

A

-
- AAA (authentication, authorization, and accounting), 83, 120
 - architecture, 84
 - Cisco Secure ACS for Windows, 123
 - configuration, 138
 - troubleshooting, 141–143
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - login, configuring XAUTH, 504
 - methods, 89–90
 - PPP, 93–95
 - remote PC username and password, 90
 - S/Key, 90–91
 - token cards and servers, 91–93
 - perimeter routers
 - aaa accounting command, 104–106
 - aaa authentication command, 98–102
 - aaa authorization command, 102–104
 - aaa new-model command, 97–98
 - configuration, 96
 - securing access, 95–96
 - securing privileged EXEC mode, 96–97
 - RADIUS protocol, 87–89
 - security commands, 147
 - TACACS+ protocol, 87–89
 - configuring, 145–149
 - general features, 144–145
 - verification, 149–152
 - troubleshooting
 - debug aaa accounting command, 110
 - debug aaa authentication command, 106–107
 - debug aaa authorization command, 107–109
 - aaa accounting command, 95, 104–106
 - aaa accounting exec start-stop tacacs+ command, 148
 - aaa accounting network start-stop tacacs+ command, 148
 - aaa authentication command, 98–99, 146
 - AAA method specification for PPP, 100
 - accessing privileged command level, 100–101
 - application to router lines and interfaces, 101–102
 - login authentication, 99
 - aaa authentication enable default command, 100–101
 - aaa authentication local-override command, 148
 - aaa authentication login command, 98, 320, 504
 - aaa authentication login default tacacs+ enable command, 147–148

- aaa authentication ppp command, 100
- aaa authentication ppp default tacacs+ command, 148
- aaa authorization auth-proxy command, 320
- aaa authorization command, 95, 102–104, 108
- aaa authorization exec tacacs+ command, 148
- aaa authorization network command, 506, 511
- aaa authorization network tacacs+ command, 148
- aaa group server radius command, 99–102, 105
- aaa group server tacacs+ command, 99–102, 106
- aaa login authentication command, 99
- aaa new-model command, 96–98, 145–147, 319, 506
- AAA servers
 - configuring
 - ACL allowing traffic, 322
 - Cisco Secure ACS group configuration, 317–318
 - Cisco Secure ACS interface configuration, 316–317
 - creating user authorization profiles, 318–319
 - firewall authentication proxy, 319–320
- acceptable use policy, 33
- accept-dialin configuration mode, 65
- accept-dialout configuration mode, 65
- access
 - AAA
 - architecture, 84
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - methods, 89–95
 - perimeter routers, 95–106
 - RADIUS protocol, 87–89
 - TACACS+ protocol, 87–89
 - troubleshooting, 106–110
 - IP spoofing mitigation, 18
 - router administration
 - auxiliary user-level password, 59–60
 - banner messages, 67–68
 - console port connection, 52–53
 - console port user-level password, 56–57
 - console timeouts, 64
 - enable secret password configuration, 55–56
 - initial configuration dialog, 53–55
 - login failure rate, 63–64
 - MD5 hashing user passwords, 61–62
 - minimum password length, 55
 - password creation, 53
 - password encryption, 60–61
 - privilege levels, 64–67
 - ROMMON mode password recovery, 62–63
 - SNMP systems, 68–83
 - vty user-level password configuration, 57–59
- access access-list parameter, snmp-server user command, 83
- access control lists. *See* ACLs
- Access Control Server (ACS), 53
- access lists

- configuring, 730–731, 750
- IP access lists
 - extended, 737–749
 - named, 750–752
 - standard, 731–737
- access parameter, snmp-server group
 - command, 78
- access servers, RADIUS, 153
 - authentication, 153
 - client, 153
 - configuring, 153–156
 - enhancements, 156–157
 - network security, 153
- access-class command, 58
- access-list command,
 - 193–198, 343–346, 418–422, 474, 733, 738
- access-list compiled command, 204
- access-list icmp command, 741
- access-list parameter, snmp-server group
 - command, 78
- access-list tcp command, 744
- access-list udp command, 746
- accounting. *See also* AAA
 - Cisco Secure ACS for Windows, 125
 - failure, Cisco Secure ACS for Windows, 142
 - routers
 - architecture, 84
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - methods, 89–95
 - perimeter routers, 95–106
 - RADIUS protocol, 87–89
 - TACACS+ protocol, 87–89
 - troubleshooting AAA, 106–110
- Accounting Input Gigawords (RADIUS Attribute 52), 157
- Accounting Output Gigawords (RADIUS Attribute 53), 157
- ACL Default Direction (RADIUS Attribute 11), 156
- ACL Editor, SDM, 537
- ACLs (access control lists), 12, 275
 - applying to router interface, 295
 - rules, 296
 - security policy, 296–297
 - three-interface example, 298–300
 - associating proxy rules, 326
 - Cisco IOS Firewall, 47
 - configuring allowing AAA traffic, 322
 - DDoS attacks, 218
 - Stacheldraht blocking, 218–219
 - Subseven blocking, 219
 - TRIN00 blocking, 218
 - TrinityV3 blocking, 219
 - firewall filtering, 279
 - mitigating router threats, 207
 - theoretical network, 210
 - traffic filtering, 207–209
 - network traffic filtering, 213
 - DoS TCP SYN attack mitigation, 214–215
 - ICMP messages, 216–217
 - smurf attacks, 215–216
 - spoof mitigation, 213–214
 - Router MC firewall settings, 650–651
- routers, 191

- applying to interface, 202–203
 - commenting entries, 201
 - development rules, 201–202
 - directional filter, 202
 - displaying, 203–204
 - enhanced, 205–207
 - identifying, 191–193
 - IP types, 193–201
 - traffic filtering, 211–212
 - Turbo ACLs, 204–205
- ACS (Access Control Server), 53
- active directories (AD), 29
- Activities command
 - Configuration menu, 614
 - Reports menu, 664
- Activities Reports, Router MC, 664
- AD (active directories), 29
- Address Resolution Protocol (ARPs), 174
- addresses, NAT, 39–41
- address-family configuration mode, 65
- Adleman, Leonard, 447
- Admin Accounting Report, Cisco Secure ACS
 - for Windows reports, 140
- administration
 - Cisco Secure ACS for Windows, 123–124, 139–141
 - routers, securing access, 52–83
- Administration Control, Cisco Secure ACS for Windows administration, 140
- Administration tab, Router MC, 610, 665–666
- Advanced Firewall Configuration Wizard, SDM, 561–564
 - configuring DMZ services, 564, 566
 - inspection rules, 566–567
- Advanced Integration Modules (AIMs), 34
- Advanced Mode, SDM, 575
 - Interfaces and Connections icon, 578–579
 - NAT icon, 581–582
 - Overview page, 576–578
 - Routing icon, 580–581
 - Rules icon, 579–580
 - System Properties icon, 582–584
 - VPN icon, 584–585
 - WAN, 560
- Advanced Options window, SDM, 558
- AES encryption algorithm, 372
- aging passwords, 24
- AH (Authentication Header),
 - 380, 409–410, 421
- AIMs (Advanced Integration Modules), 34
- AIM-VPN/BP midsize router, 366
- AIM-VPN/Ep midsize router, 366
- AIM-VPN/HP midsize router, 366
- AIM-VPN/MP midsize router, 367
- alerts
 - CBAC, 282–283
 - Cisco IOS Firewall, 47
 - Cisco VPN Client, 527
- algorithms, IPSec encryption, 372–373
- alias keyword, no tftp-server flash command,
 - 190
- alps-ascu configuration mode, 66
- alps-circuit configuration mode, 66
- anti-DoS features, 21
- antisniffer software, packet sniffer mitigation,
 - 17
- antispoof features, DoS attack mitigation, 21
- antivirus software, 32
- any keyword, 423

- API (application program interface), 125
- AppleTalk Remote Access (ARA), 95
- application program interface (API), 125
- applications
 - attacks, 25–26
 - Cisco SAFE Blueprint, 12
- ARA (AppleTalk Remote Access), 95, 144
- ARPANet, 3
- ARPs (Address Resolution Protocol), 174
- ATM (automated teller machines), 16
- atm-bm-config configuration mode, 65
- atm-bundle-config configuration mode, 65
- atmsig_e164_table_mode configuration mode, 65
- atm-vc-config configuration mode, 65
- atomic signatures, 340
- attacks, 13
 - CBAC
 - ACLs, 279
 - alerts, 282
 - audit trails, 282
 - capabilities, 279–281
 - configuration tasks, 283–301
 - protocols supported, 281–282
 - firewalls, intrusion detection, 278
 - IDS
 - basics, 333–340
 - configuring, 340–351
 - network security threats, 14
 - signatures, 340
 - types, 14–15
 - applications, 25–26
 - DoS, 20–21
 - IP spoofing, 17–19
 - man-in-the-middle, 24–25
 - network reconnaissance, 26–28
 - operator errors, 32
 - packet sniffers, 15–17
 - password attacks, 22–24
 - port redirection, 30
 - privilege escalation, 19–20
 - Trojan horses, 31–32
 - trust exploitation, 28–29
 - unauthorized access, 31
 - viruses, 31–32
 - worms, 31–32
- Audit Trail command (Reports menu), 665
- Audit Trail Reports, Router MC, 664–665
- auditing
 - AAA architecture, 84
 - CBAC, 282–283
 - Cisco IOS Firewall, 47
 - IDS packet auditing, 344–345
 - creating and applying audit rules, 346
 - default actions for info signatures, 345
 - excluding addresses, 346–347
 - SDM, 570
 - One-Step lockdown, 573–574
 - performing, 570–573
- AUS (Auto Update Server), 610
- auth keyword, 80
- auth parameter
 - snmp-server group command, 78
 - snmp-server user command, 83
- authentication. *See also* AAA
 - CAs, 467
 - Cisco IOS Firewall, 47

- Cisco Secure ACS for Windows, 124
- Cisco VPN Client, 519
- failure, 141–142
- IKE pre-shared keys, 403
 - configuring IKE, 412–417
 - configuring IPSec, 418–429
 - IPSec encryption policy, 403–412
 - verification, 429–434
- IPSec
 - digital signatures, 376–380
 - ESP, 382–383
 - header, 381–382
 - IKE peer authentication, 390
- Kerberos, 157–158
- login, failure rate configuration, 63–64
- packet sniffer mitigation, 16
- RADIUS, 153
- routers
 - architecture, 84
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - methods, 89–95
 - perimeter routers, 95–106
 - RADIUS protocol, 87–89
 - TACACS+ protocol, 87–89
 - troubleshooting AAA, 106–110
- security policy, 33
- Authentication Header (AH), 380
- authentication method parameter, IKE policy, 406–408, 457–458
- authentication proxy
 - application, 314
 - associating proxy rules with ACL, 326
 - basics, 309–310
 - configuring, 315–319
 - configuring ACL allowing AAA traffic, 322
 - creating proxy rules, 325–326
 - defining proxy banner, 324–325
 - enabling AAA, 319–320
 - enabling router HTTP server, 322–323
 - firewall, 276–278
 - process, 312–314
 - RADIUS, 310
 - RADIUS IP address specification, 321–322
 - session initiation, 311–312
 - setting AAA authentication, 320
 - setting AAA authorization, 320
 - setting proxy idle timeout value, 323–324
 - TACACS+, 310, 320–321
 - verification and testing, 327
- authority, security policy, 33
- authorization. *See also* AAA
 - failure, Cisco Secure ACS for Windows, 142
 - Router MC, 601–603
- routers
 - architecture, 84
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - methods, 89–95
 - perimeter routers, 95–106
 - RADIUS protocol, 87–89
 - TACACS+ protocol, 87–89
 - troubleshooting AAA, 106–110

auth-password parameter, snmp-server user command, 83

auth-proxy parameter, aaa accounting command, 105

auto secure command, 242–243

Auto Update Server (AUS), 610

Autodetect Wizard, SDM, 536

automated provisioning, Cisco IOS Firewall, 46

automated teller machines (ATMs), 16

AutoSecure, 241–242

- CBAC and ingress configuring, 247–248
- CEF and ingress configuring, 246–247
- change application, 248–258
- example configuration post change application, 260–266
- example configuration prior to change application, 259–260
- global service disabling, 243–244
- initiation, 242–243
- interface services disabling, 246
- Internet connection, 243
- password configuration, 245–246
- security banner creation, 244–245

auto-summary command, 626

auxiliary user-level passwords, 59–60

B

banner command, 67–68

banner exec command, 67

banner incoming command, 67

banner login command, 67

banner messages, router administration, 67–68

banner motd command, 67

banner slip-ppp command, 67

banners, AutoSecure, 244–245

Basic Configuration window, SDM access, 544–545

Basic Firewall, SDM firewall creation, 560

Betrusted UniCERT CA server, 451

BGP (Border Gateway Protocol), 72

bgp keyword, 72, 80

BOOTP server, disabling, 168–169

Border Gateway Protocol (BGP), 72

Break key, startup configuration startup, 56

broadcast parameter, aaa accounting command, 105

brute-force computation, L0phtCrack password computing, 23

building blocks, Router MC, 652–654

Building Blocks command (Configuration menu), 629

C

cable DHCP proxy enhancement, Easy VPN Remote, 492

Calling Line Identification (CLID), 123

calltracker keyword, 72, 80

campus access policy, 33

CAs, 447–448

- (certificate authorities), 447
 - Cisco router interoperability, 450
 - Betrusted UniCERT, 451
 - Entrust/PKI, 450
 - Microsoft Certificate Services, 451–452
 - VeriSign OnSite, 450–451
 - configuring support tasks, 453–454, 459–461
 - authentication, 467
 - declaring commands, 465–467
 - IKE and IPSec preparation, 454–458
 - IKE configuration for IPSec, 472–474
 - IPSec configuration, 474
 - IPSec verification, 474–476
 - monitoring interoperability, 469–471
 - NVRAM memory usage, 461
 - router host and domain name, 462–463
 - router identity certificate, 467–469
 - router time and date, 461–462
 - RSA key pair generation, 463–465
 - saving support configuration, 469
 - verification, 471–472
 - enrolling device, 452–453
 - multiple RSA key pair support, 453
 - SCEP, 449–450
 - server parameters, 456
 - support standards, 448–449
- cas custom configuration mode, 65
- case studies, Future Corporation, 671
 - requirements, 672–675
 - solutions, 675–685
- CBAC, 276 (Context-Based Access Control), 46, 206, 275
 - ACLs, 279
 - alerts, 282
 - audit trails, 282
 - basics, 276–277
 - capabilities, 279–281
 - configuration tasks
 - alerts, 283
 - audit trail, 283
 - debug commands, 301
 - defining inspection rules, 290–295
 - global timeouts and thresholds, 283–287
 - inspection rules, 295–300
 - PAM, 287–290
 - removing configuration, 301
 - show commands, 300–301
 - protocols supported, 281–282
 - SDM, 538
- CCO (Cisco Connection Online), 90
- CDP services, disabling, 169–170
- CEF, AutoSecure enabling, 246–248
- CEP (Certificate Enrollment Protocol), 449
- certificate authorities. *See* CAs
- Certificate Enrollment Protocol (CEP), 449
- CET (Cisco Encryption Technology), 425
- Challenge Handshake Authentication Protocol. *See* CHAP
- challenge-response token cards, 92
- CHAP (Challenge Handshake Authentication Protocol), 62, 121
 - Cisco Secure ACS for Windows, 121
 - MD5 encryption, 62

- PPP authentication, 94
- security levels, 121
- Cisco
 - IDS 4200 Series sensors, 333
 - IOS Command Reference, 74
 - IOS Security Configuration Guide, 487
 - management software
 - PIX Device Manager, 35
 - VMS management applications, 35–37
 - VPN Solution Center, 35
 - PIX Firewall, 34, 276
 - RADIUS version, 154
 - Secure ACS Solution Engine, 85
 - Security Agent, 36
 - security products, 34
 - VPN 3000 Series Concentrators, 34
- Cisco Easy VPN Remote. *See* Easy VPN Remote
- Cisco Easy VPN Server. *See* Easy VPN Server
- Cisco Encryption Technology (CET), 425
- Cisco IDS Device Manager (IDM), 334
- Cisco IDS Event Viewer (IEV), 334
- Cisco Intrusion Detection System. *See* IDS
- Cisco IOS Firewall, 34, 45. *See also* firewalls
 - benefits, 46
 - features, 46–48
 - support, Easy VPN Remote, 492
- Cisco Router Web Setup (CRWS), 496
- Cisco SAFE Blueprint, 9–13
- Cisco Secure ACS, 85
 - creating user authorization profiles, 318–319
 - group configuration, 317–318
 - interface configuration, 316–317
- Cisco Secure ACS 3.0 for Windows 2000/NT Servers. *See* Cisco Secure ACS for Windows
- Cisco Secure ACS for UNIX, 134–136
- Cisco Secure ACS for Windows, 120–121
 - AAA services, 123
 - ACS user database access, 129–130
 - administration, 123–124, 139–141
 - database management, 126–127
 - distributed system, 124–125
 - external database support, 125–126
 - general features, 121–122
 - installation, 136
 - configuring server, 136–137
 - device configuration for AAA, 138
 - installing on server, 137
 - network device connection verification, 137
 - operation verification, 138–139
 - web browser configuration, 137–138
 - product enhancements, 132–134
 - service modules, 127–129
 - token card support, 131–132
 - troubleshooting, 139–141
 - accounting failure, 142
 - authentication failure, 141–142
 - authorization failure, 142
 - debug commands, 143
 - dial-in client problems, 143
 - version 3.1 product enhancements, 132–133
 - version 3.2 product enhancements, 133–134
- Windows user database access, 130–131

Cisco Security Device Manager. *See* SDM, 535

Cisco Threat Response (CTR), 334

Cisco VPN Client

- authentication, 519

- connection properties, 520–521

- Easy VPN Remote, 487–488

 - hardware client 3.x or later, 488, 490

 - PIX Firewall 501, 490

 - router clients, 491–492

 - software version later than 3.x, 488

- General tab, 524–525

- installation, 515

- log viewer, 522

- MTU size, 523–524

- multiple connection entries, 516

- new release changes, 526

 - alerts, 527

 - firewall enhancements, 528

 - GINA enhancements, 529

 - GUI environment, 527

 - log files, 528

 - RADIUS SDI XAUTH, 528

 - single VPN tunnel, 527

 - third-party compatibility, 528

 - virtual adapter, 526

- option modification, 516–517

- program menu, 521–522

- properties, 518–519

- Statistics tab, 525–526

Cisco VPN Client Release 3.5, 497

- features and benefits, 497–498

- specifications, 498–499

CiscoWorks

- adding users, Router MC, 604

- Auto Update Server Software, 36

- CD One, 36

- CiscoView, 36

- Common Services Software, 36

- login, Router MC, 601

- Management Center

 - IDS sensors, 36, 351

 - PIX Firewalls, 37

 - security, 37

 - VPN routers, 37

- Monitoring Center for Security (Security Monitor), 333, 349–351

- RME, 36

- Server desktop, 36

- user authorization, Router MC, 601–603

- VPN Monitor, 35

- clear commands, IDS configuration

 - verification, 349

- clear crypto sa command, 419

- clear ip audit configuration command, 349

- clear ip audit statistics command, 349

- clear ip auth-proxy cache command, 327

- CLID (Calling Line Identification), 123

- Client mode, Easy VPN Remote Phase II, 494

- clients

 - Easy VPN Remote, 487–488

 - hardware client 3.x or later, 488, 490

 - PIX Firewall 501, 490

 - router clients, 491–492

 - software version later than 3.x, 488

 - RADIUS, 153

 - VPN Client

- authentication, 519
- connection properties, 520–521
- General tab, 524–525
- installation, 515
- log viewer, 522
- MTU size, 523–524
- multiple connection entries, 516
- new release changes, 526–529
- option modification, 516–517
- program menu, 521–522
- properties, 518–519
- Statistics tab, 525–526
- clock set command, 459–462
- clock timezone command, 459–461
- closed networks, 5
- command syntax, ICMP, 741
- commands
 - access-list, 733, 738
 - access-list icmp, 741
 - access-list tcp, 744
 - access-list udp, 746
 - Configuration menu
 - Activities, 614
 - Building Blocks, 629
 - IKE, 632–635
 - Settings, 624
 - Translation Rules, 655
 - Tunnels, 637
 - Upload, 657
 - Deployment menu
 - Jobs, 644
 - View Configs, 646
 - Devices menu
 - Device Hierarchy, 616
 - Device Import, 618
 - extended IP access lists, 738–741
 - General menu, Failover and Routing, 627
 - Hub menu
 - Inside Interfaces, 627
 - Networks, 629
 - ip access-group, 731
 - log, 734
 - Reports menu
 - Activities, 664
 - Audit Trail, 665
 - Server Configuration menu, Setup, 604
 - Spoke menu, 629–630
 - standard IP access lists, 733–735
 - VPN/Security Management Solution
 - menu, Management Center, 604
 - commands level parameter, aaa accounting
 - command, 105
 - commands parameter, aaa authorization
 - command, 102
 - communications
 - Router MC, 596–597
 - SDM, 541–542
 - security importance, 7
 - community strings, 79
 - community-string parameter, snmp-server host
 - command, 72, 80
 - compound signatures, 340
 - Computer Oracle and Password System (COPS), 6
 - Computer Security Institute (CSI), 13
 - config keyword, 72, 80
 - config-isakmp command, 473
 - config-rtr-http configuration mode, 66
 - configuration
 - access lists, 730–731, 750

- general access lists, 730
- IP access lists, 723–753
 - extended, 737–749
 - standard, 731–737
- configuration autoloading service, disabling, 170–171
- configuration change traps, SNMP router systems, 70
- configuration dialog, router administration, 53–55
- Configuration menu commands
 - Activities, 614
 - Building Blocks, 629
 - IKE, 632–635
 - Settings, 624
 - Translation Rules, 655
 - Tunnels, 637
 - Upload, 657
- configuration parameter, aaa authorization command, 102
- Configuration tab, Router MC, 608–609, 614–615
- configure configuration mode, 65
- Configure LMI and DLCI window, SDM, 558
- connect EXEC command, 158
- Connection Information (RADIUS Attribute 77), 157
- connection parameter, aaa accounting command, 105
- consoles
 - port connection administration, 52–53
 - session timeouts, 64
 - syslog logging, 222
 - user-level password, 56–57
- context concept, SNMPv3, 75
- Context-Based Access Control. *See* CBAC
- controller configuration mode, 65
- COPS (Computer Oracle and Password System), 6
- copy rcp EXEC command, 158
- copy running-config startup-config command, 460, 469
- corporations, network security, importance, 7
- CPE (customer premises equipment), 484
- crl command, 466
- crl optional command, 469
- CRWS (Cisco Router Web Setup), 496
- crypto ACLs
 - extended IP ACLs, 422–423
 - mirror image, 423–424
 - purpose, 422
- crypto ca authenticate name command, 460
- crypto ca certificate chain command, 470
- crypto ca certificate query command, 461
- crypto ca crl request command, 469
- crypto ca crl request name command, 460
- crypto ca enroll command, 467–470
- crypto ca enroll name command, 460
- crypto ca identity command, 465–467
- crypto ca trustpoint command, 323, 460, 469
- crypto dynamic-map command, 509–510
- crypto ipsec client ezvpn xauth command, 494
- crypto ipsec df-bit command, 385
- crypto ipsec profile command, 395
- crypto ipsec profile name command, 398, 400
- crypto ipsec security-association lifetime command, 418, 421, 474
- crypto ipsec transform-set command, 418, 474

-
- crypto isakmp client configuration group command, 507
 - crypto isakmp configuration group command, 508
 - crypto isakmp enable command, 413, 473
 - crypto isakmp identity command, 416, 473
 - crypto isakmp identity hostname command, 500
 - crypto isakmp keepalive command, 512–513
 - crypto isakmp key command, 413–416
 - crypto isakmp nat-keepalive command, 440
 - crypto isakmp policy command, 413–414, 473
 - crypto isakmp xauth timeout command, 494, 504
 - crypto key generate rsa command, 235, 460–463
 - crypto key pubkey-chain rsa command, 471
 - crypto key zeroize rsa command, 460, 470
 - crypto map client authentication list command, 505
 - crypto map command, 418, 424–428, 474, 505, 512
 - crypto map ipsec-isakmp dynamic command, 512
 - crypto map isakmp authorization list command, 511–512
 - crypto map map-name client configuration command, 511
 - crypto maps
 - command example, 427–428
 - configuring, 425–426
 - interface application, 428
 - parameters, 425
 - purpose, 424–425
 - CRYPTOCARD token servers, Cisco Secure ACS for Windows, 132
 - cryptography, packet sniffer mitigation, 17
 - crypto-map configuration mode, 66
 - crypto-transform configuration mode, 66
 - CSAdmin, Cisco Secure ACS for Windows, 128
 - CSAuth, Cisco Secure ACS for Windows, 128
 - CSDBSync
 - Cisco Secure ACS for Windows, 128
 - RDBMS Synchronization, 127
 - CSI (Computer Security Institute), 13
 - CSLog, Cisco Secure ACS for Windows, 128
 - CSMon, Cisco Secure ACS for Windows, 129
 - CSRADIUS, Cisco Secure ACS for Windows, 128
 - CSTacacs, Cisco Secure ACS for Windows, 128
 - CTR (Cisco Threat Response), 334
 - customer premises equipment (CPE), 484
 - customer privacy, network security importance, 7
- ## D
-
- data, IPSec integrity, 373–376
 - Data Encryption Standard (DES), 157
 - Database Replication, Cisco Secure ACS for Windows, 126–127
 - databases
 - Cisco Secure ACS for Windows, 126

- Database Replication, 126–127
- ODBC-compliance, 127
- RDBMS Synchronization, 127
- external, Cisco Secure ACS for Windows, 125–126
- date, CAs support task configuration, 461–462
- DDoS attacks, 20
 - Stacheldraht blocking, 218–219
 - Subseven blocking, 219
 - TRIN00 blocking, 218
 - TrinityV3 blocking, 219
- debug aaa accounting command, 110
- debug aaa authentication command, 106–107, 143, 149
- debug aaa authorization command, 107–109, 143
- debug commands
 - authentication proxy verification and testing, 327
 - CBAC verification and testing, 301
 - troubleshooting AAA, 106–110
 - troubleshooting Cisco Secure ACS for Windows, 143
- debug crypto command, 432–434
- debug crypto ipsec command, 475
- debug crypto isakmp command, 475
- debug crypto key-exchange command, 475–476
- debug crypto pki command, 475–476
- debug ip auth-proxy command, 327
- debug ip inspect command, 301
- debug radius command, 110, 143, 157
- debug tacacs command, 143, 149
 - successful login, 151
 - unsuccessful login, 150–151
- debug tacacs command, 110
- debug tacacs events command, 149–152
- default inside interface, Easy VPN Remote, 492
- default parameter
 - aaa accounting command, 105
 - aaa authentication login command, 99
 - aaa authentication ppp command, 100
 - aaa authorization command, 102
- demilitarized zone (DMZ), 30
- denial of service. *See* DoS
- deny command, 196
- Department of Health and Human Services (DHHS), 9
- deployment, Cisco IOS Firewall, 46
- Deployment menu commands, 644–646
- Deployment Reports, Router MC, 663–664
- Deployment tab, Router MC, 609
- DES (Data Encryption Standard), 157, 372, 386
- des keyword, ISAKMP configuration command, 414
- design, SAFE, 227
 - architecture, 227–229
 - information flow, 229–232
 - logging, 233–234
 - OOB management guidelines, 232–233
 - SNMP secure access, 235–241
 - SSH server configuration, 234–235
- Destination URL Policy Management, Cisco IOS Firewall, 47
- Device Hierarchy command (Devices menu), 616
- Device Import command (Devices menu), 618

- device keyword, no tftp-server flash command, 190
- Devices menu commands, 616–618
- Devices tab, Router MC, 607–608
- DF Bit, Override Functionality, 385
- DH algorithm, 386
- DH key exchange, IPSec operation, 389
- DH public key exchange, IPSec, 370–371
- DHCP SDM, 538, 546–547
- dhcp configuration mode, 65
- DHHS (Department of Health and Human Services), 9
- dial-in client, troubleshooting Cisco Secure ACS for Windows, 143
- dictionary cracking, L0phtCrack password computing, 22
- digital signatures, peer authentication, 376–380
- director keyword, 80
- Disabled Accounts, Cisco Secure ACS for Windows reports, 140
- distributed denial of service (DoS), 20, 218
- distributed systems, Cisco Secure ACS for Windows, 124–125
- DMVPN (Dynamic Multipoint VPN), 393–395
 - hub router configuration, 396–398
 - IPSec profile configuration, 395–396
 - spoke router configuration, 398–401
 - verification, 401–403
- DMZ (demilitarized zone), 30
 - services, SDM firewall creation, 564–566
- DNS (Domain Name System), 26
 - network reconnaissance attacks, 26
 - SDM configuration, 547
 - server, restricting services, 171
 - sessions, CBAC idle time, 284
- dns command, 508
- domain command, 508
- Domain Name System. *See* DNS
- domains
 - names, CAs support task configuration, 462–463
 - trust exploitation, 29
- DoS (denial of service), 20
 - attacks, CBAC, 277–280
 - Cisco IOS Firewall, 47
 - DDoS attacks, 20, 218
 - mitigation, 21
 - TCP SYN attack mitigation
 - blocking external packets, 214–215
 - TCP intercept, 215
- DSL SDM, 538
- dspfarm configuration mode, 65
- dspu keyword, 72, 80
- dynamic crypto map, 509
 - creating, 509–510
 - Easy VPN Server, application to outside interface, 512
 - MC, 511
 - change application, 512
 - IKE querying for group policy, 511–512
 - router configuration, 511
 - RRI enabling, 510–511
 - transform set, 510
- dynamic crypto policies, 642
- Dynamic Multipoint VPN. *See* DMVPN
- dynamic NAT, 40
- dynamic port mapping, Cisco IOS Firewall, 47

E

EAP (Extensible Authentication Protocol),
25, 133

Easy VPN (EZVPN), 37, 483

Remote, 484

Client Release 3.5, 497–499

connection functionality, 499–503

Phase II, 493–496

supported clients, 487–492

Router, RADIUS authentication, 513–514

Server, 483–484, 487

IPSec support, 486–487

new features, 485–486

XAUTH support, 503–513

Easy VPN Remote, 484

Client Release 3.5, 497

features and benefits, 497–498

specifications, 498–499

connection functionality, 499–500

IKE Phase 1 process, 500

IKE Quick Mode, 503

IKE SA establishment, 501

MC process initiation, 502

RRI process initiation, 502–503

SA proposal acceptance, 501

username/password challenge,
501–502

Phase II

operation modes, 493–494

restrictions, 495–496

supported server, 496

supported clients, 487–488

hardware client 3.x or later, 488, 490

PIX Firewall 501, 490

router clients, 491–492

software version later than 3.x, 488

Easy VPN Router, RADIUS authentication,
513–514

Easy VPN Server, 483–484

IPSec support, 486–487

new features, 485–486

unsupported IPSec, 487

XAUTH support, 503–504

configuration, 504–505

dynamic crypto map applied to
outside interface, 512

dynamic crypto map creation,
509–511

group policy for MC push, 506–509

group policy lookup, 506

IKE DPD enabling, 512–513

ISAKMP policy, 506

local IP address pool, 505

MC application to dynamic crypto
map, 511–512

transform sets, 509

e-business, network security, 8

Egevang, Kjeld, 40

EIGRP, SDM, 538

electrical supply, mitigating secure router
installation, 51

enable keyword, method parameter, 99–100

enable password command, 54, 58, 96

enable secret command, 54–55, 96

- enable secret password command, 54–58
- Encapsulating Security Payload. *See* ESP
- encrypt kerberos keyword, 158
- encrypted parameter, snmp-server user
 - command, 83
- encryption
 - IPSec, 369, 403–404
 - ACLs compatibility, 411–412
 - algorithms, 372–373
 - current configuration check, 404–405
 - determining policy, 408–411
 - DH public key exchange, 370–371
 - IKE policy details, 405–408
 - network functionality, 411
 - types, 369–370
 - passwords
 - MD5 hashing, 61–62
 - routers, 60–61
 - TCP packets, TACACS+ feature, 144
- encryption algorithm parameter, IKE policy, 406–408, 457–458
- engine concept, SNMPv3, 74
- engine ID, SNMPv3, 75–76
- engineid-string parameter, snmp-server engine
 - ID command, 76
- enhanced ACLs, 205–207
- enrollment command, 465–466
- entity keyword, 72, 81
- Entrust/PKI CA server, 450
- environments, mitigating secure router
 - installation, 50–51
- envmon keyword, 72, 81
- errors
 - messages, ISAKMP, 434
 - standard IP access lists, 736
- ESP (Encapsulating Security Payload), 380–383
 - authentication transform, 410, 421
 - encryption transform, 410, 421
 - transforms, 409
- established keyword, 197
- everything view, 76
- exec command, 95
- exec configuration mode, 65
- EXEC mode, securing routers, 96–97
- exec parameter
 - aaa accounting command, 105
 - aaa authorization command, 102
- exec-timeout command, 64
- exit keyword, ISAKMP configuration
 - command, 414
- Extended Authentication (XAUTH), *See* XAUTH
- extended IP access lists
 - commands, 738–741
 - configuring, 723–753
 - location, 747–748
 - processing, 738–739
- extended named ACLs, 199–201
- extended numbered ACLs, 197–199
- Extensible Authentication Protocol (EAP), 25, 133
- external databases, Cisco Secure ACS for
 - Windows, 125–126
- external threats, 14
- External User Databases, Cisco Secure ACS
 - for Windows administration, 140
- EZVPN (Easy VPN), *See* Easy VPN

F

- Failed Attempts Report, Cisco Secure ACS for Windows reports, 140
- Failover and Routing command (General menu), 627
- File Transmission Protocol (FTP), 4
- filename keyword, no tftp-server flash command, 190
- filters
 - ACLs, 202
 - DDoS attacks, 218
 - Stacheldraht blocking, 218–219
 - Subseven blocking, 219
 - TRIN00 blocking, 218
 - TrinityV3 blocking, 219
 - traffic, ACLs, 207–217
- finger services, disabling, 173–174
- Firewall Status, SDM Monitor Mode, 586
- firewalls, 45, 275–276
 - authentication proxy, 277–278
 - AAA server configuration, 316–319
 - application, 314
 - associating proxy rules with ACL, 326
 - basics, 309–310
 - configuring, 315–316
 - configuring ACL allowing AAA traffic, 322
 - creating proxy rules, 325–326
 - defining proxy banner, 324–325
 - enabling AAA, 319–320
 - enabling router HTTP server, 322–323
 - process, 312–314
 - RADIUS, 310
 - RADIUS IP address specification, 321–322
 - session initiation, 311–312
 - setting AAA authentication, 320
 - setting AAA authorization, 320
 - setting proxy idle timeout value, 323–324
 - TACACS+, 310
 - TACACS+ server IP address specification, 320–321
 - verification and testing, 327
 - benefits, 46
 - CBAC, 276–277
 - ACLs, 279
 - alerts, 282
 - audit trails, 282
 - capabilities, 279–281
 - configuration tasks, 283–301
 - protocols supported, 281–282
 - Cisco IOS features, 46–48
 - Cisco IOS Firewall, 34
 - Cisco PIX Firewall, 34
 - Cisco VPN Client enhancement, 528
 - feature set, 276
 - internal router, 167
 - intrusion detection, 278
 - perimeter router, 166–167

- Router MC, 591–592
 - access rules, 651–652
 - Activities Reports, 664
 - adding users, 604
 - Administration tab, 610, 665–666
 - approving activities, 643
 - Audit Trail Reports, 664–665
 - building blocks, 652–654
 - CiscoWorks login, 601
 - communications, 596–597
 - components, 595
 - configuration file management, 656–663
 - Configuration tab, 608–609
 - configuring, 648–651
 - creating activity, 611–615
 - creating and deploying jobs, 644–647
 - defining VPN policies, 631–642
 - defining VPN settings, 623–631
 - Deployment Reports, 663–664
 - Deployment tab, 609
 - device group creation, 615–617
 - Devices tab, 607–608
 - importing devices, 617–622
 - installing, 597–600
 - key concepts, 592–594
 - launching, 604
 - main window, 605–606
 - NAT rules, 654–656
 - Reports tab, 609–610
 - supported devices, 595–596
 - tunnel technologies, 597
 - user authorization roles, 601–603
 - user interface, 606–607
 - workflow tasks, 610–611
- SDM, 560–561
 - advanced firewall creation, 563–567
 - creating, 561–563
- Flash images, 62
- flash keyword, no tftp-server flash command, 189
- flash memory, SDM, displaying, 540
- flow-cache configuration mode, 65
- FQDN (fully qualified domain name), 464
- fragmentation
 - inspections, 294
 - Router MC firewall settings, 648
- frame-relay keyword, 72, 81
- Francis, Paul, 40
- FTP (File Transmission Protocol), 4, 172
- fully qualified domain name (FQDN), 464
- Future Corporation case study, 671
 - requirements, 672–675
 - solutions, 675
 - configuration steps, 676–682
 - router configuration, 675–676, 683–685

G

- gateway configuration mode, 66
- general access lists, configuring, 730
- General menu commands, Failover and Routing, 627
- General tab, Cisco VPN Client, 524–525

- general-purpose keys, RSA keys, 464
- generic routing encapsulation (GRE), 503
- GISRA (Government Information Security Reform Act), 9
- GLBA (Gramm-Leach Bliley Act), 9
- government
 - data security importance, 7
 - security regulation policies, 8–9
- Government Information Security Reform Act (GISRA), 9
- Gramm-Leach Bliley Act (GLBA), 9
- GRE (generic routing encapsulation), 503, 625–626
- group concept, SNMPv3, 74
- group keyword, method parameter, 99–102, 106
- group radius keyword, method parameter, 99, 101, 105
- Group Setup, Cisco Secure ACS for Windows administration, 139
- group tacacs+ keyword, method parameter, 99, 101, 106
- group-based policies, Easy VPN Server, 486
- group-name parameter
 - snmp-server group command, 77
 - snmp-server user command, 82
- GUI, Cisco VPN Client new release, 527

H

- half-opened connections, TCP sessions, 284–287
- hardware
 - antisniffer software, 17
 - mitigating secure installation, 49–50
- Hardware Client, 488–490
- hash algorithm parameter, IKE policy, 406–408, 457–458
- Health Insurance Portability and Accountability Act (HIPAA), 9
- HIDS (host-based IDS), 12
- high-risk devices, secure installation, 48
- HIPAA (Health Insurance Portability and Accountability Act), 9
- HMAC, IPsec data integrity, 374–376
- HMAC-MD5 algorithm, 375
- HMAC-SHA-1 algorithm, 375
- host-addr parameter, snmp-server host command, 71
- host-address parameter, snmp-server host command, 80
- host-based IDS (HIDS), 12
- hostname command, 460–462
- hosts
 - CAs support task configuration, 462–463
 - Cisco SAFE Blueprint, 11
 - SDM configuration, 544–545
 - SNMPv3, 78–82
- hosts to be encrypted policy, IPsec encryption, 411

hsrp keyword, 72, 81

HTTP

administrative access, 52

disabling services, 174–176

HTTP Secure (HTTPS), 47

HTTP server, enabling router, 322–323

Hub Assignment command (Spoke menu), 630

Hub menu commands, 627–629

HUBs, inside interface, 627–629

ICMP (Internet Control Message Protocol), 20, 46

Cisco IOS Firewall, 46

command syntax, 741

mask requests, 178

messages

filtering, 216–217

names, 742–744

redirect messages, 179

unreachable messages, 180

identification policy, 33

IDM (Cisco IDS Device Manager), 334

IDS (Intrusion Detection System), 12, 333

application attack mitigation, 26

basics, 333–335

implementation issues, 339

network visibility, 335–336

response options, 340

signature implementation, 339–340

supported Cisco routers, 336–338

Cisco IDS device, 34

common used signatures, 352–357

configuring, 340–341

CiscoWorks Management Center for
IDS Sensors, 351

clear commands, 349

global signature disabling, 343

initializing IDS router, 341–342

packet auditing, 344–347

Security Monitor, 349–351

show commands, 347–349

signature exclusion by host or
network, 343–344

spam attack protection, 342–343

reconnaissance attack mitigation, 28

sensors, CiscoWorks Management Center,
36

IETF (Internet Engineering Task Force)

website, 449

RADIUS version, 154

IEV (Cisco IDS Event Viewer), 334

if-authenticated keyword, method parameter,
103

if-needed keyword, method parameter, 100

IKD DPD, Easy VPN Server enabling,
512–513

IKE (Internet Key Exchange), 35, 448, 485

CAs support task configuration, 454–455

IKE policy determination, 456–458

planning, 455–456

configuring for IPSec, 472–474

keepalive, Router MC, 624

- NAT, 438–439
- Phase 1 operation, 388
 - DH key exchange, 389
 - peer authentication, 390
 - transform sets, 388–389
- Phase 1 process, Easy VPN Remote, 500
- Phase 2 operation, 390
 - SA, 391–392
 - SA lifetime, 392
 - transform sets, 390–391
- policy, 632–634
 - CA enrollment, 636–637
 - dynamic pre-shared keys, 635–636
 - pre-shared keys, 634–635
- pre-shared keys, 403
 - configuring IKE, 412–417
 - configuring IPSec, 418–429
 - IPSec encryption policy, 403–412
 - verification, 429–434
- Quick Mode, Easy VPN Remote, 503
- SA, Easy VPN Remote, 501
- XAUTH, 505
- IKE command (Configuration menu), 632–635
- IKE DPD (Internet Key Exchange Dead Peer Detection), 485
- IKE SA lifetime parameter, IKE policy, 406–408, 457–458
- inactivity-timer option, 324
- incidents handling, security policy, 33
- information signatures, 340
- informs parameter, snmp-server host command, 71, 80
- ingress filters, AutoSecure enabling, 246–248
- initial configuration dialog, router, 53–55
- initial contact, Easy VPN Server, 486
- inside interface, Easy VPN Remote, 491
- Inside Interfaces command
 - Hub menu, 627
 - Spoke menu, 629
- inspection rules, CBAC
 - applying to router interfaces, 295–300
 - configuration, 290–291
 - IP packets, 294–295
 - Java applet, 291–292
 - RPC, 292–293
 - SMTP applications, 293–294
- Integrated Service Adapter (ISA), 367
- Integrated Service Module (ISM), 367
- interface command, 418, 474
- Interface Configuration, Cisco Secure ACS for Windows administration, 140
- interface configuration mode, 65
- Interface Status, SDM Monitor Mode, 586
- interface-dlci configuration mode, 65
- interfaces
 - applying CBAC inspection rules, 295
 - rules for application, 296
 - security policy, 296–297
 - three-interface example, 298–300
 - Cisco IOS Firewall, 47
 - routers, disabling unused interfaces, 190–191
 - traps, SNMP router systems, 70
 - tunnel command, 396–398
- Interfaces and Connections icon, SDM Advanced Mode, 578–579

- internal routers, securing network, 167
- internal threats, 14
- Internet
 - access policy, 33
 - NAT, 39–41
- Internet Control Message Protocol. *See* ICMP
- Internet Engineering Task Force (IETF)
 - website, 449
- Internet Key Exchange. *See* IKE
- Internet Key Exchange Dead Peer Detection, 485
- Internet Protocol (IP), 3
- Internet Protocol Security. *See* IPSec
- Internet Security Association and Key Management Protocol (ISAKMP), 448
- Internet service provider (ISP), 18
- interoperability, CAs, 449
 - Cisco routers, 450–452
 - monitoring, 469–471
- intrusion detection. *See also* IDS
 - Cisco IOS Firewall, 46
 - firewall, 276–278
- Intrusion Detection System. *See* IDS
- IOS Firewall, 34
- IP (Internet Protocol), 3
 - access lists
 - configuring, 723–753
 - extended, configuring, 737–749
 - standard, configuring, 731–737
 - wildcard masks, 729–730
 - ACLs, 193
 - extended named format, 199–201
 - extended numbered format, 197–199
 - standard named format, 195–197
 - standard numbered format, 193–195
 - addresses, 724–725
 - Cisco IOS Firewall, 47
 - NAT, 39–41
 - network classes, 725–726
 - subnet addresses, 726–729
 - WAN configuration, 557
 - compression transform, 410, 421
 - directed broadcasts, disabling, 176–177
 - identification support, 177–178
 - network ACLs filter, 213
 - DoS TCP SYN attack mitigation, 214–215
 - ICMP messages, 216–217
 - smurf attacks, 215–216
 - spoof mitigation, 213–214
 - router ACLs filter
 - routing table information, 212
 - SNMP service, 211
 - Telnet service, 211
 - source routing, 180
 - URL Filtering, Cisco IOS Firewall, 47
- ip access-group command, 203, 731
- ip access-list command, 203
- ip access-list extended command, 199
- ip access-list standard command, 195
- ip address command, 396–398, 496
- ip audit attack command, 345
- ip audit info command, 345
- ip audit name command, 346–347
- ip audit notify command, 341
- ip audit po max-events command, 342
- ip audit po protected command, 341–342
- ip audit signature command, 343–344

- ip audit smtp spam command, 342–343
- ip auth-proxy command, 326
- ip auth-proxy auth-proxy-banner command, 324
- ip auth-proxy inactivity-timer command, 323–324
- ip auth-proxy name command, 325–326
- IP classless services disabling, 176
- ip domain-name command, 234, 460, 462
- ip finger command, 173
- ip host command, 463
- ip http access-class command, 175
- ip http authentication aaa command, 322
- ip http authentication command, 175
- ip http cable-monitor command, 495
- ip http secure-server command, 323
- ip http secure-trustpoint command, 323
- ip http server command, 322
- ip inspect command, 295
- ip inspect alert-off command, 291–294
- ip inspect audit-trail command, 283, 291–294
- ip inspect dns-timeout command, 284
- ip inspect max-incomplete high command, 285
- ip inspect max-incomplete low command, 285
- ip inspect name command, 291
 - IP packets, 294–295
 - Java applets, 292
 - RPC applications, 293
 - SMTP applications, 293–294
- ip inspect name inspection-name http command, 292
- ip inspect one-minute high command, 285
- ip inspect one-minute low command, 285
- ip inspect tcp finwait-time command, 284
- ip inspect tcp idle-time command, 284
- ip inspect tcp max-incomplete host command, 287
- ip inspect tcp synwait-time command, 283
- ip inspect udp idle-time command, 284
- ip local pool command, 505
- ip mtu command, 399
- ip name-server command, 171
- ip nat inside command, 493
- ip nat outside command, 493
- ip nhrp authentication command, 397–399
- ip nhrp map command, 399–402
- ip nhrp map multicast command, 399
- ip nhrp map multicast dynamic command, 397
- ip nhrp network-id command, 397–400
- ip nhrp nhs command, 399
- IP packets, CBAC inspection rules, 294–295
- ip port-map command, 289
- IP spoofing, 17–19
- ip ssh authentication-retries command, 235
- ip ssh time-out command, 235
- ip-address parameter, snmp-server engine ID command, 76
- ipenacl configuration mode, 66
- ipmobile keyword, 72, 81
- IPSec (Internet Protocol Security), 9, 368
 - antireplay sequence number check, 380
 - CAs support task configuration, 454–455, 474
 - IKE policy determination, 456–458
 - planning, 455–456
 - verification, 474–476
 - Cisco IOS Firewall, 47
 - data integrity, 373–376

- DF Bit Override Functionality, 385
- digital signatures, 376–380
- DMVPN, 393–403
- Easy VPN Server
 - supported attributes, 486–487
 - unsupported attributes, 487
- encryption, 369
 - algorithms, 372–373
 - DH public key exchange, 370–371
 - types, 369–370
- framework, 386–387
- IKE configuration, 472–474
- IKE pre-shared keys, 403
 - configuring IKE, 412–417
 - configuring IPsec, 418–429
 - encryption policy, 403–412
 - verification, 429–434
- manual configuration, 434–436
- modes of use, 383
 - transport, 384–385
 - tunnel, 383–384
- NAT, 438
 - IKE negotiation, 438–439
 - keepalives, 440
 - transparency, 439–440
- operation steps, 387
 - data transfer, 392
 - IKE, 388–392
 - security policy determining traffic needs, 387
 - tunnel termination, 393
- protocols, 380–381
 - authentication header, 381–382
 - ESP, 382–383
 - RSA-encrypted nonces, 436–438
- ipsec keyword, 72, 81
- IPSec tunnel, Easy VPN Remote, 491
- ipsnacl configuration mode, 66
- ip-vrf configuration mode, 66
- ISA (Integrated Service Adapter), 367
- ISAKMP (Internet Security Association and Key Management Protocol), 448
 - Easy VNP Server, 506
 - enabling, 413
 - policy defining, 413
 - crypto isakmp policy command, 414
 - identity, 416
 - negotiation, 415–416
 - verification, 429–430
 - debug crypto command, 432–434
 - ISAKMP error messages, 434
 - show crypto ipsec sa command, 431
 - show crypto ipsec transform-set command, 430
 - show crypto isakmp policy command, 430
 - show crypto map command, 431–432
- ISAKMP parameter, IKE policy, 458
- ISAKMP-established SA's lifetime algorithm parameter, IKE defaults, 407
- isdn keyword, 72, 81
- ISM (Integrated Service Module), 367
- ISP (Internet service provider), 18

J-K

- Java applets
 - CBAC inspection rules, 291–292
 - Cisco IOS Firewall, 47
- JavaScript, authentication proxy, 311–312
- Jobs command (Deployment menu), 644
- Jobs page, Router MC
 - actions, 660–662
 - creation, 662
 - status, 663
- KDC (Key Distribution Center), 158
- keepalives
 - messages, 187–188
 - NAT, 440
- Kerberos, 157–158
- kerberos instance map command, 103
- key command, 507
- Key Distribution Center (KDC), 158
- key exchange parameters (DH group ID)
 - parameter
 - IKE defaults, 407
 - IKE policy, 406–408, 457–458
- krb5 keyword, method parameter, 99–100
- krb5-instance keyword, method parameter, 103
- krb5-telnet keyword, method parameter, 99

L

- L0phtCrack, 22
- L2TP (Layer 2 Tunneling Protocol), 34, 276
- Label Distribution Protocol (LDP), 72
- LAN interface, SDM configuration, 545–546
- lane configuration mode, 66
- Layer 2 Tunneling Protocol (L2TP), 34, 276
- LDAP (Lightweight Directory Access Protocol), 133
- LDP (Label Distribution Protocol), 72
- LEAP (Light Extensible Authentication Protocol), 133
- legalities, government security regulations, 8–9
- level parameter, aaa authorization command, 102
- Light Extensible Authentication Protocol (LEAP), 133
- Lightweight Directory Access Protocol (LDAP), 133
- line configuration mode, 66
- line keyword, method parameter, 99–101
- Linux, trust models, 29
- list keyword, 344
- list option, ip port-map command, 290
- listings
 - AAA Security Commands, 147
 - Access List 150 for Router R2, 213
 - access-list command, 347
 - ACL Entries Permitting IPSec Traffic for RouterA, 412
 - ACL ICMP Messages, 217
 - ACL Permitting AAA Traffic to Firewall, 322

- ACL Restricting Telnet Access, 58
- applying ACLs to interface, 203
- Authentication Commands to Router Lines/Interfaces, 101
- AutoSecure Banner Creation, 244–245
- AutoSecure Configuring CEF and Ingress Filters, 247–248, 259–266
- AutoSecure Disabling Common Attack Vectors, 244
- AutoSecure Disabling Specific Interface Services, 246
- AutoSecure Initial Dialog, 242–243
- AutoSecure Internet Questions, 243
- AutoSecure Password Configuration, 246
- Blocking External TCP SYN DoS Packets, 215
- Blocking Traceroute UDP Messages, 217
- CA Authentication, 467
- CA Enrollment, 468
- Combining ACL Functions into Larger ACLs, 220–221
- Configuration of Crypto Map for RouterA, 427
- Configuring IKE Policy 110 on RouterA, 414
- Configuring NAT Keepalives, 440
- configuring standard ACL, 194
- Configuring Syslog for Router R3, 226
- crypto isakmp policy command sample, 473
- debug aaa accounting command output, 110
- debug aaa authentication command output, 107
- debug aaa authorization command output, 108
- debug tacacs command Successful Login, 151
- debug tacacs command Unsuccessful Login, 150–151
- debug tacacs events command Output, 151
- disabling SNMP services, 186
- disabling unused router interface, 191
- enable secret password hashed with MD5, 56
- Filter Smurf Attacks, 216
- Filtering Inbound ICMP Messages, 216
- filtering OSPF service, 212
- Filtering Source Address on Outbound Packets, 214
- filtering Telnet services, 211
- General-Purpose Key Pair Generation, 464–465
- ip audit name command, 347
- ISAKMP and IPSec Debugging, 432–434
- ISAKMP and Pre-Shared Keys, 417
- ISAKMP Policy for RouterA Output, 417
- Java Applet Filtering, 292
- list option for ip port map command, 290
- no crypto map command, 426
- no ip directed-broadcast command, 177
- no ip mask-reply command, 178
- no ip proxy-arp command, 184
- no ip redirect command, 179
- no ip unreachable command, 180
- no service finger command, 173
- no service password-recovery command enabled, 62–63

- ntp disable command, 182
- number ACL example, 197
- Proxy ACL definitions, 319
- Router Initial Configuration Dialog, 54
- router timeouts for console/auxiliary lines, 64
- running-config command, 472
- service password-encryption command
 - results, 61
- show access-list compile command output, 205
- show crypto ca certificates results, 471
- show crypto ipsec sa command, 431
- show crypto isakmp policy command, 404, 430
- show crypto key mypubkey rsa results, 471
- show crypto key pubkey-chain rsa results, 472
- show crypto map command, 401–405, 431
- show ip audit configuration command
 - output, 348
- show ip audit interface command output, 348–349
- show ip nhrp command, 402
- show ip ort-map command, 290
- show running-config command output, 172, 428–429
- Using TCP Intercept, 215
- viewing an ACL, 203
- vty user-level password not configured, 57
- list-name parameter
 - aaa accounting command, 105
 - aaa authentication login command, 99
 - aaa authentication ppp command, 100
 - aaa authorization command, 102
 - LLC2 (Logical Link Control, type 2), 72
 - llc2 keyword, 72, 81
 - local authentication, 84
 - local keyword, method parameter, 99–103
 - local parameter, snmp-server engine ID command, 76
 - local-case keyword, method parameter, 99–100
- locations
 - extended IP access lists, 747–748
 - standard IP access lists, 735
- log command, 734
- log files, application attack mitigation, 26
- log keyword, 64
- Log Viewer window, Cisco VPN Client, 522
- Logged in Users, Cisco Secure ACS for Windows reports, 140
- Logging SDM Monitor Mode, 586
- logging, SAFE, 233–234
- logging command, 225
- logging console command, 195–197
- logging facility command, 225
- logging history level command, 73, 81, 239, 241
- logging level command, 223
- logging on command, 226
- logging source-interface command, 226
- logging trap command, 225
- Logging window, Router MC firewall setting, 650
- Logical Link Control, type 2 (LLC2), 72
- logins
 - authentication
 - aaa login authentication command, 99

- PPP, 93–95
- remote username and password, 90
- S/Key, 90–91
- token cards and servers, 91–93
- CiscoWorks, Router MC, 601
- failure, rate configuration, 63–64
- unsuccessful attempts, 23
- low-risk devices, secure installation, 48
- Lucent, Radius version, 155

M

- MacAnalysis, 6
- mailing lists, application attack mitigation, 26
- maintenance, mitigating secure router
 - installation, 51–52
- Maintenance Operation Protocol (MOP), 181
- management
 - Cisco SAFE Blueprint, 12–13
 - Cisco software
 - PIX Device Manager, 35
 - VMS management applications, 35–37
 - VPN Solution Center, 35
 - protocol exploitation
 - NTP, 39
 - SNMP, 38
 - syslog, 38
 - Telnet, 37–38
 - TFTP, 39
 - routers, SAFE, 227–241

- Management Center command (VPN/Security Management Solution menu), 604
- Management Center for VPN Routers. *See* Router MC
- Management Information Base (MIB), 68
- man-in-the-middle attacks, 24–25
- map-class configuration mode, 66
- map-list configuration mode, 66
- max-events keyword, 342
- Maximum Transmission Unit (MTU), 522
- max-incomplete host error messages, 286–287
- MC (Mode Configuration), 485
 - Easy VPN Server, 485, 506–507
 - DNS domain, 508
 - DNS servers, 508
 - dynamic crypto map application, 511–512
 - group file definition, 507
 - IKE pre-shared key, 507
 - IP local pool address, 509
 - WINS server, 508
- MC IDS, IDS configuring, 351
- MD4 (message digest algorithm 4), 91
- MD5
 - algorithm, 386
 - hashes, 56, 61–62
- md5 keyword, ISAKMP configuration
 - command, 414
- md5 parameter, snmp-server user command, 83
- memory
 - buffer logging, 222
 - IDS implementation issue, 339
 - NVRAM, CAs support tasks, 461
- message digest algorithm 4 (MD4), 91

- message encryption algorithm parameter
 - IKE defaults, 407
 - IKE policy, 458
- message integrity (hash) algorithm parameter, 407, 458
- messages, ICMP, names, 742–744
- method parameter
 - aaa accounting command, 105
 - aaa authentication enable default command, 100
 - aaa authentication login command, 99
 - aaa authentication ppp command, 100
 - aaa authorization command, 102
- mGRE Tunnel Interface, 394
- MIB (Management Information Base), 68
- Microsoft website, 452
- Microsoft Certificate Services server, 451–452
- Microsoft CHAP. *See* MS-CHAP
- mission-critical devices, secure installation, 48
- Mode Configuration (MC), 485
- Monitor Mode, SDM, 585–586
- monitoring, CSMon, 129
- MOP (Maintenance Operation Protocol), 181
- mpls-ldp keyword, 72, 81
- mpls-traffic-eng keyword, 73, 81
- mpls-vpn keyword, 73, 81
- mpoa-client configuration mode, 66
- mpoa-server configuration mode, 66
- MS-CHAP (Microsoft CHAP), 121
 - Cisco Secure ACS for Windows, 121
 - PPP authentication, 94–95
 - security levels, 121
- MTU (Maximum Transmission Unit), 522
- MTU end-to-end discovery, 626–627
- multiple passwords, 23

N

- named IP access lists, 750–752
- NAPT (Network Address Port Translation), 41
- NAT (Network Address Translation), 37–41, 48, 229
 - icon, SDM Advanced Mode, 581–582
 - interoperability support, Easy VPN Remote, 492
 - IPSec, 438
 - IKE negotiation, 438–439
 - keepalives, 440
 - transparency, 439–440
 - Router MC, 654
 - PAT, 655
 - traffic filter, 655–656
 - SDM, 538
- NAT Traversal (NAT-T), 41
- National Science Foundation (NSF), 4
- NAT-T (NAT Traversal), 41
- NDS (Novell NetWare Directory Service), 121
- Network Address Port Translation (NAPT), 41
- Network Address Translation. *See* NAT
- Network Configuration, Cisco Secure ACS for Windows administration, 140
- Network Extension mode, Easy VPN Remote Phase II, 494
- Network File System (NFS), 29
- network IDS (NIDS), 12
- Network Information Service plus (NIS+), trust exploitation, 29
- Network Time Protocol. *See* NTP

- networks
 - ACLs traffic filtering, 213
 - DoS TCP SYN attack mitigation, 214–215
 - ICMP messages, 216–217
 - smurf attacks, 215–216
 - spoof mitigation, 213–214
 - classes, IP addressing, 725–726
 - parameter
 - aaa accounting command, 105
 - aaa authorization command, 102
 - reconnaissance attacks, 26–28
 - router security services
 - BOOTP server, 168–169
 - CDP service, 169–170
 - configuration autoloading, 170–171
 - finger service, 173–174
 - FTP server, 172
 - gratuitous ARP messages, 174
 - HTTP services, 174–176
 - ICMP mask requests, 178
 - ICMP redirect messages, 179
 - ICMP unreachable messages, 180
 - IP classless service, 176
 - IP directed broadcasts, 176–177
 - IP identification, 177–178
 - IP source routing, 180
 - keepalive messages, 187–188
 - MOP, 181
 - NTP, 181–182
 - PAD, 183
 - proxy ARP, 183–184
 - setting DNS server name, 171
 - small servers, 186–187
 - SNMP disabling, 184–186
 - TFTP server, 188–190
- routers
 - internal router, 167
 - perimeter router and firewall, 166–167
 - perimeter router with integrated firewall, 167
 - single perimeter router, 165
- security
 - changing role, 7
 - Cisco SAFE Blueprint, 9–13
 - closed networks, 5
 - e-business, 8
 - government regulations, 8–9
 - open networks, 6
 - policies. *See* policies
 - RADIUS server, 14, 153
 - threat capabilities, 6–7
 - unused interfaces, 190–191
- Networks command (Hub menu), 629
- Next Hop Resolution Protocol (NHRP), 393–394
- NFS (Network File System), 29
- NHRP (Next Hop Resolution Protocol), 393–394
- NIDS (network IDS), 12
- NIPRNET (Nonsecure Internet Protocol Network), 4
- NIS+ (Network Information Service plus), trust exploitation, 29
- no access-list command, 412
- no addressed-key command, 460
- no boot network command, 170

- no ca trustpoint command, 460
- no cdp enable command, 170
- no cdp run command, 170
- no certificate command, 460, 468, 470
- no crypto ca trustpoint command, 470
- no crypto ipsec nat-transparency udp-encapsulation command, 440
- no debug aaa accounting command, 110
- no debug aaa authentication command, 106
- no debug aaa authorization command, 107
- no debug all command, 475
- no exec command, 59
- no ftp-server enable command, 172
- no ftp-server write-enable command, 172
- no ip bootp server command, 169
- no ip classless command, 176
- no ip directed-broadcast command, 176–177, 216
- no ip domain-lookup command, 171
- no ip finger command, 173
- no ip gratuitous-arps command, 174
- no ip http ezvpn command, 495
- no ip http server command, 175
- no ip identd command, 178
- no ip inspect command, 301
- no ip inspect alert-off command, 283
- no ip mask-reply command, 178
- no ip proxy-arp command, 184, 570
- no ip redirect command, 179
- no ip source-route command, 180
- no ip unreachable command, 180
- no mop enabled command, 181
- no named-key command, 460, 471
- no service finger command, 173–174
- no service pad command, 183
- no service password-recovery command, 62–63
- no service tcp-small-servers command, 187
- no service udp-small-servers command, 187
- no snmp-server command, 186
- no snmp-server community command, 185
- no snmp-server enable traps command, 185
- no snmp-server host command, 79
- no snmp-server system-shutdown command, 186
- no tftp-server flash command, 189
- noauth keyword, 80
- noauth parameter, snmp-server group command, 78
- none keyword, method parameter, 99–103
- none parameter, aaa accounting command, 105
- Nonsecure Internet Protocol Network (NIPRNET), 4
- nonvolatile random-access memory (NVRAM), 146
- notification, CSMon, 129
- notification type parameter, snmp-server host command, 72, 80
- notify parameter, snmp-server group command, 78
- notify-view parameter, snmp-server group command, 78
- Novell NetWare Directory Service (NDS), 121
- NSF (National Science Foundation), 4
- NTP (Network Time Protocol), 13, 39, 181
 - disabling, 181–182
 - security exploitation, 39
- ntp access-group peer command, 459

ntp access-group serve-only command, 459
 ntp disable command, 182
 null-interface configuration mode, 66
 NVRAM (nonvolatile random-access memory), 146, 461

O

ODBC, 127
 oid-tree parameter, snmp-server view command, 77
 One-Step lockdown, SDM security audits, 573–574
 one-time passwords (OTPs), 16, 89
 Online Documentation, Cisco Secure ACS for Windows administration, 140
 OOB (out-of-band), management, 13, 232–233
 open networks, 6
 Open Shortest Path First (OSPF), 625
 operating systems, 3
 operator errors, 32
 origin authentication, digital signatures, 376–380
 OSPF (Open Shortest Path First), 538, 625
 OTPs (one-time passwords), 16, 89
 out-of-band (OOB), management, 13, 232–233
 outside interface, Easy VPN Remote, 492
 Overview, SDM Monitor Mode, 586

P

packet assembler/disassembler (PAD), 183
 packets
 ACLs, 191
 applying to router interface, 202–203
 commenting entries, 201
 development rules, 201–202
 directional filter, 202
 displaying, 203–204
 enhanced, 205–207
 identifying, 191–193
 IP types, 193–201
 Turbo ACLs, 204–205
 IDS auditing, 344–345
 creating and applying audit rules, 346
 default actions for info signatures, 345
 excluding addresses, 346–347
 sniffers, 15
 mitigation, 16–17
 types, 15–16
 PAD (packet assembler/disassembler), 183
 PAM (port-to-application mapping), 275
 CBAC, 287–288
 configuration display, 290
 user-defined port mapping, 288–290
 default table entries, 288
 PAP (Password Authentication Protocol), 121
 Cisco Secure ACS for Windows, 121
 PPP authentication, 93
 security levels, 121
 parameters, IKE policy, 457–458

- partition-number keyword, no tftp-server flash command, 190
- Password Authentication Protocol. *See* PAP
- password command, 55–59
- passwords
 - attacks, 22
 - mitigation, 23–24
 - routing table modification, 22–23
 - authentication
 - remote PC users, 90
 - S/Key, 90–91
 - auxiliary user-level configuration, 59–60
 - enable secret configuration, 55–56
 - encryption, router, 60–61
 - recovery
 - enable secret password, 56
 - ROMMON mode, 62–63
 - router administration, 53–55
 - SDM configuration, 544–545
 - user-level
 - console port configuration, 56–57
 - vtv connection configuration, 57–59
 - users, MD5 hashing, 61–62
- PAT (Port Address Translation), 48, 438
 - Router MC, NAT, 655
 - SDM, 538
- patches, application attack mitigation, 26
- PEAP (Protected Extensible Authentication Protocol), 132
- peer authentication
 - digital signatures, 377
 - pre-shared keys, 377–378
 - RSA signatures, 378
 - RSA-encrypted nonces, 379–380
 - IPSec IKE operation, 390
 - peer authentication method parameter, 407, 458
 - peer host name policy, IPSec encryption, 411
 - peer IP address parameter, IKE policy, 408, 458
 - peer IP address policy, IPSec encryption, 411
 - peer routers, Cisco IOS Firewall, 48
 - peers, IPSec, 411
 - peer-to-peer (PTP), 17
 - perimeter routers
 - AAA
 - aaa accounting command, 104–106
 - aaa authentication command, 98–102
 - aaa authorization command, 102–104
 - aaa new-model command, 97–98
 - configuration, 96
 - securing access, 95–96
 - securing privileged EXEC mode, 96–97
 - securing network, 165
 - firewall, 166–167
 - internal routers, 167
- permit command, 196
- personal computers (PCs), 4
- personal identification number (PIN), 16
- per-user firewalls, Cisco IOS Firewall, 47
- physical access threats, router installation, 49
 - electrical supply mitigation, 51
 - environment mitigation, 50–51
 - hardware mitigation, 49–50
 - maintenance mitigation, 51–52
- PIM (Protocol Independent Multicast), 73

- pim keyword, 73, 81
- PIN (personal identification number), 16
- ping command, 404, 411, 455
- ping sweeps, reconnaissance attacks, 27
- PIX Device Manager, 35
- PIX Firewalls, 34, 501
 - CiscoWorks Management Center, 37
 - VPN Client, 490
- PKCS #10 (Public-Key Cryptography Standard #10), 448
- PKCS #7 (Public-Key Cryptography Standard #7), 448
- PKI (Public Key Infrastructure), 447
- plain text passwords, 23
- policies
 - government security regulations, 8–9
 - IKE
 - defining parameters, 407
 - example network, 407–408
 - parameters, 406
 - purpose, 406
 - IPSec, determine traffic needs, 387
 - network security, 32–33
 - VPNs, 631–642
- pool command, 509
- POP (Post Office Protocol), 15
- Port Address Translation (PAT), 48, 438
- port scans, reconnaissance attacks, 27
- ports
 - Cisco IOS Firewall, 47
 - redirection attacks, 30
- port-to-application mapping. *See* PAM
- PPP
 - authentication
 - CHAP, 94
 - MS-CHAP, 94–95
 - PAP, 93
 - TACACS+ feature, 144
 - ppp authentication if-needed command, 148
 - ppp authentication ms-chap command, 95
 - ppp authentication pap command, 148
 - preaut configuration mode, 66
 - pre-share keyword, ISAKMP configuration command, 414
 - pre-shared keys
 - IKE policy, 634–636
 - peer authentication, 377–378
 - principal concept, SNMPv3, 74
 - priv keyword, 80
 - priv parameter, snmp-server group command, 78
 - private VLANs, man-in-the-middle mitigation, 25
 - privilege command, 65–67
 - privilege levels, router administration, 64–67
 - privileged EXEC mode, 54
 - privileges, network attacks, 19–20
 - processing IP access lists
 - extended, 738–739
 - standard, 732–733
 - properties, Cisco VPN Client, 518–519
 - Protected Extensible Authentication Protocol (PEAP), 132
 - Protocol Independent Multicast (PIM), 73

protocols, exploitation

- NTP, 39
- SNMP, 38
- syslog, 38
- Telnet, 37–38
- TFTP, 39
- provisioning Cisco IOS Firewall, 46
- proxy ARP, disabling, 183–184
- proxyacl#n attribute, user authorization profiles, 318–319
- PTP (peer-to-peer), 17
- Public Key Infrastructure (PKI), 447
- Public-Key Cryptography Standard #10 (PKCS #10), 448
- Public-Key Cryptography Standard #7 (PKCS #7), 448

Q-R

- QoS (quality of service), 47, 276
- Quick Mode, IKE, Easy VPN Remote, 503
- Quick Setup, SDM VPNs, 568–569
- Quick Start Guide for the VPN/Security Management Solution, 598
- RADIUS, 153
 - AAA, 87–89
 - authentication, 153, 513–514
 - authentication proxy, 310
 - client, 153
 - configuring, 153–156
 - enhancements, 156–157
 - IP address specification, 321–322
 - network security, 153
 - versus TACACS+, 88, 155–156
- RADIUS Accounting Report, Cisco Secure ACS for Windows reports, 140
- RADIUS Attribute 11, 156
- RADIUS Attribute 52, 157
- RADIUS Attribute 53, 157
- RADIUS Attribute 66, 157
- RADIUS Attribute 77, 157
- radius-server command, 154
- radius-server attribute 11 command, 156
- radius-server host command, 321, 513–514
- radius-server key command, 321, 514
- radius-server retransmit command, 514
- radius-server timeout command, 514
- rcp, Kerberos, 158
- RDBMS (Relational Database Management System), 126–127
- read parameter, snmp-server group command, 78
- read-view parameter, snmp-server group command, 78
- recording, CSMon, 129
- references, access lists, 753
- reimport methods, Router MC device import, 622
- Relational Database Management System (RDBMS), 126–127
- reload traps, SNMP router systems, 70
- remark command, 201
- remote access
 - Easy VPN Remote, 484
 - Client Release 3.5, 497–499
 - connection functionality, 499–503

- Phase II, 493–496
 - supported clients, 487–492
- Easy VPN Router, RADIUS
 - authentication, 513–514
- RADIUS, 153
 - authentication, 153
 - client, 153
 - configuring, 153–156
 - enhancements, 156–157
 - network security, 153
 - security policy, 33
 - VPNs, 364
- remote host parameter, snmp-server user
 - command, 83
- remote parameter, snmp-server engine ID
 - command, 76
- remote source-route bridging (RSRB), 73
- remote users, authentication
 - PPP, 93–95
 - S/Key, 90–91
 - token cards and servers, 91–93
 - username and password, 90
- Remote Web Manager, Easy VPN Remote, 492
- repeater keyword, 73, 81
- reporting
 - Cisco SAFE Blueprint, 12–13
 - SAFE, 227
 - architecture, 227, 229
 - information flow, 229–232
 - logging, 233–234
 - OOB management guidelines, 232–233
 - SNMP secure access, 235–241
 - SSH server configuration, 234–235
 - Reports and Activity, Cisco Secure ACS for
 - Windows administration, 140
 - Reports menu commands
 - Activities, 664
 - Audit Trail, 665
 - Reports tab, Router MC, 609–610
 - Request For Comments 2827 filtering, IP
 - spoofing mitigation, 18
 - request-dialin configuration mode, 66
 - request-dialout configuration mode, 66
 - Reset to Factory Default Wizard, SDM, 574–575
 - respond keyword, 511
 - responses, CSMon, 129
 - restricted view, 76
 - reverse-access parameter, aaa authorization
 - command, 102
 - reverse-route command, 510–511
 - RFC 2827 filtering, IP spoofing mitigation, 18
 - RIP, SDM, 538
 - risk assessments, secure router installation, 48
 - Rivest, Ronald, 91, 447
 - rlogin, 158
 - rom keyword, no tftp-server flash command, 190
 - ROMMON mode (ROM Monitor mode), 56, 62–63
 - rommon xmodem command, 62
 - route-map configuration mode, 66
 - router configuration mode, 66
 - Router MC (Management Center for VPN Routers), 591–592
 - access rules, 651–652
 - Activities Reports, 664
 - Administration tab, 665–666

- approving activities, 643
- Audit Trail Reports, 664–665
- building blocks, 652–654
- CiscoWorks login, 601
- communications, 596–597
- components, 595
- configuration file management
 - deployment options, 660–663
 - upload function, 656–658
 - viewing CLI commands, 658–659
- Configuration tab, 608–609
- creating activity, 611–614
 - Configuration tab, 614–615
 - functions, 612–613
- defining VPN policies, 631–632
 - IKE policy, 632–637
 - tunnel policies, 637–642
- defining VPN settings, 623–624
 - GRE configuring, 625–626
 - hub inside interface, 627–629
 - IKE keepalive, 624
 - MTU end-to-end discovery, 626–627
 - spoke inside interface, 629–631
- Deployment Reports, 663–664
- Deployment tab, 609
- device group creation, 615–617
- Devices tab, 607–608
- firewall settings, 648
 - ACLs ranges, 650–651
 - fragmentation rules, 648
 - half-open connections, 649–650
 - Logging window, 650
 - timeouts and performances, 648–649
- importing devices, 617–618
 - method selection, 618–622
 - reimport method, 622
- installing, 597
 - client workstation requirements, 598–599
 - process, 599–600
 - server requirements, 597–598
 - SSH router configuration, 600
- jobs, creating and deploying, 644–647
- key concepts, 592–594
- launching, 604
- main window, 605–606
- NAT rules, 654
 - PAT, 655
 - traffic filter, 655–656
- Reports tab, 609–610
- supported devices, 595–596
- tunnel technologies, 597
- users
 - adding, 604
 - authorization roles, 601–603
 - interface, 606–607
 - workflow tasks, 610–611
- routers
 - AAA
 - architecture, 84
 - external servers, 86–87
 - implementation, 84–85
 - local services, 85–86
 - methods, 89–95
 - perimeter routers, 95–106
 - RADIUS protocol, 87–89
 - TACACS+ protocol, 87–89

- troubleshooting, 106–110
- ACLs, 191
 - applying to interface, 202–203
 - commenting entries, 201
 - development rules, 201–202
 - directional filter, 202
 - displaying, 203–204
 - enhanced, 205–207
 - identifying, 191–193
 - IP types, 193–201
 - mitigating threats, 207–210
 - network traffic filtering, 213–217
 - router traffic filtering, 211–212
 - Turbo ACLs, 204–205
- administrative access
 - auxiliary user-level password, 59–60
 - banner messages, 67–68
 - console port connection, 52–53
 - console port user-level password, 56–57
 - console timeouts, 64
 - enable secret password configuration, 55–56
 - initial configuration dialog, 53–55
 - login failure rate, 63–64
 - MD5 hashing user passwords, 61–62
 - minimum password length, 55
 - password creation, 53
 - password encryption, 60–61
 - privilege levels, 64–67
 - ROMMON mode password recovery, 62–63
 - SNMP systems, 68–83
 - vty user-level password configuration, 57–59
- AutoSecure, 241–242
 - CBAC and ingress configuring, 247–248
 - CEF and ingress configuring, 246–247
 - change application, 248–258
 - example configuration post change application, 260–266
 - example configuration prior to change application, 259–260
 - global service disabling, 243–244
 - initiation, 242–243
 - interface services disabling, 246
 - Internet connection, 243
 - password configuration, 245–246
 - security banner creation, 244–245
- CAs
 - time and date, 461–462
 - interoperability, 450–452
- Cisco SAFE Blueprint, 10–11
- configuring IDS
 - setting alarm notification, 341
 - setting protected network, 341–342
 - specifying maximum event notifications, 342
- DDoS attacks, 218
 - Stacheldraht blocking, 218–219
 - Subseven blocking, 219
 - TRIN00 blocking, 218
 - TrinityV3 blocking, 219

- firewalls, 45, 275–276. *See also* firewalls
 - authentication proxy, 277–278
 - benefits, 46
 - CBAC, 276–301
 - Cisco IOS features, 46–48
 - feature set, 276
 - intrusion detection, 278
- installation
 - device risks, 48
 - threat types, 49–52
- network services
 - BOOTP server, 168–169
 - CDP service, 169–170
 - configuration autoloading, 170–171
 - finger service, 173–174
 - FTP server, 172
 - gratuitous ARP messages, 174
 - HTTP services, 174–176
 - ICMP mask requests, 178
 - ICMP redirect messages, 179
 - ICMP unreachable messages, 180
 - IP classless service, 176
 - IP directed broadcasts, 176–177
 - IP identification, 177–178
 - IP source routing, 180
 - keepalive messages, 187–188
 - MOP, 181
 - NTP, 181–182
 - PAD, 183
 - proxy ARP, 183–184
 - setting DNS server name, 171
 - small servers, 186–187
 - SNMP disabling, 184–186
 - TFTP server, 188–190
- SAFE, 227
 - architecture, 227, 229
 - information flow, 229–232
 - logging, 233–234
 - OOB management guidelines, 232–233
 - SNMP secure access, 235–241
 - SSH server configuration, 234–235
- sample configuration, 219–221
- securing network
 - internal router, 167
 - perimeter router and firewall, 166–167
 - perimeter router with integrated firewall, 167
 - single perimeter router, 165
- supporting IDS, 336–338
- syslog logging, 221–222
 - commands, 225–226
 - message format, 224
 - message levels, 223–224
 - system types, 222
- unused interfaces, 190–191
- VPNs
 - CiscoWorks Management Center, 37
 - defining, 363–365
 - optimized routers, 365–367
- Routing icon, SDM Advanced Mode, 580–581
- RPC, CBAC inspection rules, 292–293
- RSA encryption algorithm, 373
- RSA keys, 449, 453, 463–464
 - examples, 464–465
 - general-purpose keys, 464
 - special-usage key generation, 464

RSA signatures, peer authentication, 378
 rsa-encr keyword, ISAKMP configuration
 command, 414
 RSA-encrypted nonces
 IPSec, 436–438
 peer authentication, 379–380
 rsakeypair command, 466
 rsa-sig keyword, ISAKMP configuration
 command, 414
 rsh, Kerberos, 158
 rsh EXEC command, 158
 RSRB (remote source-route bridging), 73
 rsrb keyword, 73, 81
 rsvp keyword, 73, 81
 rsvp_policy_local configuration mode, 66
 rtr configuration mode, 66
 rtr keyword, 73, 81
 Rules icon, SDM Advanced Mode, 579–580

S

S/Key, remote user login, 90–91
 SA (security association), 391
 Easy VPN Remote, 501
 establishment policy, IPSec encryption,
 411
 IKE Phase 2 operation, 391–392
 IPSec lifetimes, 421–422
 SAFE (Cisco SAFE Blueprint), 227
 architecture, 227–229
 information flow, 229–232

 logging, 233–234
 OOB management guidelines, 232–233
 SNMP secure access, 235–241
 SSH server configuration, 234–235
 SAINT (Security Administrator's Integrated
 Network Tool), 6
 SATAN (Security Administrator's Tool for
 Analyzing Networks), 6
 SCEP (Simple Certificate Enrollment
 Protocol), 449–450, 497
 scope, security policy, 33
 SDLC (Synchronous Data Link Control), 73
 sdlc keyword, 73, 81
 SDLLC (SDLC Logical Link Control), 73
 sdllc keyword, 73, 81
 SDM (Security Device Manager),
 175, 535–536
 Advanced Mode, 575
 Interfaces and Connections icon,
 578–579
 NAT icon, 581–582
 Overview page, 576–578
 Routing icon, 580–581
 Rules icon, 579–580
 System Properties icon, 582–584
 VPN icon, 584–585
 features, 536–538
 firewall, 560–561
 advanced firewall creation, 563–567
 creating, 561–563
 Monitor Mode, 585–586
 Reset to Factory Default Wizard, 574–575

- security audits, 570
 - One-Step lockdown, 573–574
 - performing, 570–573
- security intelligence, 536–537
- software, 538
 - communications, 541–542
 - displaying flash memory, 540
 - downloading, 539
 - installing on existing router, 539–540
 - releases and devices, 538–539
 - requirements, 541
- Startup wizard, 542–551
- troubleshooting, 551
- user interface
 - main window features, 552–553
 - menu bar, 553
 - toolbar, 553–554
 - Wizard Mode window, 554–555
- users, 537
- VPNs, 567
 - editing settings, 570
 - site-to-site with pre-shared keys, 568–569
- WAN configuration
 - advanced mode, 560
 - Advanced Options window, 558
 - Configure LMI and DLCI window, 558
 - creating new connection, 556–557
 - IP address, 557
 - Serial Wizard, 557
 - viewing connections, 559
 - Wizard Summary window, 559
- secret-key systems, Kerberos, 157–158
- Secure Internet Protocol Network (SIPRNET), 4
- Secure Sockets Layer (SSL), 310
- security
 - changing role, 7
 - Cisco products, 34
 - Cisco SAFE Blueprint, 9–13
 - CiscoWorks Management Center, 37
 - closed networks, 5
 - e-business, 8
 - government regulations, 8–9
 - NAT configuration, 39–41
 - open networks, 6
 - protocol exploitation
 - NTP, 39
 - SNMP, 38
 - syslog, 38
 - Telnet, 37–38
 - TFTP, 39
 - SDM audits, 570
 - One-Step lockdown, 573–574
 - performing, 570–573
 - SDM configuration, 548
 - SNMPv3, 74
 - threats, capabilities, 6–7
- Security Administrator's Integrated Network Tool (SAINT), 6
- Security Administrator's Tool for Analyzing Networks (SATAN), 6
- security association. *See* SA
- Security Audit Wizard, SDM, 536

- security authentication failure rate command, 63
- Security Device Manager. *See* SDM
- Security Monitor (CiscoWorks Monitoring Center for Security), 333, 349–351
- security parameter index (SPI), 486
- security passwords command, 55
- security policy, IPSec, determining traffic needs, 387
- Serial Line Interface Protocol (SLIP), 67, 144
- serial tunnel notifications (STUN), 73
- Serial Wizard, SDM, 557
- server, Easy VPN Server, 483–484
 - IPSec support, 486–487
 - new features, 485–486
 - unsupported IPSec, 487
- Server Configuration menu commands, Setup, 604
- servers
 - configuring for Cisco Secure ASC for Windows, 136–137
 - Easy VPN Server, XAUTH support, 503–513
 - RADIUS, 153
 - authentication, 153
 - client, 153
 - configuring, 153–156
 - enhancements, 156–157
 - network security, 153
- service config command, 170
- service finger command, 173
- service groups, Router MC, 654
- service password-encryption command, 54, 57, 60–61, 96, 148
- service tcp-keepalives command, 188
- service tcp-keepalives-in command, 188
- service tcp-keepalives-out, 188
- service timestamps command, parameters, 152
- set pfs command, 396
- set security association lifetime command, 396
- set session-key command, 435
- set transform-set command, 395, 510
- Settings command (Configuration menu), 624
- Setup command (Server Configuration menu), 604
- sg-radius configuration mode, 66
- sg-tacacs+ configuration mode, 66
- sha keyword, ISAKMP configuration command, 414
- sha parameter, snmp-server user command, 83
- SHA-1 algorithm, 386
- Shamir, Adi, 447
- Shared Profile Components, Cisco Secure ACS for Windows administration, 140
- show commands, 454
- show access-list compiled command, 204
- show access-lists command, 203, 404, 412, 455, 493
- show accounting command, 110
- show commands
 - authentication proxy verification and testing, 327
 - CBAC verification and testing, 300–301
 - IDS configuration verification, 347–349

- show crypto ca certificates command, 461, 470
- show crypto ipsec client ezvpn command, Easy VPN Remote, 492
- show crypto ipsec sa command, 430–431, 440, 475
- show crypto ipsec transform-set command, 405, 430, 475
- show crypto isakmp command, 454
- show crypto isakmp policy command, 403–404, 413, 417, 429–430, 473–475
- show crypto isakmp sa command, 401, 473
- show crypto key mypubkey rsa command, 461
- show crypto key pubkey-chain rsa command, 461
- show crypto map command, 401, 403, 405, 431–432, 454, 475
- show flash command, 540, 551
- show interfaces command, 397, 400
- show ip audit debug command, 348–349
- show ip audit interface command, 348
- show ip audit statistics command, 347–348
- show ip auth-proxy command, 327
- show ip inspect command, 300–301
- show ip interface command, 204
- show ip nat statistics command, 493
- show ip nhrp command, 402
- show ip port-map command, 290
- show processes cpu command, 475
- show run command, 57, 454
- show running-config command, 60, 172, 403–404, 428
- show users command, 173
- shutdown command, 190
- signatures
 - commonly used by Cisco IDS, 352–357
 - IDS, 339–340
 - exclusion by host or network, 343–344
 - global disabling, 343
 - implementation issue, 339
- Simple Certificate Enrollment Protocol (SCEP), 449–450, 497
- Simple Mail Transfer Protocol (SMTP), 28, 293–294
- Simple Network Management Protocol. *See* SNMP
- SIPRNET (Secure Internet Protocol Network), 4
- sip-ua configuration mode, 66
- Site Security Handbook, 33
- site-to-site VPNs, 365
- SLIP (Serial Line Interface Protocol), 67, 144
- small servers, disabling, 186–187
- SMTP (Simple Mail Transfer Protocol), 28, 293–294
- smurf attacks, 20, 215–216
- SNMP (Simple Network Management Protocol), 10, 52
 - ACLs router traffic filtering, 211
 - administrative access, 52
 - router administrative access, 68–83
 - SAFE, 235–241
 - security exploitation, 38
 - services disabling, 184–186
 - syslog logging, 222

- snmp enable peer-trap poor qov command, 73, 82, 241
- snmp keyword, 73, 81
- snmp server link trap command, 81
- snmp trap link-status command, 79
- snmp-server command, 69, 237
- snmp-server community command, 68, 79–82, 236, 240
- snmp-server enable command, 79–82
- snmp-server enable traps command, 70, 238
- snmp-server engineID command, 75–76
- snmp-server group command, 77–78
- snmp-server host command, 70–71, 78–82, 238–241
- snmp-server host inform command, 79
- snmp-server trap-source command, 73, 241
- snmp-server user command, 82–83
- snmp-server view command, 76–77
- SNMPv3, 74–75
 - configuring engine ID, 75–76
 - defining views, 76–77
 - group names, 77–78
 - hosts, 78–82
 - user configuration, 82–83
- soft tokens, 89
- software
 - antisniffer, 17
 - Cisco management
 - PIX Device Manager, 35
 - VMS management applications, 35–37
 - VPN Solution Center, 35
 - SDM, 538
 - communications, 541–542
 - displaying flash memory, 540
 - downloading, 539
 - installing on existing router, 539–540
 - releases and devices, 538–539
 - requirements, 541
- spam keyword, 343
- spam attacks, IDS configuring, 342–343
- SPAN (Switched Port Analyzer), 17
- Spatial Reuse Protocol (SRP), 73
- special-usage keys, RSA keys, 464
- SPI (security parameter index), 486
- split tunneling, Easy VPN Server, 486
- Spoke menu commands, 629–630
- spokes, inside interface, 629–631
- spoofing, network traffic filtering, 213–214
- SRP (Spatial Reuse Protocol), 73
- srp keyword, 73, 81
- SSH
 - administrative access, 52
 - Router MC, 600
 - server, SAFE, 234–235
- SSL (Secure Sockets Layer), 310
- Stacheldraht blocking, DDoS attacks, 218–219
- standard IP access lists
 - commands, 733–735
 - common errors, 736
 - configuring, 723–753
 - location, 735
 - processing, 732–733
- standard named ACLs, 195–197
- standard numbered ACLs, 193–195
- start-stop parameter, aaa accounting command, 105
- Startup wizard, SDM, 542–551
- state tables, CBAC, 280

- static ARP, man-in-the-middle attack
 - mitigation, 24
- static NAT, 40
- Statistics tab, Cisco VPN Client, 525–526
- Step-by-Step Wizard, SDM VPNs, 568–569
- stop-only parameter, aaa accounting command, 105
- strong passwords, 24
- structured threats, 14
- STUN (serial tunnel notifications), 73
- stun keyword, 73, 81
- subnet addresses, IP addressing, 726–727, 729
- subscriber-policy configuration mode, 66
- Subseven blocking, DDoS attacks, 219
- switched infrastructures, packet sniffer mitigation, 17
- Switched Port Analyzer (SPAN), 17
- switches
 - Cisco SAFE Blueprint, 11
 - secure installation
 - device risks, 48
 - threat types, 49–52
- Synchronous Data Link Control (SDLC), 73
- syntax
 - TCP, 744
 - UDP, 746
- syslog
 - clients, 222
 - keyword, 73, 81
 - security exploitation, 38
 - logging, 221–222
 - message format, 224
 - message levels, 223–224
 - router commands, 225–226
 - system types, 222
 - servers, 13, 222

- System Configuration, Cisco Secure ACS for Windows administration, 140
- system parameter, aaa accounting command, 105
- System Properties icon, SDM Advanced Mode, 582–584

T

- TACACS, 144
- TACACS+ (Terminal Access Controller Access Control System Plus), 10
 - AAA, 87–89
 - authentication proxy, 310
 - configuring, 145–149
 - general features, 144–145
 - verification, 149–150
 - debug tacacs command successful login, 151
 - debug tacacs command unsuccessful login, 150–151
 - debug tacacs events command output, 151–152
 - versus RADIUS, 88, 155–156
- TACACS+ Accounting Report, Cisco Secure ACS for Windows reports, 140
- TACACS+ server, IP address specification, 320–321
- tacacs-server command, 146, 149
- tacacs-server host command, 148–149, 320
- tacacs-server key command, 149, 321
- tacacs-server key ciscosecure command, 148

- tcl configuration mode, 66
- TCP (Transmission Control Protocol), 20
 - DoS TCP SYN attack mitigation, 215
 - keepalive messages, 187–188
 - packets
 - CBAC, 277
 - TACACS+ feature, 144
 - port keywords, 744
 - servers, small server disabling, 187
 - sessions, CBAC, 281
 - half-open connection limits, 284–286
 - half-open connection limits by host, 286–287
 - idle time, 284
 - wait time, 283–284
 - syntax, 744
- TCP/IP (Transmission Control Protocol/Internet Protocol), 4
- tdm-conn configuration mode, 66
- Telnet
 - ACLs router traffic filtering, 211
 - administrative access, 52
 - Kerberos, 158
 - security exploitation, 37–38
 - vtv connection, configuring user-level password, 57–59
- telnet EXEC command, 158
- telnet keyword, 158
- template configuration mode, 66
- Terminal Access Controller Access Control System Plus. *See* TACACS+0
- terminal lines, syslog logging, 222
- terrorism, network security importance, 7
- TFTP (Trivial File Transfer Protocol), 39, 60
 - TFTP server, disabling, 188–190
- theoretical network
 - ACLs router threat mitigation, 210
 - sample router configuration, 219–221
- third-party ACS, 85
- threats
 - capabilities, 6–7
 - network security, 14
 - routers
 - ACLs, 191–217
 - AutoSecure, 241–266
 - DDoS attacks, 218–219
 - Installation, 49–52
 - internal router, 167
 - network services, 168–190
 - perimeter router and firewall, 166–167
 - perimeter router with integrated firewall, 167
 - SAFE, 227–241
 - sample configuration, 219–221
 - single perimeter router, 165
 - syslog logging, 221–226
 - unused interfaces, 190–191
- 3DES algorithm, 372, 386
- time, CAs support task configuration, 461–462
- time-based token cards, 92
- timeouts
 - router administrator sessions, 64
 - XAUTH, 504
- token cards, 89
 - authentication methods, 91–93
 - Cisco Secure ACS for Windows, 131–132
- token servers, authentication methods, 91–93

traffic

- ACLs, filtering, 207–209
- networks, ACLs filtering, 213–217
- routers, ACLs filtering, 211–212

traffic type to be encrypted policy, IPSec encryption, 411

transform sets

- dynamic crypto map, 510
- Easy VPN Server, 509
- IPSec, 409–410, 418–419
 - editing, 419–420
 - encryption, 411
 - negotiation, 420–421

Router MC, 653

Translation Rules command (Configuration menu), 655

translation-rule configuration mode, 67

transport mode, IPSec, 384–385

traps parameter, snmp-server host command, 71, 80

TRIN00 blocking, DDoS attacks, 218

TrinityV3 blocking, DDoS attacks, 219

Trivial File Transfer Protocol (TFTP), 39, 60

Trojan horses, 25–26, 31–32

troubleshooting

AAA

- debug aaa accounting command, 110
- debug aaa authentication command, 106–107
- debug aaa authorization command, 107–109

Cisco Secure ACS for Windows, 139–141

- accounting failure, 142
- authentication failure, 141–142
- authorization failure, 142
- debug commands, 143
- dial-in client problems, 143

SDM, 551

trust exploitation, 28–29

tty keyword, 73, 82

Tunnel Client Endpoint (RADIUS Attribute 66), 157

tunnel destination command, 400

tunnel key command, 398–400

tunnel mode, IPSec, 383–384

tunnel mode gre multipoint command, 398–400

tunnel policies, Router MC, 637–642

tunnel protection ipsec-profile command, 398–400

tunnel source command, 397–400

tunnel technologies, Router MC, 597

Tunnels command (Configuration menu), 637

Turbo ACLs, 204–205

U

UDP (User Datagram Protocol), 20, 746

packets, CBAC, 277

servers, small server disabling, 187

sessions, CBAC, 281

half-open connection limits, 284–286

idle time, 284

udp-port number parameter, snmp-server
 engine ID command, 76
 udp-port parameter, snmp-server engine ID
 command, 76
 udp-port port parameter
 snmp-server host command, 72, 80
 snmp-server user command, 83
 unauthorized access attacks, 31
 undebug all command, 475
 UNIX
 Cisco Secure ACS, 134–136
 trust models, 29
 unstructured threats, 14
 unsupported IPSec, 487
 Upload command (Configuration menu), 657
 User Datagram Protocol (UDP), 20
 user interfaces
 Router MC, 606–607
 SDM
 main window features, 552–553
 menu bar, 553
 toolbar, 553–554
 Wizard Mode window, 554–555
 User Setup, Cisco Secure ACS for Windows
 administration, 139
 username admin password command, 148
 username parameter, snmp-server user
 command, 82
 username secret command, MD5 hashing,
 61–62
 users
 passwords
 auxiliary configuration, 59–60
 console port configuration, 56–57

 MD5 hashing, 61–62
 vty connection configuration, 57–59
 SDM, 537, 544–545
 SNMPv3, 82–83

V

v1 parameter
 snmp-server group command, 77
 snmp-server user command, 83
 v2c parameter
 snmp-server group command, 78
 snmp-server user command, 83
 v3 parameter
 snmp-server group command, 78
 snmp-server user command, 83
 VACs (VPN Acceleration Cards), 34
 VAM (VPN Acceleration Module), 367
 vc-class configuration mode, 66
 verification
 access list configuration, 750
 DMVPN, 401–403
 IPSec, 429–430
 debug crypto command, 432–434
 ISAKMP error messages, 434
 show crypto ipsec sa command, 431
 show crypto ipsec transform-set
 command, 430
 show crypto isakmp policy command,
 430
 show crypto map command, 431–432

- VeriSign OnSite CA server, 450–451
- version keyword, 79–80
- version parameter, snmp-server host command, 71, 80
- view concept, SNMPv3, 75
- View Configs command (Deployment menu), 646
- view-name parameter, snmp-server view command, 76
- Vigenere cipher, 60
- virtual adapters, Cisco VPN Client new release, 526
- Virtual Memory System (VMS), 597
- Virtual Private Dialup Network (VPDN), 123
- virtual private networks. *See* VPNs
- viruses, 31–32
- VLANs, private, man-in-the-middle attack mitigation, 25
- VMS (VPN/Security Management Solution), 35–37, 133, 597
- voice keyword, 73, 82
- voice protocols, Cisco IOS Firewall, 46
- voiceclass configuration mode, 67
- voiceport configuration mode, 67
- voidialpeer configuration mode, 67
- VPDN (Virtual Private Dialup Network), 123
- vpdn-group configuration mode, 66
- VPN Acceleration Cards (VACs), 34
- VPN Acceleration Module (VAM), 367
- VPN Interfaces command (Spoke menu), 630
- VPN Monitor, 35
- VPN Solution Center (VPNSC), 35
- VPN Status, SDM Monitor Mode, 586
- VPN/Security Management Solution (VMS), 133
- VPN/Security Management Solution menu commands, Management Center, 604
- VPNs (virtual private networks), 9
 - Cisco IOS Firewall, 47
 - Cisco VPN 3000 Series Concentrators, 34
 - CiscoWorks Management Center, 37
 - Client
 - authentication, 519
 - connection properties, 520–521
 - General tab, 524–525
 - installation, 515
 - log viewer, 522
 - MTU size, 523–524
 - multiple connection entries, 516
 - new release changes, 526–529
 - option modification, 516–517
 - program menu, 521–522
 - properties, 518–519
 - Statistics tab, 525–526
 - defining, 363–365
 - DMVPN, 393–403
 - Easy VPN, 483
 - Remote, 484–503
 - Router, 513–514
 - Server, 483–487, 503–513
 - firewall benefits, 46
 - icon, SDM Advanced Mode, 584–585
 - optimized routers, 365
 - enterprise-size environments, 367
 - large environments, 366
 - small environments, 366–367
 - Router MC, 591–592

- access rules, 651–652
- Activities Reports, 664
- adding users, 604
- Admin tab, 610
- Administration tab, 665–666
- approving activities, 643
- Audit Trail Reports, 664–665
- building blocks, 652–654
- CiscoWorks login, 601
- communications, 596–597
- components, 595
- configuration file management, 656–663
- Configuration tab, 608–609
- creating activity, 611–615
- creating and deploying jobs, 644–647
- defining policies, 631–642
- defining settings, 623–631
- Deployment Reports, 663–664
- Deployment tab, 609
- device group creation, 615–617
- Devices tab, 607–608
- firewall settings, 648–651
- importing devices, 617–622
- installing, 597–600
- key concepts, 592–594
- launching, 604
- main window, 605–606
- NAT rules, 654–656
- Reports tab, 609–610
- supported devices, 595–596
- tunnel technologies, 597
- user authorization, 601–603
- user interface, 606–607
- workflow tasks, 610–611

- SDM, 567
 - editing settings, 570
 - site-to-site with pre-shared keys, 568–569
- VPNSC (VPN Solution Center), 35
- vrf parameter, snmp-server engine ID command, 76
- vrf vrf-name parameter
 - aaa accounting command, 105
 - snmp-server host command, 73, 82
- vrf-name parameter, snmp-server engine ID command, 76
- vsimaster keyword, 73, 82
- vty connections, user-level password configuration, 57–59

W

WANs, SDM

- advanced mode, 560
- Advanced Options window, 558
- Configure LMI and DLCI window, 558
- creating new connection, 556–557
- IP address, 557
- Serial Wizard, 557
- viewing connections, 559
- Wizard Summary window, 559

web browser, Cisco Secure ACS for Windows configuration, 137–138

WEP (Wired Equivalent Privacy), 6

wildcard masks, IP access lists, 729–730

Windows

- Cisco Secure ACS, 120–121
 - AAA services, 123
 - ACS user database access, 129–130
 - administration, 139–141
 - administration features, 123–124
 - database management, 126–127
 - distributed system, 124–125
 - external database support, 125–126
 - general features, 121–122
 - installation, 136–139
 - product enhancements, 132–134
 - service modules, 127–129
 - token card support, 131–132
 - troubleshooting, 139–143
 - Windows user database access, 130–131
 - trust models, 29
- WINS (Windows Internet Name Service), 497
- wins command, 508
- Wired Equivalent Privacy (WEP), 6
- wireless access, security threats, 6
- Wizard Mode window, SDM user interface, 554–555
- Wizard Summary window, SDM, 548, 559
- wizards, SDM, 536
 - Reset to Factory Default, 574–575
 - Serial, 557
 - Startup, 542–551
 - WAN, 556–557
- worms, 26, 31–32
- write parameter, snmp-server group command, 78
- write-view parameter, snmp-server group command, 78

X-Y-Z

- X.509v3 certificates, 449
- x25 keyword, 73, 82
- XAUTH (Extended Authentication), 485
 - Easy VPN Server, 485, 503–504
 - configuration, 504–505
 - dynamic crypto map applied to outside interface, 512
 - dynamic crypto map creation, 509–511
 - group policy for MC push, 506–509
 - group policy lookup, 506
 - IKE DPD enabling, 512–513
 - ISAKMP policy, 506
 - local IP address pool, 505
 - MC application to dynamic crypto map, 511–512
 - transform sets, 509
- XTACACS, 144