INDEX

Numerics

3DES encryption, 311
802.1x port authentication, 114
    communications, 115–121
    configuring on Catalyst 6000 switches, 123–125
    functionality, 122

A

AAA (authentication, authorization and accounting)
  accounting, 469, 479
    method lists, applying, 481–482
    method lists, configuring, 479–481
  applying access lists, 486–488
  authentication, 470
    configuring, 471
    local database, configuring, 471
    method list, configuring, 471–474
  authorization, 469, 475
    method lists, applying, 477–479
    method lists, configuring, 475–476
  auth-proxy, 541–542, 544
  command authorization, configuring, 549–552
  debug commands, 670
  downloading routes, 486–488
  lock and key, configuring, 548–549
  method lists, 469
  network components, 470
  PPP
    authentication and authorization, 482–485
    timeouts, configuring, 488–489
  providing preshared keys for IPsec, 537, 539
  RADIUS, 515, 519–520, 522–530
    accounting, 531–533
    communications architecture, 516
    packet format, 517–518
    password encryption, 518–519
    router support, 521–531
  resolving common problems, 671–677
  show commands, 670
  TACACS+
    accounting, 508–512
    authentication, 498
    authorization, 499–507
    communications architecture, 494
    daemon functionality, 493–494
    header architecture, 495–497
    packet encryption, 497
  VPDN, 544, 546–547
  x-auth in ISAKMP, 539–541
acceptable usage policies, defining, 16
access control. *See also* CBAC
  PIX, 72
  switches, 75
access lists. *See* ACLs
access policies, defining, 16–17
Access-Accept messages (RADIUS), 519
accessing firewalls, vulnerabilities, 140
Access-Reject messages (RADIUS), 519
accountability policies, defining, 16
accounting, 479
  method lists
    applying, 481–482
    configuring, 479–481
  RADIUS, 515, 531–532
    IETF Accounting AV pairs, 532–533
  TACACS+, 508–512
ACEs (Access Control Elements), 567
ACKs, ZL ACKs, 248
ACLs (access control lists), 153. *See also* turbo ACLs
  applying to IP fragments, 583–584, 587–588
    overlapping fragment attacks, 589
    tiny fragment attacks, 588
  applying with AAA, 486–488
  blocking ICMP packets, 573–575
  blocking known offenders, 575
  blocking spoofed IP addresses, 575
  extended, 569, 571
  functionality, 567–568, 573
  impact on performance, 590
  implicit deny all entry, 571
  logging facility, 573
  NetFlow switching, 594–595
  restricting traffic, 572–573
  standard, 568

thwarting attacks
DoS attacks, 580–582
fraggle attacks, 578–579
smurf attacks, 576–578
SYN floods, 579–580
top-down processing, 571
active routers (HSRP), 43
addressing, NAT
debugs, 626–627
order of operations, 625–626
PIX Firewall capabilities, 155
resolving common problems, 629–633
show commands, 627–629
advanced PIX Firewall features
alias, 159
configuring, 185–188
DNS doctoring, 161–162
DNS guards, 165
flood guards, 162
frag guards, 163–164
fragment handling, 174–175
mail guards, 164
multicast support, 172
multimedia support, 166
protocol fixup, 168–169
spoof detection, 168
sysopt commands, 169–172
traffic filtering, 165
URPF, 168
Advertisement Interval field (VRRP packets), 53
aggressive mode (IKE) exchanges, 278
using preshared key authentication, 302–306
AH (Authentication Header), 317
integrity checking, 312–313
Alarm messages (POP), 432
alarms
corresponding severity levels, 447–448
false positives, 449
signatures, customizing, 463–465
alias feature (PIX Firewall), 159
configuring, 185–188
DNS doctoring, 161–162
frag guards, 164
applets (Java), blocking, 203
appliance sensors
event logging, 439–441
IP session logging, 441
application layer inspection, Cisco IOS Firewall, 202
application layer VPNs, 219
applying
ACLs
overlapping fragment attacks, 589
tiny fragment attacks, 588
to ICMP packets, 573–575
to IP fragments, 583–584, 587–588
to known IP addresses, 575
to spoofed IP addresses, 575
with AAA, 486–488
method lists, 474, 477–482
route filters, 82
URPF, 90
area filters, 101
ARP spoofing, 113
ASA (Adaptive Security Algorithm), 147
ISN, generating random sequence, 148
stateful inspection, 152
TCP connection establishment, 148–150
TCP traffic filtering, 148
UDP session establishment, 150
assessing threats to security, 6–8
assigning privilege levels to users, 549–552
associations, 114
asymmetric routing, 89, 143
atomic signatures, 420
attacks
cessation of operation
Land.c, 414–415
ping of death, 413–414
classifying with NBAR and PDLM, 607–608
Code Red worm, 608–610
DDoS, rate limiting with CAR, 619
defending against with service provider security, 557–558
DoS, 7, 401, 405
CBAC prevention mechanisms, 204–206
cessation of normal OS operation, 405
DDoS, 407–413
rate-limiting, 616–618
resource exhaustion, 405
TCP SYN floods, 405–407
thwarting with ACLs, 580–582
false positives, 449
fraggle, thwarting with ACLs, 578–579

LAN floods, preventing, 110–111
MAC address floods, 107–109
network access, 401
buffer overflows, 415–416
data access, 402
privilege escalation, 417–418
system access, 402
overlapping fragment, 175
perpetrators
experienced hackers, 404
inexperienced hackers, 403
trusted users, 403
untrusted users, 403
smurf, thwarting with ACLs, 576–578
SYN floods, thwarting with ACLs, 579–580
tiny fragment, 174–175
tracing with service provider security, 560–562
attributes payload, 318
auditing network security policies, 12
authentication, 470
configuring AAA, 471
cut-through proxy, 158–159
configuring on PIX, 188–191
EAP, 115, 118
IKE
digital signatures, 308–309
encrypted nonces, 310
preshared key, 307
local database, configuring, 471
login banners, 69, 78
method lists
applying, 474
configuring, 471–474
OSPF, 98
password management, 59–60
policies, defining, 17
port authentication, 802.1x, 114–125
PPP, 482–485
RADIUS, 515, 519
router authentication, MD5-HMAC, 84–87
TACACS+, 498
x-auth in ISAKMP, 539–541
Authentication Data field
HSRP packets, 46
VRRP packets, 54
Authentication Type field (VRRP packets), 52
authorization, 475
configuring PPP timeouts with AAA, 488–489
method lists
applying, 477–479
configuring, 475–476
PPP, 482, 484–485
privilege escalation, 402
RADIUS, 515, 520–530
IETF attribute support on Cisco routers, 521–531
vendor-specific attribute support on Cisco routers, 530–531
TACACS+, 499–507
auth-proxy, 541–542, 544. *See also* lock and key
troubleshooting, 676–677
availability statements, defining, 18

B

backscatter traceback, 560–562
backup devices
HSRP, 42
active routers, 43
Failover protocol, 49
failure detection, 43
functionality, 47, 49
implementations, 46–47
packet format, 44–46
versus VRRP, 49
routing-enabled redundancy, 39–40
dynamic, 41
static routes, 40
VRRP, 50
failure detection, 51
master router selection, 50
packet format, 51–54
backup mode (VRRP), 50
bandwidth management, CAR, 613–614
compound interest measurement, 615–616
token buckets, 614
banners, 69, 78
bastion hosts, 29
BGP (Border Gateway Protocol), 92
disabling version negotiation, 94
EBGP multihop, 94
incoming route filtering, 92–93

network advertisements, 93
outgoing route filtering, 93
peer authentication, 92
restricting communications, 94
Biotech Inc., network security design and implementation case study, 12–13
asset identification, 13
defining security policies, 15–20
risk analysis, 14–15
threat identification, 13–14
black hole filtering, 87–88
block size, 311
bottlenecks, firewall-induced, 138
bound checking buffer overflow attacks, 416
broadcast floods, preventing, 110–111
buffer overflow attacks, 415–416
burst parameters of CAR, 614
bypassing NAT, 663

C

cabling, selecting, 38
CAM overflow, preventing, 107–109
capturing core dumps, 70, 78
CAR (Committed Access Rate), 613–614
compound interest measurement, 615–616
dropping malicious traffic, 616–618
rate-limiting traffic
DDoS attacks, 619
DoS attacks, 616–618
suspected malicious traffic, 618
token buckets, 614
case studies
implementing CBAC on routers with NAT, 207–210, 212
network security design and implementation, 12–13
asset identification, 13
defining security policies, 15–20
risk analysis, 14–15
threat identification, 13–14
zoning with Cisco PIX Firewalls, 30–31
Catalyst 6000 series switches
configuring as sensors, 435, 458–461
port security, 107–109
private VLANs, 111–112
ARP spoofing, 113
configuring, 113
ports, 112
sticky ARP, 113
categories of IDS signatures, 444–445
categorizing VPNs
based on business functionality, 220
based on encryption, 217–218
based on OSI model layer
application layer VPNs, 219
data link layer VPNs, 219
network layer VPNs, 219
CBAC (context-based access control), 199
DoS attack prevention mechanisms, 204–206
functionality of, 200–201
implementing on routers with NAT, 207–212
stateful packet filtering, 200–201
threshold values, 204–205
timeouts, 204–205
CBC (Cipher Block Chaining), 311
CEF (Cisco Express Forwarding), enabling, 67
centralized administrative tools, 139
cessation-of-operation attacks, 405
Land.c, 414–415
ping of death, 413–414
challenges of implementing service provider security, 563
characteristics of firewalls, 137
Checksum field
RFC 1701 GRE header, 225
VRRP packets, 53
CIDS configuration GUI (CSPM IDS console), 434
circuit-level firewalls, 141
Cisco 7200/7500 series rouers, turbo ACLs, 590–593
Cisco IDS
shunning, 575
troubleshooting, 666–670
Cisco IOS command authorization, 549–552
Cisco IOS Firewall
features of, 201
application layer inspection, 202
DoS attack prevention, 204–206
fragment handling, 206–207
invalid command filtering, 203

Java blocking, 203
transport layer inspection, 202
Cisco PIX Firewall
access control, 72
ACLs, 153
advanced features
alias, 159–162
DNS guards, 165
flood guards, 162
frag guards, 163–164
fragment handling, 174–175
mail guards, 164
multicast support, 172
multimedia support, 166
protocol fixup, 168–169
spoof detection, 168
sysopt commands, 169–172
traffic filtering, 165
URPF, 168
alias feature, configuring, 185–188
ASA, 147
generating random ISN sequence, 148
stateful inspection, 152
TCP traffic filtering, 148–150
UDP session establishment, 150
configuration management, 71
configuring
as sensors, 454–457
with three interfaces, 176–181
connectivity, troubleshooting, 645–647
cut-through proxy authentication, 158–159, 188–191
debugs, 635–637
events logging, 74, 442–443
failover feature, 156–158, 181–184
logging capabilities, 153–154
NAT, 155
object groups, scaling configurations, 191–195
password management, 73–74
recommended timeout values, 637
redundancy, 155
resolving common problems, 643–645
routing capabilities, 155
security zones, 152–153
sensor implementaion, 448
show commands, 638–643
SSH, 73
troubleshooting, 633–634
Cisco Secure Intrusion Detection
categories of signatures, 444–445
management console. *See also* CSPM IDS Console, UNIX director
CIDS console, 433
CSPM IDS, 433
interaction with sensor, 427–428
placement, 426
UNIX director, 430–432
sensors, configuring
configd daemon, 437
fileXferd daemon, 437
inline processing, 427
interaction with management console, 427–428
loggerd daemon, 437
logging instrusions, 439–443
managed daemon, 437
packetd daemon, 437
passive monitoring, 427
placement, 426
postofficed daemon, 436–437
responses to intrusions, 438
sapd daemon, 437
shunning feature, 444
signature engines, 446–447
TCP reset mechanism, 443
types of, 435
signatures, customizing, 463–465
class maps, NBAR classification, 603–605
classifying
NBAR packets, 599–600
class maps, 603–605
packet dropping, 605–606
packet marking, 605–606
recognizable protocols, 600–603
network attacks
based on mode of attack, 401–402
based on perpetrator, 402–404
with PDLM and NBAR, 607–608
Code Red worm, 608–610

command authorization
  configuring, 549–552
  versus EXEC authentication, 551
Command messages (POP), 432
commands
  debug icmp trace, 635–637
  debug ip inspect tcp, 651
  debug ip nat, 626–627
  debug ip packet, 626
  maximum-prefix, 97
  scheduler allocate, 67
  show conn detail, 639–640
  show crypto engine connection active, 659
  show crypto isakmp sa, 659–660
  show interface, 640–643
  show ip inspect all, 648–649
  show ip nat translations, 628
  show xlate detail, 637–639
  sysopt, 169–172
communications architecture, RADIUS, 516
community ports, 112
components
  of AAA, 470
  of IKE, 276
    aggressive mode, 302–306
    main mode, 278–293, 296–302
    quick mode, 279
  of service provider security, 563
composite signatures, 420
compound interest measurement, 615–616
compulsory tunneling, 245
  setup process, 251–270
computer technology purchasing guidelines, defining, 16
concentrators, 275
configd daemon
  IDS Sensor, 437
  UNIX director, 431
configuration management, 54–55
  PIX, 71
  switches, 75
configuring
  802.1x on Catalyst 6000 switches, 123–125
  accounting, method lists, 479–482
  authentication, 147
    local database, 471
    method lists, 471–474
  authorization, method lists, 475–479
  Catalyst 6000 IDSM as sensors, 458–461
  CEF, 67
  firewalls, 139
  HTTP, 66
  IP permit lists, 109–110
  IPsec
    combined remote-access/LAN-to-LAN implementation, 369–373
    one-to-many router, 355–360
    over GRE, 360–365
    over L2TP using voluntary tunneling, 373–379
    remote-access implementations, 366–368
    router-to-router using digital signatures, 338–349
    router-to-router using preshared key authentication, 325–338
    router-to-router using RSA encrypted nonces, 349–354
    TED, 379–391
  NTP, 68
  OSPF
    loopbacks as router ID, 101
    route filtering, 101
    stub areas, 99–100
    timers, 101
  PIX Firewall
    alias feature, 185–188
    as sensors, 454–457
    cut-through proxy authentication, 188–191
    failover to secondary device, 181–184
    with 3 interfaces, 176–181
  PPP timeouts with AAA, 488–489
  private VLANs, 113
  proxy authentication, 541–544
  route dampening, 96
  routers as sensors, 449–454
  scheduler, 67
  SNMP, 64–66
  turbo ACLs, 591–593
  UNIX director, shunning, 462–463
  URPF, 89
  VPDN, 544–547
congestion, firewall-induced, 138

connecting
- IPX sites with GRE, 235–239
- multiple sites with GRE, 230–235

connectivity, Cisco PIX, troubleshooting, 645–647
control connection establishment, L2TP, 246
controlling
- LAN floods, 110–111
- PIX access, 72
- router access, 55
  - TTY, 58
  - vty, 55–57
- switch access, 75

convergence, 83
cookies, 280
core dumps, 70, 78
Count IP Addrs field (VRRP packets), 52
coup hello messages, 43
courtesy ARP, 113
crackers versus hackers, 400
creating
- DMZs, 26–30
- security policies, 8–9

CSPM IDS Console
- internal architecture, 433
  - CIDS configuration GUI, 434
  - cvtnrlog.exe, 434
  - EDI, 434
  - EVI, 434
  - nr.postofficed daemon, 433
  - nr.smid daemon, 434
  - Sensor CA, 433
- versus UNIX director, 429

customizing signatures, 463–465
cut-through proxy authentication, 158–159
- configuring on PIX Firewall, 188–191

cvtnrlog.exe (CSPM IDS console), 434

D

daemons
- CIDS console, 433–435
- Cisco IDS sensor, 436–438
- UNIX director, 431–432

damages due to successful attacks, estimating, 8
data access attacks, 402
data link layer VPNs, 219
data-link layer, L2TP, 243
- compulsory tunneling, 245, 251–270
- control connection establishment, 246
- header format, 248–250
- session establishment, 247–248
- setup process, 246
- tunnel layers, 244
- voluntary tunneling, 245

DDoS attacks, 407
- rate limiting with CAR, 619
- Stacheldraht, 411–413
- TFN, 409–411
- Trinoo, 408

debug icmp trace command, 635–637
debug ip inspect tcp command, 651
debug ip nat command, 626–627
debug ip packet command, 626
debugs
- IPsec, 654–658
- PIX, 635–637

default timeout values, PIX, 637
defining
- network security policies, 15–20
- security zones, 25–26
  - DMZs, 26–31

deliberate inside attackers, 403
denial of service, 7
DES encryption, 311
designing secure networks, 11
- case study, 12–20
- security zones, 25–26
  - case study, 30–31
  - DMZs, 26–27, 29–30

Destination Address field (VRRP packets), 51
detecting
- Code Red worm, 610
- intrusions, 418–419

devices
- AAA network components, 470
- authentication
  - digital signatures, 308–309
  - encrypted nonces, 310
  - preshared keys, 307
- Catalyst 6000 IDSM, configuring as sensor, 458–461

physical security, 36
  environmental factors, 39
  media, 38
  network topographical design, 36
  placement, 37–38
  power supply, 38
  redundant locations, 36
PIX, 71
  access control, 72
  configuration management, 71
  connectivity problems, troubleshooting, 645–647
  debugs, 635–637
  events logging, 74
  password management, 73–74
  recommended timeout values, 637
  resolving common problems, 643–645
  show commands, 638–643
  SSH, 73
  troubleshooting, 633–634
redundancy
  dynamic, 41
  HSRP, 42–49
  routing-enabled, 39–40
  VRRP, 49–54
routers
  CEF, 67
  configuration management, 54–55
  configuring as sensor, 449–454
  controlling access, 55–58
  core dumps, 70
  disabling unnecessary services, 61–63
  events logging, 61
  HTTP, 66
  login banners, 69
  loopback interfaces, 63
  Nagle protocol, 70
  NTP, 68
  password management, 59–60
  scheduler, 67
  sensor implementation, 448
  SNMP, 64–66
  SSH, 58
  traffic processing, 585
switches
  configuration management, 75
  controlling access, 75
  core dumps, 78
  events logging, 76
  IP permit lists, configuring, 109–110
  login banners, 78
  NTP, 77
  port security, 107–109
 VLANs, 105
  basic security rules, 105–106
Diffie-Hellman algorithm, 284–285
DiffServ, marking packets, 605–607
digital signatures, 308–309
directed broadcast control, 87
dirty DMZs, 28–29
disabling
  BGP version negotiation, 94
  directed broadcast control, 87
disabling unnecessary services, 61–63
DMZs, 26–30
  placement
   between firewall and public network, 27
   between stacked firewalls, 30
   outside the firewall, 28–29
DNS guards (PIX Firewall), 165
DoS attacks, 401, 405
  CBAC prevention mechanisms, 204–206
  cessation of normal OS operation, 405
  DDoS, 407
   Stacheldraht, 411, 413
   TFN, 409–411
   Trinoo, 408
  preventing on Cisco IOS Firewalls, 204–206
  rate-limiting, 616–618
  resource exhaustion, 405
  TCP SYN floods, 405–407
  thwarting with ACLs, 580–582
DPD (Dead Peer Discovery), 323
dropped packets
  NBAR, 605–606
  rate limiting, 616
DSCP (Differentiated Services Code Point), marking packets, 605–607
DTP (Dynamic Trunking Protocol), 106
dynamic network redundancy, 41
Dynamic Trunking Protocol (DTP), 106

E

EAP (Extensible Authentication Protocol), 115
  as 802.1x communications mechanism, 118
  messages, 117–118
  packet fields, 116
EAPOL (EAP over LANs), 119
ease of firewall configuration, 139
EBGP multihop, 94
EDI (Event Database Interface), CSPM IDS console, 434
elements
  of security policies, 9–10, 15–20
  of service provider security, 563
enable secrets, 59
enabling
  CEF, 67
  Nagel protocol, 70
encapsulation
  EAPOL, 121
  GRE, 223
    connecting IPX sites, 235–239
    connecting multiple sites, 230–235
    implementations, 224
    non-IP traffic, 227
    RFC 1701 implementation, 223–225
    RFC 2784 implementation, 226–227
    tunneling between private networks, 227–230
  IPsec
    AH, 317
    ESP, 316
    transport mode, 314
    tunnel mode, 314–316
encryption
  IPsec, 311
  nonces, 310
  public/private key pairs, 307
  VPNs, 218
end devices, 7
environmental considerations of physical security design, 39
Error messages (POP), 432
ESP (Encapsulating Security Payload), 316
  integrity checking, 312–313
event logging, 439–442
  in appliance sensors, 439–441
  on IDSM, 441
eventd daemon (UNIX director), 432
events logging, 61
  switches, 76
EVI (Event Viewing System), CSPM IDS console, 434
extended ACLs, 569–571
extended authentication. *See* x-auth
extranet VPNs, 220

F

failover (PIX), 155–158
  to secondary device, 181–184
Failover protocol (HSRP), 49
failure detection (HSRP), 43
false positives, 449
features of Cisco IOS Firewall, 201
  application layer inspection, 202
  DoS attack prevention, 204–206
  fragment handling, 206–207
  invalid command filtering, 203
  Java blocking, 203
  transport layer inspection, 202
fields
  of EAP packets, 116
  of EAPOL frames, 121
  of HSRP packets, 45–46
  of VRRP packets, 52–54
fileXferd daemon (IDS Sensor), 431, 437
fileXferd daemon (UNIX director), 431
filtering. *See also* protocol filtering
  incoming BGP routes, 92–93
  IP fragments, 583–588
    overlapping fragment attacks, 589
    tiny fragment attacks, 588
  MAC addresses on specific ports, 107–109
  outgoing BGP routes, 93
  RFC 1918 address space, 582
  traffic with IP permit lists, 109–110
  with ACLs
    blocking ICMP packets, 573–575
    blocking known offenders, 575
    blocking spoofed IP addresses, 575

extended, 569–571
functionality, 567–568, 573
implicit deny all entry, 571
NetFlow switching, 594–595
standard, 568
top-down processing, 571
firewalls
bastion hosts, 29
characteristics, 137
circuit-level, 141
Cisco IOS Firewall
application layer inspection, 202
CBAC, 199–201
debug commands, 650–651
DoS attack prevention, 204–206
features, 201
fragment handling, 206–207
invalid command filtering, 203
Java blocking, 203
order of operations, 648
show commands, 648–649
resolving common problems, 651–652
transport layer inspection, 202
troubleshooting, 647
Cisco PIX Firewall
ACLs, 153
advanced traffic filtering, 165
alias feature, 159, 161–162, 185–188
ASA, 147–150
configuring with three interfaces, 176–181
connectivity problems, troubleshooting, 645–647
creating zones, 30–31
cut-through proxy authentication, 158–159, 188–191
debugs, 635–637
DNS guards, 165
event logging, 442–443
failover feature, 156–158
failover to secondary device, 181, 183–184
flood guards, 162
frag guards, 163–164
fragment handling, 174–175
IP session logging, 443
logging capabilities, 153–154
mail guards, 164
multicast support, 172
multimedia support, 166
NAT, 155
protocol fixup, 168–169
redundancy, 155
resolving common problems, 643–645
routing capabilities, 155
scaling configurations, 191–195
security zones, 152–153
sensor implementation, 448
show commands, 638–643
spoof detection, 168
stateful inspection, 152
sysopt commands, 169–172
troubleshooting, 633–634
URPF, 168
device security, 140
ease of configuration, 139
interaction with IPsec, 393
layering, 144
nonstateful packet filters, 141
notification ability, 138
personal, 142
positioning, 143–144
proxy servers, 141
stateful packet filters, 142
three-legged, creating DMZs, 27
traffic processing speed, 138
Flags field (RFC 1701 GRE header), 224
flapping routes, dampening, 95
floating static routes, 40
flood guards (PIX Firewall), 162
flooded CAM tables, preventing, 107–109
frag guards (PIX Firewall), 163–164
fraggle attacks, thwarting with ACLs, 578–579
fragment handling
Cisco IOS Firewalls, 206–207
PIX Firewall, 174–175
fully meshed networks, dynamic redundancy, 41
functionality
of CBAC, 200–201
of HSRP, 47–49

G

Garfinkel, S., 8
getadmin exploits, 417–418
goal of network security, 5
gratuitous ARP, 113
GRE (Generic Routing Encapsulation), 223
  connecting IPX sites, 235–239
  connecting multiple sites, 230–235
  implementations, 224
  non-IP traffic encapsulation, 227
  RFC 1701 implementation, 224–226
  RFC 2784 implementation, 226–227
  tunneling between private networks, 227–230
Group field (HSRP), 46
guard feature (PIX Firewall)
  DNS guards, 165
  flood guards, 162
  frag guards, 163–164
  mail guards, 164

H

hackers, 400
  experienced, 404
  Metnick, Kevin, 421–422
  professional, 404
  script kiddies, 403
  versus crackers, 400
half-open SYN attacks, 405, 407
hard coding BGP version information, 94
hash payload (IKE main mode message), 290
hashing, 312–313
  MD5-HMAC, 84–87
headers
  L2TP, format, 248–250
  TACACS+, 495–497
Heartbeat messages (POP), 432
Hellotime field (HSRP), 45
heuristic/holistic classification, NBAR, 600
high-availability IPsec over GRE, 360–365
high-severity alarms, 448
HMAC (Message Authentication Codes using Hashing), integrity checking, 312–313
holdtime (HSRP active routers), 43
Holdtime field (HSRP), 45
home gateways, VPDN configuration, 544–547
Honey Pots, 558
host intrusion detection, 425
HSRP (Hot Standby Router Protocol), 42
  active routers, 43
  Failover protocol, 49
  failure detection, 43
  functionality, 47–49
  implementations, 46–47
  packet format, 44–46
  versus VRRP, 49

I

ICMP (Internet Control Message Protocol)
  floods, rate limiting with CAR, 617
  maintaining path integrity, 91
  packet filtering, 573–575
identifying resources to protect, 6
identity payload
  EAP messages, 117
  IKE main mode message, 290
IDSM
  event logging, 441–442
  IP session logging, 442
  sensor implementation, 448
IDSs
  Catalyst 6000 IDSM
    configuring as sensors, 458–461
  Cisco Secure IDS
    categories of signatures, 444–445
    management console, 426–433
    sensors, 426–428, 435–444
    signature engines, 446–447
  PIX Firewall, configuring as sensors, 454–457
  resolving common problems, 666–670
  routers, configuring as sensors, 449–454
  signature-based, 419
  statistical anomaly-based, 419
IEEE 802.1x port authentication, 114
  communications, 115–21
  configuring on Catalyst 6000 switches, 123–125
  functionality, 122
IETF Accounting AV pairs (RADIUS), 532–533
IETF attributes supported on Cisco routers, 521–531

IKE (Internet Key Exchange), 276
  aggressive mode using preshared key authentication, 302–306
  Diffie-Hellman algorithm, 284–285
  digital signature authentication, 308–309
  encrypted nonces, 310
  main mode, 278
    using digital signature authentication, 298–302
    using preshared key authentication, 280—297
  preshared key authentication, 307
  quick mode, 279
  SA, 279, 284
implementations
  of GRE, 224
    RFC 1701, 224–226
    RFC 2784, 226–227
  of HSRP, 46–47
implementing
  CBAC on routers with NAT, 207–210, 212
  network security policies, 10–20
  service provider security, 563
implicit deny all entry (ACLs), 571
improving network security policies, 12
incoming BGP routes, filtering, 92–93
incoming call establishment
  L2TP, 247
ingress filtering, 82
inside global addresses, 628
inside local addresses, 628
integrity checking, 312–313
intranet VPNs, 220
intrusion detection, 418
  motivation for, 399–400
  responses, 438
    event logging, 439–442
    IP session logging, 441–443
    shunning, 443
    TCP reset, 443
invalid command filtering, Cisco IOS Firewall, 203
invalid IP addresses, blocking with ACLs, 581–582
IOS Firewalls
  CBAC, 199
    functionality of, 200–201
    stateful packet filtering, 200–201
  debug commands, 650–651
  order of operations, 648
  resolving common problems, 651–652
  show commands, 648–649
  troubleshooting, 647
IP Address field (VRRP packets), 53
IP addressing, NAT, 129
  security benefits, 130
  vulnerabilities, 131
IP fragments
  filtering, 583–584, 587–588
  overlapping fragment attacks, 589
  tiny fragment attacks, 588
IP log messages (POP), 432
IP permit lists, configuring, 109–110
IP session logging, 441–443
  in appliance sensors, 441
  on IDSM, 442
  on PIX Firewall, 443
  on router-based sensors, 443
IP source routing, maintaining path integrity, 91
IPsec
  AH, 317
  combined LAN-to-LAN/remote access configuration, 369–373
  components, 276
  compulsory tunneling, 266–270
  debugs, 654–658
  DPD, 323
  encryption mechanisms, 311
  ESP, 316
  high-availability configuration over GRE, 360–365
  IKE, 276
    aggressive mode, 302–306
    digital signature authentication, 308–309
    encrypted nonces, 310
    main mode, 278–302
    preshared key authentication, 307
    quick mode, 279
  integrity checking, 312–313
  interaction
    with firewalls, 393
    with NAT, 391–393
  LAN-to-LAN implementations, 274
  MTU issues, troubleshooting, 664–666
  one-to-many router configuration, 355–360
  order of operations, 653–654

over L2TP using voluntary tunneling, 373–379
preshared keys, obtaining from AAA, 537–539
remote-access client implementation, 366–368, 275, 317–318
extended authentication, 318–320
mode configuration, 321
NAT transparency, 321
router-to-router
using digital signatures, 338–349
using preshared key authentication, 325–338
using RSA encrypted nonces, 349–354
show commands, 658–660
TED, configuring, 379, 381–391
transport mode, 314
troubleshooting common problems, 661–666
tunnel mode, 314–316
VPNs, order of events, 653–654
IPv4 GRE, 223
RFC 1701 implementation, 223–225
RFC 2784 implementation, 226–227
IPX sites, connecting with GRE, 235–239
ISAKMP, 277
x-auth, 541
x-auth for remote-access clients, 539–540
ISN (Initial Sequence Number), generating random sequences, 148
isolated ports, 112
ISPs, net police filters, 82

J-K

Java blocking (Cisco IOS Firewall), 203

Key field (RFC 1701 GRE header), 225
key-exchange process (IKE), 276
aggressive mode exchange with preshared key authentication, 302–306
main mode exchange, 278
with digital signature authentication, 298–302
with preshared key authentication, 280–297
quick mode exchange, 279
known offenders, blocking, 575

L

L2TP (Layer 2 Tunneling Protocol), 243
compusory tunnels, 245
setup process, 251–270
control connection establishment, 246
header format, 248–250
session establishment, 247–248
setup process, 246
three-way message exchange, 246
tunnel layers, 244
voluntary tunnels, 245
LAN switching
basic security rules, 105–106
flood attacks, preventing, 110–111
IP permit lists, configuring, 109–110
port authentication, 114
communications, 121
IEEE 802.1x, 114–125
port security, 107–109
Land.c attacks, 414–415
LAN-to-LAN IPsec implementations, 274
combining with remote-access configuration, 369–373
layering firewalls, 144
Length field (L2TP header), 250
likelihood of attack, assessing, 7–8
Livingston Enterprises, Inc., RADIUS, 515
lock and key, configuring, 548–549
loggerd daemon, 431
IDS Sensor, 437
UNIX director, 431
logging
ACLs, 573
BGP neighbor status changes, 97
events, 61
intrusions
event logs, 439–442
IP session logs, 441–443
PIX events, 74
switches, 76
syslog messages on PIX, 153–154
login banners, 69
switches, 78
loopbacks, 63
configuring as router ID (OSPF), 101
low-severity alarms, 447

M

MAC addresses, restricting on specific ports, 107–109
mail guards (PIX Firewall), 164
main mode (IKE) exchanges, 278
  using digital signature authentication, 298– 302
  using preshared key authentication, 280– 298
    ISAKMP message payloads, 281–284
    PFS, 291–292
maintaining
  path integrity. 91
  routing table stability, 94
    maximum-prefix command, 97
    route dampening, 95–96
maintenance policies, defining, 18
malicious attacks, false positives, 449
malicious traffic, dropping with CAR, 616–618
managed daemon (IDS Sensor), 437
management console (Cisco Secure IDS)
  CSPM IDS console, 433
    CIDS configuration GUI, 434
    cvtnrlog.exe, 434
    EDI (Event Database Interface), 434
    EVI, 434
    nr.postofficed daemon, 433
    nr.smid daemon, 434
    Sensor CA, 433
  interaction with sensor, 427–428
  placement, 426
  UNIX director, 430
    configd daemon, 431
    eventd daemon, 432
    fileXferd daemon, 431
    loggerd daemon, 431
    POP, 432
    postofficed daemon, 430
    sapd daemon, 431
    shunning, 462–463
    smid daemon, 431
management protocols
  HTTP, 66
  SNMP, 64–66
managing NBAR classified traffic, 606–607
marking packets, NBAR, 605–606
master routers, 50
masters (Trinoo), 408
MD-5 challenge messages (EAP), 117
MD5-HMAC, 84–87
medium-severity alarms, 448
messages, TLS, 118
method lists, 469
  applying, 474–482
  configuring, 471–474
    for AAA accounting, 479–481
    for AAA authorization, 476
Metnick, Kevin, attack on Tsutomu Shimomura's computers, 421–422
misconfiguration
  of access lists, troubleshooting, 662
  of firewalls, 139
mode configuration (remote access IPsec), 321
motivation
  for IDSs, 399–400
  for service provider security, 557
    ability to track source of attacks, 560–562
    defense against attacks, 557–558
multicast support, PIX Firewall, 172
multimedia support, PIX Firewall, 166
multiple sites, connecting with GRE, 230–235

N

Nagle protocol, enabling, 70
NAK messages (EAP), 117
NAT (Network Address Translation), 129
  bypassing, 663
  common problems, troubleshooting, 629–633
  debugs, 626–627
  interaction with IPsec, 391–393
  order of operations, 625–626
  PIX Firewall capabilities, 155
  security benefits, 130
  show commands, 627–629
  transparency (remote access IPsec), 321
  vulnerabilities, 131
NBAR (Network-Based Application Recognition), 599–600
  class maps, 603–605
  classifying attacks with PDLM, 607–608
  detection of Code Red worm, 608–610
  dropping packets, 605–606

effect on performance, 608
marking packets, 605–606
non-TCP-based recognizable protocols, 602–603
non-UDP-based recognizable protocols, 602–603
TCP-based recognizable protocols, 600–602
UDP-based recognizable protocols, 600–602
negotiation (IKE)
aggressive mode exchanges using preshared key authentication, 302–306
main mode exchanges
ISAKMP message payloads, 281–284
PFS, 291–292
using digital signature authentication, 298–302
using preshared key authentication, 280–298
neighbor database filters, 101
neighbor status (BGP), logging changes in, 97
net police filters, 82
NetFlow switching, ACL enhancements, 594–595
network access attacks, 401–402
network advertisements, BGP, 93
network attacks, 401
cessation-of-operation
Land.c, 414–415
ping of death, 413–414
DoS, 401, 405
cessation of normal OS operation, 405
DDoS, 407–413
resource exhaustion, 405
TCP SYN floods, 405–407
network access, 401
buffer overflows, 415–416
data access, 402
privilege escalation, 417–418
system access, 402
network flows, 594
network intrusion detection, 425
network layer VPNs, 219
network security policies
auditing, 12
creating, 8–9
defining, 15–20
design issues, 11
elements of, 9–10
implementing, 10–11
nonbroadcast neighbor configuration, OSPF, 98–99
nonces, 285
nonencrypted VPNs, 218
noninitial fragment inspection (Cisco IOS Firewall), 206
non-IP traffic encapsulation, 227
nonstateful packet filters, 141
non-TCP-based protocols recognized by NBAR, 602–603
non-UDP-based protocols recognized by NBAR, 602–603
notification ability of firewalls, 138
notification messages (EAP), 117
notify payload (DPD), 323
Nr field (L2TP header), 250
nr.postofficed daemon (CSPM IDS console), 433
nr.smid daemon (CSPM IDS console), 434
Ns field (L2TP header), 250
NTP (Network Time Protocol)
configuring, 68
switch implementations, 77
null route filtering, 87

O

Oakley, 277
object groups, scaling PIX configurations, 191–195
Offset field (L2TP header), 250–251
one-time password messages (EAP), 117
one-to-many router IPsec configuration, 355–360
OSPF (Open Shortest Path First)
configuring loopbacks as router ID, 101
nonbroadcast neighbor configuration, 98–99
route filtering, 101
router authentication, 98
stub areas, configuring, 99–100
timers, configuring, 101
outgoing BGP routes, filtering, 93
outgoing call establishment, L2TP, 247–248
out-of-sequence fragments, stateful inspection of with Cisco IOS Firewall, 207
outside global addresses, 628

outside local addresses, 628
overlapping fragment attacks, 175, 589
Overload NAT, 129

P

packet filters
  nonstateful, 141
  stateful, 142
packetd daemon (IDS Sensor), 437
packets
  classifying with NBAR, 599–603
    class maps, 603–605
  dropping, 605–606
  EAP, fields, 116
  HSRP, 44–46
  ICMP, blocking with ACLs, 573, 575
  marking with NBAR, 605–606
  network flows, 594
  RADIUS, 517–518
  TACACS+, encryption, 497
  VRRP, 51–54
PAE (Port Access Entity), 115
passive monitoring, 427
passwords
  authentication, 470
  encryption with RADIUS, 518–519
  PIX, managing, 73–74
PAT (Port Address Translation), 129
path integrity, maintaining, 91
PDLM (Protocol Description Language Module), classifying attacks with NBAR, 607–608
peer authentication (BGP), 92
performance, effect of NBAR on, 608
permissive security policies, 9
perpetrators of network attacks
  experienced hackers, 404
  inexperienced hackers, 403
  trusted users, 403
  untrusted users, 403
personal firewalls, 142
PFS (Perfect Forward Secrecy), 291–292
physical security, 36
  environmental factors, 39
  network topographical design, 36
  power supply, 38
  redundant locations, 36
  selecting secure locations, 37–38
ping of death attacks, 413–414
PIX Firewall, 71
  access control, 72
  ACLs, 153
  advanced features
    DNS guards, 165
    flood guards, 162
    frag guards, 163–164
    fragment handling, 174–175
    mail guards, 164
    multicast support, 172
    multimedia support, 166
    protocol fixup, 168–169
    spoof detection, 168
    sysopt commands, 169–172
    traffic filtering, 165
    URPF, 168
  alias feature, configuring, 159–162, 185–188
  ASA, 147
    generating random ISN sequence, 148
    stateful inspection, 152
    TCP traffic filtering, 148–150
    UDP session establishment, 150
  configuration management, 71
  configuring
    as sensors, 454–457
    with three interfaces, 176–181
  connectivity, troubleshooting, 645–647
  cut-through proxy authentication, 158–159, 188–191
  debugs, 635–637
  events logging, 74, 442–443
  failover, 156–158
    to secondary devices, 181–184
  logging capabilities, 153–154
  NAT, 155
  object groups, scaling configurations, 191–195
  password management, 73–74
  recommended timeout values, 637
  redundancy, 155
  resolving common problems, 643–645
  routing capabilities, 155
  security zones, 152–153
  sensor implementation, 448
  show commands, 638–643

SSH, 73
troubleshooting, 633–634
zones, creating, 30–31
placement
of DMZs
between firewall and public network, 27
between stacked firewalls, 30
outside the firewall, 28–29
of firewalls, 143
policies, 5
auditing, 12
creating, 8–9
defining, 15–20
design issues, 11
elements of, 9–10
implementing, 10–11
policing, managing NBAR classified traffic, 607
policy routing, dropping/marking NBAR classified traffic, 606
POP (Post Office Protocol), Cisco Secure IDS communications, 432
ports
authentication, 802.1x, 114
communications, 115–121
configuring on Catalyst 6000 switches, 123–125
functionality, 122
on private VLANs, 112
security, 107–109
positioning firewalls, 143–144
postofficed daemon
IDS Sensor, 436–437
UNIX director, 430
power supplies, designing physical security, 38
PPP (Point-to-Point Protocol)
AAA authentication and authorization, 482–485
L2TP, 243
compusory tunnels, 245, 251–270
control connection establishment, 246
header format, 248–250
session establishment, 247–248
setup process, 246
tunnel layers, 244
voluntary tunnels, 245
timeouts, configuring with AAA, 488–489
prefix lists, filtering incoming BGP routes, 92–93
preshared key authentication, 307
authenticating ISAKMP in IPsec implementations, 537–539
preventing flood attacks, 110–111
Priority field
HSRP, 46
L2TP header, 250
VRRP packets, 52
private networks
route filtering, 81
address spaces, 82
applying, 82
ingress filtering, 82
net police filters, 82
tunneling between with GRE, 227–230
VPDN, 544–547
private VLANs, 111–112
ARP spoofing, 113
configuring, 113
ports, 112
sticky ARP, 113
privilege levels
assigning to users, 549–552
escalating, 402, 417
getadmin exploits, 418
unicode exploits, 418
processing, order of operations
ACLs, 571
IPsec, 653–654
NAT, 625–626
professional hackers, Metnick, Kevin, 421–422
promiscuous ports, 112
Protocol Description Language Module. *See* PDLM
Protocol field (VRRP packets), 51
protocol filtering, controlling LAN floods, 110–111
protocol fixup, PIX Firewall, 168–169
Protocol Type field (RFC 1701 GRE header), 225
proxy authentication, configuring, 541–544
proxy servers, 129
firewalls, 141
public/private key pairs, 307

Q

QoS (quality of service)
  CAR, 613–614
    compound interest measurement, 615–616
    dropping malicious traffic, 616–618
    token buckets, 614
  NBAR, 599–600
    classifying attacks with PDLM, 607–608
    detection of Code Red worm, 608–610
    effect on performance, 608
    marking/dropping packets, 605–606
    recognizable protocols, 600–603
qualitative risk assessment, 8
quick mode (IKE), 279
  timeout negotiation, 293

R

RADIUS, 515
  accounting, 531–532
    IETF Accounting AV pairs, 532–533
  authentication, 519
  authorization, 520–530
    IETF attributes, 521–531
    vendor-specific attributes, 530–531
  communications architecture, 516
  packet format, 517–518
  password encryption, 518–519
rate limiting
  CAR, 613–614
    compound interest measurement, 615–616
    dropped packets, 616
    dropping malicious traffic, 616–618
    token buckets, 614
  DoS attacks, 616–618
  suspicious traffic, 618
recommended PIX timeout values, 637
redundancy
  HSRP, 42
    active routers, 43
    Failover protocol, 49
    failure detection, 43
    functionality, 47–49
    implementations, 46–47
    packet format, 44–46
    versus VRRP, 49
  physical security, 36
  PIX Firewall capabilities, 155–158
  routing-enabled, 39–40
    dynamic, 41
    static routes, 40
  VRRP, 50
    failure detection, 51
    master router selection, 50
    packet format, 51–54
remote-access clients, x-auth, 539–541
remote-access IPsec, 275, 317–318, 366–368
  combining with LAN-to-LAN configuration, 369–373
  extended authentication, 318–320
  mode configuration, 321
  NAT transparency, 321
resolving common issues
  AAA-related problems, 671–677
  IDS-related problems, 666–670
  IOS-related Firewall problems, 651–652
  IPsec-related problems, 661–666
  NAT-related problems, 629–633
resource exhaustion DoS attacks, 405
  DDoS
    Stacheldraht, 411–413
    TFN, 409–411
    Trinoo, 407–408
  simple DoS attacks. TCP SYN floods, 406–407
responses to intrusions (IDS Sensor), 438
  event logging, 439–442
  IP session logging, 441–443
  shunning, 444
  TCP reset, 443
restricting
  BGP communications, 94
  MAC addresses on specific ports, 107–109
  traffic
    with ACLs, 572–573
    with IP Permit lists, 109–110
restrictive security policies, 9
RFC 1701 GRE implementation, 224–226

RFC 1918 addressing
- address space, filtering, 582
- NAT, 129–130
- vulnerabilities of, 131

RFC 2409, IKE, 277
RFC 2784 GRE implementation, 226–227
RFC 2890 GRE implemenation, 226
risk assessment, likelihood of attacks, 7–8
route dampening, 95–96
route filtering, 81
- address spaces, 82
- applying, 82
- ingress filtering, 82
- net police filters, 82
- OSPF, 101

Router and PIX Firewall sensors, 435
router-based sensors
- event logging, 442–443
- IP session logging, 443

routers
- CBAC implementation case study, 207–212
- CEF, enabling, 67
- configuration management, 54–55
- configuring as sensors, 449–454
- controlling access, 55
  - TTY, 58
  - vty, 55–57
- core dumps, 70
- disabling unnecessary services, 61–63
- events logging, 61
- HTTP, configuring, 66
- login banners, 69
- loopback interfaces, 63
- Nagle protocol, 70
- NTP, configuring, 68
- password management, 59–60
- scheduler, configuring, 67
- securing access, 58
- sensor implementation, 448
- sinkholes, 558
- SNMP, configuring, 64–66
- standby mode, 42
- traffic processing, 585

routing
- asymmetric, 89
- black hole filtering, 87–88
- convergence, 83
- directed broadcast control, 87
- maintaining path integrity
  - ICMP redirects, 91
  - IP source routinng, 91
- PIX Firewall capabilities, 155
- route authentication, 83
  - clear-text passwords, 84–87
  - MD5-HMAC, 84–87
  - OSPF, 98
- static routes, 83
- URPF, 88
  - applying, 90
  - configuring, 89

Routing field (RFC 1701 GRE header), 226
routing protocols
- BGP, 92
  - disabling version notification, 94
  - EBGP multihop, 94
  - incoming route filtering, 92–93
  - logging neighbor status changes, 97
  - network advertisements, 93
  - outgoing route filtering, 93
  - peer authentication, 92
  - restricting BGP communications, 94
- OSPF
  - configuring loopbacks as router ID, 101
  - nonbroadcast neighbor configuration, 98–99
  - route filtering, 101
  - router authentication, 98
  - stub areas, 99–100
  - timers, configuring, 101

routing tables, maintaining stability, 94
- maximum-prefix command, 97
- route dampening, 95–96

routing-enabled redundancy, 39–40
- dynamic, 41
- static routes, 40

S

SA (security association), 279
sapd daemon, 431
- IDS Sensor, 437
- UNIX director, 431

scaling PIX configurations, 191–195
scheduler, configuring, 67
script kiddies, 403
security policies, 5
  auditing, 12
  creating, 8–9
  defining, 15–20
  design issues, 11
  elements of, 9–10
  incident reporting, 18
  implementing, 10–11
security zones
  defining, 25–26
  DMZs, 26–30
    case study, 30–31
    placement, 28–30
  PIX, 152–153
selecting
  secure locations for devices, 37–38
  secure media, 38
  VRRP master routers, 50
Sensor CA (CSPM IDS console), 433
sensors
  Catalyst 6000 IDSM, configuring as, 458–461
  Cisco Secure IDS
    configd daemon, 437
    fileXferd daemon, 437
    inline processing, 427
    interaction with management console, 427–428
    loggerd daemon, 437
    managed daemon, 437
    packetd daemon, 437
    passive monitoring, 427
    placement, 426
    postofficed daemon, 436–437
    sapd daemon, 437
    types of, 435
  PIX Firewall, configuring as, 454–457
  responses to intrusions, 438
    event logging, 439–442
    IP session logging, 441–443
    shunning, 444
    TCP reset, 443
  routers, configuring as, 449–454
  signature engines, 446–447
  signatures, corresponding alarms and severity levels, 447–448
Sequence field (L2TP header), 250
Sequence Number field (RFC 1701 GRE header), 225
service provider security
  backscatter traceback, 560–562
  components of, 563
  implementing, 563
  motivation for, 557
    ability to track source of attacks, 560–562
    defense against attacks, 557–558
  sinkhole routers, 558
session establishment, L2TP, 247–248
Session ID field (L2TP header), 250
setup process, L2TP, 246
  compulsory tunnels, 251–266
    with IPsec, 266–270
severity levels of alarms, 447–448
Shimomura, Tsotomu, 421–422
show conn detail command, 639–640
show crypto engine connection active command, 659
show crypto isakmp sa command, 659–660
show interface command, 640–643
show ip inspect all command, 648–649
show ip nat translations command, 628
show xlate detail command, 637–639
shunning, 443, 575
  configuring on UNIX director, 462–463
  managed daemon (Cisco IDS sensor), 437
signature engines, 446–447
signature-based IDSs, 419
signatures, 419, 463–465
  corresponding alarms and severity levels, 447–448
  IDS signature categories, 444–445
simple-text password authentication (VRRP), 53
sinkhole routers, 558
SIS (state information structure), 200–201
site to site IPsec VPNs, 274
SKEME, 276
smashing the stack, 416
smid daemon, 431
smid daemon (UNIX director), 431

smurf attacks, thwarting with ACLs, 576, 578
SNMP (Simple Network Management Protocol), configuring, 64–66
son-of-IKE initiative, 277
Source Address field (VRRP packets), 51
source of attacks, tracking with service provider security, 560–562
Spafford, G., 8
speak state (HSRP routers), 43
spoof detection, PIX Firewall, 168
spoofed IP addresses
    blocking, 575
    source IP addresses, 88–89
SSH (secure shell), 58
    PIX implementation, 73
Stacheldraht attack, 411–413
standalone IDS 4200 series sensors, 435
standard ACLs, 568
standards, IEEE 802.1x
    configuring on Catalyst 6000 switches, 123–125
    functionality, 122
    port authentication, 114–121
standby groups (HSRP), 43
standby mode (HSRP), 42
state information, 147
    SIS, 200–201
stateful inspection, 152
    packet filters, 142
    TCP packets, 148
static routes, 83
    routing-enabled redundancy, 40
statistical anomaly-based IDSs, 419
sticky ARP, 113
stub areas, configuring, 99–100
subport classification, NBAR, 600
supplicants (IEE 802.1x), 114
    communications with authenticator, 119–121
suspicious content, rate-limiting, 618
switches
    access control, 75
    Catalyst 6000 private VLANs, 111–112
        ARP spoofing, 113
        configuring, 113
        ports, 112
        IEEE 802.1x, configuration, 123–125
        sticky ARP, 113
    configuration management, 75
    core dumps, 78
    events logging, 76
    login banners, 78
    NTP, 77
switching
    basic security rules, 105–106
    IP permit lists, configuring, 109–110
    LAN floods, controlling, 110–111
    port authentication, 114
        communications, 115–121
        functionality, 122
    port security, 107–109
SYN floods
    rate limiting with CAR, 617
    thwarting with ACLs, 579–580
synchronization, NTP
    configuring, 68
    switch implementations, 77
syslog messages, PIX, 153–154
sysopt commands, 169–172
system access attacks, 402

T

TACACS+ (Terminal Access Controller Access Control Server plus)
    accounting, 508–512
    authentication, 498
    authorization, 499–507
    communications architecture, 494
    daemon functionality, 493–494
    header architecture, 495–497
    packet encryption, 497
TCP (Transmission Control Protocol)
    connection establishment through PIX, 148–150
    ISN, generating with ASA, 148
    NBAR recognized protocols, 600–602
    packet filtering with ASA, 148
TCP port 179, restricting BGP communications, 94
TCP reset, 443
TCP SYN floods, 405–407
    preventing with Cisco IOS Firewalls, 206
TED (Tunnel Endpoint Discovery), configuring, 379–391

TFN (tribal flood network) attack, 409–411
TFN2K attack, 411
threats, assessing, 6–7
three-legged firewalls, creating DMZs, 27
three-message exchange, L2TP, 246
threshold values, CBAC, 204–205
thwarting attacks with ACLs
  DoS attacks, 580–582
  fraggle attacks, 578–579
  smurf attacks, 576–578
  SYN floods, 579–580
timeout negotiation, 293
timeout values
  CBAC, 204–205
  PIX, 637
timers, OSPF configuration, 101
tiny fragment attacks, 174–175, 588
TLS (Transport-Layer Security) messages, 118
token buckets, 614–616
top-down processing (ACLs), 571
topographical designs, physical security, 36
ToS (type of service), marking packets, 605–607
traffic. *See also* traffic filters
  classifying with NBAR, 599–600
    recognizable protocols, 600–603
  controlling with CAR, 613–614
    compound interest measurement, 615–616
    dropping malicious traffic, 616–618
    token buckets, 614
  network flows, 594
  policing, 607
traffic filters
  ACLs, 572–573
    blocking IMP packets, 573–575
    blocking known offenders, 575
    blocking spoofed IP addresses, 575
    extended, 569–571
    functionality, 567–568, 573
    impact on performance, 590
    implicit deny all entry, 571
    logging facility, 573
    standard, 568
    thwarting DoS attacks, 580–582
    thwarting fraggle attacks, 578–579
    thwarting smurf attacks, 576–578
    thwarting SYN floods, 579–580
    top-down processing, 571
  black hole filtering, 87–88
  PIX Firewall, 165
transform payloads, IKE SA timeout negotiation, 284
transport layer inspection, Cisco IOS Firewall, 202
transport mode (IPsec) encapsulation, 314
Trinoo DDoS attack, 408
troubleshooting
  AAA, 670–677
  IDS problems, 666–670
  IOS Firewalls, 647–648
    common problems, 651–652
    debug commands, 650–651
    show commands, 648–649
  IPsec problems, 661–666
  NAT, 629–633
  PIX, 633–634, 643–645
    common problems, 643–645
    connectivity, 645–647
trunking, VLAN security, 106
Tsutomu Shimomura, 421–422
TTL field (VRRP packets), 51
TTY lines, 55
  controlling router access, 58
Tunnel ID field (L2TP header), 250
tunnel mode (IPsec) encapsulation, 314–316
tunneling
  IPsec, IKE negotiation
    aggressive mode exchange process, 302–306
    main mode exchange process, 280–302
  L2TP, 243
    compulsory tunnels, 245, 251–270
    control connection establishment, 246
    header format, 248–250
    session establishment, 247–248
    setup process, 246
    tunnel layers, 244
    voluntary tunnels, 245
  voluntary, 373–379
  with GRE between private networks, 227–230
turbo ACLs, 590–591
  configuring, 591–593
Type field
  L2TP header, 250
  VRRP packets, 52

U

UDP (User Datagram Protocol)
- transmission through PIX, 150
- NBAR recognized protocols, 600–602

unauthorized access, restricting with ACLs, 572–573
Unicast Reverse Path Forwarding. *See* URPF
unicode exploits, 418
unintentional inside attackers, 403
UNIX director
- configuring routers as sensors, 449–454
- internal architecture, 430
  - configd daemon, 431
  - eventd daemon, 432
  - fileXferd daemon, 431
  - loggerd daemon, 431
  - POP, 432
  - postofficed daemon, 430
  - sapd daemon, 431
  - smid daemon, 431
- shunning configuration, 462–463
- versus CSPM IDS Console, 429

unstable routing tables, controlling, 94
- maximum-prefix command, 97
- route dampening, 95–96

URPF (Unicast Reverse Path Forwarding), 88–89
- applying, 90
- configuring, 89
- PIX Firewall, 168

V-W

vendor-specific attributes supported on Cisco routers, 530–531
Version field
- L2TP header, 250
- VRRP packets, 52

Virtual IP Address field (HSRP), 46
virtual reassembly, 163
Virtual Router Redundancy Protocol. *See* VRRP
virtual routers, 42
Virtual Rtr ID field (VRRP packets), 52
viruses, Code Red worm, 608–610
VLANs, 105
- basic security rules, 105–106
- versus private VLANs, 111

voluntary tunneling, 245, 373–379
VPDN (Virtual Private Dialup Networking), 544–547
VPNs
- application layer, 219
- data link layer, 219
- encrypted, 218
- extranet, 220
- high-availability IPsec over GRE, 360–365
- intranet, 220
- IPsec, 653–654
  - debugs, 654–658
  - show commands, 658–660
- misconfigured access lists, troubleshooting, 662
- network layer, 219
- nonencrypted, 218
- one-to-many router IPsec, 355–360
- remote-access IPsec implementations, 366–368
- router-to-router IPsec
  - using digital signatures, 338–349
  - using preshared key authentication, 325–338
  - using RSA encrypted nonces, 349–354

VRRP (Virtual Router Redundancy Protocol)
- failure detection, 51
- master router selection, 50
- packet format, 51–54
- versus HSRP, 50

vty router access, 55
- controlling, 55–57

vulnerabilities
- assessing, 6–7
- of NAT, 131
- of underlying firewall operating systems, 140

X-Y-Z

x-auth (extended authentication), 318–320, 539–541
    for remote-access clients, 539–540
    VPN users, 541
x bits field (L2TP header), 250

ZLB ACKs, 248
zoning secure networks, 25–26
    case study, 30–31
    DMZs, 26–30