

Structured Threats	21
External Threats	22
Internal Threats	22
Network Attacks	22
Reconnaissance Attacks	22
Access Attacks	23
Data Retrieval	23
System Access	24
Privilege Escalation	24
DoS Attacks	24
Anatomy of an Attack	25
Overview of IDS	25
Types of IDS	26
Network IDS	26
Host IDS	27
Others	28
How Does IDS Work?	28
Signature-Based IDS	30
Anomaly-Based IDS	31
Defeating an IDS	32
Summary	34
Solutions Fast Track	35
Frequently Asked Questions	37
Chapter 2 Cisco Intrusion Detection	39
Introduction	40
What Is Cisco Intrusion Detection?	41
Cisco's Network Sensor Platforms	42
Cisco IDS Appliances	43
4210 Sensor	45
4215 Sensor	45
4230 Sensor	45
4235 Sensor	46
4250 Sensor	46
4250 XL Sensor	46
The Cisco IDS Module for Cisco 2600, 3600, and 3700 Routers	46

The Cisco 6500 Series IDS Services Module	47
Cisco's Host Sensor Platforms	49
Cisco Host Sensor	50
Managing Cisco's IDS Sensors	51
Cisco PostOffice Protocol	53
Remote Data Exchange Protocol	55
Deploying Cisco IDS Sensors	56
Understanding and Analyzing the Network	57
Identifying the Critical Infrastructure and Services	58
Placing Sensors Based on Network and Services Function	59
Case Study 1: Small IDS Deployment	60
Case Study 2: Complex IDS Deployment	62
Summary	69
Solutions Fast Track	70
Frequently Asked Questions	72

Chapter 3 Initializing Sensor Appliances 75

Introduction	76
Identifying the Sensor	76
Initializing the Sensor	79
What Is the root User?	81
What Is the netrangr User?	83
What Is sysconfig-sensor?	83
Configuring the Sensor	83
The Display	93
Using the Sensor Command-Line Interface	94
cidServer	95
idsstatus	95
idsconns	96
idsvers	97
idsstop	97
idsstart	98
Configuring the SPAN Interface	98
Spanning Ports	99
Spanning VLANs	99
Recovering the Sensor's Password	100
Reinitializing the Sensor	102

Downloading the Image	102
Using the CD	102
Using the Recovery Partition	103
Uninstalling an Image	107
Upgrading a Sensor from 3.1 to 4.0	107
Upgrading a Sensor BIOS	108
Initializing a Version 4.0 Sensor	109
Summary	113
Solutions Fast Track	114
Frequently Asked Questions	117
Chapter 4 Cisco IDS Management	119
Introduction	120
Managing the IDS Overview	121
Using the Cisco Secure Policy Manager	123
Installing CSPM	123
Logging In to CSPM	128
Configuring CSPM	129
Adding a Network	130
Adding a Host	132
Adding a Sensor	135
The Properties Tab	137
The Sensing Tab	138
The Blocking Tab	139
The Filtering Tab	142
The Logging Tab	145
The Advanced Tab	146
The Command Tab	148
The Control Tab	149
Signature Updates	150
Configuring IPSec	151
Viewing Alarms	152
Using the CSID Director for Unix	155
Installing and Starting the Director	155
How to Configure the CSID Director	157
Adding a New Sensor	157
Event Processing	159

Using the IDS Device Manager	160
How to Configure IDS Device Manager	161
Logging In	162
Configuring the IDS Device Manager	164
The Device Tab	165
The Configuration Tab	168
The Monitoring Tab	172
The Administration Tab	175
Using the Cisco Network Security Database	178
Summary	180
Solutions Fast Track	180
Frequently Asked Questions	183

Chapter 5 Configuring the Appliance Sensor 185

Introduction	186
Configuring SSH	186
Cisco IDS Software v3	190
Cisco IDS Software v4.0	192
Configuring SSH Using IDM	198
Compatible Secure Shell Protocol Clients	200
Configuring Remote Access	201
Terminal Server Setup	202
BIOS Modifications for IDS 4210/4220/4230 Sensors	203
The IDS-4210 Sensor	203
The BIOS Setup for the	
IDS-4220 and IDS-4230 Sensors	204
Applying the Sensor Configuration	204
Cisco Enabling and Disabling Sensing Interfaces	205
Adding Interfaces to an Interface Group	207
Configuring Logging	208
Configuring Event Logging (IDS version 3.1)	208
Exporting Event Logs	209
Configuring Automatic IP Logging	211
Configuring IP Logging	212
Generating IP Logs	214
Upgrading the Sensor	216
Upgrading from 3.1 to 4.x	216

Updating Sensor Software (IDS 4.0) from the Command Line	219
Updating Sensor Software (IDS 4.0) with IDM	219
Updating Sensor Software (IDS 4.0) Using the IDM	221
Upgrading Cisco IDS Software from Version 4.0 to 4.1	222
Updating IDS Signatures	222
Updating Signatures (IDS 3.0)	223
Automatic Updates	223
Updating Signatures (IDS 4.0)	225
How to Restore the Default Configuration	226
Summary	227
Solutions Fast Track	228
Frequently Asked Questions	231
Chapter 6 Configuring the Cisco IDSM Sensor	233
Introduction	234
Understanding the Cisco IDSM Sensor	234
Configuring the Cisco IDSM Sensor	236
Setting Up the SPAN	244
Setting Up the VACLs	244
Configuring Trunks to Manage Traffic Flow	246
Verifying the Configuration	246
Updating the Cisco IDSM Sensor	247
Booting the IDSM Sensor from Partition 2	247
Upgrading the IDSM Sensor	250
Verifying the IDSM Sensor Upgrade	254
Shutting Down the IDSM Sensor	256
Updating the IDSM Sensor Signatures and Service Packs	258
Troubleshooting the Cisco IDSM Sensor	259
Summary	265
Solutions Fast Track	266
Frequently Asked Questions	268
Chapter 7 Cisco IDS Alarms and Signatures	271
Introduction	272
Understanding Cisco IDS Signatures	272
Signature Implementation	274
Signature Classes	275

Signature Structure	275
Signature Types	276
Cisco IDS Signature Micro-Engines	277
The ATOMIC Micro-Engines	281
The SERVICE Micro-Engine	286
The FLOOD Micro-Engine	289
The STATE.HTTP Micro-Engine	293
The STRING Micro-Engine	296
The SWEEP Micro-Engine	302
The OTHER Engine	311
Understanding Cisco IDS Signature Series	314
Configuring the Sensing Parameters	315
TCP Session Reassembly	315
No Reassembly	316
Loose Reassembly	316
Strict Reassembly	316
Configuring TCP Session Reassembly	316
IP Fragment Reassembly	317
Configuring IP Fragment Reassembly	317
Internal Networks	319
Adding Internal Networks	319
Sensing Properties	320
Configuring Sensing Properties	320
Excluding or Including Specific Signatures	321
Excluding or Including Signatures in CSPM	321
Excluding or Including Signatures in IDM	322
Creating a Custom Signature	323
Creating Custom Signatures Using IDM	324
Creating Custom Signatures Using CSPM	326
Working with SigWizMenu	326
Starting SigWizMenu	327
Tune Signature Parameters	328
Adding a New Custom Signature	330
Understanding Cisco IDS Alarms	334
Alarm Level 5 – High Severity	334
Alarm Level 4 – Medium Severity	335

Alarm Level 3 – Low Severity	335
Sensor Status Alarms	335
Identifying Traffic Oversubscription	337
Summary	338
Solutions Fast Track	339
Frequently Asked Questions	345
Chapter 8 Configuring Cisco IDS Blocking	347
Introduction	348
Understanding the Blocking Process	349
What Is Blocking?	351
Access Control Lists	351
Device Management	357
Understanding Master Blocking	358
Using ACLs to Perform Blocking	360
General Considerations for Implementation	361
Where Should I Put My Access Control Lists?	365
Configuring the Sensor to Block	366
Configuring a Router for a Sensor Telnet Session	366
Configuring the Sensor	368
The Never Block IP Addresses Setup	370
Using the Master Blocking Sensor	371
Manually Blocking and Removing a Block	372
Determining the Status of the Managed Device and Blocked Addresses	373
Summary	376
Solutions Fast Track	377
Frequently Asked Questions	380
Chapter 9 Capturing Network Traffic	383
Introduction	384
Switching Basics	385
Configuring SPAN	388
Configuring an IOS-Based Switch for SPAN	388
Configuring 2900/3500 Series Switches	389
Configuring a 4000/6000 Series IOS-Based Switch	393
Configuring a SET-Based Switch for SPAN	395
Configuring RSPAN	401

Configuring an IOS-Based Switch for RSPAN	403
Source Switch Configuration	403
Destination Switch Configuration	403
Configuring a SET-Based Switch for RSPAN	404
Source Switch Configuration	404
Destination Switch Configuration	405
Configuring VACLs	406
Using Network Taps	411
Using Advanced Capture Methods	415
Capturing with One Sensor and a Single VLAN	415
Capturing with One Sensor and Multiple VLANs	417
Capturing with Multiple Sensors and Multiple VLANs	418
Dealing with Encrypted Traffic and IPv6	419
Summary	423
Solutions Fast Track	424
Frequently Asked Questions	427
Chapter 10 Cisco Enterprise IDS Management	429
Introduction	430
Understanding the Cisco IDS Management Center	431
IDS MC and Security Monitor	431
The IDS MC and Sensors	432
IDS MC and Signatures	433
IDS MC and Security Policy	433
Installing the Cisco IDS Management Center	435
Server Hardware Requirements	435
CiscoWorks Architecture Overview	436
IDS MC Installation	438
IDS MC Processes	439
VMS Component Compatibility	439
Client Installation Requirements	440
Installation Steps	441
Getting Started	442
Authorization Roles	443
Installation Verification	444
Adding Users to CiscoWorks	445
The IDS MC	446

Setting Up Sensors and Sensor Groups	447
The IDS MC Hierarchy	448
Creating Sensor Subgroups	449
Adding Sensors to a Sensor Group	450
Deleting Sensors from a Sensor Group	453
Deleting Sensor Subgroups	454
Configuring Signatures and Alarms	455
Configuring Signatures	455
Configuring General Signatures	455
Configuring Alarms	457
Tuning General Signatures	458
How to Generate, Approve, and Deploy IDS Sensor	
Configuration Files	460
Reviewing Configuration Files	460
Generating Configuration Files	461
Approving Configuration Files	461
Deploying Configuration Files	462
Configuring Reports	464
Audit Reports	464
The Subsystem Report	465
The Sensor Version Import Report	465
The Sensor Configuration Import Report	465
The Sensor Configuration Deployment Report	465
The Console Notification Report	465
The Audit Log Report	466
Generating Reports	466
Viewing Reports	467
Exporting Reports	467
Deleting Generated Reports	467
Editing Report Parameters	468
Example of IDS Sensor Versions Report Generation	468
Security Monitor Reports	470
Administering the Cisco IDS MC Server	471
Database Rules	471
Adding a Database Rule	471
Editing a Database Rule	473

Viewing a Database Rule	473
Deleting a Database Rule	473
Updating Sensor Software and Signatures	474
Defining the E-mail Server Settings	474
Summary	475
Solutions Fast Track	476
Frequently Asked Questions	478
Appendix A Cisco IDS Sensor Signatures	513
IP Signatures 1000 Series	514
ICMP Signatures 2000 Series	516
TCP Signatures 3000 Series	518
UDP Signatures 4000 series	540
Web/HTTP Signature 5000 Series	546
Cross Protocol Signature 6000 series	582
ARP Signature 7000 Series	588
String Matching Signature 8000 Series	589
Back Door signature Series 9000 Series	590
Policy Violation Signature 10000 Series	595
Sensor Status Alarms	596
IDS Signatures Grouped by Software Release Version	598
Index	631