Index

Numerics

3DES (Triple Data Encryption Standard), 406

802.1x standard

authentication, 359, 377, 561
Cisco Secure ACS, 369, 377
client negotiation, 377–378
components, 357–359
configuration, verifying, 387–389
EAP, 359
operation, 359–362
options
defaults, resetting, 386
frame-retransmission number, 384–385
guest VLANs, 385–386
multiple hosts, 385
quiet period, 383
re-authentication, 382–383
retransmission times, 384
port-based authentication, 378–382
port state, 362
servers, authentication, 359
supplicants, 359
switch ports, 381
unauthorized state, 362

A

AAA (authentication, authorization, and accounting)

802.1x protocol, 377
access control, 125
accounting
Cisco IOS Software, 130, 140
Cisco Secure ACS, 181–182
configuring, 140
RADIUS, 164–165
TACACS+, 157
attributes, IETF, 115
authentication
Cisco Secure ACS, 178–179
configuring, 129–136
proxy, 72, 75, 129–130, 338, 584, See also authentication proxy
RADIUS, 162–163
TACACS+, 155–156
authorization
Cisco IOS Software, 130, 136–137
Cisco Secure ACS, 180–181, 210
configuring, 136–140
RADIUS, 163–164
TACACS+, 156
Cisco Secure ACS, 173, 178–182, 556–557
clients, 205
configuring
accounting, 140
authentication, 131–136
authorization, 136–140
overview, 130, 146, 338
RADIUS, 160–162, 169
TACACS+, 153–154, 169
databases
backup, 186
replication, 183–186
defense in depth, 50, 55
Easy VPN Remote, 597–599
Easy VPN Server, 593–596
ERROR responses, 130
FAIL responses, 130
IETF attributes, 115
RADIUS
accounting, 164–165
authorization, 163–164
configuring, 160–162, 169
overview, 122

    - *testing/troubleshooting, 166–167*
  - RDBMS synchronization, 186
  - responses, 130
  - server support, 72, 75, 116
  - switch ports, 381
  - TACACS+
    - *accounting+, 157*
    - *authentication, 155–156*
    - *authorization, 156*
    - *configuring, 153–154, 169*
    - *overview, 122*
    - *testing/troubleshooting, 157*
  - troubleshooting, 142
- **abbreviated commands, 67**
- **ACCEPT responses, RADIUS, 115**
- **acceptable use policies, 10**
- **access**
  - attacks, 37–39, 42
  - control
    - *accounting, 130*
    - *authentication, 129–130*
    - *authorization, 130*
    - *CBAC configuration, 585–586*
    - *interactive, 91*
    - *overview, 125, 129*
- **access control lists**
  - See ACLs
- **Access VPNs, 402**
- **accounting**
  - AAA, 130
  - Cisco IOS Software, 130, 140
  - Cisco Secure ACS, 181–182
  - RADIUS, 164–165
  - TACACS+, 157
- **ACEs (access control list entries), 221**
- **ACLs (access control lists), 71, 75, 221, 237, 247**
  - 802.1x protocol, 358
  - ACEs, 221
  - bypassing feature, 313
  - CBAC, 222, 309–318
  - Cisco Secure ACS, 180
  - configuring, 222, 228–230
  - crypto ACLs, 417, 574–576
  - dynamic ACLs, 71, 75
  - functions, 221
  - IP
    - *certificate-based, 228*
    - *extended, 226*
    - *overview, 222–226*
    - *reflexive, 226–227*
    - *time-based, 227–228*
  - packets, 228–230
  - permit statements, 222
  - VACLs, 296
- **Active Directory, Windows, 192**
- **addresses**
  - address pools, 490–491
  - addressing schemes, 10
  - dynamic secure, 286
  - lookup tables, 279
  - MAC addresses, 283
  - spoofing, 291–294
  - static/sticky secure, 286
- **Advanced Security feature set**
  - firewall engine, 245–246
  - routing support, 248
- **AH (Authentication Header), 409**
- **alerts, 72, 76, 310–311**
- **Apple clients, 179**
- **applets, 247**
- **applications**
  - attack targets, 50, *See also attacks*
  - weaknesses, 33
- **Arspoof tool, 292**
- **atomic signatures, 260**
- **Attack-drop.sdf, 260, 266**
- **attacks**
  - access attacks, 37–42
  - applications, 50

Arpspoof, 292
Attack-drop.sdf, 260, 266
block scans, 38
CAM table overflow attacks, 283–288
data, 50
DDoS attacks, 39, 49
DHCP
snooping, 292–293, 562
starvation, 296
dictionary attacks, 92
DNS
queries, 37
spoofing, 93
DoS attacks
CBAC, 310
DDoS attacks, 39, 49
firewalls, 248
overview, 37–42, 75, 92, 234, 260
EAP attacks, 296–298
exploits, 260
fabrication, 39
firewalls, 49
FTP sweeps, 38
gobbler tool, 296
horizontal scans, 38
hosts, 50
interception, 38
IP
source routing, 93
spoofing, 93
Layer 2 attacks, 283–300, 561–562
MAC address spoofing, 291–294
Macof, 285
management components, 50
man-in-the-middle attacks, 93, 291–294
misuse, 260
mitigating
CAM table overflow attacks, 286–288
DHCP starvation attacks, 296
EAP attacks, 297–300
MAC address spoofing, 292–294
man-in-the-middle attacks, 292–294
on private VLANs, 295
STP manipulation attacks, 290–291
VLAN hopping attacks, 289
modification, 39
motivations for, 30–36, 41
networks, 50
physical security, 54
ping sweeps, 38
reconnaissance attacks, 37–42, 260
routers, 49
scans, 38
session-hijacking attacks, 93
signatures
atomic, 260
attack signatures, 259
unsupported signatures, 261
Smurf attacks, 232
SNMP traps, 92
spoofing
DNS, 93
IP, 93
MAC addresses, 292–294
STP manipulation attacks, 289–291
switches, 49, 279
SYN floods, 71, 310
targets, 49
unstructured threats, 34
Trojan horses, 39
vertical scans, 38
viruses, 39
VLANs
hopping attacks, 288–289
vulnerabilities, 294–295
vulnerabilities, 29, 40–41
worms, 39
attributes field, RADIUS, 115
auditing
audit trails, 247–249
CBAC, 310–311
overview, 71–75
authentication
802.1x
client negotiation, 377–378
defaults, resetting 386
configuration, verifying, 387–389
frame-retransmission number, 384–385
guest VLANs, 385–386
multiple hosts, 385
quiet period, 383
re-authentication, 382–383
retransmission time, 384
port-based, 378–382
overview, 377, 561
Active Directory, 192
CAs, 438–440
Cisco Secure ACS, 178–179, 189–191, 210
configuring

    - *line password authentication, 111–112*
    - *login authentication, 132–133*
    - *overview, 131–132*
    - *PPP authentication, 134–136*
    - *usernames, 112*
- EAP
    - *EAP-FAST, 366–367*
    - *EAP-MD5, 363*
    - *EAP-TLS, 364–365*
    - *LEAP, 363*
    - *network requirements, 368*
    - *PEAP, 365–366*
- Easy VPN, 488
- firewalls, 72
- frame-retransmission number, 384–385
- hosts, multiple 385
- IKE, 405, 439
- IPsec, 439
- line password authentication, 111–112
- login authentication, 132–136
- MD5, 234, 363
- method list, 130
- neighbor routers, 72, 76
- NFS, 33
- OTPs, 111
- passwords, 111, 133–134
- peer routers, 247
- PPP, 134–136
- protocols
    - *CHAP, 117–119*
    - *EAP, 120–121*
    - *MS-CHAP, 119–120*
    - *PAP, 118*
    - *routing, 233–234*
- proxy, 72, 75, 129–130, 338, 584
- quiet periods, 383
- RADIUS, 162–163
- re-authentication, 382–383
- remote security servers
    - *CHAP, 118–119*
    - *EAP, 120–121*
    - *Kerberos, 117*
    - *MS-CHAP, 119–120*
    - *PAP, 118*
    - *RADIUS, 114*
    - *TACACS, 112–114*
- remote users, 118–122
- retransmission time, 384
- routers
    - *CA support, 438–439*
    - *neighbor routers, 72, 76*
    - *peer routers, 247*
    - *routing protocols, 233–234*
- RSA keys, 439
- SNMPv3, 231
- switch ports, 381
- TACACS+, 155–156
- token cards, 111
- usernames, 111–112
- users, remote 117
- VLANs, 385–386
- X.509 standard, 439

Authentication Header (AH), 409

authentication proxy
- AAA, 72, 75, 129–130, 338, 584
- CBAC, 336
- Cisco IOS Firewall, 248, 333, 336
- Cisco Secure ACS, 344–349
- configuration
    - *types, 337*
    - *overview, 337–339*
    - *AAA, 584*
    - *HTTP servers, 585*
    - *inbound/outbound authentication, 341–342*
    - *routers, 585*
    - *testing/verifying 584–585*
- features, 336
- firewalls, 336
- HTTP
    - *connections, 335*
    - *servers, 339*
- IPsec encryption, 336
- limitations, 349
- RADIUS, 347–349
- TACACS+, 344–347
- VPNs, 336

authentication, authorization, and accounting
- *See* AAA

authenticator field, RADIUS, 114

authorization
- AAA, 130
- Cisco Secure ACS, 180–181, 210
- configuring, 136–140
- RADIUS, 163–164
- overview, 72, 76
- TACACS+, 156

AutoSecure feature, 99
auxiliary connections, 68, 74
availability, 129, 358

B

backup databases, 186
banners, 90–91
block scan attacks, 38
border routers, 222
BPDU guard, STP, 290
broadcasts, 232–233
bypassing feature, ACL, 313

C

CAM (content-addressable memory)
- entries, 98
- lookup tables, 279
- overflow attacks, 283–288

CAs (certificate authorities)
- configurations, verifying, 450
- digital signatures, 437
- interoperability, 433
- IPsec, 440–450, 578–579
- peer authentication, 440
- routers, 441
- SCEP, 439–440
- show commands, 460
- X.509 standard, 439

CBAC (Context-Based Access Control)
- ACLs, 222, 309–318
- alerts/audit trails, 309–311
- authentication proxy, 336
- Cisco IOS Firewall, 585–586
- configuring, 318, 324–325, 585–586
- CPU/performance impact, 317–318
- debug commands, 323–324
- DoS attacks, 310
- firewalls, 585–586
- H.323 inspection, 316
- ICMP types supported, 310–311
- inspection rules, 320–323
- interfaces, 318
- Java applets, 322
- operation, 311–314
- overview, 71–75
- PAM, 319–320, 251
- protocols, 314–316
- restrictions, 314
- RTSP, 315–316
- sessions, 311–314
- show commands, 323–324
- timeouts/thresholds, 319
- utilization, improving, 317
- verifying/debugging, 323–324

CDP (Cisco Discovery Protocol), 235, 562
certificates
- certificate-based IP ACLs, 228
- certificate revocation lists (CRLs), 440
- Cisco Secure ACS, 566
- Easy VPN, 488
- IPsec, 577–579
- overview, 437, 566
- X.509 standard, 439

Challenge Handshake Authentication Protocol (CHAP), 118–122, 179
- *See* CHAP

CHALLENGE responses, RADIUS, 115
change management, 10
CHANGE PASSWORD responses, RADIUS, 115
CHAP (Challenge Handshake Authentication Protocol), 118–122, 179
Chargen port, 234
Cisco Discovery Protocol (CDP), 235
Cisco IOS Firewall
- advanced firewall engine, 246
- authentication proxy, 248, 333, 336
- CBAC
  - *alerts/audit trails, 309–311*
  - *configuring, 318, 585–586*
  - *CPU/performance impact, 317–318*
  - *DoS attacks, 310*
  - *H.323 inspection, 316*
  - *inspection rules, 320–322*
  - *operation, 311–314*
  - *PAM, 319–320*
  - *protocols, 314–315*
  - *restrictions, 314*
  - *RTSP, 315–316*
- DoS attacks, 248
- feature set, 361, 241–246 333
- features/functions, 71–74 245
- IDS, 336, 255
- IPS, 71, 75, 246, 255
- overview, 61, 241, 305
- transparency, 247
- URLs, 251
- VPNs, 246
- *See also* firewalls

Cisco IOS Intrusion Detection System (IDS), 336, 255

Cisco IOS Intrusion Prevention System (IPS)
- CLI, 262
- configuration
  - *process, 262–266*
  - *verifying 270–273*
- deployment strategies, 273–274
- false positive/negative, 267
- features, 259–260
- firewalls, 71, 75, 246, 255
- functions, 260
- malicious traffic, 262
- notification types, 263
- rules, 268–269
- SDF, 260, 266
- signatures, 260–261
- SME, 260

Cisco IOS Software
- accounting, 130, 140
- Advanced Security feature set, 248
- authorization, 130, 136–137
- configuring
  - *RADIUS, 160–162*
  - *TACACS+, 153–154*

Cisco Router and Security Device Manager
- *See* SDM

Cisco Secure ACS (Access Control Server)
- 802.1x authentication, 369, 377
- AAA, 173, 178–182, 556–557
- ACLs, 180
- accounting, 181–182
- administration, 182–183
- Apple clients, 179
- attributes, vendor-specific, 181
- authentication
  - *overview, 178–179*
  - *proxy, 344–349*
  - *users, 189–191*
- authorization, 180–181
- certificates, 566
- CHAP, 179
- databases
  - *backup/replication, 183–186*
  - *external users, 178*
  - *local, 191–192*
  - *support, 189–191*
- deploying, 203–209
- LDAP, 193
- maximum numbers
  - *AAA clients, 205*
  - *users, 204*
- PAP, 179
- passwords
  - *aging, 179*
  - *protocols, 179, 190–191*
- PEAP, 562–568
- RDBMS synchronization, 186
- services, 187–189
- token server, 193
- transactions per second, 205
- troubleshooting, 209–211
- UCP, 194
- vendor attributes, 181
- Windows
  - *installing for, 205, 208*
  - *Windows NT/2000, 192–193*

Cisco Secure Policy Manager (CSPM), 264

Cisco Security Device Manager
- *See* SDM

Cisco Unix Director, 264

CiscoSecure Integrated Software (CSIS), 71

CiscoWorks VPN/Security Management Solution IDS Management Center (VMS IDS), 263

clear commands
- clear crypto isakmp command, 473
- clear crypto sa command, 473
- clear crypto sa counters, 474
- connecttivity, 460, 472
- overview, 273

CLI (command-line interface) routers, 68–70, 74

client mode, 525

clock commands, 571

Code field, EAP, 360

code field, RADIUS, 114

commands
- ?, 67
- 802.1x, enabling, 297, 381
- AAA commands
  - *accounting, 141*
  - *authentication, 131*
  - *authentication attempts login, 136*
  - *authentication enable default, 133*
  - *authentication login, 132*
  - *authentication ppp, 134*
  - *authorization, 138*
  - *troubleshooting 142–143*

audit trails, 249
abbreviated, 67
attacks
  private VLAN proxy attacks, mitigating 295
  router attacks, preenting 237
authentication
  802.1x port-based, 380
  proxy, 339
banner login commmand, 90
CA configurations, verifying 450
clear commands, 273, 460, 472–474
configuring
  AAA, 338
  authentication proxy, 339
  AutoSecure, 100
  console interface, 85
  DAI, 294
  DHCP snooping, 293
  dynamic port security, 288
  HTTP servers, 339
  interface inspection rules, 323
  notification types, 264
  queue size, 265
  Reverse Telnet, 96
  SCP, 94–96
  SSH
crypto ca trustpoint command, 444
debug commnds, 273
  802.1x authentication, 390
  aaa accounting, 145, 167
  aaa authentication, 144, 157
  aaa authorization, 144
  connectivity, 460, 467
  crypto engine, 468
  crypto ipsec, 468
  crypto isakmp, 467
  crypto key-exchange, 467
  crypto pki, 470
  crypto pki transactions, 471
  radius, 166
  tacacs, 158
  tacacs events, 158
enable commands
  password command, 85
  secret command, 86–87
encryption
  MD5, 88
  passwords, 112
EXEC mode, accessing, 85
exec-timeout command, 92
IPS configurations, veifying, 270–273
logging, 249
login, blocking 93
MD5 encryption, 88
passwords, encrypting 112
period re-authentication, 382
policies, attaching to signatures, 267
ppp authentication command, 135
private VLAN proxy attacks, mitigating 295
privilege command, 88
privilege level, 86
radius-server host command, 160
radius-server retry method command, 161
router attacks, preventing, 237
SDFs, 266
service password-encryption command, 88
show commands
  802.1x authentication, 387–389
  aaa servers, 142
  aaa user, 143
  accounting, 167
  overview, 89, 270
  VPN connectivity, 459–466
tacacs-server host command, 153
transport input, command 91
username secret command, 88
compound signatures, 260
confidentiality, 93, 129
configuration
  802.1x protocol, 387–389
  AAA, 131–140
  ACLs, 222, 228–230
  CAs, 450
  CBAC, 585–586
  IKE, 412–414, 572–573
  IPSs, 262–266
  IPsec, 449–450
  management, 10
  network, 31–32
  RADIUS servers, 160–162, 169
  routers modes
    global configuration mode, 66, 73
    interface configuration mode, 66
    line configuration mode, 66
    privileged EXEC mode, 65, 73
    ROM monitor mode, 65, 73
    user EXEC mode, 65, 73
  TACACS, 153–154, 169

console access, 84–85
connections, 68, 74
Context-Based Access Control
See CBAC
continuity, 30, 40
correlation, 53, 56
crackers, 34, 41
CRLs (certificate revocation lists), 440
crypto
ACLs, 417, 574, 576
maps, 418–419, 464, 494–495, 574–580
CSAdmin service, 187–188
CSAuth service, 187–188
CSDBSync service, 186–188
CSIS (CiscoSecure Integrated Software), 71
CSLog service, 187–188
CSMon service, 187, 189
CSPM (Cisco Secure Policy Manager), 264
CSRadius service, 187, 189
CSTacacs service, 187, 189
cyber-attacks
See attacks
cyber-warfare, 36

D

DAI (Dynamic ARP inspection) feature, 293
Data Encryption Standard (DES), 406
Data field, EAP, 360
Database Replication Report, 186
Daytime port, 234
DDoS (distributed denial-of-service) attacks, 39, 49
dead peer detection (DPD), 487, 495
debug command, 273
802.1x authentication, 390
AAA, 142–145
aaa accounting command, 145, 167
aaa authentication command, 144, 157
aaa authorization command, 144
CBAC, 323–324
connectivity, 460, 467
crypto engine command, 468
crypto ipsec command, 468
crypto isakmp command, 467
crypto key-exchange command, 467
crypto pki command, 470
crypto pki transactions command, 471
IKE/IPSsec, 581
radius command, 166
tacas command, 158
tacas events command, 158
defense in depth, 49–55
demilitarized zones (DMZs), 298
denial-of-service attacks
See DoS attacks
DES (Data Encryption Standard), 406
DHCP (Dynamic Host Configuration Protocol)
guest VLANs, 386
snooping, 292–293, 562
starvation attacks, 296
dictionary attacks, 92
Diffie-Hellman encryption, 407
digital certificates
Easy VPN, 488
IPsec, 57–579
X.509 standard, 439
See also certificates
directed broadcasts, disabling, 232–233
diaster recovery, 30, 40
Discard port, 234
distributed denia-of-service (DDoS) attacks, 39, 49
See DoS attacks
distribution, security policies, 17
DMVPNs (Dynamic Multipoint VPNs), 530–534
DMZs (demilitarized zones), 298
DNS (Domain Name Server)
domains, 560
queries, 37
spoofing, 93
domain names, 94
DoS (denial-of-service) attacks
CBAC, 310
DDoS attacks, 39, 49
firewalls, 248
overview, 37–42, 49, 75, 92, 234
SYN floods, 71, 310
double tagging, 289
DPD (dead peer detection), 487, 495
Dynamic ARP inspection (DAI) feature, 293
Dynamic Multipoint VPNs, 530–534

E

EAP (Extensible Authentication Protocol)
802.1x, 359
attacks, 296–298
EAP-FAST, 366–367

EAP-MD5, 363
EAPOL, 360
EAP-TLS, 364–365
frame format, 360–362
LEAP, 363
network requirements, 368
overview, 120–122
PEAP, 365–366
response frames, 384

EAP Flexible Authentication via Secure Tunneling (EAP-FAST), 366–367

EAP over LANS (EAPOL), 360

EAP Transport Layer Security (EAP-TLS), 364–365

EAP-FAST (EAP Flexible Authentication via Secure Tunneling), 366–367

EAPOL (EAP over LANs), 360

EAP-TLS (EAP Transport Layer Security), 364–365

Easy VPN
address pools, 490–491
authentication, 488
configuring, 489–496
crypto maps, 494–495
DPD, 495
group policies, 492–493
group policy lookup, 491
ISAKMP policies, 492
modes, 496
operation, 488–489
overview, 479
Remote, 484–485, 525–526, 597–599
routers, 491
SDM
Remote, 525–526, 597–599
Server, 528–530
Server
configuring, 489–496
functionality, 483–488
SDM, 528–530
transform sets, 493–494
Xauth, 496

Echo port, 234

e-mail, 10

enable password, 85–86

Encapsulating Security Payload (ESP), 409

encryption
Diffie-Hellman, 407
interception attacks, 38
IPsec, 94, 336, 404
MD5, 88, 407
NFS, 33
passwords, 87–88
public key cryptography, 437
RSA-encrypted nonces, 405, 423–427
SNMPv3, 231
SSH, 68, 94

endpoints, 401

ERROR responses, AAA, 130

escalation, privilege, 39

ESMTP (Extended Simple Mail Transport Protocol), 315

ESP (Encapsulating Security Payload), 409

Ethernet switches, 97–98

events
buffers, 265
Event Log, 186
logging, 72, 76, 247
security, 10

EXEC mode, 85

Execution Shell, 94

exploit attacks, 260

Extended Simple Mail Transport Protocol (ESMTP), 315

Extensible Authentication Protocol
See EAP

extranet VPNs, 402

F

fabrication attacks, 39

Factory Reset Wizard, SDM 536–537

FAIL responses, AAA, 130

Failed Attempts Report, 209

failover, 247

false negatives/positives, 267

feasibility, security policies, 15

feature sets
Advanced Security, 241
Firewall, 61, 241–246 333
IPS, 259

filtering
traffic, 71, 247
URLs, 247, 251

finger service, 235

fingerprinting, 235

Firewall feature set, 61, 241–246 333

firewalls
applets, blocking, 247

attack target, 49
audit trails, 247
authentication proxy, 248, 333, 336
CBAC
alerts/audit trails, 309–311
configuring, 318
CPU/performance impact, 317–318
defining inspection rules, 320–322
DoS attacks, 310
H.323 inspection, 316
operation, 311–314
PAM, 319–320
protocols, 314–315
restrictions, 314
RSTP, 315–316
event logging, 247
features, 71–72
filtering
traffic, 247
URLs, 247, 251
managing, 247
mitigating DoS attacks, 247–248
NAT, 247
overview, 61, 79, 241, 245, 305
port mapping, 247
SDM, 515, 541
advanced options, 519–521
applying config to routers, 518–519
configuring interfaces, 516–518
selecting type, 515–516
traffic, filtering, 247
URLs, filtering 247, 251

flexibility, security policies, 16
frames, 360–362, 384
FTP sweeps, 38

G

GARP (Gratuitous ARP), 292
Generic Lightweight Directory Access Protocol (LDAP), 193
global
configuration mode, 66, 73
filtering, URLs, 251
implementation, security policies, 15
goals
network attacks, 37
security policies, 12–13, 20
gobbler tool, 296
group policies, Easy VPN, 491–493
guidelines, security policies, 13–21

H

H.323 inspection, 316
hackers
ethical hackers, 34
hacktivism, 36
Microsoft, 32
motivations, 34–36, 41
half-open sessions, 314
handshakes, 118
hardware weaknesses, 33
hash, 234
high availability, 129, 358
hijacking, sessions, 93, 297
HMAC (Keyed-Hashing for Message Authentication), 406
hopping attacks, VLANs, 288–289
horizontal scan attacks, 38
hosts
802.1x authentication, 385
attack target, 50
host-based defenses, 53
hostile, 52
IPSs, 56
names, 94, 560
port mapping, 320
HTTP
authentication proxy, 585
connections, 335
SDM, 511
servers, 339
HTTPS (Secure HTTP), 232, 511

I

IBNS (Identity-Based Networking Services), 353
ICMP types, CBAC, 310–311
Identifier field
EAP, 360
RADIUS, 114
Identity frames, 384
IDS (intrusion detection system), 255, 336
IDS Management Center (MC), 264
IEEE 802.1x standard
See 802.1x standard
IETF (Internet Engineering Task Force) attributes, RADIUS, 115

IKE (Internet Key Exchange)
- configuring, 412–414, 572–573
- crypto maps, 580
- debut command output, 581
- DPD, 487, 495
- enabling, 575
- IPsec, preparing for, 571–572
- ISAKMP peers, 406
- keys, 405
- overview, 404, 439–441, 448
- Phase 1, 405–408
- policies, 579–580
- preshared keys, 405, 572–573
- RSA
  - *signatures, 405, 575–576*
  - *encrypted nonces, 405*
- SAs, 583
- transform sets, 580
- Xauth, 487

in traffic, 226

incident-response plans, 17–18

infrastructure, network, 10

inspection, 320–322

integrity, 93, 129

interactive access, 91

interception
- attacks, 38
- passwords, 93

interesting traffic, 417

interface configuration mode, 66

interleaved mode, 316

Internet
- access, 10
- services, 31, 41

Internet Control Message Protocol (ICMP) types, CBAC, 310–311

Internet Key Exchange
- *See* IKE

Internet Security Association and Key Management Protocol (ISAKMP), 461

internetworking, 49

interoperability, CAs, 433

intranet VPNs, 402

intruders, 34–36, 41

intrusion detection system
- *See* IDS

intrusion prevention system
- *See* IPS

IP
- ACLs
  - *certificate-based, 228*
  - *extended, 226*
  - *reflexive, 226–227*
  - *standard, 222–226*
  - *time-based, 227–228*
- source routing, 93
- spoofing, 93

IPS (intrusion prevention system)
- Cisco, 586–592
- CLI, 262
- configuring, 262–266
- deployment strategies, 273–274
- false positive/negative, 267
- features, 259–260
- functions, 260
- malicious traffic, 262
- notification types, 263
- rules, 268–269
- SDF, 260, 266
- SDM, 586–592
- signatures, 260–261
- SME, 260

IPsec
- CAs, 433
- certificates, 577–579
- configuration
  - *ACLs, 412, 417–418*
  - *connectivity, verifying, 411*
  - *crypto maps, 417–418*
  - *IKE, 404–407, 412–414*
  - *transform sets, 415–416*
  - *overview, 449–450*
  - *policies, 408–411*
  - *manual configuration, 423*
  - *preshared keys, using, 573–575*
  - *router configurations, verifying, 411*
  - *SA lifetimes, 416–417*
  - *testing/verifying, 419*
- debugging, 581
- encryption, 94, 336
- IKE, 404, 412–414
- modes, 408
- overview, 403
- preshared keys, configuring with, 574–575
- policies, 408–411

RSA-encrypted nonces
configuring host/domain name, 423–424
planning for, 424
RSA keys, 424–427
SAs, 416–417, 462, 574–583
transforms, 410
transparent mode, 408
tunnel mode, 408
VPNs
CAs, 437
configuring, 440–450
digital signatures, 437
tunnels, 403–404
ISAKMP (Internet Security Association and Key Management Protocol)
debugging
commands, 467
events, 581
overview, 461
peers, 406
policies, 406, 492
See also IKE
ISAKMP/Oakley key exchange, 439

J–K

jargon, security policies, 15
Java
blocking, 322
code, 71, 75
inspection, 322
Kerberos, 72, 75, 117
Keyed-Hashing for Message Authentication (HMAC), 406
keys
IKE, 405
distribution, 405
preshared
common convention, establishing, 570
Easy VPN, 488
IKE, 405, 572–573
IPsec, 573–575
overview, 413
router setup, 570–571
RSA
deleting, 443
overview, 95, 439
show commands, 465–466
signatures, 448
encrypted nonces, 423
SSH, 560

L

LAN Wizard, SDM, 513
Layer 2 attacks
CAM table overflow attacks, 283–288
DHCP starvation attacks, 296
IEEE 802.1x EAP attacks, 296–298
MAC address spoofing, 291–294
man-in-the-middle attacks, 291–294
mitigating
CAM table overflow attacks, 286–288
DHCP starvation attacks, 296
EAP attacks, 297–300
MAC address spoofing, 292–294
man-in-the-middle attacks, 292–294
private VLAN attacks, 295
STP manipulation attacks, 290–291
VLAN hopping attacks, 289
overview, 561–562
STP manipulation attacks, 289–291
VLAN hopping attacks, 288–289
Layer 3 switching, 49
LDAP (Generic Lightweight Directory Access Protocol), 193
LEAP (Lightweight Extensible Authentication Protocol), 363
least-privilege policy, 10
legal issues, security, 19, 90
Length field
EAP, 360
RADIUS, 114
line configuration mode, 66
link-down traps, 98
LLQ (low-latency queuing), 248
load balancing, 161, 169
Local Authentication Service, 358
lock-and-key traffic filtering, 71
lockdown, MAC address, 97
logging
AAA, 140
logs, 10
overview, 72, 76, 249
SDM, 544
logins
attempts, limiting, 136
authentication, 132–133, 335
features, 92
RADIUS, 115

lookup tables, 279
low-latency queuing (LLQ), 248

M

MAC addresses
lockdown, 97
modes, 97
port security, configuring 99
spoofing, 291–294
Macof tool, 285
man-in-the-middle attacks, 93, 291–297
manipulation attacks, STP, 289–291
maps, crypto, 418–419, 464, 494–495, 574–580
MC (Management Center), IDS, 264
MD5 (Message Digest 5)
authentication, 234, 363
encryption, 88, 407
message
digests, 234, 406
integrity, SNMPv3, 231
method lists, 130
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 119–122
misuse attacks, 260
modes
client, 525
Easy VPN Server, 496
EXEC, 85
interleaved, 316
IPsec, 408
MAC addresses, 97
monitor, 541, 544
network extension, 526
push configuration, 492–493
restrictive, 97
router configuration
global configuration, 66, 73
interface configuration, 66
line configuration, 66
privileged EXEC, 65, 73
ROM monitor, 65, 73
user EXEC, 65, 73
shutdown, 97
modification attacks, 39
monitoring
general, 10, 53
monitor mode, 541, 544
MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 119–122
multicast/multiprotocol support, 248

N

naming conventions, 10
NAT (Network Address Translation), 72, 76, 247, 538
network extension mode, 526
Network File System (NFS), 33
Network Time Protocol (NTP), 235
networks
addressing schemes, 10
attack targets, 50
configuration weaknesses, 31–32
hostile networks, 52
infrastructure policies, 10
overview, 5
security, *See* security
segmentation, 52, 55
NFS (Network File System), 33
notification, legal 90, 263
NTP (Network Time Protocol), 235

O–P

one-step lockdown, SDM, 536
one-time passwords (OTPs), 111
out traffic, 226
out-processing procedures, 36
overflow attacks, 283–288
Packet Type field, EAPOL, 361
packets, 114, 228, 259
PAM (port to application mapping) feature
CBAC, 319–320
overview, 72, 75, 249
port mapping
host-specific, 251
system-defined, 249
user-defined, 250–251
PAP (Password Authentication Protocol), 118, 122, 179
passwords
aging, 179
authentication, 111
case sensitivity, 111
Cisco Secure ACS, 179, 190–191
console access, securing, 84
default, 32

enable password, 85–86
encryption, 87–86
interception, 93
privilege levels, 84, 89, 133–134
SSH, 92
Telnet, 92
weak/exposed, 31, 41

PAT (Port Address Translation), 72

patches
managing, 30
security policy, 10

PEAP (Protected EAP), 365–366, 562–568

Perfect Forward Secrecy, 411

perimeter security, 53–55

permit statements, 222

Phase 1, IKE, 405–407

Phase 2, IKE, 408

phreakers, 34, 41

physical terminal lines, 91

ping sweeps, 38

PKI debug commands, 470–471

policies, security, 10–20

POP (PostOffice Protocol), 263

Port Address Translation (PAT), 72

ports
mapping
host-specific, 251
overview, 247–249, 320
system-defined, 249
user-defined, 250–251
See also *PAM*
security, 97–98
802.1x security, 358
Cisco Secure ACS, 208
NFS, 33
private VLANs, 294
small server services, 234
trunk, 98, 561

Post Office Protocol (POP), 263

preshared keys
configuring/verifying initial router setup, 570–571
Easy VPN, 488
establishing common convention, 570
IKE, 405, 572–573
IPsec, 573–575
See also keys

private VLANs, 294–295

privileges
escalation, 39
levels, 84
authentication proxy, 333
configuring multiple levels, 88–89
enable password, 85–86
passwords, 89
unauthorized escalation, 39

privileged EXEC mode, 65, 73, 84–85

process, security, 18–21, 54–56

protect
actions, 286
mode, 97

Protected EAP (PEAP), 365–366
protocols
See specific protocol

proxy, authentication
AAA, 72, 75, 129–130, 338, 584
CBAC, 336
Cisco IOS Firewall, 248, 333, 336
Cisco Secure ACS, 344–349
configuration
types, 337
overview, 337–339
AAA, 584
HTTP servers, 585
inbound/outbound authentication, 341–342
routers, 585
testing/verifying 584–585
features, 336
firewalls, 336
HTTP
connections, 335
servers, 339
IPsec encryption, 336
limitations, 349
RADIUS, 347–349
TACACS+, 344–347
VPNs, 336

public key cryptography, 437, 439

Q–R

QoS (quality of service)
LLQ, 248
SDM, 538, 541

question mark (?) command, 67

quiet period, 92, 383

RADIUS (Remote Authentication Dial-In User Service)
- ACCEPT responses, 115
- authentication
  - *802.1x 381–382*
  - *overview, 162–163*
  - *proxy, 347–349*
- accounting, 164–165
- authorization, 163–164
- CHALLENGE responses, 115
- CHANGE PASSWORD responses, 115
- Cisco Secure ACS, 347–349
- configuring, 160–162
- firewalls, 72–75
- load balancing, 161
- login, 115
- overview, 114, 122, 169
- packet fields, 114
- REJECT responses, 115
- responses, 115
- TACACS+, versus, 116
- testing/troubleshooting, 166–167
- VLAN assignment, 380

RDBMS (relational database management system) synchronization, 186

RDT (RealNetworks Real Data Transport) protocol, 316

Real-Time Streaming Protocol (RTSP), 315–316

Real-Time Transport Protocol (RTP), 316

re-authentication, 382–383

reconnaissance attacks, 37–38, 42, 260

redundancy, 247

reflexive
- ACLs, 71, 75
- IP ACLs, 222, 226–227

REJECT responses, RADIUS, 115

relational database management system synchronization (RDBMS), 186

remote access, **Easy VPN, 479**

Remote Authentication Dial-In User Service
- *See* RADIUS

remote security servers
- CHAP, 118–122, 179
- EAP, *See* EAP
- Kerberos, 72, 75, 117
- MS-CHAP, 119–120
- PAP, 118, 122, 179
- RADIUS, *See* Radius
- TACACS, 112–114, *See also* TACACS+

Remote Site IEEE 802.1x Local Authentication Service, 358

remote users
- CHAP authentication, 118–119
- EAP authentication, 120–121
- MS-CHAP authentication, 119–122
- PAP authentication, 118

remote-access VPNs, 402

replication, databases, 183–186

responses
- AAA, 130
- incident-response plans, 17–18
- RADIUS, 115
- security events, 11

responsibilities/roles, security policies, 16

restrict actions, 286

restrictive mode, 97

retransmission, 384–385

reverse route injection (RRI), 489

reverse Telnet, 96

risk, analyzing, 11

roles/responsibilities, security policies, 16

ROM monitor mode, 65, 73

root guard, STP, 290

routers
- ACLs, 221–222
  - *certificate-based IP, 228*
  - *configuring, 228–230*
  - *extended IP, 226*
  - *reflexive IP, 226–227*
  - *standard IP, 223–226*
  - *time-based IP, 227–228*
- advanced support, 248
- attack target, 49
- authentication
  - *CA support, 438–439*
  - *neighbor routers, 72, 76*
  - *peer routers, 247*
  - *proxy, 585*
  - *routing protocols, 233–234*
- border routers, 222
- browsers, controlling access via, 231
- CAs, 438–441
- CBAC, 585–586
- CDP, 235
- Cisco IOS
  - *Firewall, 61, 245*
  - *router, 61*
- CLI, 68–70, 74
- configuration
  - *process, 558–560*
  - *modes, 65–68, 73*

directed broadcasts, disabling, 232–233
Easy VPN, 491
finger service, 235
global configuration mode, 66, 73
in/out traffic, 226
interface configuration mode, 66
IPsec VPNs, 437, 440–450
line configuration mode, 66
memory, 265
modes
global configuration, 66, 73
interface configuration, 66
line configuration, 66
privileged EXEC, 65, 73
ROM monitor, 65, 73
user EXEC, 65, 73
NTP, 235
peer routers, authenticating, 247
preshared keys, 570–571
privileged EXEC mode, 65, 73
ROM monitor mode, 65, 73
routing protocol, authenticating, 233–234
securing, 558–560
small server services, 234
SNMP, 230–231
SSH, 94–96, 69, 560
support, advanced, 248
TCP services, 234
Telnet, 32, 68
UDP services, 234
user EXEC mode, 65, 73
routing tables, 233
RRI (reverse route injection), 489
RSA (Rivest, Shamir, and Adelman) keys
deleting, 443
encrypted nonces, 405, 423–427
overview, 95, 439
show commands, 465–466
signatures, 405, 448, 575–576
RTP (Real-Time Transport Protocol), 316
RTSP (Real-Time Streaming Protocol), 315–316

S

SAFE, 54
SAs (security associations)
clearing, 581
counters, resetting, 474
IKE, 583
IPsec, 416–417, 462, 574–583
transform sets, 576
scan attacks, 38
SCEP (Simple Certificate Enrollment Protocol), 439–440
SCP (Secure Copy Protocol), 94–96
script kiddies, 34, 42
SDEE (Security Device Event Exchange), 263
SDF (signature definition file), 260, 266
SDM (Security Device Manager)
advanced options, 538–540
audits, 534–536
browsers, 510
configuring
DMVPN, 530–534
Easy VPN Remote, 525–526
Easy VPN Server, 528–530
site-to-site, 521–525
Easy VPN
Remote, 525–526, 597–599
Server, 528–530, 593–596
firewalls, 515–521, 541
hardware, 509
intrusion prevention, 538, 586–592
logging, 544
monitor mode, 541, 544
NAT, 538
OS requirements, 509
options, advanced 538–540
overview, 263, 505, 509
QoS, 538, 541
routing configuration, 538
security audits, 534–536
smart wizards, 509
software, 510–511
user interface, 511–513
wizards
Firewall, 515–521
Factory Reset, 536–537
LAN, 513
Security Audit, 534–536
smart wizards, 509
Secure Copy Protocol (SCP), 94–96
Secure Hash Algorithm 1 (SHA-1), 406
Secure HTTP (HTTPS), 232
Secure Shell
See SSH
Secure Sockets Layer (SSL), 232
Security
associations, *See* SAs
audits, 509, 534–536

events, 10
policies, 10–20
posture assessments (SPAs), 18
servers, remote, 112–120
wheel, 18, 54
zones, 298
See also attacks
Security Audit Wizard, SDM, 534–536
Security Device Event Exchange (SDEE), 263
Security Device Manager
See SDM
segmentation, 51, 55
session hijacking attacks, 93, 297
SHA-1 (Secure Hash Algorithm), 406
show commands
802.1x authentication, 387–389
AAA, troubleshooting, 142–145
CBAC, 323–324
overview, 270
privilege levels, 89
VPN connectivity
show crypto ca certificates, 460
show crypto ipsec sa, 462
show crypto ipsec security-assocation lifetime, 463
show crypto ipsec transform-set, 464
show crypto isakmp key, 464
show crypto isakmp policy, 461
show crypto key mypubkey rsa, 466
show crypto key pubkey-chain rsa, 465
show crypto map, 464
shutdown
actions, 286
mode, 97
signatures
atomic, 260
attack, 259
Attack-drop.sdf, 260
compound, 260
definition file, *See* SDF
IPSs, 53, 260–261
false positive/negative, 267
micro-engine, *See* SME
memory consumption, 261
merging files, 266
RSA keys, 405, 448, 575–576
SDF, 260, 266
unsupported, 261
VPNs, 437
Simple Certificate Enrollment Protocol (SCEP), 439–440
Site Security Handbook, 9, 19
site-to-site VPNs, 401, 521–525
smart wizards, SDM, 509
SME (signature micro-engine), 260
SMIL (Synchronized Multimedia Integration Language), 316
Smurf attacks, 232
SNMP (Simple Network Management Protocol)
routers, 230–231
traps, 92, 98
snooping, DHCP, 292–293, 562
soft tokens, 111
SPAs (security posture assessments), 18
SPAN (Switched Port Analyzer) ports, 98
Spanning Tree Protocol (STP)
BPDU guard, 290
manipulation attacks, 289–291
parameters, 562
root guard, 290
split tunneling, 486
spoofing, 93, 291–294
DNS spoofing, 93
IP spoofing, 93
man-in-the-middle attacks, 291–294
switches, 288
SSH (Secure Shell)
AutoSecure feature, 101
configuring
routers, 69
SSHv2 using host/domain name, 94
SSHv2 using RSA key pairs, 95–96
keys, 560
overview, 68, 87, 93–94
passwords, 92
reverse Telnet, 96
routers, 560
SCP, 94–96
setting up, 94
SSL (Secure Sockets Layer), 232
standard
ACLs, 71, 75
IP ACLs, 222–224, 226

starvation attacks, DHCP, 296
state, maintaining, 71
static/sticky secure MAC addresses, 286
STP (Spanning Tree Protocol)
- BPDU guard, 290
- manipulation attacks, 289–291
- parameters, 562
- root guard, 290

structured threats, 34
supplicants, 802.1x, 359
support, management, 14
sweep attacks, 38
Switched Port Analyzer (SPAN) ports, 98
switches
- attack target, 49
- attacks, 279
- ports, 98, 381
- security, 298
- spoofing, 288
- SSH, 94–96

SYN floods, 71, 310
Synchronized Multimedia Integration Language (SMIL), 316
syslog servers, 249
system
- auditing, 71, 75
- management, 10
- port mapping, 320

T

TACACS (Terminal Access Controller Access Control System), 112–114
TACACS+,
- accounting, 157
- authentication, 155–156
- authentication proxy, 344–347
- authorization, 156
- Cisco Secure ACS, 344–347
- configuring, 153–154
- firewalls, 72, 75
- overview, 113–114, 122, 169
- RADIUS, versus, 116
- testing/troubleshooting, 157–158

tagging, 289
targets, attacks, 49
TCP
- half-open sessions, 314
- inspection, CBAC, 322
- intercept, 71, 75
- services, 234
- SYN floods, 71, 310
- three-way handshake, 310

TCP/IP, 33
Telnet
- CLI, 68
- connections, 68, 74
- default, 32
- interactive access, 91
- passwords, 92, 112
- reverse Telnet, 96
- routers, 32, 68

Terminal Access Controller Access Control System
- *See* TACACS/TACACS+

terminal lines, 111–112
TFTP servers
- enable secret command, 87
- MD5 encryption, 88

threats, 34, 41
- *See also* attacks

three-way handshake, 310
thresholds, 319
throughput, 317
timeouts
- CBAC, 319
- vts, 92

TLS (Transport Layer Security), 232
token cards, 111
traffic, interesting 417
transform sets
- Easy VPN, 493–494
- IKE, 580
- IPsec, 415–416
- overview, 410, 464, 574–576

transparent mode, 408
Transport Layer Security (TLS), 232
transport protocols, 116
trending, 53, 56
Triple Data Encryption Standard (3DES), 406
Trojan horses, 39
trunk ports, 98, 561
ttys (physical terminal lines), 91
tunnels, 316, 389, 408

U

UCP (User Changeable Passwords), 194
UDP
  CBAC
    inspection, 322
    sessions, 313
  half-open sessions, 314
  services, 234
unauthorized state, 802.1x, 362
Unity Protocol, 485
unstructured threats, 34
  See also *attacks*
URLs, filtering, 247, 251
usage policy statements, 9
User Changeable Passwords (UCP) feature, 194
user EXEC mode, 65, 73, 84
usernames, 111–112
users
  account policies, 10
  group security, 298
  interface, SDM, 511, 513
  filtering, URLs, 251
  port mapping, 320

V

V3PNs (Voice and Video over VPNs), 248
VACLs (VLAN ACLs), 296
varsdb.MDB file, 192
vertical scan attacks, 38
violations, security policies, 17
Virtual Terminal Protocol (VTP), 562
virtual ttys
  See vtys
viruses, 39
VLAN ACLs (VACLs), 296
VLANs
  802.1x
    authentication, 385–386
    guest VLANs, 358
  hopping attacks, 288–289
  IBNS, 358
  ports, 294
  VACLs, 296
  voice ID, 358
  vulnerabilities, 294–295
VMS IDS (CiscoWorks VPN/Security Management Solution IDS Management Center), 263
Voice and Video over VPNs (V3PNs), 248
voice VLAN ID, 358
VoIP, 248
VSAs (vendor-specific attributes), 115
VTP (Virtual Terminal Protocol), 562
vtys (virtual ttys)
  passwords, 112
  securing access, 91–92
vulnerabilities, 29, 40–41
  See also attacks

W–X

warning banners, 90–91
weaknesses
  applications, 33
  hardware, 33
  network configuration, 31–32
  operating systems, 32
  passwords, 41
  protocol suites, 32
  security policies, 30–31
  TCP/IP, 33
  technology, 32–33
websites
  ACLs, certificate-based, 228
  authentication proxy, 337
  Kerberos, 117
  SAFE, 54
wheel, security, 18, 54
wizards
  Firewall, 515–521
  Factory Reset, 536–537
  LAN, 513
  Security Audit, 534–536
  smart wizards, 509
workstation configuration policy, 10
worms, 39
X.509 standard, 439
Xauth, 487, 496, 526, 530