

Numerics

500 series PIX Security Appliance, 130-132

802.1x authentication, 234-235, 313

- authentication initiation process, 318
- Cisco IOS Software applications, 316-317
- components, 315
- enabling, 330-331
- port-based
 - configuring, 328-330*
 - default values, resetting, 334*
 - multiple hosts, enabling, 334*
 - periodic reauthentication, enabling, 333*
 - point-to-point configuration, 235-236*
 - port-connected clients, reauthenticating, 334*
 - port states, 318-320*
 - statistics, displaying, 335*
 - switch-to-RADIUS server communication configuring, 332-333*

802.1x framework, 314

3000 series concentrators, 535

5500 series Adaptive Security Appliance models, 132

- back panel, 133
- connectors, 134
- front-panel LEDs, 133

A

AAA (authentication, authorization, and accounting)

- configuring for authentication proxy, 277-280
- RADIUS, 222
 - authentication methods, 223*
 - NAS, 222*
 - versus TACACS+, 223-224*
- session failures, 265
- troubleshooting
 - on CS ACS, 261-262*
 - on PIX Security Appliance, 304-307*

aaa authorization command, 746

AAA Flood Guard, configuring on PIX Security Appliance, 483

AAA servers

- configuring for authentication proxy, 276
- PIX Security Appliance, supported protocols, 285-286

access, controlling. *See security management*

access attacks, 22, 27

- man-in-the-middle, 30
- password attacks, 27
- phishing, 30
- port redirection, 29-30
- social engineering, 30
- trust exploitation, 28-29

access authentication

- configuring on PIX Security Appliance, 287
- on PIX Security Appliance, 283

access lists. *See ACLs*

access profiles, 327

- configuring on Cisco Secure ACS, 327

access routers, configuring as Cisco Easy VPN Remote clients, 632-634

accessing

- configuration mode on PIX Security Appliance, 141
- help system on PIX Security Appliance, 142
- network devices, routers, 84
- websites from WebVPN, 650

accounting, configuring on PIX Security Appliance, 285, 301-302

- command accounting, 304
- console session accounting, 303
- on PIX Security Appliance

ACEs (access control entries), line numbers, 377

ACLs (access control lists), 340, 345-346, 374. *See also object groups, 391*

- ACE line numbers, 377*
- applying to interfaces, 363-367
- configuring
 - for transparent firewall mode, 736*
 - on FWSM, 215*
 - on PIX Security Appliance, 376-377*
 - on private VLANs, 449*
 - on WebVPN, 660-661*
- crypto ACLs, creating, 560-561
- crypto maps
 - applying to interfaces, 565*
 - creating, 562-564*

- downloadable, configuring on PIX Security Appliance, 299-301
- Ethertype ACLs, configuring for transparent firewall mode, 737
- packet filtering, 340
 - stateful*, 342-343
- Turbo ACLs, 381-382
- web access, restricting, 382-384
- activating query mode, 586**
- activation keys, 135**
 - upgrades, troubleshooting, 751
- active mode FTP inspection, 412**
- active security monitoring, 55**
- active/active failover, 726**
 - configuring, 731-732
 - virtual context feature, 732
- active/standby failover, 725**
 - LAN-based, configuring, 731
 - serial cable-based, configuring, 730
- ActiveX filtering, 387**
- activities, 686**
- Adaptive Security Appliance system management, password recovery, 746-747**
- adding protocol inspection to port numbers, 410**
- address translation, 167**
 - dynamic inside NAT, 168
 - outside NAT, 174
 - PAT, 170
 - addresses, backing up*, 173
 - applying to outside interface address*, 171
 - global pools, augmenting*, 173
 - static PAT*, 175-176
 - subnets, mapping to PAT addresses*, 172
 - with overlapping address space*, 175
 - static translations, 173
- admin context, 722**
- Admin tab (Router MC), 697**
- admin-context command, 725**
- administrative access modes, PIX Security Appliance, 140**
- agents (SNMP), 701**
- aggressive mode (IKE), 531**
- AH (Authentication Header), 522-523**
 - header structure, 524
- alarms, 460**
- alerts (CBAC), configuring, 352-353**
- allocating interfaces to security context, 723**
- anomaly-based detection, 462**
- antivirus software, deploying on network hosts, 60**
- applets, 386**
- appliance-based firewalls, 63, 113**
- application inspection, 407**
 - configuring on CBAC
 - ICMP*, 361-363
 - Java*, 359
 - RPC*, 359-360
 - SMTP*, 360
- application layer protocol inspection (CBAC), 349**
- application-level security, 6**
- applying**
 - ACLs to interfaces, 363-367
 - crypto maps to interfaces, 563-565
 - inspection rules to interfaces, 363-367
 - object groups to commands, 391
 - PAT to outside interface address, 171
 - Turbo ACLs, 382
- areas (OSPF), configuring on PIX Security Appliance, 204**
- ARP (Address Resolution Protocol) inspection, 441**
 - configuring for transparent firewall mode, 737
 - DAI, 444
 - MAC spoofing attacks, mitigating, 441
- ARP interface tests, 728**
- ARP spoofing, 441-442**
- ARP-based attacks, mitigating with DHCP snooping, 442-443**
- ASA (Adaptive Security Algorithm), 119, 375**
 - application inspection, 407
- ASA (Adaptive Security Appliance), 463**
 - 5500 series models
 - 5510 Adaptive Security Appliance*, 132
 - 5520 Adaptive Security Appliance*, 132
 - 5540 Adaptive Security Appliance*, 133
 - back panel*, 133
 - connectors*, 134
 - front-panel LEDs*, 133
 - licensing, 137-138
- ASDM (Adaptive Security Device Manager)**
 - Configuration window, 192-193
 - Home window, 191
 - operating requirements, 186
 - workstation requirements*, 187-188
 - PIX Security Appliance, managing, 185, 188-193
- asset identification, 5**
- assigning**
 - hostname to CA server, 586-587
 - privilege levels to commands, 743-744
- asymmetric encryption, 496-498**

atomic signatures, 461**attack guards, configuring on PIX Security Appliance**

- AAA Flood Guard, 483
- DNS Guard, 480
- Frag Guard and Virtual Reassembly, 481-482
- Mail Guard, 479
- SYN cookies, 485-486
- SYN Flood Guard, 483-484
- TCP Intercept, 484

attack signatures, 462**attack-class signatures, 487****attack-drop.sdf, 474****attacks**

- access-related, 22, 27
 - man-in-the-middle, 30*
 - password attacks, 27*
 - phishing, 30*
 - port redirection, 29-30*
 - social engineering, 30*
 - trust exploitation, 28-29*
- DDoS, 34
 - malicious code, 36-39*
 - Smurf, 35-36*
 - TFN, 36*
- DoS, 23, 31
 - chargen, 32*
 - CPU hogging, 32*
 - e-mail bombs, 32*
 - Land.c, 33*
 - malicious applets, 32*
 - out-of-band, 32*
 - ping of death, 31*
 - SYN flood, 32*
 - Targa.c, 33*
 - teardrop.c, 33*
- IP spoofing, 33-34
- masquerade, 33-34
- reconnaissance, 22
 - example of, 24*
- Stacheldraht, 36
- Trojan horses, 23
- viruses, 23
- worms, 23

audit trail information, configuring on CBAC, 352-353**auditing, 73-74**

- excluding signatures from, 490
- on PIX Security Appliance, 488

authentication

- biometrics, 231-232
- digital certificates, 228-230

- for Cisco Easy VPN Client for Windows, configuring, 624-626
- methods available on Cisco Easy VPN Remote, 647-649
- of CAs, 591
- of CS ACS users, 253
 - external user database, configuring, 254*
 - token cards, 255-256*
 - Windows 200 Server user database, 253*
- on PIX Security Appliance
 - methods available on PIX Security Appliance, 283-284*
 - timeouts, 291-292*
- one-time passwords, 226
- port-level, 234
- static passwords, 225
- token cards, 227-228
- tunnel user authentication, 296-297
- virtual HTTP authentication, 295
- virtual Telnet pre-authentication, 294

authentication initiation process (802.1x), 318**authentication proxy, 274-275**

- AAA
 - configuring, 277-278*
 - traffic, allowing to router, 278-280*
- AAA server, configuring, 276
- global timers, configuring, 280
- rules, configuring, 280-282
- verifying configuration, 282-283

authenticator, 314**authorization**

- configuring on PIX Security Appliance, 297-299, 284-285
- lockouts, 745

AVVID (Architecture for Voice, Video and Integrated Data), 74**B****back panel, 5500 series ASA models, 133****backing up PAT addresses, 173****backup VPN servers, configuring on Cisco Easy VPN Client for Windows, 628****Baltimore Technologies. UniCERT CA server, 509-510****best practices for Layer 2 security, 678****bidirectional replication, 251****binding table, 443****biometrics, 231-232****black hats, 21****BPDU guard, 450****broadcast ping interface test, 728**

browsing files with WebVPN, 650

brute-force attacks, 27

building blocks, 687

C

CA servers

- Entrust CA server, 508-509
- support, configuring on Cisco IOS Software, 584-585
 - CA interoperability, maintaining, 593-595
 - CA, authenticating, 591
 - CA, declaring, 590-591
 - certificate, requesting, 592
 - hostname, assigning, 586-587
 - NVRAM management, 585-586
 - RSA key pair, generating, 588
 - system clock, setting, 586
 - verifying configuration, 596
- VeriSign OnSite CA server, 509
- UniCERT, 509-510

cabling

- between failover units, 728
- LAN-based failover, configuring, 731
- serial cable-based failover, configuring, 730

CAM (content addressable memory) table

- MAC spoofing, 440-441
- overflow attacks
 - macof tool, 437
 - mitigating, 438, 673

CAs (certificate authorities), 228

- devices, enrolling, 511
- prerequisites for, 507
- restrictions on, 506

Catalyst switches

- 6500 series switches, FWSM, 209-211
 - installing, 211-214
 - operating requirements, 211
- 7600 series switches, FWSM, 209-211
 - installing, 211-214
 - operating requirements, 211
- 802.x port-based authentication, configuring, 328-330
- security features, 679

CBAC (Context-Based Access Control), 344-346

- ACLs, configuring, 351-352
- application layer protocol inspection, 349
- audit trails, configuring, 352-353
- configuring, 349-351
- global thresholds, configuring, 354
- global timeouts, configuring, 353-355
- half-open connection limits, configuring, 355-356

- inspection rules, 347
 - configuring, 358
 - for IP fragmentation, defining, 360-361
- packets, 345
- PAM, configuring, 356-358
- session layer inspection, 348
- temporary ACL entries, 348
- threshold values, 347
- timeout values, 347
- verifying configuration, 367
 - debug commands, 368

CERT/CC (CERT Coordination Center), 14

certificates

- deleting, 595
- SCEP, 507
 - enrollment using pre-shared keys, 507
 - manual enrollment process, 507

CET (Cisco Encryption Technology), 521

change control, 83

chargen attacks, 32

choosing tunneling protocols, 517

CIPA (Children Internet Protection Act), 13

Cisco ASA, 117-118

- WebVPN support, configuring, 649, 652-655

Cisco ASA 5500 product line features, expanding, 140

Cisco AutoSecure, 41

Cisco Easy VPN, 535, 608

Cisco Easy VPN Client for Windows

- authentication method, configuring, 624-626
- backup VPN servers, configuring, 628
- configuring, 622-623
- dialup networking, configuring, 629-630
- transparent tunneling, configuring, 626-627

Cisco Easy VPN Remote, 609

- access router clients, configuring, 632-634
- authentication methods, 647-649
- configuring, 629
- operation, 610-613
 - restrictions, 609
- PIX 501/506E clients, configuring, 646
- verifying configuration, 635-637

Cisco Easy VPN Server, 609

- configuring, 613-622
- DPD, configuring, 619
- dynamic crypto map with RRI, configuring, 617-619
- group policy lookup, configuring, 614
- IKAKMP policy, configuring, 615
- XAUTH, configuring, 620, 622

Cisco IDS Network Module, 464

Cisco IDSM-2 (Intrusion Detection System Services Module), 464

Cisco IOS Firewalls

- authentication proxy, 274-275
 - AAA, *configuring*, 277-278
 - AAA server, *configuring*, 276
 - AAA traffic, *allowing to router*, 278-280
 - global timers, *configuring*, 280
 - rules, *configuring*, 280-282
 - verifying configuration*, 282-283
- configuring with SDM, 369

Cisco IOS Intrusion Prevention System, 470

- 4200 series sensors, 465
- features of, 471-472
- impact on router performance, 472
- installing, 475-476
- ip audit command support, *configuring*, 476
- logging, *configuring*, 476
- origins of, 472
- signatures
 - attack-drop.sdf file*, 474
 - SDF*, 473
 - SMEs*, 474
- verifying configuration*, 478
 - with clear commands*, 478
 - with debug commands*, 478-479
 - with show commands*, 478

Cisco IOS Software

- 802.1x applications, 316-317
- ACLs. *See* ACLs
- CA support, *configuring*, 584-585
 - CA interoperability, maintaining*, 593-595
 - CA, authenticating*, 591
 - CA, declaring*, 590-591
 - certificate, requesting*, 592
 - hostname, assigning*, 586-587
 - NVRAM management*, 585-586
 - RSA key pair, generating*, 588
 - system clock, setting*, 586
 - verifying configuration*, 596
- network services, 93-98
- password protection schemes, 89-90
- privilege levels, *configuring*, 92
- query mode, *activating*, 586
- SNMPv3, *configuring*, 707-710

Cisco IOS XR Software, 44**Cisco IPS 4200 series sensors, 465****Cisco IPsec VPN Services Module, 536****Cisco Output Interpreter, 41****Cisco PIX Security Appliance, 115**

- Finesse operating system, 118

Cisco Router Audit Tool, 44-45**Cisco Secure ACS, 323-325**

- AAA, *troubleshooting*, 261-262
- access profile configuration, 327
- database replication, 250
- for Windows, *web browser interface*, 259
- navigation buttons, 259-260
- for Windows architecture, 252
- installing, *information gathering procedures*, 258-259
- large network deployment, 326
- OBDC import definitions, 252
- RDBMS synchronization, 251
- small LAN deployment, 325
- TACACS+
 - enabling*, 262-264
 - verifying configuration*, 265
- UCP, 256-257
- user accounts, *creating*, 249-250
- user authentication, 253
 - external user database, configuring*, 254
 - token cards*, 255-256
 - Windows 2000 Server user database*, 253
- user database, 249

Cisco Security Appliance product line, PIX Security Appliance 500 series, 130-132**Cisco Security Device Manager, 120****Cisco Self-Defending Networks, 76**

- identity management solutions, 78-79
- secure connectivity system, 76
- threat defense system, 77
- trust and identity solutions, 78-79

Cisco VPN 3000 series concentrators, 535**Cisco VPN 3002 Hardware Client, 536****Cisco VPN Client, 535-536****CiscoView, 706****CiscoWorks Common Services, 684****CiscoWorks Router Management Center, 682****CiscoWorks VMS, 70-72****class maps, *configuring*, 402****class-map command, 401****classless routing, 101****clear commands, *verifying Cisco IOS IPS configuration*, 478****clear icmp command, 379****clearing SDEE events, 478****client initiated remote-access VPNs, 513****client mode (Cisco Easy VPN Remote), 629-630****clock timezone command, 586****closed networks, 3****closed security models, 10**

command authorization, PIX Security Appliance system management, 742, 745**command channel, 412****commands**

- class-map, 401
- aaa authorization, 746
- admin-context, 725
- clear icmp, 379
- clock timezone, 586
- config-url, 724
- configuring on PIX Security Appliance, 304
- crypto ca certificate query, 585
- crypto ikakmp identity hostname, 611
- crypto isakmp policy, 599
- crypto pki enroll, 593
- crypto pki trustpoint, 590
- debug crypto isakmp, 568
- dot1x port-control, 319
- duplex, 149
- enable, 141
- failover active, 726
- filter url, 389
- firewall transparent, 735
- floodguard, 483
- global, 152-153
- hostname, 144
- icmp, 378
- import all, 632
- inspect http, 415
- interface, 145
- ip address, 146-147
- ip address dhcp, 147
- ip audit name, 489
- logo, 654
- name, 154
- nameif, 146
- nat, 150
- nat 0, 176-177, 379
- nat-control, 150
- network, 632
- passive-interface, 104
- ping, 159-160
- policy-map, 401
- privilege levels, assigning, 743-744
- route, 153-154
- secondary text-color, 655
- security level, 148
- security passwords, syntax, 91
- service password-recovery, 91, 747
- service-policy, 401
- show, 155-158
- show conn, 178
- show conn detail, 179
- show context, 725
- show crypto ca certificate, 603
- show crypto ca roots, 596

- show crypto map, 568
- show fragment, 482
- show ip dhcp snooping binding, 444
- show ip inspect, 367
- show local-host, 180-181
- show logging, 163
- show mode, 722
- show privilege level, 744
- show run access-list, 575
- show run crypto isakmp, 574
- show runnign configuration, 553
- show timeout, 182
- show version, 749
- show xlate, 181
- show xlate detail, 181
- spanning-tree portfast, 451
- speed, 148-149
- static, 173
- static pat, 176
- tacacs, 265-266
- title-color, 654
- transport input none, 85
- vpn-tunnel-protocol, 655
- WebVPN subcommand mode, 652-653

Common Criteria, 15**community ports, 448****community strings, 700****comparing**

- FWSM and PIX features, 210
- FWSM and PIX Firewall, 120
- IPsec and WebVPN, 517
- RADIUS and TACACS+, 223-224

compatibility of ACLs with IPsec, verifying, 550**composite signatures, 461****config-url command, 724****configurable proxy ping, 378****configuration commands on PIX Security Appliance, 144-163****configuration files, copying, 749****configuration mode, accessing on PIX Security Appliance, 140-141****Configuration tab (Router MC), 694-695****configuration weaknesses, 18-19****Configuration window (ASDM), 192-193****configuring**

- 802.1 port-based authentication, switch-to-RADIUS server communication, 332-333
- 802.1x port-based authentication, 328-330
- ACLs
 - for transparent firewall mode, 736*
 - on FWSM, 215*

- on PIX Security Appliance, 376-377*
 - on private VLANs, 449*
 - on WebVPN, 660-661*
- ASDM for PIX Security Appliance management, 188-193
- authentication proxy
 - AAA, 277-280
 - AAA server, 276
 - global timers, 280
 - rules, 280-282
 - verifying configuration, 282-283
- CA support on Cisco IOS Software, 584-585
 - CA interoperability, maintaining, 593-595
 - CA, authenticating, 591
 - CA, declaring, 590-591
 - certificate, requesting, 592
 - hostname, assigning, 586-587
 - NVRAM management, 585-586
 - RSA key pair, generating, 588
 - system clock, setting, 586
 - verifying configuration, 596
- CBAC, 349-351
 - ACLs, 351-352
 - alert messages, 352-353
 - audit trails, 352-353
 - global thresholds, 354
 - global timeouts, 353-355
 - half-open connection limits, 355-356
 - inspection rules, 358
 - IP fragmentation inspection rules, 360-361
 - PAM, 356-358
- Cisco ASA, WebVPN support, 649, 652-655
- Cisco Easy VPN Client for Windows, 622-623
 - authentication method, 624-626
 - backup VPN servers, 628
 - dialup networking, 629-630
 - transparent tunneling, 626-627
- Cisco Easy VPN Remote, 629
 - access router clients, 632-634
- Cisco Easy VPN Server, 613-622
 - DPD, 619
 - dynamic crypto map with RRI, 617-619
 - group policy lookup, 614
 - ISAKMP policy, 615
 - XAUTH, 620-622
- Cisco IOS Firewall with SDM, 369
- Cisco IOS IPS
 - ip audit command support, 476
 - logging, 476
 - verifying configuration, 478-479
- class maps, 402
- DHCP snooping, 443, 668
- dynamic ARP inspection, 669
- enhanced HTTP inspection, 416
- external user database for CS ACS authentication, 254
- failover
 - active/active, 731-732
 - active/standby failover, 725, 730-731
- FTP deep packet inspection, 414
- FWSM
 - access lists, 215
 - interfaces, 213
- IDS policies, 489-490
- IPsec, 601
- multiple interfaces, 182-185
- object groups, 392-393
 - nested, 396-397
- passwords in Cisco IOS Software, 89
- PIX Security Appliance, 141
 - AAA Flood Guard, 483
 - access authentication, 287
 - accounting, 301-304
 - ACLs, 376-377
 - as Easy VPN Server, 637-644
 - authorization, 297-299
 - cut-through proxy authentication, 292-294
 - DNS Guard, 480
 - downloadable ACLs, 299-301
 - Frag Guard and Virtual Reassembly, 481-482
 - IDS, 488-489
 - interactive user authentication, 287-290
 - local user database authentication, 290-291
 - logical interfaces, 194-197
 - Mail Guard, 479
 - multicast routing, 205-209
 - multiple context mode, 718, 722
 - NAT with three interfaces, 169-170
 - NAT with two interfaces, 168
 - OSPF, 201-205
 - RIP routing, 198-200
 - security contexts, 723-724
 - shun feature, 491-492
 - site-to-site VPN using digital certificates, 602-604
 - static routing, 198-200
 - SYN cookies, 485-486
 - SYN Flood Guard, 483-484
 - syslog, 161-163
 - system clock, 160-161
 - TCP Intercept, 484
 - virtual HTTP authentication, 295
 - virtual Telnet pre-authentication, 294
 - VLANs, 193-198
- policy maps, 404-406
- port security, restricted traffic, 438-440
- privilege levels for Cisco IOS Software, 92

- protocol inspection
 - ESMTP application inspection, 419*
 - ICMP inspection, 420*
 - RSH inspection, 417-418*
 - SNMP inspection, 421-422*
 - SQL*Net inspection, 418-419*
- RADIUS, 268-269
- routers
 - IKE using pre-shared keys, 551-556*
 - IPsec using pre-shared keys, 557-565*
- service policies, 406
- site-to-site VPNs
 - IPsec configuration tasks, 542-544*
 - between PIX Security Appliances with pre-shared keys, 570-578*
- site-to-site VPNs using digital certificates, 597-601
- SNMPv3
 - on Cisco IOS Software, 707-710*
 - on PIX Security Appliance, 710-712*
- static routes, 102-104
- STP
 - BPDU guard, 451*
 - root guard, 450*
- TACACS+ on CS ACS, 262-264
- transparent firewall mode
 - ACLs, 736-737*
 - ARP inspection, 737*
- tunnel groups, 572-574
- tunnel interfaces, 520
- VPNs with SDM, 569-570
- WAN connection with SDM, 126
- WebVPN
 - ACLs, 660-661*
 - content filters, 660-661*
 - e-mail proxy mode, 659*
 - file access, 656*
 - port forwarding, 651-652, 657-659*
- connections, 164, 177**
- connectivity**
 - of networks, testing before IPsec configuration, 549
 - of PIX Security Appliance, verifying, 159-160
- connectors for 5500 series ASA models, 134**
- consequences of compromised security, legal liability, 12-13**
- console ports, 84**
- console session accounting, configuring on PIX Security Appliance, 303**
- content filters, configuring on WebVPN, 660-661**
- controlling vty lines, 86**
- copying configuration files, 748-749**
- counteracting eavesdropping, 26**

- CPU hogging, 32**

- crackers, 21**

- creating**

- crypto ACLs, 560-561
- crypto maps, 562-564
- CS ACS user accounts, 249-250
- customized firewalls, 114
- DHCP server address pool, 632
- directories, 748
- IKE policies, 551, 599
 - parameters, 552*
 - transform sets for Cisco Easy VPN Remote clients, 615-617

- crypto ACLs creating, 560-561**

- crypto ca certificate query command, 585**

- crypto isakmp identity hostname command, 611**

- crypto isakmp policy command, 599**

- crypto maps**

- applying to interfaces, 565
- creating, 562-564

- crypto pki enroll command, 593**

- crypto pki trustpoint command, 590**

- CSAccupdate service, 252**

- CTIQBE, 427**

- customizing**

- firewalls, 114
- WebVPN look-and-feel configuration, 654-655

- cut-through proxy authentication**

- configuring on PIX Security Appliance, 292-294
- on PIX Security Appliance, 283

D

- DAI (Dynamic ARP Inspection), 444**

- data channel, 412**

- Data Privacy Directives, 12**

- database replication on CS ACS database, 250**

- date and time, configuring**

- on Cisco IOS Software, 586
- on PIX Security Appliance, 160-161

- DDoS attacks, 34**

- malicious code, 36
 - Trojan horses, 39*
 - viruses, 39*
 - worms, 37-38*
- Smurf, 35-36
- Stacheldraht, 36
- TFN, 36

- debug commands**

- verifying CBAC installation, 368
- verifying Cisco IOS IPS configuration, 478-479
- debug crypto isakmp command, 568**
- debug tacacs command, 265-266**
- declaring a CA, 590-591**
- default routes, configuring on FWSM, 214**
- defining**
 - inspection rules, 358
 - IPsec security policy, 544
 - ACL compatibility, verifying, 550*
 - connectivity on network, testing, 549*
 - IKE phase 1 details, identifying, 544-545*
 - IKE phase 2 details, identifying, 547-548*
 - validity of current policies, verifying, 548-549*
 - URLs in WebVPN, 656
- defining CA characteristics, 590**
- deleting**
 - certificates, 595
 - public keys from peers, 595
- deploying Cisco Secure ACS**
 - in large networks, 326
 - in small LAN environment, 325
- deployment scenarios for Ipsec, 522**
- Deployment tab (Router MC), 695**
- design phase (PDIOO), 82**
- developing security policies, 57-58**
- devices**
 - Cisco IDS/IPS, 462, 464-465
 - enrolling with CAs, 511
 - hardening, 59
- Devices tab (Router MC), 693**
- DHCP (Dynamic Host Configuration Protocol)**
 - server address pool, creating, 632
 - starvation attacks, mitigating, 444-445
- DHCP snooping, 442**
 - binding table, 443
 - configuring, 443, 668
- DHCPOFFER messages, 445**
- dialup networking, configuring on Cisco Easy VPN Client for Windows, 629-630**
- dictionary cracking, 28**
- Diffie-Hellman algorithm, 499-500**
- digital certificates, 228-230, 504**
- digital signatures, 502, 505**
- directories**
 - contents, displaying, 747-748
 - creating, 748
- disabling**
 - 802.1x authentication, 331
 - CBAC alert messages, 352
 - DNS name resolution, 106
 - network services on Cisco IOS Software, 96-98
 - protocol inspection, 409
 - reverse Telnet, 85
 - SNMP, 105
- disclosure, 703**
- displaying**
 - 802.1x statistics, 335
 - crypto map configuration, 568
 - directory contents, 747-748
 - IKE event messages, 568-569
 - IPsec events, 568
 - IPsec SA configuration, 567
 - ISAKMP events, 568
 - ISAKMP policies, 566
 - object groups, 398
 - status of PIX Security Appliance, 155-158
 - transform set configuration, 566
- DNS (Domain Name System) name resolution), disabling, 106**
- DNS Guard, configuring on PIX Security Appliance, 480**
- DNS inspection, 428, 430**
- DoS attacks, 23, 31**
 - Targa.c, 33
 - teardrop.c, 33
 - CBAC thresholds, 347
 - chargen, 32
 - CPU hogging, 32
 - e-mail bombs, 32
 - Land.c, 33
 - malicious applets, 32
 - out-of-band, 32
 - ping of death, 31
 - SYN flood, 32
- dot1x port-control command, 319**
- double tagging, 446**
- downloadable ACLs, configuring on PIX Security Appliance, 299-301**
- downloading software images via TFTP, 750**
- DPD (dead peer detection), 619**
- drivers influencing network security**
 - Internet connection speeds, 13
 - ISO/IEC 17799 standard, 14
 - IT staffing shortages, 13
 - wireless access, 13
- DSA, 230**

due care, 12
due diligence, 12
duplex command, 149
dynamic ARP inspection, configuring, 669
dynamic inside NAT, 168
dynamic key distribution, 314
dynamic ports, 330
dynamic-access ports, 330

E

e-mail proxy mode, configuring on WebVPN, 659
EAP (Extensible Authentication Protocol), 313

- EAP-TLS, 322
- LEAP, 321
- PEAP, 322
- selecting, 320

EAP-FAST, 320
EAP-MD5, 320
EAP-TLS, 320-322
EAPOL (EAP over LAN), 317
Easy VPN Server, configuring PIX Security Appliance, 637-644
eavesdropping, 24-25

- counteracting, 26

e-mail bombs, 32
embryonic connections, limiting on servers, 486
enable command, 141
enabling

- 802.1x authentication, 330-331
- CBAC audit trail messages, 352
- transparent firewall mode on PIX Security Appliance, 735

encrypting data as reconnaissance attack countermeasure, 26-27
encryption

- asymmetric, 497-498
- Diffie-Hellman algorithm, 499-500
- digital certificates, 504
- digital signatures, 502, 505
- symmetric, 496-497

encryption licenses, 136
enhanced HTTP inspection, 415

- configuring, 416

enrolling

- PIX Security Appliance with CA, 602-604
- devices with CAs, 511
- using pre-shared keys (SCEP), 507

Entrust CA server, 508-509

ESMTP application inspection. configuring, 419
ESP (Encapsulating Security Payload), 522-524

- packet header format, 525

EtherChannel ports, 330
Ethernet ACLs, configuring for transparent firewall mode, 736-737
events (ISAKMP), displaying, 568
examples of reconnaissance attacks, 24
excluding signatures from auditing, 490
expansion slots

- on PIX 515E, 138
- on PIX 525, 138
- on PIX 535, 139

external threats, 20

F

face recognition, 231
Factory Reset Wizard (SDM), 126-127
failover

- active/active
 - configuring, 731-732
 - virtual context feature, 732
- active/standby, 725
 - LAN-based, configuring, 731
 - serial cable-based, configuring, 730
- cabling, 728
- interface tests, 728
- licensing, 727
- UR licenses, 727

failover active command, 726
false negatives/positives, 459
features

- of Cisco ASA 5500 ASA family, expanding, 140
- of Cisco IOS Firewall, 114
- of Cisco IOS IPS, 471-472
- of IBNS, 313
- of NAC, 239-240

FERPA (Family Educational Rights and Privacy Act), 13
file access, configuring on WebVPN, 656
file management, displaying directory contents, 747-748
files, copying, 748
filter url command, 389
filtering FTP commands, 414
Finesse operating system, 118
fingerprint scanning, 231
FIPS (Federal Information Processing Standard), 16
firewall transparent command, 735

firewalls

- appliance-based, 63
- customized, creating, 114
- deploying on network hosts, 59
- server-based, 64
- transparent, 718

floodguard command, 483**FO (failover) licenses, 727**

- Active/Active licenses, 135
- Active/Standby licenses, 135

FQDN (fully qualified domain name), 586**Frag Guard and Virtual Reassembly, configuring on PIX Security Appliance, 481-482****fragmentation inspection, defining inspection rules, 360-361****front panel LEDs, 5500 series ASA models, 133****FTP commands, filtering, 414****FTP inspection, 410**

- active mode, 412
- passive mode, 413

FWSM (Firewall Services Module), 119-120, 209-211

- access lists, configuring, 215
- default routes, configuring, 214
- installing, 211-214
- interfaces, configuring, 213
- operating requirements, 211
- operating with PDM, 215-216

G**general-purpose keys, generating, 589****generating, RSA key pair, 588****GLB (Gramm-Leach-Bliley) Act, 12****global command, 152-153****global pools, augmenting with PAT, 173****global timers, configuring**

- CBAC, 353-355
- for authentication proxy, 280

goals of network security, 2**GRE tunneling, 518-520****group policy lookup, configuring on Cisco Easy VPN Server, 614****H****H.323, 426****hackers, 21****half-open connections limiting**

- on CBAC, 355-356
- on servers, 486

hardening network hosts, 59**hardware failover, 725-727****hashing, 500**

- HMAC, 501-502

help system, accessing on PIX Security Appliance, 142**HIDS (host-based intrusion detection system), 457****hierarchical object groups. *See* nested object groups****hierarchy of device groups, 686****HIPAA (Health Insurance Portability and Accountability Act of 1996), 13****HIPS (host-based intrusion prevention system), 457****HMAC, 501-502****home page (WebVPN), 649**

- customizing, 654-655

Home window (ASDM), 191**host analysis, 45-46****Host Unreachable messages (ICMP), protecting from exploitation, 101****host-based intrusion detection, deploying on network hosts, 61-62****hostname, assigning to CA server, 586-587****hostname command, 144****HTTP inspection, 416-416****hub-and-spoke topologies, 685****I****IBNS (Identity Based Networking Services), 80, 232-234, 312****802.1x, 234-235***authentication initiation process, 318**enabling, 330-331**port-based authentication, point-to-point configuration, 235-236**port states, 318-320***802.1x framework, 313***Cisco IOS Software applications, 316-317**components of, 315*

benefits of, 313

Cisco Secure ACS, 323-325*large network deployment, 326**small LAN deployment, 325***EAP***EAP-TLS, 322**LEAP, 321*

- PEAP*, 322
 - selecting*, 320
 - features, 313
- icmp command**, 378
- ICMP inspection, configuring**, 361–363, 420
- ICMP messages, protecting from exploitation**
 - Host Unreachable messages, 101
 - Mask Reply messages, 102
 - Redirect messages, 101
- ICMP-type object groups**, 391
 - configuring, 394
- ICSA Labs**, 16
- identifying**
 - IKE phase 1 details for IPsec security policy planning, 544-545
 - IKE phase 2 details for IPsec security policy planning, 547-548
 - network assets, 5
 - vulnerabilities
 - Knoppix STD*, 46-47
 - Microsoft Baseline Security Analyzer*, 47
- identity**, 69
- identity NAT rules**, 379
- IDSs (intrusion detection systems)**, 486
 - alarms
 - false negatives*, 459
 - false positives*, 459
 - true negatives*, 460
 - true positives*, 460
 - anomaly -based detection, 462
 - configuring on PIX Security Appliance, 488-489
 - HIDS, 457
 - network-based, 458
 - NIDS, 65
 - policies, configuring, 489-490
 - signature-based detection, 460
 - signatures, 461
- IGMP (Internet Group Management Protocol), configuring on PIX Security Appliance**, 206-209
- IKE (Internet Key Exchange)**, 505, 532
 - aggressive mode, 531
 - component technologies, 533
 - event messages, displaying, 568-569
 - main mode, 531
 - peer authentication, 533
 - phase 1, 531
 - details, identifying*, 544-545
 - phase 2 details, identifying, 547-548
 - policies, creating, 551-552, 599
 - session negotiation, 530
 - using pre-shared keys, routers configuration, 551-556
- import all command**, 632
- improvement phase of security wheel**, 56
- inbound connections**, 164
- individual user authentication on Cisco Easy VPN Remote clients**, 648-649
- info signatures**, 462
- information gathering**, 26
 - for CS ACS installation, 258-259
- information security organizations**
 - CERT/CC, 14
 - ISC2, 15
 - SANS Institute, 15
 - US-CERT, 15
- information theft**, 26
- informational signagures**, 487
- Initial Configuration Dialog option**, 85
- inserting ACEs in ACLs**, 378
- inside interfaces**, 166
- inspect http command**, 415
- inspection engines**
 - anomaly-based detection, 462
 - signature-based detection, 460
- inspection rules**
 - applying to interfaces, 363-367
 - CBAC, 347
 - defining, 358
 - for IP fragmentation, defining, 360-361
- installing**
 - Cisco IOS IPS, 475-476
 - Cisco VPN Client 4.x, 622
 - Cisco Secure ACS, information gathering procedures, 258-259
 - FWSM, 211-214
 - Router MC, 688-690
- integrated firewalls**, 113
- integrated security**
 - IBNS, 80
 - perimeter security, 80
- interactive user authentication, configuring on PIX Security Appliance**, 287-290
- interface command**, 145
- interfaces**
 - ACLs, applying, 363-367
 - allocating to security context, 723
 - configuring on FWSM, 213
 - crypto maps, applying, 563
 - inside, 166
 - inspection rules, applying, 363-367
 - multiple, configuring, 182-185

- outside, 166
 - security levels, 142
 - internal threats, 21**
 - international security organizations**
 - Common Criteria, 15
 - FIPS, 16
 - ICSA Labs, 16
 - Internet connection speeds, effect on network security, 13**
 - intrusion detection, deploying on network hosts, 61**
 - inventorying network hosts, 62**
 - ip address command, 146-147**
 - ip address dhcp command, 147**
 - ip audit command support, configuring on Cisco IOS IPS, 476**
 - ip audit name command, 489**
 - IP classless routing, 101**
 - IP directed broadcast, 100**
 - IP fragmentation inspection rules, defining, 360-361**
 - ip inspect name command, 359**
 - IP multicast, configuring on PIX Security Appliance, 205-209**
 - IP source routing, 99**
 - IP directed broadcast, 100
 - proxy ARP, 99
 - IP spoofing attacks, 33-34**
 - IP Telephony required protocols, 426**
 - CTIQBE, 427
 - H.323, 426
 - MGCP, 428
 - SCCP, 427
 - SIP, 426
 - IP VPNs, 66**
 - IPsec, 519–521, 525**
 - AH, 523
 - header structure, 524*
 - configuring, 601
 - deployment scenarios, 522
 - ESP, 524
 - packet header format, 525*
 - events, displaying, 568
 - negotiation process, 530
 - packet processing flowchart, 534-535
 - router configuration, verifying, 566-570
 - SAs, 528-529
 - transport mode, 526-527
 - L2TP, 576*
 - tunnel mode, 526-527
 - using pre-shared keys, router configuration, 557-565
 - security policies, 544
 - ACL compatibility, verifying, 550*
 - IKE phase 1 details, identifying, 544-545*
 - IKE phase 2 details, identifying, 547-548*
 - testing network connectivity, 549*
 - validity of current policies, verifying, 548-549*
 - verifying for IPsec with pre-shared key configuration, 559-560*
 - ISAKMP, 532**
 - configuring on Cisco Easy VPN Server, 615
 - events, displaying, 568
 - identity, configuring, 554-555
 - policy negotiation, 553-554
 - ISC2 (International Information Systems Security Certification Consortium), 15**
 - ISO/IEC 17799 standard, effect on network security, 14**
 - IT staffing shortages, effect on network security, 13**
-
- ## J-K
- Java applet filter, 386**
 - Java inspection, configuring on CBAC, 359**
 - Knoppix STD, 46-47**
-
- ## L
- L2TP (Layer 2 Tunneling Protocol), 517**
 - IPsec transport mode, 576
 - LAN-based failover**
 - cabling, 729
 - configuring, 731
 - Land.c attacks, 33**
 - large networks, deploying Cisco Secure ACS, 326**
 - launching Router MC, 690**
 - Layer 2 attacks**
 - ARP spoofing, 441-442
 - CAM table overflow attacks, mitigating, 673
 - DHCP starvation attacks, 444
 - mitigating, 445*
 - MAC spoofing, mitigating, 440-441, 668, 672
 - macof tool, 437
 - overflow attacks, mitigating, 438
 - private VLANs
 - ACLs, configuring, 449*
 - vulnerabilities, 448*
 - security best practices, 678
 - spanning tree attacks, mitigating, 670
 - VLAN hopping
 - double tagging, 446*
 - mitigating, 447, 669-671*
 - switch spoofing, 446*
 - vulnerabilities, mitigating, 675-679

layers of SAFE security blueprint, 74

LEAP (Lightweight Extensible Authentication Protocol), 313, 320-321

legal liability as consequence of compromised security, 12-13

legislation

- CIPA, 13
- FERPA, 13
- GLB Act, 12
- HIPAA, 13

licenses

- activation keys, 135
- ASA Security Appliance, 137-138
- for PIX Security Appliance, 135
 - failover*, 727
- security contexts, upgrading, 136

limitations of IKE peer authentication with pre-shared keys, 543

LinkUp/Down interface tests, 728

local user accounts, creating in Cisco IOS Software, 92

local user database, configuring on PIX Security Appliance, 290-291

lockouts, 745

logging

- configuring on Cisco IOS IPS, 476
- syslog, configuring on PIX Security Appliance, 161-163

logical interfaces, configuring on PIX Security Appliance, 194-197

logo command, 654

M

MAC address learning, PIX Security Appliance, 738-739

MAC spoofing attacks, 440

- mitigating, 441, 668, 672

macof tool, 437

- overflow attacks, mitigating, 438

Mail Guard, configuring on PIX Security Appliance, 479

main mode (IKE), 531

maintaining CA interoperability, 593-595

malicious code, 36

- applets, 32
- filtering
 - ActiveX filtering*, 387
 - Java applet filtering*, 386
- viruses, 39
- Trojan horses, 39
- worms, 37-38

man-in-the-middle attacks, 30

managed devices (SNMP), 700-701

managed objects (SNMP), 700

managing

- passwords, best practices, 90
- PIX Security Appliance with ASDM, 185-193

manual enrollment (SCEP), 507

mapping subnets to PAT addresses, 172

Mask Reply messages (ICMP), protecting from exploitation, 102

masquerade attacks, 33-34

match criteria for class maps, 403

MBSA (Microsoft Baseline Security Analyzer), 47

MD (Message Digest), 501

media gateways, 428

memory requirements for Turbo ACLs, 382

MGCP (Media Gateway Control Protocol), 428

MIBs, 700

Microsoft Certificate Services, 510

mitigating

- ARP-based attacks with DHCP snooping, 442-443
- CAM table overflow, 673
- DHCP starvation attacks, 445
- Layer 2 vulnerabilities, 675-679
- MAC spoofing attacks, 440-441, 668, 672
- spanning tree attacks, 670
- VLAN hopping attacks, 447, 669-671

monitor mode (PIX Security Appliance), 140

Monitor mode (SDM), 127, 130, 681

MPF (Modular Policy Framework), 400

- class maps, configuring, 402
- policy maps, configuring, 404-406
- service policies, configuring, 406

MPLS (Multiprotocol Label Switching), 519

multicast routing, configuring on PIX Security Appliance, 205-209

multiple context mode, configuring on PIX Security Appliance, 718-722

multiple hosts, enabling, 334

multiple interfaces, configuring, 182-185

mutual peer authentication (IKE), 533

N

NAC (Network Admission Control), 236

- components of, 236-237
- features, 239-240
- Phase 1, 238
- Phase 2, 238

NAC Program, vendor participation, 240-241

name command, 154
name-to-address mapping, defining for CA server support, 587
nameif command, 146
NAS (network access server), 222
NAS-initiated remote-access VPNs, 513
NAT (Network Address Translation), 149, 166
 outside NAT, 174
 with three interfaces, configuring, 169-170
 with two interfaces, configuring, 168
nat 0 command, 176-177, 379
nat command, 150
nat-control command, 150
navigation buttons, CS ACS web browser interface, 259-260
NBNS (NetBIOS Name Service) servers, configuring, 653
nested object groups, 394
 configuring, 396-397
network activity interface tests, 728
network analysis, 41
 Cisco IOS XR Software, 44
 Cisco RAT, 44-45
 RSCG, 43
network command, 632
network devices
 remote administration with SSH, 87-88
 SSH client, 88
 SSH server, 88-89
 routers, securing tty ports, 85
 vty line, controlling, 86
network extension mode (Cisco Easy VPN Remote), 630-631
network extension plus mode (Cisco Easy VPN Remote), 630
network hosts
 antivirus software, deploying, 60
 hardening, 59
 intrusion detection/prevention, deploying, 61
 host-based, 62
 inventorying, 62
 operating system patches, deploying, 60
 personal firewalls, deploying, 59
 virus definitions, updating, 63
network management
 SNMP, CiscoView, 706
 SNMPv3, 704
 applications supporting, 705
 configuring on Cisco IOS Software, 707-710
 configuring on PIX Security Appliance, 710-712
network object groups, 391
 configuring, 393

network service support on Cisco IOS Software, 93-98
network-based intrusion detection, 458
NIDS (network-based intrusion detection system), 65
NMSs (network management stations), 104
nonrepudiation, 498
NTP (Network Time Protocol), 104
NVRAM (nonvolatile RAM), local certificate storage, 585-586

O

object groups, 374
 configuring, 392-393
 nested, 394
 configuring, 396-397
 removing, 399
 viewing, 398
ODBC import definitions for Cisco Secure ACS, 252
OIDs (object identifiers), 700
on-demand DPD, 619
one-time passwords, 226
open networks, 3
open security model, 7
operating requirements
 for FWSM, 211
 for ASDM, 186
 workstation requirements, 187-188
operating system patches, deploying on network hosts, 60
operation phase (PDIOO), 83
optimization phase (PDIOO), 83
origins of Cisco IOS IPS, 472
OSPF (Open Shortest Path First), configuring on PIX Security Appliance, 201-205
OTPs (one-time passwords), 248
out-of-band attacks, 32
outbound connections, 164
outside interfaces, 166
 PAT, applying, 171
outside NAT, 174
overflow attacks
 macof tool, 437
 mitigating, 438
overloading, 112

P

packet filtering, 340
 ACLs, 345-346
 stateful, 119, 342-343

packet processing flowchart, IPsec, 534-535

packets, CBAC, 345

PAM (port-to-application mapping), configuring on CBAC, 356-358

parameters defined in IKE policies, 552

passive mode FTP inspection, 413

passive security monitoring, 55

passive-interface command, 104

password attacks, 27

passwords

lockouts, 745

OTPs, 248

protection schemes in Cisco IOS Software, 89-90

recovering

on Adaptive Security Appliance, 746-747

on PIX Security Appliance, 745-746

service password encryption, 90

UCP, 256-257

PAT (port address translation), 170

addresses, backing up, 173

applying to outside interface address, 171

global pools, augmenting, 173

static PAT, 175-176

with overlapping address space, 175

patches, applying to network hosts, 60

PDIOO (Plan, Design, Implement, Operate, Optimize), 81

design phase, 82

implementation phase, 83

operation phase, 83

optimization phase, 83

planning phase, 82

PDM (PIX Device Manager), operating with FWSM, 215-216

PEAP, 320, 322

peer authentication (IKE), 533

perimeter security, 80

periodic DPD, 620

personal firewalls, deploying on network hosts, 59

Phase 1 (NAC), 238

Phase 2 (NAC), 238

phishing, 21, 30

phreaking, 21

ping command, 159-160, 378

ping interface test, 728

ping of death attacks, 31

PIX Firewall, comparing with FWSM, 120

PIX Password Lockout Utility, 746

PIX Security Appliance, 463

AAA

access authentication, configuring, 287

authentication prompts and timeout, 291-292

interactive user authentication, configuring, 287-290

local user database authentication, configuring, 290-291

troubleshooting, 304-307

AAA Flood Guard, configuring, 483

AAA server support, 285-286

accounting, 285

configuring, 301-304

ACLs, configuring, 376-377

administrative access modes, 140

auditing, 488

authentication

virtual HTTP authentication, 295

virtual Telnet pre-authentication, 294

authentication methods, 283-284

authorization, 284-285

configuring, 297-299

configuration commands, 144-160, 163

configuration mode, accessing, 141

configuring, 141

as Easy VPN Server, 637-644

connectivity, displaying, 159-160

cut-through proxy authentication, configuring, 292, 294

DNS Guard, configuring, 480

downloadable ACLs, configuring, 299, 301

failover

cabling, 728

interface tests, 728

requirements, 727

Frag Guard and Virtual Reassembly, configuring, 481-482

help system, accessing, 142

IDS, configuring, 488-489

Java applet filter, 386

licenses, 135

upgrading, 750-751

logical interfaces, configuring, 194-197

MAC address learning, 738-739

Mail Guard, configuring, 479

managing with ASDM, 185, 188-193

multicast routing, configuring, 205-209

multimedia support, 421-422

multiple context mode, configuring, 718, 722

OSPF, configuring, 201-205

PIX 501 Security Appliance, 130

PIX 501/506E, configuring Cisco Easy VPN Remote client, 646

PIX 506E Security Appliance, 131

PIX 515E Security Appliance, 131

expansion slots, 138

- PIX 525 Security Appliance, 131
 - expansion slots, 138*
 - PIX 535 Security Appliance, 132, 139
 - protocol inspection, 408
 - RIP routing, configuring, 198-200
 - security contexts
 - configuring, 724*
 - interfaces, allocating, 723*
 - security levels, 142
 - shun feature, configuring, 491-492
 - site-to-site VPNs
 - using digital certificates, configuring, 602-604*
 - verifying configuration, 578-579*
 - SNMPv3, configuring, 710-712
 - software image, upgrading, 751
 - static routing, configuring, 198-200
 - status of, displaying, 155-158
 - supported IDS signatures, 487
 - SYN cookies, configuring, 485-486
 - SYN Flood Guard, configuring, 483-484
 - syslog, configuring, 161-163
 - system clock, configuring, 160-161
 - system management, 718, 739
 - command authorization, 742, 745*
 - password recovery, 745-746*
 - SSH access, 741-742*
 - Telnet access, 739-740*
 - TCP Intercept, configuring, 484
 - transparent firewall mode, 733
 - ACLs, 736-737*
 - ARP inspection, configuring, 737*
 - enabling, 735*
 - tunnel user authentication, 296-297
 - URL filtering, 388-390
 - VLANs, 198
 - configuring, 193-198*
 - VPN encryption licenses, 136
 - PKCS#10 (Public-Key Cryptography Standard #10), 506**
 - PKCS#7 (Public-Key Cryptography Standard #7), 506**
 - planning IPsec security policy, 544**
 - compatibility of IPsec with ACLs, verifying, 550
 - connectivity of network, testing, 549
 - IKE phase 1 details, identifying, 544-545
 - IKE phase 2 details, identifying, 547-548
 - validity of current policies, verifying, 548-549
 - planning phase (PDIOO), 82**
 - policy identification, 40**
 - policy maps, configuring, 404-406**
 - policy server (NAC), 237**
 - policy-map command, 401**
 - port forwarding on WebVPN, configuring, 651-652, 657-659**
 - port redirection, 29-30, 175-176**
 - port-connected clients, reauthenticating, 334**
 - port-level authentication, 234**
 - ports, restricting traffic, 438-440**
 - prerequisites for CAs, 507**
 - pre-shared keys, configuring site-to-site VPN between PIX Security Appliances, 555-556, 570-578**
 - private VLANs**
 - ACLs, configuring, 449
 - vulnerabilities, 448
 - privilege levels for Cisco IOS Software, configuring, 92**
 - privileged mode (PIX Security Appliance), 140**
 - promiscuous ports, 448**
 - protecting routing table integrity, 102-104**
 - protocol inspection, 408**
 - adding to port numbers, 410
 - disabling, 409
 - DNS inspection, 428-430
 - ESMTP application inspection, configuring, 419
 - FTP inspection, 410
 - active mode, 412*
 - passive mode, 413*
 - HTTP inspection, 415
 - enhanced HTTP inspection, 415-416*
 - ICMP inspection, configuring, 420
 - RSH inspection, configuring, 417-418
 - SNMP inspection, configuring, 421-422
 - SQL*Net inspection, configuring, 418-419
 - protocol object groups, 391**
 - configuring, 393
 - proxy ARP, 99**
 - public key encryption algorithms, 498**
 - public keys, deleting from peers, 595**
-
- Q-R**
- query mode, activating, 586**
 - Quick setup, configuring site-to-site VPNs, 569**
 - R (restricted) licenses, 135**
 - RADIUS (Remote Authentication Dial-In User Service), 222**
 - access profiles, 327
 - authentication methods, 223
 - comparing with TACACS+, 223-224
 - configuring, 268-269
 - NAS, 222

RAT (Router Audit Tool), 44-45

RDBMS Synchronization feature (CS ACS), 251

RealNetworks RDT transport mode (RTSP), 424-425

reauthenticating

- on 802.1x port-based authentication, 333
- port-connected clients, 334

rebooting FWSM, 216

reconnaissance attacks, 22

- eavesdropping, 25
- counteracting, 26
- example of, 24

recovering lost passwords

- on Adaptive Security Appliance, 746-747
- on PIX Security Appliance, 745-746

Redirect messages (ICMP), protecting from exploitation, 101

remote network administration, SSH, 87

- SSH client, 88
- SSH server, 88-89

remote-access VPNs, 67, 513

removing

- CBAC configuration, 369
- object groups, 399
- security contexts, 725

replication CS ACS database, 250

Reports tab (Router MC), 696

requesting certificates, 592

requirements

- for ASDM operation, 186
- workstation requirements, 187-188
- for PIX Security Appliance failover, 727

resetting

- 802.1x configuration default values, 334
- FWSM, 216

restricting

- traffic through ports, 438-440
- web access with ACLs, 382-384

restrictions

- for Cisco Easy VPN Remote operation, 609
- on CAs, 506

restrictive security model, 8-9

reverse Telnet, disabling, 85

RIP routing, configuring on PIX Security Appliance, 198, 200

risk analysis, 5

- asset identification, 5
- threat identification, 6
- vulnerability assessment, 5

rogue DHCP servers, 444

roles defined in 802.1x authentication process, 314

root guard, 450

route command, 153-154

routed mode (FWSM), 210

Router MC, 683

- activities, 686
- building blocks, 687
- device groups, 686
- installing, 688-690
- jobs, 686
- launching, 690
- tasks, 698-699
- tunneling technologies, 687-688
- user interface, 691-693
 - Admin tab, 697*
 - Configuration tab, 694-695*
 - Deployment tab, 695*
 - Devices tab, 693*
 - Reports tab, 696*
- VPN settings and policies, 685

routers

- accessing, 84
- Cisco IOS, password protection schemes, 89-90
- IKE with pre-shared keys, configuring, 551-556
- IPsec configuration, verifying, 566-570
- IPsec with pre-shared keys, configuring, 557-565
- logging in, 85
- tty ports, securing, 85

routing table integrity, protecting, 102-104

RPC inspection, configuring on CBAC, 359-360

RSA key pairs, generating, 588

RSCG (Router Security Configuration Guide), 43

RSH inspection, configuring, 417-418

RTP transport mode (RTSP), 423-424

RTSP (Real-Time Streaming Protocol), 423

- RealNetworks RDT mode, 424-425
- standard RTP mode, 423-424

rules, configuring for authentication proxy, 280-282

S

S/Key, one-time passwords, 226

SAFE security blueprint, 74-76

SANS (SysAdmin, Audit, Network, Security) Institute, 15

SAs (security associations), 528-529

SCCP (Skinny Client Control Protocol), 427

SCEP (Simple Certificate Enrollment Protocol), 507

SDEE (Security Device Event Exchange), 470, 476

- event notification method, specifying, 477
- events, clearing, 478
- prerequisites, 477

SDFs (Signature Definition Files), 473

- attack-drop.sdf, 474

SDM (Security Device Manager), 120-121

- Cisco IOS Firewall, configuring, 369
- Factory Reset Wizard, 126-127
- Monitor mode, 127, 130
- security audit feature, 680-682
- Startup Wizard, 122-123
- user interface, 124
- VPNs, configuring, 569-570
- WAN connection, configuring, 126
- wizard options, 125

secondary text-color command, 655**secret key encryption, 496****secure ports, 330****security audit feature (SDM), 680-682****security contexts, 136, 718**

- configuration files, 720, 724
- configuring, 724
- interfaces, allocating, 723
- licenses, upgrading, 136
- multiple context mode, configuring on PIX Security Appliance, 718-722
- removing, 725

security level command, 148**security levels**

- on PIX Security Appliance, 142
- SNMP, 704

security management, 69

- auditing, 73-74
- CiscoWorks VMS, 70-72
- console ports, 84

security models, 704

- restrictive, 8-9
- closed, 10
- open, 7

security parameters of SPI, 528-529**security passwords command, syntax, 91****security policies, 6, 56**

- as network security vulnerability, 19
- developing, 57-58
- policy identification, 40
- procedures, developing, 58

security wheel

- improving security, 56
- monitoring the system, 54
- securing the system, 53
- testing phase, 55

selecting

- EAP, 320
- tunneling protocols, 517

Self-Defending Networks. *See* Cisco Self-Defending Networks**serial failover cable, 729**

- failover, configuring, 730

server-based firewalls, 64, 113**service object groups, 391**

- configuring, 393

service password encryption, 90**service password-recovery command, 91, 747****service policies, configuring, 406****service-policy command, 401****session layer inspection (CBAC), 348****SHA (Secure Hash Algorithm), 501****show commands, 155-158**

- verifying Cisco IOS IPS configuration, 478

show conn command, 178**show conn detail command, 179****show context command, 725****show crypto ca certificate command, 603****show crypto ca roots command, 596****show crypto map command, 568****show fragment command, 482****show ip dhcp snooping binding command, 444****show ip inspect command, 367****show local-host command, 180-181****show logging command, 163****show mode command, 722****show privilege level command, 744****show run access-list command, 575****show run crypto ikakmp command, 574****show running configuration command, 553****show timeout command, 182****show version command, 749****show xlate command, 181****show xlate detail command, 181****shun feature (PIX Security Appliance), configuring, 491-492****signature recognition, 232****signature-based detection, 460****signatures, 461, 473**

- attack-class, 487
- excluding from auditing, 490
- informational, 487

- SDFs, 473
 - attack-drop.sdf*, 474
 - SMEs, 474
 - SIP (Session Initiation Protocol), 426**
 - site-to-site VPNs, 67, 69, 512. *See also* Router MC**
 - between PIX Security Appliances, configuring with pre-shared keys, 570-578
 - configuring, 542, 597-601
 - configuring with SDM, 569-570
 - IPsec configuration tasks, 542-544
 - Slammer worm, 23**
 - small LAN environments, deploying Cisco Secure ACS, 325**
 - SMEs (signature micro engines), 474**
 - SMTP inspection, configuring on CBAC, 360**
 - Smurf attacks, 35-36**
 - SNMP (Simple Network Management Protocol), 105**
 - agents, 701
 - CiscoView, 706
 - commands, 702
 - disabling, 105
 - managed devices, 701
 - traps, 700
 - SNMP inspection, configuring, 421-422**
 - SNMPv3, 704**
 - applications supporting, 705
 - configuring
 - on Cisco IOS Software, 707-710*
 - on PIX Security Appliance, 710-712*
 - social engineering, 30**
 - software images**
 - downloading via TFTP, 750
 - upgrading on PIX Security Appliance, 751
 - spammers, 21**
 - SPAN destination ports, 330**
 - spanning tree attacks, mitigating, 670**
 - spanning-tree portfast command, 451**
 - special-usage keys, generating, 588**
 - specifying CA characteristics, 590**
 - speed command, 148-149**
 - SPI (Security Parameter Index), 529**
 - SQL*Net inspection, configuring, 418-419**
 - SSH (Secure Shell)**
 - managing access on PIX Security Appliance, 741-742
 - remote network administration, 87-89
 - Stacheldraht attacks, 36**
 - stateful failover, 727**
 - cabling, 729
 - stateful packet filtering, 119, 342-343**
 - static command, 173**
 - static passwords, 225**
 - static PAT, port redirection, 175-176**
 - static pat command, 176**
 - static routes, configuring, 102-104**
 - on PIX Security Appliance, 198-200
 - static translations, 173**
 - statistics for 802.1x, displaying, 335**
 - STP (Spanning Tree Protocol), 449**
 - BPDU guard, 450
 - configuring, 451*
 - manipulation, preventing, 450
 - root guard, *configuring, 450*
 - structured threats, 20**
 - SUA (Secure Unit Authentication), 647-648**
 - subnets, mapping to PAT addresses, 172**
 - supplicants, 234-314**
 - supported Cisco IOS IPS signatures, 473**
 - switch spoofing, 446**
 - switch-to-RADIUS server communication, configuring, 332-333**
 - switch ports, restricting traffic, 438-440**
 - switching, Layer 2 attacks, 436**
 - ARP spoofing, 441-442
 - DHCP starvation attacks, 444
 - MAC spoofing, 440-441
 - VLAN hopping, 446-447
 - symmetric cryptography, 496**
 - symmetric encryption, 496-497**
 - SYN cookies, configuring on PIX Security Appliance, 485-486**
 - SYN flood attacks, 32**
 - SYN Flood Guard, configuring on PIX Security Appliance, 483-484**
 - syslog, configuring on PIX Security Appliance, 161, 163**
 - system clock, configuring on Cisco IOS Software, 586**
 - system-defined PAM, configuring on CBAC, 356**
-
- ## T
- TACACS+, 220-221**
 - AAA session failures, 265
 - enabling on CS ACS, 262-264
 - verifying configuration, 265*
 - troubleshooting, 266
 - versus RADIUS, 223-224
 - Targa.c attacks, 33**
 - tasks (Router MC), 698-699**

TCP (Transmission Control Protocol), 165

- half-open connections, limiting on servers, 486
- packet filtering, 345
- packet inspection, CBAC, 348
- stateful packet filtering, 342-343
- SYN flood attacks, 32

TCP Intercept, configuring on PIX Security Appliance, 484**teardrop.c attacks, 33****technology weaknesses, 17-18****Telnet access, managing on PIX Security Appliance, 739-740****testing**

- CBAC installation, 367
 - debug commands*, 368
- connectivity on network, 549
- IPsec configuration, 566-570, 601

testing phase of security wheel, 55**TFN (Tribe Flood Network) attacks, 36****TFN2K (Tribe Flood Network 2000) attacks, 36****TFTP (Trivial File Transport Protocol), downloading software images, 750****threats**

- external, 20
- internal, 21
- structured, 20
- black hats, 21
- crackers, 21
- hackers, 21
- phishers, 21
- phreakers, 21
- spammers, 21
- unstructured, 20
- white hats, 21

three-interface firewall, applying inspection rules, 366-367**threshold values, CBAC, 347****time and date of PIX Security Appliance, configuring, 160-161****timeout values, CBAC, 347****timeouts (authentication), 291-292****title-color command, 654****token cards, 227-228**

- CS ACS user authentication, 255-256

traffic class, 403**transform sets, 576**

- configuring, 557-559
- creating for Cisco Easy VPN Remote clients, 615-617

translations, 177**transparent firewall mode (PIX Security Appliance), 733**

- ACLs, 736-737

- ARP inspection, configuring, 737
- enabling, 735

transparent firewalls, 718**transparent mode (FSWM), 210****transparent tunneling, configuring on Cisco Easy VPN Client for Windows, 626-627****transport input none command, 85****transport mode (IPsec), 526-527**

- L2TP, 576

transport protocols, 164

- TCP, 165
- UDP, 165-166

traps, 700**traversal operations, 702****Trojan horses, 23, 39****troubleshooting**

- AAA configuration on PIX Security Appliance, 304-307
- activation key upgrades, 751
- CS ACS, AAA problems, 261-262
- TACACS+, 266

true negatives, 460**true positives, 460****trunk ports, 329****trust, 69**

- exploiting, 28-29

trusted interfaces, 443**trustpoint configuration commands, 591****tty ports, securing, 85****tunnel access authentication on PIX Security Appliance, 284****tunnel groups, configuring, 572-574****tunnel interfaces, 520-521****tunnel mode (IPsec), 526-527****tunnel user authentication, 296-297****tunneling protocols, 517-519**

- GRE encapsulation, 518
- L2TP, 517
- Router MC supported technologies, 687-688

turbo ACLs, 381-382**two-interface firewall, applying inspection rules, 364-365****U****UCP (User-Changeable Passwords), 256-257****UDP (User Datagram Protocol), 165-166**

- packet filtering, 343-345
- packet inspection, CBAC, 348

UniCERT CA server, 509-510

unprivileged mode (PIX Security Appliance), 140

unqualified names, 587

unstructured threats, 20

untrusted interfaces, 443

updating virus definitions on network hosts, 63

upgrading

- PIX Security Appliance
 - license, 750-751*
 - software image, 751*
 - security context licenses, 136

UR (unrestricted) licenses, 135, 727

URL filtering, 344, 388, 390

URLs, defining in WebVPN, 656

US-CERT (United States Computer Emergency Readiness Team), 15

user accounts (Cisco Secure ACS), creating, 249-250

user interface of Router MC, 691-693

- Admin tab, 697
- Configuration tab, 694-695
- Deployment tab, 695
- Devices tab, 693
- Reports tab, 696

user-defined PAM, configuring on CBAC, 357-358

user-defined privilege levels, assigning to PIX Security Appliance commands, 744

V

validity of current IPsec policies, verifying, 548-549

vendor participation in NAC Program, 240-241

verifying

- authentication proxy configuration, 282-283
- CA support configuration, 596
- CBAC installation, 367
 - debug commands, 368*
- Cisco Easy VPN Remote configuration, 635-637
- Cisco IOS IPS configuration, 478
 - with clear commands, 478*
 - with debug commands, 478-479*
 - with show commands, 478*
- compatibility of ACLs with IPsec, 550
- IKE with pre-shared key configuration on routers, 556
- IPsec configuration, 601
- IPsec router configuration, 566-570
- PIX Security Appliance connectivity, 159-160
- port security configuration, 440
- site-to-site VPN configuration between PIX Security Appliances, 578-579
- TACACS+ configuration on Cisco Secure ACS, 265
- validity of current IPsec policies, 548-549

VeriSign OnSite CA server, 509

version information, viewing, 749

viewing

- MAC address table on PIX Security Appliance, 739
- object groups, 398
- privilege level command assignments, 744
- version information, 749

virtual contexts, 732

virtual HTTP authentication, configuring on PIX Security Appliance, 295

virtual Telnet pre-authentication, configuring on PIX Security Appliance, 294

viruses, 23, 39

- definitions, updating on network hosts, 63

VLAN hopping attacks

- double tagging, 446
- mitigating, 447, 669-671
- switch spoofing, 446

VLANs

- configuring on PIX Security Appliance, 193-194, 196-198
- support on PIX Security Appliance, 198

VMS (CiscoWorks VMS), 70-72

voice recognition, 231

VPN encryption licenses, 136

vpn-tunnel-protocol command, 655

VPNs, 66

- Cisco VPN 3000 series concentrators, 535
- Cisco IPsec VPN Services Module, 536
- Cisco VPN 3002 Hardware Client, 536
- Cisco VPN Client, 535-536
- configuring with SDM, 569-570
- IP VPNs, 66
- remote-access, 67, 513
- site-to-site, 67-69, 512
 - configuring, 542-544*
- tunneling protocols, 517-519
- WebVPN, 515
 - comparing with IPsec, 517*
 - features, 516*

vty lines, controlling, 86

vulnerabilities, 17. See also vulnerability analysis

- assessing, 5
- configuration weaknesses, 18-19
- identifying
 - Knoppix STD, 46-47*
 - Microsoft Baseline Security Analyzer, 47*
- security policy weaknesses, 19
- technology weaknesses, 17-18

vulnerability analysis

- host analysis, 45
- network analysis, 41
 - Cisco IOS XR Software*, 44
 - Cisco RAT Software*, 44-45
 - host analysis, 46
 - RSCG*, 43
- policy identification, 40

W

WAN connections, configuring with SDM, 126**warning messages, configuring on PIX Security Appliance, 163****web access, restricting with ACLs, 382, 384****web browser interface, CS ACS for Windows, 259-260****websites, URL filtering, 344, 388-390****WebVPN, 515**

- ACLs, configuring, 660-661
- comparing with IPsec, 517
- content filters, configuring, 660-661
- e-mail proxy mode, configuring, 659
- features, 516
- file access, configuring, 656
- home page, 649
- port forwarding, 651-652, 657-659
- URLs, defining, 656
- websites, accessing, 650

WebVPN

- subcommand mode, 652-653
- support, configuring on Cisco ASA, 649, 652-655

white hats, 21**wireless access, effect on network security, 13****wizard options for SDM, 125****workflow within Router MC, 698-699****workstation requirements for ASDM operation, 187-188****worms, 23, 37-38**

X-Y-Z

X.509v3 certificate support, 506**XAUTH**

- Cisco Easy VPN Remote access router client configuration, 634-635

XTACACS, 220