 387, 399, 512
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
  enable password commands, 384–387, 394
  enable secret commands, 384–387
  PIX firewall basic access, 393
  PIX firewall privilege access, 393
  services, 512–513
enable modes (privilege access mode), 379
enable services, AAA authentication, 511
Encapsulating Security Payload, 139, 582
encryption
  advanced firewall architecture, 467, 471
  algorithm, OSPF, 229
  asymmetric, 11, 15
  Caesar Cipher algorithm, 8
  data
    CMS, 76
    confidentiality, sample policy, 342–343
  IPsec protocol suite, 86, 91
  Kerberos protocol, 64, 66
  PIX firewall, 394
  public key, 579
  RADIUS, 62
  S/MIME, 198
  service password-encryption commands, 384
  symmetric, 6, 9
    3DES, 10
    AES, 10–11
    DES, 9
    IDEA, 10
    RC-4, 10
  TACACS+, 62
  virtual dial-in access, 539
    CET, 539, 548
    GRE tunneling, 539, 548
    IPsec, 548, 554
    L2TP with IPsec, 554, 572
  WEP, 166–169
Encryption Control Protocol (ECP), 143
endpoint authentication, 598
Enhanced Interior Gateway Routing Protocol. *See* EIGRP
enterprise networks
  protocol vulnerabilities, 258
    DNS, 268–271
    FTP, 272–273
    ICMP, 265–268
    NFS service, 275
    NIS service, 275
    NNTP, 271
    SMTP, 271–272
    TCP/IP, 258, 264
    UDP, 264–265
    X Window System, 275
  security policies, 304–306
  threats
    denial of service (DoS), 253–254
    distributed denial–of–service (DDoS), 254–257
    impersonation, 250–253
    motivation for, 257–258
    unauthorized access, 242, 249
enveloped data content type, CMS, 75
environment safeguards, physical device security, 321–322
equipment certification, network administrator security policy, 348
erase commands, Cisco IOS privilege access, 381
escrow keys, 5
ESP (Encapsulating Security Payload), 87, 139, 582
established keywords, 455–456
Ethernet
  10BASE-T switch, 245
  packet decorder, 244
ETSI (European Telecommunications Standards Institute), 152
European Telecommunications Standards Institute (ETSI), 152
evaluations, risk assessment, 299–302
exclusive function (XOR), 59, 166
exec events, AAA accounting, 522
EXEC service type, AAA authorization, 516
exec-timeout commands, 397
exit commands
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
Extended Authentication (Xauth), 140
extended IP ACLs, 451–455
extended IV and sequencing rules, TKIP protocol, 171
Extensible Authentication Protocol. *See* EAP
Exterior Gateway Protocol, 208
external peer, 234
extranet, VPNs, 137, 150–151

F

failover active commands, 422
failover commands, 421–423
failover lan commands, 422
failover mac address commands, 423
false positives, 345
FASP (Federal Agency Security Practices), website, 612
FCC (Federal Communications Commission), 156
FCS (Frame Check Sequence), 46
FDDI, MTUs, 266
feasible successors, 221
Federal Agency Security Practices, 612
Federal Communications Commission (FCC), 156
Federal Information Processing Standards Publication 197 (FIPS 197), 10
Federal Information Processing Standards Publications (FIPS PUBs), 612
FHSS (Frequency-Hopping Spread Spectrum), 157
FIB (Forwarding Information Base), 645
File Transfer Protocol. *See* FTP
files, FORTEZZA protocol, 71
filters
    ACLs, 448–449
        extended, 451–455
        named, 456
        reflexive, 456–459
        standard IP, 449–450
        Turbo, 455
    CBAC packet session filtering, 476–479
    circuit, 336
    DDoS attacks, 633–635, 643
    deploying, 643
    firewalls
        application content, 461–462
        packet session, 460–461
    packet, 336
    routing, 328, 412–414
    traffic, 323
    URL, 462
FIN flag, TCP, 260
financial data, asset value, 296
Finger protocol, 464
fingerprints
    digital signatures, 17–20
    hash function, 16
FIPS 197 (Federal Information Processing Standards Publication 197), 10
FIPS PUBs (Federal Information Processing Standards Publications), 612
fire detection, 321
firewalls, 445
    advanced architecture, 459
        application content filtering, 461–462
        authentication, 466–467
        authorization, 466–467
        common application protocols, 462–466
        e-mail, 462
        encryption, 467, 471
        NAT, 472, 475
        packet session filtering, 460–461
        SMTP, 462
        URL-blocking, 462
        URL-filtering, 462
    attacks to random hosts, 340
    basic access mode, 393–395
    Cisco IOS
        CBAC, 476–479
        sample configuration, 480–485
    deployment, 335
    impersonation, 252
    infrastructure integrity, 335–337
    Internet access, 445–447
    IPSec uses, 468
    line access controls, 402–405
    network availability, 421–423
    PIX, 485–486
        advanced features, 490
        Cut-Thur-Proxy feature, 488–490
        HTTP security, 408
        inbound access, 486–487
        intrusion detection, 433–434
        outbound access, 488
        sample configuration, 490
    privilege access mode, 393–395
    published resources, 611
    SIP, 601–602
Firewalls and Internet Security, 258
fixed-length output, hash, 16
fixup protocol commands, 599
flags, TCP, 260
FMS attacks, 281
FORTEZZA protocol, 69–71
Forwarding Information Base (FIB), 645
Fox, Andy, *Cisco Secure PIX Firewalls,* 490
fraggle attacks, 253
fragmentation attacks, corporate networks, 424
fragments, 79
Frame Check Sequence (FCS), 46
Frequency-Hopping Spread Spectrum (FHSS), 157
FTP (File Transfer Protocol), 272
    ACLs, 454
    CBAC inspection, 477
    passive mode, 273
    protocol, 465
    vulnerabilities, 272–273
FTP-control protocol, IANA-assigned ports, 82
FTP-data protocol, IANA-assigned ports, 82
functions
    hash cryptography, 16–17
    mathematical cryptography, 6

G

GAO (U.S. Government Accounting Office), 356
Garcia-Luna-Aceves, Dr. J. J., DUAL, 221
Garfinkel, Simson, dialup modems, 247
gatekeepers, H.323 standard components, 181
gateways, 207
  application, 336
  H.323 standard components, 180
  MGCP, 602
  SIP, 602
  SIP client, 188
Generic Routing Encapsulation. *See* GRE
Generic Token Card, 52
Gigabit Ethernet
  MTUs, 266
  switches, intrusion detection system, 361
globally unique addresses, 473
Gopher protocol, 463
GRE (Generic Routing Encapsulation protocol), 111, 143, 540
  PPTP IP tunneling, 112–113
  tunneling, 540
greed, attack motivation, 258
greeting messages, logical security controls, 333
groom commands, PIX firewall privilege access, 393
group keyword, 386, 399, 405
groups, inherited trusts, 21
GTC (Generic Token Card), 52
guest methods
  AAA authentication, 512
  services, 513

H

H.225 standard
  H.323 standard component, 182
  H.323 call setup security, 194
H.225.0 RAS, H.323 standard component, 182
H.245 standard
  H.323 standard component, 183
  H.323 call control security, 195
H.323 standard, 180, 463
  CBAC inspection, 477
  components, 180–182
    protocol suite, 182–183
    RAS signaling protocols, gatekeeper call-signaling flow, 184–186
  protocol security, 193
    call control, 195
    call setup, 194
    encrypted media streams, 195–196
    RAS authentication, 193–194
  SIP interaction, 192–193
h323 keyword, 605
Halabi, Sam, *Internet Routing Architectures,* 234
handlers, DDoS, 254
handshake process, SSL, 80–81
handshake protocol, SSL, 79
hardware, network assets, 296
hash (message digest), 211
  algorithm, S/MIME communication, 76
  fixed-length output, 16
  functions, cryptography, 16–17
HDLC (High-Level Data Link Control), 45, 107
hello packets, EIGRP, 223
help commands
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 381
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
hidden-node problem, 161
HIDS (host-based IDS), 345
High-Level Data Link Control (HDLC), 45, 107
HiperLAN, 152
history commands
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
HMAC-MD5-96, 87
hold time, 222
HomeRF SWAP, 152
honey pots, intrusion detection system, 363
hop count (metric), 214
host-based IDS, 345
hosts
  attacks behind firewall, 340
  internal client attacks, 341
  source, 451
Hot Standby Router Protocol, 416
HSRP (Hot Standby Router Protocol), 416
HTTP
  digest authentication, 197–198
  firewall authentication, 466
  firewalls, encrypted authentication, 470
  protocol, 463
    IANA-assigned ports, 82
  security, 406
    Cisco IOS devices, 406–408
    Cisco PIX firewall, 408
http commands, PIX firewall privilege access, 393
HTTP Digest, SIP-based networks, 285
hubs *versus* switch functionality, 361
humidity controls, 322
HYPER channel, MTUs, 266

I

"I Love You" virus, 357
IANA (Internet Assigned Numbers Authority), 141, 634
  ports, 629–630
ICMP (Internet Control Message Protocol), 244, 265, 450
  echo request packet, 266

packets, rate limiting, 265, 644
vulnerabilities, 265–266
Ping of Death, 266–267
smurf attack, 267
teardrop.c attack, 267–268
ICV (integrity check value), 168
IDEA (International Data Encryption Algorithm), 9–10
Identd protocol, 465
identification, FORTEZZA protocol, 71
identity, 37
authentication, 378–408
authorization, 378–408
security architecture, 306–307
technologies, 38–39
authentication verification, 55, 72
passwords, 39–44
PPP, 45, 54
type, EAP packet format, 52
VoIP network
access control, 599–602
authentication, 597–599
VPNs, 577
access control, 586–588
application authentication methods, 584– 585
authentication, 577
device authentication methods, 579–582
entities authenticated, 577–578
user authentication methods, 583–584
various authentication methods, 585–586
wireless networks, 592
access control, 593–594
authentication, 593
IDS (intrusion detection system), 244, 309, 345, 361
IEEE 802.1x standard, 71–72
IETF (Internet Engineering Task Force), 140, 213
website, 213
if-authenticated commands, 391
If-Authenticated methods, AAA authorization, 518
if-con commands, VIP console, 652
if-con slot, 652
if-needed methods
AAA authentication, 512
services, 513
if-quit commands, VIP console, 653
ignorance, attack motivation, 258
IGP (Interior Gateway Protocol), 208–209
IKE (Internet Key Exchange), 91, 229, 276, 469, 548
Phase 1 policy, 548
UDP port number changes, 142
versus PPP authentication, 147
illegal addresses, 342
illegal commands, 462
image authentication, 408–409
IMAP protocol, IANA-assigned ports, 82, 464
impersonation
enterprise network threats, 250–253
VoIP, 284
VPN, 277
wireless networks, 279
implicit trusts, 22
inbound traffic, 336
incidents (security breach), 355
contributing factors for, 356
detection, 359–360
intrusion detection systems, 360–365
tracking information, 360
examples, 625–626
handling, 365
alert procedures, 367–369
assessing damage, 366
prioritizing actions, 366
reporting procedures, 367–369
recovery, 372
responding to, 369
acceptable-use policy violation, 370–371
documentation, 369–370
malicious internal hosts, 370
random network interloping, 371–372
response guideline, 615
documents, 621
employees, 619–620
investigations, 616, 622–623
legal processes, 618
managers, 622
networks, 618–619
protecting materials, 620–622
reporting, 622
reports, 616
security policies, 617–618
response team, 358–359, 613
timeline, 356–357
information seeking protocol, 463
information systems department, 294
infrastructures
corporate networks, 378
physical network, 314–319
mode, 154, 278
site security policies, 335
authenticated data, 339–340
common attack deterrents, 340–341
firewalls, 335–337
network services, 337–339
sample policy, 341–342
ingress
filtering, DDoS attacks, 635
advanced filtering, 639–643
simple filtering policy, 636–639
Internet, 272
inherited trusts, groups, 21
initialization, PKI function, 122
initialization vectors (IV), 8, 166, 281
Insertion, Evasion, and Denial Of Service, “Eluding Network Intrusion Detection,” 364
inside interfaces, 403
instances, Kerberos protocol, 63
intrusion detection systems, 360–361

  limitations, 363–365
  published resources, 611
  security policy monitoring, 345–347
  switched networks, 361–363
Integrated Services Digital Network. *See* ISDN
integrity, 5
  corporate networks, 408
    image authentication, 408–409
    routing authentication, 410–412
    routing filers, 412–414
    workgroups, 409–410
  data, 37
    asymmetric encryption, 13
    one-way hash function, 16–17
  security architecture, 307
  VoIP networks, 603
  VPNs, 588
  wireless networks, 594
integrity check value (ICV), 168
interfaces, RIP, 214
Interior Gateway Protocol, 208
Intermediate System-to-Intermediate System (IS-IS), 209, 411
internal client hosts, attack deterrents, 341
internal peer, 234
International Data Encryption Algorithm, 9
International Telecommunications Union (ITU), 180, 319
Internet
  access
    architecture, 445–447
    enterprise network components, 306
    routing, 328
  Cisco IOS firewall
    CBAC, 476–479
    sample configuration, 480–485
  DDoS attacks
    filtering, 633–634
    mitigating steps, 646–651
    preventive measures, 635, 646
    rate limiting, 633–634
  dial-in access, 502
  DoS attacks, 633
  egress, 272
  external screening router architecture, 447– 448
    Cisco IOS filters, 448, 459
  firewalls, 445, 459. *See also* PIX firewall
    advanced packet session filtering, 460– 461
    application content filtering, 461–462
    authentication, 466–467
    authorization, 466–467
    common application protocols, 462–466
    e-mail, 462
    encryption, 467–471
    NAT, 472–475
    SMTP, 462
    URL blocking, 462
    URL filtering, 462
  ingress, 272
  phone protocol, 463
  PIX firewall, 485–486
    advanced features, 490
    Cut-Thur-Proxy feature, 488–490
    inbound access, 486–487
    outbound access, 488
    sample configuration, 490
  policies, 445
  reporting crimes, 369
  router
    advanced filtering, 643
    simple filtering policy, 638–639
  single router access, 469
  spoofing attacks, 258
  unauthorized access, 242
    port scanning, 242–244
    reach ability check, 242
  working group, standard publications, 612
Internet Assigned Numbers Authority (IANA), 141, 629–634
Internet Control Message Protocol, 244, 265, 450
Internet Engineering Task Force (IETF), 140, 213
Internet Key Exchange. *See* IKE 229, 276, 469, 548
Internet Protocol, 258
Internet Relay Chat (IRC), 370, 465
Internet Routing Architectures, 234, 327
Internet Security Association and Key Management Protocol, 86
Internet service provider, 61, 244
Internet telephone service providers, 598
Internet Worm, 356
Internetwork Packet Exchange (IPX), 144
Inter-Switch Link, 329
Interzone ClearToken, 598
intranets, VPNs, 136, 150–151
intruders, 241
intrusion detection systems, 244, 309, 323, 345, 447
  corporate networks, 431–432
    Cisco IOS, 432–433
    PIX firewall, 433–434
  embedding within switch, 362
  selection, 365
invariance weaknesses, 281
inventories, network assets, 296
investigations, incidents, 616–623
INVITE, SIP signaling message type, 189
IOS routers, sample configuration, 490
IP (Internet Protocol), 258
  addresses, 324
    DDoS attacks, characteristics, 634
    firewalls, 337
    peer identification, 143
    RIP routing database, 214
    tracking spoofed addresses, 656, 662
    unicast, 324
  extended ACLs, 451–455
  firewalls, private *versus* public addresses, 472–474

header format, 259
protocol suite, 50–51, 139, 259
routing, 259
standard ACLs, 449–450
telephony devices, 178
tunnel, PPTP link-layer security, 112–113
vulnerabilities, 258–260
land.c attack, 264
sequence number attack, 261–263
session hijacking, 263
TCP SYN attack, 263–264
three-way handshake connection, 260– 261
ip accounting access-violations commands, 428
ip audit commands, 433
ip auth-proxy commands, 584
ip cef commands, 657
ip cef distributed commands, 657
ip inspect name commands, 477
ip permit commands, 439
ip route-cache flow commands, 658
IP Security. *See* IPsec
ip trigger-authentication commands, 584
IP unicast reverse-path forwarding (uRPF), 645
IPsec (IP Security), 85, 276
authentication, 467–468
encrypted traffic, 467–471
multiplexing data streams, 142
protocol suite, 85–86
authentication, 86–91
cryptographic keys, 92, 107
encryption, 86–91
SA, 91–92
routing protocols, 213
security management, 345
SIP protocol, 199–200
uses through firewall, 468
virtual dial-in access encryption, 548, 554
VPNs tunneling protocol, 139–141
L2TP combination, 145–146
NAT/PAT, 141–143
IPv4, special use address blocks, 634
IPv6, OSPF, 228
authentication, 228
authentication algorithm, 229
confidentiality, 228
encryption algorithm, 229
key management, 229
replay protection, 229
RIPng, 220
IPX (Internetwork Packet Exchange), 144
IRC (Internet Relay Chat), 370, 465
IS department (information systems department), 294
ISAKMP (Internet Security Association and Key Management Protocol), 86, 548
ISDN (Integrated Services Digital Network), 241
ISDN BRI/PRI, MTUs, 266
isdn commands, Cisco IOS privilege access, 381
IS-IS (Intermediate System-to-Intermediate System), 209, 229–231, 411
authentication, 231–232
cryptographic, 232–233
simple password, 232
ISL (Inter-Switch Link), 329
ISP (Internet service provider), 61, 244
iteration counts, 39
ITSPs (Internet telephone service providers), 598
ITU (International Telecommunications Union), 180
IVs (initialization vector), 8, 166, 281
IZCT (Interzone ClearToken), 598

J

Java
applets
application content filtering, 461–462
block encapsulated, 462
CBAC inspection, 477
inspections, ACLs, 478
jumphosts, 331
Jupiter Media Metrix, 358

K

KDCs (key distribution center), 23, 63–64
distributing keys, 24
KEA (Key Exchange Algorithm), 70
Kerberized, Kerberos protocol, 63
Kerberos
authentication, 580
identity, 64
protocol, 63, 463
application request and response, 66–67
considerations if using, 68
credential reuse, 67–68
realm, 64
request and reply, 64–66
sever, 64
terminology, 63–64
key agreement, CEK encryption, 75
key distribution centers, 23, 63–64
Key Exchange Algorithm (KEA), 70
key generation, PKI function, 122
key pair recovery, PKI function, 122
Key Scheduling Algorithm, 280
key transports, CEK encryption, 75
key updates, PKI function, 123
keyinit commands, 41
keys
cryptographic IPsec protocol suite, 92, 107
cryptography, 5–6
escrow, 5, 31
business needs, 31
human element, 32
U.S. government policies, 31–32

management, 23
creating public keys, 27–31
creating secret keys, 23–27
distributing public keys, 27–31
distributing secret keys, 23–27
OSPF, 229
preshared, VPN vulnerabilities, 277
shared, VPN vulnerabilities, 277
key-signing parties, 28
keyspaces, 6
keywords
established, 455–456
group, 386, 399
h323, 605
primary, 391, 421
remote, 391
syslog, 605
voip, 605
kill commands, PIX firewall privilege access, 393
Koblas, David (SOCKS developer), 83
Koblas, Michelle (SOCKS developer), 83
krb5 methods, AAA authentication, 399, 512
krb5-instance methods, AAA authorization, 518
krb5-telnet
AAA authentication, 512
methods
AAA authentication, 399
services, 513
KSA (Key Scheduling Algorithm), 280

L

L2F protocol (Layer 2 Forwarding protocol), 107–109
L2TP (Layer 2 Tunneling Protocol), 113, 139, 276
header format, 115–116
IPsec, 554, 572
link-layer security, 113–114
overview, 114–118
sample scenario, 118–120
network server, 114
VPNs tunneling protocol, 144–145
IPsec combination, 145–146
L2TP access concentrator (LAC), 114, 144
L2TPv2, 145
L2TPv3, 145
LAC (L2TP access concentrator), 114, 144
land.c attacks, 253, 264
LANs
ad hoc wireless, 278
relative risk calculation, 301
wireless, interference considerations, 280
lat commands, Cisco IOS privilege access, 381
Law Enforcement Access Field (LEAF), 71
laws, 624–625
Layer 2 Forwarding protocol, 107
Layer 2 Tunneling Protocol. *See* L2TP
Layer 3 switching (routing), 327
LCF (location confirmation), 598
lconfiguration, metro Ethernet, 243–255, 259–273, 280–283, 315–328, 335–336, 378, 403, 409, 412–418, 426, 501
LCP (Link Control Protocol), 45
LDAP (Lightweight Directory Access Protocol), 128
PKI certificate distribution, 128–129
protocol, IANA-assigned ports, 82
LEAF (Law Enforcement Access Field), 71
LEAP (Light Extensible Authentication Protocol), 176, 248
legal authorities, standard of conduct sample, 293
legal processes, incidents, 618
legalities, audits, 350
Light Extensible Authentication Protocol (LEAP), 248
Lightweight Directory Access Protocol, 128
line access controls, 395–396
Cisco IOS
auxiliary ports, 400–401
console ports, 396–400
virtual terminal ports, 401
Cisco PIX firewall, 402–405
Cisco switches, 401–402
HTTP security, 406
Cisco IOS devices, 406–408
Cisco PIX firewall, 408
SNMP security, 405–406
line methods
AAA authentication, 399, 512
services, 512
Link Control Protocol, 45
link-layer, security technologies, 107
L2F protocol, 107–109
L2TP protocol, 113, 120
PPPoE, 120–121
PPTP, 110–113
link-state databases, 224–229
link-state packets, 230
listings
AAA login authentication method, 386
assigning commands to different privilege levels, 387
authenticated SSH access to PIX firewall, 404– 405
authentication and authorization profiles on TACACS+ server, 534–536
authentication and authorization with RADIUS, 519–520
automated double authentication configuration file, 537–539
auxiliary port, 401
branch router configuration, 508–509
advanced filtering, 641
simple filtering policy, 637
branch router configuration commands, 540–542
Catalyst switch security template, 439–441
Cisco IOS IDS configuration, 433
Cisco router security template, 436–439
CiscoSecure server syntax, 520–521

configuration for EIGRP route authentication, 411
configuring for route filtering, 414
configuring console access, 398–399
configuring local use login database, 398
configuring locally defined enable password, 391
configuring multiple TACACS+ or RADIUS servers, 386
configuring PIX Telnet password, 403
configuring privilege levels, 387
console connection authentication, 400
corporate access router configuration, 504–508
double-authentication configuration on Cisco NAS, 534
enable password and enable secret command options, 384
enable password encrypted, 394
enable secret and enable password configuration file, 385
enable? command output, 383
Estonia remote branch router configuration, 543–548
Home Gateway router configuration, 556–562
ICMP traffic rate limiting configuration, 644
Internet router configuration
  advanced filtering, 643
  simple filtering policy, 638
IPsec branch router configuration, 552–554
ISP NAS configuration, 556–572
lock and key configuration, 529
lock and key using AAA, 530–531
lock and key with multiple access privileges, 532
NAS router configuration
  advanced filtering, 642
  simple filtering policy, 637
NAS server configuration, 524–525
PIX firewall privilege access, 395
PIX firewall security template, 441–442
PIX IDS configuration, 434
port security on catalyst switch, 410
PPP authentication using RADIUS, 514–515
PPP authentication using TACACS+, 514
primary router HSRP configuration, 417
remote branch router in New York configuration, 556–571
remote branch router in Toronto configuration, 556–567
restricted Telnet access using AAA, 404
restricting vty access to Cisco IOS routers, 401
securing HTTP access in Cisco IOS software, 408
setting up console access, 397
setting up password for console access, 398
setting up privilege level for specific commands, 395
standby router HSRP configuration, 417
switch with SSH access, 402
Syslog logging and accurate time stamps using NTP
  Catalyst switch, 430
  Cisco IOS router, 429–430
  PIX firewall, 430–431
TACACS+ server configuration, 524–532
TACACS+ switch privilege access mode authentication and authorization, 392
TCP SYN traffic rate limiting configuration, 645
uRPF configuration, 646
Vancouver home gateway configuration, 543–545
LNS (L2TP network server), 114
local controls, authentication methods, 38
local methods
  AAA authentication, 399, 512
  AAA authorization, 518
  services, 512
locations
  confirmation, 598
  physical device security, 319–320
  request, 598
lock and key feature (Cisco IOS Software), 526
  access operation, 526–528
  authentication, 526
  branch router access, 530–532
  multiple access privileges, 532
  telecommuter access, 528–530
lock commands, Cisco IOS privilege access, 381
Lockmanager protocol, 465
log files, security, 309
logging, corporate networks, 427–428
  Syslog managment, 428–431
logical securities, 307–308
  access controls, 330–331
    authentication, 331–333
    greeting messages, 333
    passwords, 331
    users, 333
  controls, 322–323
  sample policy, 334
  subnet boundaries, 324–327
    routing, 327–329
    VLAN, 329–330
login
  authentication commands, 399
  modes (basic access mode), 379
  services, AAA authentication, 511
login commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
  lock and key authentication, 526
log-input, tracing DDoS attacks, 648–650
log-input commands, 424
log-input parameters, 451
logout commands
  AAA authorization, 387
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
logs, tracking incidents, 360
look commands, Cisco IOS basic access, 380
Lotus Notes protocol, 464

LRQ (location request), 598
LSPs (link-state packets), 230
Lucifer algorithm, 9

M

MAC
- Media Access Control, 279
- message authentication code, 76

magnetic fields, protection, 322
mail, protocol, 464
main campus infrastructure, enterprise network components, 305
management
- risks, 343
- site security policies, 344–345

managers, incident response guidelines, 622
man-in-the-middle attacks, 17, 278
- Diffie-Hellman algorithm, 26
- impersonation, 250

MANs, 243– 273, 280–283, 315–328, 335– 336, 378, 403, 409–418, 426, 501
mapping, networks, 343
market timing, 304
market trends, data classification, 297
Martin, Janice, 257
masks
- network, 325
- subnet, 326

Massachusetts Institute of Technology (MIT), 63
master keys, 140
mathematical functions, cryptography, 6
maximum transmission units (MTUs), 265, 589, 647
MCU (multipoint control unit), H.323 standard components, 181
MD4 algorithm (Message Digest 4 algorithm), 17
MD5 (Message Digest 5), 210
- authentication, 211–213, 217
- CHAP one-way hash function, 51

MD5 algorithm (Message Digest 5 algorithm), 17
md5 option, hash algorithm, 549
MD5-Challenge type, EAP packet format, 52
media encryptors, FORTEZZA protocol, 71
Media Access Control, 279
media access controls, 802.11, 160–162
Media Gateway Control Protocol. *See* MGCP
media gateway controllers (MGCs), 187
media gateways (MGs), 187
Melissa virus, 356
message authentication code, 76
message digest (hash), 16, 211
Message Digest 4 algorithm (MD4 algorithm), 17
Message Digest 5 algorithm (MD5 algorithm), 17, 210
message format S/MIME communication, 76
Message Integrity Check (MIC), 171, 594
messages, coded, 5
method lists
- authentication, 511–514
- linking to interface, 514–515
- linking to line, 514–515

methods
- AAA authentication, 399
- authentication, 21

metric (hop count), 214
MGCP (Media Gateway Control Protocol), 186, 602
- binding gateway interfaces, 602
- VoIP network protocols, 186–187

MGCs (media gateway controllers), 187
MGs (media gateways), 187
MIC (message integrity check), 171
- TKIP protocol, 172

microcode commands, Cisco IOS privilege access, 382
Microsoft Challenge Handshake Protocol (MS- CHAP), 144
Microsoft Pint-to-Point Compression Protocol (MPPC protocol), 143
Microsoft Point-to-Point Encryption Protocol (MPPE protocol), 143
Mirkovic, Jelena, 257
mirror ports, intrusion detection system, 362
MISSI (Multilevel Information Systems Security Initiative), 69, 71
MIT (Massachusetts Institute of Technology), 63
mitigations, risk, 302–304
Mitnick, Kevin, incidents website, 356
Mobile IP, 163–164
ModeConfig (Mode Configuration), 140
modems, scanners, 247
modemui commands, Cisco IOS privilege access, 380–382
modulus operators, 26
monitor commands, Cisco IOS privilege access, 382
monitor ports, intrusion detection system, 362
monitoring
- corporate networks, 427–431
- security policy, 343
  - accounting, 344
  - intrusion detection, 345, 347
  - sample policy, 347
  - secure management, 344–345
  - vulnerability scanners, 343

more commands, Cisco IOS privilege access, 382
Mountd protocol, 465
MPLS (Multiprotocol Label Switching), 575
MPLS and VPN Architectures, Volume II, 575
mpoa commands, Cisco IOS privilege access, 382
MPPC protocol (Microsoft Pint-to-Point Compression Protocol), 143
MPPE protocol (Microsoft Point-to-Point Encryption Protocol), 143
mrinfo commands
- Cisco IOS basic access, 380
- Cisco IOS privilege access, 382

mrm commands, Cisco IOS privilege access, 382
MS-CHAP, 51 (Microsoft Challenge Handshake Protocol), 144
MS-CHAPv2, 51
mstat commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 382
mtrace commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 382
MTUs (maximum transmission unit), 265–266, 589, 647
multicast discovery, H.323 call-signaling flow, 184
Multilevel Information Systems Security Initiative (MISSI), 69, 71
Multiple Default IP Gateways feature, 421
multiplexing, IPsec data streams, 142
multipoint control units (MCU), 181
Multiprotocol Label Switching, 575

N

Nak type, EAP packet format, 52
name-connection commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 382
named ACLs, 456
namespaces, authentication, 22–23
NAS (network access server), 510
    PPTP link-layer security, 111
    Reverse Telnet, 517
    routers
        advanced filtering, 641–642
        simple filtering policy, 637–638
NASA WANK (Worms Against Nuclear Killers), 356
nasi service, AAA authentication, 511
NAT (Network Address Translation), 90, 141, 342, 472, 576
    firewalls, 472
        functionality, 474–475
        private versus public addresses, 472, 474
    IPsec tunneling protocol, 141–143
    PIX firewall, 487
    routers, 474
    Traversal, 142–143
nat commands, 487
National Information Infrastructure (NII), 69
National Institute of Standards and Technology (NIST), 9
National Security Agency (NSA), 9, 69
natural disaster protection, 322
natural mask, 487
NBT protocol, 465
ncia commands, Cisco IOS privilege access, 382
NCPs (Network Control Protocols), 45
need-to-know policies, 303–304
neighbor discovery/recovery mechanism, 221
neighbor tables, EIGRP routing concepts, 222
NetFlow v1.0, monitoring DoS attacks, 651–656
netmasks, 487
NetMeeting protocol, 463
network access server. *See* NAS
Network Address Translation. *See* NAT
Network Control Protocols, 45
network events, AAA accounting, 522
Network File System. *See* NFS
network IDS, 345
Network Information Service. *See* NIS
network interface cards. *See* NICs
network intrusion detection system. *See* NIDS
network layers, security protocols, 85, 107
network masks, 325
Network News Transfer Protocol. *See* NNTP
Network service type, AAA authorization, 516
Network Time Protocol, 412, 465
network topology, spoofed IP addresses, 658–659
networks
    assets, 295–296
    corporate networks, 377
    documents on security, 612
    edge, 306
    enterprise, 242
    importance, 301
    incidents, 618–619
    Internet, access architecture, 445–447
    mapping, 343
    OOB management, 344
    physical infrastructure, security controls, 314–319
    routing, basics, 207–213
    routing protocols, vulnerabilities, 287–288
    screen router, architecture, 459
    security resources, 611
    services, infrastructure integrity, 337–339
    switched, intrusion detection system, 361–363
    VoIP networks, 177
        deployment models, 178–179
        IP telephony components, 178
        protocols, 180, 193
        security protocols, 193, 200
        security solutions, 200–202
        security technologies, 597–605
        vulnerabilities, 283–287
    VPNs, 135
        deployment models, 135–139
        security, 139, 148
        security application, 148–151
        security technologies, 575–591
        vulnerabilities, 276–277
    wireless, 248
        security technologies, 592–596
        vulnerabilities, 278–282
    WLANs, 151
        components, 153
        deployment models, 153–154
        security, 165, 177

spread-spectrum radio technology, 156, 164
wireless technology types, 151–152
new product features, data classification, 297
Newsham, Timothy N., “Insertion, Evasion, and Denial of Service Eluding Network Intrusion Detection,” 364
newtear.c attack, 267
NFS (Network File System), 466
protocol, 466
vulnerabilities, 275
NICs (network interface cards), 280, 459
WLANs component, 153
NIDS (network intrusion detection system), 345, 361
intrusion detection system
attack limitations, 364
bypass, 364
NII (National Information Infrastructure), 69
Nimda virus, 357
NIS (Network Information Service), 275, 466
protocol, 466
vulnerabilities, 275
NIST (National Institute of Standards and Technology), 9
NNTP (Network News Transfer Protocol), 271
IANA-assigned ports, 82
protocol, 463
vulnerabilities, 271
no access-list commands, 450
no commands, Cisco IOS privilege access, 382
no exec commands, 400
no failover active commands, 422
no failover commands, 422
no ip directed-broadcast commands, 425
none commands, 391
none keywords
AAA accounting, 523
authentication, 515
none methods
AAA authentication, 399, 512
AAA authorization, 518
services, 512
none option, 401
nonrepudiation, asymmetric encryption, 14–15
nonvolatile random-access memory, 385
notification type, EAP packet format, 52
notoriety, attack motivation, 258
NSA (National Security Agency), 9, 69
NTP (Network Time Protocol), 412, 465
null authentication, OSPF, 226
NVRAM (nonvolatile random-access memory), 385

O

object identifiers authentication, 22–23
OFB (Output Feed Back), 7
OFDM (orthogonal frequency-division multiplexing), 158–160
One-Time Passwords, 41, 52
one-way hash function, 16–17
ONS, metropolitan Ethernet, 243–273, 280–283, 315–336, 378, 403, 409–418, 426, 501–504, 524–530, 542, 551–555, 636–639, 659
ONS 15454/15327 optical platforms
MANs selection, 243–283, 315–336, 378, 403, 409–418, 426, 501
OOB management, 344
Open Shortest Past First. *See* OSPF
Open Software Foundation website, 69
operators, modulus, 26
optical fiber cables, 314
optical splitters, 315
optical time domain reflectometer tool, 314
option negotiations, SHTTP protocol, 73
OPTIONS, SIP signaling message type, 189
ORAs (Organizational registration authorities), 122
orthogonal frequency-division multiplexing (OFDM), 158
OSPF (Open Shortest Past First), 209, 224–225, 411, 548
authentication, 225
cryptographic, 226–228
null, 226
simple password, 226
IPv6, 228
authentication, 228
authentication algorithm, 229
confidentiality, 228
encryption algorithm, 229
key management, 229
replay protection, 229
packet header, 225
OTDR tool (optical time domain reflectometer tool), 314
OTP (One-Time Password), EAP packet format, 52
outbound commands, 488
outbound traffic, 336
outgoing_dest options, apply commands, 488
outgoing_src option, apply commands, 488
out-of-band management, 344
Output Feed Back, 7
outside interfaces, 403

P

PAC (PPTP access concentrator), 111
packets
advanced session filtering, 460
TCP protocol traffic, 460
UDP protocol traffic, 461
checksums, 340
DDoS attack, capture packet samples, 647
decoders, 24
DoS attacks, 633
EIGRP, 223–224
filtering, 336

  - ICMP, 265, 644
  - PPTP IP tunneling, 112–113
  - session filtering, CBAC, 476–479
  - sniffing, 318
    - tracking incidents, 360
  - snooping, 244
    - unauthorized access, 244–245
  - spoofed corporate networks, 423–424
  - spoofing, 250
  - TCP SYN, rate limiting, 644–645
- pad commands, Cisco IOS basic access, 380
- PAN (personal-area network), 152
- PAP (Password Authentication Protocol), 45, 579
  - PPP protocol, 47–48
  - simple corporate environment authentication, 504
  - strengths, 54
  - weaknesses, 54
- passive interface commands, 414
- passive mode FTP, 273
- passive states, EIGRP routing concepts, 223
- Password Authentication Protocol. *See* PAP
- password commands, lock and key authentication, 393, 403, 526
  - passwords, 39
  - CEK encryption, 75
  - Cisco IOS privilege access mode, 384–385
  - logical security controls, 331–333
  - protocol enforcement, 333
  - S/Key One-Time Password System, 39–41
  - security architecture, 307
  - selection guidelines, 332
  - statically configured, 579
  - token authentication systems, 42–44
- PAT (Port Address Translation), 141–143, 582
- Paxon, Vern, Bro, “A System for Detecting Network Intruders in Real-Time,” 364
- PBX (private branch exchange), 246
- PDUs (protocol data units), 45, 111
- PEAP (Protected Extensible Authentication Protocol), 176–177, 248, 593
- peer-to-peer WLAN, 153–154
- PEM (privacy-enhanced mail), 125
- people, network assets, 296
- per call authentication, 598
- perimeter security, 307
- permissions, 20
- permit commands, 456
- permit keyword, 550
- per-packet key mixing, TKIP protocol, 171
- personal identification code, 306
- personal identification number, 42
- personal-area network (PAN), 152
- personnel, 309–310, 350
- PGP (Pretty Good Privacy), 197, 271
- phones, SIP client, 188
- physical device security
  - access, 320–321
  - environmental safeguards, 321–322
  - location, 319–320
- physical network infrastructures, security controls, 314
  - cable selection, 314–318
  - topography, 318–319
- physical security, 308
  - controls, 314
  - device security
    - access, 320–321
    - environmental safeguards, 321–322
    - location, 319–320
  - network infrastructure, 314
    - cable selection, 314–318
    - topography, 318–319
  - sample policy, 322
- physical site surveys, performing, 243–273, 280–283, 315–328, 335– 336, 378, 403, 409–418, 426, 501–504, 524–530, 542, 551–555, 636–639, 659
- PIN (personal identification number), 42, 306
- ping commands, 242
  - Cisco IOS basic access, 380
  - Cisco IOS privilege access, 382
  - Cisco switch privilege access, 390
  - Cisco switches basic access, 389
  - PIX firewall privilege access, 393
- Ping of Death attacks, 253, 266–267
- ping sweeps, 244
- pirated music, 355
- pirated software, 355
- PIX (Private Internet Exchange), 393, 485
  - firewall, 485–486
    - advanced features, 490
    - basic access mode, 393–395
    - Cut-Thur-Proxy feature, 488–490
    - HTTP security, 408
    - inbound access, 486–487
    - intrusion detection, 433–434
    - line access controls, 402–405
    - network availability, 421–423
    - outbound access, 488
    - privilege access modes, 393–395
    - sample configuration, 490
  - security levels, 486
- pixfirewall# ? commands, PIX firewall privilege access, 393
- pixfirewall>? commands, PIX firewall basic access, 393
- PKCS (Public Key Cryptography Standards), 74
- PKI (Public Key Infrastructure), 121–122, 235, 579
  - certificate distribution, 128–129
  - certificates, 124–125
  - functions, 122–123
  - sample scenario, 123–124
  - X.509 standard, 125
    - X.509v2 CRL, 127–128
    - X.509v3 certificate, 126
- plain old telephone service (POTS), 503
- plaintext authentication, 211, 216–217
- PNS (PPTP network server), 111

- Pointcast by Pointcast protocol, 463
- Point-to-Point MTUs, 266
- point-to-point architecture, 243–273, 280–283, 315–336, 378, 403, 409–418, 426, 501–504, 524–530, 542, 551–555, 636–639, 659
- Point-to-Point Protocol. *See* PPP
- Point-to-Point Tunneling Protocol. *See* PPTP
- policies
  - acceptable use, 355
  - California state laws, 624–625
  - documents on network security, 612
  - Internet firewall, 445
  - Internet standard publications, 612
  - need-to-know, 303–304
  - security, 309
    - corporate standard of conduct sample, 292–294
    - enterprise network components, 304–306
    - personnel, 309–310
    - risk management, 295, 304
    - security architecture, 306–309
  - simple filtering, 636
    - branch routers, 636–637
    - Internet router, 638–639
    - NAS router, 637–638
  - site security
    - awareness training, 351–352
    - data confidentiality, 342–343
    - data integrity, 335, 342
    - infrastructure, 335, 342
    - logical security controls, 322, 334
    - monitoring, 343–347
    - network administrators, 347–351
    - physical security controls, 314, 322
    - verification, 343–347
  - U.S. Section 1832, Theft of Trade Secrets, 625
  - validation, 343
  - wireless network, 279
- POP (Post Office Protocol), 464
- POP3 protocol, IANA-assigned ports, 82
- Port Address Translation (PAT), 141, 582
- portable tools, network administrator security policy, 348
- ports
  - auxiliary, 400–401
  - console, 396–400
  - Ethernet switches, 245
  - IANA (Internet Assigned Numbers Authority), 629–630
  - NAT, 475
  - numbers, firewalls, 337
  - scanning, 242–244
  - security, 409
  - TCP protocol numbers, 451
  - UDP protocol numbers, 452
  - virtual terminal, 401
- Post Office Protocol, 464
- POTS (plain old telephone service), 503
- PPP (Point-to-Point Protocol), 45, 503
  - authentication protocols, 45–46
    - CHAP, 48–51
    - EAP, 51–54
    - PAP, 47–48
    - summary, 54
  - frame format, 45–46
  - link layer, 45
  - negotiations, 46
  - *versus* IKE authentication, 147
  - *versus* SLIP, 503
- ppp commands
  - Cisco IOS basic access, 380
  - Cisco IOS privilege access, 382
- PPP over Ethernet. *See* PPPoE
- ppp services, AAA authentication, 511
- PPPoE (PPP over Ethernet), 120
  - frame format, 121
  - link-layer security overview, 120–121
- PPTP (Point-to-Point Tunneling Protocol), 139
  - link-layer security
    - NAS functionality, 111
    - overview, 111–113
  - VPNs tunneling protocol, 143–144
- PPTP access concentrator (PAC), 111
- PPTP network server (PNS), 111
- pranks, attack motivation, 258
- pre-share option, authentication, 549
- preshared keys, VPN vulnerabilities, 277
- Pretty Good Privacy (PGP), 197, 271
- preventative controls, logical security, 330
- primary keyword, 391, 421
- prime numbers, 27
- principal, Kerberos protocol, 64
- priori authentication, 20
- privacy, SIP-based networks, 287
- privacy-enhanced mail (PEM), 125
- private branch exchange, 246
- private hosts, 473
- Private Internet Exchange. *See* PIX
- private IP addresses, firewalls, 472–474
- private keys, key escrow, 31
  - business needs, 31
  - human element, 32
  - U.S. government policies, 31–32
- privilege access modes (enable mode), 379
  - Cisco IOS devices, 379–383
    - AAA authentication, 385–386
    - multiple privilege levels, 386–389
    - passwords, 384–385
  - Cisco PIX firewall, 393–395
    - multiple privilege levels, 395
  - Cisco switches, 389–392
- privilege level commands, 387
- privilege ticket-granting ticket (PTGT), 69
- procedures
  - network administrator security policy
    - audits, 348–350
    - backups, 347–348

equipment certification, 348
portable tools, 348
network administrator site security policies and procedures, sample policy, 350–351
professional responsibilities, standard of conduct sample, 293
proprietary data, asset value, 297
Protected Extensible Authentication Protocol (PEAP), 176, 248, 593
protecting materials, 620–622
protocol data units (PDUs), 45, 111
protocols
common applications, 463–466
infrastructure integrity, 337–339
routing, 208–210
authentication, 210–213
BGP-4, 234–236
EGP, 209
EIGRP, 221–224
IGP, 209
IPSec, 213
IS-IS, 229–233
OSPF, 224–229
RIP, 213, 220
VoIP networks, 180
H.323 standard, 180
H.323 standard components, 180–186
MGCP, 186–187
SIP, 187, 193
vulnerabilities, 258
DNS, 268–271
FTP, 272–273
ICMP, 265–268
NFS service, 275
NIS service, 275
NNTP, 271
SMTP, 271–272
TCP/IP, 258, 264
UDP, 264–265
X Window System, 275
provisional codes, 189
proxies, 264
proxy servers, SIP servers, 189
proxy-authorization header, 197
pseudo_pad, TACACS+ protocol, 58
PSH flag, TCP, 260
PSTNs (Public Switched Telephone Networks), 246, 501
Ptacek, Thomas H., "Insertion, Evasion, and Denial Of Service Eluding Network Intrusion Detection," 364
PTGT (privilege ticket-granting ticket), 69
public hosts, 473
public IP addresses, firewalls, 472–474
Public Key Cryptography Standards, 74
public keys
certificates, 124
creating, 27–28
certificate authorities, 29–31
digital certificates, 28–29
distributing, 27–28
certificate authorities, 29–31
digital certificates, 28–29
encryption, 11, 579
infrastructure, 121, 235, 579. *See also* PKI
Public Switched Telephone Networks, 246–501
publications
Cisco Secure PIX Firewalls, 490
cryptography resources, 611
The Cuckoo's Egg, 348
documents on network policies, 612
firewall resources, 611
Firewalls and Internet Security, 258
instrusion detection resources, 611
Internet Routing Architectures, 234, 327
Internet standards, 612
network security resources, 611
Repelling the Wily Hacker, 258
The Site Security Handbook, 291
pwd commands, Cisco IOS privilege access, 382

Q

Q.931 standard, H.323 call setup security, 194
qualitative risks, 300
quantitative risks, 299
queries, DNS, 269
query packets, EIGRP, 224
quit commands
Cisco switch privilege access, 390
Cisco switches basic access, 389
PIX firewall basic access, 393
PIX firewall privilege access, 393

R

radio commands
Cisco IOS basic access, 380
Cisco IOS privilege access, 382
RADIUS, 510
authentication, 510–511
method list, 511–515
authorization, 516
CiscoSecure server syntax, 520–521
methods, 517–520
service types, 516–517
EAP, 54
methods
AAA accounting, 523
AAA authentication, 399, 512
AAA authorization, 518
services, 513
protocol, 60, 464
accounting, 61
authentication, 61
authorization, 61
encryption, 62
transactions, 61–62

radius-server commands, PIX firewall privilege access, 393
random hosts, attacks behind firewall, 340
random network interloping, incident violation, 371–372
RAS, signaling authentication, 193–194, 465
rate limiting, DDoS attacks, 633–634, 644
  ICMP packets, 644
  preventive measures, 644
  TCP SYN packets, 644–645
RC-4 (Rivest Cipher 4), 9–10
RDN (relative distinguished name), 129
reachability checks, Internet unauthorized access, 242
read-only (ro) options, 406
read-write (rw) options, 406
RealAudio protocol, CBAC inspection, 477
Real-Time Control Protocol (RTCP), 183
Real-Time Transport Protocol (RTP), 183
recomputations, 223
reconfirm commands, Cisco switch privilege access, 390
reconnaissance, port scanning, 242–244
record protocol, SSL, 79
redirect servers, SIP servers, 189
redundancy, network availability, 416
  Cisco IOS, 416–417
  Cisco PIX firewall, 421–423
  Cisco switches, 418–421
  reflexive ACLs, 456–459
REGISTER, SIP signaling message type, 189
registrar service, SIP server, 189
registration
  PKI function, 122
  requests, 598
Reicher, Peter, 257
relative distinguished name (RDN), 129
relatively prime numbers, 27
RelAudio protocol, 463
Reliable Transport Protocol, 221
reload commands
  Cisco IOS privilege access, 382
  PIX firewall privilege access, 393
RelVideo protocol, 463
remote accesses, 305, 328
remote dial-in accesses, unauthorized, 246–247
remote keyword, 391
remote procedure call services, protocol, 466
rename commands, Cisco IOS privilege access, 382
Repelling the Wily Hacker, 258
replacement values, assets, 296
replay attacks, 39, 250, 340
replay protection, OSPF, 229
reply packets, EIGRP, 224
reporting
  incident handling, 367–369
  rewards, 622
reporting incidents, 616
Request for Comments (RFCs), 46
research data, asset value, 297
reset commands, Cisco switch privilege acc, ss, 390
Resource Manager Essentials, 596
resources
  configuring WEP, 594
  cryptography, 611
  firewall resources, 611
  IEEE 802.1x port-based authentication on Catalyst switches, 584
  intrusion detection, 611
  IPsec and L2TP/IPsec scenarios, 589
  L2TP authentication with RADIUS, 583
  NAT VPN environments, 582
  network security, 611
  PEAP on the Aironet 1200 series, 593
  PEAP on the Aironet 350 series, 593
  risk assessment availability, 299
  user authentication based on Xauth, 583–584
  VPN device authentication, 580–581
response teams, incidents, 358
  core team, 359
  guidelines, 615
    documents, 621
    employees, 619–620
    investigations, 616–623
    legal processes, 618
    managers, 622
    networks, 618–619
    protecting materials, 620–622
    reporting, 622
    reports, 616
    security policies, 617–618
resume commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
revenge, attack motivation, 258
Reverse Telnet, port accessibility, 517
Reverse-Access service type, AAA authorization, 516
revocation, PKI function, 123
Rexec protocol, 465
RFCs (Request for Comments), 46
  RFC 1058, 214
  RFC 1195, 229
  RFC 1321, 218
  RFC 1422, 125
  RFC 1723, 216
  RFC 1760, 39
  RFC 1771, 234
  RFC 1918, 342, 634–638
  RFC 1928, 84
  RFC 1962, 143
  RFC 1968, 143
  RFC 1994, 51
  RFC 2002, 163
  RFC 2080, 220
  RFC 2082, 216
  RFC 2118, 143
  RFC 2196, 367
  RFC 2315, 75
  RFC 2328, 224

  RFC 2385, 234
  RFC 2401, 85
  RFC 2402, 86
  RFC 2406, 86
  RFC 2408, 86
  RFC 2631, 74
  RFC 2632, 74
  RFC 2633, 74
  RFC 2634, 74
  RFC 2637, 110
  RFC 2716, 175
  RFC 2827, 635
  RFC 3078, 143
  RFC 3193, 145
  RFC 3369, 74
  RFC 3370, 74
  RFC 3377, 128
Rice University website, 281
Rijmen, Dr. Vincent (Rijndael algorithm developer), 10
Rijndael algorithm, 10
RIP (Routing Information Protocol), 209–215, 251
  authentication, 216
    cryptographic, 217–220
    plaintext, 216–217
  packet format, 215
    MD5, 217
  RIPng, 220
RIPng, 220
RIPv2 (Routing Information Protocol version 2), 411
  RIPng, 220
risk assessments, 295. *See also* risks
  evaluations, 299–302
  network assets, 295–296
  threats, 297–298
    data compromises, 298
    data integrity, 298–299
    resource unavailability, 299
  value of assets, 296–297
  vulnerability, 297–298
    data compromises, 298
    data integrity, 298–299
    resource unavailability, 299
risks. *See also* risk assessments
  analysis tools, 300
  assessment procedure, 342
  calculation, 300
  management, site security policy, 295, 343
    risk assessment, 295, 302
    risk mitigation, 302–304
  mitigations, 302–304
Rivest Cipher 4, 9
Rivest, Ron, RC-4 inventor, 10
rlogin commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 382
Rlogin protocol, 465
RME (Resource Manager Essentials), 596
Ron Rivest, Adi Shamir, and Leonard Adleman algorithm (RSA algorithm), 15
route authentication, 210, 410
Route Switch Processor (RSP), 651
Router#? commands, Cisco IOS privilege access, 381
Router>? commands, Cisco IOS basic access, 379
routers, 207. *See also* routing
  branch
    advanced filtering, 640–641
    simple filtering policy, 636–637
  filtering, DDoS attacks, 633–634
  impersonation, 251–252
  Internet
    advanced filtering, 643
    simple filtering policy, 638–639
  NAS
    advanced filtering, 641–642
    simple filtering policy, 637–638
  NAT, 474
  RIP protocol, 214
  screening
    architecture, 459
    Internet access, 447
    sample configuration, 490
  single, Internet access, 469
  tracking spoofed IP addresses, 657–658
routing. *See also* routers
  authentication, 410–412
  basics, 207–208
    protocol classification, 208–209
    protocol security, 210–213
  boundaries, 327–329
  filters, 412–414
  gatekeeper services, 181
  impersonation, 252
  Layer 3 switching, 327
  protocol vulnerabilities, 287–288
  protocols
    BGP-4, 234–236
    EIGRP, 221–224
    IS-IS, 229–233
    OSPF, 224–229
    RIP, 213–220
  updates, 339–340
Routing Information Protocol. *See* RIP
Routing Information Protocol version 2 (RIPv2), 411
RPC protocol, CBAC inspection, 477
RRQ (registration requests), 598
RSA algorithm (Ron Rivest, Adi Shamir, and Leonard Adleman algorithm), 15
rsa-encr option, authentication, 549
rsa-sig option, authentication, 549
rsh commands, Cisco IOS privilege access, 382
Rsh protocol, 465
RSP (Route Switch Processor), 651
RST flag, TCP, 260
Rstat protocol, 466
RTCP (Real-Time Control Protocol), 183
RTP (Real-Time Transport Protocol), 183, 221
  H.323 standard component, 183
rule-based analysis, intrusion detection system, 361
Rwall protocol, 466

S

S/Key One-Time Password System, 39–41
S/MIME (Secure Multipurpose Internet Mail Extensions), 73–77, 271
    SIP authentication, 198
    SIP-based networks, 285
S/MIMEv2, 74
SA (security association), 91–92
Sapphire worm (Slammer), 357
SAs (security associations), 86, 229
S-BGP (Secure BGP), 235
SBU data (sensitive-but-unclassified data), 70
SCP (Secure Copy Protocol), 273, 454
screening routers
    architecture, 447–448, 459
    Internet access, 447
    sample configuration, 490
sdlc commands, Cisco IOS privilege access, 382
secret keys
    creating, 23–27
    Diffie-Hellman algorithm, 25–27
    distributing, 23–27
    encryption, 6
    key escrow, 31
        business needs, 31
        human element, 32
        U.S. government policies, 31–32
Section 1832, Theft of Trade Secrets, 625
Secure BGP, 235
Secure Copy Protocol (SCP), 273, 454
Secure Hash Algorithm (SHA), 17
Secure HyperText Transport Protocol, 73
Secure ID protocol, 464
secure management, 344–345
Secure Multipurpose Internet Mail Extensions, 73
Secure Origin BGP, 236
Secure Real-Time Transport Protocol (sRTP), 200
Secure Shell (SSH), 83, 273
Secure Socket Layer, 345, 463
Secure Socket Layer /Transport Layer Security protocol, 78
security
    associations, 91, 229
    breach, 355
    Cisco product information, 613
    policies, 309
        awareness training, 351–352
        corporate standard of conduct sample, 292–294
        data confidentiality, 342–343
        data integrity, 335–342
        enterprise network components, 304–306
        guidelines, 617–618
        infrastructure, 335–342
        logical security controls, 322, 334
        monitoring, 343–347
        network administrators, 347–351
        personnel, 309–310
        physical security controls, 314, 322
        risk management, 295, 304
        security architecture, 306–309
        verification, 343–347
    protocol, 463–464
    sample survey questionnaire, 292–294
    standards publications, 612
    vulnerability assessment, 343
    websites, 613
security parameter index (SPI), 91
security policy database (SPD), 92
send commands, Cisco IOS privilege access, 382
sensitive-but-unclassified data (SBU data), 70
sequence numbers
    TCP connection, 261
    TCP/IP protocol attack, 261–263
Serial Line Internet Protocol. *See* SLIP
Series L Recommendations, 319
service credential, Kerberos protocol, 64
sdlc commands, Cisco IOS privilege access, 382
service password-encryption commands, 384
Service Set Identifiers, 248
services
    attacks, deterrents, 340
    networks, infrastructure integrity, 337–339
session commands
    Cisco switch privilege access, 390
    Cisco switches basic access, 389
    PIX firewall privilege access, 393
Session Initiation Protocol. *See* SIP
sessions, 23
    hijacking, TCP/IP protocol, 263
    keys, 140
set authentication login commands, 401
set commands
    Cisco switch privilege access, 390
    Cisco switches basic access, 389
    set enable commands, 439
    set enablepass commands, 391
    set help commands, 389–390
    set ip permit commands, 402
    set password commands, 439
    set spantree root commands, 421
setup commands, Cisco IOS privilege access, 382
SHA (Secure Hash Algorithm), 17
sha options, hash algorithm, 549
shadow copies, 129
shared key authentication, 170
shared keys, VPN vulnerabilities, 277
shared secret (authentication key), 210
Shared Wireless Access Protocol (SWAP), 152
Shipley, Peter, dialup modems, 247
shortest-path first, 224
shortest-path tree, 230
show commands, 387, 434
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 382

Cisco switch privilege access, 390
Cisco switches basic access, 389
show config commands, 388
show failover commands, 422
show failover lan commands, 422
show help commands, 389–390
show interfaces rate-limit commands, 645
show ip arp mac-address commands, 648
show ip cache flow commands, VIP console, 654
show line vty commands, 401
show privilege all commands, 393
show proc cpu commands, VIP console, 654
show proc cpu option, 651
show running-config commands, 387
show startup-config commands, 388
SHTTP protocol (Secure HyperText Transport Protocol), 73–74
signature algorithm, 126
S/MIME communication, 76
signatures, digital, 579
signed data content type, CMS, 75
silent processes, 215
simple filtering policies, 636
branch routers, 636–637
Internet router, 638–639
NAS router, 637–638
Simple Mail Transfer Protocol. *See* SMTP
Simple Network Auto Provisioning, 604
Simple Network Management Protocol. *See* SNMP
simple password authentication
IS-IS, 232
OSPF, 226
single router, Internet access, 469
single-site campus, VoIP deployment model, 178
SIP (Session Initiation Protocol), 187, 284
binding gateway interfaces, 602
firewall, 601–602
network vulnerabilities
HTTP Digest, 285
privacy, 287
S/MIME, 285
TLS, 286–287
VoIP network protocol, 187–188
components, 188–189
H.323 standard interaction, 192–193
operation, 189–192
VoIP network protocol security, 196–197
HTTP digest authentication, 197–198
IPsec, 199–200
network layer, 198–199
S/MIME authentication, 198
TLS, 199
transport, 198–199
The Site Security Handbook, 291
site security policies
corporate standard of conduct sample, 292–294
data confidentiality, 342–343
data integrity, 335
authenticated data, 339–340
common attack deterrents, 340–341
firewalls, 335–337
network services, 337–339
sample policy, 341–342
infrastructure, 335
authenticated data, 339–340
common attack deterrents, 340–341
firewalls, 335–337
network services, 337–339
sample policy, 341–342
logical security controls, 322–323
access controls, 330–333
sample policy, 334
subnet boundaries, 324, 330
monitoring, 343
accounting, 344
intrusion detection, 345, 347
sample policy, 347
secure management, 344–345
vulnerability scanners, 343
physical security controls, 314
device security, 319–322
network infrastructure, 314–319
sample policy, 322
risk management, 295
risk assessment, 295, 302
risk mitigation, 302–304
verification, 343
accounting, 344
intrusion detection, 347
intrusion detection system, 345
sample policy, 347
secure management, 344–345
vulnerability scanners, 343
site surveys, 243–273, 315–328, 378, 403, 409–418, 426, 501–504, 524–530, 542, s551–555, 636–639, 659
site-to-site VPNs, 137
Slammer (Sapphire worm), 357
SLIP (Serial Line Internet Protocol), 503
MTUs, 266
versus PPP, 503
slip commands
Cisco IOS basic access, 380
Cisco IOS privilege access, 382
Cisco switch privilege access, 390
SMTP (Simple Mail Transfer Protocol), 271, 462
advanced firewall architecture, 462
CBAC inspection, 477
protocol, 82, 464
vulnerabilities, 271
Smurf attacks, 253
ICMP, 267
tracing DDoS attacks, 649
SNAP (Simple Network Auto Provisioning), 604
sniffing packets, 318

SNMP (Simple Network Management Protocol), 307, 405, 465
 protocol, 465
 security, line access control, 405–406
 Trap protocol, 465
SOBGP (Secure Origin BGP), 236
social engineering
 security awareness training, 352
 threats to corporate networks, 288
SOCKS protocol (Socket Security protocol), 83–84
software
 network assets, 296
 pirated, 355
source addresses, NAT, 475
source port numbers, 453
spam attacks, SMTP, 272
spamming, e-mail, 272
span ports, intrusion detection system, 362
Spanning Tree Protocol (STP), 418
spanning-tree protocols, authentication, 340
SPD (security policy database), 92
special use addresses, 634
SPF (shortest-path first), 224, 230
SPI (security parameter index), 91
splitters, optical, 315
spoofing attacks, 250–258
 DDoS attacks, ingress/egress filtering, 635, 643
 deterrents, 341
 IP addresses, tracking, 656, 662
 packets, corporate networks, 423–424
 TCP/IP sequence number, 262
spread-spectrum radio technology, 156
 802.11 media access controls, 160–162
 DSSS, 156–157
 FHSS, 157
 OFDM, 158–160
 wireless roaming, 163–164
SQL Server protocol, 464
SQL*Net protocol, 464
 CBAC inspection, 477
squeeze commands, Cisco IOS privilege access, 382
sRTP (Secure Real-Time Transport Protocol), 200
SRVTAB, Kerberos protocol, 64
SSH (Secure Shell), 83, 273, 331
ssh commands, 380, 404
SSID (Service Set Identifier), 165, 248
SSL (Secure Socket Layer), 345, 463
 firewalls, 469
 handshake process, 80–81
SSL/TLS protocol (Secure Socket Layer /Transport Layer Security protocol), 78–82
Stacheldraht attack program, 257
staff
 security policies and procedures
  audits, 348–350
  backups, 347–348
  equipment certification, 348
  portable tools, 348
 site security policies and procedures, sample policy, 350–351
standard IP ACLs, 449–450
standard of conduct sample, 292–294
standby commands, Cisco switch privilege access, 390
starred physical topography, 319
start-chat commands, Cisco IOS privilege access, 383
start-stop keywords, AAA accounting, 523
state information, intrusion detection system limitations, 364
stateful modes, PIX firewall, 422
stateless modes, PIX firewall, 421
static addresses, NAT, 475
start-chat commands, Cisco IOS privilege access, 383
static commands, 486
static routing, 208, 210
statistical analysis, intrusion detection system, 361
Stoll, Cliff, *The Cuckoo's Egg,* 348
stop-only keywords, AAA accounting, 523
storage, data, audits, 349–350
STP (Spanning Tree Protocol), 418, 420
StreamWorks protocol, 463, 477
subnet boundaries, logical security controls, 324–327
 routing boundaries, 327–329
 VLAN boundaries, 329–330
subnet masks, 326
subnetworks, 325
subscription-based authentication, 194
SWAP (Shared Wireless Access Protocol), 152
switch commands, Cisco switch privilege access, 390
Switch> (enable) ? commands, Cisco switch privilege access, 390
Switch> ? commands, Cisco switches basic access, 389
switches
 10BASE-T Ethernet, 245
 basic access mode, 389–392
 command-line interface, 401
 embedding intrusion detection system, 362
 impersonation, 252
 intrusion detection system, 361–363
 line access controls, 401–402
 network availability, 418–421
 privilege access mode, 389–392
 versus hub functionality, 361
symmetric encryption, 6–9
 3DES, 10
 AES, 10–11
 DES, 9
 IDEA, 10
 RC-4, 10
 S/MIME communication, 76
symmetric encryption-based authentication, 193
symmetric key-encryption key, CEK encryption, 75
SYN flag, TCP, 260
SYN flood, tracing DDoS attacks, 648–649
SYN packet (synchronize/start packet), 263

SYN/ACK packet (synchronize acknowledge packet), 263
synchronize acknowledge packet, 263
synchronize/start packet, 263
Syslog, management, 428–431
syslog commands, PIX firewall privilege access, 393
syslog keyword, 605
Syslog protocol, 465
systat commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
system events, AAA accounting, 522

T

TACACS, 55
tacacs commands, TACACS+ authorization, 388
TACACS+, 510
  accounting, 522–523
  authentication, 510–515
  authorization, 388, 516
    CiscoSecure server syntax, 520–521
    methods, 517–520
    service types, 516–517
  billing, 524–525
  methods
    AAA accounting, 523
    AAA authentication, 399, 512
    AAA authorization, 517
  protocol, 55, 463
    accounting, 58
    authentication, 56–57
    authorization, 57
    encryption, 62
    transactions, 58–59
tacacs+ commands, 391
tacacs-server commands, PIX firewall privilege access, 394
tagging, EIGRP routing concepts, 223
TCP (Transmission Control Protocol), 259
  flags, 260
  half-open session, 479
  header format, 259
  protocol
    advanced packet session filtering, 460
    CBAC inspection, 477
    filter parameters, 451
    port numbers, 451
    services, 464–465
    vulnerabilities, 258–260
    land.c attack, 264
    sequence number attack, 261–263
    session hijacking, 263
    TCP SYN attack, 263–264
    three-way handshake connection, 260– 261
TCP SYN attacks, 253
  corporate networks, 425–426
  TCP/IP protocol, 263–264
TCP SYN packets, rate limiting, 644–645
TCP/IP (Transmission Control Protocol/Internet Protocol), 402
  vulnerabilities, 258–260
    land.c attack, 264
    sequence number attack, 261–263
    session hijacking, 263
    TCP SYN attack, 263–264
    three-way handshake connection, 260– 261
TDR tool (time domain reflectometer tool), 314
teardrop.c attacks, 253
  ICMP, 267–268
technologies
  application layer security protocols, 73
    S/MIME, 74–77
    SHTTP, 73–74
  EIGRP, 221–222
  identity, 38–39
  authentication verification, 55, 72
    passwords, 39, 44
    PPP, 45, 54
  link-layer security, 107
    L2F protocol, 107–109
    L2TP protocol, 113, 120
    PPPoE, 120–121
    PPTP, 110–113
  network layer security protocols, 85
    IPsec protocol suite, 85, 107
  PKI, 121–122
    certificate distribution, 128–129
    certificates, 124–125
    functions, 122–123
    sample scenario, 123–124
    X.509 standard, 125–128
  spread-spectrum radio, 156
    802.11 media access controls, 160–162
    DSSS, 156–157
    FHSS, 157
    OFDM, 158–160
    wireless roaming, 163–164
  transport layer security protocols, 77–78
    SOCKS protocol, 83–84
    SSH protocol, 83
    SSL/TLS protocol, 78–82
  VoIP networks, 597
    audit, 605
    availability, 604–605
    confidentiality, 603
    design references, 605
    identity, 597–602
    integrity, 603
  VPNs, 575–577
    audit, 590
    availability, 589
    confidentiality, 589
    design example, 590–591

identity, 577–588
integrity, 588
wireless network, 592
audit, 595–596
availability, 594–595
confidentiality, 594
design example, 596
identity, 592–594
integrity, 594
Telecommunications Network Protocol, 465
telecommuters, 528, 530
telephony gateways, 186
Telnet (Telecommunications Network Protocol), 465
IANA-assigned ports, 82
passwords, 331
Reverse, 517
telnet commands, 403
Cisco IOS basic access, 380
Cisco IOS privilege access, 383
Cisco switch privilege access, 390
PIX firewall privilege access, 394
temperature controls, 322
Temporal Key Integrity Protocol (TKIP), 171, 248, 282, 594
TEN (Tribal Flood Network) attack program, 257
terminal commands
Cisco IOS basic access, 380
Cisco IOS privilege access, 383
terminal line ports (tty ports), 395
terminals, H.323 standard components, 180
test commands
Cisco IOS privilege access, 383
Cisco switch privilege access, 390
test help commands, Cisco switch privilege access, 390
TFN2K attack program, 257
TFTP (Trivial File Transfer Protocol), 402, 465
CBAC inspection, 477
TGTs (ticket-granting tickets), 63–68
third parties, authentication methods, 38
Thomas, Rob, monitoring DoS attacks, 651
threats
enterprise networks
denial of service (DoS), 253–254
distributed denial-of-service (DDoS), 254, 257
impersonation, 250–253
motivation for, 257–258
protocol vulnerabilities, 258, 275
unauthorized access, 242–249
risk assessment, 297–298
data compromises, 298
data integrity, 298–299
resource unavailability, 299
routing protocols, 287–288
social engineering, 288
VoIP, 283
denial of service (DoS), 284
impersonation, 284
SIP-based networks, 284–287
unauthorized access, 283
VPN, 276
denial of service (DoS), 277
impersonation, 277
unauthorized access, 276
wireless networks, 278
denial of service (DoS), 279
impersonation, 279
unauthorized access, 278–279
WEP, 280–282
three-way handshakes, TCP/IP connection, 260–261
ticket-granting tickets (TGTs), 63–68
time domain reflectometer tool, 314
Time protocol, 465
timeout periods, 457
timers, RIP, 214
time-synchronous token systems, 44
time-to-live, 269
TKIP protocol (Temporal Key Integrity Protocol), 171–172, 248, 282, 594
TLS (transport layer security), 286
SIP protocol, 199
SIP-based networks, 286–287
TLV (type-length-value), 232
token authentication systems, 42–44
token cards, 42
tokenless call authorization, 602
topographies, network
physical security controls, 318–319
spoofed IP addresses, 658–659
topology tables, EIGRP routing concepts, 222
traceroute commands
Cisco IOS basic access, 380
Cisco IOS privilege access, 383
tracing DDoS attacks, 647–648
access list logging, 650–651
log-input, 648
Smurf attack, 649
SYN flood, 648–649
without log-input, 650
trade secrets, data classification, 297
traffic
filtering, 323
flow, firewalls, 335–336
applications, 337
authentication, 337
direction, 336
IP address, 337
origin, 337
port numbers, 337
intrusion detection system limitations, 363
shaping, DDoS attack preventive measures, 644
ICMP packets, 644
TCP SYN packets, 644–645
valid, 335
training, security awareness, 351–352
transaction modes, SHTTP protocol, 73
translation slots, 486
Transmission Control Protocol. *See* TCP
Transmission Control Protocol/Internet Protocol, 402
transmission media, consistent use example, 317

transport input commands, 400
transport layer, security protocols, 77–78, 286
    SOCKS protocol, 83–84
    SSH protocol, 83
    SSL/TLS protocol, 78–82
transport modes, 89, 140
transporting metropolitan Ethernet, ONS products, 243–273, 315–328, 378, 403, 409–418, 426, 501–504, 524– 530, 542, 551–555, 636–639, 659
Tribal Flood Network (TEN) attack program, 257
Trinoo attack program, 256
triple Data Encryption Standard, 9
Trivial File Transfer Protocol, 402
trust domains, namespaces, 22–23
trust models, authorization, 21–22
TTL (time-to-live), 269
tty ports (terminal line ports), 395
tunnel commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 383
tunneling
    GRE, 540
    interfaces, 90
    modes, 90, 140
    packets, 107
    protocols, 139, 146
    VPNs, 137
Turbo ACLs, 455
twisted pair cables, 314
type-length-value, 232

U

U.S. government, key escrow, 31–32
U.S. Government Accounting Office (GAO), 356
U.S. policies, Section 1832, Theft of Trade Secrets, 625
UDP (User Datagram Protocol), 264
    header format, 265
    NFS system, 275
    NIS system, 275
    packets, 370
    protocol
        advanced packet session filtering, 461
        CBAC inspection, 477
        port numbers, 452
        services, 464–465
    vulnerabilities, 264
udptn commands
    Cisco IOS basic access, 380
    Cisco IOS privilege access, 383
UID (user ID), 69
unauthorized access, 242
    common scenarios, 249
    Internet, 242–244
    internet, reachability check, 242
    packet snooping, 244–245
    remote dial-in access, 246–247
    VoIP, 283
    VPN, 276
    wireless access, 248–249
    wireless networks, 278–279
undebug commands, Cisco IOS privilege access, 383
unicast addresses, IP, 324
unicast discovery, H.323 call-signaling flow, 184
universal unique ID (UUID), 69
UNIX
    NES system, 275
    NIS system, 275
UNIX R, CBAC inspection, 477
UNIX-to-UNIX Copy Program, 465
unregistration request, 598
update packets, EIGRP, 223
uplink groups, 420
UPlinkFast feature, 420
upload commands, Cisco switch privilege access, 390
uptime commands
    PIX firewall basic access, 393
    PIX firewall privilege access, 394
URG flag, TCP, 260
uRPF (IP unicast reverse-path forwarding), 645–646
URQ (unregistration request), 598
User Datagram Protocol. *See* UDP
user ID (UID), 69
username commands, 518, 526
users
    authentication VPNs, 578, 583–584
    logical security controls, 333
    passwords, logical security controls, 331
    VPNs authentication
        application access, 578
        network access, 577
UUCP (UNIX-to-UNIX Copy Program), 465
UUID (universal unique ID), 69

V

valid traffic, 335
validate-update-source commands, 411
validations, security policy, 343
values, assets, 296–297
variable-length subnetting, 224
VDOLive protocol, 463, 477
verifications, security policy, 343
    accounting, 344
    intrusion detection, 347
    intrusion detection system, 345
    sample policy, 347
    secure management, 344–345
    vulnerability scanners, 343
verify commands, Cisco IOS privilege access, 383
Versatile Interface Processor (VIP), 651
video codecs, H.323 standard component, 183
video streaming, 463

VIP (Versatile Interface Processor), 651
  if-con command, 652
  monitoring DoS attacks, 651–656
virtual dial-in access, encryption, 539
  CET, 539, 548
  GRE tunneling, 539, 548
  IPsec, 548, 554
  L2TP with IPsec, 554, 572
virtual http commands, 585
virtual local-area networks, 323
virtual private dial-in networks, 501
Virtual Private Networks. *See* VPNs
virtual telnet commands, 585
virtual terminal ports (vty ports), 395, 401
VLANs (virtual local-area networks), 323
  boundaries, 329–330
  protocols, authentication, 340
voice commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
voice gateways, VoIP network components, 178
Voice over IP networks (VoIP networks). *See* VoIP
"voice over misconfigured Internet telephones" (vomit), 283
voice-mail systems, VoIP network components, 178
VoIP (voice over IP network), 135, 177, 283
  deployment models, 178–179
  IP telephony components, 178
  protocols, 180
    H.323 standard, 180
    H.323 standard components, 180–186
    MGCP, 186–187
    port numbers, 600
    SIP, 187, 193
  security protocols, 193
    H.323 standard protocol security, 193–196
    SIP, 196–200
  security solutions, 200–202
  security technologies, 597
    audit, 605
    availability, 604–605
    confidentiality, 603
    design references, 605
    identity, 597–602
    integrity, 603
  vulnerabilities, 283
    denial of service (DoS), 284
    impersonation, 284
    SIP-based networks, 284–287
    unauthorized access, 283
voip keywords, 605
voluntary tunnels, 150
"vomit" (voice over misconfigured Internet telephones), 283
VPDNs (virtual private dial–in networks), 501
VPNs (Virtual Private Networks), 135, 241, 276, 575
  deployment models, 135–137
    client-to-site, 138–139
    site-to-site, 137
  large corporate scenario, 592
  port numbers, 587
  security, 139
    application, 148–151
    authentication, 147–148
    technologies, 575–578, 588–591
    tunneling protocols, 139, 146
  small corporate scenario, 591
  vulnerabilities, 276
    denial of service (DoS), 277
    impersonation, 277
    unauthorized access, 276
  wireless security, 177
vty ports (virtual terminal ports), 395
vulnerabilities, risk assessment, 297–298, 343
  data compromises, 298
  data integrity, 298–299
  resource unavailability, 299

W

WAIS (Wide Area Information Servers), 463
wait commands
  Cisco switch privilege access, 390
  Cisco switches basic access, 389
wait-start keywords, AAA accounting, 523
WAN (Wide Area Networks)
  centralized call processing, 179
  distributed call processing, 179
war dialing, 246–247
water hazard prevention, 321
weak keys, asymmetric encryption, 15
Web IVs, collision attack, 282
websites
  Airsnort, 281
  Anti-Spam, 272
  Bernard Aboba, 177
  CAUCE, 272
  CCIPS, 369
  CIAC, 369
  Cisco, 580, 613
  FASP, 612
  IEFT, 612
  IETF, 213
  Mitnick, Kevin, 356
  Open Software Foundation, 69
  Rice University, 281
  security, 613
  U.S. Government key escrow position, 32
weight arguments, 413
WEP (Wired Equivalent Privacy), 166, 248, 594
  bit-flipping vulnerability, 283
  decryption, 168
  encryption, 166–169
  key length, 169
  weak key attack, 281
  wireless network vulnerabilities, 280–282

where commands
  Cisco IOS basic access, 380
  Cisco IOS privilege access, 383
who commands
  PIX firewall basic access, 393
  PIX firewall privilege access, 394
Who protocol, 465
Wide Area Information Servers, 463
Wi-Fi Protected Access (WPA), 171
window advertisement, TCP, 261
wire taps, 31, 317
Wired Equivalent Privacy. *See* WEP
wireless LANS. *See* WLANs
wireless networks
  interference considerations, 280
  policy, 279
  security technologies, 592
    audit, 595–596
    availability, 594–595
    confidentiality, 594
    design example, 596
    identity, 592–594
    integrity, 594
  unauthorized access, 248–249
  vulnerabilities, 278
    denial of service (DoS), 279
    impersonation, 279
    unauthorized access, 278–279
    WEP, 280–282
wireless roaming, Mobile IP, 163–164
wireless technologies, WLANs, 151–152
wiretaps, detection, 31, 314
WLANs (wireless LANS), 151
  components, 153
  deployment models
  infrastructure mode, 154
  peer-to-peer WLAN, 153–154
  security
    basics, 165–166
    cryptographic authentication, 169–170
    enhancements, 170, 177
    VPN, 177
    WEP encryption, 166–169
  spread-spectrum radio technology, 156
    802.11 media access controls, 160–162
    DSSS, 156–157
    FHSS, 157
    OFDM, 158–160
    wireless roaming, 163–164
  wireless technology types, 151–152
workgroups
  Internet standard publications, 612
  security, 409–410
WORM drives (write-once, read many drives), 349
Worms Against Nuclear Killers (NASA WANK), 356
WPA (Wi-Fi Protected Access), 171
write commands, 403
  Cisco IOS privilege access, 383
  Cisco switch privilege access, 390
  PIX firewall privilege access, 394
write memory commands, 388, 423
write terminal commands, 387
write-once, read many drives (WORM drives), 349

X–Z

X Window System, vulnerabilities, 275
X.25, MTUs, 266
X.509 certificate format, 29
X.509 standard, PKI, 125
  X.509v2 CRL, 127–128
  X.509v3 certificate, 126
X.509v2 CRL, 127–128
X.509v3 certificates, 126
X11 protocol, 465
x3 commands, Cisco IOS basic access, 380
Xauth (Extended Authentication), 140
xlate, 486
XOR function, 59
XTACACS, 55