

# Index

---

## A

**access control lists.** *See* **ACLs**

**access routers**

- CLI, 51
- network module for, 23
- NM-CIDS, 493–494
  - architecture*, 495–497
  - clocks*, 506–508
  - configuring*, 503–506
  - external Fast Ethernet interfaces*, 498
  - Flash*, 498
  - front panels*, 494
  - installing*, 502–503
  - internal Fast Ethernet interfaces*, 498
  - logging in*, 509–510
  - maintenance*, 510–516
  - memory*, 498
  - packet monitoring*, 509
  - specifications*, 494
  - traffic capture*, 498–502
  - UART*, 498

**access-list command**, 64

**accounts**

- root, 66
- senior user, 109
- Service, 57

**ACLs (access control lists)**

- configuring*, 537–541, 544
- interfaces*
  - external/internal*, 311
  - IP blocking*, 309
- NM-CIDS, 499
- placement (IP blocking)*, 310–312
- VACLs, 534

**action subcommand**, 538

**actions, 300–302**

- assigning*, 314
- blocking*, 92

*events*

- filtering*, 281–284
- overriding*, 279–281
- inline signatures*, 298–300
- logging*, 300–302
- signatures*
  - response*, 162
  - viewing*, 149–150

**Actions group box (Event Viewer)**, 381

**activating event rules**, 368

**adding, 357–361**

- event rules*, 364–368
- inline functionality*, 298–300
- known SSH hosts*, 60
- users*, 59

**Address Resolution Protocol (ARP)**, 177

**addresses**

- blocking*, 317–319
- IP (Internet Protocol)*
  - blocking*, 303–312, 314–330
  - logging*, 300–302
  - NM-CIDS*, 501
- targets*, 243

**Administrator roles**, 65

**advanced signature configuration, 225–230**

- customizing*, 242–253
- MEG*, 230–237
- tuning*, 238–242

**Adware, viewing signatures**, 139

**AIC (Application Inspection and Control)**

**engines**, 238

**alarms**

- CiscoWorks 2000*, 347–356
- Fire All*, 153
- Fire Once*, 153
- managing*, 151–155

**alerts, frequency fields (signatures)**, 230

**allowed hosts, configuring**, 107–109

**allowed keyword, 539**  
**alternate TCP-reset interface, 120**  
**analysis, 535–537**  
    engines  
        category (IDM), 89  
        mode (CLI command mode), 68  
        sensors, 126–128  
    packets, 300–302  
    RSPAN, 533  
    signatures, 244  
    SPAN, 533  
**anomaly detection (IPS triggers), 11**  
**antispoofing mechanisms, 307**  
**appliance sensors, 49. *See also* sensors**  
**Application Inspection and Control (AIC)**  
    engines, 238  
**applications**  
    images  
        booting, 516  
        installing, 515  
    policy enforcement (FTP/HTTP), 237–238  
    signatures, 143  
    types, 416  
**ARP (Address Resolution Protocol), 177**  
**asset value of targets, 16**  
**assignment, 543–544**  
    blocking actions, 314  
**asymmetric mode, 275**  
**attacks, 171–215. *See also* security**  
    Cisco IPS signatures, 171  
    deny Attacker inline action, 298  
    inline actions (duration parameters), 299  
    IPS, 5  
        bypasses, 26  
        configuring, 25–26  
        deploying, 27–30  
        hardware, 17–25

        hybrid IPS/IDS solutions, 13–14  
        meta-event generators, 16–17  
        monitoring, 12–13  
        overview of, 9  
        protocols, 30  
        risk rating, 14–16  
        terminology, 10–11  
        triggers, 11–12  
    signatures, 137–139  
    TTL, 267  
    types of, 244

**authentication mode (CLI command mode), 69**  
**Auto mode (IPS), 26**  
**Auto Update (IDM), 94**  
**automatic alarm summarization, 154**

## B

**Back icon (IDM), 96**  
**basic signature fields, 227**  
**Block Properties option (IDM), 93**  
**blocking**  
    actions, 92  
    addresses, 317–319  
    assigning, 314  
    devices, 321–326  
    durations, 309  
    hosts, 330  
    IP, 303–312, 314–330  
    manual, 330–334  
    networks, 332  
    properties, 315–316  
**boot loaders, configuring, 513**  
**booting, 516**  
    helper images, 514  
**boundaries, 28**  
**Boundaries group box (Event Viewer), 383**

**bridging traffic, 527**

**bypasses**

interfaces, 123

IPS, 26

## C

**calculating risk ratings, 14–16**

**capturing traffic, 527**

Catalyst 6500 switches, 542–544

devices, 529–531

inline mode, 527–529

promiscuous mode, 529

switches, 532–534

TCP resets and switches, 535

**case sensitivity commands, 63**

**Catalyst 6000 switches, 469–475, 477–483**

blocking interfaces, 326

IDS/SM, 469–470

as IP blocking devices, 305

**Catalyst 6500 switches, 23, 476–477**

**cells (Event Viewer), 381**

**children events, 385**

**Cisco 4215 appliance sensor, 18**

**Cisco 4235 appliance sensor, 19**

**Cisco 4240 diskless appliance sensor, 20**

**Cisco 4250 appliance sensor, 21**

**Cisco 4250XL appliance sensor, 21**

**Cisco 4255 diskless appliance sensor, 22**

**Cisco IDS 4200 series network**

sensors, 17–23

**Cisco IDS Module, 465, 469**

access routers

*clocks (NM-CIDS), 506–508*

*configuring NM-CIDS, 503–506*

*installing NM-CIDS, 502–503*

*logging in (NM-CIDS), 509–510*

*maintenance (NM-CIDS), 510–512*

*monitoring packets (NM-CIDS), 509*

*NM-CIDS, 493–498*

*recovery (NM-CIDS), 512–516*

*traffic capture (NM-CIDS), 498–502*

features of, 470

IDS/SM-2, 23

*Catalyst 6500 switches, 476–477*

*configuring, 472–474*

*deploying, 469–470*

*managing, 477–478*

*ports, 475*

*traffic flow, 471*

*troubleshooting, 478–483*

**Cisco IOS, 360–361**

**Cisco IPS. *See* IPS**

**Cisco PIX Firewalls**

adding devices, 361

as IP blocking devices, 306

sensors (Cisco IOS IDS), 24

**CiscoWorks 2000, 347**

adding users, 349

authorization, 348–349

login, 347–348

Security Monitor, 351–356

*adding devices, 356–361*

*configuring, 356*

*event notification, 363–368*

*Event Viewer, 374–386*

*importing devices, 361–363*

*managing, 387–392*

*monitoring devices, 368–374*

*reports, 393–397*

**CLI (command-line interface), 45, 415, 427**

configuring, 73–74

initializing sensors, 51–61

installing sensors, 49–51

managing, 73

modifying, 61–73

**client requirements (Security**

**Monitor), 352**

**clock set command, 58**

**clocks, configuring, 58**

**cloning signatures, 253**

**Code Execution attacks, 139**

**command and control interface, 475–477**

**Command Execution attacks, 139**

**Command Timeout, 381**

**command-line interface. *See* CLI**

**commands**

access-list, 64

case sensitivity, 63

CLI command modes, 66

clock set, 58

configure terminal, 67

copy, 451

default service, 425

downgrade, 94, 423

interface vlan, 540

ip access-list, 539

ip inspect, 539

- mls ip ids, 539
  - monitor session, 535–536
  - no access-list, 64
  - no remote-span, 537
  - packet capture, 450
  - packet display, 450
  - password, 59
  - recall, 63
  - recover application-pattern, 424
  - remote-span, 536
  - reset, 57, 427, 478
  - service notification, 455
  - session, 474
  - session slot, 474
  - set security acl, 541
  - set vlan, 476
  - setup, 52–57
  - show configuration, 438
  - show events, 444
  - show interfaces, 448
  - show inventory, 441
  - show module, 479–481
  - show module switch, 472
  - show port, 482
  - show statistics, 441
  - show tech-support, 448, 452
  - show trunk, 483
  - show version, 438
  - shun, 306
  - ssh host-key, 60
  - subcommands. *See* subcommands
  - switchport access vlan, 476
  - switchport capture, 539–541
  - switchport capture allowed vlan, 541
  - switchport trunk, 543
  - upgrade, 49, 419
  - username, 59
  - vlan filter, 538
- communication parameter configuration (IDM), 97–98**
- completion, tabs, 63**
- configuration, 109, 356–366, 476, 544**
- blocking properties, 315–316
  - boot loaders, 513
  - CLI, 61
  - destination ports, 542
  - events, 276
    - filtering actions*, 281–284
    - overriding actions*, 279–281
    - Target Value Rating*, 279
    - variables*, 277, 279
  - hosts (SSH), 116–118
  - IDM, 79, 83
    - Back icon*, 96
    - communication parameters*, 97–98
    - Forward icon*, 96
    - Help icon*, 96
    - Master Blocking Sensors*, 328
    - monitoring*, 94–95
    - navigating*, 84–94
    - Refresh icon*, 96
    - system requirements*, 83
  - interfaces
    - inline pairs*, 121–123
    - inline software bypasses*, 123
    - IPS*, 14
  - IPS, 25–26
    - bypasses*, 26
    - CLI*, 73–74
  - logical devices (IDM), 319–321
  - responses, 297
    - inline actions*, 298–300
    - IP blocking*, 303–312, 314–330
    - logging actions*, 300–302
    - manual blocking*, 330–334
    - Master Blocking Sensors*, 313–314
    - TCP reset*, 334
  - Security Monitor, 356, 387, 393–397
  - sensors, 27, 107
    - accessing SNMP*, 455–457
    - analysis engines*, 126–128
    - debugging*, 448–453
    - events*, 443–447
    - hosts*, 107–118
    - interfaces*, 118–126
    - statistics*, 441–443
    - viewing*, 437–440
  - Service accounts, 57
  - signatures, 137, 155–162
    - customizing*, 242–253
    - FTP/HTTP policy enforcement*, 237–238
    - groups*, 137–151
    - managing alarms*, 151–155
    - MEG*, 230–237
    - optimizing*, 225–230
    - tuning*, 238–242
  - system clocks, 58
  - tabs (Security Monitor), 353

**configuration** (*continued*)

- time parameters (sensors), 112
- time zones (sensors), 113
- traffic flow notifications, 124–126
- verifying, 437

**Configuration icon (IDM), 84–86****configure terminal command, 67****connections**

- blocking signatures, 92
- deny Connection Inline action, 298
- Request Block Connection action, 303
- TCP reset, 334

**content**

- areas (Security Monitor), 356
- type parameters, 174

**copy command, 451****copying signatures, 253****creating. See formatting****critical hosts (IP blocking), 308****Custom Signature Wizard, 90, 248****customization, 109, 356–366, 476, 544**

- blocking properties, 315–316
- boot loaders, 513
- CLI, 61
- destination ports, 542
- events, 276
  - filtering actions, 281–284*
  - overriding actions, 279–281*
  - Target Value Rating, 279*
  - variables, 277–279*
- fields, 227–230
- hosts (SSH), 116–118
- IDM, 79, 83
  - Back icon, 96*
  - communication parameters, 97–98*
  - Forward icon, 96*
  - Help icon, 96*
  - Master Blocking Sensors, 328*
  - monitoring, 94–95*
  - navigating, 84–94*
  - Refresh icon, 96*
  - system requirements, 83*
- interfaces
  - inline pairs, 121–123*
  - inline software bypasses, 123*
  - IPS, 14*
- IPS, 25–26
  - bypasses, 26*
  - CLI, 73–74*

## logical devices (IDM), 319–321

## responses, 297

- inline actions, 298–300*
- IP blocking, 303–312, 314–330*
- logging actions, 300–302*
- manual blocking, 330–334*
- Master Blocking Sensors, 313–314*
- TCP reset, 334*

## Security Monitor, 356, 387, 393–397

## sensors, 29, 107

- accessing SNMP, 455–457*
- analysis engines, 126–128*
- debugging, 448–453*
- events, 443–447*
- hosts, 107–118*
- interfaces, 118–126*
- statistics, 441–443*
- viewing, 437–440*

## Service accounts, 57

## signatures, 137, 155–162

- customizing, 242–253*
- FTP/HTTP policy enforcement, 237–238*
- groups, 137–151*
- managing alarms, 151–155*
- MEG, 230–237*
- optimizing, 225–230*
- tuning, 238–242*

## system clocks, 58

## tabs (Security Monitor), 353

## time parameters (sensors), 112

## time zones (sensors), 113

## traffic flow notifications, 124–126

## verifying, 437

**D****Database group box (Event Viewer), 384****databases, viewing NSDB, 156–159****date parameters, 114****daylight savings time, configuring, 114–115****DDoS (Distributed Denial of Service)****attacks, 139****default keyword, 64****default service command, 425****Define Web Traffic Policy signature****type, 175****defining**

- addresses, 317–319
- Master Blocking Sensors, 328–330

- parameters, 244
  - signatures, 161–162
  - trunks for traffic capture, 543–544
  - deleting users, 59**
  - Denial of Service (DoS) attacks, 139**
  - Deny Attacker Inline action, 298**
  - Deny Connection Inline action, 298**
  - Deny Packet Inline action, 298**
  - deployment, 109, 356–366, 476, 544**
    - blocking properties, 315–316
    - boot loaders, 513
    - CLI, 61
    - destination ports, 542
    - events, 276
      - filtering actions, 281–284*
      - overriding actions, 279–281*
      - Target Value Rating, 279*
      - variables, 277, 279*
    - hosts (SSH), 116–118
    - IDM, 79, 83
      - Back icon, 96*
      - communication*
        - parameters, 97–98*
      - Forward icon, 96*
      - Help icon, 96*
      - Master Blocking Sensors, 328*
      - monitoring, 94–95*
      - navigating, 84–94*
      - Refresh icon, 96*
      - system requirements, 83*
    - interfaces
      - inline pairs, 121–123*
      - inline software bypasses, 123*
      - IPS, 14*
    - IPS, 25–26
      - bypasses, 26*
      - CLI, 73–74*
    - logical devices (IDM), 319–321
    - responses, 297
      - inline actions, 298–300*
      - IP blocking, 303–312, 314–330*
      - logging actions, 300–302*
      - manual blocking, 330–334*
      - Master Blocking Sensors, 313–314*
      - TCP reset, 334*
    - Security Monitor, 356, 387, 393–397
    - sensors, 27, 107
      - accessing SNMP, 455–457*
      - analysis engines, 126–128*
      - debugging, 448–453*
      - events, 443–447*
      - hosts, 107–118*
      - interfaces, 118–126*
      - statistics, 441–443*
      - viewing, 437–440*
    - Service accounts, 57
    - signatures, 137, 155–162
      - customizing, 242–253*
      - FTP/HTTP policy*
        - enforcement, 237–238*
      - groups, 137–151*
      - managing alarms, 151–155*
      - MEG, 230–237*
      - optimizing, 225–230*
      - tuning, 238–242*
    - system clocks, 58
    - tabs (Security Monitor), 353
    - time parameters (sensors), 112
    - time zones (sensors), 113
    - traffic flow notifications, 124–126
    - verifying, 437
  - description (interface), 119**
  - description fields (signatures), 228**
  - desktops, IPS deployment, 29**
  - destination ports, configuring, 542**
  - devices. *See also* IDM**
    - blocking, 321–326
    - IP blocking, 304–306
    - logging, 309
    - logical, 319–321
  - Distributed Denial of Service (DDoS)**
    - attacks, 139**
  - DoS (Denial of Service) attacks, 139**
  - downgrade command, 94**
  - downgrading images, 423**
  - duplex (interface), 119**
  - duration**
    - inline actions, 299
    - IP blocking, 309
- ## E
- editing**
    - monitoring interfaces, 119–121
    - signatures, 160
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 243**
  - e-mail (spam), 245**

**enabling**

- monitoring interfaces, 118
- signatures, 159

**engines**

- AIC, 238
- signatures
  - selecting, 243–244*
  - viewing, 150–151*

**engine-specific signature fields, 229****Enhanced Interior Gateway Routing Protocol (EIGRP), 243****entry points, IP blocking, 308****evasion techniques, 267**

- encryption, 265
- flooding, 263

**Event Action Filters option (IDM), 91****Event Action Overrides option (IDM), 91****Event Action Rules category (IDM), 90****Event Security Indicator, 383****Event Variables option (IDM), 91****event-action-rules mode (CLI command mode), 69****events, 276**

- actions
  - filtering, 281–284*
  - overriding, 279–281*
- counter fields (signatures), 229
- MEG, 230–237
- meta-event generators, 16–17
- severity, 15
- signatures, 228
- Target Value Rating, 279
- variables, 277, 279

**EventStore statistics, 372****execution of setup command, 52–57****expansion boundary (Event Viewer), 383****Exploit Signature page (NSDB), 156****expressions, matching strings, 225–227****extensions (Cisco IPS), 417****external interfaces (ACLs), 311****external sensor communication, 30****Extranet boundaries, deploying sensors, 28****F****false negatives, 266****fields**

- CiscoWorks Add User, 350
- signatures, 227–230

**File Access attacks, 139****File Transfer Protocol (FTP), 237–238****files (NM-CIDS), transferring, 515****filtering, 245–251, 281–284****Fire All alarm, 153****Fire Once alarm, 153****firewalls. *See also* security**

- adding devices, 361
- as IP blocking devices, 306
- sensors (Cisco IOS IDS), 24

**flooding, 263****flow (traffic) notifications, 124–126****formatting, 109, 356–366, 476, 544**

- blocking properties, 315–316
- boot loaders, 513
- CLI, 61
- destination ports, 542
- events, 276
  - filtering actions, 281–284*
  - overriding actions, 279–281*
  - Target Value Rating, 279*
  - variables, 277–279*

**fields, 227–230****hosts (SSH), 116–118****IDM, 79, 83**

- Back icon, 96*
- communication*
  - parameters, 97–98*
- Forward icon, 96*
- Help icon, 96*
- Master Blocking Sensors, 328*
- monitoring, 94–95*
- navigating, 84–94*
- Refresh icon, 96*
- system requirements, 83*

**interfaces**

- inline pairs, 121–123*
- inline software bypasses, 123*
- IPS, 14*

**IPS, 25–26**

- bypasses, 26*
- CLI, 73–74*

**logical devices (IDM), 319–321****responses, 297**

- inline actions, 298–300*
- IP blocking, 303–312, 314–330*
- logging actions, 300–302*
- manual blocking, 330–334*

- Master Blocking Sensors*, 313–314
- TCP reset*, 334
- Security Monitor, 356, 387, 393–397
- sensors, 29, 107
  - accessing SNMP*, 455–457
  - analysis engines*, 126–128
  - debugging*, 448–453
  - events*, 443–447
  - hosts*, 107–118
  - interfaces*, 118–126
  - statistics*, 441–443
  - viewing*, 437–440
- Service accounts, 57
- signatures, 137, 155–162
  - customizing*, 242–253
  - FTP/HTTP policy enforcement*, 237–238
  - groups*, 137–151
  - managing alarms*, 151–155
  - MEG*, 230–237
  - optimizing*, 225–230
  - tuning*, 238–242
- system clocks, 58
- tabs (Security Monitor), 353
- time parameters (sensors), 112
- time zones (sensors), 113
- traffic flow notifications, 124–126
- verifying, 437
- Forward icon (IDM)**, 96
- forwarding packets**, 501–502
- FTP (File Transfer Protocol)**, 237–238
- functionality, verifying signatures**, 244

## G - H

- Global Configuration mode**, 67
- GRE packets (NM-CIDS)**, 501
- group signatures**, 137–151
- guidelines for IP blocking**, 307–310
- hardware**
  - IPS, 17–25
  - NM-CID architecture, 497
- help (CLI)**, 62
- Help icon (IDM)**, 96
- helper images, booting**, 514
- host-based intrusion systems**, 12
- hosts**
  - blocking, 330
  - critical (IP blocking), 308
  - modes, 69

- Request Block Host action, 303
- sensors, 107–118
- SSH
  - adding known*, 60
  - configuring*, 116–118
- HTTP (Hypertext Transfer Protocol)**, 237–238
- hubs, traffic capture**, 530
- hybrid IPS/IDS solutions**, 13–14
- Hypertext Transfer Protocol (HTTP)**, 237–238

## I

- ICMP (Internet Control Message Protocol)**
  - atomic IP signature parameters, 180
  - flood host signature parameters, 184
  - Sweep signature engines, 211
- identifying**
  - signatures, 146
  - traffic, 133
- IDIOM (Intrusion Detection Interaction and Operations Messages)**, 31
- IDM (IPS Device Manager)**, 79, 83, 415, 427–428
  - Back icon, 96
  - blocking, 316
  - communication parameters, 97–98
  - devices, 321–322
  - Forward icon, 96
  - Help icon, 96
  - logical devices, 319–321
  - Master Blocking Sensors, 328
  - monitoring, 94–95
  - navigating, 84–94
  - Refresh icon, 96
  - signatures
    - Custom Signature Wizard*, 248
    - customizing*, 246
  - system requirements, 83
- IDS (Intrusion Detection System)**. *See* **IPS**
  - evasion techniques, 263
    - encryption*, 265
    - flooding*, 263
    - fragmentation*, 263–265
    - obfuscation*, 265–267
    - TTL manipulation*, 267
  - firewall sensors, 24
  - inline mode sensor support, 25
  - router sensors, 24



**IDSM (Cisco IDS Module), 465, 469**

## access routers

*clocks (NM-CIDS)*, 506–508  
*configuring NM-CIDS*, 503–506  
*installing NM-CIDS*, 502–503  
*logging in (NM-CIDS)*, 509–510  
*maintenance (NM-CIDS)*, 510–512  
*monitoring packets (NM-CIDS)*, 509  
*NM-CIDS*, 493–498  
*recovery (NM-CIDS)*, 512–516  
*traffic capture (NM-CIDS)*, 498–502

## features of, 470

## IDSM-2, 23

*Catalyst 6500 switches*, 476–477  
*configuring*, 472–474  
*deploying*, 469–470  
*managing*, 477–478  
*ports*, 475  
*traffic flow*, 471  
*troubleshooting*, 478–483

**images, 423–424**

## applications

*booting*, 516  
*installing*, 515

## helper, 514

**implementation, 109, 356–366, 476, 544**

## blocking properties, 315–316

## boot loaders, 513

## CLI, 61

## destination ports, 542

## events, 276

*filtering actions*, 281–284  
*overriding actions*, 279–281  
*Target Value Rating*, 279  
*variables*, 277–279

## fields, 227–230

## hosts (SSH), 116–118

## IDM, 79, 83

*Back icon*, 96  
*communication parameters*, 97–98  
*Forward icon*, 96  
*Help icon*, 96  
*Master Blocking Sensors*, 328  
*monitoring*, 94–95  
*navigating*, 84–94  
*Refresh icon*, 96  
*system requirements*, 83

## interfaces

*inline pairs*, 121–123  
*inline software bypasses*, 123  
*IPS*, 14

## IPS, 25–26

*bypasses*, 26  
*CLI*, 73–74

## logical devices (IDM), 319–321

## responses, 297

*inline actions*, 298–300  
*IP blocking*, 303–312, 314–330  
*logging actions*, 300–302  
*manual blocking*, 330–334  
*Master Blocking Sensors*, 313–314  
*TCP reset*, 334

## Security Monitor, 356, 387, 393–397

## sensors, 29, 107

*accessing SNMP*, 455–457  
*analysis engines*, 126–128  
*debugging*, 448–453  
*events*, 443–447  
*hosts*, 107–118  
*interfaces*, 118–126  
*statistics*, 441–443  
*viewing*, 437–440

## Service accounts, 57

## signatures, 137, 155–162

*customizing*, 242–253  
*FTP/HTTP policy enforcement*, 237–238  
*groups*, 137–151  
*managing alarms*, 151–155  
*MEG*, 230–237  
*optimizing*, 225–230  
*tuning*, 238–242

## system clocks, 58

## tabs (Security Monitor), 353

## time zones (sensors), 113

## traffic flow notifications, 124–126

## verifying, 437

**initializing sensors (IPS), 51–61****inline action signatures, 298–300****inline deep-packet inspection (IPS), 16****inline mode, 13**

*configuring*, 25–26  
*interfaces*, 121–123  
*sensor support*, 25

**installing, 515**

## Security Monitor, 352

## sensors (IPS), 49–51

**instructions box (Security Monitor), 355**

**Interface Configuration category, 88–89**

**interface vlan command, 540**

**interfaces, 493–494**

- ACLs, 309
- CLI, 45, 415
- command and control, 475–477
- devices, 324
- IDM, 83
  - Back icon, 96*
  - communication parameters, 97–98*
  - Forward icon, 96*
  - Help icon, 96*
  - monitoring, 94–95*
  - navigating, 84–94*
  - Refresh icon, 96*
  - system requirements, 83*
- IPS, 14
- mode, 70
- Security Monitor, 353–356
- sensors, 118–126

**internal clocks, configuring, 112**

**internal interfaces (ACLs), 311**

**Internet boundaries, deploying sensors, 28**

**Internet Control Message Protocol (ICMP)**

- atomic IP signature parameters, 180
- flood host signature parameters, 184
- Sweep signature engines, 211

**Internet Protocol. *See* IP**

**Intranet boundaries, deploying sensors, 28**

**Intrusion Detection Interaction and Operations Messages (IDIOM), 31**

**Intrusion Prevention System. *See* IPS**

**Intrusion Detection System (IDS). *See* IPS**

**IOS, 360–361**

**IP (Internet Protocol)**

- blocking, 303–312, 314–330
- logging, 300–302
- NM-CIDS, 501

**ip access-list command, 539**

**ip inspect command, 539**

**IPS (Intrusion Prevention System), 5**

- analysis engines, 126–128
- bypasses, 26
- CLI, 45
  - configuring, 73–74*
  - initializing sensors, 51–61*
  - installing sensors, 49–51*

*managing, 73*

*modifying, 61–73*

configuring, 25–26, 107

deploying, 27–30

hardware, 17–25

*Cisco IDS 4200 series networks, 17–23*

*Cisco IDSM-2, 23*

*firewalls sensors, 24*

*inline sensor support, 25*

*network modules, 23*

*router sensors, 24*

hosts, 107–118

hybrid IPS/IDS solutions, 13–14

interfaces, 118–126

meta-event generators, 16–17

monitoring, 12–13

overview of, 9

protocols, 30

responses, 297

*inline actions, 298–300*

*IP blocking, 303–312, 314–330*

*logging actions, 300–302*

*manual blocking, 330–334*

*Master Blocking Sensors, 313–314*

*TCP reset, 334*

risk rating, 14–16

signatures, 133

*configuring, 137, 155–162*

*customizing, 242–253*

*FTP/HTTP policies, 237–238*

*groups, 137–151*

*managing alarms, 151–155*

*MEG, 230–237*

*optimizing configuration, 225–230*

*tuning, 238–242*

terminology, 10–11

triggers, 11–12

**IPS Device Manager (IDM), 79, 83, 415, 427–428**

Back icon, 96

blocking, 316

communication parameters, 97–98

devices, 321–322

Forward icon, 96

Help icon, 96

logical devices, 319–321

Master Blocking Sensors, 328

monitoring, 94–95

**IPS Device Manager (IDM) (continued)**

- navigating, 84–94
- Refresh icon, 96
- signatures
  - Custom Signature Wizard*, 248
  - customizing*, 246
- system requirements, 83

**K - L**

- keywords, 64**
  - allowed, 539
  - CLI, 63
- killing TCP connections, 334**
- known host parameters, 117**
- L2/L3/L4 Protocol signatures, viewing, 140**
- layer signatures, viewing, 140–141**
- Log Attacker Packets action, 300**
- Log Pair Packets action, 300**
- Log Victim Packets, 300**
- logger mode (CLI command mode), 71**
- logging, 300–302, 309**
- logical devices, configuring, 319–321**
- loose TCP streams, 275**

**M**

- maintenance for sensors, 411, 415**
  - automatic software updates, 421–422
  - CLI software installations, 419
  - downgrading images, 423
  - IDM software installations, 420–421
  - image recovery, 424
  - resetting, 427–428
  - restoring default configurations, 425–426
  - saving current configurations, 418
  - updating
    - licenses*, 423
    - software*, 415–418
- major versions (Cisco IPS), 416**
- management**
  - alarms, 151–155
  - CiscoWorks 2000, 347
    - adding users*, 349
    - authorization*, 348–349
    - login*, 347–348
    - Security Monitor*, 351–356

- IDM, 79, 83
  - Back icon*, 96
  - communication parameters*, 97–98
  - Forward icon*, 96
  - Help icon*, 96
  - monitoring*, 94–95
  - navigating*, 84–94
  - Refresh icon*, 96
  - system requirements*, 83

IPS, 73

sensors, 29

**manual blocking, 330–334****manual configuration**

- sensor clocks, 112
- system clocks, 58

**manual IP logging, 301–302****Master Blocking Sensors, 313–314**

- defining, 328–330

**match subcommand, 538****matching strings, 225–227****maximum block entries parameter, 316****MEG (Meta-Event Generator), 230–237****messages, e-mail (spam), 245****Meta-Event Generator, 230–237****minor versions (Cisco IPS), 416****Miscellaneous option (IDM), 90****misuse detection (IPS triggers), 11****mls ip ids command, 539****modes**

- alarm summaries, 151–155
- asymmetric, 275
- CLI, 66

**modification**

- of IPS CLIs, 61–73
- of passwords, 59

**modules, IDSM, 465. See also IDSM****monitor session command, 535–536****monitoring**

- IDM, 94–95
- interfaces
  - editing*, 119–121
  - enabling*, 118
- IP, 14
- IPS, 12–13
- NM-CIDS, 493–494
- sensors, 29
- traffic (Catalyst 6500 switches), 477

**Msg Body signature type, 175****multiple sensors, configuring, 30**

## N

**NAC (Network Access Controller), 305**  
**names, viewing signatures, 146**  
**NAT (Network Address Translation), 499–500**  
**navigating**  
     IDM, 84–94  
     Security Monitor, 353–356  
**Network Access Controller (NAC), 305**  
**Network Address Translation (NAT), 499–500**  
**Network Module-Cisco IDS (NM-CIDS), 493–516**  
**network modules for access routers, 23**  
**Network Security Database, 155–159**  
**Network Time Protocol (NTP), 113**  
**network-access mode, 71**  
**network-based intrusion systems, 13**  
**networks, 527–535, 542–544**  
     blocking, 332  
     NM-CIDS architecture, 496  
     protocols, 243  
     sniffing, 13  
     tap traffic flow, 530  
     topologies, 308  
     traffic, 527  
**never-block entries, 317**  
**NM-CIDS (Network Module-Cisco IDS), 493–516**  
**no access-list command, 64**  
**no remote-span command, 537**  
**notifications**  
     configuring, 124–126  
     mode, 71  
**NSDB (Network Security Database), 155–159**  
**NTP (Network Time Protocol), 113**

## O

**Off mode (IPS), 26**  
**On mode (IPS), 26**  
**operating system (OS), viewing, 141**  
**Operator role, 65**  
**optimizing**  
     sensors, 268–269  
         *configuring IP, 269–271*  
         *enforcing, 272–273*  
         *reassembly policies, 274–276*

signature configuration, 225–230  
     *customizing, 242–253*  
     *MEG, 230–237*  
     *tuning, 238–242*

### **Options bar (Security Monitor), 354** **options, 109, 356–366, 476, 544**

blocking properties, 315–316  
 boot loaders, 513  
 CLI, 61  
 destination ports, 542  
 events, 276  
     *filtering actions, 281–284*  
     *overriding actions, 279–281*  
     *Target Value Rating, 279*  
     *variables, 277, 279*  
 fields, 227–230  
 hosts (SSH), 116–118  
 IDM, 79, 83  
     *Back icon, 96*  
     *communication parameters, 97–98*  
     *Forward icon, 96*  
     *Help icon, 96*  
     *Master Blocking Sensors, 328*  
     *monitoring, 94–95*  
     *navigating, 84–94*  
     *Refresh icon, 96*  
     *system requirements, 83*  
 interfaces  
     *inline pairs, 121–123*  
     *inline software bypasses, 123*  
     *IPS, 14*  
 IPS, 25–26  
     *bypasses, 26*  
     *CLI, 73–74*  
 logical devices (IDM), 319–321  
 responses, 297  
     *inline actions, 298–300*  
     *IP blocking, 303–312, 314–330*  
     *logging actions, 300–302*  
     *manual blocking, 330–334*  
     *Master Blocking Sensors, 313–314*  
     *TCP reset, 334*  
 Security Monitor, 356, 387, 393–397  
 sensors, 29, 107  
     *accessing SNMP, 455–457*  
     *analysis engines, 126–128*  
     *debugging, 448–453*  
     *events, 443–447*  
     *hosts, 107–118*

**options** (*continued*)

- interfaces*, 118–126
- statistics*, 441–443
- viewing*, 437–440
- Service accounts, 57
- signatures, 137, 155–162
  - customizing*, 242–253
  - FTP/HTTP policy enforcement*, 237–238
  - groups*, 137–151
  - managing alarms*, 151–155
  - MEG*, 230–237
  - optimizing*, 225–230
  - tuning*, 238–242
- system clocks, 58
- tabs (Security Monitor), 353
- time zones (sensors), 113
- traffic flow notifications, 124–126
- verifying, 437
- OS (operating system), viewing**, 141
- overlapping fragments**, 264

**P****packet capture command**, 450**packet display command**, 450**packets**

- analyzing logging actions, 300–302
- Deny Packet inline action, 298
- NM-CIDS, 501–502
- TCP reset, 334

**pairs (interface), configuring**, 121–123**parameters**

- Cisco IPS signatures, 173
- communication (IDM), 97–98
- content types, 174
- dates, 114
- duration of inline actions, 299
- ip access-list command, 539
- known hosts, 117
- monitoring interfaces, 119–121
- set vlan command, 476
- signatures, 244
- time, 112
- traffic flow notification, 125

**passwords**

- commands, 59
- CLI, 51
- modifying, 59

**path bar (Security Monitor)**, 355**patterns, searching**, 225–227**performance**, 469. *See also* **optimizing****perimeters**, 28**PIX Firewalls**

- adding devices, 361
- as IP blocking devices, 306
- sensors (Cisco IOS IDS), 24

**placement**

- of ACLs (IP blocking), 310–312
- of sensors, 29

**policies, FTP/HTTP enforcement**, 237–238**Policy Violation signatures**, 139**ports**

- destination, 542
- RSPAN, 533–537
- SPAN, 533–536
- targets, 243
- VLANs, 543–544

**PostOffice devices, adding**, 359**powering down sensors**, 427–428**Privileged Exec mode**, 67**processes, IP blocking**, 310**promiscuous mode, configuring**, 25–26**prompts (CLI)**, 62**properties**

- blocking, 93, 315–316
- CLI, 61

**protocols**

- analysis (IPS triggers), 12
- ARP, 177
- EIGRP, 243
- FTP
  - IC signature engine parameters*, 173
  - policy enforcement*, 237–238
- HTTP, 237–238
- IOS, 360–361
- IP, 300–302
- L2/L3/L4, 140
- networks, 243
- NTP, 113
- PIX, 361
- PostOffice, 359
- RDEP, 31, 356–359
- sensors, 30
- signatures, 144–146
- SNMP, 93
- TCP, 334

## R

- rating, 279**
  - risks, 14–16
  - Target Values, 279
- RDEP (Remote Data Exchange Protocol), 31, 356–359**
- readme extension, 417**
- recall commands, 63**
- reconnaissance signatures, 139**
- recover application-partition command, 424**
- Refresh icon (IDM), 96**
- regular expressions, 225–227**
- Related Threats field (NSDB), 157**
- releases, viewing signatures, 143**
- reloading NM-CIDS, 511**
- remote access boundaries, sensors, 28**
- Remote Data Exchange Protocol (RDEP), 31, 356–359**
- Remote Switched Port Analyzer (RSPAN), 533–537**
- remote-span command, 536**
- Request Block Connection action, 303**
- Request Block Host action, 303**
- Request Methods signature type, 175**
- requirements**
  - clients, 352
  - servers, 352
- reset command, 57, 478**
- resetting**
  - NM-CIDS, 511
  - sensors, 427–428
  - TCP, 334
- responses**
  - actions, 149–150
  - IPS, 297
    - inline actions, 298–300*
    - IP blocking, 303–312, 314–330*
    - logging actions, 300–302*
    - manual blocking, 330–334*
    - Master Blocking Sensors, 313–314*
    - TCP reset, 334*
  - signatures, 161–162
- restoring, 425–426**
- retiring signatures, 160**
- risk rating (RR), 14–16**
- roles**
  - Administrator, 65
  - Operator, 65
  - Service, 66
  - user (CiscoWorks 2000), 349
  - users, 64
  - Viewer, 66

- root accounts, 66**

- routers**

- access, 23
- as IP blocking devices, 304
- sensors (Cisco IOS IDS), 24

- rpm.pkg extension, 417**

- RR (risk rating), 14–16**

- RSPAN (Remote Switched Port Analyzer), 533–537**

- rules for events**

- activating, 368
- adding, 364–368

## S

- searching patterns, 225–227**

- Secure Shell (SSH), 31, 60**

- security**

- IPS

- bypasses, 26*
- configuring, 25–26*
- deploying, 27–30*
- hardware, 17–25*
- hybrid IPS/IDS solutions, 13–14*
- meta-event generators, 16–17*
- monitoring, 12–13*
- overview of, 9*
- protocols, 30*
- risk rating, 14–16*
- terminology, 10–11*
- triggers, 11–12*

- NSDB, 156–159

- Security Monitor**

- configuring, 356
  - adding devices, 356–361*
  - event notification, 363–368*
  - Event Viewer, 374–386*
  - importing devices, 361–363*
  - monitoring devices, 368–374*
- managing, 387
  - data, 387, 390–391*
  - Event Viewer preferences, 392*
  - system configuration, 391–392*
- reports, 393–397

**selecting**

- event types, 446
- IP blocking, 308
- signature engines, 243
- strong passwords, 51

**senior user accounts, configuring, 109****Sensor Setup (IDM), 87–88****sensors, 527**

- analysis engines, 126–128
- clocks, 112
- configuring, 107
- events, 276
  - filtering actions*, 281–284
  - overriding actions*, 279–281
  - Target Value Rating*, 279
  - variables*, 277, 279
- hosts, 107–118
- IDS evasion, 263
  - encryption*, 265
  - flooding*, 263
  - fragmentation*, 263–265
  - obfuscation*, 265–267
  - TTL manipulation*, 267
- IDSM, 469
  - Catalyst 6500 switches*, 476–477
  - configuring IDSM-2*, 472–474
  - deploying IDSM-2*, 469–470
  - features of*, 470
  - managing (IDSM-2)*, 477–478
  - ports (IDSM-2)*, 475
  - traffic flow (IDSM-2)*, 471
  - troubleshooting (IDSM-2)*, 478–483
- interfaces, 118–126
- IPS, 5
  - bypasses*, 26
  - Cisco IDS 4200 switches*, 17–23
  - Cisco IDSM-2 (for Catalyst 6500)*, 23
  - configuring*, 25–26
  - deploying*, 27–30
  - firewalls*, 24
  - hardware*, 17–25
  - hybrid IPS/IDS solutions*, 13–14
  - IDM*. *See also* IDM, 79
  - initializing*, 51–61
  - inline sensor support*, 25
  - installing*, 49–51
  - meta-event generators*, 16–17
  - monitoring*, 12–13
  - network module for access routers*, 23

- overview of*, 9
- protocols*, 30
- risk rating*, 14–16
- routers*, 24
- terminology*, 10–11
- triggers*, 11–12

**maintenance, 411, 415**

- automatic software updates*, 421–422
- CLI software installations*, 419
- downgrading images*, 423
- IDM software installations*, 420–421
- image recovery*, 424
- licenses*, 423
- resetting*, 427–428
- restoring configurations*, 425–426
- saving current configurations*, 418
- updating software*, 415–418

**optimizing, 268–269**

- configuring IP log settings*, 269–271
- enforcing application policies*, 272–273
- reassembly options*, 274–276

**responses, 297**

- inline actions*, 298–300
- IP blocking*, 303–312, 314–330
- logging actions*, 300–302
- manual blocking*, 330–334
- Master Blocking Sensors*, 313–314
- TCP reset*, 334

**signatures, 133**

- configuring*, 137, 155–162
- customizing*, 242–253
- FTP/HTTP policy enforcement*, 237
- groups*, 137–151
- managing alarms*, 151–155
- MEG*, 230–237
- optimizing configuration*, 225–230
- tuning*, 238–242

**virtual, 89****servers**

- IPS deployment, 29
- NTP, 113
- requirements, 352

**Service accounts, creating, 57****Service mode (CLI command mode), 68****service notification command, 455****service packs, 417****Service role, 66****services, viewing signatures, 144–146**

**session command, 474**

**session slot command, 474**

**set security acl command, 541**

**set vlan command, 476**

**setup command, 52–57**

**severity (event), 15**

**show commands**

show configuration command, 438

show events command, 444

show interfaces command, 448

show inventory command, 441

show module command, 479–481

show module switch command, 472

show port command, 482

show statistics command, 441

show tech-support command, 448, 452

show trunk command, 483

show version command, 438

**shun command, 306**

**shutting down NM-CIDS, 511**

**Signature Configuration option (IDM), 90**

**Signature Definition category (IDM), 90**

**signature fidelity ratings, 15**

**Signature Variables option (IDM), 90**

**signature-definition mode, 72**

**signatures**

Cisco IPS, 171, 417

*AIC FTP engines, 173*

*AIC HTTP engines, 173–176*

*atomic engines, 177–183*

*engines, 171–172*

*flood engines, 183–186*

*Meta Signature engines, 187*

*Normalizer Signature engines, 188*

*parameters, 172*

*service signature engines, 189–204*

*state signature engines, 204–207*

*String signature engines, 208–209*

*Sweep signature engines, 210–215*

*Trojan horse signature engines, 215*

cloning, 253

connections, 92

creating, 160

defining, 161–162

editing, 160

enabling, 159

engines, 243–244

fields, 227–230

filtering, 245–251

functionality, 244

IPS, 133

*configuring, 137, 155–162*

*customizing, 242–253*

*FTP/HTTP policy enforcement, 237–238*

*groups, 137–151*

*managing alarms, 151–155*

*MEG, 230–237*

*optimizing configuration, 225–230*

*tuning, 238–242*

parameters, 244

responses, 297

*inline actions, 298–300*

*IP blocking, 303–312, 314–330*

*logging actions, 300–302*

*manual blocking, 330–334*

*Master Blocking Sensors, 313–314*

*TCP reset, 334*

retiring, 160

selecting, 308

testing, 245

**Simple Mail Transport Protocol, 207**

**Simple Network Management Protocol (SNMP), 93**

**single sensors, configuring, 30**

**SMTP (Simple Mail Transport Protocol), 207**

**sniffing networks, 13**

**SNMP (Simple Network Management Protocol), 93**

**software types, 416**

**Sort By group box (Event Viewer), 382**

**spam, 245**

**SPAN (Switched Port Analyzer), 533**

configuring, 535–536

**speed (interface), 119**

**spoofing, antispoofing mechanisms, 307**

**Spyware signatures, viewing, 139**

**SQL (Structured Query Language), 198**

**SSH (Secure Shell), 31, 60**

**ssh host-key command, 60**

**ssh-known-hosts mode, 72**

**status**

fields (signatures), 230

NM-CIDS, 512

**streams**

loose TCP, 275

strict TCP, 275

**strict TCP streams, 275**



- strings, matching, 225–227
- Structured Query Language (SQL), 198
- subcommands
  - action, 538
  - match, 538
- summaries of alarms, 151–155
- summertime settings, configuring, 114–115
- Switched Port Analyzer (SPAN), 533
  - configuring, 535–536
- switches
  - Catalyst 6000
    - as blocking devices, 326
    - as IP blocking devices, 305
  - IDS/SM, 469
  - traffic flow, 532
- switchport access vlan command, 476
- switchport capture allowed vlan command, 541
- switchport capture command, 539–541
- switchport trunk command, 543
- syntax for regular expressions, 225–227
- system clocks, configuring, 58
- system configuration. *See* configuration
- system requirements, 83

## T

- tabs
  - completion, 63
  - configuration, 353
- tap (network) traffic flow, 530
- Target Value Rating, 91, 279
- targets
  - addresses, 243
  - asset value of, 16
  - ports, 243
- TCP (Transmission Control Protocol)
  - atomic IP signature parameters, 181
  - Normalizer signature engines, 188
  - reset, 334
  - Sweep signature engines, 211
- testing signatures, 245
- threats (NSDB), 157
- time
  - events, 385
  - frames for events, 447
  - sensors, 112
  - zones, 113

- Time to Live, 267
- TOC (Security Monitor), 355
- tools
  - bar (Security Monitor), 356
  - CiscoWorks 2000, 347
- topologies, IP blocking, 308
- traffic
  - blocking, 92
  - bridging, 527
  - capturing, 527
    - Catalyst 6500 switches, 542–544
    - devices, 529–531
    - inline mode, 527–529
    - promiscuous mode, 529
    - switches, 532–534
    - TCP resets and switches, 535
  - Catalyst 6500 switches, 477
  - Cisco IPS signatures, 171
  - flow, 124–126
  - identifying, 133
  - IPS
    - bypasses, 26
    - configuring, 25–26
    - deploying, 27–30
    - hardware, 17–25
    - hybrid IPS/IDS solutions, 13–14
    - meta-event generators, 16–17
    - monitoring, 12–13
    - overview of, 9
    - protocols, 30
    - risk rating, 14–16
    - terminology, 10–11
    - triggers, 11–12
- Transfer Encodings signature type, 176
- transferring files (NM-CIDS), 515
- transitions, Cisco Login state machines, 206
- Transmission Control Protocol (TCP). *See* TCP
- triggers
  - IPS, 11–12
  - responses, 297
    - inline actions, 298–300
    - IP blocking, 303–312, 314–330
    - logging actions, 300–302
    - manual blocking, 330–334
    - Master Blocking Sensors, 313–314
    - TCP reset, 334
  - signatures, 228

**Trojan horse signatures, 139**

**troubleshooting**

CLI, 62

signatures, 245

**trunking, 543–544**

**trusted-certificates mode, 72**

**TTL (Time to Live), 267**

**tuning**

existing signatures, 238–242

sensors, 268–269

*configuring IP logs, 269–271*

*encryption, 265*

*enforcing policies, 272–273*

*flooding, 263*

*fragmentation, 263–265*

*IDS evasion, 263*

*obfuscation, 265–267*

*reassembly options, 274–276*

*TTL manipulation, 267*

**types**

of attacks

*selecting signature engines, 244*

*viewing signatures, 137–139*

of content, 174

of events, 446

of layers, 140–141

of software, 416

## U

**UART (Universal Asynchronous**

**Receiver/Transmitter), 498**

**UDP (User Datagram Protocol)**

atomic Ip signature parameters, 182

flood host signature parameters, 185

**Universal Asynchronous Receiver/**

**Transmitter, 498**

**updating, 415–423**

Auto Update (IDM), 94

**upgrade command, 49, 419**

**User Datagram Protocol. *See* UDP**

**username command, 59**

**users**

adding/deleting, 59

CiscoWorks 2000, 349

roles, 64

senior accounts, 109

## V

**VACL (VLAN Access Control List),**

**311, 534**

configuring, 537–541, 544

**values**

asset value of targets, 16

signatures, 228

**variables**

alarm summarization, 154

events, 277–279

**verifying, 437–445, 447–457**

signature functionality, 244

system configuration, 437

**versions, Cisco IPS, 416**

**Viewer role, 66**

**viewing**

NM-CIDS, 512

NSDB, 156–159

signatures, 137–151

**virtual LANs (VLANs). *See* VLANs**

**Virtual Sensor option (IDM), 89**

**virus signatures, 139**

**VLAN Access Control List (VACL),**

**311, 534**

configuring, 537–541, 544

**vlan filter command, 538**

**VLANs (virtual LANs)**

Catalyst 6500 switches, 476

ports, 543–544

traffic capture, 527–529

## W - Z

**war dialers, 29**

**web-server mode (CLI command**

**mode), 73**

**Windows Security Monitor, installing, 352**

**wizards, Custom Signature Wizard,**

**90, 248**

**worm signatures, 139**

**zip extension, 417**

**zones (time), configuring, 113**