## Index

Д	events
	filtering, 281–284
access control lists. See ACLs	overriding, 279–281
access routers	inline signatures, 298–300
CLI, 51	logging, 300–302
network module for, 23	signatures
NM-CIDS, 493–494	response, 162
architecture, 495–497	viewing, 149–150
clocks, 506–508	Actions group box (Event Viewer), 381
configuring, 503–506	activating event rules, 368
external Fast Ethernet interfaces, 498	adding, 357–361
Flash, 498	event rules, 364–368
front panels, 494	inline functionality, 298-300
installing, 502–503	known SSH hosts, 60
internal Fast Ethernet interfaces, 498	users, 59
logging in, 509–510	Address Resolution Protocol (ARP), 177
maintenance, 510–516	addresses
memory, 498	blocking, 317–319
packet monitoring, 509	IP (Internet Protocol)
specifications, 494	blocking, 303–312, 314–330
traffic capture, 498–502	logging, 300–302
UART, 498	NM-CIDS, 501
access-list command, 64	targets, 243
accounts	Administrator roles, 65
root, 66	advanced signature configuration, 225-230
senior user, 109	customizing, 242–253
Service, 57	MEG, 230–237
ACLs (access control lists)	tuning, 238–242
configuring, 537–541, 544	Adware, viewing signatures, 139
interfaces	AIC (Application Inspection and Control)
external/internal, 311	engines, 238
IP blocking, 309	alarms
NM-CIDS, 499	CiscoWorks 2000, 347–356
placement (IP blocking), 310–312	Fire All, 153
VACLs, 534	Fire Once, 153
action subcommand, 538	managing, 151–155
actions, 300–302	alerts, frequency fields (signatures), 230
assigning, 314	allowed hosts, configuring, 107–109
blocking, 92	

allowed keyword, 539	hybrid IPS/IDS solutions, 13–14
alternate TCP-reset interface, 120	meta-event generators, 16–17
analysis, 535–537	monitoring, 12–13
engines	overview of, 9
category (IDM), 89	protocols, 30
mode (CLI command	risk rating, 14–16
mode), 68	terminology, 10–11
sensors, 126–128	triggers, 11–12
packets, 300–302	signatures, 137–139
RSPAN, 533	TTL, 267
signatures, 244	types of, 244
SPAN, 533	authentication mode (CLI command
anomaly detection (IPS triggers), 11	mode), 69
antispoofing mechanisms, 307	Auto mode (IPS), 26
appliance sensors, 49. See also sensors	Auto Update (IDM), 94
Application Inspection and Control (AIC)	automatic alarm summarization, 154
engines, 238	
applications	Б
images	В
booting, 516	Back icon (IDM), 96
installing, 515	basic signature fields, 227
policy enforcement (FTP/HTTP),	Block Properties option (IDM), 93
237–238	blocking
signatures, 143	actions, 92
types, 416	addresses, 317–319
ARP (Address Resolution Protocol), 177	assigning, 314
asset value of targets, 16	devices, 321–326
assignment, 543–544	durations, 309
blocking actions, 314	hosts, 330
asymmetric mode, 275	IP, 303–312, 314–330
attacks, 171–215. See also security	manual, 330–334
Cisco IPS signatures, 171	networks, 332
deny Attacker inline action, 298	properties, 315–316
inline actions (duration parameters), 299	boot loaders, configuring, 513
IPS, 5	booting, 516
bypasses, 26	helper images, 514
configuring, 25–26	boundaries, 28
deploying, 27–30	Boundaries group box
hardware, 17–25	(Event Viewer), 383
	(Evelle viewel), 303

bridging traffic, 527	traffic flow, 471
bypasses	troubleshooting, 478–483
interfaces, 123	Cisco IOS, 360-361
IPS, 26	Cisco IPS. See IPS
	Cisco PIX Firewalls
	adding devices, 361
C	as IP blocking devices, 306
calculating risk ratings, 14–16	sensors (Cisco IOS IDS), 24
capturing traffic, 527	CiscoWorks 2000, 347
Catalyst 6500 switches, 542–544	adding users, 349
devices, 529–531	authorization, 348–349
inline mode, 527–529	login, 347–348
promiscuous mode, 529	Security Monitor, 351–356
switches, 532–534	adding devices, 356–361
	configuring, 356
TCP resets and switches, 535	event notification, 363–368
case sensitivity commands, 63	Event Viewer, 374–386
Catalyst 6000 switches, 469–475, 477–483	importing devices, 361–363
blocking interfaces, 326	managing, 387–392
IDSM, 469–470	monitoring devices, 368–374
as IP blocking devices, 305	reports, 393–397
Catalyst 6500 switches, 23, 476–477	CLI (command-line interface), 45, 415, 427
cells (Event Viewer), 381	configuring, 73–74
children events, 385	initializing sensors, 51–61
Cisco 4215 appliance sensor, 18	installing sensors, 49–51
Cisco 4235 appliance sensor, 19	managing, 73
Cisco 4240 diskless appliance sensor, 20	modifying, 61–73
Cisco 4250 appliance sensor, 21	client requirements (Security
Cisco 4250XL appliance sensor, 21	Monitor), 352
Cisco 4255 diskless appliance sensor, 22	clock set command, 58
Cisco IDS 4200 series network	clocks, configuring, 58
sensors, 17–23	cloning signatures, 253
Cisco IDS Module, 465, 469	Code Execution attacks, 139
access routers	command and control interface, 475–477
clocks (NM-CIDS), 506–508	Command Execution attacks, 139
configuring NM-CIDS, 503–506	Command Timeout, 381
installing NM-CIDS, 502–503	command-line interface. See CLI
logging in (NM-CIDS), 509–510	commands
maintenance (NM-CIDS), 510–512	access-list, 64
monitoring packets (NM-CIDS), 509	case sensitivity, 63
NM-CIDS, 493–498	CLI command modes, 66
recovery (NM-CIDS), 512–516	clock set, 58
traffic capture (NM-CIDS), 498–502	configure terminal, 67
features of, 470	copy, 451
IDSM-2, 23	default service, 425
Catalyst 6500 switches, 476–477	downgrade, 94, 423
configuring, 472–474	interface vlan, 540
deploying, 469–470	ip access-list, 539
managing, 477–478	ip inspect, 539
ports, 475	-pp,

1 : :1 520	T (VI D ( 270
mls ip ids, 539	Target Value Rating, 279
monitor session, 535–536	variables, 277, 279
no access-list, 64	hosts (SSH), 116–118
no remote-span, 537	IDM, 79, 83
packet capture, 450	Back icon, 96
packet display, 450	communication parameters, 97–98
password, 59	Forward icon, 96
recall, 63	Help icon, 96
recover application-pattern, 424	Master Blocking Sensors, 328
remote-span, 536	monitoring, 94–95
reset, 57, 427, 478	navigating, 84–94
service notification, 455	Refresh icon, 96
session, 474	system requirements, 83
session slot, 474	interfaces
set security acl, 541	inline pairs, 121–123
set vlan, 476	inline software bypasses, 123
setup, 52–57	IPS, 14
show configuration, 438	IPS, 25–26
show events, 444	bypasses, 26
show interfaces, 448	CLI, 73–74
show inventory, 441	logical devices (IDM), 319–321
show module, 479–481	responses, 297
show module switch, 472	inline actions, 298–300
show port, 482	IP blocking, 303–312, 314–330
show statistics, 441	logging actions, 300–302
show tech-support, 448, 452	manual blocking, 330–334
show trunk, 483	Master Blocking Sensors, 313–314
show version, 438	TCP reset, 334
shun, 306	Security Monitor, 356, 387, 393-397
ssh host-key, 60	sensors, 27, 107
subcommands. See subcommands	accessing SNMP, 455–457
switchport access vlan, 476	analysis engines, 126–128
switchport capture, 539–541	debugging, 448–453
switchport capture allowed vlan, 541	events, 443–447
switchport trunk, 543	hosts, 107–118
upgrade, 49, 419	interfaces, 118–126
username, 59	statistics, 441–443
vlan filter, 538	viewing, 437–440
communication parameter configuration	Service accounts, 57
(IDM), 97–98	signatures, 137, 155–162
completion, tabs, 63	customizing, 242–253
configuration, 109, 356–366, 476, 544	FTP/HTTP policy enforcement, 237–238
blocking properties, 315–316	groups, 137–151
boot loaders, 513	managing alarms, 151–155
CLI, 61	MEG, 230–237
destination ports, 542	optimizing, 225–230
events, 276	tuning, 238–242
filtering actions, 281–284	system clocks, 58
overriding actions, 279–281	tabs (Security Monitor), 353
overriumg actions, 2/3-201	taus (Security Montton), 333

configuration (continued)	logical devices (IDM), 319–321
time parameters (sensors), 112	responses, 297
time zones (sensors), 113	inline actions, 298–300
traffic flow notifications, 124-126	IP blocking, 303-312, 314-330
verifying, 437	logging actions, 300–302
Configuration icon (IDM), 84–86	manual blocking, 330–334
configure terminal command, 67	Master Blocking Sensors, 313–314
connections	TCP reset, 334
blocking signatures, 92	Security Monitor, 356, 387, 393-397
deny Connection Inline action, 298	sensors, 29, 107
Request Block Connection action, 303	accessing SNMP, 455-457
TCP reset, 334	analysis engines, 126–128
content	debugging, 448–453
areas (Security Monitor), 356	events, 443–447
type parameters, 174	hosts, 107–118
copy command, 451	interfaces, 118–126
copying signatures, 253	statistics, 441–443
creating. See formatting	viewing, 437–440
critical hosts (IP blocking), 308	Service accounts, 57
Custom Signature Wizard, 90, 248	signatures, 137, 155–162
customization, 109, 356–366, 476, 544	customizing, 242–253
blocking properties, 315–316	FTP/HTTP policy enforcement, 237–238
boot loaders, 513	groups, 137–151
CLI, 61	managing alarms, 151–155
destination ports, 542	MEG, 230–237
events, 276	optimizing, 225–230
filtering actions, 281–284	tuning, 238–242
overriding actions, 279–281	system clocks, 58
Target Value Rating, 279	tabs (Security Monitor), 353
variables, 277–279	time parameters (sensors), 112
fields, 227–230	time zones (sensors), 113
hosts (SSH), 116–118	traffic flow notifications, 124–126
IDM, 79, 83	verifying, 437
Back icon, 96	vernying, 437
communication parameters, 97–98	_
Forward icon, 96	D
Help icon, 96	Databasa group boy (Event Viewer) 394
Master Blocking Sensors, 328	Database group box (Event Viewer), 384
monitoring, 94–95	databases, viewing NSDB, 156–159
navigating, 84–94	date parameters, 114
0 0	daylight savings time, configuring, 114–115
Refresh icon, 96	DDoS (Distributed Denial of Service)
system requirements, 83 interfaces	attacks, 139
	default keyword, 64
inline pairs, 121–123	default service command, 425
inline software bypasses, 123	Define Web Traffic Policy signature
IPS, 14	type, 175
IPS, 25–26	defining
bypasses, 26	addresses, 317–319
CLI, 73–74	Master Blocking Sensors, 328–330

parameters, 244	debugging, 448–453
signatures, 161–162	events, 443–447
trunks for traffic capture, 543–544	hosts, 107–118
deleting users, 59	interfaces, 118–126
Denial of Service (DoS) attacks, 139	statistics, 441–443
Deny Attacker Inline action, 298	viewing, 437–440
Deny Connection Inline action, 298	Service accounts, 57
Deny Packet Inline action, 298	signatures, 137, 155–162
deployment, 109, 356-366, 476, 544	customizing, 242–253
blocking properties, 315–316	FTP/HTTP policy
boot loaders, 513	enforcement, 237–238
CLI, 61	groups, 137–151
destination ports, 542	managing alarms, 151–155
events, 276	MEG, 230–237
filtering actions, 281–284	optimizing, 225–230
overriding actions, 279–281	tuning, 238–242
Target Value Rating, 279	system clocks, 58
variables, 277, 279	tabs (Security Monitor), 353
hosts (SSH), 116–118	time parameters (sensors), 112
IDM, 79, 83	time zones (sensors), 113
Back icon, 96	traffic flow notifications, 124-126
communication	verifying, 437
parameters, 97–98	description (interface), 119
Forward icon, 96	description fields (signatures), 228
Help icon, 96	desktops, IPS deployment, 29
Master Blocking Sensors, 328	destination ports, configuring, 542
monitoring, 94–95	devices. See also IDM
navigating, 84–94	blocking, 321–326
Refresh icon, 96	IP blocking, 304–306
system requirements, 83	logging, 309
interfaces	logical, 319–321
inline pairs, 121–123	Distributed Denial of Service (DDoS)
inline software bypasses, 123	attacks, 139
IPS, 14	DoS (Denial of Service) attacks, 139
IPS, 25–26	downgrade command, 94
bypasses, 26	downgrading images, 423
CLI, 73–74	duplex (interface), 119
logical devices (IDM), 319–321	duration
responses, 297	inline actions, 299
inline actions, 298–300	IP blocking, 309
IP blocking, 303–312, 314–330	
logging actions, 300–302	_
manual blocking, 330–334	E
Master Blocking Sensors, 313–314	editing
TCP reset, 334	monitoring interfaces, 119–121
Security Monitor, 356, 387, 393-397	signatures, 160
sensors, 27, 107	EIGRP (Enhanced Interior Gateway
accessing SNMP, 455–457	Routing Protocol), 243
analysis engines, 126–128	e-mail (spam), 245
	C-man (Spam), 273

enabling	File Access attacks, 139
monitoring interfaces, 118	File Transfer Protocol (FTP),
signatures, 159	237–238
engines	files (NM-CIDS), transferring, 515
AIC, 238	filtering, 245–251, 281–284
signatures	Fire All alarm, 153
selecting, 243–244	Fire Once alarm, 153
viewing, 150–151	firewalls. See also security
engine-specific signature fields, 229	adding devices, 361
Enhanced Interior Gateway Routing	as IP blocking devices, 306
Protocol (EIGRP), 243	sensors (Cisco IOS IDS), 24
entry points, IP blocking, 308	flooding, 263
evasion techniques, 267	flow (traffic) notifications, 124–126
encryption, 265	formatting, 109, 356–366, 476, 544
flooding, 263	blocking properties, 315–316
Event Action Filters option (IDM), 91	boot loaders, 513
Event Action Overrides option (IDM), 91	CLI, 61
Event Action Rules category (IDM), 90	destination ports, 542
Event Security Indicator, 383	events, 276
Event Variables option (IDM), 91	filtering actions, 281–284
event-action-rules mode (CLI command	overriding actions, 279–281
mode), 69	Target Value Rating, 279
events, 276	variables, 277–279
actions	fields, 227–230
filtering, 281–284	hosts (SSH), 116–118
overriding, 279–281	IDM, 79, 83
counter fields (signatures), 229	Back icon, 96
MEG, 230–237	communication
meta-event generators, 16–17	parameters, 97–98
severity, 15	Forward icon, 96
signatures, 228	Help icon, 96
Target Value Rating, 279	Master Blocking Sensors, 328
variables, 277, 279	monitoring, 94–95
EventStore statistics, 372	navigating, 84–94
execution of setup command, 52–57	Refresh icon, 96
expansion boundary (Event Viewer), 383	system requirements, 83
Exploit Signature page (NSDB), 156	interfaces
expressions, matching strings, 225–227	inline pairs, 121–123
extensions (Cisco IPS), 417	inline software bypasses, 123
external interfaces (ACLs), 311	IPS, 14
external sensor communication, 30	IPS, 25–26
Extranet boundaries, deploying sensors, 28	bypasses, 26
	CLI, 73–74
_	logical devices (IDM), 319–321
F	responses, 297
false negatives, 266	inline actions, 298–300
fields	IP blocking, 303–312, 314–330
CiscoWorks Add User, 350	logging actions, 300–302
signatures, 227–230	manual blocking, 330–334

Master Blocking Sensors, 313–314	Request Block Host action, 303
TCP reset, 334	sensors, 107–118
Security Monitor, 356, 387, 393–397	SSH
sensors, 29, 107	adding known, 60
accessing SNMP, 455–457	configuring, 116–118
analysis engines, 126–128	HTTP (Hypertext Transfer Protocol),
debugging, 448–453	237–238
events, 443–447	hubs, traffic capture, 530
hosts, 107–118	hybrid IPS/IDS solutions, 13–14
interfaces, 118–126	Hypertext Transfer Protocol (HTTP), 237–238
statistics, 441–443	
viewing, 437–440	I
Service accounts, 57	1
signatures, 137, 155–162	ICMP (Internet Control Message Protocol)
customizing, 242–253	atomic IP signature parameters, 180
FTP/HTTP policy enforcement, 237–238	flood host signature parameters, 184
groups, 137–151	Sweep signature engines, 211
managing alarms, 151–155	identifying
MEG, 230–237	signatures, 146
optimizing, 225–230	traffic, 133
tuning, 238–242	<b>IDIOM (Intrusion Detection Interaction</b>
system clocks, 58	and Operations Messages), 31
tabs (Security Monitor), 353	IDM (IPS Device Manager), 79, 83, 415,
time parameters (sensors), 112	427–428
time zones (sensors), 113	Back icon, 96
traffic flow notifications, 124–126	blocking, 316
verifying, 437	communication parameters, 97–98
Forward icon (IDM), 96	devices, 321–322
forwarding packets, 501–502	Forward icon, 96
FTP (File Transfer Protocol), 237–238	Help icon, 96
functionality, verifying signatures, 244	logical devices, 319–321
	Master Blocking Sensors, 328
G - H	monitoring, 94–95
	navigating, 84–94
Global Configuration mode, 67	Refresh icon, 96
GRE packets (NM-CIDS), 501	signatures
group signatures, 137–151	Custom Signature Wizard, 248
guidelines for IP blocking, 307–310	customizing, 246
Landman	system requirements, 83
hardware	IDS (Intrusion Detection System). See IPS
IPS, 17–25	evasion techniques, 263
NM-CID architecture, 497	encryption, 265
help (CLI), 62	flooding, 263
Help icon (IDM), 96	fragmentation, 263–265
helper images, booting, 514	obfuscation, 265–267
host-based intrusion systems, 12	TTL manipulation, 267
hosts	firewall sensors, 24
blocking, 330	inline mode sensor support, 25
critical (IP blocking), 308	**
modes, 69	router sensors, 24

IDSM (Cisco IDS Module), 465, 469	interfaces
access routers	inline pairs, 121–123
clocks (NM-CIDS), 506–508	inline software bypasses, 123
configuring NM-CIDS, 503-506	IPS, 14
installing NM-CIDS, 502–503	IPS, 25–26
logging in (NM-CIDS), 509–510	bypasses, 26
maintenance (NM-CIDS), 510–512	CLI, 73–74
monitoring packets	logical devices (IDM), 319–321
(NM-CIDS), 509	responses, 297
NM-CIDS, 493–498	inline actions, 298–300
recovery (NM-CIDS), 512–516	IP blocking, 303–312, 314–330
traffic capture (NM-CIDS),	logging actions, 300–302
498–502	manual blocking, 330–334
features of, 470	Master Blocking Sensors, 313–314
IDSM-2, 23	TCP reset, 334
Catalyst 6500 switches, 476–477	Security Monitor, 356, 387, 393-397
configuring, 472–474	sensors, 29, 107
deploying, 469–470	accessing SNMP, 455–457
managing, 477–478	analysis engines, 126–128
ports, 475	debugging, 448–453
traffic flow, 471	events, 443–447
troubleshooting, 478–483	hosts, 107–118
images, 423–424	interfaces, 118–126
applications	statistics, 441–443
booting, 516	viewing, 437–440
installing, 515	Service accounts, 57
helper, 514	signatures, 137, 155–162
implementation, 109, 356–366, 476, 544	customizing, 242–253
blocking properties, 315–316	FTP/HTTP policy enforcement, 237–238
boot loaders, 513	groups, 137–151
CLI, 61	managing alarms, 151–155
destination ports, 542	MEG, 230–237
events, 276	optimizing, 225–230
filtering actions, 281–284	tuning, 238–242
overriding actions, 279–281	system clocks, 58
Target Value Rating, 279	tabs (Security Monitor), 353
variables, 277–279	time zones (sensors), 113
fields, 227–230	traffic flow notifications, 124–126
hosts (SSH), 116–118	verifying, 437
IDM, 79, 83	initializing sensors (IPS), 51–61
Back icon, 96	inline action signatures, 298–300
communication parameters, 97–98	inline deep-packet inspection (IPS), 16
Forward icon, 96	inline mode, 13
Help icon, 96	configuring, 25–26
Master Blocking Sensors, 328	interfaces, 121–123
monitoring, 94–95	sensor support, 25
navigating, 84–94	installing, 515
Refresh icon, 96	Security Monitor, 352
system requirements, 83	sensors (IPS), 49–51

instructions box (Security Monitor), 355	managing, 73
Interface Configuration category,	modifying, 61–73
88–89	configuring, 25–26, 107
interface vlan command, 540	deploying, 27–30
interfaces, 493–494	hardware, 17–25
ACLs, 309	Cisco IDS 4200 series networks,
CLI, 45, 415	17–23
command and control, 475-477	Cisco IDSM-2, 23
devices, 324	firewalls sensors, 24
IDM, 83	inline sensor support, 25
Back icon, 96	network modules, 23
communication parameters, 97–98	router sensors, 24
Forward icon, 96	hosts, 107–118
Help icon, 96	hybrid IPS/IDS solutions, 13-14
monitoring, 94–95	interfaces, 118–126
navigating, 84–94	meta-event generators, 16–17
Refresh icon, 96	monitoring, 12–13
system requirements, 83	overview of, 9
IPS, 14	protocols, 30
mode, 70	responses, 297
Security Monitor, 353–356	inline actions, 298–300
sensors, 118–126	IP blocking, 303–312, 314–330
internal clocks, configuring, 112	logging actions, 300–302
internal interfaces (ACLs), 311	manual blocking, 330–334
Internet boundaries, deploying sensors, 28	Master Blocking Sensors, 313–314
Internet Control Message Protocol (ICMP)	TCP reset, 334
atomic IP signature parameters, 180	risk rating, 14–16
flood host signature parameters, 184	signatures, 133
Sweep signature engines, 211	configuring, 137, 155–162
Internet Protocol. See IP	customizing, 242–253
Intranet boundaries, deploying sensors, 28	FTP/HTTP policies, 237–238
Intrusion Detection Interaction and	groups, 137–151
Operations Messages (IDIOM), 31	managing alarms, 151–155
Intrusion Prevention System. See IPS	MEG, 230–237
Intrusion Detection System (IDS). See IPS	optimizing configuration, 225–230
IOS, 360–361	tuning, 238–242
IP (Internet Protocol)	terminology, 10–11
blocking, 303-312, 314-330	triggers, 11–12
logging, 300–302	IPS Device Manager (IDM), 79, 83, 415,
NM-CIDS, 501	427–428
ip access-list command, 539	Back icon, 96
ip inspect command, 539	blocking, 316
IPS (Intrusion Prevention System), 5	communication parameters, 97–98
analysis engines, 126–128	devices, 321–322
bypasses, 26	Forward icon, 96
CLI, 45	Help icon, 96
configuring, 73–74	logical devices, 319–321
initializing sensors, 51–61	Master Blocking Sensors, 328
installing sensors, 49–51	monitoring, 94–95

IPS Device Manager (IDM) (continued)	IDM, 79, 83
navigating, 84–94	Back icon, 96
Refresh icon, 96	communication parameters, 97–98
signatures	Forward icon, 96
Custom Signature Wizard, 248	Help icon, 96
customizing, 246	monitoring, 94–95
system requirements, 83	navigating, 84–94
	Refresh icon, 96
	system requirements, 83
< - L	IPS, 73
keywords, 64	sensors, 29
allowed, 539	manual blocking, 330–334
CLI, 63	manual configuration
killing TCP connections, 334	sensor clocks, 112
known host parameters, 117	system clocks, 58
known nost parameters, 117	manual IP logging, 301–302
L2/L3/L4 Protocol signatures, viewing, 140	Master Blocking Sensors, 313–314
layer signatures, viewing, 140–141	defining, 328–330
Log Attacker Packets action, 300	match subcommand, 538
Log Pair Packets action, 300	matching strings, 225–227
Log Victim Packets, 300	maximum block entries parameter, 316
logger mode (CLI command mode), 71	MEG (Meta-Event Generator), 230–237
logging, 300–302, 309	messages, e-mail (spam), 245
logical devices, configuring, 319–321	Meta-Event Generator, 230–237
loose TCP streams, 275	minor versions (Cisco IPS), 416
loose 1 St Streams, 272	Miscellaneous option (IDM), 90
	misuse detection (IPS triggers), 11
λЛ	mls ip ids command, 539
M	modes
maintenance for sensors, 411, 415	alarm summaries, 151–155
automatic software updates, 421–422	asymmetric, 275
CLI software installations, 419	CLI, 66
downgrading images, 423	modification
IDM software installations, 420–421	of IPS CLIs, 61–73
image recovery, 424	of passwords, 59
resetting, 427–428	modules, IDSM, 465. See also IDSM
restoring default configurations, 425-426	monitor session command, 535-536
saving current configurations, 418	monitoring
updating	IDM, 94–95
licenses, 423	interfaces
software, 415–418	editing, 119–121
major versions (Cisco IPS), 416	enabling, 118
management	IP, 14
alarms, 151–155	IPS, 12–13
CiscoWorks 2000, 347	NM-CIDS, 493–494
adding users, 349	sensors, 29
authorization, 348–349	traffic (Catalyst 6500 switches), 477
login, 347–348	Msg Body signature type, 175
Security Monitor, 351–356	multiple sensors, configuring, 30

N	signature configuration, 225-230
	customizing, 242–253
NAC (Network Access Controller), 305	MEG, 230–237
names, viewing signatures, 146	tuning, 238–242
NAT (Network Address Translation),	Options bar (Security Monitor), 354
499–500	options, 109, 356–366, 476, 544
navigating	blocking properties, 315–316
IDM, 84–94	boot loaders, 513
Security Monitor, 353–356	CLI, 61
Network Access Controller (NAC), 305	destination ports, 542
Network Address Translation (NAT), 499–500	events, 276
Network Module-Cisco IDS (NM-CIDS),	filtering actions, 281–284
493–516	overriding actions, 279–281
network modules for access routers, 23	Target Value Rating, 279
Network Security Database, 155–159	variables, 277, 279
Network Time Protocol (NTP), 113	fields, 227–230
network-access mode, 71	hosts (SSH), 116–118
network-based intrusion systems, 13	IDM, 79, 83
networks, 527–535, 542–544	Back icon, 96
blocking, 332	communication parameters, 97–98
NM-CIDS architecture, 496	Forward icon, 96
protocols, 243	Help icon, 96
sniffing, 13	Master Blocking Sensors, 328
tap traffic flow, 530	monitoring, 94–95
topologies, 308	navigating, 84–94
traffic, 527	Refresh icon, 96
never-block entries, 317	system requirements, 83
NM-CIDS (Network Module-Cisco IDS),	interfaces
493–516	inline pairs, 121–123
no access-list command, 64	inline software bypasses, 123
no remote-span command, 537	IPS, 14
notifications	IPS, 25–26
configuring, 124–126	bypasses, 26
mode, 71	CLI, 73–74
NSDB (Network Security Database),	logical devices (IDM), 319–321
155–159	responses, 297
NTP (Network Time Protocol), 113	inline actions, 298–300
	IP blocking, 303–312, 314–330
^	logging actions, 300–302
U	manual blocking, 330–334
Off mode (IPS), 26	Master Blocking Sensors, 313–314
On mode (IPS), 26	TCP reset, 334
operating system (OS), viewing, 141	Security Monitor, 356, 387, 393-397
Operator role, 65	sensors, 29, 107
optimizing	accessing SNMP, 455–457
sensors, 268–269	analysis engines, 126–128
configuring IP, 269–271	debugging, 448–453
enforcing, 272–273	events, 443–447
reassembly policies, 274–276	hosts, 107–118

options (continued)	patterns, searching, 225–227
interfaces, 118–126	performance, 469. See also optimizing
statistics, 441–443	perimeters, 28
viewing, 437–440	PIX Firewalls
Service accounts, 57	adding devices, 361
signatures, 137, 155–162	as IP blocking devices, 306
customizing, 242–253	sensors (Cisco IOS IDS), 24
FTP/HTTP policy enforcement, 237–238	placement
groups, 137–151	of ACLs (IP blocking), 310–312
managing alarms, 151–155	of sensors, 29
MEG, 230–237	policies, FTP/HTTP enforcement,
optimizing, 225–230	237–238
tuning, 238–242	Policy Violation signatures, 139
system clocks, 58	ports
tabs (Security Monitor), 353	destination, 542
time zones (sensors), 113	RSPAN, 533–537
traffic flow notifications, 124-126	SPAN, 533–536
verifying, 437	targets, 243
OS (operating system), viewing, 141	VLANs, 543–544
overlapping fragments, 264	PostOffice devices, adding, 359
	powering down sensors, 427–428
_	Privileged Exec mode, 67
P	processes, IP blocking, 310
packet capture command, 450	promiscuous mode, configuring,
packet capture command, 450 packet display command, 450	25–26
packets	prompts (CLI), 62
analyzing logging actions, 300–302	properties
Deny Packet inline action, 298	blocking, 93, 315–316
NM-CIDS, 501–502	CLI, 61
TCP reset, 334	protocols
pairs (interface), configuring, 121–123	analysis (IPS triggers), 12
parameters	ARP, 177
Cisco IPS signatures, 173	EIGRP, 243
communication (IDM), 97–98	FTP
content types, 174	IC signature engine parameters, 173
dates, 114	policy enforcement, 237–238
duration of inline actions, 299	HTTP, 237–238
ip access-list command, 539	IOS, 360–361
known hosts, 117	IP, 300–302
monitoring interfaces, 119–121	L2/L3/L4, 140
set vlan command, 476	networks, 243
signatures, 244	NTP, 113
time, 112	PIX, 361
traffic flow notification, 125	PostOffice, 359
passwords	RDEP, 31, 356–359
commands, 59	sensors, 30
CLI, 51	signatures, 144–146
modifying, 59	SNMP, 93
path bar (Security Monitor), 355	TCP, 334
r ( (	

₹	Service, 66
-	user (CiscoWorks 2000), 349
rating, 279	users, 64
risks, 14–16	Viewer, 66
Target Values, 279	root accounts, 66
RDEP (Remote Data Exchange Protocol),	routers
31, 356–359	access, 23
readme extension, 417	as IP blocking devices, 304
recall commands, 63	sensors (Cisco IOS IDS), 24
reconnaissance signatures, 139	rpm.pkg extension, 417
recover application-partition	RR (risk rating), 14–16
command, 424	RSPAN (Remote Switched Port Analyzer),
Refresh icon (IDM), 96	533–537
regular expressions, 225–227	rules for events
Related Threats field (NSDB), 157	activating, 368
releases, viewing signatures, 143 reloading NM-CIDS, 511	adding, 364–368
remote access boundaries, sensors, 28	
Remote Data Exchange Protocol (RDEP), 31, 356–359	S
Remote Switched Port Analyzer (RSPAN),	searching patterns, 225–227
533–537	Secure Shell (SSH), 31, 60
remote-span command, 536	security
Request Block Connection action, 303	IPS
Request Block Host action, 303	bypasses, 26
Request Methods signature type, 175	configuring, 25–26
requirements	deploying, 27–30
clients, 352	hardware, 17–25
servers, 352	hybrid IPS/IDS solutions,
reset command, 57, 478	13–14
resetting	meta-event generators, 16–17
NM-CIDS, 511	monitoring, 12–13
sensors, 427–428	overview of, 9
TCP, 334	protocols, 30
•	risk rating, 14–16
responses	terminology, 10–11
actions, 149–150 IPS, 297	triggers, 11–12
	NSDB, 156–159
inline actions, 298–300	Security Monitor
IP blocking, 303–312, 314–330	configuring, 356
logging actions, 300–302	adding devices, 356–361
manual blocking, 330–334	event notification, 363–368
Master Blocking Sensors, 313–314	Event Viewer, 374–386
TCP reset, 334	importing devices, 361–363
signatures, 161–162	monitoring devices, 368–374
restoring, 425–426	<del>-</del>
retiring signatures, 160	managing, 387
risk rating (RR), 14–16	data, 387, 390–391
roles	Event Viewer preferences, 392
Administrator, 65	system configuration, 391–392
Operator, 65	reports, 393–397

selecting	overview of, 9
event types, 446	protocols, 30
IP blocking, 308	risk rating, 14–16
signature engines, 243	routers, 24
strong passwords, 51	terminology, 10–11
senior user accounts, configuring, 109	triggers, 11–12
Sensor Setup (IDM), 87–88	maintenance, 411, 415
sensors, 527	automatic software updates, 421–422
analysis engines, 126–128	CLI software installations, 419
clocks, 112	downgrading images, 423
configuring, 107	IDM software installations, 420–421
events, 276	image recovery, 424
filtering actions, 281–284	licenses, 423
overriding actions, 279–281	resetting, 427–428
Target Value Rating, 279	restoring configurations, 425–426
variables, 277, 279	saving current configurations, 418
hosts, 107–118	updating software, 415–418
IDS evasion, 263	optimizing, 268–269
encryption, 265	configuring IP log settings, 269–271
flooding, 263	enforcing application
fragmentation, 263–265	policies, 272–273
obfuscation, 265–267	reassembly options, 274–276
TTL manipulation, 267	responses, 297
IDSM, 469	inline actions, 298–300
Catalyst 6500 switches, 476–477	IP blocking, 303–312, 314–330
configuring IDSM-2, 472–474	logging actions, 300–302
deploying IDSM-2, 469–470	manual blocking, 330–334
features of, 470	Master Blocking Sensors, 313–314
managing (IDSM-2), 477–478	TCP reset, 334
ports (IDSM-2), 475	signatures, 133
traffic flow (IDSM-2), 471	configuring, 137, 155–162
troubleshooting (IDSM-2), 478–483	customizing, 242–253
interfaces, 118–126 IPS, 5	FTP/HTTP policy enforcement, 237
bypasses, 26	groups, 137–151 managing alarms, 151–155
Cisco IDS 4200 switches, 17–23	MEG, 230–237
Cisco IDSM-2 (for Catalyst 6500), 23	optimizing configuration, 225–230
configuring, 25–26	tuning, 238–242
deploying, 27–30	virtual, 89
firewalls, 24	servers
hardware, 17–25	IPS deployment, 29
hybrid IPS/IDS solutions, 13–14	NTP, 113
IDM. See also IDM, 79	requirements, 352
initializing, 51–61	Service accounts, creating, 57
inline sensor support, 25	Service mode (CLI command mode), 68
installing, 49–51	service notification command, 455
meta-event generators, 16–17	service packs, 417
monitoring, 12–13	Service role, 66
network module for access routers, 23	services, viewing signatures, 144–146

session command, 4/4	functionality, 244
session slot command, 474	IPS, 133
set security acl command, 541	configuring, 137, 155–162
set vlan command, 476	customizing, 242–253
setup command, 52–57	FTP/HTTP policy enforcement, 237–238
severity (event), 15	groups, 137–151
show commands	managing alarms, 151–155
show configuration command, 438	MEG, 230–237
show events command, 444	optimizing configuration, 225–230
show interfaces command, 448	tuning, 238–242
show inventory command, 441	parameters, 244
show module command, 479–481	responses, 297
show module switch command, 472	-
•	inline actions, 298–300 IP blocking, 303–312, 314–330
show port command, 482	9
show statistics command, 441	logging actions, 300–302
show tech-support command, 448, 452	manual blocking, 330–334
show trunk command, 483	Master Blocking Sensors, 313–314
show version command, 438	TCP reset, 334
shun command, 306	retiring, 160
shutting down NM-CIDS, 511	selecting, 308
Signature Configuration option (IDM), 90	testing, 245
Signature Definition category (IDM), 90	Simple Mail Transport Protocol, 207
signature fidelity ratings, 15	Simple Network Management Protocol
Signature Variables option (IDM), 90	(SNMP), 93
signature-definition mode, 72	single sensors, configuring, 30
signatures	SMTP (Simple Mail Transport
Cisco IPS, 171, 417	Protocol), 207
AIC FTP engines, 173	sniffing networks, 13
AIC HTTP engines, 173–176	SNMP (Simple Network Management
atomic engines, 177–183	Protocol), 93
engines, 171–172	software types, 416
flood engines, 183–186	Sort By group box (Event Viewer), 382
Meta Signature engines, 187	spam, 245
Normalizer Signature engines, 188	SPAN (Switched Port Analyzer), 533
parameters, 172	configuring, 535–536
service signature engines, 189–204	speed (interface), 119
state signature engines, 204–207	spoofing, antispoofing mechanisms, 307
String signature engines, 208–209	Spyware signatures, viewing, 139
Sweep signature engines, 210–215	SQL (Structured Query Language), 198
Trojan horse signature engines, 215	SSH (Secure Shell), 31, 60
cloning, 253	ssh host-key command, 60
connections, 92	ssh-known-hosts mode, 72
creating, 160	status
defining, 161–162	fields (signatures), 230
editing, 160	NM-CIDS, 512
enabling, 159	
engines, 243–244	streams
fields, 227–230	loose TCP, 275
	strict TCP, 275
filtering, 245–251	strict TCP streams, 275

strings, matching, 225–227	Time to Live, 267
Structured Query Language (SQL), 198	TOC (Security Monitor), 355
subcommands	tools
action, 538	bar (Security Monitor), 356
match, 538	CiscoWorks 2000, 347
summaries of alarms, 151–155	topologies, IP blocking, 308
summertime settings, configuring,	traffic
114–115	blocking, 92
Switched Port Analyzer (SPAN), 533	bridging, 527
configuring, 535–536	capturing, 527
switches	Catalyst 6500 switches, 542–544
Catalyst 6000	devices, 529–531
as blocking devices, 326	inline mode, 527–529
as IP blocking devices, 305	promiscuous mode, 529
IDSM, 469	switches, 532–534
traffic flow, 532	TCP resets and switches, 535
switchport access vlan command, 476	Catalyst 6500 switches, 477
switchport capture allowed vlan	Cisco IPS signatures, 171
command, 541	flow, 124–126
switchport capture command, 539–541	identifying, 133
switchport trunk command, 543	IPS
syntax for regular expressions, 225–227	bypasses, 26
system clocks, configuring, 58	configuring, 25–26
system configuration. See configuration	deploying, 27–30
system requirements, 83	hardware, 17–25
system requirements, 63	hybrid IPS/IDS solutions, 13–14
	meta-event generators, 16–17
Γ	monitoring, 12–13
	overview of, 9
tabs	protocols, 30
completion, 63	risk rating, 14–16
configuration, 353	terminology, 10–11
tap (network) traffic flow, 530	triggers, 11–12
Target Value Rating, 91, 279	Transfer Encodings signature type, 176
targets	transferring files (NM-CIDS), 515
addresses, 243	transitions, Cisco Login state machines, 206
asset value of, 16	Transmission Control Protocol (TCP).
ports, 243	See TCP
TCP (Transmission Control Protocol)	triggers
atomic IP signature parameters, 181	IPS, 11–12
Normalizer signature engines, 188	responses, 297
reset, 334	inline actions, 298–300
Sweep signature engines, 211	IP blocking, 303–312, 314–330
testing signatures, 245	logging actions, 300–302
threats (NSDB), 157	manual blocking, 330–334
time	Master Blocking Sensors,
events, 385	master blocking Sensors, 313–314
frames for events, 447	515–514 TCP reset, 334
sensors, 112	
zones, 113	signatures, 228

Trojan horse signatures, 139	V
troubleshooting	WAR WANT OF A 1110
CLI, 62	VACL (VLAN Access Control List),
signatures, 245	311, 534
trunking, 543–544	configuring, 537–541, 544
trusted-certificates mode, 72	values
TTL (Time to Live), 267	asset value of targets, 16
tuning	signatures, 228
existing signatures, 238–242	variables
sensors, 268–269	alarm summarization, 154
configuring IP logs, 269–271	events, 277–279
encryption, 265	verifying, 437–445, 447–457
enforcing policies, 272–273	signature functionality, 244
flooding, 263	system configuration, 437
fragmentation, 263–265	versions, Cisco IPS, 416
IDS evasion, 263	Viewer role, 66
obfuscation, 265–267	viewing
reassembly options, 274–276	NM-CIDS, 512
TTL manipulation, 267	NSDB, 156–159
types	signatures, 137–151
of attacks	virtual LANs (VLANs). See VLANs
selecting signature engines, 244	Virtual Sensor option (IDM), 89
viewing signatures, 137–139	virus signatures, 139
of content, 174	VLAN Access Control List (VACL),
of events, 446	311, 534
of layers, 140–141	configuring, 537–541, 544
of software, 416	vlan filter command, 538
or software, 110	VLANs (virtual LANs)
	Catalyst 6500 switches, 476
1	ports, 543–544
<b>.</b>	traffic capture, 527–529
UART (Universal Asynchronous	•
Receiver/Transmitter), 498	
UDP (User Datagram Protocol)	W - Z
atomic Ip signature parameters, 182	war dialers, 29
flood host signature parameters, 185	web-server mode (CLI command
Universal Asynchronous Receiver/	mode), 73
Transmitter, 498	
updating, 415–423	Windows Security Monitor, installing, 352
Auto Update (IDM), 94	wizards, Custom Signature Wizard,
upgrade command, 49, 419	90, 248
User Datagram Protocol. See UDP	worm signatures, 139
username command, 59	415
users	zip extension, 417
adding/deleting, 59	zones (time), configuring, 113
CiscoWorks 2000, 349	
roles, 64	
senior accounts, 109	