

Index

Symbols

> (right-angle) bracket symbol, 63

? (question mark) symbol, 65

Numerics

3DES(TripleDataEncryptionStandard),312

A

AAA (authentication, authorization, and accounting), 47, 52

accounting, 120, 128–130

authentication, 119

configuring, 121–124

failed access attempts, 120

method lists, 119

authorization, 120, 125–127

Cisco Secure ACS, 162

configuring IOS firewall, 260

configuring services, 120

local database authentication, 406

overview, 119

troubleshooting, 130–132

aaa accounting auth-proxy default start-stop group tacacs+ command, 260

aaa accounting commands, 129

aaa accounting network start-stop radius command, 150

aaa authentication commands, 121, 142

aaa authentication login admins local command, 150

aaa authentication login default command, 260

aaa authentication login test radius local command, 148

aaa authentication ppp test if-needed radius command, 148

aaa authentication ppp test1 radius local command, 149

aaa authorization auth-proxy default command, 260

aaa authorization commands, 126

aaa authorization exec radius command, 148

aaa authorization network radius command, 148

aaa authorization network radius local command, 150

aaa new-model command, 142, 260

access attacks, 33–34

access control (CBAC), 235

configuration example, 245–246

DoS detection/protection, 235

functionality, 236

global timeouts and thresholds, 240

inspection rules, 241–243

inspection rules, applying to an interface, 244

IP access lists, 240

memory and performance impact, 239

protocols, 238

restrictions, 238

selecting an interface, 239

verifying and debugging, 244

access control lists. See ACLs

access lists

antispoofing, 408–409

CBAC, 69

Cisco IOS firewalls, 69

creating, 290

crypto maps, 414–415

access to commands, 83

access VPNs, 308

access-list numbers, 209

accounting, 120

- Cisco Secure ACSs, 165
- configuring, 128–130
- RADIUS, 148
- troubleshooting, 130–132

ACLs (access control lists), 207

- configuring on routers, 214
- crypto, 323
- overview, 207
- types of, 208
 - extended IP, 212*
 - reflexive, 212*
 - standard IP, 209–210*
 - time-based, 213–214*

administration

- Secure ACS, 165
- security
 - configuring multiple privilege levels, 87–88*
 - console access, 84*
 - enable password, 84–85*
 - enable secret command, 86*
 - service password-encryption command, 87*
 - warning banners, 89–90*

AH (Authentication Header), 315**AH-MD5-HMAC transform, 316****AH-SHA-HMAC transform, 316****alarms (Cisco IOS firewall IDS), 288****algorithms, hash, 312****anomaly-based IDS systems, 49****antispoofing, 408–409****applications**

- potential targets, 46
- weaknesses, 30

attack signatures, 288**attacks, 39**

- DoS, 11, 30

intruder motivation, 31

potential targets, 46

reasons for success, 28

smurf, 196

types of, 33

access, 34

DoS, 36

reconnaissance, 34

audits

Cisco IOS firewall IDS rules, 290

exclusions, 291

authentication, 119

CHAP, 110

Cisco Secure ACS, 162, 183

configuring, 121

line password, 105

login authentication, 122

password protection, 123

PPP authentication, 124

TACACS+, 141

username password, 105

failed access attempts, 120

method lists, 119

methods, 104

MS-CHAP, 111

overview, 104

PAP, 109

RADIUS, 148

remote security servers, 106–108

routing protocols, 197

troubleshooting, 130–132

Authentication Header (AH), 315**authentication proxy, 223, 251**

appearance, 256

case study, 423

compatibility with other features, 258

configuring, 258–265

functionality, 255

- overview, 255
- RADIUS, 270
- TACACS+, 266–269
- unidirectional function, 265

authentication, authorization, and accounting. See AAA

authorization, 120

- Cisco Secure ACS, 164, 183
- configuring, 125–127
- RADIUS, 148
- troubleshooting, 130–132

auth-proxy keyword, 260

auxiliary connection (Cisco IOS routers), 66

B

balancing business needs with security needs, 9

block scans, 34

breaches

- incident response plans, 16
- lack of understanding of computers or networks, 31

C

CA support, configuring (case study), 416

- enrolling routers, 418–419
- host/domain name, 417
- NTP, 417

CAs, 343

- authentication, 349
- Cisco routers, 343
- communicating with routers, 351
- configuring, 351
- declaring, 348
- interoperability, 343
- standards (RSA keys), 343

CBAC (context-based access control), 69, 222, 258

- configuration example, 245–246
- configuring
 - global timeouts and thresholds, 240*
 - inspection rules, 241–244*
 - IP access lists, 240*
 - selecting an interface, 239*
- DoS detection/protection, 235
- features, 235

- functionality, 236
- implementing (case study), 424–425
- memory and performance impact, 239
- protocols, 238
- restrictions, 238
- verifying and debugging, 244

CDP (Cisco Discovery Protocol), 199

Central Management Post Office Parameter, 286

certificate revocation list (CRL), 344

Challenge Handshake Authentication Protocol (CHAP), 110

cisco command, 325

Cisco Discovery Protocol (CDP), 199

Cisco Easy VPN. See Easy VPN

Cisco IOS

- CLI, 83
- RADIUS
 - configuring, 146–148*
 - troubleshooting, 150–151*
- router, 59
- TACACS+
 - configuring, 140–143*
 - troubleshooting, 144–145*

Cisco IOS firewall, 59

- AAA server support, 73
- access lists, 69
- authentication proxy, 70, 255, 272–273
 - appearance, 256*
 - compatibility with other features, 258*
 - configuring, 258–265*
 - functionality, 255*
- CBAC, 235
 - configuration example, 245–246*
 - DoS detection/protection, 235*
 - functionality, 236*
 - global timeouts and thresholds, 240*
 - inspection rules, 241–243*
 - inspection rules, applying to an interface, 244*
 - IP access lists, 240*
 - memory and performance impact, 239*
 - protocols, 238*
 - restrictions, 238*
 - selecting an interface, 239*
 - verifying and debugging, 244*
- configuring
 - for AAA, 260*

- for an internal source and an external destination, 264
 - event logging, 70
 - feature set, 222
 - Authentication proxy, 223
 - IDS, 224
 - logging and audit trail, 224
 - port-to-application mapping (PAM), 225–227
 - features, 72
 - functioning as HTTP servers, 261
 - IDS, 70, 279
 - adding to centralized management, 292
 - audit rules, 290–291
 - case study, 420–421, 423
 - Central Management Post Office parameter, 286
 - clear commands, 294
 - debug commands, 294
 - defining the protected network, 288
 - info and attack signatures, 288
 - initializing on routers, 286
 - maximum queue for alarms, 288
 - verifying configuration, 292
 - IPSec network security, 70
 - Java blocking, 69
 - NAT, 70
 - neighbor router authentication, 70
 - PAM, 70
 - real-time alerts, 70
 - security server support, 70
 - system auditing, 69
 - TCP intercept, 69
 - user authentication and authorization, 70
- Cisco IOS routers**
- accessing CLI, 66
 - configuration commands, 65
 - configuration modes, 63, 71
 - configuring CLI access, 68
 - enabling SSH server, 67
- Cisco Secure ACS (Cisco Secure Access Control Server), 157, 175**
- accounting, 165
 - administration, 165
 - authentication, 162
 - authorization, 164
 - deploying, 178
 - browser compatibility, 179
 - hardware requirements, 178
 - OS requirements, 178
 - installing, 180–181
 - ports requirements, 181
 - troubleshooting, 182–183
 - UNIX, 169–170
 - Windows, 161, 166
 - AAA, 162
 - CSAuth, 167
 - CSDBSync, 168
 - CSLog, 168
- CiscoSecure Intrusion Detection Sensor, 279**
- CiscoSecure Integrated Software, 69**
- CiscoWorks 2000**
- Router MC, 389
 - Sun Solaris installation, 384
 - user accounts, 397
 - Windows installation, 383
- clear ip audit configuration command, 294**
- clear ip audit statistics command, 294**
- CLI (command-line interface), 59, 63, 66–68, 83**
- client mode (Easy VPN), 371**
- clock set command, 346**
- clock timezone command, 346**
- command prompts, 65**
- command-line interface, 59, 63, 66–68, 83**
- commands**
- aaa accounting, 129
 - aaa authentication, 121
 - aaa authorization, 126
 - Cisco IOS router configuration, 65
 - configuring
 - AAA, 260
 - authentication proxy, 262
 - enable password, 84–85
 - enable secret, 86
 - service password-encryption, 87
 - verifying and debugging CBAC, 244
- compound signatures, 288**
- computers, vulnerabilities, 27**
- config-if command, 64**
- configuration weaknesses (network devices), 29**
- configure terminal command, 64**
- configuring**
- AAA services, 120
 - accounting, 128–130
 - authentication, 121

- authorization*, 125–127
 - login authentication*, 122
 - password protection*, 123
 - PPP authentication*, 124
 - ACLs on routers, 214
 - authentication proxy on IOS firewall, 258–265
 - AAA, 260
 - HTTP servers, 261
 - verifying configuration, 262
 - CA support (case study), 416
 - enrolling routers*, 418–419
 - host/domain name*, 417
 - NTP*, 417
 - CBAC
 - global timeouts and thresholds*, 240
 - inspection rules*, 241, 243
 - inspection rules, applying to an interface*, 244
 - IP access lists*, 240
 - selecting an interface*, 239
 - centralized manager for Cisco IOS firewall
 - IDS, 292
 - Cisco IOS routers, 63
 - CLI access*, 68
 - commands*, 65
 - global configuration mode*, 64
 - interface configuration mode*, 64
 - line configuration mode*, 65
 - privileged EXEC mode*, 63
 - ROM monitor mode*, 63
 - user EXEC mode*, 63
 - crypto maps, 414–415
 - CSACS for RADIUS, 270
 - Director's Post Office protocol, 288
 - enable password, 84–86
 - HTTP servers, 261
 - IKE parameters, 411–412
 - IKE with RSA signatures, 353
 - Internet services, 29
 - IPSec, 324, 354
 - IPSec parameters, 413–414
 - IPSec SA lifetimes, 323
 - IPSec with RSA encrypted nonces, 328–330
 - line password authentication, 105
 - local database authentication, 406
 - manual IPSec, 328
 - multiple privilege levels, 87–88
 - port security, 93
 - Post Office Protocol, 287
 - preshared keys, 319
 - RADIUS, 146–147
 - accounting*, 148
 - authentication and authorization*, 148
 - troubleshooting*, 150–151
 - remote access, 359, 363–370
 - routers
 - for IPSec*, 309–313, 316–321, 326
 - for IPSec with CA support*, 345–349
 - RSA keys, 329
 - SNMP, 194–199
 - SSH parameters (Cisco IOS routers), 67
 - TACACS+, 140
 - accounting*, 143
 - authentication*, 141–143
 - CSACS, 266–269
 - encryption key*, 141
 - troubleshooting*, 144–145
 - username password authentication, 105
 - warning banners, 89–90
 - xauth, 370
- configuring routers for IPSec, 311–313**
- consistency, 13**
- console administration, 84**
- console connection (Cisco IOS routers), 66**
- context-based access control. See CBAC, 258**
- continuity, lack of leading to attacks, 28**
- corporate assets, 10**
- correlation, 50, 53**
- cost savings, 11**
- crackers, 27**
- creating**
- dynamic crypto maps with RRI, 368
 - IKE policies, 319
- CRL (certificate revocation list), 344**
- crl option command, 348**
- crypto ACLs, 323**
- crypto key zeroize rsa command, 332**
- crypto maps, 324**
- configuring, 414–415
 - example, 325
- CSACS**
- configuring for RADIUS, 270
 - configuring TACACS+, 266–269
- CSAuth, 167**
- CSDBSync, 168**
- CSIDS (Cisco Secure Intrusion Detection System), 279**

CSIS (CiscoSecure Integrated Software), 69
 CSLog, 168
 CSRADIUS, 168
 CSTacacs, 168
 Ctrl-Z command, 64

D

data

- fabrication, 35
- interception, 34
- modification, 35
- potential targets, 47
- vulnerabilities, 27

Data Encryption Standard (DES), 312

database authentication, 406

DDoS (distributed denial of service), 33

DDoS attacks, 35–36

dead peer detection (DPD), 363

debug aaa accounting command, 151

debug aaa authentication command, 144

debug command, 63, 130–132

debug crypto ipsec command, 326

debug crypto isakmp command, 326

debug ip audit detailed command, 294

debug ip audit ftp-token command, 294

debug ip audit function-trace command, 294

debug ip audit icmp command, 294

debug ip audit ip command, 294

debug ip audit object-deletion command, 294

debug ip audit rpc command, 294

debug ip audit smtp command, 294

debug ip audit tcp command, 294

debug ip audit tftp command, 294

debug ip audit timers command, 294

debug ip audit udp command, 294

debug radius command, 150

debug tacacs command, 145

debug tacacs events, 145

debugging CBAC, 244

debug ip audit ftp-cmd command, 294

debug ip audit object-creation command, 294

debug ip audit object-deletion command, 294

default settings (network devices), 29

defense, 46

- components used, 47
- correlation and trending, 50
- effective monitoring, 50

- host-based, 49

- identifying targets, 46

- layering, 46

- network segmentation, 49

- physical security, 51

defining Group Policy Configuration mode, 367

deploying Cisco Secure ACS, 178–179

DES (Data Encryption Standard), 312

designing networks, 403–405

devices

- configuration weaknesses, 29

- default settings, 29

Diffie-Hellman key exchange, 312

directed broadcasts, disabling, 196

Director's Post Office protocol, 288

disable command, 63

disabling

- directed broadcasts, 196

- finger services, 198

- unnecessary services, 407

disaster recovery plans, 28

distributed denial of service attacks (DDoS attacks), 33, 35–36

distributing security policies, 16

DNS whois queries, 34

DoS attacks (denial-of-service), 11, 33, 36

- Cisco IOS firewall DoS mitigation, 70

- detection and protection, 235

- ICMP, 30

DPD (dead peer detection), 363

dynamic access lists (Cisco IOS firewalls), 69

dynamic command, 325

dynamic crypto maps

- applying mode configuration, 369

- applying to interfaces, 369

- creating with RRI, 368

dynamic perimeter security, 49, 52

E

Easy VPN, 365

- configuring remote access, 364

- creating ISAKMP policy, 366*

- enabling IKE DPD, 370*

- group policy lookup, 366*

- mode configuration requests, 369*

- transform sets, 368*

- xauth configuration, 370*

- modes of operation, 371
- overview, 362
- server functionality, 363

enable command, 63**enable password command, 84–85****enable secret command, 86****enabling IKE DPD, 370****Encapsulating Security Payload (ESP), 314****encryption**

- configuring IPSec on Cisco routers, 310–311
- enable secret command, 86

end command, 64**endpoints, 307****enrollment mode ra command, 348****enrollment retry-count command, 348****enrollment retry-period command, 348****enrollment url command, 348****enterprise VPN routers**

- managing, 383–384
- Router MC, 386–394
- VMS (VPN/Security Management Solution), 385

ESP (Encapsulating Security Payload), 314**ESP-3DES transform, 316****ESP-DES transform, 316****ESP-MD5-HMAC transform, 316****ESP-SHA-HMAC transform, 316****Ethernet switches, 92–93****ethical hackers, 31****event logging, 70****EXEC mode, 83****exit command, 65****expanded IP ACLs, 209****exposed passwords, 29****extended IP ACLs, 69, 212****extended authentication (xauth), 363****extranet VPNs, 308****F****finger services, disabling, 198****firewalls, 12**

- Cisco IOS, 59, 255
 - AAA server support, 73*
 - access lists, 69*
 - authentication proxy, 70*
 - event logging, 70*
 - features, 72*

*IPSec network security, 70**Java blocking, 69**NAT, 70**neighbor router authentication, 70**PAM, 70**real-time alerts, 70**security server support, 70**system auditing, 69**TCP intercept, 69**user authentication and authorization, 70*

IDS, 279

known hostile entities, 49

overview, 222

potential target, 46

flexibility of security measures, 15**FTP security settings, 29****G–H****global configuration mode (Cisco IOS routers), 64****Group Policy Configuration mode, 367****group policy lookup, 366****Group Setup Configuration Window, 270****guidelines (security policies), 13, 20****hackers, 31****hactivision, 33****hardware**

- default settings, 29
- potential attack targets, 46
- weaknesses, 30

hardware weaknesses, 30**hash (message integrity) algorithm, 312****hashes, 198****horizontal scans, 34****host-based defense, 49****hostile entities, 49****hosts (potential target), 46****host-specific port mapping, 227****HTTP servers, configuring, 261****I****ICMP (DoS attacks), 30****IDSs (intrusion detection systems), 49, 279**

Cisco IOS firewall, 70, 224

adding to centralized management, 292

- audit rules, 290–291*
 - clear commands, 294*
 - debug commands, 294*
 - defining the protected network, 288*
 - deployment strategies, 295*
 - info and attack signatures, 288*
 - maximum queue for alarms, 288*
 - verifying configuration, 292*
 - host-based, 49
 - IETF (Internet Engineering Task Force), 18**
 - IKE (Internet Key Exchange), 309–313**
 - CAs, 343
 - configuring
 - parameters, 411–412*
 - with RSA signatures, 353*
 - dead peer detection (DPD), 363
 - defining policy, 310
 - enabling, 319, 370
 - extended authentication (xauth), 363
 - polices, 319
 - policy parameters, 313
 - verifying configuration, 320
 - implementing**
 - CBAC (case study), 424–425
 - security policies, 14, 17
 - steps of, 17*
 - testing, 18*
 - incident response plans, 16**
 - info signatures (atomic signatures), 288**
 - inspection rules (CBAC), 241**
 - applying to an interface, 244
 - java, 243
 - TCP and UDP inspection, 243
 - installing**
 - Cisco Secure ACS, 180–181
 - CiscoWorks 2000, 384
 - Router MC, 389–390
 - interactive router access, 90**
 - interception, 34**
 - interesting traffic, 323**
 - interface command, 64, 142**
 - interface configuration mode (Cisco IOS routers), 64**
 - Internet Engineering Task Force (IETF), 18**
 - Internet Key Exchange. See IKE**
 - Internet Protocol (IP), 29**
 - Internet services, configuration weaknesses, 29**
 - internetworking, 46**
 - interoperability, 343**
 - intranet VPNs, 308**
 - intruder motivation, 31**
 - intrusion detection systems. See IDS**
 - IOS Cisco firewall, 295**
 - ip audit command, 292**
 - ip audit notify log command, 286**
 - ip audit notify nr-director command, 286**
 - ipauth-proxyauth-cache-timecommand, 262**
 - ipauth-proxyauth-proxy-bannercommand, 262**
 - ip http authentication aaa command, 261**
 - ip http server command, 261**
 - ip inspect command, 241**
 - ip inspect name command, 241**
 - IPSec**
 - configuring, 354
 - encryption on Cisco routers, 310–311*
 - manually, 328*
 - parameters, 413–414*
 - RSA encrypted nonces, 328–330*
 - SA lifetimes, 323*
 - configuring routers for, 309–311, 321
 - enabling IKE, 319*
 - testing configuration, 326*
 - transforms, 316*
 - verifying connectivity, 317*
 - verifying current configuration, 317*
 - verifying IKE configuration, 320*
 - creating transform set, 322
 - crypto maps, 324
 - defining policies, 313
 - overview, 309
 - Router MC, 388
 - IPSec network security, 70**
 - ipsec-isakmp command, 325**
 - ISAKMP, creating policy for remote VPN clients, 366**
 - ISAKMP/Oakley (Internet Security Association and Key Management Protocol [with Oakley distribution]), 310**
- ## J–K–L
- Java applets, 29**
 - Java blocking Cisco IOS firewalls, 69**
 - java inspection rules, 243**
 - Java script, 29**

Kerberos, 109
keys
 preshared, 311, 319
 RSA, 329–330
legal issues (network security), 18
line configuration mode (Cisco IOS routers), 65
line password authentication, 105
login authentication, 122
login authentication admins command, 150

M

MAC address lockdown, 92
management components, 47
managing enterprise VPN routers, 383–384
 Router MC, 386–390, 392–394
 VMS (VPN/Security Management Solution), 385
maximum queue, 288
MD5 (Message Digest 5), 312
message digest, 312
message integrity (hash) algorithm, 312
method lists, 119
Microsoft Challenge Handshake Authentication Protocol
 (MS-CHAP) authentication, 111
mode configuration push, 367
modification of resources, 35
MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) authentication, 111

N

NAT (Network Address Translation), 48, 70, 258
neighbor router authentication, 70
network extension mode (Easy VPN), 371
Network File System, 30
network infrastructure policy, 10
network security, 5, 30
 attacks, 23
DoS, 36
potential targets, 46
reasons for success, 28
types of, 33–34
 balancing needs, 9

defense, 46
components used, 47
host-based, 49
 definition of, 9
 devices, configuration weaknesses, 29
 dynamic perimeter security, 49
 firewalls, 12, 59
 incident response plans, 16
 intruder motivation, 31
 legal issues, 18
 misconfigured Internet services, 29
 passwords, 29
 patches, 27
 physical, 51
 policies, 6, 9, 47
consistency, 13
creating, 11
distributing, 16
feasibility, 11
flexibility, 15
goals of, 12, 19
guidelines, 13, 20
implementing, 14
network infrastructure, 10
patch management, 10
preparation for, 10
topics to address, 10
weaknesses of, 28
writing direction of, 14
 process of, 20, 50
 responding to threats, 11
 sanctions for violations, 16
 security wheel, 6
 technology weaknesses, 30
 threats, 38
categories of, 31
curiosity, 32
fun and pride, 32
lack of understanding, 31
political, 33
revenge, 32
 theft, 32
 Trojan horses, 35
 user accounts, 10
 self-imposed vulnerabilities, 27
 worms, 35

Network Time Protocol (NTP), 199

networks

- design, 403–405
- disaster recovery plans, 28
- equipment weaknesses, 30
- interactive access, 90
- internetworking, 46
- remote access case study, 419–425
- security. *See* network security
- segmentation, 49, 52
- site-to-site connectivity, 409–410
- vulnerabilities, 27

NFS (Network File System), 30

NTP (Network Time Protocol), 199, 416–417

ntp access-group command options, 347

O–P

operating systems, weaknesses, 30

option, 348

PAM (port-to-application mapping), 70, 225–227

PAP (Password Authentication Protocol), 109–110

password protection, 123

passwords

- encryption, 86–87
- exposed, 29
- vtty, 69
- weak, 29

PAT (Port Address Translation), 48

patch management policy, 10

patches, 27–28

peer authentication method, 312

peer command, 347

performance, CBAC's impact on, 239

perimeter security, 49

physical security, 51

ping sweeps, 34

PKCS#10, 344

PKCS#7, 344

policies (network security), 6, 47, 52

- balancing needs of business with security needs, 9
- consistency, 13
- creating, 11
- definition of, 9

disaster recovery plans, 28

distributing, 16

feasibility, 11

flexibility, 15

goals of, 12, 19

guidelines, 13, 20

IKE, 319

implementing, 14, 17

ISAKMP, 366

legal issues, 18

mode configuration push, 367

network infrastructure, 10

patch management, 10

preparation for, 10

sanctions for violations, 16

topics to address, 10

user account, 10

weaknesses of, 28

workstation configuration, 10

writing direction of, 14

political threats, 33

Port Address Translation (PAT), 48

ports (security), 93

port-to-application mapping (PAM), 70, 225–227

Post Office Protocol, configuring, 287

PPP authentication, 109, 124, 142

ppp authentication command, 142

ppp authentication pap checkin command, 150

preparing routers for, 365

preshared keys, 311

configuring, 319

configuring routers for IPSec, 309–310, 321

privilege levels, 83, 88

privileged EXEC mode (Cisco IOS routers), 63, 83

prompt command, 65

protocols

authentication, 109

CBAC supported, 238

IKE, 310

routing, 197

weaknesses, 30

proxies, authentication, 70, 251

appearance, 256

compatibility with other features, 258

- configuring, 258–265
- functionality, 255
- limitations, 272–273
- overview, 255

Q–R

QoS (quality of service), 10

query url command, 348

query-only command, 347

question mark (?) symbol, 65

RADIUS

- authentication proxy, 270
- configuring, 146–147
 - accounting, 148*
 - authentication and authorization, 148*
 - troubleshooting, 150–151*
- features of, 108
- overview, 107
- responses to login attempts, 108

radius-server host command, 146–147

radius-server key command, 146

reconnaissance attacks, 33–34

reflexive access lists (Cisco IOS firewalls), 69

reflexive ACLs, 212

remote access

- case study, 419
 - authentication proxy, 423*
 - Cisco IOS firewall IDS, 420–423*
 - implementing CBAC, 424–425*
- configuring with Easy VPN, 359, 363–366
 - creating ISAKMP policy, 366*
 - enabling IKE DPD, 370*
 - mode configuration requests, 369*
 - transform sets, 368*
 - xauth configuration, 370*
- securing router access (case study), 406

remote access VPNs, 308

remote security servers

- Kerberos, 109
- RADIUS, 107–108
- TACACS, 106
- TACACS+, 108

resources

- fabrication, 35
- modification, 35

Reverse Route Injection (RRI), 368

RFC 2196 Site Security Handbook, 9

right-angle bracket (>) symbol, 63

ROM monitor mode (Cisco IOS routers), 63

Router MC

- basic concepts, 386–387
- installation and login, 389–390
- integration with CiscoWorks common services, 389
- job statuses, 394
- tunneling technologies, 388
- user accounts, 397
- workflows, 392–393

Router# (config) ip routing command, 65

Router# (config)hostname RouterA command, 65

Router# configure terminal command, 65

Router> enable command, 65

RouterA# (config) Ctrl-Z command, 66

RouterA# (config) end command, 66

RouterA# (config) interface Ethernet 0/0 command, 66

RouterA# (config) ip address 10.10.10.254 255.255.255.0 command, 66

RouterA# (config)exit command, 66

RouterA# (config)no shutdown command, 66

routers

- administrative access, 405
- CA support, 343
- Cisco IOS, 59, 63, 71
- communicating with CAs, 351
- configuring
 - ACLs, 214*
 - host/domain names, 330*
 - IKE parameters, 411*
 - IPSec encryption, 310–311*
 - as SSH client, 91*
- configuring for IPSec, 345–349
- disabling unnecessary services (case study), 407
- enterprise VPN, 383–384
- initializing Cisco IOS firewall IDS, 286
- interactive access, 90
- potential target, 46
- preparing for Easy VPN servers, 365
- securing all in network (case study), 404–405
- securing remote access (case study), 406

RRI (Reverse Route Injection), 368

RSA encrypted nonces, 328–330

RSA keys

- configuring, 329
- generating, 330
- managing, 332
- planning VPN implementation, 329
- verifying configuration, 331

RSA signatures, 311

rules (RFC 2196 Site Security Handbook), 9

S

SA lifetime, 313, 323

sanctions, 16

saving CA configuration, 350

script kiddies, 31

Secure Access Control Server. See Cisco

Secure ACS

Secure Hash Algorithm 1 (SHA-1), 312

security

- access control, 235
- accounting, 120
- administration
 - configuring multiple privilege levels, 87–88*
 - console access, 84*
 - enable password, 84–85*
 - enable secret command, 86*
 - service password-encryption command, 87*
 - warning banners, 89–90*
- authentication, 119
 - failed access attempts, 120*
 - line password, 105*
 - method lists, 119*
 - methods, 104*
 - overview, 104*
 - remote security servers, 106–108*
 - username password, 105*
- authentication proxy, 255
- authorization, 120
- IDS, 279
- interactive router access, 90
- network design case study, 403–405
- port security for Ethernet switches, 92–93
- SSH, 91
- vt, 90

security posture assessment. See SPA

security wheel, 6, 17, 50

self-imposed vulnerabilities, 27, 37

serve command, 347

serve-only command, 347

servers (Easy VPN), 363–364

service password-encryption command, 87, 105

session keys (Kerberos), 109

SHA-1 (Secure Hash Algorithm 1), 312

show accounting command, 151

show command, 63

show crypto ca certificates command, 352

show crypto dynamic-map command, 326

show crypto ipsec sa command, 326

show crypto ipsec transform set command, 326

show crypto isakmp policy command, 317

show crypto key mypubkey rsa command, 352

showcryptokeypubkey-chainrsacommand, 353

show crypto map command, 317, 326

show ip audit configuration command, 293

show ip audit interface command, 293

show ip audit statistics command, 293

show running-configuration command, 317

signature based IDS systems, 49

signature disable command, 289

signatures

Cisco IOS firewall IDS, 288

excluding, 290

RSA, 311

Site Security Handbook, 8–9

site-to-site connectivity (case study), 409–410

site-to-site VPNs, 307–308

smurf attacks, 196

SNMP

securing the network, 194

CDP, 199

controlling interactive access, 195

disabling directed broadcasts, 196

NTP, 199

protocol authentication, 197

small server services, 198

version differences, 194

SNMPv2, 194

SNMPv3, 194

software vulnerabilities, 27

SPA (security posture assessment), 17–18

split tunneling, 363

- SSH, 91
- SSH parameters, 67
- SSH server, 67
- standard IP access lists (Cisco IOS firewalls), 69
- structured threats, 31
- switches
 - configuring as SSH client, 91
 - Ethernet, 92–93
 - potential target, 46
- SYN floods, 236
- system auditing (Cisco IOS firewalls), 69
- system prompts, changing, 65
- system-defined mapping, 225

T

- TACACS, 106
- TACACS+, 106
 - authentication proxy, 266–269
 - configuring, 140, 143
 - authentication, 141, 143
 - encryption key, 141
 - troubleshooting, 144–145
 - features of, 108
- tacacs-server host command, 140–142
- TCP inspection, 243
- TCP intercept, 69
- TCP/IP weaknesses, 30
- technical documents, differing from security policy, 14
- technology weaknesses, 30
- telnet, SSH advantages, 91
- telnet connection (Cisco IOS routers), 66
- testing
 - IPSec configuration, 326
 - security implementations, 18
- threats, 38
 - categories, 31
 - curiosity, 32
 - dynamic perimeter security, 49
 - fun and pride, 32
 - intruder motivation, 31
 - lack of understanding, 31
 - political, 33
 - profit and theft, 32
 - responding to, 11
 - revenge, 32

- SNMP, 194
 - CDP, 199
 - controlling interactive access, 195
 - disabling directed broadcasts, 196
 - NTP, 199
 - protocol authentication, 197
 - small server services, 198

- weaknesses
 - security policies, 28
 - technology, 28–30

- thresholds, configuring for CBAC, 240

- time-based ACLs, 213–214

- timeouts configuring for CBAC, 240

- traffic

- interception, 34

- interesting, 323

- signatures, 289

- transforms, IPSec, 316, 322

- transport input ssh command, 67

- transport mode (VPNs), 313

- trending, 50, 53

- TripleDataEncryptionStandard(3DES), 312

- Trojan horses, 35

- troubleshooting

- AAA services, 130–132

- Cisco Secure ACS, 182–183

- RADIUS configuration, 150–151

- SNMP weaknesses, 194

- CDP, 199

- controlling interactive access, 195

- disabling directed broadcasts, 196

- NTP, 199

- protocol authentication, 197

- small server services, 198

- TACACS+ configuration, 144–146

- tunnel mode (VPNs), 313

- tunnels, split tunneling, 363

U–V

- UDP inspection, 243

- UDP sessions, 237

- UNIX, Secure ACSs, 169–170

- unstructured threats, 31

- crypto key generate rsa command, 348

- user accounts, 10, 397

- user EXEC mode (Cisco IOS routers), 63

- user-defined port mapping, 227

username password authentication, 105

verifying

- CA configuration, 351
- CBAC, 244
- Cisco IOS firewall IDS configuration, 292
- IPSec configuration, 326
- RSA key configuration, 331

vertical scans, 34

virtual terminal (vty) connections, 68

VMS (VPN/Security Management Solution), 385

VPN/Security Management Solution (VMS), 385

VPNs (virtual private networks), 47

- Cisco Easy VPN. See Easy VPN
- configuration parameters, 409
- connectivity, 47, 52
- endpoints, 307
- IPSec, 309
- managing enterprise VPN routers, 383–384
- planning implementations with RSA keys, 329
- Router MC, 386–394
- site-to-site, 307–308
- transport mode, 313
- tunnel mode, 313

VPNsVMS (VPN/Security Management Solution), 385

vtys, restricting access, 90

vulnerabilities, 27, 37

W–X

warning banners, 89–90

web administration (Cisco Secure ACSs), 165

whois queries, 34

Windows

- Cisco Secure ACSs, 161, 166
 - AAA, 162
 - accounting, 165
 - authorization, 164
 - CSAuth, 167
 - CSDBSync, 168
 - CSLog, 168
- CiscoWorks 2000, 383

workflow, Router MC, 392–393

workstation configuration policy, 10

worms, 35

X.509v3 certificates, 344

xauth, 363, 370

xauth (extended authentication), 363

XTACACS, 106