



## Symbols

---

## Numerics

---

3DES (Triple DES) encryption algorithm, 526

## A

---

AAA (authentication, authorization, and accounting) architecture, 111, 157, 408–412  
 access traffic, 112  
 accounting, 112, 126–127  
   configuring, 168  
 authentication, 111  
   CHAP (Challenge Handshake Authentication Protocol), 121–122, 124–125  
   methods, 114–125  
   PAP (Password Authentication Protocol), 121–125  
   passwords, 114–117  
   S/Key, 117–120  
   token cards, 120  
   token servers, 120  
   usernames, 114, 116–117  
 authentication profiles, configuring, 163  
 authorization, 111  
   configuring, 166  
 character-mode traffic, 113  
 configuring, 205  
   debugging, 169  
 enabling, 205  
 local security databases, 127  
 NAS (Network Access Server), 158–174  
   globally enabling, 162  
   privileged EXEC (enable) mode, 160  
 network access  
   securing, 111–114

  packet-mode traffic, 114  
 PIX Firewall, configuring, 401–412  
 remote security databases, 128–130  
   CiscoSecure ACS, 148  
   Kerberos, 142–151  
   RADIUS, 136–142  
   standards, 130–151  
   TACACS+, 131–136  
   security servers, 127–151  
 aaa authentication command, 197, 199  
 aaa authentication login command, 147  
 aaa authentication ppp command, 146  
 AAA configuration commands, 199  
 aaa new-model command, 159, 197  
 Acceptable Use Policy, 696–697  
 access  
   administrative interfaces, console, 70–76  
   HTTP, controlling, 95–96  
   perimeter routers, controlling, 234–237  
   physical access, securing, 69–70  
   securing, AAA architecture, 111–114  
   SNMP, controlling, 81–86  
   Telnet, controlling, 80–81  
 access lists  
   configuring, 713  
   verifying, 734–735  
   IP access lists, extended IP access lists, 714–734  
   named IP access lists, 735–737  
   references, 106  
   SNMP, 85  
 access traffic, AAA architecture, 112  
 access-list command, 552, 716, 722  
 access-list icmp command, 725  
 access-list tcp command, 728  
 access-list udp command, 730  
 accounting, AAA architecture, 112, 126–127, 168  
 Adaptive Security Algorithm. *See* ASA (Adaptive Security Algorithm)  
 administration  
   Cisco IOS Firewall, 277–279

- CSNT, 192, 194–195
- administrative interfaces
  - banner messages, setting, 79–80
  - console, access security, 70–76
  - password encryption, 73
  - privilege levels, setting multiple, 77–78
  - securing, 70–86
  - SNMP, access control, 81–86
  - Telnet, access control, 80–81
- Advanced PIX Firewall, configuring, 443–447
- AH (Authentication Header) encryption
  - algorithm, 525, 527
  - IPSec, 527–528
- alias command, 359
- AppleTalk Remote Access Protocol. *See* ARAP (AppleTalk Remote Access Protocol)
- application gateways, firewalls, 229
- application layer encryption, 458
- applications, encryption, 456
- apply, 661
- apply command, 323, 359, 419
- ARAP (AppleTalk Remote Access Protocol), 114, 180
  - packet-mode traffic, 114
- ASA (Adaptive Security Algorithm), 292–296
- Ascend, RADIUS, 137
- assumes, 552
- attacks
  - initial access, 24
  - password attacks, 24
  - remote-access services, 24
  - secondary access, 24
  - session hijacking, 31
  - session replays, 31
- attributes, RADIUS, 140
- audit trails, Cisco IOS Firewall, 261
- audits, 46
- authentication, 111
  - AAA architecture, 114–125
    - CHAP (Challenge Handsahke Authentication Protocol), 121–125
    - PAP, 122–125

- PAP (Password Authentication Protocol), 121
  - passwords, 114, 116–117
  - S/Key, 117–120
  - token cards, 120
  - token servers, 120
  - usernames, 114–117
- CAs, 658
- guidelines, 697
- IPSec
  - configuring, 565–593
  - RSA-encrypted nonces, 594–603
- PPP, Kerberos, 145
- routing protocols, 86–90
- Authentication Header. *See* AH (Authentication Header) encryption
- authentication profiles, AAA, configuring, 163
- authentication proxy, Cisco IOS Firewall, 260
- authentication, authorization, and accounting architecture. *See* AAA (authentication, authorization, and accounting) architecture
- authorization, 111
  - AAA architecture, 125–126
- Axent token card servers, 188

## B-C

---

- Baltimore Technologies, VPNs, 552
- banner command, 79
- banner messages, setting, 79–80
- bastion hosts, perimeter security, 228
- branch offices, policies, 700
- ca enroll command, 663
- CA support
  - configuring, 648–670
  - planning for, 648
- ca zeroize rsa command, 673
- Campus Access Policy, 698
- campuses, security, 67–69
- CAs
  - authenticating, 658
  - declaring, 654

- interoperability, managing, 667
- IPSec, 548–552
- PIX Firewall, configuring, 645–673
- routers, configuring, 645–673
- standards, 550
- case studies, network security, 48–60
- CBAC (Context-Based Access Control), 259
  - Cisco IOS Firewall, 260–264
    - configuring, 266–277
    - memory, 265
    - performance, 265
    - restrictions, 264–265
  - debugging, 277
  - global timeouts, configuring, 268–271
  - inspection rules
    - applying, 276
    - defining, 271–276
  - interfaces, choosing, 266
  - IP access lists, configuring, 267
  - monitoring, 276
  - testing, 276–277
  - thresholds, configuring, 268–271
  - verifying, 276–277
- CBAC (context-based access control)
  - perimeter routers, 226
- Certificate Revocation Lists. *See* CRLs (Certificate Revocation Lists)
- CET (Cisco Encryption Technology), 241, 453, 471–479
  - configuration procedures job aid, 512
  - configuring, 479–505, 510
  - crypto engines, 471–473
  - cryptosystems, forming, 460–468
  - data integrity, 453–460
  - designing, 508–509
  - diagnosing, 505–507
  - DSS keys
    - generating, 480–483
    - sending from passive side, 486
  - DSS public keys
    - accepting, 486
    - authenticating, 486
    - exchanging, 483–490
  - encryption
    - testing, 499–505
    - verifying, 499–505
  - encryption export policy, 511
  - encryption job aid, planning for, 511–512
  - encryption solutions, 453–460
  - exchange connections
    - enabling from active side, 485
    - enabling from passive side, 484
  - global encryption policies, defining, 490–493
  - implementing, 508–510
  - network layer encryption, 459
  - per-session encryption policy, configuring, 493–498
  - references, 469
  - troubleshooting, 505–507
- CHAP (Challenge Handshake Authentication Protocol), 114
  - AAA architecture, 121–125
- character-mode traffic, AAA architecture, 113
- circuit-level gateways, firewalls, 229
- Cisco, 137
- Cisco ConfigMaker, 259, 278
- Cisco Encryption Technology. *See* CET (Cisco Encryption Technology)
- Cisco IOS crypto engine, 472
- Cisco IOS Firewall, 259
  - administration, 277–279
  - audit trails, 261
  - authentication proxy, 260
  - CBAC, 260–264
    - configuring, 266–277
    - memory, 265
    - performance, 265
    - restrictions, 264–265
  - configuring, 260–262, 280–284
  - DoS (denial of eervice), 260
  - dynamic port mapping, 261
  - event logging, 261
  - features, 260–261
  - firewalls, managing, 261
  - IDS (Intrusion Detection System), 262

- intrusion detection, 260
- IPSec encryption, 261
- Java applet blocking, 261
- NAT (network address translation), 261
- peer router authentication, 261
- planning, 263–265
- QoS (Quality of Service), 261
- real-time alerts, 261
- security, problems, 259–260
- time-based access lists, 261
- VPNs (virtual private networks), 261
- Cisco IOS Firewall feature set, 226
- Cisco IOS firewalls, 230
- Cisco IOS Security Configuration Guide, 125, 474, 478
- Cisco PIX firewalls, 230
- CiscoSecure ACS, CSNT, system requirements, 185
- CiscoSecure ACS (Access Control Server), 177
  - CSNT (CiscoSecure ACS for NT), 178–195
    - administering, 192–195
    - architecture, 185–188
    - features, 181–185
    - installing, 190–191
    - token card support, 188–189
    - troubleshooting, 192–195
  - CSUNIX (CiscoSecure ACS 2.3 for UNIX), 195–197
    - features, 196–197
    - system requirements, 197
- operating systems, 177–178
- RADIUS
  - configuring, 205–210
  - support, 178
  - testing, 208–210
  - troubleshooting, 208–210
- remote security databases, 148
- TACACS+
  - configuring, 197–205
  - debugging, 202–204
  - support, 178
- CiscoSecure ACS for NT. *See* CSNT (CiscoSecure ACS for NT)
- CiscoSecure ACS for UNIX, 150
- CiscoSecure GRS, 151
- CiscoSecure Integrated Software. *See* CSIS (CiscoSecure Integrated Software)
- CiscoSecure PIX 515, 520, 305–307
- clear arp command, 326
- clear commands, 586
- clear configure primary command, 313
- clear ip permit command, 99
- clear xlate command, 391
- CLI (command-line interface), 311–314
- command syntax, ICMP, 725
- commands, 166
  - aaa authentication, 197, 199
  - aaa authentication login, 147
  - aaa authentication ppp, 146
  - aaa new-model, 159, 197
  - access-list, 552, 716, 722
  - access-list icmp, 725
  - access-list tcp, 728
  - access-list udp, 730
  - alias, 359
  - apply, 323, 359, 419
  - banner, 79
  - ca enroll, 663
  - ca zeroize rsa, 673
  - clear, 586
  - clear arp, 326
  - clear configure primary, 313
  - clear ip permit, 99
  - clear xlate, 391
  - conduit, 298, 359, 362, 364–365, 392–396
  - config-isakmp, keywords, 568
  - configure terminal, 313
  - connect, 147
  - copy rcp, 148
  - copy running-config startup-config, 481
  - crypto ca, 553
  - crypto ca enroll, 661
  - crypto ca identity, 655

- crypto gen-signature-keys, 481
- crypto ipsec transform-set, 552
- crypto isakmp, 553
  - crypto isakmp enable, 567
  - crypto isakmp policy, 553
  - crypto key generate dss, 481
  - crypto key generate rsa, 653
  - crypto key pubkey-chain rsa, 598
  - crypto key zeroize dss, 505
  - crypto key zeroize rsa, 672
  - crypto key-timeout, 497
- crypto map, 541, 553, 630
  - crypto map local-address, 661
  - crypto pregen-dh-pairs, 498
- debug, 169, 193, 586
  - debug aaa, 169
  - debug crypto ca, 673
  - debug crypto pki, 672
  - debug icmp trace, 327, 353
  - debug ip icmp, 353
  - debug ip packet, 353
  - debug packet, 327
- disable, 313
- enable, 161, 313
  - enable password, 74, 312
  - enable secret, 75, 160
- encryption, 161
- esp-md5-hmac, 574
- esp-sha-hmac, 574
- established, 354
- exec-timeout, 76
- extended IP access lists, 722, 724–725
- failover active, 433
- failover reset, 433
- fixup, 426
  - fixup protocol, 366–367
- flash, 442
- global, 310, 320–325, 340, 359, 386–391
- hostname, 596, 651
- IKE, 587
- interface, 310
  - interface type number, 244
- ip access-group, 713
  - ip address, 310
  - ip domain-name, 650
  - ip host, 651
  - ip http access-class, 96
  - ip http authentication, 96
  - ip nat inside, 244
  - ip nat outside, 244
  - ip route, 233
  - ip tcp intercept, 240
  - isakmp policy, 638
  - key chain, 88
  - kill, 313
  - link, 435
  - linkpath, 435
  - log, 717
  - logging message, 427
  - logging trap debugging, 247
  - login local, 237
  - login tacacs, 237
  - mailhost, 359
  - MD5, 88
  - nameif, 298, 310, 387, 391
  - nat, 310, 320–325, 342, 359, 386–391
  - nat 0, 344
  - netmask, 341, 388
  - no ca enroll, 663
  - no ca identity, 673
  - no cdp enable, 232
  - no cdp run, 231
  - no crypto ca identity, 672
  - no crypto map, 505
  - no debug all, 277
  - no ip bootp server, 231
  - no ip directed-broadcast, 232
  - no ip domain-lookup, 230
  - no ip identd, 231
  - no ip mroute-cache, 231
  - no ip proxy-arp, 231
  - no ip rcpm rcp-enable, 231
  - no ip redirects, 231
  - no ip route-cache, 231
  - no ip rsh-enable, 231
  - no ip source-route, 231

- no ip tcp path-mtu-discovery, 231
- no ip tcp selective-ack, 231
- no ip unreachable, 231
- no mop enabled, 231
- no service finger, 230
- no service tcp-small-servers, 230
- no service udp-small-servers, 230
- norandomseq, 342
- outbound, 323, 419
- outside, 342
- overload, 246
- password-encryption, 161
- ping, 14, 327, 365, 566
- PIX Firewall, 317–325
- rcp, 21
- rlogin, 21, 148
- route, 300
- route inside, 301
- rsh, 21, 148
- serverfarm, 383
- service, 161
- service password-encryption, 73
- service timestamps, 247
- services password-encryption, 160
- set enablepass, 97
- set ip permit disable, 99
- set ip permit enable, 99
- set port security, 98
- show, 391, 566, 586
- show arp, 326
- show ca certificate, 672
- show ca configure, 672
- show ca identity, 672
- show ca mypubkey rsa, 672
- show conn, 391
- show crypto ca certificates, 671
- show crypto cisco algorithms, 491
- show crypto isakmp policy, 566
- show crypto key mypubkey, 671
- show crypto key mypubkey dss, 481
- show crypto map, 555, 566
- show ip address, 325
- show isakmp, 555
- show isakmp policy, 555
- show nat, 391
- show port, 98
- show running-config, 73, 232
- show tcp intercept connections, 240
- show tcp intercept statistics, 240
- show version, 307
- show xlate, 391
- snmp-server, 429
- snmp-server community, 84
- standard IP access lists, 716–718
- static, 298, 300, 340, 356–359, 392–394
- tacacs-server host, 197
- tacacs-server key, 197
- telnet, 148, 384, 388
- test crypto initiate-session, 499–500
- tftp, 442
- timeout xlate, 390
- traceroute, 300, 388
- undebg all, 277
- url-cache, 426
- write, 310
- write memory, 391, 434
- write standby, 434
- write terminal, 73, 555, 566
- xlate, 368
- community strings, SNMP, 84
- compliance requirements, 697
- Computer Oracle and Password System. *See* COPS (Computer Oracle and Password System)
- conduit command, 298, 359–365, 392–396
- conduits, PIX Firewall, inbound access, 296–303
- config-isakmp command, keywords, 568
- ConfigMaker, 278
- configuration
  - AAA, 205
    - accounting, 168
    - authentication profiles, 163
    - authorization, 166
    - debugging, 169
  - access lists, 713

- verifying, 734–735
- CA support, 648–670
  - PIX Firewall, 645–673
  - routers, 645–673
- CET (Cisco Encryption Technology), 479–505, 510
  - per-session encryption policy, 493–498
- Cisco IOS Firewall, 260–262, 280–284
  - CBAC, 266–277
- dynamic crypto maps, 673
- dynamic NAT, 244
- general access lists, 712
- IKE Mode Configuration, 676
  - IPSec, 670
  - preshared keys, 567, 613
  - references, 608
  - RSA-encrypted nonces, 602
  - verifying, 618–619
- IP access lists, 705–738
  - extended IP access lists, 720–734
  - standard IP access lists, 714–720
- IPSec
  - encryption task overview, 554–558
  - PIX Firewall, 619
  - preparing, 566, 594–602
  - preshared keys, 565–593, 603–606
  - references, 608
  - RSA-encrypted nonces, 594–603
  - security association lifetime, 626–628
  - testing, 636–638
  - verification, 636–638
  - verifying, 634–635
  - Xauth (Extended Authentication), 678
- NAS AAA, 158–170
- PAT, 246
- perimeter routers, 248–254
- PIX Firewall, 310, 330–335
  - AAA (authentication, authorization, and accounting) server, 401–407
  - commands, 391
  - failover, 430–433
  - FTP, 426–428
  - inside interfaces, 386–391
  - IPSec, 611–638
  - Java applet blocking, 422–423
  - multiple interface access, 381–401
  - multiple interfaces, 408–412
  - NAT 0, 417–418
  - outbound access control, 339–355
  - outside to DMZ, 392–394
  - PPTP (Point-to-Point Tunneling Protocol), 437–439
  - secured bidirectional communication, 375–378
  - SNMP (Simple Network Management Protocol), 428–430
  - Syslog Server, 396–400
  - testing, 325–330
  - URL filtering, 423–425
  - URL logging, 426–428
  - user authentication, 401–407
  - VPNs, 434–439
  - preshared keys, 616–618
- RADIUS, CiscoSecure ACS, 205–210
- SNMP agent, 84
- TACACS+
  - AAA configuration caommands, 199
  - CiscoSecure ACS, 197–205
- transform sets, 624–627
- VPNs (virtual private networks),
  - verification, 671–672
- Configuration Fundamentals Configuration Guide, 89
- configuration procedures job aid, CET (Cisco Encryption Technology), 512
- configure terminal command, 313
- connect command, 147
- connections, PIX Firewall, licensing, 391
- console, administrative interface, access security, 70–76
- Context-Based Access Control. *See* CBAC (Context-Based Access Control)
- COPS (Computer Oracle and Password System), 47
- copy rcv command, 148



copy running-config startup-config command, 481

credentials, Kerberos, 144

CRLs (Certificate Revocation Lists), 551  
requesting, 667

crypto access lists, creating, 620, 622–624

crypto ca command, 553

crypto ca enroll command, 661

crypto ca identity command, 655

crypto engines  
CET (Cisco Encryption Technology), 471–473  
Cisco IOS, 472  
ESA (Encryption Service Adapter) crypto engine, 471  
VIP2 (Versatile Interface Processor), 471

crypto gen-signature-keys command, 481

crypto ipsec transform-set command, 552

crypto isakmp command, 553

crypto isakmp enable command, 567

crypto isakmp policy command, 553

crypto key generate dss command, 481

crypto key generate rsa command, 653

crypto key pubkey-chain rsa command, 598

crypto key zeroize dss command, 505

crypto key zeroize rsa command, 672

crypto key-timeout command, 497

crypto map command, 541, 553, 630

crypto map local-address command, 661

crypto maps  
creating, 628–633  
dynamic crypto maps, configuring, 673  
interfaces, applying to, 633–634

crypto pregen-dh-pairs command, 498

CryptoCard token card server, CSNT, 188–189

cryptosystems, forming, 460, 462–468

CSIS (CiscoSecure Integrated Software), 259

CSNT (CiscoSecure ACS for NT), 178–195  
administering, 192–195  
architecture, 185–188  
features, 181–185  
installing, 190–191  
system requirements, 185

token cards, support, 188–189  
troubleshooting, 192–195

CSPM (CiscoSecure Policy Manager), PIX Firewall, 439

CSUNIX (CiscoSecure ACS 2.3 for UNIX), 195–197  
features, 196–197  
system requirements, 197

cut-through user authentication, PIX Firewall, 301, 303

## D

Data Encryption Standard. *See* DES (Data Encryption Standard)

data integrity  
CET (Cisco Encryption Technology), 453–460  
encryption, 454

data link layer encryption, 459

data manipulation threats, 30–32

data transfers, IPSec, 527

DDoS attacks, preventing, 238

debug aaa commands, 169

debug command, 193

debug commands, 169, 586

debug crypto ca command, 673

debug crypto pki command, 672

debug icmp trace command, 327, 353

debug ip icmp command, 353

debug ip packet command, 353

debug packet command, 327

debugging  
AAA configuration, 169  
CBAC, 277  
TACACS+, 202–204

defining, global encryption policies, CET, 490–493

demilitarized zone. *See* DMZ (demilitarized zone)

Denial of Service. *See* DoS (denial of service)

departments

- DES (Data Encryption Standard) encryption
    - algorithm, 462–464, 526, 535
    - IPSec, 535–537
  - designing, CET (Cisco Encryption Technology), 508–509
  - device banner messages, setting, 79–80
  - DHCP (Dynamic Host Configuration Protocol), 52
  - diagnosis, CET (Cisco Encryption Technology), 505–507
  - dialup access, XYZ Company network scenario, 688
  - Diffie-Hellman Key agreement, IPSec, 541–543
  - Diffie-Hellman Key exchange, 467–468
  - Digital Encryption Standard. *See* DES (Digital Encryption Standard)
  - Digital Signature Standard. *See* DSS (Digital Signature Standard)
  - disable command, 313
  - disabling IKE, 613
  - DMZ (demilitarized zone), 223, 228
    - firewalls, 381
    - PIX Firewall, 385
      - configuring, 392–394
  - DNS (domain name system), references, 389
  - DNS and BIND, 389
  - DNS Guard, PIX Firewall, 370–374
  - DoS (denial of service)
    - attacks, preventing, 237–240
      - Cisco IOS Firewall, 260
      - PIX Firewall, 370–374
    - threats, 24–25, 27–29
  - Double Authentication
    - PPP sessions, 210–212
    - prerequisites, 212
  - DSS (Digital Signature Standard), 465–466, 476
  - DSS keys, generating, CET, 480–483
  - DSS public keys, exchanging, CET, 483–490
  - dual-homed hosts, 228
  - dynamic crypto maps, configuring, 673
  - Dynamic Host Configuration Protocol, 52
  - Dynamic NAT, 340
    - configuring, 244
  - dynamic port mapping, Cisco IOS Firewall, 261
- ## E
- 
- eavesdropping, 17
  - ECRA (Export Compliance and Regulatory Affairs), 511
  - EIGRP, MD5 authentication, 88
  - enable command, 161, 313
  - enable password command, 74, 312
  - enable secret command, 75, 160
  - enabling IKE, 613
  - Encapsulating Security Payload. *See* ESP (Encapsulating Security Payload)
  - enciphering. *See* encryption
  - encrypted sessions
    - establishing, 477
    - terminating, 478
  - encryptio algorithms, IPSec, 525
  - encryption, 454–456
    - alternatives, 458
    - application layer encryption, 458
    - applications, 456
    - CET (Cisco Encryption Technology), 471–479
      - configuration procedures job aid, 512
      - configuring, 479–505, 510
      - crypto engines, 471–473
      - cryptosystems, 460–468
      - designing, 508–509
      - diagnosing, 505–507
      - DSS keys, 480–483
      - DSS public keys, 483–490
      - encryption export policy, 511
      - encryption job aid, 511–512
      - global encryption policies, 490–493
      - implementing, 508–510
      - testing, 499–505

- troubleshooting, 505–507
- verification, 499–505
- CET (Cisco Encryption Technology), 453–460
- cryptosystems, forming, 460–468
- data integrity, 454
- data link layer encryption, 459
- data privacy, 454
- DES (Digital Encryption Standard), 462–464
- Diffie-Hellman Key exchange, 467–468
- DSS (Digital Signature Standard), 465–466
- encrypted sessions, 477
  - terminating, 478
- MD5 (Message Digest 5), 464
- network layer encryption, 459, 474
- nonrepudiation, 455
- passwords, administrative interfaces, 73
- planning, 474
- policies, 700
- references, 469
- encryption command, 161
- encryption export policy, CET (Cisco Encryption Technology), 511
- encryption job aid, CET (Cisco Encryption Technology), planning for, 511–512
- encryption task overview (IPSec), configuring, 554–558
- Entrust Technologies, VPNs, 552
- equipment security, 699
- errors, standard IP access lists, 719
- ESA (Encryption Service Adapter) crypto engine, 471
- ESP (Encapsulating Security Payload), 526, 529
  - IPSec, 529–535
- ESP HMAC, 529
- esp-md5-hmac command, 574
- esp-sha-hmac command, 574
- established command, 354

- Ethernet switches
  - management access, controlling, 97
  - port security, 97
  - references, 106
  - securing, 97–99
- event logging, Cisco IOS Firewall, 261
- events, perimeter routers, logging, 247
- exec-timeout command, 76
- exploitation, 14
- Extended Authentication. *See* Xauth
- extended IP access lists
  - commands, 722–725
  - configuring, 705–738
  - location, 732
  - processing, 721–722
- extranets, policies, 700

---

## F

- failover, PIX Firewall, configuring, 430–433
- failover active command, 433
- failover reset command, 433
- filtering ICMP messages, PIX Firewall, 395–396
- filters
  - incoming network filters, 93
  - traffic control, 91–92
- fine-tuning passwords, line parameters, 76
- firewalls, 698
  - application gateways, 229
  - circuit-level gateways, 229
  - Cisco IOS firewalls, 230
  - Cisco PIX firewalls, 230
  - DMZ (demilitarized zone), 381
  - packet filters, 229
  - perimeter security, 229
  - proxy servers, 229
  - see also*, Cisco IOS Firewall and PIX Firewall
- fixup commands, 426
- fixup protocol command, 366–367

flash command, 442  
 FTP, PIX Firewall, configuring, 426–428

## G-H

general access lists, configuring, 712  
 global command, 310, 340–359  
   inside interfaces, configuring, 386–391  
 global commands, PIX Firewall, 320–325  
 global encryption policies, CET, defining, 490–493  
 global IPSec security association lifetime, configuring, 626–628  
 global timeouts, CBAC, configuring, 268–271  
 GRE (Generic Routing Encapsulation), 520  
 Hashed Message Authentication Codes, 543–545  
 hashes, 88  
 HMACs (Hashed Message Authentication Codes), 543–545  
 home access, policies, 700  
 hostname command, 596, 651  
 HSRP (Hot Standby Router Protocol), 430  
 HTTP (Hypertext Transport Protocol), access, controlling, 95–96

## I

ibound packet filtering, 234–235  
 ICMP  
   command syntax, 725  
   messages, names, 725, 727–728  
 ICMP messages, PIX Firewall, filtering, 395–396  
 Identification and Authentication Policy, 697  
 IDS (Intrusion Detection System)  
   Cisco IOS Firewall, 262, 701  
 IETF, RADIUS, 137  
 IKE (Internet Key Exchange), 537, 550  
   commands, 587  
   configuring  
     IPSec, 670

    preshared keys, 567, 613  
     references, 608  
     RSA-encrypted nonces, 602  
     verifying, 618–619  
   disabling, 613  
   enabling, 613  
   IOS software, 552–553  
   IPSec, 537–541  
   policies, creating, 613, 615  
 IKE Mode Configuration, 676  
 IKE Phase 1 (IPSec), 524  
 IKE Phase 2 (IPSec), 525  
 implementation, CET (Cisco Encryption Technology), 508–510  
 inbound access, PIX Firewall, 296–303  
 inbound access control, PIX Firewall, 351–354  
 Incident Response Procedure, 701  
 incident-handling procedures, 700–703  
 incoming network filters, 93  
 inform requests, SNMP notifications, 83  
 information theft, 17  
 initial access attacks, 24  
 inside global addresses, NAT, 243  
 inside hosts  
   access control, PIX Firewall, 356–374  
   PIX Firewall  
     DNS Guard, 370–374  
     DoS (denial of service), 370–374  
     ping access, 369–370  
     static translation, 356–368  
 inside interfaces, PIX Firewall, 385  
   configuring, 386–391  
 inside local addresses, NAT, 243  
 inspection rules, CBAC  
   applying, 276  
   defining, 271–276  
 installation, CSNT, 190–191  
 intended audiences, security policies, 693  
 interface command, 310  
 interface type number command, 244  
 interfaces, CBAC  
   choosing, 266  
   commands, PIX Firewall, 317–320

- crypto maps, applying, 633–634
- naming, 383
- PIX Firewall, 307–309
  - configuring, 392–394, 408–412
  - DMZ interfaces, 392–394
  - inside interfaces, 386–391
  - security, 314–317
- security levels, 384
- Internet access, XYZ Company network
  - scenario, 689
- Internet Access Policy, 698
- Internet Key Exchange. *See* IKE (Internet Key Exchange)
- interoperability, CAs, managing, 667
- intrusion detection, Cisco IOS Firewall, 260
- Intrusion Detection Software (Intrusion Detection Software), 262, 701
- IOS software
  - IKE, 552–553
  - IPSec, 552–553
- IP access lists
  - CBAC, configuring, 267
  - configuring, 705–738
  - extended IP access lists, configuring, 720–734
  - standard IP access lists, configuring, 714–720
  - wildcard masks, 711–712
- ip access-group command, 713
- ip address command, 310
- IP addresses, managing, perimeter routers, 242–246
- IP addressing, 706–707
  - network classes, 707–708
  - subnet addresses, 708–710
- ip domain-name command, 650
- ip host command, 651
- ip http access-class command, 96
- ip http authentication command, 96
- ip nat inside command, 244
- ip nat outside command, 244
- ip route command, 233
- IP spoofing, 31
- ip tcp intercept command, 240
- IPSec, 520–527
  - AH (Authentication Header), 527–528
  - CAs, 548–552
  - configuring
    - PIX Firewall, 619
    - preparing, 566, 594–602
    - preshared keys, 565–593, 603–606
    - references, 608
    - RSA-encrypted nonces, 594–603
    - testing, 636–638
    - verification, 634–638
  - data transfers, 527
  - DES (Data Encryption Standard), 535–537
  - Diffie-Hellman Key agreement, 541–543
  - encryption algorithms, support, 525
  - encryption task overview, configuring, 554–558
  - equipment infrastructure, 522
  - ESP (Encapsulating Security Payload), 529–535
  - features, 520
  - HMACs (Hashed Message Authentication Codes), 543–545
  - IKE (Internet Key Exchange), 537–541, 670
  - IKE Phase 1, 524
  - IKE Phase 2, 525
  - IOS software, 552–553
  - network-layer encryption, 242
  - PIX Firewall
    - configuring, 611–638
    - preparing, 612
    - preshared keys, 638–639, 641
  - PKI (Public Key Infrastructure), 548–552
  - process initiation, 523
  - RSA security, 546–548
  - security association lifetime, configuring, 626–628
  - security associations, 521–522
  - standards, 561
  - technologies, 527–548

- testing, 586–588, 590–593
- tunnel termination, 527
- verifying, 586–593
- VPNs, securing, 519–520
- Xauth (Extended Authentication)
  - configuring, 678
- IPSec encryption, Cisco IOS Firewall, 261
- isakmp policy command, 638
- isolation LAN. *See* DMZ (demilitarized zone)
- issues, security, reasons, 6–13

## J-K

---

- Java applet blocking, PIX Firewall,
  - configuring, 422–423
- KDC (key distribution center), 142–144
- Kerberized, 144
- Kerberos
  - authentication, PPP, 145
  - components, 143
  - credentials, 144
  - features, 143
  - generic authentication, 145
  - KDC (key distribution center), 142–144
  - Kerberized, 144
  - KINIT, 144
  - login authentication, 146
  - operations, 145
  - realms, 144
  - remote security databases, 142–151
  - service credentials, 145
  - terminology, 144
  - TGT (Ticket Granting Ticket), 145
- key chain command, 88
- key distribution center, 142–144
- keywords, config-isakmp command, 568
- kill command, 313
- KINIT, Kerberos, 144

## L

---

- L2F (Layer 2 Forwarding), 520
- L2TP (Layer 2 Tunneling Protocol), 520
- licensing, PIX Firewall, connections, 391
- line parameters, passwords, fine-tuning, 76
- link command, 435
- linkpath command, 435
- local authentication, local security databases, 128
- local security databases
  - AAA architecture, 127
  - local authentication, 128
- locations
  - extended IP access lists, 732
  - standard IP access lists, 718–719
- lock-and-key security, perimeter routers, 235–237
- log command, 717
- logging events, perimeter routers, 247
- logging message command, 427
- logging trap debugging command, 247
- login local command, 237
- login tacacs command, 237

## M

---

- Mail Guard, PIX Firewall, configuring, 366
- mailhost command, 359
- Management Information Bases, 81
- MCNS (Managing Cisco Network Security)
  - course, 687
- MD5 (Message Digest 5) encryption
  - algorithm, 464, 526
  - EIGRP, 88
  - routing protocols, 88
- md5 command, 88
- memory usage, managing, 650
- messages, ICMP, names, 725, 727–728
- MIBs (Management Information Bases), 81
- Microsoft Dial-Up Networking Configuration Screen, 438

- Microsoft Point-to-Point Encryption, 520
- Microsoft Windows 2000 Certificate Services 5.0, VPNs, 552
- mobile computing, policies, 699
- models, PIX Firewall, 305–307
- monitoring security, 45
- MPPE (Microsoft Point-to-Point Encryption), 520
- multimedia applications, PIX Firewall, 354–355
- multiple interfaces, PIX Firewall, access configuration, 381–401

## N

---

- named IP access lists, 735–737
- nameif command, 298, 310, 387, 391
- naming interfaces, 383
- NAS (Network Access Server), 157, 177
  - AAA (authentication, authorization, and accounting) security, 158–174
    - globally enabling, 162
    - privileged EXEC (enable) mode, 160
- NASI (NetWare Access Server Interface), 114
  - packet-mode traffic, 114
- NAT (Network Address Translation), 242, 261, 339
  - Cisco IOS Firewall, 261
  - configuring
    - nat 0 configuration, 344–347
    - outbound access control, 341–344
  - Dynamic NAT, 244, 340
  - IP addresses, managing, 242–246
  - overloading, 245
  - PAT (Port Address Translation), 340, 347–349
  - PIX Firewall, 340–344
  - Static NAT, 340
  - terminology, 243
- nat 0 command, 344, 417–418
- nat command, 310, 342, 359
- NetBIOS, PIX Firewall, 349–350
- netmask command, 341, 388
- NetWare Access Server Interface. *See* NAS (NetWare Access Server Interface)
- Network Access Server. *See* NAS (Network Access Server)
- Network Address Translation. *See* NAT (Network Address Translation)
- network classes, IP addressing, 707–708
- network layer encryption, 459
- network security policies, analyzing, 42–43
- network snooping, 17
- network-layer encryption, 474
  - IPSec, 242
  - perimeter routers, 241–242
- networks
  - access, securing, 111–114
  - protecting, importance of, 39–40
  - security, case studies, 48–60
  - suppressing, 92–93
- NICs (network interface cards), PIX Firewall, 308–309
- no ca enroll command, 663
- no ca identity command, 673
- no cdp enable command, 232
- no cdp run command, 231
- no crypto ca identity command, 672
- no crypto map command, 505
- no debug all command, 277
- no ip bootp server command, 231
- no ip directed-broadcast command, 232
- no ip domain-lookup command, 230
- no ip identd command, 231
- no ip mroute-cache command, 231
- no ip proxy-arp command, 231
- no ip rcmd rcp-enable command, 231
- no ip redirects command, 231
- no ip route-cache command, 231
- no ip rsh-enable command, 231
- no ip source-route command, 231
- no ip tcp path-mtu-discovery command, 231
- no ip tcp selective-ack command, 231

- no ip unreachable command, 231
- no mop enabled command, 231
- no service finger command, 230
- no service tcp-small-servers command, 230
- no service udp-small-servers command, 230
- nonprivileged access, SNMP, 84
- nonrepudiation, encryption, 455
- nonvolatile random-access memory, 75
- norandomseq command, 342
- notifications, SNMP, 83
- NVRAM (nonvolatile random-access memory), 75

## O

- operating systems, CiscoSecure ACS, 177–178
- outbound access control, PIX Firewall, 339–355
  - NAT (Network Address Translation), 341–344
- outbound command, 323, 419
- outbound packet filtering, 235
- outbound access, PIX Firewall, controlling, 419–422
- outside command, 342
- outside global addresses, NAT, 243
- outside interfaces, PIX Firewall, 385
  - configuring, 392–394
- outside local addresses, NAT, 243
- overload command, 246
- overloading, NAT, 245

## P

- packet filtering
  - firewalls, 229
  - inbound packet filtering, 234–235
  - outbound packet filtering, 235
- packet mode traffic, AAA, 114
- packet sniffing, 17
- packet-capturing utilities, 17

- PAP (Password Authentication Protocol), 52, 114, 180
  - AAA architecture, 121–125
- password attacks, 24
- Password Authentication Protocol. *See* PAP (Password Authentication Protocol)
- password-based attacks, 20
- password-encryption command, 161
- passwords
  - authentication, AAA architecture, 114, 116–117
  - encryption, administrative interfaces, 73
  - line parameters, fine-tuning, 76
  - management guidelines, 697
  - recovering, PIX Firewall, 440
- PAT (Port Address Translation), 242, 339
  - configuring, 246
  - IP addresses, managing, 242–246
  - NAT (Network Address Translation), 340, 347–349
- peer router authentication, Cisco IOS Firewall, 261
- perimeter routers, 224–228
  - access, controlling, 234–237
  - CBAC (context-based access control), 226
  - Cisco IOS Firewall feature set, 226
  - configuring, 248, 250, 252–254
  - DMZ (demilitarized zone), 228
  - DoS attacks, preventing, 237–240
  - events, logging, 247
  - features, 225
  - inbound packet filtering, 234–235
  - IP addresses, managing, 242–246
  - lock-and-key security, 235–237
  - network-layer encryption, 241–242
  - outbound packet filtering, 235
  - rerouting attacks, preventing, 232–233
  - route advertisement, controlling, 233
  - route authentication, 233
  - screened subnet architecture, 224
  - static routes, 232
- perimeter security, 223–230
  - bastion hosts, 228



- firewalls, 229
- perimeter routers, 224–228
- per-session encryption policy, CET, configuring, 493–498
- physical devices, securing, 69–70
- ping access, PIX Firewall
  - inside hosts, 369–370
  - permitting, 395–396
- ping command, 14, 327, 365, 566
- PIX Firewall, 291–292
  - (Private Internet Exchange)
  - AAA (authentication, authorization, and accounting) server, configuring, 401–407
  - ASA (Adaptive Security Algorithm), 292
  - CA support, configuring, 645–673
  - CLI (command-line interface), 311–314
  - components, 303–309
  - conduits, inbound access, 296–303
  - configuring, 310, 330–335
    - Advanced PIX Firewall, 443–444, 446–447
    - commands, 391
    - multiple interface access, 381–401
    - multiple interfaces, 408–412
    - outbound access control, 339–355
    - outside to DMZ, 392–394
    - secured bidirectional communication, 375–378
    - testing, 325–330
    - URL logging, 426–428
    - user authentication, 401–407
  - connections, licensing, 391
  - CSPM (CiscoSecure Policy Manager), 439
  - cut-through user authentication, 301, 303
  - DNS Guard, 370–374
  - DoS (denial of service), 370–374
  - entering, 293–303
  - failover, configuring, 430–433
  - features, 293
  - FTP, configuring, 426–428
  - global commands, 320–325
  - ICMP messages, filtering, 395–396
  - inbound access control, 351–354
  - inside hosts
    - access control, 356–374
    - ping access, 369–370
    - static translation, 356–362, 364–368
  - inside interfaces, configuring, 386–391
  - interface commands, 317–320
  - interfaces
    - DMZ, 385
    - inside, 385
    - outside, 385
    - security, 314–317
  - ip address commands, 317–320
- IPSec
  - configuring, 611–638
  - overall configuration, 636–638
  - preparing, 612
- Java applet blocking, configuring, 422–423
- Mail Guard, configuring, 366
- maintenance, 440–443
- models, 303–309
- multimedia applications, 354–355
- NAT (Network Address Translation), 340–344
  - nat 0 configuration, 344–347
  - outbound access control, 341–344
  - PAT (Port Address Translation), 347–349
- NAT 0, configuring, 417–418
- nat commands, 320–325
- NetBIOS translation, 349–350
- network interfaces, 307–309
- NICs (network interface cards), 308–309
- operations, 293
- outbound access, controlling, 419–422
- outbound access control, 351–354
- password recovery, 440
- ping access, permitting, 395–396
- PPTP (Point-to-Point Tunneling Protocol) configuring, 437–439

- Private Link encryption, 434–437
- SNMP (Simple Network Management Protocol), configuring, 428–430
- software licensing, 308
- software upgrades, 441–442
- statics, inbound access, 296–303
- SYN (synchronize segment) flood attacks, 372–374
- Syslog Server, configuring, 396–400
- URL filtering, configuring, 423–425
- VPNs, configuring, 434–439
- PKCS #10 (Public-Key Cryptography Standard #7), 550
- PKCS #7 (Public-Key Cryptography Standard #7), 550
- PKI (Public Key Infrastructure), 548
  - IPSec, 548–552
- plaintext authentication
  - routing protocols, 87
  - security, 87
- planning encryption, 474
- points of contact, incident response teams, 702
- Point-to-Point Protocol. *See* PPP (Point-to-Point Protocol)
- Point-to-Point Tunneling Protocol. *See* PPTP (Point-to-Point Tunneling Protocol)
- policies
  - Acceptable Use Policy, 696–697
  - analyzing, 42–43
  - Campus Access Policy, 698
  - Identification and Authentication Policy, 697
  - IKE, creating, 613, 615
  - implementation, 696
  - intended audiences, 693
  - Internet Access Policy, 698
  - Remote Access Policy, 699–700
  - scope, 694
  - stakeholders, 694
  - system administrators, responsibilities, 695
  - user education, 696
- Port Address Translation. *See* PAT (Port Address Translation)
- postures, improving, 47
- PPP (Point-to-Point Protocol), 52
  - authentication, Kerberos, 145
  - Double Authentication, 210–212
  - packet-mode traffic, 114
- PPTP (Point-to-Point Tunneling Protocol), 437, 520
  - PIX Firewall, configuring, 437–439
- presared keys
  - configuring, 616–618
  - IKE, configuring, 567, 613
  - IPSec, configuring, 565–593, 603–606
  - PIX Firewall, configuring for, 638–639, 641
- presared keys (IKE), 539
- Private Internet Exchange Firewall. *See* PIX (Private Internet Exchange)
- Private Link encryption, PIX Firewall, 434–437
- privilege levels, administrative interfaces, setting multiple, 77–78
- privileged access, 21
  - SNMP, 85
- processing
  - extended IP access lists, 721–722
  - standard IP access lists, 714–716
- protocol analyzers, 17
- protocols, VPNs, 520
- proxy servers, firewalls, 229
- Public Key Infrastructure. *See* PKI (Public Key Infrastructure)
- Public-Key Cryptography Standard #10. *See* PKCS #10 (Public-Key Cryptography Standard #10)
- Public-Key Cryptography Standard #7. *See* PKCS #7 (Public-Key Cryptography Standard #7)

## Q-R

---

### QoS

- Cisco IOS Firewall, 261
- RA (Registration Authority), 551
- RADIUS (Remote Access Dial-In User Service), 177
  - accounting process, 139
  - attributes, 140
  - authentication process, 138
  - authorization, 138
  - CiscoSecure ACS, 178
  - configuring, CiscoSecure ACS, 205–210
  - features, 137
  - remote security databases, 136–142
  - TACACS+, compared, 141
  - testing, 208–210
  - troubleshooting, 208–210
  - versions, 137
- rcp command, 21
- realms, Kerberos, 144
- real-time alerts, Cisco IOS Firewall, 261
- reconnaissance threats, 14–18
- recovering passwords, PIX Firewall, 440
- references
  - AAA (authentication, authorization, and accounting), 413
  - access lists, 738
  - CET (Cisco Encryption Technology), 515
  - Cisco IOS Firewall, configuring, 286
  - CiscoSecure Policy Manager, 449
  - CiscoSecure Software Center, 449
  - CiscoSecure ACS, 219
  - CLI, 336
  - conduit commands, 379
  - DNS, 389
  - DoS attacks, 379
  - encryption, 469
  - ESA (Encryption Service Adapter), 515
  - Ethernet switches, 106
  - firewall configuration, 285
  - general router configuration, 105
  - hackers, 336
  - hacking, 336
  - IKE, configuring, 608
  - IPSec, configuration, 608
  - NAT, 336
  - neighbor routing authentication, 106
  - network security, 336
  - PIX Firewall, 379, 413
  - PPTP (Point-to-Point Tunneling Protocol), 448
  - Private Link Encryption, 448
  - security, 34
  - security policy configuration, 218
  - SNMP, 106
  - standard and extended access lists, 106
  - TACACS+/RADIUS, 219
  - TFTP servers, 448
  - token servers, 152
  - URL filtering, 448
  - xlate commands, 379
- Registration Authority. *See* RA (Registration Authority)
- Remote Access Dial-In User Service. *See* RADIUS (Remote Access Dial-In User Service)
- Remote Access Policy, 699–700
- remote security databases
  - AAA architecture, 128–130
  - CiscoSecure ACS, 148
  - Kerberos, 142–151
  - RADIUS, 136–142
  - standards, 130–151
  - TACACS+, 131–136
- remote-access services, 24
- rerouting attacks, preventing, 232–233
- reverse DNS, references, 389
- rlogin command, 21, 148
- route advertisement, controlling, 233
- route authentication, perimeter routers, 233
- route command, 300
- route inside command, 301
- router configuration files, securing, 90–91

- routers
    - CA support, configuring, 645–673
    - HTTP access, controlling, 95–96
    - perimeter routers, 224–226, 228
  - router-to-router communications
    - router configuration files, securing, 90–91
    - routing protocols, authenticating, 86–90
    - securing, 86–96
    - traffic control, filters, 91–92
  - routing protocols, authenticating, 86–90
  - RSA, 550
  - RSA key pairs, generating, 652
  - RSA security, IPSec, 546–548
  - RSA signatures (IKE), 539
  - RSA-encrypted nonces, IPSec, configuring, 594, 596–603
  - RSA-encrypted nonces (IKE), 539
  - rsh command, 21, 148
- S**
- 
- S/Key authentication
    - AAA architecture, 117–120
    - client software, 118
    - hosts, 119
    - users, 119
  - SafeWord, 188
  - scaling VPNs (virtual private networks), 673–680
  - SCEP (Simplified Certification Enrollment Protocol), 551
  - scope, policies, 694
  - screened subnet architecture, perimeter routers, 224
  - secondary access, 21, 24
  - secured bidirectional communication, PIX Firewall, configuring, 375–378
  - security, 5
    - AAA (authorization, authentication, and accounting), NAS (Network Access Server), 158, 160–174
    - administrative interfaces, 70–86
      - access, 70–76
      - banner messages, 79–80
      - password encryption, 73
      - privilege levels, 77–78
    - campuses, 67–69
    - case studies, 48–60
    - Cisco IOS Firewall, problems, 259–260
    - cost considerations, 39
    - DoS attacks, preventing, 237–240
    - encryption, 454–456
      - alternatives, 458
      - applications, 456
      - CET (Cisco Encryption Technology), 453–460
      - DES (Digital Encryption Standard), 462–464
      - Diffie-Hellman Key exchange, 467–468
      - DSS (Digital Signature Standard), 465–466
      - MD5 (Message Digest 5), 464
      - references, 469
    - Ethernet switches, 97–99
    - importance of, 39–40
    - issues, reasons, 6–13
    - lock-and-key security, 235–237
    - monitoring, 45
    - necessity of, 5–6
    - network-layer encryption, 241–242
    - opportunities, 33
    - perimeter routers, access, 234–237
    - perimeter security, 223–230
      - perimeter routers, 224–228
    - physical devices, 69–70
    - PIX Firewall, interfaces, 314–317
    - references, 34
    - rerouting attacks, preventing, 232–233
    - router-to-router communications, 86–88, 90–96
      - router configuration files, 90–91
      - routing protocol authentication, 86–90

- traffic control, 91–92
- SNMP, access control, 81–86
- SPA (security posture assessment), 40–47
- statements of authority and scope, 693–696
- SYN attacks, preventing, 239
- TCP/IP, controlling, 230–232
- Telnet, access, 80–81
- testing, 46
- threats
  - data manipulation threats, 30–32
  - DoS (denial of service) threats, 24–29
  - reconnaissance threats, 14–18
  - types, 13–33
  - unauthorized remote access threats, 18–24
- trusted access, 24
- VPNs, IPsec, 519–520
- Web sites, 35
- XYZ Company network scenario, 690–691
- security association lifetime, IPsec, configuring, 626–628
- security associations, IPsec, 521–522
- security audits, 46
- Security Configuration Guide and Security Configuration Command Reference, 510
- Security Dynamics, Inc., 188
- security levels, interfaces, 384
- security policies
  - Acceptable Use Policy, 696–697
  - analyzing, 42–43
  - Campus Access Policy, 698
  - Identification and Authentication Policy, 697
  - implementation, 696
  - intended audiences, 693
  - Internet Access Policy, 698
  - Remote Access Policy, 699–700
  - scope, 694
  - stakeholders, 694
  - system administrators, responsibilities, 695
  - user education, 696
- security posture assessment. *See* SPA (security posture assessment)
- security postures, improving, 47
- security servers, AAA architecture, 127–151
- sensitivity levels, information, 693–696
- serverfarm command, 383
- service command, 161
- service credentials, Kerberos, 145
- service password-encryption command, 73, 160
- service timestamps command, 247
- session hijacking, 31
- session replays, 31
- set enablepass command, 97
- set ip permit disable command, 99
- set ip permit enable command, 99
- set password command, 97
- set port security command, 98
- SHA-1 (Secure Hash Algorithm-1) encryption algorithm, 526
- show arp command, 326
- show ca certificate command, 672
- show ca configure command, 672
- show ca identity command, 672
- show ca mypubkey rsa command, 672
- show commands, 391, 566, 586
- show conn command, 391
- show crypto ca certificates command, 671
- show crypto cisco algorithms command, 491
- show crypto isakmp policy command, 566
- show crypto key mypubkey command, 671
- show crypto key mypubkey dss command, 481
- show crypto map command, 555, 566
- show ip address command, 325
- show isakmp command, 555
- show isakmp policy command, 555
- show nat command, 391
- show port command, 98
- show running-config command, 73, 232
- show tcp intercept connections command, 240
- show tcp intercept statistics command, 240
- show version command, 307
- show xlate command, 391

signatures, 14

Simple Network Management Protocol. *See* SNMP (Simple Network Management Protocol), 67, 428

Simple WATCHdog, 47

Simplified Certification Enrollment Protocol. *See* SCEP (Simplified Certification Enrollment Protocol)

SNMP (Simple Network Management Protocol), 67, 82, 428

- access, controlling, 81–86
- access lists, 85
- agent, configuring, 84
- community strings, 84
- nonprivileged access, 84
- notifications, 83
- PIX Firewall, configuring, 428–430
- privileged access, 85
- references, 106
- versions, 83

snmp-server command, 429

snmp-server community command, 84

software licensing, PIX Firewall, 308

software upgrades, PIX Firewall, 441–442

SPA (security posture assessment), 40, 42–47

stakeholders, policies, 694

standard IP access lists

- commands, 716–718
- common errors, 719
- configuring, 705–738
- location, 718–719
- processing, 714–716

standards, remote security databases, 130–151

statements of authority and scope, 693–696

static command, 298–300, 340, 356–359, 392–394

Static NAT, 340

static routes, perimeter routers, 232

static translation, PIX Firewall, inside hosts, 356–368

statics, PIX Firewall, inbound access, 296–303

subnet addresses, IP addressing, 708–710

suppressing networks, 92–93

Swatch (Simple WATCHdog), 47

switches, Ethernet, securing, 97–99

SYN (synchronize segment) flood attacks

- attacks, controlling, 239
- PIX Firewall, 372–374

syntax

- TCP, 728
- UDP, 730

Syslog Server, PIX Firewall, configuring, 396–400

system administrators, policies, responsibilities, 695

system requirements

- CSNT, 185
- CSUNIX, 197

## T

TACACS (Terminal Access Controller Access Control System), versions, 131

TACACS+ (Terminal Access Controller Access Control System Plus), 132, 177

- accounting process, 135
- authentication process, 133
- authorization process, 134
- CiscoSecure ACS, 178
- configuring
  - AAA configuration commands, 199
  - CiscoSecure ACS, 197–205
- debugging, 202–204
- features, 132
- RADIUS, compared, 141
- remote security databases, 131–136

tacacs-server host command, 197

tacacs-server key command, 197

TARA (Tiger Analytical Research Assistant), 47

TCP (Transport Control Protocol)

- port keywords, 729
- syntax, 728

TCP intercept, 239

TCP/IP, controlling, 230–232

technologies, IPsec, 527–548  
TED (Tunnel Endpoint Discovery), 679  
telecommuters, policies, 700  
Telnet, access, controlling, 80–81  
telnet command, 148, 384, 388  
Terminal Access Controller Access Control System+. *See* TACACS+ (Terminal Access Controller Access Control System Plus)  
terminology, Kerberos, 144  
test crypto initiate-session command, 499–500  
testing  
    CBAC, 276–277  
    CET encryption, 499–505  
    IPsec, 586–593  
    PIX Firewall, configuration, 325–330  
    RADIUS, 208–210  
    security, 46  
TFTP (Trivial File Transport Protocol), 67  
tftp command, 442  
TGT (Ticket Granting Ticket), 145  
threats, security  
    data manipulation threats, 30–32  
    DoS (denial of service) threats, 24–29  
    reconnaissance threats, 14–18  
    types, 13–33  
    unauthorized remote access threats, 18–24  
thresholds, CBAC, configuring, 268–271  
Ticket Granting Ticket, 145  
Tiger Analytical Research Assistant. *See* TARA (Tiger Analytical Research Assistant)  
time-based access lists, Cisco IOS Firewall, 261  
timeout xlate command, 390  
token cards, authentication, AAA architecture, 120  
token servers  
    authentication, AAA architecture, 120  
    references, 152  
traceroute command, 300, 388  
traffic, controlling, filters, 91–92  
transform sets, configuring, 624–627  
traps, SNMP notifications, 83  
Triplight, 47

Trivial File Transport Protocol, 67  
troubleshooting  
    CET (Cisco Encryption Technology), 505–507  
    CSNT, 192–195  
    RADIUS, 208–210  
trust relationships, 698  
trusted access, 24  
trusted computers, 21  
Tunnel Endpoint Discovery. *See* TED (Tunnel Endpoint Discovery)  
tunnel termination, IPsec, 527

---

## U

UDP, syntax, 730  
unauthorized remote access threats, 18–24  
undebug all command, 277  
UNIX, CiscoSecure ACS, 177–178  
updates, network suppression, 92–93  
upgrades, PIX Firewall software, 441–442  
url-cache command, 426  
URLs  
    filtering, PIX Firewall, 423–425  
    logging, PIX Firewall, 426–428  
user authentication, PIX Firewall, configuring, 401–407  
user education, policies, 696  
usernames, authentication, AAA architecture, 114–117

---

## V

verification  
    access list configuration, 734–735  
    CET encryption, 499–500, 502–505  
    IKE, configuration, 618–619  
    IPsec, 586–593  
        configuration, 634–635  
    VPNs, configuration, 671–672  
VeriSign, VPNs, 552

- VIP2 (Versatile Interface Processor) crypto engine, 471
- VLANs (virtual local-area networks), 98
- VPNs (virtual private networks)
  - Baltimore Technologies, 552
  - Cisco IOS Firewall, 261
  - configuring, verifying, 671–672
  - Entrust Technologies, 552
  - Microsoft Windows 2000 Certificate Services 2.0, 552
  - PIX Firewall, configuring, 434–439
  - protocols, 520
  - scaling, 673–680
  - securing, IPSec, 519–520
  - VeriSign, 552
- vulnerabilities, 14

## W-Z

---

- Web sites, security, 35
- wildcard masks, IP access lists, 711–712
- Windows NT, CiscoSecure ACS, 177–178
- write command, 310
- write memory command, 391, 434
- write standby command, 434
- write terminal command, 73, 555–566
- X.509v3 certificates, 550
- Xauth (Extended Authentication), 678
  - IPSec, configuring, 678
- xlate command, 368
- XTACACS, 132
- XYZ Company network scenario, 687–688
  - departments, 689–690
  - dialup access, 688
  - Internet access, 689
  - security, 690–691