



Numerics

- 2F (Layer 2 Forwarding), 369
- 3DES (Triple Data Encryption Standard)
 - connections, 94

A

- AAA (authentication, authorization, and accounting), 74, 356–358
 - accounting, configuring, 366–367
 - ACS (Access Control Server), 303–305
 - applying simultaneously, 367–368
 - authorization, configuring, 364–365
 - commands, PIX firewalls, 128–129
 - dual DMZ configuration, 121, 123–134
 - NAS (Network Access Server), 334–335
 - RADIUS/TACACS+, configuring, 358–364
- aaa accounting command, 366
- aaa authentication command, 129
- aaa authentication local-override command, 361
- aaa authentication login administrative none command, 364
- aaa authentication login default tacacs+ command, 364
- aaa authentication password-prompt text-string command, 361
- aaa authorization command, 365
- aaa new-model command, 334, 359, 367
- aaa-server command, 128
- absolute command, 159
- abstracts, security blueprints for enterprise networks, 399
- access
 - back-end servers, 381
 - banners, 56
 - CBAC (context-based access control), 167
 - compatibility, 172–173
 - configuring, 173–175, 177–182
 - events, 170
 - executing, 168–170
 - protocol sessions, 172
 - dial-in, 436
 - inbound control, configuring, 450
 - Layer 3, 452
 - line, controlling, 48–49
 - NAS, configuring, 334–339
 - passwords. *See* passwords
 - Ping, 385
 - PIX firewalls, configuring, 455
 - unauthorized, 375, 470
- access control lists. *See* ACLs
- Access Control Server. *See* ACS
- access lists
 - CBAC
 - configuring interfaces, 175
 - CSIS (Cisco Secure Integrated Software), 155
 - customizing, 165
 - routers, 37–38
- Access Policy, 326
- access-class command, 48
- access-group command, 48, 130, 133
- access-list command, 130, 133, 383
- accounting, 366–367. *See also* AAA
 - ACS, 88
 - NAS, configuring, 339
 - RADIUS Accounting report, 332
 - TACACS+ Accounting report, 331
- ACLs (Access Control Lists), 53
- ACS (Access Control Server), 74, 87–88, 303
 - AAA, 304–305
 - Administration Control, 325–326
 - Backup and Restore report, 332
 - Backup option, 323
 - configuring, 313–342, 346
 - features, 303
 - installing, 310–312
 - Interface Configuration, 323–324
 - Network Configuration, 318, 321
 - Online Documentation screen, 333
 - RADIUS, 307
 - Reports and Activity screen, 330–333
 - Restore option, 323
 - Service Management option, 323
 - Service Monitoring report, 333
 - System Configuration, 321–322
 - TACACS+, 307–310
 - User and Group Setup configuration, 315
- active probes, configuring, 234
- Adaptive Security Algorithm (ASA), 98

- Address Resolution Protocol (ARP), 14, 383
- addresses (IP), 9
 - assigning, 103
 - PIX-to-PIX configuration, 150–151
 - Secure Scanner, 82
- administration
 - ACS, Web-based configuration, 313
 - alerts, 168
 - out-of-band security, 49–50
 - passwords, 45–46
 - enable password command, 46
 - enable secret command, 47
 - Policy Manager, 84, 86
 - security, 36
 - monitoring, 75
 - physical, 47–49
 - Policy Manager, 76
 - SNMP (Simple Network Management Protocol), 52–54
 - TACACS+ Administration report, 331
- Administration Control screen, ACS (Access Control Server), 325–326
- Administrative Audit report, 333
- advanced options, ACS (Access Control Server), 325
- advanced TACACS+ settings, 315
- agents, 186
- alerts, 168
- algorithms
 - ASA (Adaptive Security Algorithm), 98
 - SHA (Secure Hash Algorithm), 52
- allow automatic local login setting (ACS), 326
- analysis
 - enterprise edge (SAFE), 425
 - corporate Internet module, 426–432
 - e-commerce module, 439–443
 - options, 444
 - VPN and remote-access module, 432–437
 - WAN module, 438
 - Secure Scanner data, 232
- AppleTalk Remote Access (ARA), 310
- applets, blocking, 178
- application layer
 - attacks, 467
 - filtering, 168
- applications, 76, 470
 - ACS. *See* ACS
 - as targets (SAFE), 407–408
 - CSPM
 - features, 253–255
 - installing, 255–269
 - dictionary, 375
 - IDS (Intrusion Detection System), 79–81, 185
 - host-based, 186
 - network-based, 186–187
 - platforms, 188
 - Integrated Software, 78–79
 - layer attacks, 6
 - PIX Firewall, 77–78
 - Policy Manager, 84–86
 - Secure Scanner, 81–82
 - trojan horses, 470
 - vulnerabilities, 381
- apply command, 129–132
- applying
 - AAA, 367–368
 - access lists, 43
- ARA (AppleTalk Remote Access), 310
- architecture
 - corporate Internet module, 432
 - module concepts, 402
 - SAFE, 401–402, 404–410
 - building access module, 419–420
 - building distribution module, 417–418
 - core module, 416
 - edge distribution module, 422–423
 - future near-term goals, 416
 - server module, 420–421
 - taxonomy, 471
- ARP (Address Resolution Protocol), 14, 22., 62 383
- arp timeout commands, PIX firewalls, 107
- ASA (Adaptive Security Algorithm), 98
- assigning IP address, 103
- attacks, 375, 379, 381
 - application layer, 6, 467
 - banners, 56
 - DDoS (distributed denial of service), 406–407
 - dictionary, 47, 375
 - DoS (Denial of Service), 6, 27, 58, 377–378, 465
 - Ping attacks, 30
 - smurf attacks, 30

- SYN flood attacks, 28–29
 - TCP intercepts, 64
 - eavesdropping, 376
 - firewalls
 - configuring, 384–385
 - implementing, 381–383
 - revised problems, 385
 - IP spoofing, 463–464
 - land, 379
 - LAND.c attacks, 28–29
 - man-in-the-middle, 467
 - network intrusion, 375
 - passwords, 466–468
 - Ping, 30
 - ping of death, 378
 - port redirection, 469
 - smurf, 30, 378
 - taxonomy, 461–469
 - TCP SYN flooding, 28, 377
 - teardrop, 379
 - trojan horses, 470
 - unauthorized access, 470
 - viruses, 470
- attribute-value (AV), 306
- Audit Policy (ACS), 327
- audits
 - Administrative Audit report, 333
 - trails, 168, 180
- authentication. *See also* AAA
 - ACS, 87, 304
 - CHAP, 356
 - FTP servers, 388
 - NAS, configuring, 335–337
 - routers, 157
 - services, 9
- authentication, authorization, and accounting. *See* AAA
- authorization. *See also* AAA
 - ACS, 88
 - NAS, 337–338
 - services, 9
- automatic Telnet denial, 99
- AV (attribute-value), 306
- axioms, SAFE, 404–410

B

- back-end servers, 374, 393
 - access, 381
 - threats, 394
 - troubleshooting, 394
- bandwidth, e-commerce, 443
- banners, 56
- basic configuration, PIX firewalls, 100–107
- Berners-Lee, Tim, 386
- BGP (Border Gateway Protocol), 442
- bit buckets, 163–164
- blocking Java, 178
- blueprints
 - architecture, 401–410
 - security, 399
- bootstrap settings, 258, 264
- bootstrapping, CSPM, 267
- Border Gateway Protocol (BGP), 442
- branch-office users, 362
- Brief Technical Report (Secure Scanner), 238
- broadcasts, directed, 62
- building access module (SAFE), 419–420
- building distribution module (SAFE), 417–418
- building method lists, 360–362

C

- CAs, PIX firewalls, 147
- caches, ARP, 107
- callin keyword, 363
- capture ports, configuring, 454
- captures, data configuration, 231
- CAR (committed access rate), 428
- Cat 6000 IDS module, configuring capture ports, 454
- Catalyst 3500 XL private VLANs, 457
- caveats, SAFE operation, 400–401
- CBAC (context-based access control), 7, 155, 167
 - compatibility, 172–173
 - configuring, 173–182
 - events, 170, 172
 - executing, 168, 170
- CCO (Cisco Connection Online), 241
- CDP (Cisco Discovery Protocol), 50
- CEF (Cisco Express Forwarding), 63

- CERT (Computer Emergency Response Team), 465
- CET (Cisco Encryption Technology), 369
- Challenge Handshake Authentication Protocol (CHAP), 356, 436
- CHAP (Challenge Handshake Authentication Protocol), 356, 436
- chap keyword, 363
- Chart Wizard, 248
- charts, Secure Scanner, 237–238
- Cisco Connection Online (CCO), 241
- Cisco Discovery Protocol (CDP), 50
- Cisco Encryption Technology (CET), 369
 - CBAC compatibility, 172–173
- Cisco Express Forwarding (CEF), 63
- Cisco product family, 76
 - ACS (Access Control Server), 87–88
 - IDS (Intrusion Detection System), 79–81
 - Integrated Software, 78–79
 - PIX Firewall, 77–78
 - Policy Manager, 84, 86
 - Secure Scanner, 81–82
- Cisco Secure Database Replication option (ACS), 322
- Cisco Security Solution, 73
 - data privacy, 75
 - perimeter security, 74
 - Policy Manager, 76
 - security monitoring, 75
- clear rip commands, 127
- clear route command, 107
- clear xlate command, 105, 121
- CLI (command-line interface), 76
 - AAA, 306
 - PIX firewalls, 100
- clients
 - ACS, configuring, 313–333
 - NAS, configuring, 340–342, 346
 - VPN, 368–369
- client-server systems (CSPM), 261
- CMD.EXE command, 391
- collected data (Secure Scanner), 230–232
 - interpreting, 247–248
 - reporting, 249
- command-line interface (CLI), 76
- commands, 49, 103, 217
 - AAA, PIX firewalls, 128–129
 - aaa accounting, 366
 - aaa authentication, 129
 - aaa authentication login administrative none, 364
 - aaa authentication login default tacacs+, 364
 - aaa authentication password-prompt text-string, 361
 - aaa authentication username-prompt text-string, 361
 - aaa authentication-local override, 361
 - aaa authorization, 365
 - aaa new-model, 334, 359, 367
 - aaa-server, 128
 - absolute, 159
 - access-class, 48
 - access-group, 48, 130, 133
 - access-list, 130 133, 383
 - arp timeout, 107
 - clear rip, 127
 - clear route, 107
 - clear xlate, 105, 121
 - CMD.EXE, 391
 - conduit, 112–113, 383–385
 - copy, 107
 - Create New Session, 243
 - crypto ipsec, 142–144
 - crypto map, 140, 370
 - crypto map branchoffice 10 ipsec-isakmp, 370
 - deny, 133
 - device-specific command sets, publishing, 296–297
 - enable password, 46–47
 - enable secret, 46–47
 - enablepass, 102
 - established, 104
 - except, 131
 - EXEC, 364
 - exec-timeout, 49
 - failover, 124–127
 - filter, 119
 - fixup, 99, 116
 - fixup protocol, 116–117
 - global, 104, 110, 266
 - hostname, 116
 - interface, 103, 116
 - ip access-class, 43
 - ip access-group, 43
 - ip address, 265, 269

- ip address interface_name, 103
- ip http access-class, 51
- ip http server, 51
- ip inspect name, 177–178
- ip inspect udp idle-time, 179
- ip local pool, 135
- ip nat inside source list 1 pool nat 1, 268
- ip nat outside, 268
- ip port map, 167
- ip route, 267
- ip verify unicast reverse-path, 63
- isakmp, 145
- kerberos instance map, 365
- lin econ 0, 364
- logging, 118
- logging host, 118
- logging on, 118
- logging trap, 118
- mailhost, 111
- match address, 370
- nameif, 102, 107
- nameif hardware_id if_name security_level, 265
- nat, 105–106, 266
- nat 0, 106, 109
- no ip directed-broadcast, 62
- no ip proxy-arp, 62
- no ip source route, 63
- no ip unreachable, 60
- no logging console, 118
- no rip interface_name, 127
- no service finger, 59
- no shut, 103
- null route, 163–164
- outbound, 129–132
- pager line, 128
- password, 102
- periodic, 159
- permit, 133
- privilege exec, 49
- privilege level, 47
- radius-server host ip address, 335
- radius-server key key, 335
- reload, 367
- rip, 127
- route, 106–107, 267
- route inside, 267
- route outside, 266
- service password encryption, 46, 305
- service router-encryption, 47
- set peer, 370
- set transform-set, 370
- show access-list, 161
- show access-lists, 156
- show config, 100
- show ip audit attack, 220
- show ip audit info, 220
- show ip audit interface, 220
- show ip audit interfaces, 217
- show ip audit name, 218–220
- show rip, 127
- show static, 112
- snmp-server communityname, 53
- snmp-server trap-authentication, 53
- static, 105, 111–112
- sysopt, 137
- sysopt connection permit-pptp, 137
- tacacs-server host host ip-address, 359
- tacacs-server host ip address, 334
- tacacs-server key key, 334
- tacacs-server key serverkey, 359
- telnet, 118, 266
- threshold, 177
- timeout, 177
- udp idle timeout, 170
- vpdn, 136–137
- write, 107
- write erase, 108–110
- write floppy, 108
- write memory, 269, 331
- write standby, 125
- write terminal, 108
- committed access rate (CAR), 428
- communication, server-to-server, 381
- comparisons, RADIUS/TACACS+, 309–310
- compatibility
 - AAA, 361
 - CBAC , 172–173
- Computer Emergency Response Team (CERT), 465
- conduit command, 112–113, 383–385
- conduit statements, 113

configuration

- AAA, 334–335, 358–364
 - accounting, 339
 - ACS, 340–342, 346
 - ACS (Access Control Server), 313–333
 - User and Group Setup, 315
 - active probe, 234
 - Administration Control screen, ACS, 325–326
 - audit trails, 180
 - authentication, NAS, 335–337
 - authorization, NAS, 337–338
 - capture ports, 454
 - CBAC, 173–182
 - connections, properties, 48
 - crypto, 459
 - data capture, 231
 - databases, 329
 - default IOS firewall parameters, 450
 - DNS servers, 393
 - encrypted in-band network management, 450
 - enterprise networks, 410
 - External Users Database screen (ACS), 327–329
 - firewalls, 384–385, 437
 - FTP servers, 389
 - hosts, 449
 - HTTP (Hypertext Transfer Protocol), 51
 - IDS (Intrusion Detection System), 215–222
 - inbound access control, 450
 - Interface Configuration (ACS), 323–324
 - Internet e-mail servers, 391
 - IOS Firewall, 216–217
 - IPSec (Internet Protocol Security), 370–371
 - Layer 3
 - access, 452
 - VLAN settings, 453
 - logging trails, 180
 - NAS, 334–342, 346
 - NAT, 459
 - networks
 - ACS, 318, 321
 - topology, 270, 272–273, 281, 286
 - out-of-band security, 49–50
 - PAM (Port Application Mapping), 167
 - passwords, 45–46
 - enable password command, 46
 - enable secret command, 47
 - PIX firewalls, 100–107, 218–221
 - CAs, 147
 - dual DMZ, 121–134
 - realistic, 108–113
 - remote site, 113
 - single DMZ, 114–121
 - PIX-to-PIX, 148–149, 151
 - ports, 245
 - private VLANs, 457
 - probes, 245
 - recommended minimum IOS security settings, 57–60, 62–63
 - Reports and Activity screen, 330–333
 - routers, 446–447
 - SAFE, 401–402, 414–415
 - building access module, 452–453
 - building distribution module, 452
 - core module, 451
 - corporate Internet module, 455–457
 - edge distribution module, 454
 - management module, 450–451
 - server module, 453–454
 - validating, 445–449
 - VPN and remote access module, 457–459
 - WAN module, 460
 - Secure Scanner, 242–248
 - security policies, 291
 - sessions, 229, 244
 - SNMP, 54
 - stateful failover, 126–127
 - switches, 448
 - System Configuration (ACS), 321–322
 - VLAN mappings, 453
 - Web servers, 387
- configuration services, 51
 - confirmation, vulnerability, 233–234
 - connections, 106
 - 3DES (Triple Data Encryption Standard), 94
 - half-open, 28
 - PIX Firewall, 265
 - ports, 374
 - properties, configuring, 48
 - TCP intercepts, 64
 - VPN, 10, 368–369
 - console ports, preventing access, 48
 - contact-based access control (CBAC), 155
 - controlling line access, 48–49

Convery, Sean, 399
 copy command, 107
 core module (SAFE), 416
 corporate Internet module, 426–432
 corporate networks
 dial-in security, 353–358
 protecting, 174
 security policies, creating, 30
 Create New session command, 243
 crypto ipsec command, 142–144
 crypto map branchoffice 10 ipsec-isakmp
 command, 370
 crypto map command, 370
 crypto map commands, 140
 CSIS (Cisco Secure Integrated Software)
 access lists, 155
 configuring, 216
 dynamic access lists, 155–157
 null route command, 163–164
 PAM, 165–166
 reflexive access lists, 160–162
 time-based access lists, 158–159
 CSPM (Cisco Secure Policy Manager), 253
 bootstrapping, 267
 feature sets, 258
 features, 253–255
 hardware requirements, 256
 installing, 255–261, 263–269
 interfaces, 281
 policy enforcement points, 257
 software requirements, 256
 customizing TCP, 165
 cut-through proxies, 98

D

DARPA (U.S. Defense Advanced Research Projects Agency), 12
 data
 analysis (Secure Scanner), 232
 captures (Secure Scanner), 243–245
 collection (Secure Scanner), 230–232
 interpreting, 247–248
 presentation (Secure Scanner), 235, 238
 privacy, 75
 reporting (Secure Scanner), 249

Data Encryption Standard (DES), 52
 Database Group Mappings screen (ACS), 328
 Database Replication reports, 333
 databases
 AAA, configuring, 358–364
 configuring, 329
 External User Databases screen (ACS),
 327–329
 NSDB (Network Security Database), 235–238
 DDoS (Distributed Denial of Service) attacks, 27,
 406–407
 declarations, static, 113
 decryption, VPNs, 10
 defaults
 IDS signatures, 210
 IOS firewall parameters, configuring, 450
 defining inspection rules (CBAC), 177–178
 demilitarized zone (DMZ), 174
 demo systems (CSPM), 263
 Denial of Service (DoS) attacks, 27, 58,
 377–378, 465
 LAND.c, 28–29
 Ping, 30
 smurf, 30
 SYN flood, 28
 deny command, 133
 deny parameter, 39
 denying RFC 1918 routes, 57–58
 Department of Defense (DoD), 12
 deploying device-specific commands, 298
 DES (Data Encryption Standard), 52
 design
 building access module (SAFE), 420
 building distribution module (SAFE), 418
 core modules (SAFE), 417
 corporate Internet module, 429
 e-commerce module (enterprise edge), 441
 edge distribution module (SAFE), 424
 enterprise networks, 410
 FTP servers, 388
 SAFE, 401–402, 414–415
 server module (SAFE), 422
 VPN and remote-access module (enterprise
 edge), 435
 WAN module (enterprise edge), 438
 determining needs for network security, 461–469

devices

- CDP (Cisco Discovery Protocol), 50
- key
 - building access module (SAFE), 419
 - building distribution module (SAFE), 417
 - core module (SAFE), 417
 - corporate Internet module, 427
 - e-commerce module (enterprise edge), 439
 - edge distribution module (SAFE), 422
 - server module (SAFE), 420
 - VPN and remote access module (enterprise edge), 433
 - WAN module (enterprise edge), 438
- key (SAFE), 412
- management module, 412–416
- managing, 36
- SAFE
 - building access module, 452–453
 - building distribution module, 452
 - core module, 451
 - corporate Internet module, 455–457
 - edge distribution module, 454
 - management module, 450–451
 - server module, 453–454
 - validating, 445–449
 - VPN and remote-access module, 457–459
 - WAN module, 460
- standby, 125
- device-specific command sets, publishing, 296–297
- DHCP (Dynamic Host Configuration Protocol), support, 99
- dial-in access, 436
 - ACS (Access Control Server), 303
 - security, 353–358
- dictionary attacks, 47, 375
- directed broadcasts, 62
- Disabled Accounts report, 332
- Distributed denial of service (DDoS), 27
- distributed denial of service (DDoS) attacks, 406–407
- distributed systems (CSPM), 261
- DMZs (demilitarized zones), configuring, 174
 - dual DMZ, 121–134
 - single DMZ, 114–121

- DNS (Domain Name System), 373
 - guards, 99
 - servers, 374, 392
 - configuring, 393
 - threats, 392
 - troubleshooting, 393
- DoD (Department of Defense), 12
- Domain Name System (DNS), 373
- DoS (denial of service) attacks, 6, 58, 377–378, 465
 - Ping attacks, 30
 - smurf attacks, 30
 - SYN flood attacks, 28–29
 - TCP intercepts, 64
- dynamic access lists, CSIS, 155–157
- dynamic statements, 157

E

- eavesdropping, 376
- echoes, ICMP, 229
- e-commerce
 - firewalls, 442
 - module (enterprise edge), 439, 441–443
- edge distribution module, SAFE, 422–423
- EIGRP (Enhanced Interior Gateway Routing Protocol), 437
- EIOS-21, 450
- EIOS-23 and 24, 456
- EIOS-27 and 28, 459
- EIOS-61, 460
- EL2SW-11 and 12, 453
- EL3SW-1 and 2, 453
- EL3SW-5, 452
- e-mail. *See also* SNMP
 - guards, 99
 - servers, 374, 389
 - threats, 390
 - troubleshooting, 391
- embedded operating systems, 98
- embryonic connections, 106
- enable password command, 46
- enable secret command, 46–47
- enablepass command, 102
- Encapsulating Security Payload (ESP), 434

- encryption
 - CET, 369
 - DES, 52
 - in-band network management, configuring, 450
 - VPN, 10
- Enhanced Interior Gateway Routing Protocol (EIGRP), 437
- enterprise edge (SAFE), 425
 - corporate Internet module, 426–432
 - e-commerce module, 439–443
 - options, 444
 - VPN and remote-access module, 432–437
 - WAN module, 438
- enterprise networks, 410
 - architecture, 402–410
 - campus, 411
 - building access module, 419–420
 - building distribution module, 417–418
 - core module, 416
 - edge distribution module, 422–423
 - management module, 412–416
 - server module, 420–421
 - expected threats, 410
 - modules, 410
 - PIX 535 firewalls, 97
 - SAFE
 - audience, 400
 - block diagrams, 403
 - caveats, 400–401
 - mitigation strategies, 444–445
 - security blueprints, 399
- EPIX-31/33, configuration, 455
- EPIX-32 and 34, 458
- ESP (Encapsulating Security Payload), 434
- established command, 104
- Ethernet0 interfaces, nameif command, 102
- events
 - AAA accounting, 366
 - CBAC , 170
- except command, 131
- EXEC commands, 364
- exec-timeout 5 0 command, 49
- executing
 - AAA simultaneously, 367–368
 - Secure Scanner, 242
- Executive Summary (Secure Scanner), 238
- expected threats, 410

- exploitation
 - of services, 376
 - of trust, 469
- extended access lists, 43
- Extended Authentication (Xauth), 433
- external interfaces, 36
- External User Databases screen, ACS, 327, 329

F

- Failed Attempts report, 332
- failover
 - features, 126
 - stateful configuration, 126–127
- failover command, 124–127
- failover features, 125
- false positives, 408
- feature sets (CSPM), 258
- features
 - ACS , 303
 - CSIS, 165–166
 - CSPM, 253–255
 - failover, 125–126
 - PIX, 98–100
 - Secure Scanner, 226–239
- File Transfer Protocol (FTP), 233, 373–374
- filter command, 119
- filtering
 - application-layer, 168
 - interfaces, 454
 - perimeter security, 75
 - stateful, 98
 - URL, 119–120
- finger services, 59
- firewalls
 - AAA commands, 128–129
 - access-group commands, 133
 - access-list commands, 133
 - ACS (Access Control Server), 303
 - apply commands, 129–132
 - arp timeout commands, 107
 - conduit commands, 112–113
 - configuring, 437
 - e-commerce, 442
 - failover commands, 124–125
 - fixup commands, 116

- global commands, 104
 - implementing, 381–383
 - interface commands, 103
 - IOS Firewall, 209, 216–218
 - logging commands, 118
 - nameif commands, 102
 - nat commands, 105–106
 - outbound commands, 129–132
 - pager line commands, 128
 - password commands, 102
 - PIX, 77–78, 210–215
 - AAA commands, 128–129
 - access-group commands, 133
 - access-list commands, 133
 - apply commands, 129–132
 - CAs (Certificate Authorities), 147
 - conduit commands, 112–113
 - configuring, 100–107, 218–221
 - connecting, 265
 - dual DMZ configuration, 121–134
 - failover commands, 124–125
 - features, 98–100
 - fixup commands, 116
 - global commands, 104
 - interface commands, 103
 - logging commands, 118
 - models, 94, 96–97
 - nameif commands, 102
 - nat commands, 105–106
 - outbound commands, 129–132
 - pager line commands, 128
 - password commands, 102
 - PIX-to-PIX configuration, 148–151
 - realistic configuration, 108–113
 - remote site configuration, 113
 - rip commands, 127
 - route commands, 106–107
 - single DMZ configuration, 114–121
 - SNMP commands, 117
 - static commands, 111–112
 - telnet commands, 118
 - VON with IPSEC and manual keys, 139–144
 - VPN with PPTP, 134–138
 - VPN with preshared keys, 144–147
 - write commands, 107
 - rip commands, 127
 - route commands, 106–107
 - routers, creating temporary openings, 169
 - security policies, 383
 - services, 8–10
 - SNMP commands, 117
 - static commands, 111–112
 - static translations, 383
 - telnet commands, 118
 - write commands, 107
 - fixup command, 99, 116–117
 - flood attacks, TCP SYN, 28
 - flood defenders, 99
 - flood guards, 99
 - formats, IP header datagram, 15
 - formatting
 - building access module (SAFE), 420
 - building distribution module (SAFE), 418
 - core modules (SAFE), 417
 - corporate Internet module, 429
 - corporate security policies, 30
 - e-commerce module (enterprise edge), 441
 - edge distribution module (SAFE), 424
 - SAFE, 401–402
 - server module (SAFE), 422
 - sessions, Secure Scanner, 243–245
 - VPN and remote-access module (enterprise edge), 435
 - WAN module (enterprise edge), 438
 - fragmentation
 - inspection, 179
 - IP packet prevention, 168
 - fragmenting packets, 16
 - FTP (File Transfer Protocol), 233, 373
 - servers, 374, 388
 - configuring, 389
 - threats, 388
 - troubleshooting, 389
 - Full Technical Report (Secure Scanner), 238
 - future near-term goals, SAFE architecture, 416
- ## G
-
- generating device-specific command sets, 296–297
 - Generic Route Encapsulation (GRE), 75, 369, 433
 - global addresses, 9
 - global commands, 104, 110, 266

global timeouts, CBAC, 176–177

goals

- corporate Internet module, 432
- SAFE architecture, 416

GRE (generic route encapsulation), 75, 369, 433

green-field modular approaches, 402

grid browser (Secure Scanner,) 236

groups, User and Group Setup configuration, 315

guidelines

- design
 - building access module (SAFE), 420
 - building distribution module (SAFE), 418
 - core modules (SAFE), 417
 - corporate Internet module, 429
 - e-commerce module (enterprise edge), 441
 - edge distribution module (SAFE), 424
 - SAFE, 414–415
 - server module (SAFE), 422
 - VPN and remote-access module (enterprise edge), 435
 - WAN module (enterprise edge), 438
- SAFE implementation, 445–447, 449
 - core module, 451
 - management module, 450–451

H

half-open connections, 28

half-open sessions, 377

hardware, CSPM (Cisco Secure Policy Manager), 256

headers, IP datagram formats, 15

HIDS (host-based IDS), 407

hijacking sessions, 376

host-based IDS (Intrusion Detection System), 186, 407

hostname command, 116

hosts

- as targets (SAFE), 405
- management module, 412–413, 415–416
- network mapping, 226, 229
- SAFE configuration, 449

host-specific port mapping, 166

Hot Standby Router Protocol (HSRP), 60, 125, 456

HSRP (Hot Standby Router Protocol), 60, 125, 456

HTTP (Hypertext Transfer Protocol), 6, 51

Hypertext Transfer Protocol (HTTP), 6, 51

ICMP (Internet Control Message Protocol), 59, 384, 23–25

- deny, 99
- Echo Reply, redirect messages, 60

identical internal IP address, PIX-to-PIX configuration, 150–151

IDS (Intrusion Detection System), 76, 79–81, 185

- configuring, 215–222
- host-based, 186–188
- IOS Firewall, 209, 216–218
- monitoring, 221
- PIX Firewall, 100, 210–215, 218–221
- platforms, 209
- support, 168

IEFT (Internet Engineering Task Force), 52

IKE (Internet Key Exchange), 369, 434

IMAP4 (Internet Message Access Protocol revision 4) servers, 389

- configuring, 391
- threats, 390
- troubleshooting, 391

implementation

- building access module (SAFE), 420
- building distribution module (SAFE), 418
- core modules (SAFE), 417
- corporate Internet module, 429
- e-commerce module (enterprise edge), 441
- edge distribution module (SAFE), 424
- firewalls, 381–383
- FTP servers, 388
- SAFE
 - building access module, 452–453
 - building distribution module, 452
 - core module, 451
 - corporate Internet module, 455–457
 - edge distribution module, 454
 - implementing, 445–447, 449
 - management module, 450–451
 - server module, 453–454
 - VPN and remote-access module, 457, 459

- WAN module, 460
- server module (SAFE), 422
- VPN and remote-access module (enterprise edge), 435
- WAN module (enterprise edge), 438
- in-band network management, configuring, 450
- inbound access control, configuring, 450
- Initial Sequence Number (ISN), 26
- inspection rules
 - CBAC, defining, 177–178
 - fragmentation, 179
 - TCP, 179
 - UDP, 179
- installation
 - ACS (Access Control Server), 310–312
 - CSPM (Cisco Secure Policy Manager), 255–269
 - Secure Scanner applications, 241
- Integrated Software, 78–79. *See also* CSIS
- intercepts, TCP, 64
- interface commands, 103, 116
- interfaces, 37–45
 - ACS, configuring, 323–324
 - ARP, 22
 - CBAC
 - configuring IP access lists, 175
 - selecting, 174
 - CLI (command-line interface), 76, 100
 - filtering, 454
 - internal, 36
 - method lists, linking, 362–363
 - nameif command, 102
 - null, 6, 163–164
 - Policy Manager, 281
 - private, configuring firewalls, 437
 - public, 116
- Internet
 - e-mail servers, 374, 389
 - threats, 390
 - troubleshooting, 391
 - services, 374
 - threats, 5–6, 375, 379–381
 - configuring firewalls, 384–385
 - DoS (denial of service), 377–378
 - implementing firewalls, 381–383
 - network intrusion, 375
 - revised problems, 385
 - Internet Control Message Protocol (ICMP), 59–60, 384
 - Internet Engineering Task Force (IETF), 52
 - Internet Key Exchange (IKE), 369, 434
 - Internet Message Access Protocol revision 4 (IMAP4), 390
 - Internet Protocol Security. *See* IPSec
 - Internet Protocol. *See* IP
 - Internet Security Association and Key Management Protocol (ISAKMP), 144
 - interpreting collected data (Secure Scanner), 247–248
 - intrusion
 - Cisco Security Solution, 73–74
 - data privacy, 75
 - perimeter security, 74
 - Policy Manager, 76
 - security monitoring, 75
 - networks, 375
 - Intrusion Detection Director, 80
 - Intrusion Detection Post Office, 81
 - Intrusion Detection Sensor, 79
 - Intrusion Detection System. *See* IDS
 - IOS firewalls, 209, 216–218
 - parameters, configuring, 450
 - IP (Internet Protocol), 14, 59–60
 - access lists, configuring CBAC interfaces, 175
 - addresses
 - assigning, 103
 - PIX-to-PIX configuration, 150–151
 - Secure Scanner, 82
 - spoofing, 6
 - directed broadcasts, 62
 - header datagram format, 15
 - packet fragmentation prevention, 168
 - source routing, 63
 - spoofing, 463–464
 - ip access-class command, 43
 - ip access-group command, 43
 - ip address a.a.a.a.m.m.m.m command, 269
 - ip address command, 103
 - ip address int_name a.a.a.a m.m.m.m command, 265
 - ip address interface_name ip_address subnet_mask command, 103
 - IP Frag Guard, 99
 - ip http access-class command, 51
 - ip http server command, 51

ip inspect name command, 177–178
 ip inspect udp idle-time command, 179
 ip local pool command, 135
 ip nat inside source list 1 pool nat1 command, 268
 ip nat outside command, 268
 ip port-map command, 167
 ip route 0.0.0.0.0.0.0 a.a.a.a command, 267
 ip route 0.0.0.0.0.0.0 212.1.157.1 command, 267
 ip route command, 267
 ip verify unicast reverse-path command, 63
 IPSec (Internet Protocol Security), 75

- CBAC compatibility, 172–173
- configuring, 370–371
- VPN with manual keys, 139–144

 ISAKMP (Internet Security Association and Key Management Protocol), 144
 isakmp commands, 145
 ISN (Initial Sequence Number), 26
 ISP (Internet service provider), PIX 535 firewalls, 97

J-K

Java, blocking, 178

kerberos instance map command, 365
 key devices

- building access module (SAFE), 419
- building distribution module (SAFE), 417
- core module (SAFE), 417
- corporate Internet module, 427
- e-commerce module (enterprise edge), 439
- edge distribution module (SAFE), 422
- SAFE, 412
- server module (SAFE), 420
- VPN and remote access module (enterprise edge), 433
- WAN module (enterprise edge), 438

keywords

- callin, 363
- chap, 363
- nornadomseq, 106
- pap, 363
- protocols, 178

L

L2TP (Layer 2 Tunneling Protocol), 75, 369
 LANs, directed broadcasts, 62
 land attacks, 379
 Layer 2 Forwarding (L2F), 369
 Layer 2 Tunneling Protocol (L2TP), 75, 369
 Layer 3 access, 452
 line access, controlling, 48–49
 line con 0 command, 364
 linking method lists, 362–363
 lists

- access. *See* access lists
- method
 - building, 360–362
 - linking, 362–363

 local-ip parameter, 105
 Logged-In Users report, 332
 logging, 409–410

- accounting, 306
- trails, configuring, 180

 logging commands, PIX firewalls, 118
 logging host command, 118
 logging on command, 118
 Logging option (ACS), 322
 logging trap command, 118
 login authentication administrative command, 364

M

mail, guards, 99
 mail exchange (MX), 392
 mailhost command, 111
 management

- alerts, 168
- module, 412–416
- OOB (out-of-band), 409
- passwords, 45–46
 - enable password command, 46
 - enable secret command, 47
- Policy Manager, 84, 86
- security, 36, 409–410
 - monitoring, 75
 - out-of-band, 49–50

- physical, 47–49
- Policy Manager, 76
- SNMP, 52–54
- Management Information Base (MIB), 117
- man-in-the-middle attacks, 467
- manual keys, VPN with IPSec, 139–140, 142–144
- mapping
 - network, 226, 229
 - PAM (Port Application Mapping). *See* PAM
 - VLANs, 453
- masks, wildcard, 40–42
- match address command, 370
- max connections parameter, 106
- maximum transmission unit (MTU), 15
- messages, redirect, 60
- method lists
 - building, 360–362
 - linking, 362–363
- methods of authentication, 336
- metric parameter, 107
- MIBs (Management Information Bases), 117
- minimum hardware requirements, CSPM, 256
- mitigating
 - strategies (SAFE), 444–445
- mitigating threats
 - enterprise edge
 - corporate Internet module, 428
 - e-commerce module, 440
 - VPN and remote access module, 434
 - WAN module, 438
 - SAFE, 413
 - building access module, 419
 - building distribution module, 418
 - core module, 417
 - edge distribution module, 423
 - server module, 421
- models, PIX, 94, 96–97
 - PIX 506, 94
 - PIX 515, 95–96
 - PIX 520/525, 96
 - PIX 535, 97
- module concepts
 - SAFE, 402
- modules, 410
 - enterprise campus, 411
 - building access, 419–420
 - building distribution, 417–418

- core, 416
- edge distribution, 422–423
- management module, 412–416
- server, 420–421
- enterprise edge (SAFE), 425
 - corporate Internet module, 426–432
 - e-commerce module, 439–443
 - options, 444
 - VPN and remote-access module, 432–437
 - WAN module, 438
- monitoring, 75
 - ACS Service Monitoring report, 333
 - IDS, 221
- MTU (maximum transmission unit), 15
- multiple dial-in entry points, 354
- multiple ports, CBAC (context-based access control), 167
 - compatibility, 172–173
 - configuring, 173–175, 177–182
 - events, 170
 - executing, 168, 170
 - protocol sessions, 172
- multiple static commands, 113
- MX (mail exchange), 392

N

- named access lists, 45
- nameif command, 102, 107
- nameif hardware_id if_name security_level command, 265
- NAS (network access servers), 303
 - configuring, 334–342, 346
- NASI (Novell Asynchronous Services Interface), 310
- NAT (Network Address Translation), 57, 382
 - configuration, 459
 - PIX firewalls, 98
- nat 0 command, 106, 109
- nat command, 105–106, 266
- nat statements, 113
- navigation, Secure Scanner, 235, 238
- near-term architecture goals, corporate Internet module, 432
- netmask parameter, 105

- network access servers (NAS), 303
 - Network Address Translation. *See* NAT
 - Network Configuration, ACS, 318, 321
 - network IDS (network IDS), 407
 - Network Security Database (NSDB), 235, 238
 - Network Time Protocol (NTP), 55
 - Network Topology Wizard, 273
 - network-based IDS (Intrusion Detection System), 186–187
 - networks
 - AAA (authentication, authorization, and accounting), 356–358
 - as targets (SAFE), 406–407
 - attack taxonomy, 461–469
 - Cisco Security Solution, 73–74
 - data privacy, 75
 - perimeter security, 74
 - Policy Manager, 76
 - security monitoring, 75
 - corporate
 - dial-in security, 353, 355
 - protecting, 174
 - eavesdropping, 376
 - enterprise
 - architecture, 401–410
 - expected threats, 410
 - mitigation strategies, 444–445
 - modules, 410
 - SAFE, 400–401
 - security blueprints, 399
 - intrusion, 375
 - management, configuring encrypted inband, 450
 - NTP (Network Time Protocol), 55
 - PIX firewalls, features, 98–100
 - PSTN, 74, 458
 - reconnaissance, 468
 - Secure Scanner
 - configuring, 242–248
 - data analysis, 232
 - data collection, 230–232
 - data presentation, 235, 238
 - features, 226, 229–239
 - installing, 241
 - network mapping, 226, 229
 - reporting, 238
 - vulnerability confirmation, 233–234
 - security, 6
 - authorization services, 9
 - decryption services, 10
 - determining needs, 461–469
 - encryption services, 10
 - firewall services, 8
 - NAT services, 9
 - proxy services, 11
 - router services, 6–7
 - simple hosted, 219
 - SNMP, 52–54
 - threats, 385
 - topology, configuring, 270, 272–273, 281, 286
 - NIDS (network IDS), 407
 - no ip directed-broadcast command, 62
 - no ip proxy-arp command, 62
 - no ip source-route command, 63
 - no ip unreachable command, 60
 - no logging console command, 118
 - no rip interface_name default command, 127
 - no rip interface_name passive command, 127
 - no service finger command, 59
 - no shut command, 103
 - norandomseq keyword, 106
 - Novell Asynchronous Services Interface (NASI), 310
 - NSDB (Network Security Database), 235, 238
 - NTP (Network Time Protocol), 55
 - null interfaces, 6
 - null route command, 163–164
-
- O**
-
- ODBC (Open Database Connectivity), 304
 - Online Documentation screen (ACS), 333
 - OOB (out-of-band), 409
 - Open Database Connectivity (ODBC), 304
 - open relay, 390
 - Open Relay Behavior-modification System (ORBS), 390
 - Open System Interconnection (OSI), 13
 - operating systems
 - PIX firewalls, 98–100
 - vulnerabilities, 381
 - optimizing AAA, 364

options

- CSPM installations, 260
 - enterprise, 444
- ORBS (Open Relay Behavior-modification System), 390
- OSI (Open System Interconnection), 13
- outbound command, 129–132
- outgoing_src parameter, 131
- out-of-band (OOB), 409
 - security, 49–50P-Q

P-Q

packets

- access lists, 37–38
 - directed broadcasts, 62
 - extended access lists, 43
 - fragmenting, 16
 - named access lists, 45
 - routing, 14
 - sniffers, 6, 417, 462
 - standard access lists, 39, 42–43
- pager line commands, 128
- PAM (Port Application Mapping), CSIS, 165–166
- pap keyword, 363
- parameters
- crypto map mapname, 140
 - default IOS firewalls, configuring, 450
 - deny, 39
 - local_ip, 105
 - max connections, 106
 - metric, 107
 - netmask, 105
 - outbound command, 130
 - outgoing_src, 131
 - permit, 39
 - rip commands, 127
- password command, 102
- Password Validation option (ACS), 322
- passwords
- attacks, 466–468
 - eavesdropping, 376
 - enable password command, 46
 - enable secret command, 47
 - managing, 45–46
- PAT (Port Address Translation), 98, 282, 383

- perimeter security, 74
- periodic command, 159
- permit parameter, 39
- permit statements, 112, 133
- physical security, 47–49
- ping, 228, 385
- ping of death attacks, 378
- PIX (Private Internet Exchange), 74, 77–78, 210–221
 - access, configuring, 455
 - CAs, 147
 - configuration, 100–107
 - connecting, 265
 - dual DMZ configuration, 121–134
 - features, 98, 100
 - models, 94, 96–97
 - PIX 506, 94
 - PIX 515, 95–96
 - PIX 520/525, 96
 - PIX 535, 97
 - PIX-to-PIX configuration, 148–151
 - realistic configuration, 108–113
 - remote site configuration, 113
 - single DMZ configuration, 114–121
 - static translations, 383
 - VPN with IPsec and manual keys, 139–144
 - VPN with PPTP, 134–138
 - VPN with preshared keys, 144–147
- plain old telephone service (POTS), 353
- planning CSPM installations, 257–262
- platforms, IDS, 188, 209
- Point-to-Point Protocol (PPP), 356, 436
- policies
 - corporate security, 30
 - firewall security, 383
 - security, 470
 - configuring, 291
 - unknown users, 327
- Policy Administrator (CSPM), 259
- policy enforcement points, 257, 264
- Policy Manager, 76, 84–86. *See also* CSPM interfaces, 281
- Policy Monitor (CSPM), 259
- Policy Proxy (CSPM), 259
- Policy Proxy-Monitor (CSPM), 260
- Policy Server (CSPM), 259

- POP3 (Post Office Protocol Version 3), 390–391
 - servers, 389
- Port Address Translation (PAT), 282–383
- ports, 374
 - access, preventing, 48
 - capture, configuring, 454
 - CBAC, 167
 - compatibility, 172–173
 - configuring, 173–182
 - events, 170
 - executing, 168–170
 - protocol sessions, 172
 - configuration settings, 245
 - customizing, 165
 - redirection, 469
 - scans, 6, 230
- Post Office Protocol Version 3 (POP3), 390
- POTS (plain old telephone service), 353
- PPP (Point-to-Point Protocol), 356, 436
- PPTP (Point-to-Point Tunneling Protocol), 134–138
- preshared keys, VPN, 144–147
- prevention
 - console ports, accessing, 48
 - IP packet fragmentation, 168
- private addresses, 9
- private interfaces, configuring, 437
- Private Internet Exchange (PIX), 74
- privilege exec command, 49
- privilege level command, 47
- probes, configuration settings, 245
- procedures, CSPM installations, 264–268
- products, 76
 - ACS (Access Control Server), 87–88
 - IDS (Intrusion Detection System), 79–81
 - Integrated Software, 78–79
 - PIX Firewall, 77–78
 - Policy Manager, 84, 86
 - SAFE implementation, 449
 - Secure Scanner, 81–82
- protection
 - Cisco Security Solution, 73–74
 - data privacy, 75
 - perimeter security, 74
 - Policy Manager, 76
 - security monitoring, 75
 - corporate networks, 174
- IDS, 185
 - configuring, 215–222
 - host-based, 186
 - IOS Firewall, 209, 216–218
 - network-based, 186–187
 - PIX Firewall, 210–221
 - platforms, 188, 209
- protocols, 233
 - access lists, 37
 - ACS (Access Control Server), 307–310
 - ARA (AppleTalk Remote Access), 310
 - ARP (Address Resolution Protocol), 14, 22, 62, 383
 - BGP (Border Gateway Protocol), 442
 - CBAC (context-based access control), 172
 - CDP (Cisco Discovery Protocol), 50
 - CHAP (Challenge Handshake Authentication Protocol), 356, 436
 - EIGRP (Enhanced Interior Gateway Routing Protocol), 437
 - FTP (File Transfer Protocol), 373
 - HSRP (Hot Standby Router Protocol), 60, 125, 456
 - HTTP (Hypertext Transfer Protocol), 6, 51
 - ICMP (Internet Control Message Protocol), 23–25, 59–60, 384
 - IP (Internet Protocol), 14
 - ISAKMP (Internet Security Association and Key Management Protocol), 144
 - keywords, 178
 - L2TP (Layer 2 Tunneling Protocol), 75, 369
 - NTP (Network Time Protocol), 55
 - PPP (Point-to-Point Protocol), 356, 436
 - PPTP (Point-to-Point Tunneling Protocol), 134–138
 - RARP (reverse address resolution protocol), 14
 - SLIP (Serial Line Internet Protocol), 356
 - SMTP (Simple Mail Transfer Protocol), 390
 - SNMP (Simple Network Management Protocol), 52–54
 - TCP (Transmission Control Protocol), 25–26, 58, 308
 - TFTP (Trivial File Transfer Protocol), 410
 - UDP (User Datagram Protocol), 27, 58, 308, 374
- Proxy Address Resolution Protocol (ARP), 62

PSTN (Public Switched Telephone Network),
74, 458
public addresses, 9
public interfaces, 116
Public Switched Telephone Network (PSTN),
74, 458
publishing, device-specific command sets, 296–297

R

R&D (research and development), 418
RADIUS (Remote Access Dial-In User Service), 74
AAA, configuring, 358–364
ACS, 307–310, 325
RADIUS Accounting report, 332
radius-serve host ip address command, 335
radius-server key key command, 335
RARP (reverse address resolution protocol), 14, 22
read-only (RO), 117
realistic configuration, PIX firewalls, 108–113
recommended minimum IOS security settings,
57–63
reconnaissance, networks, 468
redirect messages, 60
redirection, ports, 469
reflexive access lists, CSIS, 160–162. See also
access lists
reload command, 367
Remote Access Dial-In User Service (RADIUS), 74
Remote Shell (RSH), 233
reporting, 409–410
collected data (Secure Scanner), 249
Secure Scanner, 84, 238
reports
accounting, 306
ACS Backup and Restore, 332
ACS Service Monitoring, 333
Administrative Audit, 333
Database Replication, 333
Disabled Accounts, 332
Failed Attempts, 332
Logged-In Users, 332
RADIUS Accounting, 332
TACACS+ Accounting, 331
TACACS+ Administration, 331
Reports and Activity screen, ACS, 330–333
requirements, CSPM hardware/software, 256–257
research and development (R&D), 418
restricting traffic, 229
reverse address resolution protocol (RARP), 14
revised problems, Internet service security, 385
RFC 172, 388
RFC 791, 63
RFC 1918, 57–58
rip commands, 127
RO (read-only), 117
round-robin load balancing, 392
route command, 106–107, 267
route inside command, 267
route outside command, 266
route statements, 121
routers, 14
access lists, 37–38
as targets (SAFE), 404
authentication, 157
banners, 56
basic configuration, PIX firewalls, 101
CEF, 63
extended access lists, 43
finger services, 59
firewalls, creating temporary openings, 169
interfaces
access lists, 37–38
extended access lists, 43
named access lists, 45
standard access lists, 39–43
IP source routing, 63
named access lists, 45
physical security, 47–49
RADIUS, configuring, 358
recommended minimum IOS security settings,
57–63
SAFE configuration, 446–447
services, 6–7
standard access lists, 39, 42–43
TACACS+, configuring, 358
VPN traffic, 435
RSH (Remote Shell), 233
rules of inspection, CBAC, 177–178

S

SAs (Security Associations), 94

SAFE

- abstract, 399
- architecture, 401–410, 416
- audience, 400
- axioms, 404–410
- caveats, 400–401
- design guidelines, 414–415
- enterprise campus, 411
 - building access module, 419–420
 - building distribution module, 417–418
 - core module, 416
 - edge distribution module, 422–423
 - enterprise module, 412–416
 - server module, 420–421
- enterprise edge, 425
 - corporate Internet module, 426–432
 - e-commerce module, 439–443
 - options, 444
 - VPN and remote-access module, 432–437
 - WAN module, 438
- mitigation strategies, 444–445
- validating, 445–447, 449
 - building access module, 452–453
 - building distribution module, 452
 - core module, 451
 - corporate Internet module, 455–457
 - edge distribution module, 454
 - management module, 450–451
 - server module, 453–454
 - VPN and remote-access module, 457–459
 - WAN module, 460

saving policies, 296–297

scalability, host-based IDS, 186

scanning

- ports, 6, 230
- Secure Scanner, 81–82, 245
 - configuring, 242–248
 - features, 226, 229–239
 - installing, 241

script kiddies, 377

Secure Hash Algorithm (SHA), 52

Secure Scanner, 81–82

- configuring, 242–248
- data analysis, 232

data collection, 230–232

data presentation, 235, 238

features, 226–239

installing, 241

network mapping, 226, 229

reporting, 238

vulnerability confirmation, 233–234

security

blueprints, 399

- audience, 400
- caveats, 400–401

dial-in, 353–358

firewalls

- configuring private interfaces, 437
- e-commerce, 442
- PIX-to-PIX configuration, 148–151
- policies, 383
- VPN with PPTP, 134–138

management, 36, 409–410

mitigation strategies (SAFE), 444–445

module concepts, 402

monitoring, 75

networks, 6

- authentication services, 9
- authorization services, 9
- decryption services, 10
- determining needs, 461–469
- encryption services, 10
- firewall services, 8
- NAT services, 9
- proxy, 11
- router services, 6–7

out-of-band, 49–50

physical, 47–49

PIX firewalls

- CAs (Certificate Authorities), 147
- configuring, 100–107
- dual DMZ, 121–134
- features, 98–100
- models, 94–97
- realistic configuration, 108–113
- remote site, 113
- single DMZ, 114–121

policies, 470

- configuring, 291
- creating, 30

recommended minimum IOS settings, 57–63

- reporting, 409–410
- TCP/IP, 12–22
- threats, 375, 379–381
 - configuring firewalls, 384–385
 - DoS (denial of service), 377–378
 - implementing firewalls, 381–383
 - network intrusion, 375
 - revised problems, 385
- Security Associations (SAs), 94
- selection
 - CBAC interfaces, 174
 - passwords, 45–46
- sensors, Intrusion Detection Sensor, 79
- sequence random numbering, 98
- Serial Line Internet Protocol (SLIP), 356
- server module (SAFE), 420–421
- servers
 - ACS (Access Control Server), 74, 87–88
 - configuring, 340–342, 346
 - configuring), 313–315, 318, 321–326, 329, 332–333
 - features, 303
 - back-end, 374, 393
 - access, 381
 - threats, 394
 - troubleshooting, 394
 - DNS, 373–374, 392
 - configuring, 393
 - threats, 392
 - troubleshooting, 393
 - FTP, 388
 - configuring, 389
 - threats, 388
 - troubleshooting, 389
 - Internet e-mail, 374, 389
 - configuring, 391
 - threats, 390
 - troubleshooting, 391
 - NAS (network access server), 303
 - configuring, 334–339
 - TCP (Transmission Control Protocol), 58
 - Web, 374, 386
 - configuring, 387
 - threats, 387
- server-to-server communication, 381
- Service Control option (ACS), 322
- service password-encryption command, 46, 305
- service router-encryption command, 47
- services, 59, 338
 - ACS Service Monitoring report, 333
 - authentication, 9
 - authorization, 9
 - decryption, 10
 - eavesdropping, 376
 - encryption, 10
 - exploitation of, 376
 - firewalls, 8
 - HTTP (Hypertext Transfer Protocol), 51
 - Internet, 374
 - NAT, 9
 - PAM (Port Application Mapping), 165
 - POTS (plain old telephone service), 353
 - proxy, 11
 - routers, 6–7
- Session Policy (ACS), 326
- sessions
 - configuring, 229
 - half-open, 377
 - hijacking, 376
 - replay attacks, 376
 - Secure Scanner, creating, 243
- set peer command, 370
- set transform-set command, 370
- SHA (Secure Hash Algorithm), 52
- show, 49
- show access-list commands, 156, 161
- show commands, 49
- show config command, 100
- show ip audit attack command, 220
- show ip audit configuration, 217
- show ip audit configuration command, 217
- show ip audit info command, 220
- show ip audit interface command, 220
- show ip audit interfaces command, 217
- show ip audit name command, 218, 220
- show rip command, 127
- show static command, 112
- shunning, 76
- signatures, attacks, 468
- simple hosted networks, 219
- Simple Mail Transfer Protocol (SMTP), 390
- Simple Network Management Protocol. See SNMP
- site-to-site VPNs, 436
 - crypto configuration, 459

- SLIP (Serial Line Internet Protocol), 356
- SMTP (Simple Mail Transfer Protocol), 390
 - servers, 389
 - configuring, 391
 - threats, 390
 - troubleshooting, 391
- smurf attacks, 377–378
- sniffing, 6, 417, 462
 - eavesdropping, 376
- SNMP (Simple Network Management Protocol), 52–54, 117
- snmp-server communityname command, 53
- snmp-server enable traps snmp authentication md5 command, 53
- snmp-server trap-authentication command, 53
- social engineering, 375
- software
 - CSPM, 256, 264
 - dictionary, 375
 - vulnerabilities, 381
- solutions
 - back-end servers, 394
 - DNS servers, 393
 - FTP servers, 389
 - Internet e-mail, 391
 - Web servers, 387
- source routing, IP, 63
- sources, parameters, 39
- spammers, 390
- spoofing (IP), 6, 463–464
- SQL (Structured Query Language), 442
- SSH (Secure Shell), 99
- standalone systems (CSPM), 260
- standard access lists, 39, 42–43
- standby devices, 125
- starting Secure Scanner, 242
- stateful failover configuration, 126–127
- stateful filtering, 98
- stateful inspection, 382
- statements
 - apply, 131
 - conduit, 113
 - dynamic, 157
 - nat, 113
 - periodic, 159
 - permit, 112, 133
 - route, 121
 - static command, 105, 111–112
 - static declarations, 113
 - static NAT, configuring, 459
 - static translations, 383
 - strategies, mitigating SAFE, 444–445
 - Structured Query Language (SQL), 442
 - subnets, Layer 3 access, 452
 - support
 - DHCP, 99
 - dial-in security, 353–355
 - IDS, 168
 - SSH, 99
 - switches
 - as targets, 404–405
 - SAFE configuration, 448
 - SYN flood attacks, 28
 - synchronization, NTP, 55
 - sysopt command, 137
 - sysopt connection permit-pptp command, 137
 - System Configuration, ACS , 321–322
 - system-defined port mapping, 165

T

- TACACS+ (Terminal Access Controller Access Control System Plus), 74
 - AAA, configuring, 358–364
 - Accounting Report, 331
 - ACS, 307–310, 324
 - Administration report, 331
 - advanced settings, 315
- tacacs-server host ip address command, 334, 359
- tacacs-server key key command, 334
- tacacs-server key serverkey command, 359
- targets
 - applications as, 407–408
 - hosts as, 405
 - networks as, 406–407
 - routers as, 404
 - switches as, 404–405
- taxonomy
 - architecture, 471
 - network attacks, 461–469

TCP (Transmission Control Protocol), 25–26, 165, 308

- inspecting, 179
- intercepts, 64, 100
- SYN flooding attacks, 377

TCP/IP

- ARP (Address Resoluton Protocol), 22
- ICMP (Internet Control Message Protocol), 123–25
- security, 12–22
- UDP (User Datagram Protocol), 27

teardrop attacks, 379

telnet commands, 118, 266

temporary openings, creating, 169

Terminal Access Controller Access Control System Plus. *See* TACACS+

TFN (Tribe Flood Network), 465

TFN2K (Tribe Flood Network 2000), 465

TFTP (Trivial File Transfer Protocol), 410

threats, 5–6, 375, 379–381

- back-end servers, 394
- building access module (SAFE), 419
- building distribution module (SAFE), 418
- core module (SAFE), 417
- corporate Internet module (enterprise edge), 428
- DNS servers, 392
- DoS, 377–378
- e-commerce module (enterprise edge), 440
- edge distribution module (SAFE), 423
- expected, 410
- firewalls
 - configuring, 384–385
 - implementing, 381–383
 - revised problems, 385
- FTP servers, 388
- Internet e-mail servers, 390
- mitigated (SAFE), 413
- network intrusion, 375, 385
- server module (SAFE), 421
- VPN and remote access module (enterprise edge), 434
- WAN module (enterprise edge), 438
- Web servers, 387

thresholds, CBAC, 176–177

time, NTP (Network Time Protocol), 55

time-based access lists, 158–159

timeouts, CBAC, 176–177

tools, 76

topologies, configuring, 270–273, 281, 286

traffic

- eavesdropping, 376
- e-commerce, 439
- restricting, 229
- VPN and remote-access module (enterprise edge), 435

trails

- audits, 168, 180
- logging, 180

Transmission Control Protocol (TCP), 58, 308

Tribe Flood Network (TFN), 465

Tribe Flood Network 2000 (TFN2K), 465

Triple Data Encryption Standards (3DES) connections, 94

Trivial File Transfer Protocols (TFTP), 410

trojan horses, 6, 470

troubleshooting

- back-end servers, 394
- DNS servers, 393
- Internet e-mail servers, 391
- Web server threats, 387

Trudel, Bernie, 399

trust exploitation, 469

tunneling, GRE (Generic Routing Encapsulation), 369

U

U.S. Defense Advanced Research Projects (DARPA), 12

UDP (User Datagram Protocol), 27, 58, 308, 374

- customizing, 165
- inspecting, 179

udp idle timeout command, 170

unauthorized access, 375, 470

- Cisco Security Solution, 73–74
 - data privacy, 75
 - perimeter security, 74
 - security monitoring, 75

- UNIX, installing ACS, 310–312
- unknown user policy, 327
- unreachables, 59–60
- updating policies, 296–297
- URLs (uniform resource locators), filtering, 119–120
- User and Group Setup configuration (ACS), 315
- User Data Configuration screen (ACS), 324
- User Datagram Protocol (UDP), 58, 308, 374
- user-defined port mapping, 166
- users
 - branch-office, 362
 - dial-in access, 436
 - External User Databases screen (ACS), 327–329
 - finger services, 59
 - unknown user policy, 327
- utilities, Policy Manager, 76

V

- validation, SAFE, 445–447, 449
 - building access module, 452–453
 - building distribution module, 452
 - core module, 451
 - corporate Internet module, 455–457
 - cVPN and remote-access module, 457, 459
 - edge distribution module, 454
 - management module, 450–451
 - server module, 453–454
 - WAN module, 460
- Virtual Private Dial-up Network (VPDN), 369
- Virtual Private Network (VPN), 368
- viruses, 470
- VLANs (virtual LANs)
 - Layer 2 settings, 453
 - mappings, 453
 - private, configuring, 457
- VPDN (Virtual Private Dial-up Network), 369
- vpdn commands, 136
- vpdn enable interface command, 136
- vpdn enable outside command, 136
- vpdn group 1 client authentication local command, 137
- vpdn group 1 ppp authentication mschap command, 136

- VPN and remote-access module, 432–437
- VPNs (virtual private networks), 10, 368–369
 - IPSec with manual keys, 139–144
 - PPTP, 134–138
 - preshared keys, 144–147
 - site-to-site, 436
 - traffic, 435
- vulnerabilities
 - applications, 381
 - confirmation, 233–234
 - IP source routing, 63
 - operating systems, 381

W-X-Y-Z

- WAN module (enterprise edge), 438
- war-dialers, 411
- Web
 - ACS configuration, 313–333
 - servers, 374, 386
 - configuring, 387
 - threats, 387
 - threats, 5–6, 375, 379, 381
 - configuring firewalls, 384–385
 - DoS (denial of service), 377–378
 - implementing firewalls, 381–383
 - network intrusion, 375
 - revised problems, 385
- wildcard masks, 40–42
- Windows, installing ACS (Access Control Server), 310–312
- wizards
 - Chart, 248
 - Network Topology, 273
- write commands, 107
- write erase command, 108
- write floppy command, 108
- write memory command, 269, 331
- write rease command, 110
- write standby command, 108, 125
- write terminal command, 108

Xauth (Extended Authentication), 433