

Symbols

- # (pound sign), 178
- ? (question mark), 174

A

access

- access lists. *See* ACLs
- dialup, sensor deployment, 724
- maps, VLANs, 729–730
- restrictions, 74
- telecommuters, 725–726

Access Control Lists. *See* ACLs

- accessList command, 189, 288
- access-list-number parameter, ip access-list command, 152
- access-log parameter, ip access-list command, 152
- AccountName parameter, SERVICE.SMB signature engine, 467
- accounts, attacks, 16
- acl_name parameter, set security acl ip command, 148
- AclDataSource parameter, SERVICE.SYSLOG signature engine, 469
- AclFilterName parameter, SERVICE.SYSLOG signature engine, 469
- ACLs (Access Control List), 59, 116, 147
 - active, 378
 - configuring VACLs, 147–152
 - IDS-2, 728–729
 - IP blocking, 385–387
 - existing ACLs, 388–389
 - external *versus* internal interfaces, 387
 - versus* VACLs, 388
 - multiple IDS-2, 732

- action command, 729
- actions, CTR, 663
- Actions group box, Event Viewer preferences, 637–638
- active ACLs, 378
- active defenses, 88–92
- active hosts, 515
- activity bars, IDM, 226
- ad hoc attacks, 14
- Address Resolution Protocol (ARP), 19, 333
- addresses, IP, IEV filtering, 240–241. *See also* IP addresses
 - Admin User ID parameter, protected host, 688
 - administration (Security Monitor), 645
 - database maintenance, 645–648
 - Event Viewer preferences, 649
 - sensors, 307
 - diagnostic information, 308–310
 - rebooting, 310–311
 - system information, 307
 - sources, 136
 - System Configuration, 648–649
 - tools, reconnaissance attack, 19
 - Administration privilege, Users, 704
 - Administration tab, IDM, 223
 - administrators
 - CLI tasks, 183
 - CLI user roles, 176
 - networks, limiting access, 36
 - roles, user accounts, 125
 - Advanced Configuration privilege, Users, 704
 - agent kits, 533
 - controlling IP address registration, 536
 - creating, 533–534
 - installation, 491
 - software updates, 536–538
 - Agent Service Control rule, CSA policies, 525

- agents, 28
- aggregation switches, 133
- Alarm Aggregation table, 258
 - alarm status, 261–262
 - content data buffer, 263–264
 - Expanded Details Dialog table, 258–259
 - IEV event data, 254
 - Notes field, 262–263
 - viewing individual alarms, 260
- Alarm Details tab, 695
- Alarm Filter pane, CTR alarms, 695
- Alarm Information Dialog table, IEV event data, 254
- Alarm Information Dialog window, 260
- Alarm Status field, Alarm Aggregation table, 261
- alarm-channel-configuration modes, CLI, 181
- AlarmDelayTimer parameter, master signature, 438
- AlarmInterval parameter, master signature, 438
- alarms, 60, 435
 - CTR, 663, 677–681, 692–693
 - Alarm Filter pane, 695
 - Alarm Filter tabs, 695
 - Critical Alarm pane, 695
 - Display button, 694
 - Downgraded Alarm panel, 696
 - filtering, 697–698
 - icon bar, 693–694
 - reports, 699–700
 - status buttons, 694
 - Time button, 695
 - Under-Investigation Alarm pane, 696
 - false, 60–61, 98
 - IEV, 230
 - accessing IDM, 238
 - adding devices, 233–237
 - Alarm Aggregation table, 258–264
 - application paths, 271–272
 - configuring views, 247–254
 - database administration, 272–275
 - deleting device, 237
 - device properties, 237
 - event data, 254–258
 - filter configuration, 238–247
 - installation, 231–232
 - launching, 233
 - NSDB, 264–267
 - preferences, 267–271
 - system requirements, 230–231
 - uninstalling, 232
 - viewing device status, 237–238
 - management, Cisco future updates, 717–718
 - sensor status, 436
 - sensors, management, 98–101
 - severity levels, 435
 - signatures, 429
 - alarm throttle modes, 429–431
 - regular expression matching, 433–435
 - throttle modes, 429–433
 - true, 61
- Alarms page, CTR interface, 675
- AlarmSeverity parameter, master signature, 438
- AlarmThrottle master signatures, 429
- AlarmThrottle parameter, 438
- AlarmTraits parameter, 439
- alert parameter, show events command, 565
- alerts, CSA monitoring, 506–508
- All Signatures group, IDM, 330
- American Registry for Internet Numbers (ARIN), 11
- amplification, 25
- analysis engine statistics, 625
- anomaly detection, 62–63
 - benefits, 63–64
 - drawbacks, 64–65
- anonymous access, securing network, 37

- anonymous shares, 16
- Anonymous Users, privilege hierarchy, 36
- antispoofing mechanisms, IP blocking, 382–383
- any keyword, 149
- appliances, 162
 - Cisco SAFE, 54
 - CLI, 173
 - administrative tasks, 183
 - case sensitivity, 175
 - command help, 174
 - command modes, 178–182
 - configuring tasks, 183
 - keywords, 176
 - prompts, 173–174
 - recalling commands, 175
 - tab completion, 175
 - user roles, 176–178
 - hardware, 167
 - BIOS, 168–169
 - interface cards, 169–170
 - keyboards, 167–168
 - monitors, 167–168
 - spare hard drives, 168
 - IDS 4210, 162–163
 - IDS 4215, 163–164
 - IDS 4235, 165
 - IDS 4250, 166
 - IDS 4250XL, 166
 - IDS XL card, 170–172
 - installation, 183
 - configuration tasks, 186–193
 - restrictions, 167
 - upgrading from version 3.1 to 4.0, 184–186
- Application Control rule, CSA policies, 525
- applications
 - Cisco SAFE, 55
 - classes, CSA policies, 529
 - dynamic, 530–531
 - static, 529–530
 - profiling, 490
 - proxy, firewall, 38
 - application-specific integrated circuit (ASIC), 143
 - Approver user role, CiscoWorks, 493, 573
 - Architecture for Voice, Video, and Integrated Display. *See* AVVID
 - architecture
 - communication, 121
 - basics, 121–122
 - IDAPI, 122
 - RDEP, 122–124
 - IDS MC, 577–579
 - pre-Cisco IDS 4.0 editions, 115–116
 - software, 116, 118
 - authentication process, 119–120
 - cidCLI process, 121
 - cidWebServer application, 118–119
 - ctlTransSource application, 120
 - Event Store, 121
 - logApp application, 119
 - mainApp process, 119
 - NAC, 120
 - sensorApp process, 120–121
 - user accounts, 124–126
 - Administrator role, 125
 - Operator role, 125
 - Service role, 125–126
 - Viewer role, 125
 - ArgNameRegex parameter, SERVICE.HTTP signature engine, 458
 - ARIN (American Registry for Internet Numbers), 11
 - ARP (Address Resolution Protocol), 19, 333
 - ArpOperation parameter, ATOMIC.ARP signature engine, 442

- ASIC (application-specific integrated circuit), 143
- asym TCP reassembly mode, 326
- Atomic signature engines, 437, 441–442
 - ATOMIC.ARP, 442–443
 - ATOMIC.ICMP, 443–444
 - ATOMIC.IPOPTIONS, 444–445
 - ATOMIC.L3.IP, 445–446
 - ATOMIC.TCP, 446–447, 736–737
 - ATOMIC.UDP, 441, 448
- Attack signature group, IDM, 331–332
- Attacker address event rules, 616
- attackers, 5
- attacks
 - alarms, 60–61
 - approaches, 14–15
 - CSA, 489
 - application profiling, 490
 - malicious behavior, 489
 - security policies, 489–490
 - CTR, 661
 - benefits, 661–663
 - configuration, 677–692
 - installation, 669–676
 - investigation levels, 664
 - policies, 665–666
 - requirements, 666–669
 - terms, 663–664
 - customizing signatures, 360
 - evasion techniques, 74–75
 - encryption, 77
 - flooding, 75
 - fragmentation, 75–76
 - obfuscation, 77–78
 - TTL manipulation, 79
 - hybrid systems, 72–73
 - monitoring, intrusive activity, 68–72
 - network protocols, 17–19
 - network resources, 15
 - account access, 16
 - anonymous shares, 16
 - privilege-escalation, 17
 - trust relationships, 17
 - phases, 10
 - collecting information, 11–13
 - compromising the host, 13–14
 - goals, 10
 - response techniques, 73–74
 - techniques, 19
 - compromising weaknesses, 20–24
 - DoS attack, 24–28
 - reconnaissance tools, 19–20
 - triggering mechanisms, 62
 - anomaly detection, 62–65
 - misuse detection, 65–67
 - protocol analysis, 68
 - auditing, 10
 - authentication, 9
 - attacks on weaknesses, 21–22
 - RSA/DSA, SSH authorized keys, 290–292
 - securing networks, 35
 - administrative access, 36
 - anonymous access, 37
 - common privilege groups, 35–36
 - default passwords, 36–37
 - one-time passwords, 38
 - trust relationships, 37
 - software architecture, 119–120
 - statistics, 625
- Authentication parameter, show statistics
 - command, 564
- authorization, 9, 573–574
- authorized keys, RSA/DSA authentication, 290–292
- auto parameter, set trunk command, 155
- automated script attacks, 15
- availability, 10

AVVID (Architecture for Voice, Video, and Integrated Display), 34, 50, 571

- architecture, 50
 - clients, 51
 - communication, 52
 - intelligent network services, 51–52
 - Internet business solutions, 52–53
 - network platforms, 51
 - unified control plane, 52
- benefits, 53
- security configuration, 49

B

BadPortCmdAddress parameter, SERVICE.FTP signature engine, 456

BadPortCmdPort parameter, SERVICE.FTP signature engine, 456

BadPortCmdShort parameter, SERVICE.FTP signature engine, 456

bandwidth consumption, 25

Basic Configuration privilege, Users, 704

Benign Trigger(s) field, 738

“best-of-breed” solutions, 51

BIOS, appliance installation, 168–169

blocking, 379

- IDSMS-2, 727–730
- sensors, 378

both parameter

- monitor session command, 140
- set rspan command, 144
- set span command, 142

Boundaries group box, Event Viewer preferences, 639

Browsing privilege, Users, 704

BruteForceCount parameter, SERVICE.SNMP signature engine, 467

Bugtraq, 48

C

CA (certificate authority), 228

CAM (content addressable memory), 134

capture keyword, 145

capture parameter, set security acl ip command, 148

capture ports

- assigning, multiple IDSMS-2, 734
- configuring, 730
- IDSMS-2 initialization, 202
- trunking modifications, 734–736

case sensitivity, CLI commands, 175

Catalyst 2900XL/3500XL switches, SPAN, 137–138

- monitor session command, 139–141
- port monitor command, 138–139

Catalyst 4000 and 6500 switches, SPAN, 137, 141–142

Catalyst 6000 switches, IP blocking, 380, 406–407, 412–414

Catalyst 6500

- chassis, multiple IDSMS-2, 730–732
 - assigning capture ports, 734–736
 - committing VACLs to hardware, 733
 - defining ACLs, 732
 - mapping VACLs to VLANs, 733–734
- IDSMS-2 specifications, 198

CatOS, configuring VACLs, 146–147

- assigning capture ports, 150–151
- committing to memory, 149–150
- defining security ACLs, 147–149
- mapping to VLANs, 150

CCO Login field, CiscoWorks, 575

CCO Password field, CiscoWorks, 575

cd command, 583

Cells section, Event Viewer preferences, 638–639

Cerebus Internet Scanner (CIS), testing network security, 46

certificate authority (CA), 228

- certificates, sensors, 296
 - generating host certificate, 298
 - trusted hosts, 296–298
 - viewing server certificate, 299
- ChokeThreshold parameter, master signature, 439
- cidCLI process, software architecture, 121
- CIDD (Cisco Intrusion Detection Director), 99
- cidWebServer application, 118
- circular queue, 124
- CIS (Cerebus Internet Scanner), testing network security, 46
- Cisco Active Update Notification System Web site, 546
- Cisco Architecture for Voice, Video, and Integrated Data. *See* AVVID
- Cisco IDS 4215, 713
- Cisco IDS Network Module, 714
- Cisco IDS version 3.1, upgrading to 4.0, 184–186
- Cisco IDS version 4.1, 714–715
- Cisco Intrusion Detection Director (CIDD), 99
- Cisco PIX firewalls, IP blocking, 381–382
- Cisco routers, IP blocking, 379–380
- Cisco SAFE, 34, 54
 - benefits, 55
 - modular framework, 54–55
 - security configuration, 49
- Cisco Secure Intrusion Detection System*, 99
- Cisco Secure Policy Manager (CSPM), 99
- Cisco Security Agent. *See* CSA
- Cisco Security Agent Management Center (CSA MC), 492
- Cisco Threat Response. *See* CTR
- CiscoWorks, 571–572
 - IDS MC architecture, 577–578
 - launching IDS MC, 585
 - login process, 572–573
 - users
 - adding users, 574–575
 - authorization roles, 573–574
 - creating users, 493–494
- CiscoWorks VPN/Security Monitoring System
 - software, CTR, 668–669
- clear keyword, 558
- clear events command, 304
- clear parameter, show statistics command, 564
- clear security acl map command, 147
- clear trunk command, 209, 212, 735
- CLI
 - IDS appliance, 173
 - administrative tasks, 183
 - case sensitivity, 175
 - command help, 174
 - command modes, 178–182
 - configuring tasks, 183
 - keywords, 176
 - prompts, 173–174
 - recalling commands, 175
 - tab completion, 175
 - user roles, 176–178
 - IDS-2 support, 200
 - software installation, 549–551
- clients
 - AVVID architecture, 51
 - CTR requirements, 667–668
- clocks, IDS appliance configuration, 190
- Code Red, 25
- collaboration, AVVID communication, 52
- columns, Event Viewer
 - collapsing, 631–633
 - deleting, 630–631
 - expanding, 634–635
 - moving, 629
- COM (Component Object Model), 526, 529
- COM Component Access Control rule, CSA policies, 525

- command and control ports, 203
 - IDS-2, Catalyst 6500 configuration, 205–206
 - IDS-2 initialization, 202
- commands
 - action, 729
 - clear trunk, 735
 - CLI modes, 178
 - alarm-channel-configuration, 181
 - global configuration, 179
 - host, 181–182
 - interface command-control configuration, 179
 - interface group configuration, 180
 - interface sensing configuration, 180
 - NetworkAccess, 182
 - privileged EXEC, 178–179
 - service, 180
 - virtual-sensor-configuration, 182
 - match, 729
 - security acl, 732
 - set security acl capture-ports, 734
 - set security acl ip, 733
 - set security acl map, 734
 - set trunk, 736
 - vlan, 730
 - vlan access-map, 729
- commit security acl command, 149, 208–210
- common privilege groups, 35–36
- Common Services, CiscoWorks, 577–578
- communication
 - architecture, 121
 - basics, 121–122
 - IDAPI, 122
 - pre Cisco IDS 4.0 editions, 115–116
 - RDEP, 122–124
 - AVVID architecture, 52
 - Communication Protocol parameter, IDS device field, 233
 - CommunityName parameter, SERVICE.SNMP signature engine, 467
 - Component Object Model (COM), 526
 - compromising the host, 13–14
 - conferencing, AVVID communication, 52
 - confidentiality, 9
 - Config page, CTR interface, 676
 - configuration
 - CTR, 677
 - advanced tasks, 692
 - alarm sources, 677–681
 - protected systems, 686–691
 - Quick Start Wizard, 672–673
 - reports, 700–701
 - security zones, 681–686
 - files, improving security, 49
 - improving security, 49
 - tabs, Security Monitor user interface, 605
 - tasks, IDS appliance installation, 186
 - access list configuration, 189–190
 - accessing CLI, 186–187
 - CSA MC, 493–494
 - IDS MC interface, 586–587
 - password changes, 191
 - setting system clock, 190
 - setup command, 187–189
 - SSH known hosts, 192–193
 - users, 191–192
 - Configuration tab, IDM, 223
 - configuration terminal command, 179, 292
 - Confirm Password field, CiscoWorks, 575
 - Connection Rate Limit rule, CSA policies, 525
 - Connection Shun field, IP blocking manually, 417
 - connections
 - extranets sensor deployment, 724
 - intranets sensor deployment, 724–725

- Console transition,
 - STATE.STRING.CISCOLOGIN signature engine, 472
 - content addressable memory (CAM), 134
 - content area
 - IDM, 226
 - IDS MC interface, 588
 - Security Monitor user interface, 606
 - content routing, AVVID communication, 52
 - context buffers, Event Viewer, 642–643
 - context data buffer, Alarm Aggregation table, 263–264
 - ControlOpCode parameter, SERVICE.NTP signature engine, 463
 - cookies, IDM, 227
 - Coordinated Universal Time (UTC), 301
 - copy current-config command, 556
 - Crack, 21
 - CrackerJack, 21
 - crackers, 5
 - create parameter
 - set rspan command, 145
 - set span command, 142
 - Critical Alarm pane, CTR alarms, 695
 - CSA (Cisco Security Agent), 488, 718, 722
 - agent kits, 533
 - controlling IP address registration, 536
 - creating, 533–534
 - attack protection, 489
 - application profiling, 490
 - malicious behavior, 489
 - security policies, 489–490
 - deployment, 490
 - installation, 491
 - supported platforms, 490–491
 - event monitoring, 496
 - alerts, 506–508
 - Event Log Management, 502–504
 - Event Log view, 497–501
 - Event Monitor, 504
 - Event Sets menu option, 505–506
 - Status Summary option, 496–497
 - Management Center. *See* CSA MC
 - policies, 490, 516
 - access monitoring, 519
 - allow *versus* deny, 517–518
 - application classes, 529–531
 - configuring, 520–524
 - global events, 532
 - mandatory policies, 519
 - rules, 524–526
 - secondary precedence, 518–519
 - user queries, 519–520
 - variables, 527–529
 - Profiler, 538
 - software updates, 536
 - available, 536
 - scheduled, 536–538
- CSA MC (Cisco Security Agent Management Center), 492
- agent kits, 533
 - controlling IP address registration, 536
 - creating, 533–534
 - Cisco Security Agent Management Center, 492
 - creating CiscoWorks users, 493–494
 - CSA deployment, 490
 - installation, 491
 - supported platforms, 490–491
 - policy deployment, 494–495
 - reports, 538
 - security policies, 492–493
 - software updates, 536
 - available, 536
 - scheduled, 536–538
- CSPM (Cisco Secure Policy Manager), 99

ctlTransSource application, software architecture, 120
 CTR (Cisco Threat Response), 85, 98, 661

- alarms, 692–693
 - Alarm Filter pane, 695
 - Alarm Filter tabs, 695
 - Critical Alarm pane, 695
 - Display button, 694
 - Downgraded Alarm panel, 696
 - filtering, 697–698
 - icon bar, 693–694
 - status buttons, 694
 - Time button, 695
 - Under-Investigation Alarm pane, 696
- benefits, 661–662
 - advanced analysis, 662–663
 - basic analysis, 662
 - forensic data capture, 663
- configuration, 677
 - advanced tasks, 692
 - alarm sources, 677–681
 - protected systems, 686–691
 - security zones, 681–686
- installation, 669
 - GUI, 669–670
 - interface, 673–676
 - Quick Start Wizard, 671–673
- investigation levels, 664
- maintenance, 702
 - automatic updates, 702–704
 - users, 704–705
- policies, 665–666
- reports, 699
 - alarms, 699–700
 - configuration, 700–701
- requirements, 666
 - CiscoWorks VPN/Security Monitoring System software migration, 668–669

- clients, 667–668
- firewall port settings, 668
- IDS, 668
 - server, 666–667
- terms, 663–664
- customizing signatures, 351, 358
 - ATOMIC.TCP, 736–737
- attack types, 360
- functionality verification, 360–361
- inspection criteria, 360
- network protocol, 359
- parameters, 361
- sensitive file protection, 362–373
- target address, 359
- target port, 359
- testing, 361

D

Daily Beginning parameter, Security Monitor database, 648
 Daily Metrics Report, 651
 data

- IEV archival, 269–271
- protection, 488

 Data Access Control rule, CSA policies, 525
 data sets, CSA policy variable, 529
 Database Freespace Less Than (Megabytes) parameter, 647
 Database group box, Event Viewer preferences, 640
 Database Used Space Greater Than (Megabytes) parameter, 647
 databases

- IEV, 272
 - deleting events, 274–275

- exporting table, 273–274
- importing log files, 272–273
- Security Monitor administration, 645–648
- sensors, 107
- date, IEV filters, 243–244
- day parameter
 - clock set command, 190
 - show events command, 565
- daylight savings time, sensor configuration, 302–304
- DDoS (Distributed Denial of Service), 27–28
- default keyword, 176
- defense in depth, 92
- Dell D1025HT monitor, 168
- demilitarized zone (DMZ), 39, 726
- deny any any command, 147
- deny parameter, ip access-list command, 152
- Deobfuscate parameter, SERVICE.HTTP
 - signature engine, 459
- Deploy Date field, 596
- deploy task, CSA MC, 493–494
- Deployment>Deploy option, IDS MC change deployment, 593
 - Pending option, 595–596
 - Submit option, 593–595
- Deployment>Generate option, IDS MC change deployment, 591–592
- Description parameter, IDS, 679
- desirable parameter, set trunk command, 155
- desktops
 - maintenance, 488
 - sensor deployment, 105, 109
- dest_ip_spec parameter, set security acl ip command, 148
- dest_mod/dest_port parameter, set span command, 141
- Destination Address field, IP blocking manually, 417
- Destination IP parameter, security zones, 683
- destination parameter
 - monitor session command, 139
 - show tech-support command, 563
- Destination Port field, IP blocking manually, 417
- destination ports, 136
- destination_IP parameter, ip access-list command, 152
- destination_wildcard parameter, ip access-list command, 152
- destination-url parameter, show tech-support command, 563
- detection, active IDS defense, 88
- device management, 378
- Device Name parameter, IDS, 679
- Device Name sensor field, 673
- Device tab, IDM, 223
- devices
 - IP blocking, 379, 402
 - Catalyst 6000 switches, 380
 - Cisco PIX firewalls, 381–382
 - Cisco routers, 379–380
 - IDM, 402–407
 - IDS MC, 408–415
 - login, IP blocking, 384–385
 - managed, 379
 - Security Monitor, 607, 623
 - importing, 614–615
 - IOS devices, 612–614
 - monitoring connections, 623–625
 - monitoring events, 627–629
 - monitoring statistics, 625–627
 - PIX devices, 614
 - PostOffice, 610–611
 - RDEP, 608–609
- diagnostics
 - information, sensors, 308–310
 - modes, FLOOD.NET signature engine, 452

dialup access, sensor deployment, 724

digital subscriber lines (DSLs), 3

Direction parameter

- SERVICE.FTP signature engine, 456
- SERVICE.IDENT signature engine, 461
- SERVICE.RPC signature engine, 464
- SERVICE.SSH signature engine, 468
- STATE.STRING signature engine, 470
- String signature engine, 472

directories, IDS MC sensor management, 578

disable parameter

- set rspan command, 144
- set span command, 141

Display button, CTR alarms, 694

Distributed Denial of Service (DDoS), 27

DMZs (demilitarized zone), 39, 726

DNS (Domain Name System), 572

- cache poisoning, 23
- host mapping, 12

Domain Administrators, privilege hierarchy, 36

Domain Name System. *See* DNS

Domain parameter, protected domains, 691

domains

- CTR, protected systems, 690–691
- protected, 664

DoS attacks, 24

- bandwidth consumption, 25
- DDoS attack, 27–28
- host resources, 26
- protocol attacks, 17

dot1q parameter, set trunk command, 155

downgrade command, 555

downgrade all policy, CTR, 665

downgrade and clear all policy, CTR, 665

Downgraded Alarm panel, CTR alarms, 696

downgrading sensors, 555–556

Drill Down Dialog table, IEV event data, 254

drillsheets, 629

DSLs (digital subscriber lines), 3

DstPort parameter

- ATOMIC.TCP signature engine, 446
- ATOMIC.UDP signature engine, 448
- SERVICE.GENERIC signature engine, 457

dynamic application classes, 530–531

E

egress traffic, 136

include filters, ATOMIC.TCP, 737

E-Mail field, CiscoWorks, 575

Email Report To property, 595

Enabled parameter, master signature, 439

encryption

- evasion technique, 77
- securing network, 41–42

End Date parameter, 244

End Time parameter, 244

EndMatchOffset parameter

- STATE.STRING signature engine, 470
- String signature engine, 472

endpoint security devices, 487–488

Engines group, IDM, 331

entry points, IP blocking, 383

error parameter, show events command, 565

established parameter, set security acl ip

- command, 148

Ethereal, sniffer, 40

Ethernet, 101, 132

Ettercap, 20

evasion techniques, 74–75

- encryption, 77
- flooding, 75
- fragmentation, 75–76
- obfuscation, 77
- hexadecimal values, 78

- special characters, 77
- Unicode, 78
- TTL manipulation, 79
- Even Severity Indicator options, Event Viewer preferences, 639–640
- Event Log Management, CSA monitoring, 502–504
- Event Log view, CSA monitoring, 497–498
 - characteristic filtering, 499–500
 - filter defining, 500–501
- Event Monitor, CSA monitoring, 504
- Event Server servlet, 119
- Event Sets menu option, CSA monitoring, 505–506
- Event Store, software architecture, 121
- Event Type parameter, Event Sets menu option, 506
- Event Viewer, Security Monitor, 629
 - collapsing columns, 631–633
 - creating graphs, 640–641
 - deleting , 630–631
 - display preferences, 636–640
 - expansion
 - boundary, 633
 - columns, 634–635
 - freezing, 635–636
 - moving columns, 629
 - preferences, 649
 - View option, 642–644
- EventAction parameter, master signature, 439
- events
 - CSA, 496
 - alerts, 506, 508
 - Event Log Management, 502–504
 - Event Log view, 497–501
 - Event Monitor, 504
 - Event Sets menu option, 505–506
 - Status Summary option, 496–497
 - CTR, 663, 698
 - filters
 - adding with IDM, 342–345
 - adding with IDS MC, 341, 345–350
 - horizon, misuse detection, 66–67
 - messages, RDEP operations, 124
 - retrieval method, IDSM-2 support, 200
 - Security Monitor, 616–618
 - activating rules, 623
 - adding rules, 618–622
 - monitoring, 627–629
 - server statistics, 625
 - store statistics, 625
- Events by Group report, CSA MC, 538
- Events by Severity report, CSA MC, 538
- Events tab, Alarm Filter tabs, 695
- Events to Retrieve parameter, IDS device field, 233
- EventServer parameter, show statistics command, 564
- EventStore parameter, show statistics command, 564
- Every Day at Time parameter, 269–270
- Every N Hour(s) parameter, 269–270
- Every N Minute(s) parameter, 269–270
- exclude filters, ATOMIC.TCP, 737
- Excluded Severity Levels parameter, IDS device field, 233
- ExcludeDst1 parameter, FLOOD.HOST.UDP signature engine, 450
- ExcludeDst2 parameter, FLOOD.HOST.UDP signature engine, 450
- ExcludeDst3 parameter, FLOOD.HOST.UDP signature engine, 450
- ExcludeSrc1 parameter, FLOOD.HOST.UDP signature engine, 450
- ExcludeSrc2 parameter, FLOOD.HOST.UDP signature engine, 450
- ExcludeSrc3 parameter, FLOOD.HOST.UDP signature engine, 450

exclusive security stance, 40
 exit command, 174
 Expanded Details Dialog table, 254, 258–259
 expansion boundaries, Event Viewer, 633
 Exploit Signature page, NSDB, 265–266
 Extensible Markup Language (XML), 122
 extensions, file formats, 548
 external interfaces, ACLs, 387
 external threats, 8
 extranets

- boundaries, sensor placement, 104
- sensor deployment, 108, 724

F

fabric enabled, IDSM-2 support, 200
 Facility parameter, SERVICE.SYSLOG signature engine, 469
 false alarms, 60–61, 98, 712
 Fast Ethernet, 101
 File Access Control rule, CSA policies, 525
 File Monitor rule, CSA policies, 525
 File Version Control rule, CSA policies, 525
 FileName parameter, SERVICE.SMB signature engine, 467
 files

- customizing signatures, 362
 - IDM, 362–364
 - IDM Signature Wizard, 367–373
 - IDS MC, 364–366
- sets, CSA policy variable, 528
- software updates, 546
 - Cisco IDS version, 547
 - extensions, 548
 - service packs, 548
 - signature version, 548
 - type, 547

filter vlan(s) parameter

- set rspan command, 145
- set span command, 142

 filters

- CTR, 697
 - events, 698
 - source addresses, 697–698
 - target addresses, 698
- exclude filters, ATOMIC.TCP, 737
- IEV, configuring, 238–247
- include filters, ATOMIC.TCP, 737
- signatures, 340
 - adding event filter with IDM, 342–345
 - adding event filter with IDS MC, 345–350
 - defining event filter, 341
 - process, 342

 finger command, 20
 FireAll option, alarm throttle modes, 431
 FireOnce option, alarm throttle mode, 431
 Firewall, 20
 firewalls, 38

- CTR, port settings, 668
- IOS, configuring VACLs, 151–153
- IP blocking, 381–382
- port settings, 668
- security zones, 39–40
- sensors, 97
- traffic restrictions, 39

 FlipAddr parameter, master signature, 439
 Flood signature engines, 437, 448–449

- FLOOD.HOST.ICMP, 449–450
- FLOOD.HOST.UDP, 450–451
- FLOOD.NET, 451–452

 flooding, evasion technique, 75
 flows, 145, 207
 forensic data capture, CTR, 663
 Fraggie, 25
 fragmentation, 72, 75–76

G

- Gap parameter, FLOOD.NET signature engine, 451
- Gigabit Ethernet, 101
- global configuration modes, CLI, 179
- global sensing
 - internal networks, 317–318
 - IDM, 318–320
 - IDS MC, 320–322
 - reassembly options, 322
 - IDS MC, 327–328
 - IP fragment, 323–324
 - TCP, 325–327
- GlobalSummarize mode, alarm throttle mode, 432
- GMT (Greenwich Mean Time), 301
- graphical user interface (GUI), 669
- graphs
 - Event Viewer, 640–641
 - IEV event data, 254–258
- Greenwich Mean Time (GMT), 301
- Group Detail report, CSA MC, 538
- Groups parameter
 - Event Sets menu option, 506
 - protected host, 688
- Guest Users, privilege hierarchy, 36
- GUI (graphical user interface), 669–670

H

- hackers, techniques, 5, 19
 - compromising weaknesses, 20–24
 - DoS attack, 24–28
 - reconnaissance tools, 19–20
- handlers, 28
- handshaking, TLS security, 228
- hard drives, spares, 168
- HasBadOption parameter, ATOMIC.IPOPTIONS signature engine, 444
- HasBadPort parameter, SERVICE.IDENT signature engine, 461
- HasNewLine parameter, SERVICE.IDENT signature engine, 461
- HeaderRegex parameter, SERVICE.HTTP signature engine, 458
- help
 - IDS appliance CLI, 174
 - IDS MC sensor management, 589
- Help Desk user role, CiscoWorks, 493, 573
- hexadecimal values, obfuscation, 78
- hh, show events command, 565
- HijackMaxOldAck parameter, OTHER signature engine, 452
- HijackReset parameter, OTHER signature engine, 452
- HIP (Host Intrusion Protection), 487, 718
 - CSA, 488
 - agent kits, 533–536
 - attack protection, 489–490
 - deployment, 490–491
 - event monitoring, 496–508
 - management center, 492–495
 - Management Center. *See* CSA MC
 - policies, 516–532
 - Profiler, 538
 - software updates, 536–538
 - endpoint devices, 487–488
 - host groups, 509
 - configuring, 509–514
 - Hosts menu option, 514–516
 - reports, 538
- HitCount parameter, SERVICE.SMB signature engine, 466
- Home page, CTR interface, 674–675

- Host Detail report, CSA MC, 538
 - host groups, 509
 - configuring, 509–514
 - Hosts menu option, 514
 - active hosts, 515
 - last poll time, 516
 - protected hosts, 515
 - text mode, 516
 - verifying agent software, 516
 - Host ID parameter, IDS MC installation, 582
 - Host Intrusion Protection. *See* HIP
 - host modes, CLI, 181–182
 - Host Name parameter, IDS MC installation, 582
 - Host parameter, show statistics command, 564
 - host-based IDSs, monitoring intrusive activity, 68–70
 - hosts
 - agents, sensors, 97
 - compromising, 13–14
 - CTR, protected systems, 687–689
 - Ethernet MAC address, 132
 - Event Viewer, names, 643–644
 - groups. *See* host groups
 - HIP, 718
 - IP blocking manually, 417–418
 - protected, 664
 - sensors, 288
 - SSH
 - configuring known keys, 293–296
 - generating key, 292–293
 - SSL/TLS
 - generating certificate, 298
 - trusted host certificates, 296–298
 - statistics, 625
 - Hosts menu option, 514
 - active hosts, 515
 - last poll time, 516
 - protected hosts, 515
 - test mode, 516
 - verifying agent software, 516
 - host-to-host encryption, 41–42
 - HTTP, RDEP operations, 122
 - hubs, 131–132
 - hybrid systems, 72–73
-
- I**
-
- ICMP (Internet Control Message Protocol), 13
 - icmp l 1 parameter, set security acl ip command, 148
 - IcmpCode parameter
 - ATOMIC.ICMP signature engine, 443
 - set security acl ip command, 148
 - IcmpId parameter, ATOMIC.ICMP signature engine, 443
 - IcmpMaxCode parameter, ATOMIC.ICMP signature engine, 443
 - IcmpMaxSeq parameter, ATOMIC.ICMP signature engine, 443
 - icmp-message parameter, set security acl ip command, 148
 - IcmpMinCode parameter, ATOMIC.ICMP signature engine, 443
 - IcmpMinSeq parameter, ATOMIC.ICMP signature engine, 443
 - IcmpSeq parameter, ATOMIC.ICMP signature engine, 443
 - IcmpType parameter
 - ATOMIC.ICMP signature engine, 443
 - FLOOD.HOST.ICMP signature engine, 449
 - FLOOD.NET signature engine, 451
 - set security acl ip command, 148
 - SWEEP.HOST.ICMP signature engine, 474
 - icon bar, CTR alarms, 693–694

- IDAPI (Intrusion Detection Application Program Interface), 121–122
- IDIOM (Intrusion Detection Interaction and Operations Messages), 123
- IDM (IDS Device Manager), 99, 221
 - accessing, 226
 - accessing through IEV, 238
 - activity bar, 226
 - adding users, 305
 - configuration tabs, 223
 - configuring allowed hosts, 288
 - content area, 226
 - cookies, 227
 - customizing signatures, 362–364, 367–373
 - diagnostic report, 310
 - event filters
 - adding, 342–345
 - defining, 341
 - IDS-2 support, 200
 - installation, 222
 - Instructions box, 225
 - internal networks, 318–320
 - IP blocking
 - Catalyst 6000 switch, 406–407
 - devices, 402–404
 - interface devices, 404–406
 - master blocking sensor configuration, 415–416
 - never-block addresses, 397–399
 - properties, 394–395
 - IP fragment reassembly, 323–324
 - IP logging, 419–420
 - network settings, 285–287
 - new server certificate, 298
 - online documentation, 226
 - options bar, 224
 - path bar, 225
 - sensor management, 99–100
 - servlet, 119
 - setting time, 301
 - signature groups, 328–330
 - All Signatures, 330
 - Attack type, 331–332
 - Engines, 331
 - L2/L3/L4 Protocol, 333
 - Operating System, 334–335
 - Service, 335–336
 - software installation, 551–553
 - system requirements, 221
 - TCP reassembly options, 326–327
 - TLS protocol, 227–229
 - TOC, 224
 - tools bar, 225
 - trusted host certificates, 297
 - tuning signatures, 354–356
 - viewing server certificate, 299
- IDS (Intrusion Detection System)
 - active defense, 88
 - detection, 88
 - prevention, 89
 - reaction, 89–92
 - defense in depth, 92
 - defining, 59–60
 - IPS, 86–87
 - application attack resistance, 87
 - enhanced security, 86
 - sensor range, 87
 - signature defense, 87
 - technology advancements, 87
- IDS 4210, 162–163
- IDS 4215, 163–164
- IDS 4235, 165
- IDS 4250, 166, 170–172
- IDS 4250XL, 166, 727
- IDS Alarm Destination Report, 651
- IDS Alarm Report, 651

- IDS Alarm Source Report, 651
- IDS Alarm Source/Destination Pair Report, 650
- IDS Alarms by Day Report, 650
- IDS Alarms by Hour Report, 650
- IDS Alarms by Sensor Report, 650
- IDS Device Manager (IDM), 99, 184
- IDS Event Viewer (IEV), 99
- IDS MC (IDS Management Center), 99, 282
 - adding individual sensors, 283–285
 - configuring allowed hosts, 289
 - configuring reassembly options, 327–328
 - customizing signatures, 364–366
 - defining sensor groups, 282
 - deploying changes, 590
 - approval, 592
 - Deployment>Deploy option, 593–596
 - Deployment>Generate option, 591–592
- event filters
 - adding, 345–350
 - defining, 341
- internal networks, 320–322
- IP blocking
 - Catalyst 6000 switch, 412–414
 - devices, 408–409
 - master blocking sensor configuration, 416
 - never-block addresses, 399–400
 - PIX device, 414–415
 - properties, 395–397
 - router devices, 410–411
- IP logging, 420–421
- network settings, 285–287
- sensor management, 100, 575–576
 - architecture, 577–579
 - client system requirements, 584
 - installation process with Windows, 580–582
 - interface, 585–589
 - launching, 585
 - online help, 589
 - server requirements, 580
 - Solaris installation, 582–584
 - signature groups, 337–340
 - software installation, 553–555
 - tuning signatures, 356, 358
- IDS Summary Report, 650
- IDS Top Alarms Report, 650
- IDS Top Destinations Report, 650
- IDS Top Source/Destination Pairs Report, 650
- IDS Top Sources Report, 650
- IDS XL card, 170–172
- IDS-2, 197–198
 - router sensor, 96–97
 - sensors, 95
 - switch sensor capabilities, 198–199
 - versus* IDS-2, 199–200
- IDS-2
 - administrative tasks, 212
 - memory test, 212–213
 - proper shut down, 213
 - blocking, 727–728
 - ACLs, 728–729
 - capture ports, 730
 - TCP reset ports, 730
 - VLAN access maps, 729–730
 - Catalyst 6500 switch configuration, 204–205
 - command and control port, 205–206
 - monitoring ports, 206–211
 - trunking tasks, 212
 - compared to IDS 4250XL, 727
 - configuration, 200
 - initialization, 200–202
 - ports, 202–203

- traffic capture, 203
- traffic flow, 204
- internal ports, 728
- multiple IDSM-2, 730–732
 - assigning capture ports, 734–736
 - committing VACLs to hardware, 733
 - defining ACLs, 732
 - mapping VACLs to VLANs, 733–734
- specifications, 197
 - Catalyst 6500 requirement, 198
 - performance capabilities, 197–198
- TCP reset, 727–728
 - ACLs, 728–729
 - capture ports, 730
 - ports, 730
 - VLAN access maps, 729–730
- troubleshooting, 213
 - show module switch command, 214–215
 - show port command, 215–216
 - show trunk switch command, 216
 - status LED, 213–214
- versus* IDSM, 199–200
- IEV (IDS Event Viewer), 99, 230
 - accessing IDM, 238
 - adding devices, 233–237
- Alarm Aggregation table, 258
 - alarm status, 261–262
 - context data buffer, 263–264
 - Expanded Details Dialog table, 258–259
 - Note field, 262–263
 - viewing individual alarms, 260
- application paths, 271–272
- database administration, 272
 - deleting events, 274–275
 - exporting table, 273–274
 - importing log files, 272–273
- deleting device, 237
- device properties, 237
- event data, 254–255
 - graphs, 256, 258
 - Realtime Dashboard, 256
 - table columns, 255
- filter configuration, 238–240
 - alarm severity, 241
 - alarm status, 245
 - creating filter, 246
 - date and time, 243–244
 - deleting filters, 247
 - destination address, 240–241
 - IDS devices, 243
 - properties, 246
 - signature names, 242
 - source address, 240–241
- IDSM support, 200
- installation, 231–232
- launching, 233
- NSDB, 264
 - accessing, 264–265
 - Exploit Signature page, 265–266
 - user notes, 267
 - Vulnerability page, 266
- preferences, 267
 - data archival, 269–271
 - refresh cycle, 268–269
- sensor management, 100
- software updates, 549
- system requirements, 230–231
- uninstalling, 232
- viewing device status, 237–238
- views, 247–248
 - creating, 251–253
 - defaults, 248–249
 - deleting, 254
 - editing properties, 253–254
 - navigating, 249

- Ignore Broadcast zone, Quick Start Wizard, 681
- ignore DNS activity policy, CTR, 666
- ignore threat response activity policy, CTR, 666
- Immediate property, 595
- in-band management network, sensor management, 106
- inclusive security stance, 40
- infrastructure, Cisco SAFE, 54
- ingress traffic, 136
- initialization, IDSM-2, 200
 - basic tasks, 201
 - capture ports, 202
 - command and control port, 202
 - line card verification, 200–201
- in-line IDS processing, 715
- innovation, AVVID benefits, 53
- inpkts disable parameter
 - set rspan command, 144
 - set span command, 142
- inpkts enable parameter
 - set rspan command, 144
 - set span command, 142
- Insert By field, Deploy>Pending Window, 596
- Insert Time field, Deploy>Pending Window, 596
- installation
 - CSA, 491
 - CTR, 669
 - GUI, 669–670
 - interface, 673–676
 - Quick Start Wizard, 671–673
 - IDM, 222
 - IDS appliance, 183
 - configuration tasks, 186–193
 - upgrading from version 3.1 to 4.0, 184–186
 - IEV, 231–232
- instructions box
 - IDM, 225
 - IDS MC interface, 588
 - Security Monitor user interface, 606
- integration, AVVID benefits, 53
- integrity, 9
- intelligence, AVVID benefits, 53
- intelligent network services, AVVID architecture, 51–52
- interface command-control configuration modes, CLI, 179
- interface parameter
 - monitor session command, 139
 - port monitor command, 138
- interface sensing configuration modes, CLI, 180
- interface vlan command, 153
- interface/direction, 379
- interfaces
 - ACLs, IP blocking, 385
 - cards
 - appliance installation, 169–170
 - hubs, 132
 - CTR, 673
 - Alarms page, 675
 - Config page, 676
 - Home page, 674–675
 - Reports page, 676
 - group configuration modes, CLI, 180
 - IDM, 221
 - accessing, 226
 - activity bar, 226
 - configuration tabs, 223
 - content area, 226
 - cookies, 227
 - installation, 222
 - Instructions box, 225
 - online documentation, 226
 - options bar, 224
 - path bar, 225
 - system requirements, 221

- TLS protocol, 227–229
- TOC, 224
- tools bar, 225
- IDS MC, 585–586
 - configuration tasks, 586–587
 - content area, 588
 - instructions box, 588
 - object bar, 588
 - object selector handle, 588
 - options bar, 587
 - path bar, 588
 - table of contents, 587
 - tools bar, 589
- managed, 379
- IntermediateInstructions parameter,
 - SERVICE.GENERIC signature engine, 457
- internal interfaces, ACLs, 387
- internal networks, 317–318
 - IDM, 318–320
 - IDS MC, 320–322
- internal ports, IDSM-2, 728
- internal threats, 8–9
- Internet
 - AVVID, 50
 - architecture, 50–53
 - benefits, 53
 - boundaries, sensor placement, 103–104
 - business solutions, AVVID architecture, 52–53
 - Cisco SAFE, 54
 - benefits, 55
 - modular framework, 54–55
 - IDM documentation, 226
 - sensors, deployment scenarios, 108
- Internet Control Message Protocol (ICMP), 13
- Internet Security Scanner, 46
- Internet zone, Quick Start Wizard, 681
- Internetworking Operating System. *See* IOS
- interoperability, AVVID benefits, 53
- intranets
 - boundaries, sensor placement, 104
 - sensor deployment, 108–109, 724–725
- Intrusion Detection Application Program Interface (IDAPI), 121–122
- Intrusion Detection Interaction and Operations Messages (IDIOM), 123
- Intrusion Detection Manager. *See* IDM
- intrusion detection system. *See* IDS
- Intrusion Detection System Module. *See* IDSM
- intrusion protection system. *See* IPS
- InvertedSweep parameter, SWEEP.PORT.TCP signature engine, 479
- IOS (Internetworking Operating System), 96, 151, 612
 - configuring VACLs, 151
 - ACLs application to VLAN, 153
 - assigning capture port, 153
 - extended ACLs creation, 151–152
 - Security Monitor, 612–614
- IP (Internet Protocol)
 - addresses, IEV filtering, 240–241
 - fragment reassembly, 323–324
 - log messages, RDEP operations, 124
 - logging, 419
 - IDSM-2 support, 200
 - manual logging, 421–422
 - parameters in IDM, 419–420
 - parameters in IDS MC, 420–421
- ip l 0 parameter, set security acl ip command, 148
- ip access-list command, 151–152
- IP Address field
 - IDM master blocking sensor, 415
 - IP blocking manually, 418
- IP Address parameter
 - IDS, 679
 - IDS MC installation, 582
 - protected host, 688
- IP Address sensor field, 673

- IP blocking, 377–378
 - ACLs, 386–387
 - existing ACLs, 388–389
 - external *versus* internal interfaces, 387
 - versus* VACLs, 388
 - common terms, 378–379
 - configuring, 391
 - assigning block action, 391–392
 - blocking properties, 393–397
 - devices, 402–415
 - logical devices, 400–401
 - master blocking sensors, 415–416
 - never-block addresses in IDM, 397–399
 - never-block addresses in IDS MC, 399–400
 - devices, 379
 - Catalyst 6000 switches, 380
 - Cisco PIX firewalls, 381–382
 - Cisco routers, 379–380
 - guidelines, 382
 - antispoofing mechanisms, 382–383
 - blocking duration, 384
 - device login, 384–385
 - entry points, 383
 - interface ACLs, 385
 - network topology, 383
 - never-block addresses, 383
 - signature selection, 384
 - intrusion response, 74
 - manual, 417
 - host blocking, 417–418
 - network blocking, 418–419
 - master blocking sensor, 389–391
 - process, 385–386
- ip inspect command, 151
- IP Log Server servlet, 119
- IP Port field, IDM master blocking sensor, 415
- Ip-address parameter, ssh host-key command, 192, 294
- IpOption parameter, ATOMIC.IPOPTIONS signature engine, 444
- IPS (intrusion protection system), 85–87
 - alarm management, 717–718
 - application attack resistance, 87
 - considerations, 711–712
 - CTR, 98
 - enhanced security, 86
 - hosts, HIP, 718
 - in-line IDS processing, 715
 - new platforms, 713
 - Cisco IDS 4215, 713
 - Cisco IDS Network Module, 714
 - new software functions, 714–715
 - sensors, 93
 - deployment, 101–109
 - firewall, 97
 - host agents, 97
 - IDSM, 95
 - management, 98–101
 - network, 94
 - router, 96–97
 - signatures, 716
 - defense, 87
 - S44 signature update, 716–717
 - S46 signature update, 717
 - technology advancements, 87
- IpTOS parameter, ATOMIC.ICMP signature engine, 443
- IsBruteForce parameter, SERVICE.SNMP signature engine, 467
- isIcmp parameter, ATOMIC.L3.IP signature engine, 445
- isImpossiblePacket parameter, ATOMIC.L3.IP signature engine, 445

IsInvalidDataPacket parameter, SERVICE.NTP signature engine, 463

IsInvalidPacket parameter, SERVICE.SNMP signature engine, 467

isl parameter, set trunk command, 155

isLocalhost parameter, ATOMIC.L3.IP signature engine, 445

IsLoki parameter, TRAFFIC.ICMP signature engine, 481

IsModLoki parameter, TRAFFIC.ICMP signature engine, 481

IsNonNtpTraffic parameter, SERVICE.NTP signature engine, 463

IsNonSnmpTraffic parameter, SERVICE.SNMP signature engine, 467

isOverrun parameter, ATOMIC.L3.IP signature engine, 445

IsPASV parameter, SERVICE.FTP signature engine, 456

IsPortMapper parameter, SERVICE.RPC signature engine, 464

isRFC1918 parameter, ATOMIC.L3.IP signature engine, 445

IsSpoolSrc parameter, SERVICE.RPC signature engine, 465

IsSweep parameter, SERVICE.RPC signature engine, 465

J-K

Job ID field, Deploy>Pending Window, 596

Job Name field, Deploy>Pending Window, 596

Job Name property, 595

John the Ripper, 21

Kernel Protection rule, CSA policies, 525

keyboards, appliance installation, 167–168

KeyLength parameter, SERVICE.SSH signature engine, 468

key-modulus-length parameter, ssh host-key command, 192

KeyTronic E03601QUS201-C keyboard, 168

KeyTronic LT DESIGNER keyboard, 168

keywords, CLI commands, 176

L

L0phtCrack 4.0, 21

L2/L3/L4 Protocol signature group, IDM, 333

LAN zone, Quick Start Wizard, 681

learning disable parameter

- set rspan command, 145
- set span command, 142

learning enable parameter

- set rspan command, 145
- set span command, 142

LED (light-emitting diode), 213–214

light-emitting diode (LED), 213

Local Password field, CiscoWorks, 575

local SPAN, 136

log files, IEV, importing, 272–273

log parameter, show events command, 565

log_input parameter, ip access-list command, 152

logApp application, software architecture, 119

Logger parameter, show statistics command, 564

logging

- CSA MC reports, 538
- IP, 419
 - manually, 421–422
 - parameters in IDM, 419–420
 - parameters in IDS MC, 420–421

logical devices, IP blocking configuration, 400–401

login, CiscoWorks, 572–573

logs, intrusion response, 74

M

- MAC (Media Access Control), 132
- MacFlip parameter, ATOMIC.ARP signature engine, 442
- mailing lists, improving network security, 48
- mainApp process, software architecture, 119
- maintenance
 - CTR, 702
 - automatic updates, 702–704
 - users, 704–705
 - reimaging sensor software, 556
 - sensor software updates, 549
 - downgrading sensor, 555–556
 - install via CLI, 549–551
 - install via IDM, 551–553
 - install via IDS MC, 553–555
 - software updates, 545–546
 - file format, 546–548
 - guidelines, 548–549
- major software updates, 547
- managed devices, 379
- managed interfaces, 379
- man-in-the-middle attacks, 17–18
- manual IP blocking, 417
 - host blocking, 417–418
 - network blocking, 418–419
- manual IP logging, 421–422
- Mask parameter
 - ATOMIC.TCP signature engine, 446
 - SWEEP.HOST.TCP signature engine, 475
 - SWEEP.PORT.TCP signature engine, 479
- master blocking sensors, 415
 - configuring on IDM, 415–416
 - configuring on IDS MC, 416
 - IP blocking, 389–391
- master signatures, parameters, 438–441
- match command, 729
- MaxArgFieldLength parameter, SERVICE.HTTP signature engine, 458
- MaxBytes parameter, SERVICE.IDENT signature engine, 461
- MaxDataLen parameter, ATOMIC.L3.IP signature engine, 445
- MaxHeaderFieldLength parameter, SERVICE.HTTP signature engine, 459
- Maximum Number of Attempts property, 595
- Maximum Reassemble Fragments parameter, 323
- maximum transmission unit (MTU), 75
- MaxInspectLength parameter, master signature, 439, 442
- MaxProto parameter, ATOMIC.L3.IP signature engine, 445
- MaxRequestFieldLength parameter, SERVICE.HTTP signature engine, 459
- MaxSizeOfControlData parameter, SERVICE.NTP signature engine, 463
- MaxTech XT-7800 monitor, 168
- MaxTTL parameter, master signature, 439
- MaxUriFieldLength parameter, SERVICE.HTTP signature engine, 458
- Media Access Control (MAC), 132
- memory, testing IDSM-2, 212–213
- messaging, AVVID communication, 52
- methodical attacks, 15
- MinDataLen parameter, ATOMIC.L3.IP signature engine, 445
- MinHits parameter, master signature, 439
- MinMatchLength parameter
 - STATE.STRING signature engine, 470
 - String signature engine, 473
- minor software updates, 547
- MinProto parameter, ATOMIC.L3.IP signature engine, 445
- MinRequestMatchLength parameter, SERVICE.HTTP signature engine, 459

MinUDPLength parameter, ATOMIC.UDP
signature engine, 448

Miscellaneous signature engines, 437

misuse detection, 65–66

benefits, 66

drawbacks, 66–67

mls ip ids command, 151–153

mod/port parameter

clear trunk command, 154

port monitor command, 138

set rspan command, 144

set trunk command, 155

set vlan command, 205

Mode parameter, SERVICE.NTP signature
engine, 463

modular frameworks, Cisco SAFE, 54–55

monitor session command, 139–141

monitor task, CSA MC, 493–494

monitoring

alarms, IEV, 233–247

appliance installation, 167–168

IDSM-2 ports, 203

interfaces, multiple, 93

intrusive activity, 68

host-based IDSs, 68–70

network-based IDSs, 70–72

network security, 44–45

automatic, 45

manual, 45

ports, 136, 206

multiple IDSM-2 using VACLs,
209–211

single IDSM-2 using SPAN, 206–207

single IDSM-2 using VACLs, 207–209

sensors, 93

firewall, 97

host agents, 97

IDSM, 95

network, 94

router, 96–97

traffic devices, 131

hubs, 131–132

network tap, 133

RSPAN, 143–145

SPAN, 135–142

switches, 134–135

VACLs, 145–153

Monitoring Center for Security. *See* Security

Monitor

Monitoring tab, IDM, 223

month parameter

clock set command, 190

show events command, 565

MTU (maximum transmission unit), 75

multicast disable parameter

set rspan command, 145

set span command, 142

multicast enable parameter

set rspan command, 145

set span command, 142

N

NAC (Network Access Controller), 120

NAC parameter, show events command, 565

Name parameter, security zones, 683

NAT (Network Address Translation), 287

NAT Address parameter, IDS, 679

negotiate parameter, set trunk command, 155

NESSUS, 20, 46

Netmask field, IP blocking manually, 418

netmask parameter, setup command, 189

Network Access Control rule, CSA policies, 525

Network Access Controller (NAC), 120

Network Address Translation (NAT), 287

- Network Administrator user role, CiscoWorks, 493, 574
- network interface card (NIC), 70
- Network Interface Control rule, CSA policies, 526
- Network Operator user role, CiscoWorks, 493, 574
- Network Security Database. *See* NSDB
- Network shield rule, 532
- Network Time Protocol (NTP), 302
- Network worm rule, 532
- networkAccess command, 288
- NetworkAccess modes, CLI, 182
- NetworkAccess parameter, show statistics command, 564
- network-based IDSs, monitoring intrusive activity, 70–72
- networkParams configuration modes, CLI, 181
- networks
 - access control statistics, 625
 - address sets, CSA policy variable, 528
 - analyzer, 135–136
 - availability, AVVID intelligent network services, 51
 - environment, sensor selection, 102
 - IDM, configuring settings, 285–287
 - IDS MC, configuring settings, 285–287
 - IP blocking, 418–419
 - media types, sensor selection, 101
 - protocols
 - attacks, 17–19
 - customizing signatures, 359
 - resources, attacks, 15
 - account access, 16
 - anonymous shares, 16
 - privilege-escalation, 17
 - trust relationships, 17
 - securing, 35
 - firewall, 38–40
 - improving, 47–49
 - monitoring, 44–45
 - strengthen authentication, 35–38
 - testing, 45–47
 - VPNs, 40–42
 - vulnerability patching, 43–44
- security
 - AVVID, 50–53
 - Cisco SAFE, 54–55
- sensor deployment, 721–722
 - dialup access, 724
 - DMZ, 726
 - extranet connections, 724
 - intranet connections, 724–725
 - perimeter, 723
 - telecommuter access, 725–726
- sensors, 94
- services, CSA policy variable, 528
- tap, 133
- topology, IP blocking, 383
- never-block addresses, IP blocking, 383
- NIC (network interface card), 70
- NMAP, 20
- no keyword, 176
- no shutdown command, 176
- nonnegotiate parameter, set trunk command, 155
- Notes field, Alarm Aggregation table, 262–263
- NSDB (Network Security Database), 264, 549, 644
 - accessing, 264–265
 - Event Viewer, 644
 - Exploit Signature page, 265–266
 - user notes, 267
 - Vulnerability page, 266
- nslookup command, 20
- NT Event Log rule, CSA policies, 525
- NTBugtraq, 48

NTP (Network Time Protocol), 302
ntPassword 4.0, 21

O

obfuscation techniques, 77
 hexadecimal values, 78
 special characters, 77
 Unicode, 78
object bars, IDS MC interface, 588
object selector handles, IDS MC interface, 588
ObjectId parameter, SERVICE.SNMP signature engine, 467
off parameter, set trunk command, 155
on parameter, set trunk command, 155
one-time passwords, authentication, 38
Operation privilege, Users, 704
operational sources, 136
operator parameter, set security acl ip command, 148
Operator roles, user accounts, 125
operators, CLI user roles, 177
options bars
 IDM configuration tabs, 224
 IDS MC interface, 587
 Security Monitor user interface, 605
Organization ID parameter, IDS MC installation, 582
Organization Name parameter, IDS MC installation, 582
Originating device address event rules, 616
Originating device event rules, 616
OS, signature group, 334–335
OTHER signature engine, parameters, 452–453
out-of-band certificate validation, TLS protocol, 228–229

out-of-band management network, sensor management, 106
Overwrite Conflicting Sensors Configuration property, 595

P

packet filtering, firewall, 38
PacketDepth parameter, SERVICE.SSH signature engine, 468
packets, sniffing, 70
page parameter, show tech-support command, 563
parameters, 437–441
 ATOMIC.ARP signature engine, 442
 ATOMIC.ICMP signature engine, 443
 ATOMIC.IPOPTIONS signature engine, 445
 ATOMIC.L3.IP signature engine, 445
 ATOMIC.TCP signature engine, 446–447
 ATOMIC.UDP signature engine, 448
 clock set command, 190
 customized signatures, 361
 FLOOD.HOST.ICMP signature engine, 449
 FLOOD.HOST.UDP signature engine, 450
 FLOOD.NET signature engine, 451
 ip access-list command, 152
 monitor session command, 140
 OTHER signature engine, 453
 port monitor command, 138
 sec security acl ip command, 148
 SERVICE.DNS signature engine, 455
 SERVICE.FTP signature engine, 456
 SERVICE.GENERIC signature engine, 457
 SERVICE.HTTP signature engine, 458–459
 SERVICE.IDENT signature engine, 461
 SERVICE.MSSQL signature engine, 462
 SERVICE.NTP signature engine, 463

- SERVICE.RPC signature engine, 464–465
- SERVICE.SMB signature engine, 467
- SERVICE.SNMP signature engine, 467
- SERVICE.SSH signature engine, 468
- SERVICE.SYSLOG signature engine, 469
- set rspan command, 144–145
- set span command, 141–142
- set trunk command, 155
- set vlan command, 156
- show events command, 565
- show statistics command, 564
- show tech-support command, 563
- ssh host-key command, 192
- STATE.STRING signature engine, 470
- String signature engine, 472–473
- SWEEP.HOST.ICMP signature engine, 474
- SWEEP.HOST.TCP signature engine, 475
- SWEEP.MULTI signature engine, 476
- SWEEP.OTHER.TCP signature engine, 477
- SWEEP.PORT.TCP signature engine, 479
- SWEEP.PORT.UDP signature engine, 480
- TRAFFIC.ICMP signature engine, 481
- passphrases, 290
- password command, 186, 191
- Password field, IDM master blocking sensor, 415
- Password parameter
 - IDS, 680
 - IDS device field, 233
 - protected domains, 691
 - protected host, 688
 - show tech-support command, 563
- Password sensor field, 673
- PasswordPresent parameter, SERVICE.MSSQL signature engine, 462
- passwords
 - cracker, 21
 - default, 36–37
 - IDS appliance configuration, 191
 - one-time, authentication, 38
 - selection, 187
- path bars
 - IDM, 225
 - IDS MC interface, 588
 - Security Monitor user interface, 606
- patient (slow) attacks, 15
- pattern matching. *See* misuse detection
- PayloadSource parameter, SERVICE.GENERIC signature engine, 457
- Peaks parameter, FLOOD.NET signature engine, 451
- Pending option, IDS MC change deployment, 595–596
- perimeters, sensor deployment, 723
- permit parameter
 - ip access-list command, 152
 - set security acl ip command, 148
- personal productivity, AVVID communication, 52
- PFC (Policy Feature Card), 143, 198
- ping command, 20
- ping sweeps, 12
- PipeName parameter, SERVICE.SMB signature engine, 467
- PIX, Security Monitor configuration, 614
- PIX devices, IP blocking, IDS MC configuring, 414–415
- platforms, AVVID architecture, 51
- policies
 - CSA, 489–490, 494
 - associating with groups, 495
 - configuring, 495
 - creating groups, 494
 - defining, 492–493
 - generating rules, 495
 - installation kits, 495
 - CSA Profiler, 538

- CTR, 665–666
 - security, 9
- Policies parameter, Event Sets menu option, 506
- Policy Detail report, CSA MC, 538
- Policy Feature Card (PFC), 143, 198
- Policy Name drop-down menu parameter,
 - security zones, 683
- port command, 456
- port monitor command, 138–139
- Port parameter, security zones, 683
- port parameter
 - set security acl ip command, 148
 - monitor session command, 140
- port-based SPAN (PSPAN), 136
- PortMapProgram parameter, SERVICE.RPC
 - signature engine, 464
- PortRange parameter
 - ATOMIC.TCP signature engine, 447
 - SWEEP.OTHER.TCP signature engine, 477
 - SWEEP.PORT.TCP signature engine, 479
- PortRangeSource parameter, ATOMIC.TCP
 - signature engine, 447
- ports
 - capture ports
 - assigning, 734
 - trunking modifications, 734–736
 - firewall settings, 668
 - IDS-M-2, 202
 - command and control, 203
 - monitoring, 203
 - TCP reset, 202
 - internal, IDS-M-2, 728
 - RSPAN, 143–145
 - SPAN, 135–136
 - Catalyst 2900XL/3500XL switches, 137–141
 - Catalyst 4000 and 6500 switches, 141–142
 - TCP reset, 137
 - terminology, 136
 - target, customizing signatures, 359
 - trunking, 153–157
 - VACLs, 145
 - configuring with CatOS, 146–151
 - configuring with IOS, 151–153
 - defining captured traffic, 146
- PortsInclude parameter, SWEEP.PORT.UDP
 - signature engine, 480
- PostOffice devices, Security Monitor, 610–611
- pound sign (#), CLI privileged EXEC mode, 178
- powerdown option, IDS-M-2, 213
- preferences, Event Viewer, 636–637
 - Actions group box, 637–638
 - Boundaries group box, 639
 - Cells section, 638–639
 - Database group box, 640
 - Even Severity Indicator options, 639–640
 - Security Monitor administration, 649
 - Sort By group box, 639
- prevention, active IDS defense, 89
- Priority parameter, SERVICE.SYSLOG signature engine, 469
- private keys, RSA/DSA authentication, 290–291
 - generating SSH key, 291–292
 - import SSH key, 292
- privileged EXEC modes, CLI, 178–179
- Privileged Users, privilege hierarchy, 36
- privilege-escalation attacks, 17
- privileges, common privilege groups, 35–36
- processes, IDS MC architecture, 579
- professionals, testing network security, 46–47
- Profiler
 - applications, 490
 - CSA, 538
- prompts, IDS appliance CLI, 173–174

protected attributes, signature engine parameter, 438

protected domains, CTR, 664, 690–691

protected hosts, CTR, 664, 687–689

protected systems, CTR, 663, 686–687

- domains, 690–691
- hosts, 687–689

protocol analysis, 68

Protocol field, IP blocking manually, 417

Protocol parameter, master signature, 439

protocol parameter

- ip access-list command, 152
- set security acl ip command, 148

Proxy Login field, CiscoWorks, 575

Proxy Password field, CiscoWorks, 575

PSPAN (port-based SPAN), 136

public keys, RSA/DSA authentication, 290–291

- generating SSH key, 291–292
- importing SSH key, 292

public-exponent parameter, ssh host-key command, 192

public-modulus parameter, ssh host-key command, 192

PuTTY Web site, 292

Pwlhack 4.10, 21

PWL-Key 1.06, 21

PWLVIEW 2.0, 21

Q

QCrack, 21

QoS (Quality of service), AVVID intelligent network services, 51

Quality of service (QoS), AVVID intelligent network services, 51

queries, RDEP operations, 123

Query Sensor button, 287

QueryChaosString parameter, SERVICE.DNS signature engine, 454–455

question mark (?), CLI command help, 174

Quick Start Wizard, CTR, 671

- configuration, 672–673
- IDS sensors, 672
- policy automatic update, 672
- security zones, 672
- server pass phrase, 671

R

rack units, 162

Rate parameter

- FLOOD.HOST.ICMP signature engine, 449
- FLOOD.HOST.UDP signature engine, 450
- FLOOD.NET signature engine, 451

RDEP (Remote Data Exchange Protocol), 118, 121, 608

- communication architecture, 122–124
- Security Monitor configuration, 608–609

reaction, active IDS defense, 89–92

readme extension, 548

readme.txt extension, 548

Realtime Dashboard, 255–256

Realtime Graph, IEV event data, 255

reassembly options, 322

- IDS MC, 327–328
- IP fragment, 323–324
- TCP, 325–327

reconnaissance

- attacks, 11
 - electronic scanning, 11–13
 - public sources, 11
- tools, 19
 - administrative, 19
 - scanning, 20

- recover command, 168, 556
- refresh cycle, IEV preferences, 268–269
- RegexString parameter
 - STATE.STRING signature engine, 470
 - String signature engine, 473
- Registry Access Control rule, CSA policies, 526
- Registry sets, CSA policy variable, 528
- regular expressions
 - signature alarms, 433–435
 - syntax, 434
- release notes, software updates, 549
- Remember parameter, protected host, 688
- Remote Data Exchange Protocol (RDEP), 118, 608
- Remote Switch Port Analyzer. *See* RSPAN
- remote-access
 - boundaries, sensor placement, 104–105
 - sensors
 - configuration, 289
 - deployment scenarios, 109
- ReplyRatio parameter, TRAFFIC.ICMP signature engine, 480
- reports
 - CSA MC, 538
 - CTR, 699
 - alarms, 699–700
 - configuration, 700–701
 - Security Monitor, 649–651
 - defining, 651
 - scheduling, 652–653
 - viewing, 653–654
- Reports page, CTR interface, 676
- RequestInbalance parameter, ATOMIC.ARP signature engine, 442
- RequestRegex parameter, SERVICE.HTTP signature engine, 458
- Require Correct Sensor Versions property, 595
- required attribute, signature engine parameter, 438
- reset CLI command, 310
- reset command, 189, 213
- ResetAfterIdle parameter, master signature, 440–442
- resets, TCP, IDSM-2, 727–730
- Resource Access Control rule, CSA policies, 526
- resources, improving network security, 47–48
- response techniques, 73–74
- Retina Network Security Scanner, 46
- RFCs, 9
- .rhosts files, 37
- root accounts, 14
- Rootkit / Kernel Protection rule, CSA policies, 526
- routers
 - IP blocking, 379–380
 - IDS MC configuring, 410–411
 - sensors, 96–97
- rows, Event viewer, deleting, 630–631
- rpcinfo command, 20
- RpcMaxLength parameter, SERVICE.RPC signature engine, 464
- RpcProcedure parameter, SERVICE.RPC signature engine, 464
- RpcProgram parameter, SERVICE.RPC signature engine, 464
- rpm.pkg extension, 548
- RSA/DSA authentication, SSH authorized keys, 290–291
 - generating key, 291–292
 - importing key, 292
- RSPAN (Remote Switch Port Analyzer), 135–136, 143–144
 - network traffic capture, 206
 - set rspan command, 144–145
- rules, CSA policies, 524–525

- UNIX, 525
- UNIX-specific, 526
- Windows, 525
- Windows-specific, 525–526
- rx parameter
 - monitor session command, 140
 - set rspan command, 144
 - set span command, 142

S

- S44 signature update, 716–717
- S46 signature update, 717
- SAINT, 20, 46
- Same code as appliance sensors, IDSM-2 support, 200
- SATAN, 20, 46
- sc0 parameter
 - set rspan command, 144
 - set span command, 141
- ScanInterval parameter, SERVICE.SMB
 - signature engine, 466
- scanning
 - hacker tools, 20
 - reconnaissance for attacks, 11–13
 - testing network security, 46
- Scheduled property, 595
- script kiddies, 6
- secure shell. *See* SSH
- Secure Sockets Layer / Transport Layer Security (SSL/TLS), 296
- security
 - AVVID intelligent network services, 51
 - concepts, 9–10
 - networks, 35
 - AVVID, 50–53
 - Cisco SAFE, 54–55

- firewall, 38–40
- improving, 47–49
- monitoring, 44–45
- strengthen authentication, 35–38
- testing, 45–47
- VPNs, 40–42
- vulnerability patching, 43–44
- policy, 9, 33
- threats, 4–5
 - external, 8
 - internal, 8–9
 - structured, 7–8
 - unstructured, 5–6
- wheel, 34
- zones
 - CTR, 663, 681–686
 - sample list, 684
- security acl command, 732
- Security Alarm Detailed Report, 650
- Security Alarm Source Report, 649
- Security Bytes* newsletter, 48
- Security Focus* newsletter, 48
- Security Focus website, 48
- Security Monitor (Monitoring Center for Security), 99, 601–602
 - administration, 645
 - database maintenance, 645–648
 - Event Viewer preferences, 649
 - System Configuration, 648–649
 - client requirements, 603
 - configuration, 607
 - adding devices, 607–614
 - event rules, 616–623
 - importing devices, 614–615
 - monitoring devices, 623–629
 - Event Viewer, 629
 - collapsing columns, 631–633
 - creating graphs, 640–641

- deleting columns, 630–631
- deleting rows, 630–631
- display preferences, 636–640
- expanding columns, 634–635
- expansion boundary, 633
- freezing, 635–636
- moving columns, 629
- View option, 642–644
- reports, 649–651
 - defining, 651
 - scheduling, 652–653
 - viewing, 653–654
- sensor management, 101
- server requirements, 602–603
- user interface, 604
 - configuration tabs, 605
 - content area, 606
 - instructions box, 606
 - options bar, 605
 - path bar, 606
 - table of contents, 605–606
 - tools bar, 606–607
- Sensor IP Address parameter, IDS device field, 233
- Sensor Name parameter, IDS device field, 233
- sensorApp process, software architecture, 120–121
- sensors, 93
 - administrative task, 307
 - diagnostic information, 308–310
 - rebooting, 310–311
 - system information, 307
 - alarms, IEV, 230–275
 - allowable hosts, 288
 - blocking, 378
 - capabilities, 94
 - certificates, 296
 - generating host certificate, 298
 - trusted hosts, 296–298
 - viewing, 299
- communication architecture, 121
 - basics, 121–122
 - IDAPI, 122
 - RDEP, 122–124
- CTR, installation, 672
- deployment, 101
 - placement, 102–105
 - scenarios, 107–109
 - selection criteria, 101–102
- deployment on networks, 721–722
 - dialup access, 724
 - DMZ, 726
 - extranet connections, 724
 - intranet connections, 724–725
 - perimeter, 723
 - telecommuter access, 725–726
- design considerations
 - database management, 107
 - management, 106
 - number of sensors, 106–107
 - software updates, 107
- firewall, 97
- host agents, 97
- IDM, 221
 - accessing, 226
 - activity bar, 226
 - configuration tabs, 223
 - content area, 226
 - cookies, 227
 - installation, 222
 - Instructions box, 225
 - network settings, 285–287
 - online documentation, 226
 - options bar, 224
 - path bar, 225
 - system requirements, 221

- TLS protocol, 227–229
- TOC, 224
- tools bar, 225
- IDS appliances, 162
 - CLI, 173–183
 - hardware considerations, 167–170
 - IDS 4210, 162–163
 - IDS 4215, 163–164
 - IDS 4235, 165
 - IDS 4250, 166
 - IDS 4250XL, 166
 - IDS XL card, 170–172
 - installation, 167, 183–193
- IDS MC, 282, 575–576
 - adding individual sensors, 283–285
 - architecture, 577–579
 - client system requirements, 584
 - defining groups, 282
 - deploying changes, 590–596
 - installation process with Windows, 580–582
 - interface, 585–589
 - launching, 585
 - network settings, 285–287
 - online help, 589
 - server requirements, 580
 - Solaris installation, 582–584
- IDSMS, 95, 197
 - IDSMS-2, 95
 - IDSMS-2 specifications, 197–198
 - original version, 95
 - switch sensor capabilities, 198–199
 - versus* IDSMS-2, 199–200
- IDSMS-2
 - administrative tasks, 212–213
 - Catalyst 6500 switch configuration, 204–212
 - configuration, 200–204
 - troubleshooting, 213–216
 - improving network security, 49
 - management, 98–99
 - IDM, 99–100
 - IDS MC, 100
 - IEV, 100
 - Security Monitor, 101
 - master blocking, 415
 - configuring on IDM, 415–416
 - configuring on IDS MC, 416
 - network, 94
 - reimaging software, 556
 - remote access, 289
 - router, 96
 - IDSMS, 96–97
 - IOS, 96
 - software architecture, 116–118
 - authentication process, 119–120
 - cidCLI process, 121
 - cidWebServer application, 118–119
 - ctlTransSource application, 120
 - Event Store, 121
 - logApp application, 119
 - mainApp process, 119
 - NAC, 120
 - sensorApp process, 120–121
 - software updates, 549
 - downgrading sensor, 555–556
 - install via CLI, 549–551
 - install via IDM, 551–553
 - install via IDS MC, 553–555
- SSH, 290
 - configuring known host keys, 293–296
 - new host key, 292–293
 - RSA/DSA authentication, 290–292
- status alarms, 436
- time, 299–301
 - correcting errors, 304
 - daylight savings time, 302–304
 - NTP server, 302
 - time zone, 301–302

- traffic devices, 131
 - hubs, 131–132
 - network tap, 133
 - RSPAN, 143–145
 - SPAN, 135–142
 - switches, 134–135
 - VACLs, 145–153
- troubleshooting, 557
 - show events command, 565–566
 - show interfaces command, 558–562
 - show statistics command, 564
 - show tech-support command, 562–563
 - show version command, 557–558
- user accounts, 124–126, 304–306
- servers
 - CTR requirements, 666–667
 - maintenance, 488
 - sensor deployment, 105, 109
- service alarm-channel-configuration command, 318
- service control, Cisco SAFE, 55
- service packs, 547–550
- Service Restart rule, CSA policies, 526
- Service role, user accounts, 125–126
- service role, CLI, 177–178
- Service signature engines, 437, 453–454
 - SERVICE.DNS, 454–456
 - SERVICE.GENERIC, 457–458
 - SERVICE.HTTP, 458–461
 - SERVICE.IDENT, 461–462
 - SERVICE.MSSQL, 462
 - SERVICE.NTP, 462–464
 - SERVICE.RPC, 464–466
 - SERVICE.SMB, 466–467
 - SERVICE.SNMP, 467–468
 - SERVICE.SSH, 468–469
 - SERVICE.SYSLOG, 469
 - STRING.TCP, 456–457
- Service signature group, IDM, 335–336
- SERVICE.DNS signature engines, 453–456
- SERVICE.FTP signature engines, 453
- SERVICE.GENERIC signature engines, 453, 457–458
- SERVICE.HTTP signature engines, 453, 458–461
- SERVICE.IDENT signature engines, 453, 461–462
- SERVICE.MSSQL signature engines, 453, 462
- SERVICE.NTP signature engines, 453, 462–464
- SERVICE.RPC signature engines, 454, 464–466
- SERVICE.SMB signature engines, 454, 466–467
- SERVICE.SMTP signature engines, 454, 471
- SERVICE.SNMP signature engines, 454, 467–468
- SERVICE.SSH signature engines, 454, 468–469
- SERVICE.SYSLOG signature engines, 469
- ServicePorts parameter
 - master signature, 440
 - OTHER signature engine, 453
 - SERVICE.FTP signature engine, 456
 - SERVICE.HTTP signature engine, 459
 - SERVICE.IDENT signature engine, 461
 - SERVICE.RPC signature engine, 464
 - SERVICE.SSH signature engine, 468
 - STATE.STRING signature engine, 470
 - String signature engine, 473
- services modes, CLI, 180
- servlets, cidWebServer application, 118
- session parameter, monitor session command, 139
- set boot device switch command, 212
- set rspan command, 144–145
- set security acl command, 149, 153
- set security acl capture-ports command, 150, 208, 211, 734
- set security acl ip command, 147–148, 733

- set security acl map command,
 - 150, 208–210, 734
- set span command, 141–142
- set span switch command, 206
- set trunk command, parameters, 155, 212, 736
- set trunk switch command, 208
- set vlan command, 156, 205
- setup command, 187–189, 201, 222, 289, 556
- Severity event rules, 617
- Severity Level parameter, Event Sets menu option, 506
- ShortUDPLength parameter, ATOMIC.UDP signature engine, 448
- show command, 557
- show events command, 565–566
- show interfaces command, 558–562
- show interfaces command-control command, 560
- show interfaces group command, 561–562
- show interfaces sensing command, 560
- show module command, 201
- show module switch command, 200, 214–215
- show port command, 215–216
- show ssh host-key command, 294
- show statistics command, 564
- show statistics WebServer command, 564
- show tech-support command, 562–563
- show tech-support CLI command, 308
- show tls fingerprint command, 229
- show trunk mod/port detail command, 155
- show trunk mod/port detail switch command, 212
- show trunk switch command, 216
- show users all command, 192
- show version command, 307, 556–558
- shun command, 120, 381, 402
- shunConnection action, 378
- shunHost action, 377
- shunning, IDSM support, 200
- shutdown command, 176
- SigComment parameter, master signature, 440
- SIGID parameter, master signature, 440
- SigName parameter, master signature, 440
- signature engines, 437
 - Atomic, 441–442
 - ATOMIC.ARP signature engine, 442–443
 - ATOMIC.ICMP signature engine, 443–444
 - ATOMIC.IPOPTIONS signature engine, 444–445
 - ATOMIC.L3.IP signature engine, 445–446
 - ATOMIC.TCP signature engine, 446–447
 - ATOMIC.UDP signature engine, 448
 - Flood, 448–449
 - FLOOD.HOST.ICMP signature engine, 449–450
 - FLOOD.HOST.UDP signature engine, 450–451
 - FLOOD.NET signature engine, 451–452
 - IDSM-2 support, 200
 - OTHER, 452–453
 - parameters, 437–438
 - engine-specific, 441
 - master signature, 438–441
 - Service, 453–454
 - SERVICE.DNS signature engine, 454–456
 - SERVICE.GENERIC signature engine, 457–458
 - SERVICE.HTTP signature engine, 458–461

- SERVICE.IDENT signature engine, 461–462
- SERVICE.MSSQL signature engine, 462
- SERVICE.NTP signature engine, 462–464
- SERVICE.RPC signature engine, 464–466
- SERVICE.SMB signature engine, 466–467
- SERVICE.SNMP signature engine, 467–468
- SERVICE.SSH signature engine, 468–469
- SERVICE.SYSLOG signature engine, 469
- STRING.TCP signature engine, 456–457
- State, 470
 - SERVICE.SMTP signature engine, 471
 - STATE.STRING signature engine, 470–471
 - STATE.STRING.CISCOLOGIN signature engine, 471–472
 - STATE.STRING.LPRFORMAT signature engine, 472
- String, 472–473
- Sweep, 473–474
 - SWEEP.HOST.ICMP signature engine, 474
 - SWEEP.HOST.TCP signature engine, 474–476
 - SWEEP.MULTI signature engine, 476
 - SWEEP.OTHER.TCP signature engine, 476–478
 - SWEEP.PORT.TCP signature engine, 478–480
 - SWEEP.PORT.UDP signature engine, 480
- TRAFFIC.ICMP, 480–481
- Trojan, 481
- signature groups
 - IDM, 328–330
 - All Signatures, 330
 - Attack type, 331–332
 - Engines, 331
 - L2/L3/L4 Protocol, 333
 - Operating System, 334–335
 - Service, 335–336
 - IDS MC, 337–340
- Signature ID event rules, 617
- Signature ID group, IDS MC, 338–340
- Signature name event rules, 617
- signature responses, 377
 - IP blocking, 377–378
 - ACLs, 386–389
 - common terms, 378–379
 - configuring, 391–416
 - devices, 379–382
 - guidelines, 382–385
 - manual, 417–419
 - master blocking sensor, 389–391
 - process, 385–386
 - IP logging, 419
 - manual logging, 421–422
 - parameters in IDM, 419–421
 - TCP reset, 422–423
- signatures, 429
 - alarm throttle modes, 429–431
 - FireAll option, 431
 - FireOnce option, 431
 - GlobalSummarize mode, 432
 - Summarize mode, 431–432
 - variable alarm summarization, 432–433
 - alarms, 435–436

- Cisco updates, 716–717
- configuring, 350–351
- customizing, 358, 736–737
 - attack type, 360
 - functionality verification, 360–361
 - inspection criteria, 360
 - network protocol, 359
 - parameters, 361
 - sensitive file protection, 362–373
 - target address, 359
 - target port, 359
 - testing, 361
- engines. *See* signature engines
- filtering, 340
 - adding event filter with IDM, 342–345
 - adding event filter with IDS MC, 345–350
 - defining event filter, 341
 - process, 342
 - groups. *See* signature groups
 - regular expression matching, 433–435
 - responses. *See* signature responses
 - software updates, 548–550
 - tuning, 352–354, 738–739
 - IDM, 354–356
 - IDS MC, 356, 358
- SigStringInfo parameter, master signature, 440
- Simple Network Management Protocol (SNMP), 496
- SinglePacketRegex parameter, ATOMIC.TCP
 - signature engine, 447
- site-to-site encryption, 41–42
- slow attacks, 15
- Smurf, 25
- Sniffer and Protocol Detection rule, CSA
 - policies, 526
- sniffers, 40, 70
- SNMP (Simple Network Management Protocol), 496
- software
 - architecture, 116, 118
 - authentication process, 119–120
 - cidCLI process, 121
 - cidWebServer application, 118–119
 - ctlTransSource application, 120
 - Event Store, 121
 - logApp application, 119
 - mainApp process, 119
 - NAC, 120
 - sensorApp process, 120–121
 - past architecture, 115–116
 - sensor deployment, 107
 - sensor reimaging, 556
 - software updates, 545–546
 - Cisco IDS, 547
 - CSA, 536–538
 - file format, 546
 - Cisco IDS version, 547
 - extensions, 548
 - service packs, 548
 - signature version, 548
 - type, 547
 - guidelines, 548–549
- Solaris, installation, 582
 - process, 583–584
 - server requirements, 583
- Sort By group box, Event Viewer preferences, 639
- Source Address field, IP blocking manually, 417
- Source IP parameter, security zones, 683
- source parameter, monitor session command, 139
- Source Port field, IP blocking manually, 417
- source ports, 136
- Source tab, Alarm Filter tabs, 695

- source vlan parameter, monitor session command, 139
- source_IP parameter, ip access-list command, 152
- source_wildcard parameter, ip access-list command, 152
- SPAN (Switch Port Analyzer), 135–136, 198, 206
 - Catalyst 2900XL/3500XL switches, 137–138
 - monitor session command, 139–141
 - port monitor command, 138–139
 - Catalyst 4000 and 6500 switches, 141–142
 - IDS/IPS-2 options, 198
 - network traffic capture, 206–207
 - TCP reset, 137
 - terminology, 136
- SPAN/RSPAN, IDS/IPS support, 199
- spoofing attacks, 18–19
- SqlUsername parameter, SERVICE.MSSQL signature engine, 462
- src_ip_spec parameter, set security acl ip command, 148
- src_mod/src_ports parameter
 - set span command, 141
 - set vlan command, 156
- src_vlan parameter, set span command, 141
- SrcPort parameter
 - ATOMIC.TCP signature engine, 447
 - ATOMIC.UDP signature engine, 448
 - SERVICE.GENERIC signature engine, 457
- SSH (secure shell), 290
 - configuring known host keys, 293–296
 - new host key, 292–293
 - RSA/DSA authentication, 290–292
- ssh authorized-key command, 292
- ssh generate-key command, 292
- ssh host-key command, parameters, 192, 294
- SSH hosts, IDS appliance configuration, 192–193
- SSL/TLS (Secure Sockets Layer / Transport Layer Security), 296–299
- Stacheldraht, 28
- standard deviation, 63
- Start Date parameter, date and time filter, 244
- Start Time parameter, date and time filter, 244
- State signature engines, 437, 470
 - SERVICE.SMTP, 471
 - STATE.STRING, 470–471
 - STATE.STRING.CISCOLOGIN, 471–472
 - STATE.STRING.LPRFORMAT, 472
- stateful packet inspection, firewall, 38
- StateName parameter, STATE.STRING signature engine, 470
- static application classes, 529–530
- Statistical Graph, IEV event data, 254
- statistics, Event Viewer, 644
- status parameter, show events command, 565
- Status Summary option, CSA monitoring, 496–497
- Stick, 75
- Stop Auto Refresh parameter, IEV, refresh cycle, 269
- String signature engines, 437, 472–473
- STRING.TCP signature engines, 456–457
- StripTelnetOptions parameter, String signature engine, 473
- Strobe, 20
- structured threats, 7–8
- Submit option, IDS MC change deployment, 593–595
- subscriptions, RDEP operations, 123
- SubSig parameter, master signature, 440
- Summarize mode, alarm throttle modes, 431–432
- SummaryKey parameter, 430, 440
- SuppressReverse parameter, SWEEP.PORT.TCP signature engine, 479
- suspicious symbolic link, 526

Sweep signature engines, 437, 473–474
 SWEEP.HOST.ICMP, 474
 SWEEP.HOST.TCP, 474–476
 SWEEP.MULTI, 476
 SWEEP.OTHER.TCP, 476–478
 SWEEP.PORT.TCP, 478–480
 SWEEP.PORT.UDP, 480

Switch Port Analyzer. *See* SPAN

switches

aggregation, 133
 IDSM, 197
 IDSM-2 specifications, 197–198
 switch sensor capabilities, 198–199
 versus IDSM-2, 199–200
 IDSM-2
 administrative tasks, 212–213
 Catalyst 6500 switch configuration, 204–212
 configuration, 200–204
 troubleshooting, 213–216
 port trunking, 153–157
 RSPAN, 143–145
 SPAN, 135–136
 Catalyst 2900XL/3500XL switches, 137–141
 Catalyst 4000 and 6500 switches, 141–142
 TCP reset, 137
 terminology, 136
 traffic monitoring, 134–135
 VACLs, 145
 configuring with CatOS, 146–151
 configuring with IOS, 151–153
 defining captured traffic, 146
 switchport capture command, 153
 SynFloodMaxEmbrionic parameter, OTHER signature engine, 453
 Syslog Control rule, CSA policies, 526

Syslog Settings option, Security Monitor, 606
 System Administrator user role, CiscoWorks, 493, 574
 System Administrators, privilege hierarchy, 36
 System Configuration settings, Security Monitor administration, 648–649

T

tab completion, IDS appliance CLI, 175
 table of contents
 IDS MC interface, 587
 Security Monitor user interface, 605–606
 tables, IEV
 event data, 254–255
 exporting, 273–274
 TAC (Technical Assistance Center), 562
 support, 674
 website, 307
 taps, network, 133
 target addresses, customizing signatures, 359
 Targets tab, Alarm Filter tabs, 695
 TCP (Transmission Control Protocol), 137, 423
 reassembly options, 325–327
 reset, 202, 422–423
 ports, configuring, 730
 IDSM-2 support, 200, 727–730
 intrusion response, 73–74
 SPAN, 137
 tcp | 6 parameter, set security acl ip command, 148
 TcpFlags parameter
 ATOMIC.TCP signature engine, 447
 SWEEP.HOST.TCP signature engine, 475
 SWEEP.OTHER.TCP signature engine, 477
 SWEEP.PORT.TCP signature engine, 479

- TcpInterest parameter, SWEEP.MULTI signature engine, 476
- Technical Assistance Center (TAC), 562, 674
- telecommuters, sensor deployment, 725–726
- telephony processing, AVVID communication, 52
- Telnet, sensor configuration, 289
- telnet command, 20
- testing
 - customized signatures, 361
 - network security, 45
 - professional evaluation, 46–47
 - scanners, 46
- Threat Response zone, Quick Start Wizard, 681
- threats, 4–5
 - external, 8
 - internal, 8–9
 - structured, 7–8
 - unstructured, 5–6
- ThrottleInterval parameter, 431–432, 440
- time
 - IEV filtering, 243–244
 - sensors, 299–300
 - correcting time errors, 304
 - daylight savings time, 302–304
 - NTP server, 302
 - setting time, 301
 - time zone, 301–302
- Time Between Attempts property, 595
- Time button, CTR alarms, 695
- Timeout (Minutes) field, IP blocking manually, 417–418
- timeParams configuration modes, CLI, 181
- Timestamps parameter, Event Sets menu option, 506
- Time-To-Live (TTL), 69
- TLS (Transport Layer Security), 227–229, 285
- tls trusted-host command, 298
- TLS/SSL (Transport Layer Security / Secure Sockets Layer), 122
- TOC (Table of Contents), IDM, 224
 - IDS MC interface, 587
 - Security Monitor user interface, 605–606
- tools bar
 - IDM, 225
 - IDS MC interface, 589
 - Security Monitor user interface, 606–607
- Total Events parameter, Security Monitor database, 648
- Total IDS Events parameter, Security Monitor database, 648
- Total Syslog Events parameter, Security Monitor database, 648
- traffic
 - Catalyst 6500 configuration, 206
 - multiple IDSM-2 using VACLs, 209–211
 - single IDSM-2 using SPAN, 206–207
 - single IDSM-2 using VACLs, 207–209
 - devices, 131
 - hubs, 131–132
 - network tap, 133
 - RSPAN, 143–145
 - SPAN, 135–142
 - switches, 134–135
 - VACLs, 145–153
 - directions, ACLs, 387
 - IDSM-2
 - capturing, 203
 - flow, 204
 - port trunking, 153–157
 - restrictions, firewall, 39
- TRAFFIC.ICMP signature engines, 480–481

- TrafficFlowTimeout parameter, OTHER signature engine, 453
- training, avoiding attacks, 64
- transaction messages, RDEP operations, 124
- Transaction Server servlet, 119
- transaction server statistics, 625
- transaction source statistics, 625
- TransactionServer parameter, show statistics command, 564
- transitions
 - SERVICE.SMTP signature engine, 471
 - STATE.STRING.CISCOLOGIN signature engine, 472
 - STATE.STRING.LPRFORMAT signature engine, 472
- Transmission Control Protocol. *See* TCP
- Transport Layer Security (TLS), 228, 285
- Transport Layer Security / Secure Sockets Layer (TLS/SSL), 122
- Tribe Flood Network, 28
- triggering mechanisms, 62
 - anomaly detection, 62–63
 - benefits, 63–64
 - drawbacks, 64–65
 - misuse detection, 65–66
 - benefits, 66
 - drawbacks, 66–67
 - protocol analysis, 68
- Trinoo, 28
- Trojan detection rule, 532
- Trojan horse program, 16
- Trojan signature engines, 481
- Trojan Whack a Mole game, 16
- TROJAN.BO2K signature engines, 481
- TROJAN.TFN2K signature engines, 481
- TROJAN.UDP signature engines, 481
- troubleshooting, 557
 - IDSM-2, 213
 - show module switch command, 214–215
 - show port command, 215–216
 - show trunk switch command, 216
 - status LED, 213–214
 - show events command, 565–566
 - show interfaces command, 558–562
 - show statistics command, 564
 - show tech-support command, 562–563
 - show version command, 557–558
- true alarms, 61
- trunking, 153–154
 - capture ports, 734–736
 - configuring, 154
 - assigning ports to VLANs, 156
 - clearing VLANs, 154–155
 - creating VACLs, 157
 - defining VLANs, 155–156
 - IDSM-2, 212
- trust relationships
 - exploiting, 17
 - securing network, 37
 - UNIX systems, 37
- TTL (Time-To-Live), 69, 79
- tune alarm channel fourth-level modes, CLI, 181
- tune micro engines modes, CLI, 182
- tune-alarm-channel, systemVariables command, 318
- tuning, signatures, 351–358, 738–739
- Twenty-four Hour Metrics Report, 651
- tx parameter
 - monitor session command, 140
 - set rspan command, 144
 - set span command, 141

U

- UDP (User Datagram Protocol), 384
- udp l 17 parameter, set security acl ip command, 148
- UdpInterest parameter, SWEEP.MULTI signature engine, 476
- Under-Investigation Alarm pane, CTR alarms, 696
- Unicode, obfuscation, 78
- unified control plane, AVVID architecture, 52
- Uniform Resource Identifier (URI), 123
- Unique parameter
 - SERVICE.RPC signature engine, 464
 - SWEEP.HOST.ICMP signature engine, 474
 - SWEEP.HOST.TCP signature engine, 475
 - SWEEP.PORT.TCP signature engine, 479
 - SWEEP.PORT.UDP signature engine, 480
- UniqueTcpPorts parameter, SWEEP.MULTI signature engine, 476
- UniqueUdpPorts parameter, SWEEP.MULTI signature engine, 476
- UNIX systems
 - assigning trust relationships, 37
 - CSA policy rules, 525–526
- unstructured threats, 5–6
- untrusted links, VPNs, 41
- updates, CTR, 672, 702–704
- upgrade command, 550, 555
- upgrade all policy, CTR, 665
- URI (Uniform Resource Identifier), 123
- uri-es-request, RDEP operations, 123
- uri-iplog-request, RDEP operations, 123
- UriRegex parameter, SERVICE.HTTP signature engine, 458
- uri-ts-request, RDEP operations, 123
- Use TLS field, IDM master blocking sensor, 415
- User Datagram Protocol (UDP), 384
- User Name field, CiscoWorks, 575
- User Name parameter, IDS, 680
- User parameter, protected domains, 691
- UserLength parameter, SERVICE.SSH signature engine, 468
- username command, 191
- Username field, IDM master blocking sensor, 415
- Username parameter, IDS device field, 233
- Username sensor field, 673
- users
 - accounts, 124–125
 - Administrator role, 125
 - Operator role, 125
 - sensors, 304–306
 - Service role, 125–126
 - Viewer role, 125
 - adding, CiscoWorks, 574–575
 - authorization, CiscoWorks, 573–574
 - CTR maintenance, 704–705
 - groups, 62
 - IDS appliance CLI, 176
 - administrator, 176
 - operator, 177
 - service, 177–178
 - viewer, 177
 - IDS appliance configuration, 191–192
 - interface, Security Monitor, 604
 - configuration tabs, 605
 - content area, 606
 - instructions box, 606
 - options bar, 605
 - path bar, 606
 - table of contents, 605–606
 - tools bar, 606–607
 - privilege hierarchy, 36
- UTC (Coordinated Universal Time), 301

V

- VACLs (VLAN Access Control Lists), 145, 198, 207
 - capture, IDSM support, 199
 - committing to hardware, 733
 - configuring with CatOS, 146–147
 - assigning capture ports, 150–151
 - committing to memory, 149–150
 - defining security ACLs, 147–149
 - mapping to VLANs, 150
 - configuring with IOS, 151
 - ACLs application to VLAN, 153
 - assigning capture port, 153
 - extended ACLs creation, 151–152
 - defining captured traffic, 146
 - IDSM-2 options, 198
 - IP blocking, 387–388
 - mapping to VLANs, 733–734
 - network traffic capture, 206
 - multiple IDSM-2, 209–211
 - single IDSM-2, 207–209
- variables, CSA policies, 527–528
 - COM component sets, 529
 - data sets, 529
 - file sets, 528
 - network address sets, 528
 - network services, 528
 - Registry set, 528
- Verification transition,
 - STATE.STRING.CISCOLOGIN signature engine, 472
- Victim address event rules, 617
- video on demand, AVVID communication, 52
- View option, Event Viewer, 642
 - context buffer, 642–643
 - host names, 643–644
 - NSDB, 644
 - statistics, 644
- viewers
 - CLI user roles, 177
 - roles, user accounts, 125
- views, IEV alarm data, 247–248
 - creating, 251–253
 - defaults, 248–249
 - deleting, 254
 - editing properties, 253–254
 - navigating, 249
- virtual alarms, 121
- Virtual Local-Area Network (VLAN), 135, 145
- virtual private network. *See* VPNs
- virtual sensors, 120–121
- virtual-sensor-configuration modes, CLI, 182
- viruses, 24
- VLAN Access Control Lists. *See* VACLs
- vlan access-map command, 729
- vlan filter command, 730
- vlan parameter
 - monitor session command, 140
 - port monitor command, 138
- vlan_num parameter, set vlan command, 156, 205
- VLAN-based SPAN (VSPAN), 136
- vlan-id parameter
 - monitor session command, 140
 - port monitor command, 138
- VLANs (Virtual Local-Area Network), 135, 145
 - access maps, 729–730
 - mapping VACLs to, 733–734
 - trunking, 212
- vlangs parameter
 - clear trunk command, 154
 - set rspan command, 144
 - set trunk command, 155
- VMS (VPN/Security Management Solution), 100, 281, 583

VPN/Security Management Solution (VMS),
100, 281, 583
VPNs (virtual private networks), 40–41
 endpoint defining with encryption, 41–42
 untrusted links, 41
VSPAN (VLAN-based SPAN), 136
Vulnerability page, NSDB, 266
vulnerability patching, 43–44

W

WAN (wide-area network), 25
wanSrcBroadcast parameter, ATOMIC.ARP
 signature engine, 442
wantDstBroadcast parameter, ATOMIC.ARP
 signature engine, 442
WantFrag parameter, master signature, 440
WantRequest parameter, TRAFFIC.ICMP
 signature engine, 480
war dialers, 105
weaknesses, attack techniques, 20
 application holes, 23–24
 authentication, 21–22
 network services, 22
 protocols, 22–23
 trust relationships, 23
 viruses, 24
Web Port sensor field, 673
Web Server Port parameter
 IDS, 679
 IDS device field, 233
Web servers, statistics, 625
Websites
 improving network security, 48
 Security Focus, 48
 vulnerability patches, 44

WebServer parameter, show statistics command,
564
white papers, Cisco SAFE, 54
wide-area network (WAN), 25
Windows
 CSA policy rules, 525–526
 IDS MC installation
 process, 580–582
 server requirements, 580
worms, 24

X-Y-Z

XML (Extensible Markup Language), 122
year parameter
 clock set command, 190
 show events command, 565
zero-day protection, 487
zip extension, 548