INDEX

A

- AAA, 201
  - accounting, 226–227
    - broadcast accounting, 229–230
    - configuring, 227
    - enabling, 227–229
    - suppressing null username records, 229
    - troubleshooting, 230
  - authentication, 213–214
    - login banners, 218–219
    - method lists, 214–215
    - privileged EXEC shell access, 217
    - user EXEC shell access, 216–217
    - username and password prompts, 218
  - authorization, 222
    - configuring, 222
    - example of, 225
    - restricting command execution, 223–224
    - troubleshooting, 224
  - centralizing, 203
    - server groupings, 208
    - server protocol example configuration, 211–212
    - with RADIUS, 205–208
    - with TACACS+, 203–205
  - configuring, 202
    - on perimeter routers, case study, 817–820
  - functions of, 202
- aaa accounting command, 227
- aaa authentication login command, 216
- aaa authorization command command, 225
- aaa new-model command, 204
- absolute command, creating time ranges, 286
- absolute timer (lock-and-key), 556
- access, controlling, 43
- access attacks, 22–24
  - data manipulation attacks, 24–25
  - session attacks, 25–29
    - masquerading attacks, 26
    - preventing, 28–29
    - repudiation attacks, 28
    - session-hijacking attacks, 26–27
    - session-replay attacks, 26
- access profiles, 568
- access-class command, 123
- accessing Cisco routers, 117
  - aging password authentication, 113–114
  - local access, 118–120
  - no password authentication, 111–112
  - OTPs, 114–115
  - privileged EXEC mode, 146–152
  - remote access, 121–145
  - static password authentication, 112–113
  - token card services, 115–117
- access-restrict command, 796
- accounting, 226–227
  - broadcast accounting, 229–230
  - configuring, 227
  - enabling, 227–229
  - suppressing null username records, 229
  - troubleshooting with debug aaa accounting command, 230
- acl command, 796
- ACLs (access control lists), 237–238, 259–260
  - accounting
    - defining thresholds, 294
    - filtering information, 293–294
    - limiting transit records, 294–295
  - activating, 252
  - bogon addresses
    - egress filtering, 305–307
    - ingress filtering, 302–305
  - configuring
    - on internal routers, case study, 823–825
    - on perimeter routers, case study, 820–823
  - controlling address translation, 514–515
  - creating, 250–251
  - deleting entries from, 261
  - detecting DoS attacks, 665–672
  - editing, 252–253
  - example, 238
  - extended, 264
    - named extended ACLs, 273
    - numbered extended ACLs, 264–272
    - three-interface router example, 275–278
    - two-interface router example, 273–275
  - fragments, filtering, 282–285
  - lock-and-key, 551–552
    - configuring, 555–560
    - example, 563–564
    - operation, 553–554

remote administration access, 560–562
troubleshooting, 562–563
when to use, 552
logging updates, 291
threshold, changing, 291–292
violations, accounting, 292–293
monitoring rcp command usage, 327
placement of, 248–249
preventing attacks
fraggle attacks, 310–311
smurf attacks, 308–310
TCP SYN floods, 307–308
processing, 241
conditions, 241
rules, 246–247
statement order, 243–246
RACLs, 351
building, 358
configuring, 365–374
examples of, 374–378
filtering returning traffic, 359–360
limitations of, 361–364
removing entries, 360–361
traffic processing, 357
versus extended ACLs, 352–356
remarks, 251
adding, 290
securing routing protocols, 613–614
sequenced
configuring, 296–298
deleting entries, 299
inserting entries, 300–301
resequencing, 298–299
standard, 260
examples of, 263–264
named standard ACLs, 262–263
numbered standard ACLs, 261–262
timed, 285
activating time ranges, 287
creating time ranges, 285–287
distributed, 287–288
example configuration, 288–289
Trojan horse attacks, blocking, 325–326
turbo, configuring, 295–296
types of, 240–241
verifying configuring, 278–280
wildcard masks, converting from subnet masks, 254–256
activating
ACLs, 252
AP policies, 580–581
CBAC inspection rules, 410
crypto maps, 773
time ranges for timed ACLs, 287
adding remarks to ACLs, 290
address overloading, 480–481
address translation
configuring on perimeter routers, case study, 827–830
connection limits, configuring, 500
controlling
with ACLs, 514–515
with route maps, 517
with route maps with dynamic NAT, 515–519
with route maps with static NAT, 520–521
dynamic translation, 477
embedded addressing information, 509–510
ALG support, 511–512
supported protocols, 511
extended translation, 477
IP NAT Service, 512
configuring, 513–514
limitations of, 484
NAT, 474–477
configuring, 484–488
global addresses, 476
local addresses, 476–477
overlapping addresses, 479
static NAT redundancy with HSRP, 522–526
with CBAC, configuring, 505–507
overlapping addresses, configuring, 493–497
PAR, configuring, 491, 493
PAT, 480–481
configuring, 489–491
private addresses, 473–474
simple translation, 477

SNAT, 526
configuring with HSRP, 527–531
configuring without HSRP, 531–534
verifying configuration, 534–535
static translation, 477
statistics, displaying, 502–503
timeout limits, configuring, 500–501
traffic distribution, 482
configuring, 498–499
translation table entries, removing, 503–504
troubleshooting with debug ip nat command, 504
verifying with show commands, 501–502
address-translation firewalls, 72
advantages of, 75
applications of, 76
filtering process, 72–75
limitations of, 75–76
administering firewall systems, 101
agents (DDoS attacks), 317
AGFs (application gateway firewalls), 64
advantages of, 70
applications of, 72
authentication methods, 66–67
authentication process, 65–66
CGFs, 67–68
cut-through proxy firewalls, 69–70
limitations of, 70–71
aging password authentication, 113
susceptibility to eavesdropping attacks, 114
AIM (AOL Instant Messenger), filtering, 333–334
alerts
CBAC, 383
URL filtering, 437
alerts (CBAC), configuring, 414
ALG (Application Layer Gateway), address translation support, 511–512
amplification attacks, 310
amplifiers, discovering, 313–314
disabling directed broadcasts, 311
filtering directed broadcasts, 311, 313
victims, discovering, 313–314
anomaly-based IDS solutions, 93
antispoofing, 327
AP (authentication proxy), 567
AAA, configuring, 576
access profiles, 568
applications of, 573–574
authentication process, 570–572
banners, creating, 582–583
configuring, 575
AAA server configuration, 576–579
policies, activating, 580–581
preparing for HTTP/HTTPS, 579–580
example configuration, 587–594
features, 568–569
JavaScript, 572–573
limitations of, 574–575
troubleshooting
with clear commands, 587
with debug commands, 587
with show commands, 584–586
tuning, 582–583
versus lock-and-key, 569
watch lists, configuring, 583–584
Apple iChat, filtering, 338
application attacks, 31
application inspection, CBAC, 389
applications
Apple iChat, blocking use of, 338
file-sharing, filtering, 338–341, 343–347
ICQ, blocking use of, 334–335
IM, blocking use of, 333–334
MSN Messenger, blocking use of, 335
Yahoo! Messenger, blocking use of, 336–338
applying dynamic crypto maps, 800
are-u-there command, 796
assigning
privilege levels to commands, 146–149
static passwords to auxiliary line, 119
static passwords to console line, 118
attacks
access, 22–24
data manipulation attacks, 24–25
session attacks, 25–29
amplification, discovering intended victims, 313–314
DDoS, 317–319
agents, 317
client, 317
handler, 317
Stacheldraht, 322–323
TFN, 319–320
TFN2K, 320

Trinity, 324
Trinoo, 321–322
DoS, 31–33
detecting, 661–662, 665–676
preventing, 33–34
Smurf, 677
symptoms, 662–664
feint, 318
Land.c, 304
reconnaissance, 19, 314
eavesdropping attacks, 20–21
preventing with egress traffic filtering, 315–316
preventing with ingress ICMP filtering, 315
preventing with traceroute, 316
scanning attacks, 19–20
TCP SYN flood, preventing with TCP Intercept, 679–686
Trojan horses, 29–31, 325
blocking with ACLs, 325–326
detecting, 325
monitoring rcp command usage with ACLs, 327
viruses, 29–31
worms, 29–31
AudioGalaxy, filtering, 345–346
audits (CBAC)
configuring, 414
URL filtering, 438–439
authentication, 213–214
aging password configuration, 113
susceptibility to eavesdropping, 114
basic configuration example, 156–158
centralizing, 24
example of, 220–221
for local Cisco router access, 120
login banners, 153–154, 218–219
configuring, 154–156
MD5, configuring
on BGP, 617
on EIGRP, 608
on HSRP, 615–616
on IS-IS, 609–611
on OSPF, 608–609
on RIP, 606–607
method lists, 214–215
no password configuration, 111–112
NTP, 728–729
of IGPs, 604
MD5 authentication, 606
plain-text authentication, 605
passwords
encrypting, 152–153
OTPs, 114–115
privileged EXEC shell access, 217
static password configuration, 112–113
token card services, 115–117
troubleshooting, 219–220
user EXEC shell access, 216–217
username and password prompts, 218
authorization, 222
configuring, 222
example of, 225
restricting command execution, 223–224
troubleshooting, 224
AutoSecure feature, 184
configuring, 187–188
forwarding plane, 186
management plane, 185
sample script, 188–198
verifying configuration, 198
auxiliary line
assigning passwords, 119
configuring access to Cisco routers, 119

B

banners, 153–154, 218–219
AP authentication banners, creating, 582–583
configuring, 154–156
BGP (Border Gateway Protocol), 617
MD5 authentication, caveats, 606
MD5 authentication, configuring, 617
route flap dampening, configuring, 618–619
secure configuration example, 620–624
black hole routing, configuring, 598–604
blocking
applications, 332–333
Apple iChat, 338
ICQ, 334–335
IM, 333–334
MSN Messenger, 335
Yahoo! Messenger, 336–338

bogons, 302
egress filtering, 305–307
ingress filtering, 302–305
Stacheldraht attacks, 322–323
TFN attacks, 320
TFN2K attacks, 320
Trinity attacks, 324
Trinoo attacks, 321–322
Trojan horse attacks with ACLs, 325–326
bogons, 301
blocking, 302
egress filtering, 305–307
IANA listing, 301
ingress filtering, 302–305
BootP, disabling, 170
broadcast accounting, 229–230
broadcast-based NTP configuration, 725
building RACLs, 358, 368–374

C

capturing accounting information, 226–229
broadcast accounting, 229–230
suppressing null username records, 229
CAR (committed access rate), limiting DoS attack damage, 694–698
CAs (Certificate Authorities), 29
configuring HTTPS access to Cisco routers, 134–139
case studies
branch offices, 812
corporate offices
internal routers, 811
perimeter routers, 809–811
internal routers
ACL configuration, 823–825
CBAC configuration, 827
configuring, 814
perimeter routers
AAA configuration, 817–820
ACL configuration, 820–823
address-translation configuration, 827–830
CBAC configuration, 825–826
CBAC threshold configuration, 833
configuring, 813–814
IDS configuration, 832
NTP configuration, 835
rate limiting configuration, 833–834
remote access VPNs configuration, 839–842
RPF configuration, 831
site-to-site VPNs configuration, 836–838
static route configuration, 830
sylog configuration, 836
proposals, 812–813
remote access users, 812
unnecessary services, disabling, 815–817
CBAC (Context-Based Access Control)
alerts, 383
configuring, 414
audits, configuring, 414
configuring, 398–399
ACL creation, 400
global timeouts, 400–401
inspection rules, 405–410
interface selection, 399
on internal routers, case study, 827
on perimeter routers, case study, 825–826
PAM, 401–405
enhancements exclusive to, 385
application inspection, 389
DoS detection and prevention, 389–390
embedded addressing information, 387–388
extra connections, 387
ICMP traffic, 386
TCP traffic, 385–386
UDP traffic, 386
example configuration, 691
of inspection rules, 415–417
three-interface configuration, 418, 420–422
two-interface configuration, 417–418
flexibility of configuration, 385
inspection rules
activating, 410
configuring, 405–409
intrusion detection, 383
Java inspection, 426

configuring, 426
example, 426–428
limitations of, 397–398
misconfiguration, preventing, 399
operation, 383–385
PAM
configuring, 401–403
example configuration, 405
verifying configuration, 404
performance, 395
connections per second, 396–397
CPU utilization, 397
throughput, 396
preventing DoS attack, 690
removing from router, 415
state table, changing connection timeouts, 400–401
supported protocols, 390
H.323, 392–393
RTSP, 390
SIP, 394–395
Skinny, 393–394
thresholds, 687
configuring on perimeter routers, case study, 833
connection thresholds, 688–689
timeouts, 687
connection timeouts, 688
traffic filtering, 382–383
traffic inspection, 383
troubleshooting, 410
with debug commands, 413–415
with show commands, 411–413
URL inspection
alerts, 437
audits, 438–439
configuring, 433–435
example, 443–444
logging, 439
maximum requests, 436
maximum responses, 436
troubleshooting, 442
verifying, 440–441
with NAT, configuring, 505–507
CDP (Cisco Discovery Protocol), disabling, 162–163, 173
CEF (Cisco Express Forwarding), 678–679
centralizing AAA, 203
authentication processes, 24
server groupings, 208
server protocol example configuration, 211–212
with RADIUS, 205–208
with TACACS+, 203–205
CGFs (connection gateway firewalls), 67–68
challenge-based authentication, 116
Chargen, 32
cipher suites, 131
Cisco IOS Firewall feature set, 103–104
features, 381–382
Cisco IOS Firewalls, application of, 105–106
Cisco IOS IDS, 644
configuring, 652–656
example configuration, 658–659
performance issues, 652
signature support, 645–650
verifying configuration, 657–658
Cisco IOS Software
ALG address translation support, 511–512
applications of, 102
real server attributes, 542–543
SLB, 536–537
configuring, 541–544
example configuration, 545–546
limitations of, 540
load balancing algorithms, 538
load balancing features, 539–540
verifying configuration, 544
virtual server attributes, 543–544
Cisco routers, 79–80
accessing, 117
privileged EXEC access, 146
assigning privilege levels, 146–149
local authentication database, 150–152
password levels, 146, 149–150
remote access
via HTTPS, 130–139
via SNMP, 139–145
via SSH, 123–127
via VTY lines, 121–123
via web browser, 127–130
user EXEC access
local access, 118–120
remote access, 121

Cisco Secure ACS authentication server, token card support, 117
clear commands
  removing translation table entries, 503–504
  troubleshooting AP, 587
clearing URL filtering cache, 434
clear-text passwords, 118–119
CLI configuration, SDM, 99
client (DDoS attacks), 317
Code Red worm, 676–677
  filtering, 463–466
commands
  aaa accounting, 227
  aaa authentication login, 216
  aaa authorization, 225
  aaa new-model, 204
  access-class, 123
  clear, 503–504
  crypto ca trustpoint, 135
  debug aaa accounting, 230
  debug aaa authentication, 219–220
  debug aaa authorization, 224
  debug ip nat, 504
  debug ip scp, 232
  debug ip snat, 535
  debug radius, 211
  debug tacacs, 209
  enable secret, 149
  ip access-list log-update threshold, 291
  ip http secure-client-auth, 136
  ip nat pool, 496
  ip nbar port-map, 453
  ip slb serverfarm, 541
  logging synchronous line configuration, 118
  no ip inspect, removing CBAC from router, 415
  passive-interface, 613
  privilege levels, assigning, 146–149
  radius-server host, 207
  radius-server timeout, 207
  rcp, monitoring usage with ACLs, 327
  security authentication failure rate, 198
  security passwords min-length, 198
  show, verifying address translation, 501–502
  show access-list compiled, 295–296
  show ip http server secure status, 137
  show logging, 716–717
  show logging history, 717
  show ntp associations, 730
  show ntp status, 730–731
  show privilege, 150
  show sntp, 731–732
  show tacacs, 209
  snmp server-group, 144
  snmp-server community, 141
  tacacs-server host, 205
comparing
  Cisco PIX and Cisco IOS firewall solutions, 105–106
  lock-and-key and AP, 569
  RADIUS and TACACAS+, 212–213
computer technology weaknesses, 13
  network equipment, 15
  network protocols, 13
  operating systems, 14–15
conditions (ACLs), 241
configuration autoloading, disabling, 172–173
configuring
  AAA, 202
  ACLs, 250–251
    accounting, 292–295
    remarks, 251
    verifying configuration, 278–280
  address translation
    connection limits, 500
    of overlapping addresses, 493–497
    timeout limits, 500–501
  AP, 575
    AAA, 576
    AAA server configuration, 576–579
    example configuration, 587–594
    policies, activating, 580–581
    preparing for HTTP/HTTPS, 579–580
    watch lists, 583–584
  authentication, example, 156–158
  authorization, 222
  AutoSecure, 187–188
    sample script, 188–198
    verifying configuration, 198
  basic logging, 706
  black hole routing, 599–601
    with PBR, 601–604
  CBAC, 398–399
    alerts, 414

audits, 414
connection thresholds, 688–689
connection timeouts, 688
creating ACLs, 400
flexibility of, 385
global timeouts, 400–401
inspection rules, 405–410
interface selection, 399
PAM, 401–405
verifying configuration, 410–415
Cisco IOS IDS, 652–656
ESM, 738–740
internal router, case study, 814
IP NAT Service, 513–514
IPSec site-to-site connections, 747–748
external ACL, 749
IKE phase 1, 750–753
IKE phase 1 peer authentication, 753–765
IKE phase 2 data connection, 766–774
Java inspection, 426
lock-and-key, 555–560
logging, synchronous logging, 706–708
login banners, 154–156
manual time and date, 720–722
MD5 authentication
on BGP, 617
on EIGRP, 608
on HSRP, 615–616
on IS-IS, 609–611
on OSPF, 608–609
on RIP, 606–607
NAT, 484–486
dynamic NAT, 487–488
with CBAC, 505–507
NBAR, 451–453
filtering marked traffic, 459
group classifications, 454–455
HTTP traffic filtering, 457
P2P program filtering, 455–469
PDLMs,downloading, 457
policies, 458–459
verifying configuration, 460–463
NTP, 725
authentication, 728–729
broadcast-based configuration, 725
client configuration, 723
example, 731–732
poll-based configuration, 724
restricting resources, 728
server configuration, 725–727
PAR, 491–493
passive interfaces, 612–613
PAT, 489–491
perimeter routers, case study, 813–814
RACLs, 365, 368–374
interface selection, 365–368
route flap dampening on BGP, 618–619
RPF, 629
verifying configuration, 630–631
SCP, 231
sequenced ACLs, 296–298
SLB, 541–544
SNAT
with HSRP, 527–531
without HSRP, 531–534
static crypto maps, 801
static NAT, redundancy with HSRP, 524–526
timed ACLs, example, 288–289
traffic distribution, 498–499
turbo ACLs, 295–296
URL filtering, 432–434
alerts, 437
audits, 438–439
cache, clearing, 434
exclusive domains, 435
logging, 439
maximum requests, 436
maximum responses, 436
with CLI, SDM, 99
connection thresholds, configuring on CBAC, 688–689
connections
embryonic, 13
timeouts, configuring on CBAC, 688
connections per second feature (CBAC), 396–397
console line, assigning passwords, 118
content filtering, 81. *See also* URL filtering
controlling
access to resources, 43
address translation
with ACLs, 514–515
with route maps, 517

with route maps with dynamic NAT, 515–519
with route maps with static NAT, 520–521
cost benefit analysis of security measures, 8
CPU hogging, 31
CPU utilization feature of CBAC, 397
creating
ACLs, 250–251
AP authentication banners, 582–583
dynamic crypto maps, 799–800
time ranges for timed ACLs, 285
with absolute command, 286
with periodic command, 286–287
transform sets, 800
CRLs, troubleshooting, 762
crypto ca trustpoint command, 135
crypto isakmp nat keepalive command, 797
crypto isakmp xauth timeout command, 797
crypto maps, 771–773
CSI (Computer Security Institute), 16
cut-through proxy firewalls, 69–70

D

data manipulation attacks, 24–25
DDoS attacks, 317–319
agents, 317
client, 317
handler, 317
Stacheldraht, blocking, 322–323
TFN, 319
blocking, 320
TFN2K, blocking, 320
Trinity, blocking, 324
Trinoo, blocking, 321–322
debug aaa accounting command, 230
debug aaa authentication command, 219
debug aaa authorization command, 224
debug commands
troubleshooting AP, 587
troubleshooting CBAC, 413–415
troubleshooting URL filtering, 442
debug ip nat command, 504
debug ip scp command, 232
debug ip snat command, 535
debug radius command, 211
debug tacacs command, 209
defining ACL accounting thresholds, 294
deleting entries from ACLs, 261
sequenced ACLs, 299
Deloder worm, 330
denying
fragments through ACLs, 282
traffic from a specific device, 283
design guidelines for firewall systems, 81
adhering to security policy, 81
DMZs, 85
internal DMZs, 90–91
multiple DMZs, 89
single DMZs, 87–89
traffic flow, 85–87
keeping it simple, 82
layered defense approach, 83–84
using the correct device, 82–83
designing security solutions, 34
Cisco security wheel, 35–37
destinations of logging messages
internal buffer logging, 710
line logging, 709–710
SNMP logging, 713
syslog server logging, 710–713
detecting
DoS attacks, 661–662
symptoms, 662–664
with ACLs, 665–672
with NetFlow, 672–676
intrusions with CBAC, 383
devices
amplifiers, 310
firewall component, 92
IDS component, 92–93
perimeter routers, 91
placement of firewall components, 94
enhanced firewall system design, 96–98
simple firewall system design, 95–96
token cards, 115–116
Cisco Secure ACS authentication server support, 117
synchronization with token card server, 117
VPNs component, 92
DHCP, disabling, 171

directed broadcasts
- disabling, 176, 311
- filtering, 311–313

disabling
- directed broadcasts, 311
- ICMP unreachables for black hole routes, 599

disabling unnecessary services, 815–817
- global services, 161
  - BootP, 170
  - CDP, 162–163
  - configuration autoloading, 172–173
  - DHCP, 171
  - DNS name resolution, 169–170
  - finger, 164–165
  - FTP, 167
  - HTTP, 167
  - IdentD, 165
  - IP source routing, 166
  - PAD, 172
  - SNMP, 168–169
  - TCP small servers, 163–164
  - TFTP, 167
  - UDP small servers, 163–164
- interface services, 173
  - directed broadcasts, 176
  - ICMP messages, 177–180
  - MOP, 181
  - Proxy ARP, 174–176
  - unused interfaces, 182
  - VTYs, 181–182
- with AutoSecure, 184
  - forwarding plane, 186
  - management plane, 185

disaster recovery plans, 11–12

discovering intended amplification attack victims, 313–314

displaying
- address translation statistics, 502–503
- connection timeouts for local access, 121
- sequence numbers in log messages, 714–715

distributed timed ACLs, 287–288

distribution of time, configuring, 722–723

DMZs, 85
- internal DMZ designs, 90–91
- multiple DMZ designs, 89
- single DMZ designs, 87, 89
- traffic flow, 85–87

DNS doctoring, 479

DNS name resolution, disabling, 169–170

DoS attacks, 31–33
- detecting, 661–662
  - with ACLs, 665, 667–672
  - with NetFlow, 672–676
- fraggle, preventing with ACLs, 310–311
- Land.c, 304
- preventing with CBAC, 33–34, 389–390, 690
- rate limiting, 692
  - CAR, 694–698
  - ICMP rate limiting, 692–693
  - NBAR, 700–703
- smurf
  - preventing with ACLs, 308, 310
  - via amplification, preventing, 311–313
- Smurf attacks, 677
- symptoms of, 662–664
- TCP SYN floods, preventing with ACLs, 307–308

downloading PDLMs, 457

dropped packets, logging, 279

dropping fragments, 283

dynamic ACLs. *See* lock-and-key ACLs

dynamic address translation, 477

dynamic crypto maps
- applying, 800
- creating, 799–800
- verifying, 800

dynamic NAT
- configuring, 487–488
- route maps, configuring, 515–519

dynamic translation of overlapping addresses
- configuring, 496–497

E

EasyVPN, 786
- EVS
  - RRI, 791–792
  - setup process, 793–802
- features, 787–789
- IPSec supportt, 787

eavesdropping attacks, 20–21

editing ACLs, 252–253

eDonkey, filtering, 346–347

egress filtering
  of bogon addresses, 305–307
  of ICMP traffic, 315–316
EIGRP (Enhanced IGRP), configuring MD5 authentication, 608
e-mail bombs, 28–31
embedded addressing information, 509–510
  ALG support, 511–512
  IP NAT Service, 512
    configuring, 513–514
  supported protocols, 511
embryonic connections, 13, 389
enable authentication, 217
enable secret command, 149
enabling security policies across diverse platforms, 6–7
encryption
  passwords, 152–153
  SCP, 231
    configuring, 231
    example of, 232–233
    troubleshooting, 232
  types of, 22
enforcing
  security policies, 11
  traffic filtering with NBAR, 447
enhanced features of CBAC, performance, 395
  connections per second, 396–397
  CPU utilization, 397
  throughput, 396
enhanced firewall system design, 96–98
enhancements to CBAC, 385
  application inspection, 389
  DoS detection and prevention, 389–390
  embedded addressing information, 387–388
  extra connections, 387
  ICMP traffic, 386
  TCP traffic, 385–386
  UDP traffic, 386
Error Log Count feature (Cisco IOS), 718
ESM (Embedded Syslog Manager), 705, 732–733
  configuring, 738–740
  filter modules, 733–734
    example, 737–738
    variables, 734–736
  input process, 734–735
evaluate statement, placement of in external ACLs, 372
EVC (EasyVPN client), 786
EVS (EasyVPN server), 786
  RRI, 791–792
  setup process, 793–799
examining
  log file contents, 742–743
  TCP control information, 57–59
examples
  of ACLs, 263–264
  of AP, 587, 589–594
  of authentication, 220–221
  of authorization, 225
  of BGP configuration, 620–624
  of CBAC
    inspection rules, 415–417
    three-interface CBAC, 418–422
    two-interface CBAC, 417–418
  of configuring basic authentication, 156–158
  of disabling unnecessary services on perimeter routers, 183–184
  of extended ACLs
    three-interface routers, 275–278
    two-interface routers, 273–275
  of fragment filtering, 283–285
  of IPSec remote-access, 802–805
  of IPSec site-to-site connections, 780–783
  of Java inspection, 426–428
  of lock-and-key ACLs, 563–564
  of NBAR, 463
    Code Red worm, 463–466
    Nimda, 466–467
  of NTP configuration, 731–732
  of PAM configuration, 405
  of RACLs, 374–375
    three-interface RACLs, 375–378
    two-interface RACLs, 375
  of RPF configuration, 631
  of SCP, 232–233
  of SLB configuration, 545–546
  of TCP Intercept configuration, 686–687
  of timed ACL configuration, 288–289
  of URL filtering, 443–444
exclusive domains, 431
  configuring, 435

extended ACLs, 264
- named extended, 273
- numbered extended, 264–266
  - filtering ICMP traffic, 271–272
  - filtering TCP traffic, 267–269
  - filtering UDP traffic, 269–271
- policies, configuring, 275
- three-interface router example, 275–278
- two-interface router example, 273–275
- versus RACLs, 352–356

extended address translation, 477

external threats, 17

F

FAB (Firewall ACL Bypass), 385

features
- of AP, 568–569
- of CBAC, performance enhancements, 395–397
- of EasyVPN, 787–789

feint attacks, 318

file-sharing applications, filtering, 332–333, 338–339
- AudioGalaxy, 345–346
- eDonkey, 346–347
- Gnutella, 343
- IMesh, 343–344
- Kazaa, 341–343
- Morpheus, 341–343
- Napster, 340–341
- WinMX, 344–345

filter modules (ESM), 733–734
- example, 737–738
- variables, 734–736

filtering
- ACL accounting information, 293–294
- Apple iChat application, 338
- bogon addresses with ACLs
  - egress filtering, 305–307
  - ingress filtering, 302–305
- directed broadcasts, 311, 313
- file-sharing applications, 338–339
  - AudioGalaxy, 345–346
  - eDonkey, 346–347
  - Gnutella, 343
  - IMesh, 343–344
  - Kazaa, 341–343
  - Morpheus, 341–343
  - Napster, 340–341
  - WinMX, 344–345
- ICQ applications, 334–335
- IM applications, 332–334
- Java, 426–428
- marked traffic (NBAR), 459
- MSN Messenger applications, 335
- returning traffic with RACLs, 359–360
- URLs, 428
  - advantages of, 430–431
  - alerts, 437
  - audits, 438–439
  - cache, clearing, 434
  - configuring, 432–434
  - example, 443–444
  - exclusive domains, 435
  - logging, 439
  - maximum requests, 436
  - maximum responses, 436
  - operation, 429–430
  - restrictions, 431–432
  - troubleshooting, 442
  - verifying, 440–441
- web traffic
  - Code Red worm, 463–466
  - Nimda, 466–467
- with ACLs, 237–238, 259–260
  - conditions, 241
  - example, 238
  - extended, 264–278
  - matches, 241
  - placement of, 248–249
  - rules, 246–247
  - standard, 260–264
  - statement order, 243–246
- with CBAC, 382–383
- with NBAR, 447
- Yahoo! Messenger applications, 336–338

finger, disabling, 164–165

firewalls systems, 43
- address translation, 72
  - advantages of, 75
  - applications of, 76

filtering process, 72–75
limitations of, 75–76
administering, 101
AGFs, 64
advantages of, 70
applications of, 72
authentication methods, 66–67
authentication process, 65–66
CGFs, 67–68
cut-through proxy firewalls, 69–70
limitations of, 70–71
component placement, 94
design considerations, 98–99
enhanced firewall system design, 96–98
simple firewall system design, 95–96
content filtering, 81
defining, 42
design guidelines, 81
adhering to security policy, 81
DMZs, 85–91
keeping it simple, 82
layered defense approach, 83–84
using the correct device, 82–83
host-based, 76
advantages of, 77–78
applications of, 79
hybrid, 79–80
intrusion-detection, 80
packet-filtering, 47–48
activating, 51
advantages of, 51
applying rules, 48
examining TCP control information, 58–59
filtering decisions, 49–50
limitations of, 52–53
typical applications, 53
stateful, 53–54
advantages of, 61
advantages over packet-filtering firewalls, 54
applications of, 64
limitations of, 61–64
non-stateful protocols, 62
state table, 59–60
flags, 57
flexibility of CBAC configuration, 385
forwarding plane (AutoSecure), 186
fraggle attacks, preventing with ACLs, 310–311
Fraggle DoS attack, 662
fragments, 280–281
configuring CBAC inspection rules, 409
dropping, 283
filtering, 281–282
example, 283–285
on stateful firewalls, 281
FTP, disabling, 167
functions of AAA, 202

G

generating SNMP traps, 141
global adresses, 476
global services, disabling, 161
BootP, 170
CDP, 162–163
configuration autoloading, 172–173
DHCP, 171
DNS name resolution, 169–170
finger, 164–165
FTP, 167
HTTP, 167
IdentD, 165
IP source routing, 166
PAD, 172
SNMP, 168–169
TCP small servers, 163–164
TFTP, 167
UDP small servers, 163–164
Gnutella, filtering, 343
goals of security, 7
group classifications, defining for NBAR, 454–455

H

H.323, CBAC support, 392–393
handler (DDoS attacks), 317
hardware clock, 719
headless chicken syndrome, 12
host-based firewalls, 76
advantages of, 77
limitations of, 78–79

host-based IDS solutions, 94, 639
host-specific entries (PAM), 402
HSRP (Hot Standby Router Protocol), 614
    MD5 authentication, configuring, 615–616
    SNAT configuration, 527–528, 530–531
    static NAT redundancy, 522–526
HTTP traffic fitltering
    access to Cisco routers, configuring 128–130
    CBAC inspection rules, configuring, 407–408
    disabling, 167
    NBAR configuration, 457
HTTPS, configuring access to Cisco routers, 130–131
    with CA, 134–139
    with no CA, 132–134
hybrid firewalls, 79–80

I

IANA (Internet Assigned Numbers Authority) web site, 301
ICMP (Internet Control Message Protocol)
    CBAC handling of, 386
    configuring CBAC inspection rules, 407
    disabling, 177–180
    egress traffic filtering, 315–316
    ingress traffic filtering, 315
    mask replies, disabling, 180
    rate limiting, 692–693
    redirects, disabling, 178–179
    traffic filtering with numbered extended ACLs, 271–272
    unreachables, disabling, 177–178
        for black hole routes, 599
ICQ (instant messaging) applications
    filtering, 334–335
IdentD, disabling, 165
idle timer (lock-and-key), 556
IDS (intrusion detection systems), 92–93
    anomoly-based, 93
    Cisco IOS IDS, 644
        configuring, 652–654, 656
        example configuration, 658–659
        performance issues, 652
        signature support, 645–650
        verifying configuration, 657–658
    configuring on perimeter routers, case study, 832
    false positives, 656
    host-based solutions, 94, 639
    installed components, 640
    network-based solutions, 94, 638–639
    profiles, 636
    responses to intrusions, 641
    signature-based solutions, 93
    signatures, 637, 642
        categories of, 643–644
        implementing, 642
        structures, 642–643
IGPs (interior gateway protocols)
    authentication, 604
        MD5, 606
        plain-text, 605
    EIGRP, MD5 authentication, 608
    IS-IS, MD5 authentication, 609–611
    OSPF. MD5 authentication, 608–609
    RIP, MD5 authentication, 606–607
IM (instant messaging) applications, filtering, 332–334
IMesh, filtering, 343–344
implementing firewall features, 101
importance of monitoring, 36
include-local-lan command, 796
informs (SNMP), generating, 141
ingress filtering
    of bogon addresses, 302–305
    of ICMP traffic, 315
insecure CDP interfaces, disabling, 173
inserting entries in sequenced ACLs, 300–301
inspection rules, CBAC, 383, 405–406
    activating, 410
    example configuration, 415–417
    fragments, 409
    HTTP traffic, 407–408
    ICMP traffic, 407
    RPCs, 408
    Skinny, 409
    SMTP traffic, 408
    TCP/UDP traffic, 406–407
intended amplification attack victims, discovering, 313–314

interface services, disabling, 173
- directed broadcasts, 176
- ICMP messages, 177–180
  - mask replies, 180
  - redirects, 178–179
  - unreachables, 177–178
- MOP, 181
- Proxy ARP, 174–176
- unused interfaces, 182
- VTYs, 181–182

internal buffer logging, 710

internal routers
- ACL configuration, case study, 823–825
- basic configuration, case study, 814
- CBAC configuration, case study, 827
- in corporate office, 811

internal threats, 17

intrustion detection, 80
- CBAC, 383

ip access-list log-update threshold command, 291

IP accounting, ACL configuration, 292–293
- defining thresholds, 294
- filtering accounting information, 293–294
- limiting transit records, 294–295

IP address spoofing, preventing with RPF, 625–627

IP blocking, 33

ip http secure-client-auth command, 136

ip inspect dns-timeout command, 401

ip inspect tcp finwait-time command, 401

ip inspect tcp idle-time command, 401

ip inspect tcp synwait-time command, 401

ip inspect udp idle-time command, 401

ip nat pool command, 496

IP NAT Service, 512
- configuring, 513–514

ip nbar port-map command, 453

ip slb serverfarm command, 541

IP source routing, disabling, 166

IPSec
- EasyVPN support, 787
- EVS
  - remote-access verification, 802
  - setup process, 793–800
- remote access, 785–786
  - connection process, 789–793
  - example, 802–805
- site-to-site connections
  - configuring, 747–748
  - example, 780–783
  - external ACL, configuring, 749
  - IKE phase 1, 750–765
  - IKE phase 2, data connection, 766–774
  - troubleshooting, 775–780

IRC (Internet Relay Chat) servers, susceptibility to smurf attacks, 310

IRR (Internet Routing Registry), 314

IS-IS (Intermediate System-to-Intermediate System), configuring MD5 authentication, 609–611

J

Java filtering, CBAC inspection
- configuring, 426
- example, 426–428

JavaScript, enabling for AP connections, 572–573

K

Kazaa, filtering, 341, 343

keystroke-capturing programs, 113

KISS principle, firewall system design guideline, 82

L

L2L *See* IPSec, site-to-site connections.

Land.c, 32, 304

LANguard Network Security Scanner, 19

layered defense approach to firewall system design, 83–84

layers of OSI reference model, 46

limitations
- of address translation, 484
- of AP, 574–575
- of CBAC, 397–398
- of NBAR, 451
- of RACLs, 361
  - application issues, 362
  - FTP, 363
  - passive FTP, 364
  - stateful issues, 362

of RPF for spoofing prevention, 628
of SLB, 540
of SNAT, 526
limiting ACL accounting transit records, 294–295
line logging, 709–710
link encryption, 22
load balancing, 482. *See also* traffic distribution
SLB, 536–537
algorithms used, 538
configuring, 541–544
example configuration, 545–546
features, 539–540
limitations, 540
real server attributes, 542–543
verifying configuration, 544
virtual server attributes, 543–544
local access to Cisco routers, 118–119
authentication methods, 120
via auxiliary line, 119
via console port, 118
local adresses, 476–477
local authentication database, 150–152
locating source of amplification attacks, 313–314
lock-and-key ACLs, 551–552
configuring, 555–560
example, 563–564
operation, 553–554
remote administration access, 560–562
troubleshooting, 562–563
versus AP, 569
when to use, 552
logging, 705
CBAC
alerts, 414
audits, 414
configuring, 706
destinations, 708
displaying sequence numbers, 714–715
dropped packets, 279
Error Log Count feature (Cisco IOS), 718
ESM, 733
configuring, 738–740
filter modules, 733–738
input process, 734–735
examining log file contents, 742–743
internal buffer logging, 710
line logging, 709–710
rate limiting, 715–716
severity levels, 708–709
show logging command, 716–717
show logging history command, 717
SNMP logging, 713
synchronous logging, configuring, 706–708
syslog server logging, 710–713
timestamping messages, 714
updates
adding to ACLs, 291
threshold, changing, 291–292
URL filtering messages, 439
violations, accounting on ACLs, 292–293
accounting thresholds, defining, 294
filtering accounting information, 293–294
transit records, limiting, 294–295
logging synchronous line configuration command, 118
login authentication, 216–217
login banners, 153–154, 218–219
configuring, 154–156
login connection timeouts, overriding, 120–121

M

management plane (AutoSecure), 185
managing firewall systems, 101
manual time and date configuration, 720–722
maps, creating, 800
mask replies (ICMP), disabling, 180
masquerading attacks, 26
MD5 authentication, configuring, 606
BGP, 606, 617
EIGRP, 608
HSRP, 615–616
IS-IS, 609–611
OSPF, 608–609
RIP, 606–607
method lists, 214–215
Microsoft RPC service, susceptibility to worms, 330–332
misconfiguration of CBAC, preventing, 399

monitoring
  importance of, 36
  rcp command usage with ACLs, 327
MOP, disabling, 181
Morpheus, filtering, 341, 343
MOTD banners, creating AP authentication banners, 582–583
MSN Messenger applications, filtering, 335

N

Nachi worm, 331
named extended ACLs, 273
named standard ACLs, 262–263
Napster, filtering, 340–341
NAT (Network Address Translation), 474–475, 477
  configuring, 484–486
  Default Inside Server, 491
  dynamic NAT, configuring, 487–488
  global addresses, 476
  local addresses, 476–477
  overlapping addresses, 479
  static NAT, redundancy with HSRP, 522–526
  troubleshooting with debug ip nat command, 504
  with CBAC, configuring, 505–507
NBAR, 444
  configuring, 451–453
  examples, 463
    Code Red worm, 463–466
    Nimda, 466–467
  group classifications, configuring, 454–455
  HTTP traffic filtering, configuring, 457
  limiting DoS attack damage, 700–703
  marked traffic, filtering, 459
  P2P program filtering
    configuring, 455–456
    example, 467, 469
  PDLMs, 450
    downloading, 457
  policies, configuring, 458
  policy maps, associating with router interface, 459
  restrictions, 451
  supported protocols and applications, 447–450
  traffic classification, 445–446
  traffic filtering, 447
  verifying configuration, 460–463
Nessus, 19
NetFlow, detecting DoS attacks, 672–676
network-based IDS solutions, 94, 638–639
Nimda, filtering, 466–467
no ip inspect command, removing CBAC from router, 415
no password authentication, 111–112
non-stateful protocols, 62
notifications (SNMP), 141
NTP (Network Time Protocol)
  configuring on perimeter routers, case study, 835
  example configuration, 731–732
null interfaces, black hole routes, 598
  configuring, 599, 601
numbered extended ACLs, 264–266
  ICMP traffic, filtering, 271–272
  TCP traffic, filtering, 267–269
  UDP traffic, filtering, 269–271
numbered standard ACLs, 261–262

O

opening ports with packet-filtering firewalls, 56
operating systems, weaknesses in, 14
OSI reference model, 45–46
OSPF (Open Shortest Path First), configuring MD5 authentication, 608–609
OTPs (one-time passwords), 114–115
  susceptibility to eavesdropping attacks, 115
overlapping addresses
  address translation, configuring, 493
    dynamic translation, 496–497
    static translation, 494–496
  DNS doctoring, 479
overriding login connection timeouts, 120–121

P

P2P program filtering
  AudioGalaxy, 345–346
  eDonkey, 338–339, 346–347

Gnutella, 343
IMesh, 343–344
Kazaa, 341–343
Morpheus, 341–343
NBAR configuration, 455–456, 467–469
Napster, 340–341
WinMX, 344–345
packet encryption, 22
packet filtering
ACLs
accounting information, filtering, 293–294
accounting thresholds, defining, 294
logging updates, 291–292
logging violations, accounting, 292–293
remarks, adding, 290
transit records, limiting, 294–295
denying traffic from a specific device, 283
fragments, 281–282
dropping, 283
example, 283–285
sequenced ACLs
configuring, 296–298
deleting entries, 299
inserting entries, 300–301
resequencing, 298–299
timed ACLs, 285
activating time ranges, 287
creating time ranges, 285–287
distributed, 287–288
example configuration, 288–289
turbo ACLs, 295–296
packet fragmentation and reassembly attacks, 32
packet sniffers, 21
Packet Storm website, 317
packet-filtering firewalls, 47–48
activating, 51
advantages of, 51
applying rules, 48
examining TCP control information, 58–59
filtering decisions, 49–50
limitations of, 52–53
opening ports, 56
typical applications, 53
packets
dropped, logging, 279
fragments, 280–281
CBAC inspection rules, configuring, 409
filtering, 282
PAD (packet assember/disassembler), disabling, 172
PAM (Port Application Mapping), 401
configuring, 403
entry types, 402
example configuration, 405
verifying configuration, 404
PAR (port address redirection), configuring, 491–493
passive interfaces, securing routing protocols, 612–613
passive-interface command, 613
passwords
clear-text, 118–119
encrypting, 152–153
prompts, 218
PAT (Port Address Translation), 480–481
configuring, 489–491
PBR (policy-based routing), black hole routing, 601–604
PDLMs (Packet Description Language Modules), 450
downoading, 457
PenguiNet SSH, 124
performance of CBAC, 395
connections per second feature, 396–397
CPU utilization, 397
throughput performance feature, 396
perimeter routers, 91
AAA configuration, case study, 817–820
ACL configuration, case study, 820–823
address-translation configuration, case study, 827–830
basic configuration, case study, 813–814
CBAC configuration, case study, 825–826
thresholds, 833
IDS configuration, case study, 832
in corporate office, 809, 811
NTP configuration, case study, 835
rate limiting configuration, case study, 833–834
remote-access VPN configuration, case study, 839, 841–842
restricting
access to, 111
command execution, 223–224
RPF configuration, case study, 831

- site-to-site VPN configuration, case study, 836–838
- static route configuration, case study, 830
- sylog configuration, case study, 836
- unnecessary services, disabling, 183–184

periodic command, creating time ranges, 286–287

personal firewalls, 76
- advantages of, 77
- applications of, 79
- limitations of, 78

ping of death attacks, 32

placement
- of ACLs, 248–249
- of firewall components, 94
  - design considerations, 98–99
  - enhanced firewall system design, 96–98
  - simple firewall system design, 95–96

plain-text authentication of routing protocols, 605

planning for security, 6

policies
- AP, activating, 580–581
- configuring with extended ACLs, 275
- enabling across diverse platforms, 6–7
- enforcing, 11
- weaknesses in, 9–10
  - lack of change management, 11
  - lack of disaster recovery plan, 11–12

policy maps
- associating with router interface, 459
- defining for NBAR, 458

poll-based NTP configuration, 724

ports, opening with packet-filtering firewalls, 56

port-scanning utilities, 19

preventing
- amplification attacks
  - disabling directed broadcasts, 311
  - filtering directed broadcasts, 311, 313
- CBAC misconfiguration, 399
- DoS attacks, 33–34
- eavesdropping attacks, 21
- fraggle attacks with ACLs, 310–311
- reconnaissance attacks
  - egress ICMP traffic filtering, 315–316
  - ingress ICMP traffic filtering, 314–315
- session attacks, 28–29
- smurf attacks with ACLs, 308, 310
- spoofing with RPF, 625–628
- TCP SYN flood attacks
  - with TCP Intercept, 679–686
  - with ACLs, 307–308

private addresses, 473–474

privileged EXEC access, 146
- assigning privilege levels, 146–149
- local authentication database, 150–152
- password levels, 149–150
- passwords, 146
- securing shell access, 217

processing ACLs, 241
- conditions, 241
- matches, 241
- rules, 246–247
- tatement order, 243–246

profile-based IDS systems, 636

protocols supported by CBAC, 390
- H.323, 392–393
- RTSP, 390
- SIP, 394–395
- Skinny, 393–394

Proxy ARP, disabling, 174–176

Q-R

QoS, NBAR classification, 445–446

RACLs (reflexive ACLs), 351. *See also* CBAC
- and CBAC, 423
- building, 358
- configuring, 365, 368–374
  - interface selection, 365–368
- examples of, 374–375
  - three-interface RACLs, 375–378
  - two-interface RACLs, 375
- filtering returning traffic, 359–360
- limitations of, 361
  - application issues, 362
  - FTP, 363
  - passive FTP, 364
  - stateful issues, 362
- removing entries, 360–361
- traffic processing, 357
- versus extended ACLs, 352–356

RADIUS (Remote Access Dial-In User Service)
- centralizing AAA security policies, 205–208
  - server groupings, 208
  - server protocol example configuration, 211–212
- limitations of, 206
- troubleshooting, 210
- versus TACACS+, 212–213

radius-server host command, 207

radius-server timeout command, 207

rate limiting, 692
- configuring on perimeter routers, case study, 833–834
- ICAR, 694–698
- ICMP rate limiting, 692–693
- log messages, 715–716
- NBAR, 700–703

rcp command, monitoring use with ACLs, 327

reconnaissance attacks, 19, 314
- eavesdropping attacks, 20–21
- keystroke-capturing programs, 113
- preventing
  - with egress ICMP traffic filtering, 315–316
  - with ingress ICMP traffic filtering, 315
  - with traceroute, 316
- scanning attacks, 19–20

redirects (ICMP), disabling, 178–179

remarks (ACLs), 251
- adding, 290

remote access to Cisco routers, 121
- lock-and-key secured routers, 560–562
- privileged EXEC access, 146
  - assigning privilege levels, 146–149
  - local authentication database, 150–152
  - password levels, 149–150
  - passwords, 146
- via HTTPS, 130–139
  - configuring with CA, 134–139
  - configuring with no CA, 132–134
  - HTTPS connection components, 131
- via SNMP, 139–141
  - v1 and v2 configuration, 141–143
  - v3 configuration, 143–145
- via SSH, 123
  - client connections, 127
  - server configuration, 124–125
  - server example, 126
- via VTY lines, 121, 123
- via web browser, 127–130

remote access VPNs, Easy VPNs, 786
  - features, 787–789
  - IPSec support, 787

remote-access connection process (IPSec), 789–793

remote-access VPNs, configuring on perimeter routers, case study, 839–842

removing
- ACL entries, 261
- CBAC from router, 415
- IPSec connections from router, 780
- RACL entries, 360–361
- translation table entries with clear command, 503–504

repudiation attacks, 28

rerouting attacks, 32

resequencing sequenced ACLs, 298–299

restricting
- access to perimeter routers, 111
- command execution on perimeter router, 223–224
- NTP resources, 728

RFC 1631, address translation, 474

RIP, configuring MD5 authentication, 606–607

rotating syslog files, 741

route flap dampening, configuring on BGP, 618–619

route maps, controlling address translation, 517
- with dynamic NAT, 515–519
- with static NAT, 520–521

router time sources
- hardware clock, 719
- software clock, 719

routing protocols
- BGP, 617
  - MD5 authentication, configuring, 617
  - route flap dampening, configuring, 618–619
  - secure configuration example, 620–624
- EIGRP, MD5 authentication, 608
- IGPs
  - authentication, 604

MD5 authentication, 606
plain-text authentication, 605
IS-IS, MD5 authentication, 609–611
OSPF, MD5 authentication, 608–609
RIP, MD5 authentication, 606–607
securing
with ACLs, 613–614
with passive interfaces, 612–613
RPCs (Remote Procedure Calls), configuring CBAC inspection rules, 408
RPF (reverse-path forwarding), 626
configuring, 629, 831
limitations of, 628
per-interface statistics, 627
preventing IP spoofing, 625–627
verifying configuration, 630–631
RRI (reverse route injection), 791–792
RTSP, CBAC support, 390

S

save-password command, 796
scanning attacks, 19–20
SCEP (Simple Certificate Enrollment Protocol), 758
SCP (secure copy), 231
configuring, 231
example of, 232–233
troubleshooting, 232
SDM (Security Device Manager), 99
security authentication failure rate command, 198
security passwords min-length command, 198
security wheel, 35–37
segments (TCP), fragmentation, 280–281
sequenced ACLs
configuring, 296–298
deleting entries, 299
inserting entries, 300–301
resequencing, 298–299
services, blocking, 332–333
Apple iChat, 338
ICQ, 334–335
IM, 333–334
MSN Messenger, 335
Yahoo! Messenger, 336–338
session attacks, 25–29
masquerading attacks, 26
preventing, 28–29
repudiation attacks, 28
session-hijacking attacks, 26–27
session-replay attacks, 26
session-hijacking attacks, 26–27
session-replay attacks, 26
severity levels of logging messages, 708–709
show access-list compiled command, 295–296
show commands
troubleshooting AP, 584–586
troubleshooting CBAC, 411–413
verifying address translation, 501–502
verifying URL filtering configuration, 440–441
show ip http server secure status command, 137
show logging command, 716–717
show logging history command, 717
show ntp associations command, 730
show ntp status command, 730–731
show privilege command, 150
show sntp command, 731–732
show tacacs command, 209
shunning, 33
signature-based IDS solutions, 93
signatures, 637, 642
categories of, 643–644
implementing, 642
structures, 642–643
simple address translation, 477
simple CBAC example, 415–417
simple firewall system design, 95–96
SIP (Session Initiation Protocol), CBAC support, 394–395
site-to-site VPNs, configuring on perimeter routers, case study, 836–838
Skinny protocol
CBAC support, 393–394
configuring CBAC inspection rules, 409
SLB (Server Load Balancing), 536–537
configuring, 541–544
example configuration, 545–546
limitations of, 540
load balancing algorithms, 538
load balancing features, 539–540

verifying configuration, 544
real server attributes, 542–543
virtual server attributes, 543–544
SMTP (Simple Mail Transfer Protocol), configuring CBAC inspection rules, 408
smurf attacks, 32, 661, 677
preventing with ACLs, 308–310
preventing with amplification
disabling directed broadcasts, 311
filtering directed broadcasts, 311–313
SNAT (stateful NAT), 526
configuring with HSRP, 527–531
configuring without HSRP, 531–534
verifying configuration, 534–535
SNMP (Simple Network Management Protocol)
disabling, 168–169
logging, 713
remote access to Cisco routers, 139–141
v1 and v2 configuration, 141–143
v3 configuration, 143–145
traps, specifying destinations, 145
snmp-server community command, 141
snmp-server group command, 144
SNTP (Simple Network Time Protocol), 723
authentication, 728–729
broadcast-based configuration, 725
client configuration, 723
configuring, 725
poll-based configuration, 724
restricting resources, 728
server configuration, 725–727
social engineering, 23
SOCKS traffic, filtering with NBAR, 469
software clock, 719
sources of amplification attacks, locating, 313–314
spamming, 28
spoofing, preventing with RPF, 625–627
SQL Slammer worm, 328–329
SSH (Secure Shell)
DoS attacks, vulnerability of Cisco IOS Software, 127
remote access to Cisco routers, 123
client connections, 127
server configuration, 124–125
server example, 126
SSL (Secure Sockets Layer), configuring remote access to Cisco routers, , 130–139
Stacheldraht attacks, blocking, 322–323
standard ACLs, 260
examples of, 263–264
named standard ACLs, 262–263
numbered standard ACLs, 261–262
starting up AutoSecure, 187–188
state table
CBAC, changing connection timeouts, 400–401
stateful firewalls, 59–60
stateful firewalls, 53–54
advantages of, 61
advantages over packet-filtering firewalls, 54
applications of, 64
fragments, filtering, 281
limitations of, 61
multiple application connections, 63
non-stateful protocols, 62
state table size, 64
state table, 59–60
static address translation, 477
static crypto maps, configuring, 801
static NAT
redundancy with HSRP, 522–526
route maps, configuring, 520–521
static password authentication, 112–113
static routing, 597–598
configuring on perimeter routers, case study, 830
static translation of overlapping addresses, configuring, 494–496
statistics of address translation, displaying, 502–503
structured threats, 17
subnet masks, converting to wildcard masks, 254–256
supported protocols on CBAC, 390
H.323, 392–393
RTSP, 390
SIP, 394–395
Skinny, 393–394
sylog, configuring on perimeter routers, case study, 836
symptoms of DoS attacks, 662–664
synchronous logging, configuring, 706–708
syslog files, rotating, 741
syslog server logging, 710–713
System-defined entries (PAM), 402

T

TACACS+
- centralizing AAA security policies, 203–205
  - server groupings, 208
  - server protocol example configuration, 211–212
- troubleshooting, 209–210
- versus RADIUS, 212–213

tacacs-server host command, 205

TCP (Transmission Control Protocol)
- CBAC handling of, 385–386
- configuring CBAC inspection rules, 406–407
- control information, examining, 57–59
- segments, fragmentation, 280–281
- traffic filtering with numbered extended ACLs, 267–269
- weaknesses in, 13

TCP Intercept, 679
- example, 686–687
- preventing TCP SYN flood attacks, 679–686

TCP small servers, disabling, 163–164

TCP SYN flood attacks, 32, 662
- preventing with ACLs, 307–308

technologies, weaknesses of, 13
- network equipment, 15
- network protocols, 13
- operating systems, 14–15

TFN (tribe flood network) attacks, 319
- blocking, 320

TFN2k (tribe flood network 2K) attacks, blocking, 320

TFTP (Trivial File Transfer Protocol), disabling, 167

threats, types of, 17

three-interface CBAC, example configuration, 418–422

three-interface RACLs, example, 375–378

threshold of ACL logging, changing, 291–294

throughput performance feature of CBAC, 396

time and date configuration, 720–722

time-based authentication, 115

timed ACLs, 285
- activating time ranges, 287
- creating time ranges, 285
  - with absolute command, 286
  - with periodic command, 286–287
- distributed, 287–288
- example configuration, 288–289

timeout limits, translation table configuration, 500–501

timestamping logging messages, 714

TIS Firewall Toolkit, 48

token card services, 115–117

traceroute, preventing reconnaissance attacks, 316

tracking intended amplification attack victims and perpetrators, 313–314

traffic classification, implementing with NBAR, 445–446

traffic distribution, 482
- configuring, 498–499

traffic filtering, 237–238, 259–260
- ACL processing, 241
  - conditions, 241
  - matches, 241
  - rules, 246–247
  - statement order, 243–246
- example, 238
- CBAC, 382–383
- extended ACLs, 264
  - named extended ACLs, 273
  - numbered extended ACLs, 264–272
  - three-interface router example, 275–278
  - two-interface router example, 273–275
- implementing with NBAR, 447
- placement of ACLs, 248–249
- RACLs
  - configuring, 365–374
  - examples of, 374–378
  - filtering returning traffic, 359–360
  - limitations of, 361
    - application issues, 362
    - FTP, 363–364
    - stateful issues, 362
  - removing entries, 360–361
- standard ACLs, 260
  - examples of, 263–264
  - named standard ACLs, 262–263
  - numbered standard ACLs, 261–262

traffic inspection, CBAC, 383

transform sets, 131
- creating, 800

transit records for ACL accounting, limiting, 294–295

translation tables
- connection limits, configuring, 500
- removing entries with clear commands, 503–504
- timeout limits, configuring, 500–501

traps
- generating, 141
- specifying destinations, 145

Trinity attacks, blocking, 324

Trinoo attacks, blocking, 321–322

Trojan horses, 29–31, 325
- blocking with ACLs, 325–326
- detecting, 325
- monitoring rcp command usage with ACLs, 327

troubleshooting
- accounting with debug aaa accounting command, 230
- address translation with debug ip nat command, 504
- AP
  - with clear commands, 587
  - with debug commands, 587
  - with show commands, 584–586
- authentication, 219
  - with debug aaa authentication, 220
- authorization, 224
- CBAC, 410
  - with debug commands, 413–415
  - with show commands, 411–413
- CRLs, 762
- IPSec site-to-site connections, 775–778
  - debug commands, 778–780
- lock-and-key ACLs, 562–563
- RADIUS, 210
- SCP, 232
- TACACS+, 209–210
- URL filtering, 442

tuning AP performance, 582–583

turbo ACLs, 295
- configuring, 295–296

two-interface CBAC, example configuration, 417–418

two-interface RACLs, example of, 375

U

UAPs (user authorization profiles), 578

UDP (User Datagram Protocol)
- CBAC handling of, 386
- configuring CBAC inspection rules, 406–407
- traffic filtering with numbered extended ACLs, 269–271

UDP small servers, disabling, 163–164

unauthorized access attacks, 23–24

unicast RPF
- configuring, 629
- example configuration, 631
- preventing IP spoofing, 625–627
  - limitations, 628
  - per-interface statistics, 627
- verifying configuration, 630–631

unidirectional connections
- filtering, RACLs, 351

unnecessary services, disabling, 815–817
- global services, 161
  - BootP, 170
  - CDP, 162–163
  - configuration autoloading, 172–173
  - DHCP, 171
  - DNS name resolution, 169–170
  - finger, 164–165
  - FTP, 167
  - HTTP, 167
  - IdentD, 165
  - IP source routing, 166
  - PAD, 172
  - SNMP, 168–169
  - TCP small servers, 163–164
  - TFTP, 167
  - UDP small servers, 163–164
- interface services, 173
  - directed broadcasts, 176
  - ICMP messages, 177–180
  - MOP, 181
  - Proxy ARP, 174–176
  - unused interfaces, 182
  - VTYs, 181–182
- with AutoSecure feature, 184
  - forwarding plane, 186
  - management plane, 185

unreachables (ICMP), disabling, 177–178
  for black hole routes, 599
unstructured threats, 17
unused interfaces, disabling, 182
URL filtering, 428
  advantages of, 430–431
  alerts, 437
  audits, 438–439
  cache, clearing, 434
  configuring, 432–434
  example, 443–444
  exclusive domains, configuring, 435
  logging, 439
  maximum requests, 436
  maximum responses, 436
  operation, 429–430
  restrictions, 431–432
  troubleshooting, 442
  verifying, 440–441
user EXEC access
  local access, 118–119
    authentication methods, 120
    via auxiliary line, 119
    via console port, 118
  remote access, 121
    via HTTPS, 130–139
    via SNMP, 139–145
    via SSH, 123–127
    via VTY lines, 121, 123
    via web browser, 127–130
  securing shell access, 216–217
User-Defined Custom Application Classification feature (NB AR), 453
User-Defined Custom Application Classification feature (NBAR), 453
user-defined entries (PAM), 402
username and password prompts, 218

V

verifying
  ACL configuration, 278–280
  address translation with show commands, 501–502
  AutoSecure configuration, 198
  CBAC configuration, 410
    with debug commands, 413–415
    with show commands, 411–413
  Cisco IOS IDS configuration, 657–658
  dynamic crypto maps, 800
  NBAR configuration, 460–463
  PAM configuration, 404
  RPF configuration, 630–631
  SLB configuration, 544
  SNAT configuration, 534–535
  URL filtering configuration, 440–441
viruses, 29–31
  worms, 327
    Deloder worm, 330
    Microsoft RPC service, susceptibility to, 330–332
    SQL Slammer worm, 328–329
VPNs, 92, 786–789
VTY lines
  configuring access to Cisco routers, 119
  disabling, 181–182
  login connection timeouts, overriding, 120–121
  remote access to Cisco routers, 121–123

W

W32.Blaster worm, 676
W32.Welchia worm, 331
watch lists, configuring, 583–584
weaknesses
  in computer technologies, 13
    network equipment, 15
    network protocols, 13
    operating systems, 14–15
  in equipment configurations, 15–16
  in policy definitions, 9–10
    lack of change management, 11
    lack of disaster recovery plan, 11–12
web browsers, remote access to Cisco routers, 127–130
web traffic
  Code Red worm, filtering, 463–466
  Java inspection, 426–428
  Nimda, filtering, 466–467
  URL filtering, 428
    advantages of, 430–431

        alerts, 437
        audits, 438–439
        configuring, 432–435
        example, 443–444
        logging, 439
        maximum requests, 436
        maximum responses, 436
        operation, 429–430
        restrictions, 431–432
        troubleshooting, 442
        verifying, 440–441
websites
    IANA, 301
    Packet Storm, 317
wildcard masks (ACLs), 254–256
WinMX, filtering, 344–345
WinNuke, 33
worms, 29–31, 327
    Code Red, 676–677
    Deloder worm, 330
    Microsoft RPC service, susceptibility to, 330–332
    Nachi, 331
    SQL Slammer worm, 328–329
    W32.Blaster, 676
    W32.Welchia, 331

X-Y-Z

Yahoo! Messenger, filtering, 336–338