

Numerics

3DES (Triple DES), 51, 93

A

AAA (authentication, authorization, and accounting)

- Easy VPN Server, 733–734
- NAC, 272–273
- overview, 27, 220, 934
- RADIUS servers, 916
- server administrators, 379–380
- tunnel groups, 873
- WebVPN, 762–763
- wireless campuses, 946–947

access hours, groups, 212

Access Rights option, 377

access, administrator

- AAA servers, 379–380
- ACLs, 379
- administrator accounts, 377–378
- management protocols, 380–381
- settings, 379

accounting servers

- overview, 217–219
- RADIUS servers, 219–220

accounts, administrator, 377–378

ACLs (access control lists)

- ACL bypassing, 819
- administrator access, 379
- allowing IPsec traffic, 582–583, 818–819
- CACCTP feature, 671–673
- concentrators, 188
- configuring certificate ACLs, 613
- crypto ACLs, 644–645, 834–835
- defining how to protect traffic, 834–835
- Easy VPN Server, 736
- expired certificate ACLs, 613–614
- Network Neighborhood, 494
- specifying traffic to protect, 834
- tunneled traffic, 923
- WebVPN, 302–303

Adapter Security Appliance (ASA), 817

addresses

- clients, 108–109
- concentrators, 199
- DHCP, 222–224
- L2L connections, 331
- managing, 26–27, 520
- overlapping, 33, 346
- pools
 - Easy VPN Server, 848–849
 - overview, 225–227
 - tunnel groups, 872
- private addressing, 16
- remote access, 26–27
- translation
 - issues, 33–34, 124
 - L2L sessions, 344–349
 - L2TP, 151
 - PIX/ASA appliances, 810
 - PPTP, 143–144
 - solutions, 124–125
 - SSL, 165
- updates, 938
- VRRP, 366

admin account, 378

Administer Sessions option, 377

administration

- concentrators, 376–381
- VPN 3200, 564–568

administrative rights, SSL, 157

Advanced Encryption Standard

See AES

advanced mode, VPN Client, 436–438

AES (Advanced Encryption Standard)

- algorithms, 234
- concentrators, 186
- overview, 52, 93, 589, 922

aggregation, bandwidth, 358

aggressive mode, IPsec, 102

AH (authentication header)

- concentrators, 333
- Easy VPN Server, 732
- ESP, versus, 117

headers, 118

NAT/PAT incompatibility, 119

overview, 34, 90–93, 118–119

AI

See automatic initiation

algorithms

- AES, 52–53
 - DES/3DES, 51–52
 - Diffie-Hellman, 61–64, 95
 - L2TP versus PPTP, 151
 - overview, 24
 - anti-replay attacks, 90
 - antivirus packages, CSD, 307
 - any keyword, 834
 - application
 - support, 25
 - types, 32–33
 - Application Launcher feature, VPN Client, 424, 460
 - areas, OSPF routing, 364
 - ARP
 - split tunneling, 112
 - ASA (Adapter Security Appliance)
 - address translation, 810
 - certificates, 812
 - connections
 - ISAKMP/IKE Phase 1, 887–888
 - ISAKMP/IKE Phase 2, 833–840 901–909
 - L2L examples, 841–845
 - deployment scenarios, 809
 - L2L connections, 809–810
 - remote access connections, 809–810
 - special capabilities, 810
 - Easy VPN, 812
 - encryption, 812
 - features, 812–813
 - FOS 6.x
 - configuring Easy VPN Remote, 856–862
 - configuring Easy VPN Server, 847–855
 - FOS 7.0
 - configuring Easy VPN Server, 862–877, 883–885
 - troubleshooting Easy VPN Server, 877–883
 - IPsec traffic, allowing, 818–820
 - load balancing, 881
 - models, 814–815
 - OSPF, 812
 - overview, 817, 917–918
 - QoS, 813
 - redundancy, 811
 - RRI, 812
 - RSA algorithm, 812
 - SSL, 812
 - stateful firewall services, 810–811
 - transform sets, 835
 - VCA, 371, 880
- asymmetric keying algorithm, 61
 - asymmetric keys
 - advantages/disadvantages, 48–49
 - authentication, 47–48
 - encryption, 47
 - examples, 49
 - overview, 46–47
 - attacks
 - eavesdropping, 5–7
 - man-in-the-middle, 8–11, 65–66
 - masquerading, 7–8
 - packet replay, 92
 - audit logs, 527–530
 - authentication
 - AAA, 916, 934
 - asymmetric keys, 47–48
 - Authentication tab, 439
 - CAs, 915–916
 - CBAC, 610–612
 - CBCP, 134
 - certificates, 451, 915–916, 931
 - CHAP, 133–134
 - concentrators, 185, 200
 - CRACK, 234
 - CRLs, 613–614
 - device authentication
 - acquiring certificates, 78
 - digital certificates, 69–78, 235–247, 415–416
 - file-based enrollment, 78–80
 - network-based enrollment, 80–82
 - overview, 22–23, 66–67, 235, 914, 941
 - PIX/ASA, 823–833
 - pre-shared keys, 67–69, 235, 413–415
 - using certificates, 82–84
 - DH, 104
 - digital certificates
 - CBAC, 610–612
 - CRLs, 613–614
 - enrolling manually, 603–609
 - enrolling using SCEP, 595–603
 - expired certificate ACLs, 613–614
 - importing/exporting, 615–617

- Easy VPN, 185
- Easy VPN Remote, 751–752
- Easy VPN Server, 851–852, 876–877
- e-mail proxy, 290
- expired certificate ACLs, 613–614
- external authentication
 - assigning addresses, 221–227
 - authentication/accounting servers, 217–220
 - configuring groups, 220–221
 - creating authentication servers, 215–217
 - overview, 214–215
- importing/exporting RSA keys/certificates, 615–617
- ISAKMP/IKE Phase 1
 - digital certificates/router enrollment, 595–617
 - pre-shared keys, 588–595
 - router identity types, 587–588
- keys, 45
- L2TP, 145
- L2TP versus PPTP, 151
- man-in-the-middle attacks, 65
- mutual group authentication, 22, 86, 452
- OSPF, 365
- overview, 21, 38, 65
- packets
 - HMAC functions, 58–59
 - MD5, 55
 - overview, 24, 53–57
 - SHA, 55
- PAP, 133
- passwords, 23
- peers, 90
- PPTP, 131–134
- pre-shared keys
 - configuring, 588–589
 - overview, 22
 - protecting, 589–590
 - RSA encrypted nonces, 590–595
 - viewing, 590
- RADIUS servers, 217–220, 916
- RAs, 915–916
- RIPv2, 362
- routing protocols, 56
- save password feature, 737
- solutions, 66
- SSL
 - IPsec, versus, 167
 - overview, 159
- troubleshooting
 - certificates, 415–416
 - pre-shared keys, 413–415
 - XAUTH, 416–417
- user accounts
 - internal authentication group setup, 227
 - internal authentication user setup, 227–229
 - overview, 23, 67, 84
 - remote access, 85–86
 - XAUTH, 416–417
- usernames, 23
- VPN 3200
 - building IPsec tunnels, 553–555
 - configuring VPN 3000 concentrators, 552–553
 - Individual Unit Authentication, 551–552
 - Interactive Unit Authentication, 551
 - overview, 534, 548–549
 - Unit Authentication, 549–550
 - verifying connections, 556
- VPN Client, 439, 478–479
- WebVPN, 282
- Windows, 504
- wireless campuses, 946–947
- XAUTH, 478, 481, 851–852, 916
- authentication header
 - See* AH
- authentication, authorization, and accounting
 - See* AAA
- auto-archiving, key pairs, 628–629
- autoenrollment
 - CAs, 609
 - overview, 608
 - trustpoint configuration, 608–609
- Auto-Initiation feature, VPN Client, 424
- Automatic Client Confirmation feature, VPN Client, 425
- Automatic Dialup Connection feature, VPN Client, 424
- automatic initiation (AI)
 - using, 461, 464
 - verifying configuration, 463
 - VPN Client GUI, 464
 - vpnclient.ini file, 461–463
- Automatic Start/Disconnect feature, VPN Client, 425

automatic updates

- Automatic Updates feature, VPN Client, 425
- autoupdate.exe program, 473
- overview, 875
- AutoSetMTUparameters, 430
- availability, concentrators, 184
- AYT mode
 - concentrators, 185
 - Easy VPN Server, 736
 - firewalls, 112, 736
 - overview, 465–467
 - routers, 736

B

backup server

- concentrators, 187
- IPsec, 185
- Backup Servers tab, 442
- bandwidth
 - aggregation, 358
 - L2L sessions, 335
 - management, 186, 351
 - overview, 919
 - policies
 - activating, 355–356
 - creating, 352–355
 - QoS, 359
 - routers, 576
- base groups, 208–209
- binary_config.ini file, 471
- Binary-{Major|Minor}-4.X.Yy.Zzzz.zip file, 471
- blackhole routers, 489
- Browser Proxy feature, VPN Client, 425
- budgeting, 43

C

CA (certificate authority), 22

- additional parameters, 629–631
- autoenrollment, 609
- backing up, 638–639
- CRLs, 602, 832–833
- device authentication, 824–833
- enabling, 625

external access, 235

- generating/exporting RSA key pairs, 621
 - overview, 22, 70–71, 597–599, 915–916
 - PIX/ASA appliances, 812
 - restoring, 639–640
 - routers as
 - backing up CAs, 638–639
 - configuring RA mode on servers, 636
 - controlling certificate requests with passwords, 634
 - defining additional parameters, 629–631
 - enabling CAs, 625
 - generating/exporting RSA key pairs, 621–623
 - granting enrollment requests, 633–634
 - handling enrollment requests, 631–632
 - manually entering certificate enrollment, 634–635
 - overview, 620–621
 - protecting CA keys, 623–625
 - RA configuration/operation, 636–637
 - rejecting certificate requests, 634
 - removing CA services, 640–641
 - removing enrollment requests, 633
 - restoring CAs, 639–640
 - revoking ID certificates, 635–636
 - setting up RAs, 637
 - using auto-archiving, 628–629
 - using manual RSA keys, 625–627
 - viewing enrollment requests, 632
 - SCEP, 609
 - show commands, 601
 - SSL, 159
 - troubleshooting, 785
 - VPN Client, 444
 - WebVPN, 169
- CAC (call admission control)
implementing for IKE, 738–740
IPsec, 737
- CACCTP feature, 671–673
- cache cleaner
 - Mac/Linux, 318
 - Windows, 313
- call admission control (CAC), 737
- Callback Control Protocol
See CBCP
- callback control, PPTP, 134

- Call-Clear-Request message, PPTP, 141
- Call-Disconnect-Notify message
 - L2TP, 150
 - PPTP, 141
- caller ID value, 139
- CAST, 51
- CABAC (certificate attribute-based access control), 610-612
 - overview, 610-611
- CBCP (Callback Control Protocol), 134
- CB-LLQ (class-based low latency queuing), 577
- CB-WFQ (class-based weighted-fair queuing), 577
- Central Policy Protection/Push (CPP) firewall policy, 112
- certificate attribute-based access control (CABAC), 610-612
- context-based access control, 166
- certificate authority
 - See* CA
- Certificate Management option, 377
- certificate optimization feature, 579
- Certificate Revocation Lists
 - See* CRLs
- certificates
 - acquiring, 78-82
 - allowing external access to CAs, 235
 - certificate mapping rules, 878-880
 - configuring
 - certificate group matching parameters, 244-247
 - CRL parameters, 241-242, 244
 - connection profiles, 451-452
 - CRLs, 76-78
 - device authentication, 824-833
 - Easy VPN Remote, 858-859
 - e-mail proxy, 290
 - enrolling, 931, 940-941
 - exportable, 924
 - file-based, 236-237
 - groups, 244-247
 - identity certificates, 72, 236-241, 247
 - L2L connections, 332-333
 - obtaining certificates, network-based, 239-241
 - overview, 22, 69-70, 235, 915-916, 923
 - passwords, 451
 - PIX/ASA appliances, 812
 - PKCS, 72-73, 76, 237
 - PKI, 71-72
 - root certificates, 236-241, 247
 - SCEP, 76, 239, 447-448
 - SSL, 763-765
 - SSLSM, 579
 - standards, 70
 - status, 449
 - SVC, 305
 - troubleshooting, 415-416, 785
 - trustpoints, 827
 - using, 82-84, 247
 - VPN Client, 444
 - deleting certificates, 450
 - exporting certificates, 450-451
 - importing root certificates manually, 446
 - managing certificates, 448
 - obtaining certificates, 444-452
 - setting/changing certificate passwords, 451
 - specifying in connection profiles, 451-452
 - status, 449
 - viewing certificates, 448-450
 - wireless campuses, 944-945
 - X.509 certificates, 74, 76
- CHAP (Challenge Handshake Authentication Protocol), 133
- chassis redundancy
 - overview, 366
- VCA
 - configuring, 373-375
 - operation, 372-373
 - overview, 371
 - verifying, 376
- VRRP
 - configuration synchronization, 369-371
 - configuring, 368-369
 - overview, 366-367
- CIC (Cisco Integrated Client), 261, 464-466
- Cisco IOS Firewall feature set, 166
- Cisco IP Phones, 553
- Cisco Secure Desktop (CSD)
 - backing up/restoring, 320
 - configuring
 - cache cleaner, Mac/Linux, 318
 - upload/download settings, 318
 - for Windows, 308-313
 - enabling CSD, 319-320
 - installing on concentrators, 308

- overview, 169, 270, 307
 - saving settings, 319–320
 - using, 320
- Cisco Secure Socket Layer Services Module (SSLSM), 579
- Cisco VPN 3000 concentrators
 - See* VPN 3000 concentrators
- Cisco VPN Client
 - See* VPN Client
- CiscoWorks VMS Router Management Center (MC), 573
- class-based low latency queuing (CB-LLQ), 577
- class-based policing, 577
- class-based weighted-fair queuing (CB-WFQ), 577
- classes
 - logging
 - configuring classes, 400–403
 - configuring e-mail, 399
 - configuring SNMP server for traps, 398–399
 - configuring syslog server, 399
 - default configuration, 395–397
 - FTP backup, 398
 - overview, 394–395, 476
 - troubleshooting, 524
- clear commands
 - crypto sessions, clearing, 796–797
 - data connection management commands, 839
 - IPsec tunnels, tearing down, 753
 - ISAKMP/IKE Phase 1, 888
 - ISAKMP/IKE Phase 2, 902
 - stateful failover, 701
- clear text data, 5
- client connections, Windows, 521
 - connecting to VPN gateways, 521
 - troubleshooting, 525–530
 - verifying concentrator connection, 523
 - verifying PC connection, 522–523
- client implementations, SSL, 156–157
- client mode
 - Easy VPN Remote, 747–748
 - IPsec, 109
 - VPN 3200, 545, 557
- clientless implementations, SSL, 156
- clients
 - hardware clients, 536–537
 - See also* VPN 3200 hardware client
 - software clients, 536
- Windows
 - configuring, 500–501
 - features, 498–499
 - L2TP, requiring, 506–507
 - operational, verifying, 499–500
 - overview, 497–498
 - security policies, creating, 501–506
 - VPN connections, creating, 507–515
- Co-Existence feature, VPN Client, 425
- collisions, 55
- colors, WebVPN, 766
- committed access rate, 577
- compression
 - Compression feature, VPN Client, 425
 - PPTP, 132
 - overview, 279, 647
- compulsory tunnels, L2TP, 147, 151
- concentrators
 - accessing
 - bootup process, 190
 - CLI interface, 190–194
 - GUI, 194–205
 - HTTP, 194
 - initial configuration, 191–193
 - main menu, 203–205
 - overview, 189–190
 - password recovery, 193–194
 - quick configuration, 195–202
 - ACLs, 188
 - address translation, 810
 - administration screens, 376–377
 - administrator access, 377–381
 - AH, 333
 - authentication, 185, 188
 - auto-update, 472
 - AYT feature, 185
 - backup peers, 188
 - backup server feature, 187
 - bandwidth management, 186, 355
 - chassis redundancy
 - VCA, 371–376
 - VRRP, 366–371
 - Cisco concentrators, 185
 - client updates, adding, 469
 - compression, 279
 - configuring
 - address assignment, 199
 - administrator, 202

- authentication, 200
- interfaces, 196
- IPsec group, 200
- network extension mode, 559
- public interface, 196
- RRI, 563
- start, 195
- system information, 197
- tunneling, 198
- WebVPN, 201
- CRLs, 187
- CSACS, 188
- CSD, 189
- DH group 5, 186
- DHCP Intercept feature, 186
- DHCP relay feature, 186
- digital certificates, 187
- DPD, 188
- dynamic DNS, 187
- encryption, 186
- event logs
 - classes/logging levels, 394–403
 - date/time, 393–394
 - filterable event logs, 406–408
 - live events, 404–406
 - setting up, 393
- features, 184
 - version 3.5, 185–186
 - version 3.6, 186–187
 - version 4.0, 187–188
 - version 4.1, 188
 - version 4.7, 188–189
- file management, 382
- filtering, 187
- firewalls, 188
- Flash memory, 381
- groups
 - base/global groups, 208–209
 - external authentication, 214–227
 - General tab, 211–214
 - Identity tab, 210–211
 - overview, 207–208
 - specific groups, 209
- Internet remote access, 928
- IPsec
 - Client FW tab, 260–267
 - data SAs, 268–270
 - device authentication, 235–247
 - IKE proposals, 230–234
 - IPsec tab, 247–250
 - Mode/Client Config tab, 251–259
- IPsec over TCP, 186
- L2L connections
 - adding, 327–328
 - address translation, 344–349
 - certificates, 332–333
 - completing, 342–343
 - configuration parameters, 328–331
 - connection policies, 333–335
 - connectivity example, 323–325
 - device authentication, 332–333
 - filtering, 344
 - groups, 344
 - IPsec SAs, 344
 - local/remote networks, 341–342
 - modifying, 344
 - peer connectivity, 331–332
 - private addresses, 331–332
 - routing options, 335–341
 - setting up, 325–327
- L2TP over IPsec, 187
- load balancing, 181
- management features, 184
- models, 177–182
- modules, 182–183
- MTUs, 187
- NAC
 - exception lists, 272
 - global configuration for IPsec, 270–271
 - group configuration, 272–274
- NAT-T, 186, 487
- network extension mode, 186
- overview, 18, 918
- PIX/ASA appliances, versus, 810
- PPTP, 134
- redistribution, 341
- remote access, configuring
 - assigning addresses, 221–227
 - groups, 207–221
 - PPTP/L2TP, 277–281
 - user accounts, 227–229
 - WebVPN, 281–320
- routers, versus, 573
- routing
 - OSPF, 363–365

- RIP, 361–362
 - static routing, 359–361
- RRI, 186
- SCEP, 186
- SCP, 187
- SEP modules, 183
- session restrictions, 324
- split DNS, 187
- SSL VPN, 188
- statistic, 186
- TFTP, 382
- troubleshooting
 - common problems, 410–418
 - event logs, 393–406
 - See also* event logs
 - gathering statistics, 409–410
 - ISAKMP/IKE Phase 1 problems, 411–417
 - ISAKMP/IKE Phase 2 problems, 417–418
 - overview, 385–386, 524–525
 - system status, 386–387
 - VPN sessions, 387–392
- upgrades, 381
- user accounts
 - internal authentication group setup, 227
 - internal authentication user setup, 227–229
- verifying
 - client connections, 523
 - network extension mode, 559–561
- VPN 3000
 - addresses, managing, 520
 - groups, configuring, 518–520
 - HW Client Group tab, 552–553
 - IKE proposals, 516–517
 - IPsec SAs, 517
 - network extension mode, 559
 - overview, 516, 552
 - updates, 566–568
 - users, configuring, 520–521
- WebVPN, 188
- wireless, 943
 - AAA, 946–947
 - base configuration, 943–944
 - base group configuration, 947
 - certificate enrollment, 944–945
 - CLI Quick Configuration, 943
 - data SAs configuration, 945–946
 - ISAKMP/IKE configuration, 945
 - specific software client group configuration, 947–949
 - VCA, 949–950
 - XML, 186, 382
- confidence interval, 248
- confidentiality, 38, 90
- config account, 378
- CONFIG file, 382
- CONFIG.BAK file, 382
- congestion avoidance, 577
- connect time, groups, 213
- connections
 - certificates, 451–452
 - Easy VPN Remote, 750
 - IPsec
 - versus SSL, 167
 - VPN Client, 438–452
 - ISAKMP/IKE, 582
 - modes
 - overview, 12–13
 - transport mode, 13–14
 - tunnel mode, 14–16
 - types
 - fully meshed, 29
 - partially meshed, 30
 - point-to-point, 28
 - VPN 3200
 - building IPsec tunnels, 553–555
 - configuring VPN 3000 concentrators, 552–553
 - Individual Unit Authentication, 551–552
 - Interactive Unit Authentication, 551
 - overview, 548–549
 - Unit Authentication, 549–550
 - verifying connections, 556
 - Windows clients
 - overview, 521–523
 - troubleshooting, 525–530
- console ports, 189
- content control, SSL, 160–161
- content filtering, 161
- Content Switching Module (CSM), 579
- control messages
 - L2TP, 149–150
 - PPTP, 136–138
- cost, 43

CPP (Centralized Protection Policy), 112, 465–467
 CQ (custom queuing), 577
 CRACK authentication, 234
 credit cards, 7, 25
 CRLs (Certificate Revocation Lists)
 configuring, 241–244
 distribution points, 78
 expired certificate ACLs, 613–614
 overview, 76–78, 187, 598, 602, 832
 revoking/updating, 635
 Crypto Access Check on Clear-Text Packets
 feature, 923
 crypto ACLs
 overview, 644–645
 protecting traffic, 834–835
 troubleshooting, 906–907
 crypto maps
 activating, 839
 building, 835
 DN-based, 664–665
 dynamic, 838–839
 activating, 657–658
 configuring TED, 660–662
 creating, 656–657
 example, 658–659
 overview, 655–656
 Easy VPN Server, 740–742
 groups, 740–742
 IPsec profiles, 683
 show commands, 652–653
 static, 835–837
 activating, 652
 configuring, 653–655
 entries, 648
 not using ISAKMP/IKE, 650–652
 overview, 647
 using ISAKMP/IKE, 648–650
 viewing, 652–653
 TED, 660–662
 viewing, 652–653
 CSD (Cisco Secure Desktop)
 antivirus packages, 307
 backing up/restoring, 320
 configuring
 cache cleaner, Mac/Linux, 318
 upload/download settings, 318
 for Windows, 308–313
 enabling, 319–320

firewalls, 308
 installing on concentrators, 308
 overview, 169, 188, 270, 307
 saving settings, 319–320
 using, 320
 CSM (Content Switching Module), 579
 custom queuing (CQ), 577

D

data access sessions, IPsec
 ISAKMP/IKE Phase 2
 components, 116–117
 connection modes, 120
 data connections, 121–123
 security protocols, 117–120
 transforms, 121
 data connections
 IPsec, 96
 ISAKMP/IKE Phase 2, 121–123
 data delivery, PPTP, 132
 Data Encryption Standard
 See DES
 data SAs
 configuring, 932
 overview, 268–270
 wireless campuses, 945–946
 data transforms, troubleshooting, 906
 data transport, routers, 574–575
 data tunnels, 151
 Dead Peer Detection (DPD), 126, 586–587
 debug commands
 DPD, 587
 enrollment problems, 633
 ISAKMP/IKE Phase 1 connections
 L2L sessions, 775, 778–781
 remote access sessions, 781, 784–788
 ISAKMP/IKE Phase 2 connections
 incorrect peer address, 793
 matching on wrong crypto map, 793–794
 mismatched crypto ACLs, 792
 mismatched data transforms, 792
 overview, 790–792
 matching wrong crypto map, 908–909
 mismatched crypto ACLs, 906–907
 mismatched data transforms, 906
 overlapping crypto ACLs, 909

- stateful failover, 701
- troubleshooting
 - Easy VPN Remote, 753
 - ISAKMP/IKE Phase 1, 887–901
 - ISAKMP/IKE Phase 2, 901–909
 - SSO, 698
 - WebVPN, 768–769
- DefGroup parameters, 430
- DES (Data Encryption Standard), 51, 93
- device authentication, 22–23, 66–67
 - digital certificates
 - acquiring, 78
 - CAs, 70–71
 - CRLs, 76–78
 - file-based enrollment, 78–80
 - network-based enrollment, 80–82
 - overview, 69–70
 - PKCS, 72–73, 76
 - PKI, 71–72
 - SCEP, 76
 - standards, 70
 - using, 82–84
 - X.509 certificates, 74, 76
 - IPsec, 104–105
 - pre-shared asymmetric keys, 68–69
 - pre-shared symmetric keys, 67–68
 - remote access, 85
 - SSL, 167
- device-to-device connections, 28
- DH
 - concentrators, 186
 - device authentication, 104
 - key groups, 104, 732
 - PIX/ASA appliances, 812
- DHCP (Dynamic Host Configuration Protocol)
 - assigning addresses, 222, 224
 - DHCP relay feature, 186, 224
 - Easy VPN Remote, 749
 - L2TP, 145
 - network scope, 214
 - split tunneling, 112
 - VPN 3200, 533
- Dialup tab, 443
- Diffie-Hellman algorithm, 49, 61–64, 95
- digital certificates
 - acquiring
 - file-based enrollment, 78–80
 - network-based enrollment, 80–82
 - concentrators, 187
 - configuring
 - ACLs, 613
 - CBAC, 610–612
 - RA mode on servers, 636
 - CRLs, 76–78, 613–614
 - deleting, 603
 - Easy VPN Server, 735
 - enrolling
 - manually, 603–609
 - using SCEP, 595–603
 - expired certificate ACLs, 613–614
 - groups, 735
 - importing/exporting, 615–617
 - OCSF, 598
 - overview, 22, 69–70, 595
 - passwords, 634
 - PKCS, 72–73, 76
 - PKI, 71–72
 - RA configuration/operation, 636–637
 - removing CA services, 640–641
 - restoring CAs, 639–640
 - revoking ID certificates, 635–636
 - SCEP
 - deleting certificates, 603
 - downloading/authenticating certificates, 597–599
 - names/RSA key pairs, 597
 - overview, 76, 595–596
 - requesting router ID certificates, 600
 - saving CA/ID certificates, 601
 - verifying certificate operation, 601–602
 - verifying NVRAM fit, 596–597
 - serial numbers, 635
 - setting up RAs, 637
 - show commands, 601
 - SSL, 159
 - standards, 70
 - TFTP, 603–605
 - using, 82–84
 - WebVPN, 169
 - X.509 certificates, 74, 76
- digital signatures, 22, 48, 65, 68
- discovery process, MTU, 32
- Distinguished Name (DN)-based crypto maps, 664–666
- distribution points, CRL, 78
- DMVPNs (Dynamic Multipoint VPNs)

- configuring
 - hub configurations, 710–711
 - routing configurations, 713–714
 - spoke configurations, 712–713
- dual DMVPN with dual hubs, 924–927
- hub redundancy
 - dual DMVPN-dual hubs, 724–729
 - single DMVPN-dual hubs, 719–723
- overview, 575, 706–710
- using on hubs/spokes, 714–719
- DN (Distinguished Name)-based crypto maps, 664–666
- DNS
 - dynamic DNS, 187
 - groups, 213
 - server addresses, 493
 - spoofing, 811
 - static tables, 588
 - VPN 3002, 545
 - VPN Client, 485–486
 - WebVPN, 762–763
 - See also* split DNS
- DoS attacks, 923
 - SPI, 798
 - TCP versus IPsec, 165
- DPD (Dead Peer Detection), 126, 188, 486, 586–587
 - IPsec, 128, 441
- DSA certificates, IKE, 233
- DSA keys, 49
- dynamic crypto maps
 - groups, 740–741
 - ISAKMP/IKE profiles, 758
 - overview, 835–839
 - show commands, 657
- dynamic DNS, 187
- Dynamic DNS feature, VPN Client, 425
- dynamic IP routing protocols, 114
- Dynamic Multipoint VPNs (DMVPNs)
 - See* DMVPNs
- dynamic NAT, 345
- dynamic PAT, 345

E

- EAP (Extensible Authentication Protocol), 131
- EAPoUDP in/out filtering, 274

- Easy VPN
 - ACLs, 188
 - authentication, 185, 188
 - AYT feature, 185
 - backup peers, 188
 - backup server feature, 187
 - bandwidth management feature, 186
 - components, 177
 - concentrators
 - features, 184–189
 - models, 177–182
 - modules, 182–183
 - CRLs, 187
 - CSACS, 188
 - CSD, 189
 - DH group 5, 186
 - DHCP Intercept feature, 186
 - DHCP relay feature, 186
 - digital certificates, 187
 - DPD, 188
 - dynamic DNS, 187
 - encryption, 186
 - filtering, 187
 - firewalls, 188
 - IPsec over TCP, 186
 - L2TP over IPsec, 187
 - MTUs, 187
 - NAT-T, 186
 - network extension mode, 186
 - overview, 100, 177
 - PIX/ASA appliances, 809, 812
 - redirection messages, 373
 - RRI, 186
 - SCEP, 186
 - SCP, 187
 - split DNS, 187
 - SSL VPN, 188
 - statistics, 186
 - WebVPN, 188
 - XML, 186
- Easy VPN Remote
 - certificate enrollment, 940–941
 - concentrators, configuring
 - AAA, 934
 - accessing via web browsers, 930
 - basic administration, 930
 - basic group configuration, 934–935
 - certificate enrollment, 931

- CLI Quick Configuration, 928
- data SAs, 932
- default routes, 929–930
- filters, 932–933
- IP addressing, 928–929
- ISAKMP/IKE, 931–932
- rules, 932–933
- specific hardware client group configuration, 935
- specific software client group configuration, 936–937
- VCA, 937–938
- VPN-on-a-stick, 932–933
- configuring, 748
 - connecting to Easy VPN Server, 750–751
 - DHCP server pool, 749
 - example, 753–754
 - FOS 6.x, 856–862
 - Quick Configuration, 939–940
 - remote access user, 942
 - user authentication, 751–752
 - verifying configuration, 749–753, 859–861
- connection modes, 746–750
- connection profile, 750
- device authentication, 941
- disadvantages, 748
- groups, 750
- NAT/PAT, 747–748
- NAT-T, 748
- overview, 746, 928
- routers, 746
- VPN 3002
 - accessing, 537–538, 564–565
 - administering, 564
 - authentication/connection options, 548–556
 - CLI, 538
 - client mode, 557
 - default configuration, 537–538
 - deploying, 535–537
 - features, 533–534
 - GUI, 538–548
 - hardware client option, 536–537
 - models, 534–535
 - network extension mode, 557–559
 - routing features, 562–563
 - RRI, 563
 - software client option, 536
 - upgrading, 565–569
- XAUTH, 737, 751–752
- Easy VPN Server
 - ACLs, 736
 - AH, 732
 - AI, 461
 - authentication, 851–852
 - AYT mode, 736
 - CAC, 737
 - certificate enrollment, 940–941
 - concentrators, configuring, 928
 - AAA, 934
 - accessing via web browsers, 930
 - basic administration, 930
 - basic group configuration, 934–935
 - certificate enrollment, 931
 - CLI Quick Configuration, 928
 - data SAs, 932
 - default routes, 929–930
 - filters, 932–933
 - IP addressing, 928–929
 - ISAKMP/IKE, 931–932
 - rules, 932–933
 - specific hardware client group configuration, 935
 - specific software client group configuration, 936–937
 - VCA, 937–938
 - VPN-on-a-stick, 932–933
 - configuring
 - AAA, defining, 733–734
 - address pools, 848–849
 - example, 743–746, 883–885
 - groups, 734–742, 849–851
 - Quick Configuration, 939–940
 - remote access users, 942
 - XAUTH, 851–852
 - crypto maps, 740–742
 - device authentication, 941
 - DH group 1, 732
 - digital certificates, 735
 - firewalls, 464
 - FOS 6.x, 847–855
 - FOS 7.0, 862–885
 - group policies, defining, 864–871

- IKE Mode Config, 853
- IPsec connections
 - configuration options, 452–455
 - connecting to Easy VPN Server, 453–455
 - connecting to VPNs, 455
 - creating connection profile shortcuts, 453
 - disconnecting, 459
 - notifications, 458–459
 - Routing Information tab, 458
 - setting connection profiles as default, 452–453
 - statistics, 456
 - status, 456–459
 - Tunnel Details tab, 456–457
 - using certificates, 444–452
 - using pre-shared keys, 438–443
- IPsec over TCP, 732
- IPsec over UDP, 732
- ISAKMP/IKE policies, 479
- load balancing, 880
- manual keying, 732
- NAT-T, 487, 732
- overview, 731–732, 928
- PFS, 732, 737
- remote access/L2L simultaneous support, 877–880
- restricting number of VPN sessions, 883
- routers, 732, 745–746
- RRI, 563, 741
- RSA encrypted nonces, 732
- split DNS, 735
- split tunneling, 464, 736
- transport mode, 732
- troubleshooting firewalls, 468
- tunnel groups, creating
 - L2L tunnel groups, 875
 - remote access general properties, 871–873
 - remote access IPsec properties, 873–875
- using multiple servers for remote access, 880–883
- using XAUTH, 876–877
- VPN 3000, 731
- VPN 3200, 534
- WINS, 736
- XAUTH, 741–742
- eavesdropping attacks, 5–7
- Echo-Reply messages, PPTP, 137
- Echo-Request messages, PPTP, 137
- e-mail
 - attacks, 811
 - SMTP servers, 399
 - WebVPN, 173, 289–291
- encapsulation, 23–24
 - IPsec, 252–254
 - IPsec over TCP, 34
 - IPsec over UDP, 34
 - L2TP, 148
 - NAT-T, 34
 - transport mode, 14
 - tunnel mode, 15
- encapsulation security payload/protocol
 - See* ESP
- encrypted connections, 60
- encrypted nonces
 - See* RSA encrypted nonces
- encryption, 7, 24, 49
 - AES, 52–53, 822
 - algorithms, 24, 50
 - asymmetric keys, 47
 - concentrators, 182, 186
 - DES/3DES, 51–52
 - Diffie-Hellman, 61–64
 - hardware, 814
 - key pairs, 591–595
 - L2L connections, 333
 - L2TP versus PPTP, 151
 - MPPE, 39
 - NULL, 95
 - PIX appliances, 813
 - PIX/ASA appliances, 812
 - PPTP, 132
 - pre-shared keys, 589
 - process, 50
 - RSA encrypted nonces, 68, 590–595
 - SEAL, 646
 - SEP modules, 182
 - SSH, 615
 - SSL, 160, 167
 - VAC, 814
 - VCA messages, 374
 - VTI feature, 684
 - WebVPN, 283
- enhanced routing, 573, 810
- entities, PPTP, 135
- enveloping, 76
- Error Lookup Tool, 482

- error messages, VPN Client, 454
- ESP (encapsulation security payload/protocol)
 - address translation, 124
 - AH, versus, 117
 - IPsec, 126
 - L2L connections, 333
 - overview, 34, 90–94, 119–120, 252
 - through NAT, 674–676
- Ethernet fragmentation, 490
- Event Logging feature, VPN Client, 425
- event logs, 393
 - classes/logging levels, 394–403
 - date/time, 393–394
 - filterable event logs, 406–408
 - live events, 404–406
 - VPN 3200, 548
- Event Viewer, 527–530
- exception lists, NAC, 272
- exportable certificates, 924
- exportable keys, 924
- Extensible Authentication Protocol
 - See* EAP
- external AAA, 220
- external authentication, 214–215
 - assigning addresses, 221–227
 - authentication/accounting servers, 217–220
 - configuring groups, 220–221
 - creating authentication servers, 215–217
- extranets, 20

F

- failover, 693–694
 - configuring, 696–705
 - FOS, 811
 - IPsec, 694–695
 - PIX/ASA appliances, 811
 - restrictions/limitations, 694
 - SSP, 694
- FEP (Front End Process), PPTP, 147
- FIFO (first-in, first-out) queuing, 577
- File Management option, 377
- filtering
 - concentrators, 187
 - EAPoUDP in/out filtering, 274
 - L2L sessions, 343–344
 - OSPF, 365
 - overview, 19, 161
 - software client groups, 936
- filters
 - firewalls, 266–267
 - groups, 213
 - overview, 932–933
- Finesse Operating System
 - See* FOS
- fingerprints
 - See* digital signatures
- Firewall Integration feature, VPN Client, 425
- firewall VPNs, 19
- firewalls, 19, 33–35
 - AYT mode, 465, 736
 - CIC, 261, 464–466
 - concentrators, 185–188
 - CPP filter, 465
 - CSD, 308
 - Easy VPN, 185
 - Easy VPN Server, 464
 - filters, 266–267
 - fragmentation, 800
 - IPsec, 126–128
 - IPsec over TCP, 254, 821
 - IPsec over UDP, 440
 - ISAKMP/IKE Phase 1, 260–267
 - L2TP, 151
 - NAT-T, 440
 - perimeter, 917–918
 - PIX/ASA appliances, 810
 - rules, 264–266
 - split tunneling, 112
 - stateful, 35, 464, 810–811
 - translation tables, 487
 - VPN Client
 - enabling, 465–466
 - troubleshooting, 468
 - verifying operation, 466–467
- first-in, first-out (FIFO) queuing, 577
- Flash memory, concentrators, 382
- flexibility, 16, 43
- FloodGuard, 166
- FOS (Finesse Operating System)
 - failover, 811
 - features, 812–813
 - firewalls, 810

- FOS 6.3 L2L example, 841–842
- FOS 7.0 L2L example, 843–845
- overview, 809, 817
- redundancy, 811
- upgrades, 811
- FOS 7.0
 - Easy VPN Server configuration, 883–885
 - remote access/L2L simultaneous support, 877–880
 - restricting number of VPN sessions, 883
 - using multiple servers for remote access, 880–883
- fragmentation
 - attacks, 811
 - concerns, 799–800
 - discovery, 801
 - Ethernet, 490
 - firewalls, 800
 - investigating problems, 489–491
 - overview, 31–32, 487, 798–799
 - PPTP, 142–143
 - problems created, 488
 - solutions, 491–492
 - throughput, 488, 800
 - troubleshooting
 - PMTUD, 803–805
 - static MTU setting, 802
 - TCP MSS, 803
- Front End Process (FEP), 147
- fully meshed VPNs, 29
- functions, 12

G

- gateways, 15
 - SSL, 163–164
 - VPN, 455
 - WebVPN, 765
 - Windows, 521
- global groups, 208–209
- GoToMyPC, 811
- GRE (Generic Route Encapsulation) tunneling
 - configuring, 678–679
 - OSPF, 679–681, 683
 - overview, 37–38, 135, 677–678, 924
 - PMTUD, 805
 - PPTP, 140
- group keying, 244
- groups
 - access hours, 212
 - AYT mode, 737
 - certificates, 244–247
 - configuring, 518–520
 - certificate group matching parameters, 244–247
 - hardware clients, 935
 - software clients, 936–937
 - connect time, 213
 - DHCP network scope, 214
 - digital certificates, 735
 - DNS, 213
 - dynamic crypto maps, 740–741
 - Easy VPN Remote, 750
 - Easy VPN Server
 - dynamic crypto map entries, creating, 740–741
 - CAC for IKE, implementing, 738–740
 - monitoring groups, 742
 - static crypto map entries, creating, 741–742
 - external authentication
 - assigning addresses, 221–227
 - authentication/accounting servers, 217–220
 - configuring groups, 220–221
 - creating authentication servers, 215–217
 - filters, 213
 - idle timeouts, 213
 - IPsec tab, 248–250
 - keying, 244
 - lock feature, 738
 - passwords, 212
 - policies, defining
 - attribute configuration, 866–871
 - default, 864–865
 - locations, 864
 - PPTP/L2TP, 278–279
 - pre-shared keys, 105, 518, 735
 - remote access
 - controlling access to concentrators, 207–227
 - ISAKMP/IKE profiles, 757–758
 - viewing, 742

- SEP modules, 213
- simultaneous logins, 212
- specific groups, 209
- static crypto maps, 741–742
- strip realm, 214
- tunnel groups
 - L2L tunnel groups, 875
 - overview, 214, 863
 - remote access general properties, 871–873
 - remote access IPsec properties, 873–875
- WebVPN, 297–298
 - ACLs, 302–303
 - content filter parameters, 301–302
 - group buttons, 303–304
 - WebVPN parameters, 299–301
 - WebVPN tab, 298–303
- WINS, 213
- wireless campuses, 947–949
- groups, keys, 62
- GUI Locking feature, 432

H

- hardware appliances, 177
- hardware clients, VPN 3002
 - accessing, 537–538, 564–565
 - administering, 564
 - authentication/connection options, 548–556
 - CLI, 538
 - default configuration, 537–538
 - deploying, 535–537
 - features, 533–534
 - GUI, 538–548
 - hardware client option, 536–537
 - models, 534–535
 - routing features, 562–563
 - RRI, 563
 - software client option, 536
 - upgrading, 565–569
- Hashing Message Authentication Codes
 - See* HMAC
- Hello messages, L2TP, 150
- hex dumps, 403
- hidden communication, 16

- high availability, concentrators, 184
- HMAC (Hashing Message Authentication Codes)
 - MD5, 55
 - overview 53–54, 93
 - sending signatures via translation devices, 58
 - SHA, 55
 - sharing secret keys, 58
 - VPN implementations, 59
- hold-down routes, 338
- host names, 588
- Hot Standby Router Protocol (HSRP)
 - RRI, 687–693
- hours, access, 212
- HSRP (Hot Standby Router Protocol), 687–693
- HTTP concentrators, 382
- HTTP/HTTPS proxy service, WebVPN, 285–286
- HTTPS
 - administrators, 380
 - WebVPN, 282–284, 381, 765
- hub-and-spoke redundancy, 36

- ICMP echoes, 377
- ICV (Integrity Checksum Value), 54, 119
- IDEA (International Data Encryption Algorithm), 51
- identity
 - certificates, 72, 236–241, 247
 - router types, 587–588
- idle timeouts, groups, 213
- IE Proxy feature, 255–256
- IETF (Internet Engineering Task Force), 89
- IKE (Internet Key Exchange) protocol, 49
 - authentication problems, 413–416
 - data connections, 121–123
 - ISAKMP/IKE Phase 1, 100–116
 - ISAKMP/IKE Phase 2, 116–123
 - keepalives, 248
 - overview, 49, 90–95
 - peer descriptions, viewing, 795–796
 - policy mismatch, 411
 - proposals, 230–234, 516–517
 - transforms, 102–104, 121
 - transport mode, 120
 - tunnel mode, 120
- IKE Client Configuration
 - client addressing, 108–109

- client connection types, 109–111
 - firewalls, 112
 - split DNS, 113–114
 - split tunneling, 111–112
- IKE Mode Configuration
 - client addressing, 108–109
 - client connection types, 109–111
 - Easy VPN Server, 853
 - firewalls, 112
 - overview, 100, 107
 - split DNS, 113–114
 - split tunneling, 111–112
- image files, VPN Client, 435
- IMAP, 291
- Incoming-Call-Connected messages, PPTP, 138
- Incoming-Call-Reply messages, PPTP, 138
- Incoming-Call-Request messages, PPTP, 138
- Individual Unit Authentication, 551–552
- Individual User Authentication, 185
- initial contact feature, 128–129
- InstallPath parameters, 430
- Instant Messenger, 811
- integrity
 - data, 90
 - message, 167
 - overview, 8, 38
 - packet, 24
- Integrity Checksum Value (ICV), 54, 119
- Interactive Unit Authentication, 185, 551
- inter-chassis redundancy
 - VCA, 371–376
 - VRRP, 366–371
- interfaces
 - bandwidth policies, 355–356
 - OSPF, 364
 - VPN Client, 435
- internal authentication, 227–229
- International Data Encryption Algorithm (IDEA), 51
- Internet Engineering Task Force (IETF), 89
- Internet Key Exchange protocol
 - See* IKE
- Internet remote access
 - certificate enrollment, 940–941
 - concentrators, 928
 - device authentication, 941
 - Quick Configuration, 939–940
 - remote access user configuration, 942
 - wireless users, 951–952
- Internet Security Association and Key Management Protocol
 - See* ISAKMP
- Internet VPNs, 21
- intra-chassis redundancy, 366
- intranets, 20
- invalid security parameter index (SPI) feature, 797–798
- IP address identity types, 588
- IP headers, 799
- IP RTP prioritization, 577
- IP Security Monitor, 525–526
- IPsec
 - 3DES, 93
 - address translation
 - ESP through NAT, 674–676
 - issues, 124
 - NAT, 673–674
 - overview, 124, 673
 - solutions, 124–125
 - AES, 93
 - AH, 117–119
 - allowing IPsec traffic, 582–583, 818–820
 - automatic initiation
 - using, 464
 - verifying configuration, 463
 - VPN Client GUI, 464
 - vpnclient.ini file, 461–463
 - backup server feature, 185
 - CAC, 737
 - Client FW tab, 260–267
 - concentrators, 200
 - connections
 - building sessions, 99–100
 - SAs, 97
 - setting up, 97–98
 - data encapsulation, 252–254
 - data SAs, 268–270, 668
 - DES, 93
 - device authentication
 - certificates, 235–247
 - components, 235
 - configuring, 823–833
 - pre-shared keys, 235
 - device interactions, 94
 - DPD, 128, 441, 586–587
 - ESP, 119–120, 126
 - ESP versus AH, 117

- filtering IPsec traffic, 670–673
- firewalls, 112, 126–128
- gathering information, 581–582
- HMAC, 93
- IE Proxy feature, 255–256
- IKE protocol, 95, 230–234
- initial contact feature, 128–129
- invalid SPI conditions, 797
- IPsec tab, 247–250
- ISAKMP, setting up, 94, 820–822
- ISAKMP/IKE Phase 1
 - device authentication, 104–105
 - key exchange, 104
 - management connection, 101–104
 - remote access steps, 105–116
- ISAKMP/IKE Phase 2
 - activating crypto maps, 839
 - building crypto maps, 835–839
 - data connection management commands, 839–840
 - defining how to protect traffic, 834–835
 - specifying traffic to protect, 834
- L2L connections, 344, 840–845
- L2TP, 145, 147
- limitations, 574–575
- migrating to IPsec-based design, 669–670
- Mode/Client Configuration tab, 251–259
- NAC, 270–274
- NAT/PAT, 124
- NAT-T, 583
- non-unicast traffic, 677–683
- notifications, 458–459
- Oakley protocol, 95
- overview, 38–39, 89, 147, 163, 229–230
- Passive Mode feature, 669
- PIX/ASA appliances, 812
- policies, configuring, 822–823
- pre-shared keys, 588
- profiles, 683–684
- redirection messages, 373
- redundancy
 - HSRP with RRI, 687–693
 - stateful failover, 693–705
- remote access/L2L sessions same router, 755–761
- RFCs, 91–95
- RRI, 100
- SAs, 94, 97, 248, 517, 646
- SHA-1, 93
- simplifying configurations, 683–687
- SKEME protocol, 95
- split DNS, 113–114, 258–259
- split tunneling, 111–112, 256–258
- SSL, versus, 157, 166
- standards, 89–92
- stateful firewalls
 - ESP through NAT, 674–676
 - NAT, 673–674
- troubleshooting, 794–798
- tunneling
 - IPsec over TCP, 254
 - IPsec over UDP, 253
 - NAT-T, 254
 - network extension mode, 559–561
 - overview, 148, 252–253, 752–753
 - VPN 3200, 553–555
- VPN 3200, 534, 544, 549
- VPN Client
 - configuration options, 452–455
 - connecting to Easy VPN Server, 453–455
 - connecting to VPN gateways, 455
 - connection status, 456–459
 - creating connection profile shortcuts, 453
 - disconnecting, 459
 - notifications, 458–459
 - Routing Information tab, 458
 - setting connection profiles as default, 452–453
 - statistics, 456
 - Tunnel Details tab, 456–457
 - using certificates, 444–452
 - using pre-shared keys, 438–443
- VTI feature, 684–687
- IPsec over TCP
 - concentrators, 186
 - Easy VPN, 186
 - Easy VPN Server, 732
 - firewalls, 821
 - overview, 34, 125–126, 253–254, 821
 - VPN Client, 425
- IPsec over UDP
 - Easy VPN Server, 732
 - firewalls, 440
 - overview, 34, 125, 252–253
 - VPN Client, 425
- IPsec Passive Mode feature, 669

- ipseccmd command, 526–527
- ISAKMP (Internet Security Association and Key Management Protocol)
 - data connections, 121–123
 - overview, 90, 94
 - policies, 923
 - transforms, 102–104, 121
 - transport mode, 120
 - tunnel mode, 120
- ISAKMP/IKE
 - configuring, 931–932
 - crypto maps, 758
 - data connection, 833
 - activating crypto maps, 839
 - building crypto maps, 835–839
 - data connection management commands, 839–840
 - defining how to protect traffic, 834–835
 - specifying traffic to protect, 834
 - firewalls, 260–267
 - IKE policies, 326–327
 - management connection
 - allowing IPsec traffic, 818–820
 - configuring device authentication, 823–833
 - configuring policies, 822–823
 - data SAs, 268–270
 - dynamic crypto maps, 655–662
 - managing IPsec data SAs, 668
 - managing/viewing connections, 666–668
 - mismatched protected traffic, 418
 - mismatched transform sets, 417–418
 - setting up ISAKMP, 820–822
 - troubleshooting, 417–418, 901–909
 - viewing IPsec data SAs, 667
 - overview, 325
 - policy mismatches, 479–480
 - port 500, 675
 - profiles, 756–757
 - remote access profiles, 757–758
 - transforms, 326
 - wireless campuses, 945
- ISAKMP/IKE Phase 1
 - Client FW tab, 260–267
 - connections
 - commands, 774
 - debug crypto engine command, 786–788
 - debug crypto isakmp command, 775, 778–785
 - debug crypto pki command, 785
 - management, 101–104, 618–620, 817–833
 - show crypto isakmp sa command, 774
 - device authentication, 104–105, 235–247, 587–617
 - digital certificates/router enrollment, 595–617
 - DPD, enabling, 586–587
 - IE Proxy feature, 255–256
 - IKE proposals, 230–234
 - IPsec tab, 247–250
 - ISAKMP, enabling, 583
 - key exchange, 104
 - Mode/Client Config tab, 251–254
 - negotiating policies with peers, 585–586
 - policies
 - commands, 584–585
 - creating, 583–585
 - default, 584–585
 - pre-shared keys, 588–595
 - remote access steps, 105–116
 - router identity types, 587–588
 - routers as CAs, 620–641
 - SAs, 739
 - split DNS, 258–259
 - split tunneling, 256–258
 - troubleshooting, 411, 413, 415–417, 530, 887–899
- ISAKMP/IKE Phase 2
 - building
 - DN-based crypto maps, 664–666
 - dynamic crypto maps, 655–662
 - managing IPsec data SAs, 668
 - managing/viewing connections, 666–668
 - viewing IPsec data SAs, 667
 - components, 116–117
 - configuring
 - crypto ACLs, 644–645
 - crypto protection methods, 645–647
 - defining protected traffic, 644–645
 - DN-based crypto maps, 664–666
 - dynamic crypto maps, 655–662

- static crypto maps, 647–655
- transform sets, 645–647
- connections
 - commands, 788
 - data connections, 121–123
 - debug crypto ipsec command, 790–794
 - modes, 120
 - show crypto engine active command, 788–789
 - show crypto ipsec sa command, 789–790
- security protocols, 117–120
- transforms, 121
- isp account, 378

J–K

- jitter, 576
- KaZaA, 811
- KEA (Key Exchange Algorithm), 49
- keepalives
 - IKE, 248
 - PPTP, 137
 - See also* DPD
- Key Distribution Center, Kerberos, 92
- Key Exchange Algorithm (KEA), 49
- keyrings, 756
- keys
 - asymmetric, 46–49
 - authentication, 67
 - auto-archiving, 628–629
 - autoenrollment, 608
 - caller ID value, 139
 - CAs, 597–599
 - Diffie-Hellman algorithm, 49, 61–64
 - DSA, 49
 - Easy VPN Server, 732
 - exchanging keys
 - asymmetric keying algorithm, 61
 - encrypted connections, 60
 - IPsec, 104
 - limitations, 65
 - overview, 60, 104
 - pre-sharing, 60
 - exportable keys, 924

- key groups, 62, 104, 244
- management, 24–25
- overview, 45, 591–593
- PIX/ASA appliances, 812
- pre-shared keys
 - configuring, 588–589
 - overview, 67–69
 - protecting, 589–590
 - RSA encrypted nonces, 590–595
 - viewing, 590
- refreshing, 64
- RSA
 - backing up RSA information, 617
 - exportable key pairs, creating, 615
 - exporting key pairs, 616–617
 - importing key pairs, 617
 - public keys, configuring, 593–594
 - removing RSA keys, 594–595
 - using key pairs for certificate, 616
- secret, 104
- sharing, 58–61, 65
- SSH, 615
- symmetric, 46
- WebVPN, 763

L

- L2F (Layer-2 Forwarding), 39
- L2L (LAN-to-LAN) connections
 - adding
 - certificates, 332–333
 - completing, 342–343
 - configuration parameters, 328–331
 - connection policies, 333–335
 - device authentication, 332–333
 - filtering, 344
 - groups, 344
 - IPsec SAs, 344
 - local/remote networks, 341–342
 - modifying, 344
 - overview, 327–328
 - peer connectivity, 331–332
 - private addresses, 331–332
 - routing options, 335–341
 - address translation
 - ESP through NAT, 674–676

- NAT, 673–674
 - overview, 344–349, 673
- bandwidth
 - aggregation, 359
 - policies, 354, 358–359
 - reservations, 358
- connectivity example, 323–324, 840–845
- filtering IPsec traffic, 670–673
- hold-down routes, 338
- IKE policies, 326–327
- IPsec redundancy
 - HSRP with RRI, 687–693
 - stateful failover, 693–705
- ISAKMP/IKE Phase 2 configuration, 643
 - building dynamic crypto maps, 655–662
 - building static crypto maps, 647–653
 - configuring static crypto maps, 653, 655
 - crypto ACLs, 644–645
 - crypto protection methods, 645–647
 - defining protected traffic, 644–645
 - DN-based crypto maps, 664–666
 - dynamic crypto maps, 655–662
 - managing IPsec data SAs, 668
 - managing/viewing connections, 666–668
 - static crypto maps, 647–653, 655
 - transform sets, 645–647
 - viewing IPsec data SAs, 667
- migrating to IPsec-based design, 669–670
- NAT, 345–349
- NAT-T, 334–335
- network extension mode, 558
- non-unicast traffic, 677–683
- overlapping addresses, 346
- overview, 16, 323
- platforms, 325
- redundancy, 337
- restrictions, 324
- routers, 325
- scalability
 - configuring DMVPNs, 710–714
 - DMVPNs, 706–707
 - DMVPNs and hub redundancy, 719–729
 - non-DMVPN network, 707–710
 - using DMVPNs on hubs/spokes, 714–719
- sessions
 - IPsec, 755–761
 - ISAKMP/IKE Phase 1 debug commands, 775–781
 - Phase 2 data connections, 833–839
 - PIX/ASA appliances, 809–810
 - router deployment, 573–574
 - troubleshooting, 890–894
 - setting up, 325
 - simplifying configurations, 683–687
 - stateful firewalls, 673–676
 - tunnel groups, 875
- L2TP (Layer 2 Tunnel Protocol)
 - address translation, 151
 - authentication, 145
 - configuring groups, 278–279
 - control messages, 149–150
 - DHCP, 145
 - encapsulation, 148
 - firewalls, 151
 - global configuration, 280–281
 - IPsec, 145–148
 - NAC, 270
 - operation, 146
 - overview, 39–40, 131, 144–146, 277
 - PPTP, versus, 151–152
 - tunnels, 147–151
 - UDP, 149
 - Windows, 506–507
- L2TP Access Concentrator (LAC), 147
- L2TP Network Server (LNS), 147
- L2TP over IPsec, 187
- LAC (L2TP Access Concentrator), 147
- LAN extension mode, IPsec, 110–111
- LAN-to-LAN connections
 - See* L2L connections
- LAN-to-LAN NAT, 345–349
- Layer-2 Forwarding (L2F), 39
- Layer-2 Tunneling Protocol
 - See* L2TP
- LCP (Link Control Protocol), 133
- LEAP, 553
- Link Control Protocol (LCP), 133
- link establishment, PPTP, 133
- LNS (L2TP Network Server), 147
- load balancing
 - ASA, 881
 - concentrators, 181
 - Easy VPN Server, 880
 - failover, 811
 - FOS 7.0, 880

- VCA, 376
- VPN 3200, 534
- logging
 - classes, 394–395
 - configuring classes, 400–403
 - configuring e-mail, 399
 - configuring SNMP server for traps, 398–399
 - configuring syslog server, 399
 - default configuration, 395–397
 - event classes, 394–403
 - FTP backup, 398
 - filterable event logs, 406–408
 - live events, 404–406
 - Oakley logging, 530
 - VPN Client, 475
 - clearing logging information, 478
 - disabling logging, 477
 - formatting event information, 475–477
 - logging classes, 476
 - searching for logging information, 477–478
- logos, WebVPN, 288–289, 766
- Lotus Notes, 158
- LZS compression, 249

M

- magic cookies, 136
- main mode, IPsec, 101–102
- management connection, IPsec
 - aggressive mode, 102
 - main mode, 101–102
 - overview, 96, 101
 - transforms, 102–104
- management messages, PPTP, 136
- management protocols, administrators, 380–381
- man-in-the-middle attacks, 8–11, 65–66
- mapping, 33, 878–880
- masquerading attacks, 7–8
- Maximum Segment Size (MSS), 803
- maximum transmission unit
 - See* MTU
- MD5 (Message Digest 5), 55
- media translation, 575
- message integrity, SSL versus IPsec, 167
- message replay attacks, 165
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 134
- Microsoft Point-to-Point Encryption (MPPE) protocol, 39, 132
- mis account, 378
- MMC (Microsoft Management Console), 526
- modes
 - aggressive, 102
 - client, 109, 557
 - LAN extension, 110–111
 - main, 101–102
 - network extension mode, 186, 557–561
 - overview, 12–13
 - quick, 116
 - transport, 13–14, 92, 120
 - tunnel, 14–16, 92, 120
 - VPN 3200, 534, 545, 556
 - VPN Client, 435–438
- modules, concentrators, 182–183
- Monitoring Refresh option, 377
- Monitoring screens, 385–386
 - Sessions
 - encryption, 392
 - LAN-to-LAN Sessions table, 389–390
 - Management Sessions table, 391
 - Protocols, 392
 - Remote Access Sessions table, 391
 - Session Summary table, 388–389
 - Top Ten Lists, 392
 - statistics, 409–410
 - System Status, 386–387
- MPLS (Multi-Protocol Label Switching), 40
- MPPE (Microsoft Point-to-Point Encryption) protocol, 39, 132
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 134
- MSS (Maximum Segment Size), 803
- MTU (maximum transmission unit), 32, 534
 - fragmentation discovery, 801
 - hard-coding, 491–492
 - Network Monitor program, 490
 - ping program, 490
 - routers, 802
 - SetMTU program, 492
- MTU Sizing feature, VPN Client, 426
- MTUAdjustmentOverride parameters, 430

multicasting, 362
 multipoint mode, 926
 Multi-Protocol Label Switching (MPLS), 40
 mutual group authentication, 22, 86, 452

N

NAC (Network Access Control), 270
 AAA, 272–273
 exception lists, 272
 global configuration, 270–271
 group configuration, 272–274
 PIX/ASA appliances, 812
 RADIUS servers, 272–273
 NAD (Network Autodiscovery), 340–341
 NAT (Network Address Translation)
 AH incompatibility, 119
 dynamic, 345
 Easy VPN Remote, 747–748
 ESP through, 674–676
 IPsec, 124
 keepalives, 674
 overview, 33, 673–674
 PPTP, 143
 show commands, 674
 SSL, 165
 static NAT, 345
 VCA, 375
 NAT-T (NAT transversal/traversal)
 concentrators, 186, 487
 Easy VPN Remote, 748
 Easy VPN Server, 487, 732
 firewalls, 440
 IPsec, 583
 L2L connections, 334–335
 overview, 34, 125, 253–254, 673–674, 821, 837
 PIX appliances, 812
 VPN Client, 426
 NBAR (network-based application recognition), 577
 netstat program, 489
 Network Access Control (NAC)
 exception lists, 272
 global configuration, 270–271
 group configuration, 272–274
 Network Address Translation
 See NAT
 Network Autodiscovery (NAD), 340–341

network client implementation, SSL, 156
 network extension mode
 configuring, 558–559
 Easy VPN Remote, 747–748
 IPsec tunnels, 559–561
 L2L sessions, 558
 overview, 186
 verifying, 559–561
 VPN 3200, 545, 557–558
 network lists, 257–258
 Network Monitor program, 490
 Network Neighborhood, troubleshooting, 493–494
 network scope, DHCP, 214
 Network Time Protocol (NTP), configuring, 394
 network-based application recognition (NBAR), 577
 network-to-network connections, 28
 new_update_config.ini file, 471–472
 next header field, AH, 118
 nonces, 68
 See also RSA encrypted nonces
 non-repudiation, 25
 notifications, VPN Client, 458–459
 nslookup program, 486
 NTP (Network Time Protocol)
 3002 concentrators, 941
 configuring, 394
 overview, 923
 NULL encryption, 95
 NVRAM, 596–597

O

Oakley protocol, 95
 OCSF (Online Certificate Status Protocol), 78
 oem.ini file, VPN Client, 428–431
 on-demand mode, DPD, 586
 one-time passwords, 6, 23, 86
 Online Certificate Status Protocol (OCSP), 78, 598
 ORCA editor, 431
 OSPF, 363, 926
 authentication, 365
 configuring, 363–364
 filtering, 365
 GRE tunneling, 679–683
 interfaces, 364–365
 IP Routing screen, 363–364
 PIX/ASA appliances, 812

- RRI, 365
- spoke routers, 714
- Outgoing-Call-Reply messages
 - L2TP, 150
 - PPTP, 138
- Outgoing-Call-Request messages
 - L2TP, 150
 - PPTP, 138
- overloading addresses, 33

P

-
- PAC (PPTP Access Concentrator), 134
 - packets
 - authentication, 24, 53–59
 - integrity, 8, 24, 45
 - replay attacks, 92
 - spoofing, 24
 - PAP (Password Authentication Protocol), 133
 - PAR (port address redirection), 334
 - partially meshed VPNs, 29–30
 - Passive Mode feature, IPsec, 669
 - passwords, 23
 - certificates, 451, 634
 - Easy VPN, 737
 - groups, 212
 - Interactive UA, 551
 - one-time, 6, 23, 86
 - recovery, 193–194
 - SSL, 159
 - VPN 3200, 546
 - XAUTH, 742
 - PAT (port address translation)
 - address translation problems, 487
 - AH incompatibility, 119
 - dynamic, 345
 - Easy VPN Remote, 747–748
 - IPsec, 124
 - overview, 33
 - PPTP, 143
 - SSL, 165
 - Path MTU (PMTU), 491–492
 - Path MTU discovery (PMTUD), 32, 803–805
 - payload length field, AH, 118
 - pcf files
 - IPsec, 443
 - VPN Client, 432–435
 - Peer Certificate feature, VPN Client, 426
 - peers
 - authentication, 90
 - digital certificates, 595
 - CBAC, 610–612
 - CRLs, 613–614
 - enrolling manually, 603–609
 - enrolling using SCEP, 595–603
 - expired certificate ACLs, 613–614
 - importing/exporting, 615–617
 - DPD, 586–587
 - identity validation, IPsec, 248
 - ISAKMP/IKE Phase 1, 585–586
 - pre-shared keys, 588
 - RSA encrypted nonces
 - configuring public keys, 593–594
 - generating key pairs, 591–592
 - generating multiple key pairs, 592–593
 - removing RSA keys, 594–595
 - Perfect Forward Secrecy (PFS), 95, 737
 - perimeter routers, configuring, 920–924
 - periodic mode, DPD, 586
 - perimeter firewalls, 917–918
 - PFS (Perfect Forward Secrecy), 95, 737
 - Easy VPN Server, 732, 737
 - Ping option, 377
 - ping program, 490, 801
 - PIX appliances
 - address translations, 810
 - certificates, 812
 - connections
 - ISAKMP/IKE Phase 1 commands, 887–888
 - ISAKMP/IKE Phase 2 commands, 901–909
 - deployment scenarios, 809
 - L2L connections, 809–810
 - remote access connections, 809–810
 - special capabilities, 810
 - Easy VPN, 812
 - encryption, 812–813
 - features, 812–813
 - models, 813–814

- OSPF, 812
- overview, 325
- QoS, 813
- redundancy, 811
- RRI, 812
- RSA algorithm, 812
- stateful firewall services, 810–811
- PIX Firewall
 - FOS, 817
 - FOS 6.x
 - Easy VPN Remote, configuring, 856–862
 - Easy VPN Server, configuring, 847–855
 - FOS 7.0
 - configuring Easy VPN Server, 862–877, 883–885
 - troubleshooting Easy VPN Server, 877–883
 - IPsec traffic, allowing, 818–820
 - ISAKMP/IKE Phase 2
 - activating crypto maps, 839
 - building crypto maps, 835–839
 - data connection management commands, 839–840
 - defining how to protect traffic, 834–835
 - specifying traffic to protect, 834
 - L2L connection examples, 840–845
 - overview, 537, 917–918
 - transform sets, 835
- PKCS (Public Key Cryptography Standards)
 - overview, 72
 - PKCS #3, 62
 - PKCS #7, 76
 - PKCS #10, 72–74, 237, 444–445
- PKI (Public Key Infrastructure), 71–72
- PMTU (Path MTU), 491–492
- PMTUD (Path MTU discovery), 32, 803–805
- PNS (PPTP Network Server), 135
- point-to-point connections, 28
- Point-to-Point Protocol
 - See* PPP
- Point-to-Point Tunneling Protocol
 - See* PPTP
- policing
 - bandwidth, 352, 354–355
 - class-based, 577
- policy-based routing, 576
- pools, address, 225–227
- port 500, 675
- port address redirection (PAR), 334
- port address translation
 - See* PAT
- port forwarding, 158, 172, 294–297, 304, 768
- portal page URLs, WebVPN, 767–768
- Post Forwarding feature, WebVPN, 284
- PPoE, 533
- PPP (Point-to-Point Protocol)
 - CHAP, 133
 - overview, 39
 - payload, 143
 - phase 1, link establishment, 133
 - phase 2, user authentication, 133–134
 - phase 3, callback control, 134
 - phase 4, protocol negotiation, 134
- PPTP (Point-to-Point Tunneling Protocol)
 - address translation issues, 143–144
 - authentication, 131
 - call versus session, 138
 - client addressing, 132–134
 - components, 135
 - compression, 132
 - connection example, 141–142
 - control messages, 136–138
 - data delivery, 132
 - EAP, 131
 - encryption, 132
 - entities versus devices, 135
 - FEP, 147
 - fragmentation problems, 142–143
 - global configuration, 280
 - GRE protocol, 135, 140
 - groups, configuring, 278–279
 - L2TP, versus, 151–152
 - magic cookies, 136
 - management messages, 136
 - NAT, 143
 - operation
 - control connection, 136–138
 - tunnel connection, 138–141
 - overview, 39, 131, 277
 - PAC, 134
 - PAT, 143
 - PNS, 135
 - PPP, 133–134
 - security concerns, 143
 - servers, 135
 - TCP, 149

- tunnel packets, 140
- user authentication, 132
- PPTP Access Concentrator (PAC), 134
- PPTP Network Server (PNS), 135
- PQ (priority queuing), 576–577
- pre-shared keys
 - AES, 589
 - central office routers, 756
 - configuring, 588–589
 - device authentication, 824
 - encryption, 589
 - groups, 105, 518, 735, 738
 - IKE, 233
 - keyrings, 756
 - mismatches, 894
 - overview, 22, 60, 68–69, 235, 588
 - protecting, 589–590
 - RSA encrypted nonces, 590–595
 - show commands, 590
 - troubleshooting, 413, 415
 - viewing, 590
 - VPN Client, 438–443
 - Windows, 504
 - XAUTH, 589
- price, 43
- priority queuing (PQ), 576–577
- private addresses, 16
- proposals, IKE, 516–517
- protocol
 - analyzers, 6
 - support, 25
- proxy ARP, 27
- proxy, web browser, 171
- Public Key Cryptography Standards
 - See* PKCS
- Public Key Infrastructure (PKI), 71–72
- public keys, 593
 - See also* keys

Q

- QoS (quality of service)
 - bandwidth, 359
 - PIX/ASA appliances, 813
 - routers, 573–576
- query mode, 596
- queuing, 577

- Quick Configuration, VPN 3200
 - Admin screen, 546–547
 - DNS screen, 545
 - IPsec screen, 544
 - main GUI screen, 547–548
 - overview, 534, 539, 939–940
 - PAT screen, 545
 - Private Interface screen, 542
 - Public Interface screen, 543
 - Static Routes screen, 545–546
 - Time/Date screen, 540
 - Upload Configuration screen, 541
- quick mode, 116

R

- RADIUS servers
 - AAA, 220, 916
 - NAC, 272–273
 - overview, 217–220, 934
- random numbers, 68
- RAs, 636–637, 915–916
- RAS (remote access server), 132
- RC4, 51
- RC6, 51
- reachability, VPN 3200, 562–563
- Reboot parameters, 430
- Reboot Status option, 377
- rebooting, 377
- redirection messages, VCA, 373
- redistribution, 341
- redundancy, 35
 - chassis
 - VCA, 371–376
 - VRRP, 366–371
 - DMVPN and hub redundancy
 - dual DMVPN-dual hubs, 724–729
 - single DMVPN-dual hubs, 720–723
 - FOS, 811
 - hub-and-spoke design, 36
 - IPsec
 - HSRP with RRI, 687–693
 - stateful failover, 693–705
 - L2L sessions, 337
 - perimeter firewalls, 917–918
 - PIX/ASA appliances, 811

- static routing, 361
- VCA, 371, 937–938
- refreshing keys, 64
- registry, Windows, 506
- remote access
 - addressing, 26–27
 - bandwidth policies, 357–358
 - concentrators
 - assigning addresses, 221–227
 - configuring groups, 207–221
 - overview, 182–184
 - PPTP/L2TP, 277–281
 - user accounts, 227–229
 - WebVPN, 281–320
 - device authentication, 85
 - IPsec, 229–230
 - client addressing, 108–109
 - client connection types, 109–116
 - Client FW tab, 260–267
 - configuration example, 759–761
 - data SAs, 268–270
 - device authentication, 235–247
 - IKE Client/Mode Config, 107–114
 - IKE proposals, 230–234
 - IPsec tab, 247–250
 - Mode/Client Config tab, 251–259
 - overview, 99–100, 105–106
 - RRI, 114–116
 - SSL, versus, 157
 - user authentication, 106–116
 - XAUTH, 106–107
 - ISAKMP/IKE Phase 1 debug commands, 781–785
 - NAC
 - exception lists, 272
 - global configuration for IPsec, 270–271
 - group configuration, 272–274
 - PIX/ASA appliances, 809–810
 - PPTP, 131
 - redundancy, 371
 - router deployment, 573–574
 - troubleshooting, 895, 898–899
 - user authentication, 85–86
 - VCA, 371
 - VPNs, 17–18
- remote access server (RAS), 132
- repudiation, 25
- reservation, bandwidth, 352–354
- reserved field, AH, 118
- resolution, names, 485–486
- Reverse Route Injection (RRI), 27, 100, 687–693
- RFCs, IPsec, 91–95
- Rijndael algorithm, 52
- RIP, 361–362
- root certificates, 236–241, 247
- routers, 17
 - AYT mode, 736
 - blackhole, 489
 - CAs
 - backing up, 638–639
 - controlling certificate requests with passwords, 634
 - enabling, 625
 - enrollment requests, 631–635
 - parameters, defining, 629–631
 - protecting keys, 623–625
 - RA configuration/operation, 636–637
 - rejecting certificate requests, 634
 - removing CA services, 640–641
 - restoring CAs, 639–640
 - revoking ID certificates, 635–636
 - RSA key pairs, generating/exporting, 621–623
 - using auto-archiving, 628–629
 - using manual RSA keys, 625–627
 - viewing, 601
 - central office, 756–758
 - congestion avoidance, 577
 - deployment scenarios, 573–574
 - digital certificates
 - CBAC, 610–612
 - CRLs, 613–614
 - enrolling, 595–609
 - expired certificate ACLs, 613–614
 - importing/exporting, 615–617
 - Easy VPN Remote, 746
 - Easy VPN Server, 732, 745–746
 - identity types, 587–588
 - IOS, 537
 - IPsec sessions, 755–761
 - key pairs
 - configuring public keys, 593–594

- multiple, 591–593
 - removing RSA keys, 594–595
- L2L sessions, 325, 731
- locations, 578
- model comparisons, 577–579
- MTU size, 802
- perimeter routers, 916, 920–924
- PIX/ASA appliances, 810
- product comparisons, 579
- query mode, 597
- queuing, 577
- requesting router identity certificates, 600–601
- special capabilities
 - data transport, 574–575
 - media translation, 575
 - QoS, 575–576
 - routing scalability, 575
- throughput, 578
- VoIP, 576
- VPN sessions, 578
- WebVPN, 761–771

routing

- concentrators, 184, 359–361
- DMVPNs, 575
- enhanced, 573
- NAD, 340–341
- OSPF
 - configuring, 363–364
 - interfaces, 364–365
 - IP Routing screen, 363–364
- RIP, 361–362
- RRI, 336–339, 362
- scalability, 575
- static, 335–336

Routing Information tab, 458

routing protocol authentication, 56

routing tables

- NAD, 341
- VPN 3200, 548

RRI (Reverse Route Injection)

- concentrators, 186
- Easy VPN, 186
- Easy VPN Server, 563, 741
- HSRP, 687–693
- L2L sessions, 336–339
- OSPF, 365
- overview, 27, 100, 114–116, 362, 938, 950

- PIX/ASA appliances, 812
- VPN 3000 concentrator, 563

RSA encrypted nonces

- configuring public keys, 593–594
- Easy VPN Server, 732
- generating key pairs, 591–593
- overview, 68, 590–591
- removing RSA keys, 594–595

RSA keys

- IKE certificates, 233
- importing/exporting
 - backing up RSA information, 617
 - creating exportable key pairs, 615
 - exporting key pairs, 616–617
 - importing key pairs, 617
 - using key pairs for certificate, 616
- overview, 49
- RC6/RC4, 51
- removing, 594–595

RTP (IP) prioritization, 577

rules, 932–933

- firewalls, 264–266

S

SAs (security associations)

- data SAs
 - components, 121
 - managing, 668
 - negotiation, 122–123
 - overview, 268–270, 932
 - viewing, 667
- IPsec, 248, 517
- ISAKMP/IKE Phase 1, 739
- ISAKMP/IKE Phase 2, 121
- L2L sessions, 343
- non-unicast traffic, 677
- overview, 94, 97
- transforms, 646
- wireless campuses, 945–946

save password feature, 737

SAVELOG.TXT file, 382

scalability

- concentrators, 184
- DMVPNs, configuring
 - hub configurations, 710–711

- hub redundancy, 719–729
 - overview, 706–707
 - routing configurations, 713–714
 - spoke configurations, 712–713
 - using on hubs/spokes, 714–719
- L2L, 573
- non-DMVPN network, 707–710
- overview, 16, 43, 705–706
- Scalable Encryption Process (SEP) modules, 178
- SCEP (Simple Certificate Enrollment Protocol), 595–596
 - certificates, 239, 447–448
 - CAs, 609
 - deleting, 603
 - downloading/authenticating, 597–599
 - requesting router ID certificates, 600
 - saving CA/ID certificates, 601
 - verifying certificate operation, 601–602
 - concentrators, 186
 - Easy VPN, 186
 - enrollment requests, 633
 - names/RSA key pairs, 597
 - verifying NVRAM fit, 596–597
- SCP (Secure Copy), 187
- SDM (Security Device Manager), 573, 732
- SEAL, 646
- secret keys, 104
- Secure Copy (SCP), 187
- Secure Desktop browser, CDS, 317–318
- Secure Hashing Algorithm
 - See* SHA
- Secure Socket Layer
 - See* SSL
- Secure Socket Layer Services Module (SSLSM), 579
- security
 - AES, 234
 - AH, 118
 - Cisco PIX, 10
 - concentrators, 184
 - CSD, 189
 - firewalls, 19
 - FOS, 810
 - non-repudiation, 25
 - overview, 41–42
 - pcf files, 435
 - policies, 16, 501–506
 - PPTP, 143
 - SSL clients, 162–163
 - SSLSM, 579
 - WebVPN e-mail proxy, 291
- security appliances
 - ASA, 809–813, 817
 - data connection management commands, 839–840
 - device authentication, configuring, 823–833
 - FOS, 817
 - FOS 6.x
 - Easy VPN Remote, configuring, 856–862
 - Easy VPN Server, configuring, 847–855
 - FOS 7.0
 - configuring Easy VPN Server, configuring, 862–877, 883–885
 - troubleshooting Easy VPN Server, 877–883
 - IPsec traffic, allowing, 818–820
 - ISAKMP
 - setting up, 820–822
 - ISAKMP/IKE Phase 2, 833–839
 - L2L connection examples, 840–845
 - management connection policies, configuring, 822–823
 - overview, 917–918
 - PIX, 325, 809–813
 - troubleshooting
 - matching wrong crypto map, 908–909
 - mismatched crypto ACLs, 906–907
 - mismatched data transforms, 906
 - overlapping crypto ACLs, 909
 - overview, 887–888, 901–905
- security associations
 - See* SAs
- Security Device Manager (SDM), 573, 732
- security parameter index (SPI) field
 - AH, 118
 - ESP, 119
- SEP (Scalable Encryption Process) modules, 178
 - concentrators, 183
 - groups, 213
 - SEP-2 modules, 182
 - SEP-E modules, 182
- sequence numbers
 - AH, 118
 - TCP, 10
- serial numbers, certificates, 635

- session hijack attacks, 9
 - See also* man-in-the-middle attacks
- session replay attacks, 9
 - See also* man-in-the-middle attacks
- Set-Link-Info messages, L2TP, 150
- SetMTU program, 492
- SetMtuValue parameters, 430
- SHA (Secure Hashing Algorithm), 55
- SHA-1, 93
- sharing, keys
 - asymmetric keying algorithm, 61
 - encrypted connections, 60
 - limitations, 65
 - pre-sharing, 60
- show commands
 - CA certificates, 627
 - CAC for IKE configuration, verifying, 739–740
 - CAs, 601
 - CRLs, 602
 - crypto maps, 652–653, 657
 - DPD, 587
 - Easy VPN Remote configuration, verifying, 749, 752–753, 859–861
 - IKE peer descriptions, 795–796
 - IPsec data SAs, 667–668
 - ISAKMP/IKE Phase 1 connections, 618–619, 774, 887–889
 - ISAKMP/IKE Phase 2 connections, 788–790, 901–904
 - management connections, 618
 - NAT keepalive timer, 674
 - NVRAM use, 596
 - pre-shared keys, 590
 - public keys, 594
 - remote access groups, 742
 - router CA status, 631
 - RSA encrypted nonces, 592
 - RSA key pairs, 594
 - SSL certificates, 764
 - stateful failover, 700
 - transform sets, 647
 - WebVPN, 768–769
- sig.dat file, 471
- signatures, digital, 22, 48, 65, 68
- SilentMode parameters, 430
- Simple Certificate Enrollment Protocol
 - See* SCEP
- simple mode, VPN Client, 435, 437
- simultaneous logins, groups, 212
- site-to-site connections
 - adding
 - certificates, 332–333
 - completing, 342–343
 - configuration parameters, 328–331
 - connection policies, 333–335
 - device authentication, 332–333
 - filtering, 344
 - groups, 344
 - IPsec SAs, 344
 - local/remote networks, 341–342
 - modifying, 344
 - peer connectivity, 331–332
 - private addresses, 331–332
 - routing options, 335–341
 - address translation
 - creating rules, 346–348
 - enabling rules, 348–349
 - NAT, 673–676
 - overview, 344–346
 - concentrators, 182
 - connectivity example, 323–324
 - IKE policies, setting up, 326–327
 - IPsec
 - HSRP with RRI redundancy, 687–705
 - migrating to IPsec-based design, 669–670
 - overview, 99
 - traffic, filtering, 670–673
 - ISAKMP/IKE Phase 2 configuration
 - crypto ACLs, 644–645
 - crypto protection methods, 645–647
 - defining protected traffic, 644–645
 - DN-based crypto maps, 664–666
 - dynamic crypto maps, 655–662
 - managing IPsec data SAs, 668
 - managing/viewing connections, 666–668
 - static crypto maps, 647–655
 - transform sets, 645–647
 - viewing IPsec data SAs, 667
 - non-unicast traffic, 677–683
 - overview, 668–669
 - platforms, 325
 - routers, 325
 - scalability, 705–729
 - session restrictions, 324

- simplifying configurations
 - IPsec profiles, 683–684
 - VTI feature, 684–687
- stateful firewalls
 - ESP through NAT, 674–676
 - NAT, 673–674
 - VPNs, 16–17
 - See also* L2L connections
- SKEME protocol, 95
- SKIP, 92
- Skipjack, 51
- SNMP
 - administrator accounts, 378
 - e-mail servers, 399
- software clients, 536
- Software Update option, 377
- SPI (security parameter index) field
 - AH, 118
 - ESP, 119
- split DNS, 113–114, 187, 258–259, 426, 735
- split tunneling, 31, 111–112, 256, 919
 - Easy VPN Server, 464, 736
 - network lists, 257–258
 - options, 256–257
 - troubleshooting
 - connectivity problems, 483–485
 - name resolution problems, 485–486
 - VPN Client, 426
- spoofing
 - overview, 7, 24
 - PIX/ASA appliances, 811
- SSH (Secure Shell)
 - administrators, 380
 - RSA key pairs, 615
- SSL (Secure Socket Layer)
 - administrative rights, 157
 - advantages, 165
 - ASA appliances, 812
 - authentication, 159
 - CAs, 159
 - Cisco VPN implementation, 156
 - clients
 - implementations, 156–157
 - security, 161–163
 - web-/non-web-based applications, 161–162
 - components, 161
 - content control, 160–161
 - content filtering, 161
 - digital certificates, 159
 - disadvantages, 165
 - encryption, 160
 - features, 157–159
 - gateways, 163–164
 - HTTPS, 7
 - IPsec, versus, 157, 166
 - Java/ActiveX code, 161
 - NAT, 165
 - overview, 40–41, 155, 281
 - passwords, 159
 - PAT, 165
 - SSL VPN Client, 170
 - thin clients, 156
 - TLS, versus, 160
 - tokens, 159
 - usernames, 159
 - WebVPN, 283, 762–765
 - when to use, 164
- SSL VPN Client (SVC), 170, 188, 304
 - installing on concentrators, 304
 - nonadministrator users, 307
 - using, 305–306
- SSLSM (Secure Socket Layer Services Module), 579
- SSP (State Synchronization Protocol), 694
- standby commands, 690, 696
- Start-Control-Connection-Connected messages, L2TP, 150
- Start-Control-Connection-Reply messages
 - L2TP, 150
 - PPTP, 136
- Start-Control-Connection-Request messages
 - L2TP, 150
 - PPTP, 136
- stateful failover, 693–694
 - configuring
 - enabling, 699
 - HSRP, 696–697
 - managing/monitoring, 700–702
 - protecting SSO traffic, 699–700
 - RRI, 698–699
 - SSO, 697–698
 - tunneling, 700
 - IPsec deployment, 694–695
 - restrictions/limitations, 694
 - SSP, 694

- stateful firewalls, 127–128, 464
- static crypto maps
 - activating, 652
 - configuring, 653–655
 - entries, 648
 - groups, 741–742
 - not using ISAKMP/IKE, 650–652
 - overview, 647, 835–837
 - using ISAKMP/IKE, 648–650
 - viewing, 652–653
- static NAT, 345
- static routing
 - default route, 359–360
 - L2L sessions, 335–336
 - overview, 359–361
 - VPN 3002, 545–546
- Stop-Control-Connection-Notification messages, L2TP, 150
- Stop-Control-Connection-Request messages, PPTP, 137
- strip realm, groups, 214
- support, 42
- SVC (SSL VPN Client)
 - installing on concentrators, 304
 - nonadministrator users, 307
 - using, 304–306
- symmetric keys, 46, 588–589
- synchronization, VRRP, 369–371
- System Reboot option, 377

T

- tagging, 40
- tail dropping, 577
- TCP (Transmission Control Protocol)
 - DoS attacks, 165
 - flood attacks, 811
 - IPsec over TCP, 34
 - magic cookies, 136
 - sequence numbers, 10
- TCP Intercept, 166
- TED (Tunnel Endpoint Discovery), configuring, 660–662
- terminal packages, 189
- TFTP (Trivial File Transfer Protocol)
 - concentrators, 382
 - digital certificates, 603–605
- thin clients, 156
- throughput
 - concentrators, 182
 - fragmentation, 488, 800
 - misdiagnosing problems, 488
 - routers, 578
- titles, WebVPN, 766
- TLS (Transport Layer Security), 160
- token cards, 6, 23, 86
- tokens, SSL, 159
- Traceroute option, 377
- traffic
 - IPsec, 582–583
 - protecting, 31–33
- transform sets
 - compression, 647
 - ISAKMP/IKE Phase 1, 102–104, 326
 - ISAKMP/IKE Phase 2, 121
 - L2L connections, 326
 - mismatches, 479
 - overview, 645–647
 - PIX/ASA security appliances, 835
 - troubleshooting, 417–418
 - viewing, 647
- transparency, SSL versus IPsec, 167
- transparent tunneling, 440–441
- Transport Layer Security (TLS), 160
- transport mode
 - Easy VPN Server, 732
 - intranets, 20
 - overview, 13–14, 92, 120
 - tunnel mode, versus, 16
- Transport tab
 - DPD, 441
 - local LAN access, 441
 - Microsoft network access, 441–442
 - transparent tunneling, 440–441
- Triple DES
 - See* 3DES
- Triple-A, 220
- troubleshooting
 - authentication
 - certificates, 415–416
 - pre-shared keys, 413–415
 - certificates, 415–416
 - classes, 524
 - concentrators, 385–386, 524–525
 - common problems, 410–418

- event logs, 393–408
- gathering statistics, 409–410
- ISAKMP/IKE Phase 1 problems, 411–417
- ISAKMP/IKE Phase 2 problems, 417–418
- system status, 386–387
- VPN sessions, 387–392
- pre-shared keys, 413, 415
- protected traffic, 418
- transform sets, 417–418
- VPN 3200, 538
- trustpoints
 - autoenrollment configuration, 608–609
 - certificates, 827
- Tunnel Details tab, 456–457
- Tunnel Endpoint Discovery (TED), configuring, 660–662
- tunnel groups, 863–864, 883–885
 - AAA, 873
 - certificate mapping rules, 879
 - L2L, 875
 - remote access general properties, 871–873
 - remote access IPsec properties, 873–875
- tunnel mode
 - intranets, 20
 - overview, 14–15, 92, 120
 - transport mode, versus, 16
- tunnels
 - ACLs, 923
 - concentrators, 198
 - DMVPNs, 575
 - GRE tunnels, 558, 805
 - groups, 214
 - Interactive UA, 551
 - IPsec, 148, 252–254, 553–555, 559–561, 752–753
 - L2TP, 147–148
 - PPTP packets, 140
 - split
 - Easy VPN Server, 464, 736
 - network lists, 257–258
 - options, 256–257
 - overview, 31, 111–112, 256, 919
 - troubleshooting, 483–486
 - VPN Client, 425–426
 - Tunnel Details tab, 456–457
 - user data, 151
- Twofirst algorithm, 52

U

- UDP (User Datagram Protocol)
 - IPsec over UDP, 34
 - L2TP, 149
- unicast traffic, 677–683
- Unit Authentication, 549–550
- unprotected traffic, 31
- updates
 - PIX/ASA appliances, 812
 - VPN 3000, 566–568
 - VPN Client, 468–470
- upgrades
 - concentrators, 381
 - FOS, 811
 - VPN 3200, 565–566
- user accounts
 - authentication
 - L2TP, 151
 - overview, 23, 67, 84
 - PPTP, 133–134
 - remote access, 85–86, 227–229
 - SSL, 167
 - overview, 378
 - Windows client, configuring, 520–521
- user data tunnels, 151
- usernames, 23, 159
- user-to-user VPNs, 20

V

- VAC (VPN Accelerator Card), 814
- value, 43
- variable-length subnet masks (VLSMs), 362
- VCA (Virtual Cluster Agent)
 - ASA, 880
 - configuring, 373–375
 - default priorities, 375
 - NAT, 375
 - operation
 - electing a master, 372
 - load-balancing remote access sessions, 372–373
 - verifying master operation, 373
 - overview, 42, 366, 371, 937–938

- redirection messages, 373
- wireless campuses, 949–950
- VCs (virtual circuits), 40
- Virtual Adapter feature, VPN Client, 426
- virtual circuits (VCs), 40
- Virtual Cluster Agent
 - See VCA
- Virtual Router Redundancy Protocol (VRRP), 366–371
- virtual tunnel interface (VTI) feature, 684–685, 687
- VLAN tagging, 40
- VLSMs (variable-length subnet masks), 362
- VoIP routers, 576
- voluntary tunnels, L2TP, 147
- VPN 3000 concentrators
 - 3005, 178
 - 3015, 179–180
 - 3020, 180
 - 3030, 181
 - 3060, 181
 - 3080, 181
 - Cisco IP Phones, 553
 - configuring groups, 518–520
 - configuring users, 520–521
 - Easy VPN Server, 731
 - features, 184
 - firewalls, troubleshooting, 468
 - fragmentation, troubleshooting, 489
 - HW Client Group tab, 552–553
 - IKE proposals, 516–517
 - IPsec SAs, 517
 - ISAKMP/IKE policies, 480
 - LEAP, 553
 - managing addresses, 520
 - network extension mode, 559
 - overview, 169, 177–178, 516, 552
 - RRI, 563
 - server addresses, 493
 - tools, 385
 - transparent tunneling, 440–441
 - updating clients, 566–568
 - VCA, 371
 - version 3.5, 185–186
 - version 3.6, 186–187
 - version 4.0, 187–188
 - version 4.1, 188
 - version 4.7, 188–189
 - VPN Easy Remote, 750
 - WebVPN, 761
- VPN 3002 Hardware Client, 533
 - accessing
 - CLI, 538
 - GUI, 538–548
 - from public interface, 564–565
 - administering, 564
 - authentication/connection options
 - building IPsec tunnels, 553–555
 - configuring VPN 3000 concentrators, 552–553
 - Individual Unit Authentication, 551–552
 - Interactive Unit Authentication, 551
 - Unit Authentication, 549–550
 - verifying connections, 556
 - automatic updates, 875
 - default configuration, 537–538
 - deploying, 535–537
 - DNS, 545
 - features, 533–534
 - hardware client option, 536–537
 - modes, 545
 - models, 534–535
 - routing features, 562–563
 - RRI, 563
 - software client option, 536
 - static routes, 545–546
 - upgrading, 565
 - automatic, 566
 - manual, 565–566
 - pushing updates to clients, 569
 - VPN 3000 client updates, 566–568
- VPN 3200
 - connections
 - building IPsec tunnels, 553–555
 - client mode, 557
 - configuring VPN 3000 concentrators, 552–553
 - Individual Unit Authentication, 551–552
 - Interactive Unit Authentication, 551
 - network extension mode, 557–561
 - overview, 534, 548–549
 - Unit Authentication, 549–550
 - verifying, 556
 - DHCP, 533
 - Easy VPN Server, 534
 - event logs, 548
 - GUI main screen, 547–548
 - IPsec, 534, 544

- IPsec tunnels, 549, 553–555
- LEDs, 535
- load balancing, 534
- modes, 534
- MTU discovery, 534
- passwords, 546
- Quick Configuration
 - Admin screen, 546–547
 - DNS screen, 545
 - IPsec screen, 544
 - main GUI screen, 547–548
 - overview, 534, 539
 - PAT screen, 545
 - Private Intf screen, 542
 - Public Intf screen, 543
 - Static Routes screen, 545–546
 - Time/Date screen, 540
 - Upload Config screen, 541
- reachability, 562–563
- routing tables, 548
- system status, 548
- troubleshooting, 538
- XAUTH, 549
- VPN Accelerator Card (VAC), 814
- VPN Client
 - address translation, 486–487
 - addressing, 480–483
 - authentication, 478–479
 - auto-update, 470–473
 - certificates
 - CAs, 444
 - deleting, 450
 - exporting, 450–451
 - importing, 446
 - managing, 448
 - obtaining, 444–452
 - setting/changing certificate
 - passwords, 451
 - specifying in connection profiles, 451–452
 - viewing, 448–450
 - DNS resolution, 485–486
 - Error Lookup Tool, 482
 - error messages, 454
 - features, 424
 - fragmentation, 487
 - investigating, 489–491
 - problems created, 488
 - solutions, 491–492
 - GUI options
 - Application Launcher, 460
 - automatic initiation, 461–464
 - firewalls, 464–468
 - using, 464
 - Windows Login Properties, 460
 - installing
 - downloading, 427
 - installation files, 428–435
 - MSI installations, 431
 - pre-installation, 426–427
 - interfaces, 435
 - IPsec connections, 438
 - configuration options, 452–455
 - disconnecting, 459
 - to Easy VPN Server, 453–455
 - notifications, 458–459
 - profile shortcuts, creating, 453
 - Routing Information tab, 458
 - setting connection profiles as default, 452–453
 - statistics, 456
 - status, 456–459
 - Tunnel Details tab, 456–457
 - using certificates, 444–452
 - using pre-shared keys, 438–443
 - to VPN gateways, 455
 - ISAKMP/IKE policies, 479–480
 - logging, 475
 - clearing logging information, 478
 - disabling logging, 477
 - formatting event information, 475–477
 - logging classes, 476
 - searching for logging information, 477–478
 - viewing logs, 475–477
 - MS Network Neighborhood, 493
 - cannot browse network, 494
 - cannot map network drive, 494
 - cannot ping network resources, 493
 - logging in to domains, 493
 - notifications, 458–459
 - operating modes, 435–438
 - PKCS #10, 444–445
 - preferences, 437
 - pre-shared keys
 - Authentication tab, 439
 - Backup Servers tab, 442

- completing connection, 443
 - Dialup tab, 443
 - Transport tab, 439–442
- updating, 468–474
- troubleshooting, 474
 - address assignment, 480–483
 - address translation, 486–487
 - authentication, 478–479
 - clearing logging information, 478
 - disabling logging, 477
 - fragmentation, 487–492
 - ISAKMP/IKE policy mismatches, 479–480
 - MS Network Neighborhood, 493–494
 - searching for logging information, 477–478
 - split tunneling, 483–486
 - XAUTH, 478
- versions, 424
- website, 424
- wireless users, 951–952
- XAUTH, 478
- VPN client, Windows, 497–498
 - configuring, 500–501
 - connections, 521
 - creating, 507–515
 - verifying, 522–523
 - to VPN gateways, 521
 - features, 498–499
 - L2TP, requiring, 506–507
 - security policies, creating, 501–506
 - troubleshooting, 525–530
 - verifying operational, 499–500
 - VPN 3000 concentrator, 516–521
- VPN monitoring feature, IPsec
 - clearing crypto sessions, 796–797
 - configuring IKE peer descriptions, 795
 - overview, 794
 - seeing peer descriptions, 795–796
- VPN Services Module, 579
- vpnclient.ini file, 431–432, 461–463
- vpnclient-win-is-4.x.yy.zzzz-k9.exe file, 470
- vpnclient-win-msi-4.x.yy.zzzz-k9.exe file, 470
- VPN-on-a-stick, 916, 929, 932–933
- VPNs (virtual private networks)
 - defined, 11–12
 - extranets, 20
 - firewall, 19

- gateways, 15, 455
- hardware appliances, 177
- Internet, 21
- intranets, 20
- remote access, 18
- site-to-site, 16–17
- user-to-user, 20
- VRRP (Virtual Router Redundancy Protocol), 366–371
- VTI (virtual tunnel interface) feature, 684–687

W–Z

- WAN-Error-Notify messages,
 - L2TP, 150
- web browser proxy, 171
- web server attacks, 811
- WebVPN
 - AAA, 763
 - access categories, 170
 - ACLs, 302–303
 - application access/port-forwarding, 172
 - authentication, 282
 - colors, 766
 - concentrators, 182, 201
 - CSD
 - configuring for Windows, 308–320
 - installing on concentrators, 308
 - DNS, 763
 - e-mail client access, 173
 - encryption, 283
 - gateways, 765
 - HTTPS access, 282–284, 381, 765
 - idle timeouts, 213
 - key pairs, 763
 - logos, 766
 - network browsing/file management, 171
 - operation, 169–170
 - overview, 156, 188, 281–282, 761–762
 - Port Forwarding feature, 294–297, 304
 - portal page port forwarding, 768
 - portal page URLs, 767–768
 - Post Forwarding feature, 284
 - redirection messages, 373
 - setting up
 - example, 769–771

- global configuration, 285–297
- group configuration, 297–303
- maintaining/monitoring/troubleshooting, 768–769
- prerequisites, 762–763
- SSL, 763–765
- URL/port-forwarding, 767–768
- WebVPN, 765–767
- SSL, 283, 763–765
- SVC
 - installing on concentrators, 304
 - nonadministrator users, 307
 - using, 305–306
- titles, 766
- VPN 3000 series concentrators, 169
- web access, 170–171
- weighted random early detection (WRED), 577
- weighted round-robin queuing (WRRQ), 577
- Windows
 - authentication, 504
 - gateways, 521
 - L2TP, 506–507
 - Properties, 502, 505
 - registry, 506
 - troubleshooting
 - auditing logging, 527–530
 - Event Viewer, 527–530
 - IP Security Monitor, 525–526
 - ipseccmd command, 526–527
 - MMC, 526
 - Oakley logging, 530
- VPN client, 497–498
 - concentrator connection, verifying, 523
 - configuring, 500–501
 - features, 498–499
 - L2TP, requiring, 506–507
 - operational, verifying, 499–500
 - PC connection, verifying, 522–523
 - security policies, creating, 501–506
 - troubleshooting, 525–530
 - VPN 3000 concentrator, 516–521
 - VPN connections, 507–515, 521
- WINS (Windows Internet Naming Service)
 - Easy VPN Server, 736
 - groups, 213
 - server addresses, 493
- wireless
 - concentrators
 - AAA, 946–947
 - certificate enrollment, 944–945
 - configuration, 943–949
 - VCA, 949–950
 - transmissions, 942
 - users, 951–952
 - WRED (weighted random early detection), 577
 - WRRQ (weighted round-robin queuing), 577
- X.509 certificates, 74, 76
- XAUTH
 - Easy VPN Remote, 737, 751–752
 - Easy VPN Server, 741–742, 851–852, 876–877
 - group lock feature, 738
 - IKE, 233
 - IPsec, 106–107
 - overview, 145, 481, 916
 - passwords, 742
 - pre-shared keys, 589
 - VPN 3200, 549
 - VPN Client, 478
- XML (Extensible Markup Language)
 - concentrators, 382
 - overview, 186