CCNP Security IPS
642-627

Official Cert Guide
Learn, prepare, and practice for exam success

David Burns
Odunayo Adesina, CCIE No. 26695
Keith Barker, CCIE No. 6783

ciscopress.com
CCNP Security IPS 642-627 Official Cert Guide

David Burns
Odunayo Adesina, CCIE No. 26695
Keith Barker, CCIE No. 6783

Copyright© 2012 Pearson Education, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
First Printing October 2011

Library of Congress Cataloging-in-Publication data is on file.

Warning and Disclaimer
This book is designed to provide information about selected topics for the CCNP Security IPS 642-627 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Feedback Information
At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
About the Authors

David Burns has in-depth knowledge of routing and switching technologies, network security, and mobility. He is currently a systems engineering manager for Cisco, covering various U.S. Service Provider accounts. Dave joined Cisco in July 2008 as a lead systems engineer in a number of areas that include Femtocell, Datacenter, MTSO, and Security Architectures, working for a U.S.-based SP Mobility account. He came to Cisco from a large U.S.-based cable company, where he was a senior network and security design engineer. Dave has held various roles prior to joining Cisco during his ten-plus years in the industry, working in SP operations, SP engineering, SP architecture, enterprise IT, and also U.S. military intelligence communications engineering. He holds various sales and industry/Cisco technical certifications, including the CISSP, CCSP, and CCDP, as well as two associate-level certifications. Dave recently passed the CCIE Security Written and is currently preparing for the CCIE Security Lab. Dave is a big advocate of knowledge transfer and sharing and has a passion for network technologies, especially as they relate to network security. Dave has been a speaker at Cisco Live on topics including Femtocell (IP Mobility) and IPS (Security). Dave earned his bachelor of science degree in telecommunications engineering technology from Southern Polytechnic State University, Georgia, where he currently serves as a member of the Industry Advisory Board for the Computer & Electrical Engineering Technology School.

Odunayo Adesina, CCIE No. 26695 (Routing and Switching), is a systems engineer with Cisco in the U.S. commercial segment. In this role for over four years, Odunayo has worked with commercial customers in St. Louis, Missouri, to help develop their enterprise network architectures, which are typically a combination of borderless, collaboration, and virtualization solutions. He has more than 12 years of experience in the industry and holds various industry and Cisco certifications, including the CISSP No. 54152, CCSP, CEH, and VSP. He was one of the first few people who were CSS1 certified when the Cisco security certification was first developed. Prior to his role at Cisco, Odunayo worked with a large service provider as a network engineer, implementing and managing security, routing, and switching solutions, and later as a security specialist, driving ISO 27001 compliance, developing and enforcing security policies for the enterprise. He also worked with Cisco partners, where he implemented solutions across many industry verticals. Odunayo holds a bachelor of technology degree in electronics and electrical engineering from Ladoke Akintola University of Technology.

Keith Barker, CCIE No. 6783 R/S & Security, is a 27-year veteran of the networking industry. He currently works as a network engineer and trainer for Nova Datacom. His past experience includes EDS, Blue Cross, Paramount Pictures, and KnowledgeNET, and he has delivered CCIE-level training over the past several years. He is CISSP and CCSI certified, loves to teach, and keeps many of his video tutorials at http://www.youtube.com/keith6783. He can be reached at KBarker@NovaDatacom.com or by visiting http://www.NovaDatacom.com.
Brandon Anastasoff has been a systems engineer with Cisco Systems since October 2007, when he moved from a lead network architect role in a major newspaper publishing firm. He has spent over 20 years in the industry and has been focused on security for the last ten, obtaining certifications inside and outside of Cisco with his CISSP, CCSP, and most recently the Security CCIE. After studying in the United Kingdom, Brandon took a year off in Saudi Arabia to see what a real job would be like before proceeding to college but found the lure of an income too irresistible and never went back for the degree. Brandon had to make a choice early in his career to either follow the art of computer animation or the up-and-coming PC networking boom, and he has never regretted the decision to enter networking. He moved from early versions of Windows and Macintosh OSs through Novell’s Netware and then moved more into the infrastructure side, focusing mostly on Cisco LAN/WAN equipment. After Y2K, the focus became more security oriented, and Brandon became familiar with virus and Trojan analysis and forensic investigations. Today, Brandon is glad to be where he is and enjoys taking the opportunity to talk about security whenever the opportunity presents itself.
Dedications

“To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy’s resistance without fighting.”

—Sun Tzu, the Art of War

From David:
This book is dedicated to my wife and best friend in life, Lisa, whose love, encouragement, and support continue to drive my passion to learn, achieve, and serve; to our two boys, Will and Christian, who have an unending curiosity to learn, grow, and challenge the norm; to my extended family for their support, encouragement, and inspiration all these years; and finally to my fellow soldiers (present, past, and future) for their selfless service, integrity, honor, pride, and drive to do the right thing to protect us all—God Bless!

From Odunayo:
This book is dedicated to God for his many blessings; to my loving wife, Aramide, who always gives me great encouragement and support, especially as she did during the writing of this book; and to my parents, who have continually encouraged my brother, sister, cousins, and me and our families, in everything we’ve done. Also to the loving memories of my aunt, Olayemi Akere, and cousin, Korede Akindele, who were supportive and instrumental to my many successes.
Acknowledgments

We would like to thank many people for helping us put this book together:

The Cisco Press team: Brett Bartow, the executive editor, was the catalyst for this project, coordinating the team and ensuring that sufficient resources were available for the completion of the book. Kimberley Debus, the development editor, has been invaluable in producing a high-quality manuscript. Her great suggestions and keen eye caught some technical errors and really improved the presentation of the book. We would also like to thank the project editor team for their excellent work in shepherding this book through the editorial process.

The Cisco IPS 7.0 course development team: Many thanks to the IPS course development team members.

The technical reviewers: We would like to thank the technical reviewer of this book, Brandon Anastasoff, for his thorough, detailed review and very valuable input.

Our families: Of course, this book would not have been possible without the constant understanding and patience of our families. They have lived through the long days and nights it took to complete this project and have always been there to motivate and inspire us. We thank you all.

Each other: Last, but not least, this book is a product of work by three strangers (now friends) and colleagues, which made it even more of a pleasure to complete.

From Odunayo:

The Cisco Press team was very instrumental in the success of this book. The executive editor, Brett Bartow, did an outstanding job of coordinating the team, ensuring that timelines were met and that resources required in completing the book were available. The hard work of the development editor, Kimberley Debus, produced the brilliant formatting of the text and images, which are pivotal to the overall experience of the reader. And also Tonya Simpson, John Edwards, and Drew Cupp, for making sure the text is free of typos with dotted i’s and crossed t’s.

My St. Louis Cisco family, especially Mark Meissner, Deana Patrick, Cindy Godwin-Sak, Brian Sak, Josh Gentry, Corey Moomey, and Jeff Peterson, encouraged me through all the stages of this project and provided some of the hardware used for the practical sections of the book.

My coauthors David Burns and Keith Barker worked diligently toward the completion of this book. Keith Barker also ensured the integrity of the text as a technical reviewer with Brandon Anastasoff.

And last but not least, my family, colleagues, and friends showed tremendous support and excitement while looking forward to the book’s completion; this I found very energizing.
From Keith:
Thanks to Dave Burns, Odunayo Adesina, Brett Bartow, and Andrew Cupp for the opportunity to be part of this project, and to all those who assisted in making my words look better, including Brandon Anastasoff, Kimberley Debus, and Tonya Simpson, as well as the other amazing folks at Cisco Press. A special shout-out to Jeremy Dansie for his assistance regarding this project.

Thanks to the viewers of my YouTube channel, Keith6783, for all your requests, encouragement, and kind feedback regarding the content there. It means a lot to me.

Finally, I want to thank my wife, Jennifer, for being a solid foundation for me and our family, and to my seven children, who continue to remind me how absolutely wonderful life can be.
## Contents at a Glance

**Introduction** xxviii

### Part I  Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices  3

Chapter 1  Intrusion Prevention and Intrusion Detection Systems  5

Chapter 2  Cisco IPS Software, Hardware, and Supporting Applications  23

Chapter 3  Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures  51

Chapter 4  Network IPS and IDS Deployment Architecture  67

### Part II  Installing and Maintaining Cisco IPS Sensors  85

Chapter 5  Integrating the Cisco IPS Sensor into a Network  87

Chapter 6  Performing the Cisco IPS Sensor Initial Setup  111

Chapter 7  Managing Cisco IPS Devices  143

### Part III  Applying Cisco IPS Security Policies  171

Chapter 8  Configuring Basic Traffic Analysis  173

Chapter 9  Implementing Cisco IPS Signatures and Responses  189

Chapter 10  Configuring Cisco IPS Signature Engines and the Signature Database  237

Chapter 11  Deploying Anomaly-Based Operation  257

### Part IV  Adapting Traffic Analysis and Response to the Environment  279

Chapter 12  Customizing Traffic Analysis  281

Chapter 13  Managing False Positives and False Negatives  311

Chapter 14  Improving Alarm and Response Quality  339

### Part V  Managing and Analyzing Events  359

Chapter 15  Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors  361

Chapter 16  Managing and Investigating Events Using Cisco IPS Manager Express  389
Chapter 17 Using Cisco IPS Manager Express Correlation, Reporting, Notification, and Archiving 413
Chapter 18 Integrating Cisco IPS with CSM and Cisco Security MARS 423
Chapter 19 Using the Cisco IntelliShield Database and Services 441

Part VI Deploying Virtualization, High Availability, and High-Performance Solutions 465
Chapter 20 Using Cisco IPS Virtual Sensors 467
Chapter 21 Deploying Cisco IPS for High Availability and High Performance 481

Part VII Configuring and Maintaining Specific Cisco IPS Hardware 503
Chapter 22 Configuring and Maintaining the Cisco ASA AIP SSM Modules 505
Chapter 23 Configuring and Maintaining the Cisco ISR AIM-IPS and NME-IPS Modules 535
Chapter 24 Configuring and Maintaining the Cisco IDSM-2 555

Part VIII Final Exam Preparation 583
Chapter 25 Final Preparation 585

Part IX Appendixes
Appendix A Answers to the “Do I Know This Already?” Quizzes 595
Appendix B CCNP Security IPS 642-627 Exam Updates, Version 1.0 609
Glossary 613
Index 619
Appendix C Memory Tables (CD Only)
Appendix D Memory Tables Answer Key (CD Only)
Contents

Introduction xxviii

Part I Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices 3

Chapter 1 Intrusion Prevention and Intrusion Detection Systems 5
“Do I Know This Already?” Quiz 5
Foundation Topics 8
Intrusion Prevention Overview 8
Intrusion Detection Versus Intrusion Prevention 8
Intrusion Prevention Terminology 9
Intrusion Prevention Systems 12
Features of Network Intrusion Prevention Systems 13
Limitations of Network Intrusion Prevention Systems 14
Network Intrusion Prevention Approaches 14
Endpoint Security Controls 16
Host-Based Firewalls 17
API and System Call Interception 17
Cisco Security Agent 17
Antimalware Agents 18
Data Loss Prevention Agents 19
Cryptographic Data Protection 19
A Systems Approach to Security 20
Exam Preparation Tasks 21
Review All the Key Topics 21
Complete the Tables and Lists from Memory 21
Define Key Terms 21

Chapter 2 Cisco IPS Software, Hardware, and Supporting Applications 23
Overview 23
“Do I Know This Already?” Quiz 23
Foundation Topics 26
Cisco IPS Network Sensors 26
Cisco IPS 4200 Series Sensors 27
Cisco IPS 4240 Sensor 28
Cisco IPS 4255 Sensor 29
Cisco IPS 4260 Sensor 30
Cisco IPS 4270 Sensor 32
Sensing Interface Details 33
Chapter 3  Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures  51

Overview  51
“Do I Know This Already?” Quiz  51
Foundation Topics  54
Network IPS Traffic Analysis Methods  54
  Stateful Content Matching  54
  Protocol Decoding  55
  Traffic Correlation  55
  Rate Analysis  55
  Packet Header Matching  56
  Packet Content Matching  56
  Statistical Modeling  57
  Event Correlation  57
Network IPS Evasion Techniques  57
  Encryption and Tunneling  58
  Timing Attacks  58
  Resource Exhaustion  58
Chapter 6    Performing the Cisco IPS Sensor Initial Setup    111

Overview    111
“Do I Know This Already?” Quiz    111
Foundation Topics    114
Accessing and Using the Cisco IPS Sensor CLI    114
    IPS Modules    114
    Command-Line Interface Features    116
    Command-Line Interface Uses    119
    Command-Line Interface Modes    119
Initializing the Cisco IPS Sensor    123
Introducing and Configuring Cisco IPS Device Manager    126
Deploying and Configuring Cisco IPS Sensor Interfaces    130
    Creating Promiscuous Interfaces    132
    Creating Inline Interface Pairs    133
    Creating Inline VLAN Pairs    133
    Creating Inline VLAN Groups    133
    Configuring a CDP Policy    134
    Configuring Traffic Flow Notifications    134
    Configuring Sensor Bypass    135
Troubleshooting the Initial Cisco IPS Sensor Configuration    136
Troubleshooting the Cisco IPS Sensor Hardware    138
Restoring the Cisco IPS Sensor Default Settings    138
Summary    138
References    139
Exam Preparation Tasks    140
Review All the Key Topics    140
Definitions of Key Terms    140

Chapter 7    Managing Cisco IPS Devices    143
Overview    143
“Do I Know This Already?” Quiz    143
Chapter 9  Implementing Cisco IPS Signatures and Responses  189

Overview  189

“Do I Know This Already?” Quiz  189

Foundation Topics  192

Cisco IPS Signatures  192

  Signature Engines  193

  Alerts  193

Configuring Basic Signature Properties  197

  Enabling and Disabling Signatures  200

  Retiring and Activating Signatures  200

Configuring Signature Actions  201

  Signature Detective Actions  201

  SNMP Traps  202

  Signature Preventive Actions  202

  Managing Denied Attackers  205

  Detective Signature Action Implementation Guidelines  205

  Preventive Signature Action Implementation Guidelines  206

Configuring Remote Blocking  207

  Using ACLs on a Router  207

  Configuration Tasks  208

Configuring Packet Capture and IP Logging  214

  Downloading, Saving, and Stopping IP Logs  218

Understanding Threat and Risk Management  219

  Risk Rating Calculation  221

  Threat Rating  221

Understanding and Configuring Event Action Overrides  223

Using Event Action Filters  226

Choosing an Action Configuration Strategy  228

Examining Alerts in IPS Event Logs  229

  Viewing Events in the Cisco IDM  232

Summary  233
Chapter 10 Configuring Cisco IPS Signature Engines and the Signature Database 237

Overview 237

“Do I Know This Already?” Quiz 237

Foundation Topics 239

Using Cisco IPS Signature Engines and Configuring Common Signature Engine Parameters 239
Signature and Signature Engines 239
Trigger Counting 243
Summary Key 244
Alarm Summarization 244
Dynamic Alarm Summarization 244

Deploying ATOMIC Signature Engines 245
ATOMIC IP Signature Example 245
Implementation Guidelines for ATOMIC Signature Engines 246

Deploying STRING Signature Engines 246
STRING TCP Signature Example 246
Implementation Guidelines for STRING Signature Engines 247

Deploying SERVICE Signature Engines 247
SERVICE HTTP Signature Example 248
Implementation Guidelines for SERVICE Signature Engines 248

Deploying FLOOD Signature Engines 249
FLOOD Signature Example 249
Implementation Guidelines for FLOOD Signature Engines 249

Deploying SWEEP Signature Engines 250
SWEEP Signature Example 250
Implementation Guidelines for SWEEP Signature Engines 250

Deploying the META Signature Engine 251
META Correlation Example 251
Implementation Guidelines for META Signature Engines 251

Deploying the NORMALIZER Engine 252
NORMALIZER Engine Example 252
Implementation Guidelines for the NORMALIZER Engine 252
Chapter 11 Deploying Anomaly-Based Operation 257
Overview 257
“Do I Know This Already?” Quiz 257
Foundation Topics 259
Anomaly Detection Overview 259
Scanning Worm Details 259
Anomaly Detection Components 260
Histories 261
Zones 261
Learning 261
Signatures Related to Anomaly Detection 262
Configuring Anomaly Detection 262
Default Anomaly Detection Policy ad0 262
Verifying Anomaly Detection 271
Verifying Anomaly Detection at the Command Line 273
Troubleshooting Anomaly Detection 274
Summary 275
References 275
Exam Preparation Tasks 276
Review All the Key Topics 276
Definitions of Key Terms 276

Part IV Adapting Traffic Analysis and Response to the Environment 279

Chapter 12 Customizing Traffic Analysis 281
Overview 281
“Do I Know This Already?” Quiz 281
Foundation Topics 283
Understanding Custom Signatures 283
Chapter 13 Managing False Positives and False Negatives 311

Overview 311

“Do I Know This Already?” Quiz 311

Foundation Topics 313

Identifying False Positives and False Negatives 313

False Positives 313

False Negatives 313

Tuning Consequences 314

Tuning Process Prioritization 314

Tuning to Reduce False Positives 314

Do No Harm, Initially 315

Learning About the Signatures and Why They Triggered a False Positive 316

Selecting and Verifying Signatures and Rules in Place 316

Removing All Aggressive Actions 317

Adding Verbose Alerts and Logging 319

Using the Alert Data and Logging to Tune Out False Positives 322

Tuning the Signatures Based on Your Network 327

Removing the Preliminary Overrides and Filters 328

Tuning the Sensor to Reduce False Negatives 329

Tuning a Specific Signature 330

Promiscuous Mode IP Reassembly 331

TCP Reassembly Mode 333

Normalizer Tuning 334
Chapter 14  Improving Alarm and Response Quality  339

Overview  339
“Do I Know This Already?” Quiz  339
Foundation Topics  341
Identifying and Adjusting Risk-Rating Components  341
  Formula for Risk Rating  341
  Using Attack Severity and Signature Fidelity Ratings  342
  Target Value Ratings  343
  Attack Relevancy Rating  345
  Watch List Rating  346
Operating System Fingerprinting  346
Global Correlation and Reputation-Based Filtering  351
  Reputation Filters  351
  Global Correlation  351
Summary  355
References  355
Exam Preparation Tasks  356
Review All the Key Topics  356
Definitions of Key Terms  356

Part V  Managing and Analyzing Events  359

Chapter 15  Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors  361

Overview  361
“Do I Know This Already?” Quiz  361
Foundation Topics  364
Cisco IPS Manager Express Overview  364
  Cisco IME Versus Cisco IDM  365
Installing Cisco IPS Manager Express  366
Installing Cisco IME  367
Integrating Cisco IPS Manager Express with Cisco IPS Sensors  370
Chapter 16 Managing and Investigating Events Using Cisco IPS Manager Express 389

Overview 389

“Do I Know This Already?” Quiz 389

Foundation Topics 391

Managing IPS Events Using Cisco IPS Manager Express 391
  Event Monitoring Views 391
  Creating and Customizing Event Views 393
  View Settings 393
  Customizing Event Views 395
  Tuning and Creating IME Filters from the Event Display 398
  Saving and Deleting Events 400

Investigating IPS Events Using Cisco IPS Manager Express 401

Acting on IPS Events Using Cisco IPS Manager Express 405

Exporting, Importing, and Archiving Events 408

Summary 409

Exam Preparation Tasks 410

Review All the Key Topics 410

Complete the Tables and Lists from Memory 410

Definitions of Key Terms 410

Chapter 17 Using Cisco IPS Manager Express Correlation, Reporting, Notification, and Archiving 413

Overview 413

“Do I Know This Already?” Quiz 413

Foundation Topics 415
Chapter 18  Integrating Cisco IPS with CSM and Cisco Security MARS  423

Overview  423
“Do I Know This Already?” Quiz  423
Foundation Topics  425
Configuring Integration with Cisco Security Manager  425
  Cisco Security Manager 4.0 Features and Benefits  425
  Managing Cisco IPS Sensors Using Cisco Security Manager  428
  Adding Sensors to Cisco Security Manager  429
Configuring Integration with Cisco Security MARS  431
  Add a Cisco IPS Sensor to MARS  432
  Event Feed Verification  434
  Cisco Security Manager (CSM) and MARS Cross-Launch Capability  435
Summary  436
References  437
Exam Preparation Tasks  438
Review All the Key Topics  438
Complete the Tables and Lists from Memory  438
Definitions of Key Terms  438

Chapter 19  Using the Cisco IntelliShield Database and Services  441

Overview  441
“Do I Know This Already?” Quiz  441
Foundation Topics  443
Using Cisco Security Intelligence Operations  443
  Security Alerts  444
  Threat Analysis and Reporting  445
Resources  446
Products and Services Updates 448
IPS Threat Defense Bulletin 448
Using Cisco IntelliShield Alert Manager Service 449
Home Page 451
Alerts 452
IPS Signatures 454
Inbox 455
Product Sets 456
New Product Sets 458
Notifications 459
Reports 460
Preferences 461
Users 461
Groups 461
IntelliShield Alert Manager Service Subscription 461
Summary 461
References 462
Exam Preparation Tasks 463
Review All the Key Topics 463
Complete the Tables and Lists from Memory 463
Definitions of Key Terms 463

Part VI Deploying Virtualization, High Availability, and High-Performance Solutions 465

Chapter 20 Using Cisco IPS Virtual Sensors 467
Overview 467
“Do I Know This Already?” Quiz 467
Foundation Topics 469
Sensor Virtualization Overview 469
Virtual IPS 469
Adding, Editing, and Configuring Virtual Sensors 470
Verifying Virtual Sensor Operation 475
Summary 478
References 478
Exam Preparation Tasks 479
Review All the Key Topics 479
Complete the Tables and Lists from Memory 479
Definitions of Key Terms 479
Chapter 21  Deploying Cisco IPS for High Availability and High Performance  481

Overview  481

“Do I Know This Already?” Quiz  481

Foundation Topics  483

High-Availability Solutions for Cisco IPS Deployments  483

Switching-Based Sensor High Availability  484

EtherChannel-Based High Availability  485

Inline Mode Redundant IPS Sensor Deployment Using a Single Switch  486

Promiscuous Mode Redundant IPS Sensor Deployment Using a Single Switch  486

EtherChannel-Based High-Availability Implementation Guidelines  486

STP-Based High Availability  487

STP-Based High-Availability Implementation Guidelines  487

Routing-Based Sensor High Availability  488

Routing-Based Sensor High-Availability Implementation Guidelines  488

Cisco ASA-Based Sensor High Availability  489

Cisco ASA–Based Sensor High-Availability Implementation Guidelines  490

Cisco IPS Sensor Performance Overview  491

Performance Issues  491

Detecting Performance Issues  492

Configuring Traffic Flow Notifications  492

Inspecting Performance-Related Gadgets  493

Checking Switch SPAN Interfaces for Dropped Packets  495

Scaling SPAN Sessions  496

Increasing Performance Using Load Sharing  497

ECLB with Cisco Catalyst 6500 Series Switch and IDSM-2  497

Guidelines for Increasing Performance Using Load-Sharing Implementation  497

Increasing Performance Using Traffic Reduction  498

Cisco ASA IPS Modules—Inline Operation  498

Cisco ASA IPS Modules—Promiscuous Operation  498

Cisco Catalyst Switches—VACL Capture  498

Summary  499

References  499

Exam Preparation Tasks  500
Part VII  Configuring and Maintaining Specific Cisco IPS Hardware  503

Chapter 22  Configuring and Maintaining the Cisco ASA AIP SSM Modules  505
Overview  505
“Do I Know This Already?” Quiz  505
Foundation Topics  508
Overview of the Cisco ASA AIP SSM and AIP SSC Modules  508
  Inline Operation  510
  Promiscuous Operation  510
  Single-Mode Cisco ASA with Multiple Virtual Sensors  511
  Cisco ASA with Security Contexts and Virtual Sensors  512
  Deployment Guidelines—ASA AIP SSM and SSC  512
Initializing the Cisco ASA AIP SSM and AIP SSC Modules  512
  Initial Configuration of the AIP SSM and AIP SSC  514
  Software Update of the AIP SSM and AIP SSC  516
  Basic Configuration of the AIP SSM and AIP SSC  520
  Access the AIP SSM and AIP SSC Through the Cisco IDM or ASDM  523
Redirecting Traffic to the Cisco ASA AIP SSM and AIP SSC Modules  525
  Traffic Redirection Policy Configuration Using the Cisco ASDM  526
  Traffic Redirection Policy Configuration Using the CLI  529
Troubleshooting the Cisco ASA AIP SSM and AIP SSC Modules  530
Summary  531
References  531
Exam Preparation Tasks  532
Review All the Key Topics  532
Complete the Tables and Lists from Memory  532
Definitions of Key Terms  532

Chapter 23  Configuring and Maintaining the Cisco ISR AIM-IPS and NME-IPS Modules  535
Overview  535
“Do I Know This Already?” Quiz  535
Foundation Topics  538
Overview of the Cisco ISR AIM-IPS and NME-IPS Modules  538
  Inline Operation  540
  Promiscuous Operation  540
Chapter 24 Configuring and Maintaining the Cisco IDSM-2  555

Overview  555
“Do I Know This Already?” Quiz  555
Foundation Topics  557
Overview of the Cisco IDSM-2  557
  Inline Operation  560
  Promiscuous Operation  561
Initializing the Cisco IDSM-2  562
  Installing the Cisco IDSM-2  562
  Initial Configuration of the Cisco IDSM-2  564
  Command and Control Access for the Cisco IDSM-2  568
  Redirecting Traffic to the Cisco IDSM-2  568
Maintaining the Cisco IDSM-2  572
  Upgrade Procedure  572
  Recovery Procedure  572
  Upgrading the Application Partition  572
  Re-imaging the Maintenance Partition  577
Troubleshooting the Cisco IDSM-2  577
  Password Recovery  577
Summary  578
References  579
Exam Preparation Tasks  580
Review All the Key Topics 580
Complete the Tables and Lists from Memory 580
Definitions of Key Terms 580

Part VIII Final Exam Preparation 583

Chapter 25 Final Preparation 585
Tools for Final Preparation 585
Pearson Cert Practice Test Engine and Questions on the CD 585
Install the Software from the CD 586
Activate and Download the Practice Exam 586
Activating Other Exams 587
Premium Edition 587
Cisco Learning Network 587
Memory Tables 588
Chapter-Ending Review Tools 588
Suggested Plan for Final Review/Study 588
Step 1: Review the Key Topics and the “Do I Know This Already?” Questions from the Beginning of the Chapter 589
Step 2: Complete the Memory Tables 589
Step 3: Do Hands-On Practice 589
Step 4: Build Configuration Checklists 590
Step 5: Use the Exam Engine 590
Summary 591

Part IX Appendixes

Appendix A Answers to the “Do I Know This Already?” Quizzes 595

Appendix B CCNP Security IPS 642-627 Exam Updates, Version 1.0 609

Glossary 613

Index 619

Appendix C Memory Tables (CD Only)

Appendix D Memory Tables Answer Key (CD Only)
Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).
- **Italic** indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({} ) indicate a required choice.
- Braces within brackets ({{ }}) indicate a required choice within an optional element.

Introduction

So, you have worked on Cisco security devices for a while, designing secure networks for your customers, and now you want to get certified. There are several good reasons to do so. The Cisco certification program allows network analysts and engineers to demonstrate their competence in different areas and levels of networking. The prestige and respect that come with a Cisco certification will definitely help you in your career. Your clients, peers, and superiors will recognize you as an expert in networking.

Cisco Certified Network Professional (CCNP) Security is the professional-level certification that represents the knowledge of security in routers, switches, network devices, and appliances. The CCNP Security demonstrates skills required to design, choose, deploy, support, and troubleshoot firewalls, VPNs, and IDS/IPS solutions for network infrastructures.

Although it is not required, Cisco suggests taking the Secure v1.0, Firewall v1.0, VPN v1.0, and IPS v7.0 courses before you take the specific CCNP Security exams. For more information on the various levels of certification, career tracks, and Cisco exams, visit the Cisco Certifications page at http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html.

Our goal with this book is to help you prepare and pass the IPS v7.0 test. This is done by having assessment quizzes in each chapter to quickly identify levels of readiness or areas that you need more help on. The chapters cover all exam topics published by Cisco. Review tables and test questions will help you practice your knowledge on all subject areas.
About the 642-627 IPS v7.0 Exam

The CCNP Security IPS v7.0 exam measures your ability to deploy Cisco IPS–based security solutions. The exam focuses on small- to medium-sized networks. The candidate should have at least one year of experience in the deployment and support of small- to medium-sized networks using Cisco products. A CCNP Security candidate should understand internetworking and security technologies, including the Cisco Enterprise Network Architecture, IPv4 subnets, IPv6 addressing and protocols, routing, switching, WAN technologies, LAN protocols, security, IP telephony, and network management. The new exam adds topics such as new features introduced in the v7.0 secure data center design, and updates IPv6, complex network security rules, troubleshooting, secure WAN design, and optimizing/managing the Cisco IPS security infrastructure device performance.

The tests to obtain CCNP Security certification include Implementing Cisco Intrusion Prevention System v7.0 (IPS) Exam #642-627, Securing Networks with Cisco Routers and Switches (SECURE) Exam #642-637, Deploying Cisco ASA VPN Solutions (VPN) Exam 642-647, and Deploying Cisco ASA Firewall Solutions (FIREWALL) Exam 642-617. All four tests are computer-based tests that have 65 questions and a 90-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for course and exam updates at http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html.

You can take the exam at Pearson VUE testing centers. You can register with VUE at http://www.vue.com/cisco. The CCNP Security certification is valid for three years. To recertify, you can pass a current CCNP Security test, pass a CCIE exam, or pass any 642 or Cisco Specialist exam.
642-627 IPS v7.0 Exam Topics

Table I-1 lists the topics of the 642-627 IPS v7.0 exam and indicates the parts in the book where they are covered.

Table I-1 642-627 IPS v7.0 Exam Topics

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Part</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preproduction Design</td>
<td></td>
</tr>
<tr>
<td>Choose Cisco IPS technologies to implement HLD (High-Level Design)</td>
<td>I</td>
</tr>
<tr>
<td>Choose Cisco products to implement HLD (High-Level Design)</td>
<td>I</td>
</tr>
<tr>
<td>Choose Cisco IPS features to implement HLD (High-Level Design)</td>
<td>I</td>
</tr>
<tr>
<td>Integrate Cisco network security solutions with other security technologies</td>
<td>II</td>
</tr>
<tr>
<td>Create and test initial Cisco IPS configurations for new devices/services</td>
<td>II</td>
</tr>
<tr>
<td>Complex Support Operations</td>
<td></td>
</tr>
<tr>
<td>Optimize Cisco IPS security infrastructure device performance</td>
<td>II</td>
</tr>
<tr>
<td>Create complex network security rules to meet the security policy requirements</td>
<td>III</td>
</tr>
<tr>
<td>Configure and verify the IPS features to identify threats and dynamically block them from entering the network</td>
<td>III, IV</td>
</tr>
<tr>
<td>Maintain, update, and tune IPS signatures</td>
<td>IV, V</td>
</tr>
<tr>
<td>Use CSM and MARS for IPS management, deployment, and advanced event correlation</td>
<td>V</td>
</tr>
<tr>
<td>Optimize security functions, rules, and configuration</td>
<td>V–VII</td>
</tr>
<tr>
<td>Advanced Troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Advanced Cisco IPS security software configuration fault finding and repairing</td>
<td>II, VII</td>
</tr>
<tr>
<td>Advanced Cisco IPS Sensor and module hardware fault finding and repairing</td>
<td>II, VII</td>
</tr>
</tbody>
</table>

About the CCNP Security IPS v7.0 642-627 Official Cert Guide

This book maps to the topic areas of the 642-627 IPS v7.0 exam and uses a number of features to help you understand the topics and to prepare for the exam.
Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. The book is designed to help you pass the CCNP Security IPS v7.0 exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process through test questions on the CD

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- "Do I Know This Already?" quiz: Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
- Foundation Topics: These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- Exam Preparation Tasks: After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
  - Review All the Key Topics: The Key Topic icons appear next to the most important items in the “Foundation Topics” section of the chapter. The Review All the Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - Complete the Tables and Lists from Memory: To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list.
  - Define Key Terms: Although the exam is unlikely to ask a question such as “Define this term,” the CCDA exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
CD-Based Practice Exam: The companion CD contains an exam engine that allows you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint the topics where you need more study.

How This Book Is Organized

This book contains 24 core chapters—Chapters 1 through 24. Chapter 25 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNP Security IPS v7.0 exam. The core chapters are organized into parts. They cover the following topics:

Part I: Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

- Chapter 1, “Intrusion Prevention and Intrusion Detection Systems”: This chapter covers evaluating and choosing approaches to intrusion prevention and detection.
- Chapter 2, “Cisco IPS Software, Hardware, and Supporting Applications”: This chapter covers Cisco IPS solution components available to satisfy policy and environmental requirements.
- Chapter 3, “Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures”: This chapter covers assessing IPS analysis methods, possibilities for evasion in an environment, and choosing the correct anti-evasion methods in a Cisco IPS solution.
- Chapter 4, “Network IPS and IDS Deployment Architecture”: This chapter covers choosing an architecture to implement a Cisco IPS solution according to policy environment requirements.

Part II: Installing and Maintaining Cisco IPS Sensors

- Chapter 5, “Integrating the Cisco IPS Sensor into a Network”: This chapter covers the most optimal method of integrating a Cisco IPS Sensor into a target network.
- Chapter 6, “Performing the Cisco IPS Sensor Initial Setup”: This chapter covers configuring the basic connectivity and networking functions of a Cisco IPS Sensor and troubleshooting its initial installation.
- Chapter 7, “Managing Cisco IPS Devices”: This chapter covers deploying and managing Cisco IPS Sensor management interfaces and functions.

Part III: Applying Cisco IPS Security Policies

- Chapter 8, “Configuring Basic Traffic Analysis”: This chapter covers deploying and managing Cisco IPS Sensor basic traffic analysis parameters.
- Chapter 9, “Implementing Cisco IPS Signatures and Responses”: This chapter covers deploying and managing the basic aspects of Cisco IPS signatures and responses.
- Chapter 10, “Configuring Cisco IPS Signature Engines and the Signature Database”: This chapter evaluates the Cisco IPS signature engines and the built-in signature database.
Chapter 11, “Deploying Anomaly-Based Operation”: This chapter covers deploying and managing Cisco IPS anomaly-based detection features.

Part IV: Adapting Traffic Analysis and Response to the Environment

Chapter 12, “Customizing Traffic Analysis”: This chapter covers deploying and managing custom traffic analysis rules to satisfy a security policy.

Chapter 13, “Managing False Positives and False Negatives”: This chapter covers deploying and managing Cisco IPS Sensor features and approaches that allow the organization to optimally manage false positives and negatives.

Chapter 14, “Improving Alarm and Response Quality”: This chapter covers deploying and managing Cisco IPS features that improve the quality of prevention and detection.

Part V: Managing and Analyzing Events

Chapter 15, “Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors”: This chapter covers installing the Cisco IPS Manager Express (IME) software, integrating it with a Cisco IPS Sensor, and managing related faults.

Chapter 16, “Managing and Investigating Events Using Cisco IPS Manager Express”: This chapter covers the Cisco IME features to view, manage, and investigate Cisco IPS events.

Chapter 17, “Using Cisco IPS Manager Express Correlation, Reporting, Notification, and Archiving”: This chapter covers using Cisco IME features to correlate and report on Cisco IPS events and create notifications.

Chapter 18, “Integrating Cisco IPS with CSM and Cisco Security MARS”: This chapter covers configuring the Cisco IPS to integrate with Cisco Security MARS and choosing Cisco Security MARS features that enhance Cisco IPS event quality.

Chapter 19, “Using the Cisco IntelliShield Database and Services”: This chapter covers choosing the features of and using the Cisco IntelliShield services to gather information about event meaning and response guidelines.

Part VI: Deploying Virtualization, High Availability, and High-Performance Solutions

Chapter 20, “Using Cisco IPS Virtual Sensors”: This chapter covers deploying and managing Cisco IPS policy virtualization.

Chapter 21, “Deploying Cisco IPS for High Availability and High Performance”: This chapter covers deploying and managing features for Cisco IPS redundancy and performance optimization.

Part VII: Configuring and Maintaining Specific Cisco IPS Hardware

Chapter 22, “Configuring and Maintaining the Cisco ASA AIP SSM Modules”: This chapter covers performing initial configuration, installation, troubleshooting, and maintenance of the Cisco ASA AIP SSM hardware modules.
Chapter 23, “Configuring and Maintaining the Cisco ISR AIM-IPS and NME-IPS Modules”: This chapter covers performing the initial configuration, installation, troubleshooting, and maintenance of the Cisco ISR NME and AIM hardware modules.

Chapter 24, “Configuring and Maintaining the Cisco IDSM-2”: This chapter covers performing the initial configuration, installation, troubleshooting, and maintenance of the Cisco IDSM-2 module.

Part VIII: Final Exam Preparation

Chapter 25, “Final Preparation”: This chapter identifies tools for final exam preparation and helps you develop an effective study plan.

Part IX: Appendixes

Appendix A, “Answers to the “Do I Know This Already?” Quizzes”: This appendix includes the answers to all the questions from Chapters 1 through 24.

Appendix B, “CCNP Security IPS 642-627 Exam Updates: Version 1.0”: This appendix provides instructions for finding updates to the exam and this book when and if they occur.

Appendix C, “Memory Tables”: This CD-only appendix contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams. This appendix is available in PDF format on the CD; it is not in the printed book.

Appendix D, “Memory Tables Answer Key”: This CD-only appendix contains the answer key for the memory tables in Appendix C. This appendix is available in PDF format on the CD; it is not in the printed book.
This page intentionally left blank
642-627 IPS v7.0 exam topics covered in this part:

- Choose Cisco IPS technologies to implement HLD (High-Level Design)
- Choose Cisco products to implement HLD (High-Level Design)
- Choose Cisco IPS features to implement HLD (High-Level Design)
Part I: Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

Chapter 1: Intrusion Prevention and Intrusion Detection Systems

Chapter 2: Cisco IPS Software, Hardware, and Supporting Applications

Chapter 3: Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-evasive Countermeasures

Chapter 4: Network IPS and IDS Deployment Architecture
This chapter covers the following subjects:

- **Intrusion Detection Versus Intrusion Prevention**: Understanding the ability to view and alert versus viewing, alerting, and performing an action.

- **Intrusion Prevention Terminology**: The language and definition of the security control components and countermeasures.

- **Network Intrusion Prevention Approaches**: The options available to security administrators when deploying a network IPS in their environment.

- **Endpoint Security Approaches**: The options to protect various endpoints in a network infrastructure.

- **A Systems Approach to Security**: Security has multiple layers, and each layer has vulnerabilities that need to be protected.
Networks have evolved rapidly over the last several years, and so have the methods with which we defend those networks. Traditionally, intrusion detection systems (IDS) have been deployed as a security control or countermeasure to monitor, detect, and notify any unauthorized access to, abuse of, or misuse of information systems or network resources. There is another security control method more commonly used today than in the past known as intrusion prevention systems (IPS). This chapter will cover evaluating and choosing approaches to intrusion prevention and detection.

This chapter begins with “Intrusion Detection Versus Intrusion Prevention,” which is a review of the core concept of defense-in-depth security. Following the review, the chapter examines intrusion prevention terminology and intrusion prevention approaches, including other security controls and approaches.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz helps you determine your level of knowledge of this chapter's topics before you begin. Table 1-1 lists the major topics discussed in this chapter and their corresponding quiz questions. The answers to the “Do I Know This Already?” quiz appear in Appendix A.

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion Prevention Terminology</td>
<td>1, 2</td>
</tr>
<tr>
<td>Intrusion Detection Versus Intrusion Prevention Systems</td>
<td>3</td>
</tr>
<tr>
<td>Intrusion Prevention Approaches</td>
<td>4, 5</td>
</tr>
<tr>
<td>Endpoint Security Controls</td>
<td>6–9</td>
</tr>
<tr>
<td>A Systems Approach to Security</td>
<td>10</td>
</tr>
</tbody>
</table>
1. Which security control is a consequence of nonmalicious activity generally representing an error?
   a. True positive
   b. False positive
   c. True negative
   d. False negative

2. Which of the following terms is a weakness that can allow a compromise of the security or the functionality of a system?
   a. Exploit
   b. Vulnerability
   c. Threat
   d. Risk

3. Which of the following capabilities does an IPS have that an IDS does not?
   a. Detect
   b. Alert
   c. Prevent
   d. Monitor

4. Which of the following is not a factor that influences the addition of sensors?
   a. Performance capabilities of the sensor
   b. Exceeded traffic capacity
   c. Network implementation
   d. Performance capabilities of the host

5. Which of the following network intrusion prevention approaches observes network traffic compared to a baseline and acts if a network event outside the normal network behavior is detected?
   a. Anomaly-based network IPS
   b. Signature-based network IPS
   c. Policy-based network IPS
   d. Host-based IPS

6. Which of the following are limitations of endpoint security controls?
   a. Controls are useless if the host is compromised before endpoint security is applied.
   b. All hosts require an agent.
   c. Operating system dependent (might not be supported).
   d. No correlation is possible if a single agent is deployed.
   e. All of the above.
7. Cisco Security Agent uses API interception to control access to all of the following except for which one?
   a. Host itself
   b. Files
   c. Process
   d. Windows Registry

8. Which of the following is designed to prevent file-based malware threats and uses content scanning to identify known patterns of malware?
   a. Heuristics antimalware
   b. File-based antimalware
   c. Code emulation
   d. Pattern matching

9. Which of the following are endpoint security controls?
   a. Cryptographic data protection
   b. Antimalware agents
   c. Host-based firewalls
   d. Native operating system access controls
   e. All of the above

10. Which of the following requires a network-focused technology to provide a defense-in-depth security solution?
    a. Protection of the operating systems
    b. Protection of applications and the data they handle
    c. Detection and prevention of DoS attacks
    d. Controlling access to local host process
Intrusion Prevention Overview

All the CCNP Security exams consider CCNA Security materials as prerequisites, so the Cisco Press CCSP Exam Certification Guide series of books also assumes that you are already familiar with CCNA Security topics. However, the CCNP Security exams do test on features that overlap with CCNA Security. Additionally, most people forget some details along the way.

This book uses two methods to help you review CCNA-level Security topics. The first is an examination of concepts included in the CCNA Security certification. The second is a brief review of other CCNA-level Security features along with a deeper discussion of each topic.

To that end, the following sections begin with a review of intrusion prevention terminology. The following section details the key features and limitations of both intrusion detection and intrusion prevention systems. Finally, the last part of this chapter discusses security controls, approaches, and technologies.

Intrusion Detection Versus Intrusion Prevention

An intrusion detection system (IDS) is a security control or countermeasure that has the capability to detect misuse and abuse of, and unauthorized access to, network resources. An IDS, in most cases, is a dedicated device that monitors network traffic and detects malicious traffic or anomalies based on multiple criteria.

Figure 1-1 shows how an IDS is typically deployed. Notice the placement of the device.

Some of the most commonly detected attacks by a network IDS are as follows:

- Application layer attacks, such as directory traversal attacks, buffer overflows, or various forms of command injection.
- Network sweeps and scans (indicative of network reconnaissance).
- Flooding denial of service (DoS) attacks in the form of TCP SYN packets or large amounts of Internet Control Message Protocol (ICMP) packets. DoS attacks are those in which an attacker uses a large number of compromised systems to disrupt the operation of another system or device on a network. Attacks of this nature can impact the resources of a system and severely degrade performance.
- Common network anomalies on most Open Systems Interconnection (OSI) layers. Some of these common network anomalies detected by a network IDS include the following:
  - Invalid IP datagrams
  - Invalid TCP packets
  - Malformed application layer protocol units
  - Malformed Address Resolution Protocol (ARP) requests or replies
After an IDS detects an anomaly or offending traffic, it generates alerts, which are stored locally on the IDS and can be retrieved by a management system. The network security administrators monitor these alerts generated by the IDS and decide how to react. An IDS cannot stop an attack or malicious traffic alone.

A security control or countermeasure that has the capability to detect and prevent misuse and abuse of, and unauthorized access to, networked resources is an intrusion prevention system (IPS).

Figure 1-2 shows how an IPS is typically deployed. Notice the placement of the device or sensor.

**Intrusion Prevention Terminology**

Before digging too deeply into intrusion prevention technology, we examine terminology that is important to understand. This section only focuses on terminology as it relates to intrusion prevention; there is a more inclusive list of information security terms in the glossary.

As discussed, an IPS or IDS detects and produces alerts because of a number of factors that include legitimate malicious activity, misconfiguration, environmental changes, and so on. Security controls are classified in one of the following terms:

- **True positive:** A situation in which a signature fires correctly when intrusive traffic for that signature is detected on the network. The signature correctly identifies an attack against the network. This represents normal and optimal operation.
Host
Management interface; the interface is not used for traffic analysis. (Has IP address assigned.)
Internet
Management
Network
The sensor sits in the traffic path and has the capability to drop traffic when desired. *Inline interfaces do not have IP addresses.* Cisco IPS operates at Layer 2 and can be thought of as a “smart wire.”

**Figure 1-2** *Intrusion Prevention System*

- **False positive:** A situation in which normal user activity triggers an alarm or response. This is a consequence of nonmalicious activity. This represents an error and generally is caused by excessively tight proactive controls or excessively relaxed reactive controls.

- **True negative:** A situation in which a signature does not fire during normal user traffic on the network. The security control has not acted and there was no malicious activity. This represents normal and optimal operation.

- **False negative:** A situation in which a detection system fails to detect intrusive traffic although there is a signature designed to catch the activity. In this situation, there was malicious activity, but the security control did not act. This represents an error and generally is caused by excessively relaxed proactive controls or excessively tight reactive controls.

Most security administrators will agree that addressing false negative and false positive issues is a bit of a balancing act. While tuning a system to be less restrictive to fix false positives, you can increase the likelihood of false negatives and vice versa. Security controls should only be tuned by those expertly trained to do so to optimize these decisions.

Preventive controls, such as IPS sensors, are often tuned to be less sensitive to prevent blocking legitimate traffic, while detective controls, such as IDS sensors, are tuned to be more sensitive, which often results in false positives. Some best practices often combine a sensitive detective control with a relaxed preventive control to gain insight to the preventive control and enable incident response. This is often advantageous if the preventive control is bypassed.

Some other critical terminology that is important to understand when dealing with intrusion prevention are *vulnerability, exploit, risk,* and *threat.*
A *vulnerability* is a weakness that compromises either the security or the functionality of a system. You'll often hear the following examples listed as vulnerabilities:

- **Insecure communications**: Any form of data or voice susceptible to interception, such as system passwords, personnel records, and confidential documents.
- **Poor passwords**: Often referred to as the first line of defense. Weak or easily guessed passwords are considered vulnerabilities.
- **Improper input handling**: Software that hasn’t been through a good security and quality scan (which usually involves evaluating all possible input and results) can lead to a form of DoS or access denied or restricted to system resources.

An *exploit* is the mechanism used to leverage a vulnerability to compromise the security functionality of a system. You'll often hear the following examples listed as exploits:

- **Executable code**: Often referred to as more advanced form of an exploit, these are exploits written as executable code requiring programming knowledge and access to software tools such as a compiler.
- **Password-guessing tools**: There are tools built specifically for this function that can be easily found on the Internet designed to “guess” or “crack” passwords using knowledge of the algorithm used to generate the actual password or by attempting to access a system using combinations and permutations of different character sets.
- **Shell or batch scripts**: Scripts created to automate attacks or perform simple procedures known to expose the vulnerability.

A *threat* is defined as any circumstance or event with the expressed potential for the occurrence of a harmful event to an information system in the form of destruction, disclosure, adverse modification of data, or DoS. Examples of Internet threats that have been prevalent over the past few years include malware that utilizes HTML code or scripts that the cybercriminals place on legitimate websites. These programs generally redirect a user to a malicious user’s exploit-infected website without the user noticing. Other examples of threats include network attacks against exposed application servers, malware targeting workstations, or even physical destruction (natural or unnatural).

A *risk* is the likelihood that a particular threat using a specific attack will exploit a particular vulnerability of an asset or system that results in an undesirable consequence. Security engineers, administrators, and management will often try to determine risk in their business continuity and disaster recovery planning. A simple equation often used to equate risk is to multiply threat by vulnerability and multiply the result by the asset value. This equation might sound simple, but the vulnerability and threat of an asset depend on a number of factors to include the presence and quality of the security controls deployed to guard an asset, the capability of the attacker, and the frequency of attacks.

Some other critical terms we’ll reference throughout the study guide are as follows:

- **Risk rating (RR)**: A rating based on numerous factors besides just the attack severity.
- **Deep-packet inspection**: Decoding protocols and examining entire packets to allow policy enforcement based on actual protocol traffic (not just a specific port number).
Event correlation: Associating multiple alarms or events with a single attack.

Inline mode: Examining network traffic while having the ability to stop intrusive traffic from reaching the target system.

Promiscuous mode: Also known as passive mode, a way to passively examine network traffic for intrusive behavior.

Signature: A rule configured in a network IPS or IDS device that describes a pattern of network traffic that matches a specific type of intrusion activity.

Signature engine: An engine that supports signatures that share common characteristics (such as the same protocol, service, operating system, and so on). The Cisco IPS Sensor has multiple signature engines called microengines.

Atomic signature: A signature that triggers based on the contents of a single packet.

Flow-based signature: A signature that triggers based on the information contained in a sequence of packets between two systems (such as the packets in a TCP connection).

Anomaly-based signature: A signature that triggers when traffic exceeds a baseline.

Behavior-based signature: A signature that triggers when traffic deviates from regular user behavior.

Meta-event generator: The capability to define metasignatures based on multiple existing signatures that trigger at or near the same window of time within a sliding time interval.

Intrusion Prevention Systems

As defined earlier, an IPS (also referred as a network IPS or NIPS) is a security control put in place to detect by analyzing network traffic and prevents by attempting to block malicious network traffic. There are different aspects in which a network IPS analyzes traffic, such as the following:

Reassembles Layer 4 sessions and analyzes their contents

Monitors packet and session rates to detect and/or prevent deviations from the baseline (or normal) network profiles

Analyzes groups of packets to determine whether they represent reconnaissance attempts

Decodes application layer protocols and analyzes their contents

Analyzes packets to address malicious activity contained in a single packet

Network intrusion prevention systems provide proactive components that effectively integrate into the overall network security framework. A network IPS includes the deployment of sensors (also known as monitoring devices) throughout the network to analyze traffic as it traverses the network. An IPS sensor detects malicious and/or unauthorized activity in real time and takes action if/when required. There are various approaches to
deploying IPS sensors, which are usually deployed at designated points that enable security managers to monitor network activity while an attack is occurring in real time. The security policy will often drive the designated points in the network where the sensors are to be deployed.

Network growth will often require additional sensors, which can easily be deployed to protect the new networks. A network IPS enables security managers to have real-time insight into their networks regardless of the growth caused by more hosts or new networks. Following are some common factors that often influence the addition of sensors:

- **Network implementation**: Additional sensors might be required to enforce security boundaries based on the security policy or network design.

- **Exceeded traffic capacity**: Additional bandwidth requirements might require an addition or upgrade of network link(s), thus requiring a higher-capacity sensor.

- **Performance capabilities of the sensor**: The current sensor might not be able to perform given the new traffic capacity or requirements.

Typically, network IPS sensors are tuned for intrusion prevention analysis. In most cases, the operating system of an IPS sensor is “stripped” of any unnecessary network services while essential services are secured. To maximize the intrusion prevention analysis for networks of all types, there are three essential elements to the IPS hardware:

- **Memory**: Intrusion prevention analysis is memory intensive. The memory directly affects the ability of a network IPS to detect and prevent an attack accurately.

- **Network interface card (NIC)**: The network IPS must have the capability to connect into any network infrastructure. Network IPS NICs today include Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet.

- **Processor**: CPU power to perform intrusion prevention protocol analysis and pattern matching is required for an effective intrusion prevention system.

**Features of Network Intrusion Prevention Systems**

A network IPS has four main features:

- A network IPS can detect attacks on several different types of operating systems and applications, depending on the extent of its database.

- A single device can analyze traffic for a large scale of hosts on the network, which makes network IPSs a cost-effective solution that decreases the cost of maintenance and deployment.

- As sensors observe events from and to various hosts and different parts of the network, they can correlate the events, hosts, and networks to higher-level information. In conjunction with the correlation, they can obtain deeper knowledge of malicious activity and act accordingly.

- A network IPS can remain invisible to the attacker through a dedicated interface that monitors only network traffic and is unresponsive to various triggers or stimuli.
Limitations of Network Intrusion Prevention Systems

The most commonly known limitations of network IPS are as follows:

- The network IPS can require expert tuning to adapt the sensor to its network, host, and application environments.
- The network IPS sensor is unable to analyze traffic on the application layer when traffic is encrypted either with IPsec or SSL (Secure Socket Layer).
- The network IPS can be overloaded by network traffic if not properly sized. Thus, the IPS can easily fail to respond to real-time events in a timely manner if it is sized improperly.
- The network IPS might interpret traffic improperly, which can lead to false negatives. This is often a result of the sensor’s seeing traffic differently from how the end system or target sees the traffic.

Network Intrusion Prevention Approaches

There are three commonly used approaches to network intrusion prevention by security managers today. The security policy often helps security managers determine the approach in which they’ll deploy in their networks. In some cases, you’ll see more than one approach on one particular network. The three commonly used approaches are as follows:

- **Signature-based:** A network IPS that analyzes network traffic and compares the data in the flow against a database of known attack signatures. A signature-based IPS looks at the packet headers and/or data payloads when analyzing network traffic. All signature-based IPSs require regular updates for their signature databases. Table 1-2 outlines signature-based features and limitations.

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>Simple for administrators to add new signatures, customize signatures, extend, and so on. Often the simplest of IPS approaches to deploy (depends on the environment).</td>
<td>Sensors require constant and quick updates of the signature database to ensure that the IPS can detect the most recent attacks. Can require expert tuning to be effective in complex and unsteady environments.</td>
</tr>
<tr>
<td>Susceptibility and Accuracy</td>
<td>Relatively low false positive rate (if the IPS is properly tuned and using well-designed signatures).</td>
<td>More susceptible to evasion through complex signatures that are designed to evade a signature-based IPS. Cannot detect unknown attacks of which there is no signature in the database.</td>
</tr>
</tbody>
</table>
Chapter 1: Intrusion Prevention and Intrusion Detection Systems

■ **Anomaly-based:** A network IPS that analyzes or observes network traffic and acts if a network event outside normal network behavior is detected. The two types of anomaly-based network IPSs are *statistical anomaly detection* and *protocol verification*. Table 1-3 outlines anomaly-based features and limitations.

<table>
<thead>
<tr>
<th>Table 1-2</th>
<th>Signature-Based Features and Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
<td><strong>Feature</strong></td>
</tr>
<tr>
<td>Reporting</td>
<td>Ability to name attacks and provide the administrator with additional information about a specific attack.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 1-3</th>
<th>Anomaly-Based Features and Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td><strong>Limitations</strong></td>
</tr>
<tr>
<td>Ability to act on both known and yet-unknown threats.</td>
<td>More susceptible to evasion through complex signatures that are designed to evade an anomaly-based IPS.</td>
</tr>
<tr>
<td></td>
<td>Unable to name individual attacks.</td>
</tr>
<tr>
<td></td>
<td>Statistical approach requires a learning period to establish a normal network profile.</td>
</tr>
<tr>
<td></td>
<td>Statistical approach can cause false positives in unstable environments where it can be difficult or impossible to establish a model of a normal network traffic behavior.</td>
</tr>
</tbody>
</table>

■ **Policy-based:** A network IPS that analyzes traffic and acts if it detects a network event outside a traffic policy. A traffic policy usually involves permitted or denied communications over a network segment similar to an enterprise-class firewall. Table 1-4 outlines policy-based features and limitations.

<table>
<thead>
<tr>
<th>Table 1-4</th>
<th>Policy-Based Features and Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td><strong>Limitations</strong></td>
</tr>
<tr>
<td>Very focused on the target environment and triggers very few false positives; thus, very accurate and effective in most cases.</td>
<td>Requires the design of the policy from scratch, which in best practice should be as minimal as possible using as much detail as possible to provide the best protection.</td>
</tr>
<tr>
<td>Ability to act on both known and yet-unknown threats.</td>
<td>Unable to name individual attacks.</td>
</tr>
</tbody>
</table>
 Endpoint Security Controls

Another form of intrusion prevention is the host IPS (HIPS). Often referred to as endpoint security controls, a HIPS consists of operating system security controls or security agent software installed on hosts that can include desktops PCs, laptops, or servers. Host IPSs in most cases extend the native security controls protecting an operating system or its applications. Endpoint security controls can monitor local operating system processes and protect critical systems resources. HIPSs fundamentally have two essential elements: a software package installed on the endpoint or agent to protect it and a management system to manage the endpoints or agents.

In most cases, operating systems today split the runtime functions of the operating systems into two concurrently running modes known as Kernel mode and User mode. Kernel mode is the software that has complete access to the operating system hardware; thus, all the software running in Kernel mode can act without restrictions. Generally, the software running in Kernel mode includes the hardware drivers, operating system scheduler, and the application programming interfaces (API). User mode is the software that requires kernel services to execute applications in the form of processes but don't have direct access to the hardware components of the operating system. There is required protection in the system hardware that separates the two modes so that the User mode applications cannot tamper with the Kernel mode software.

Access control enforcement for an operating system can be done using local system resources (native operating system access control) or remote system resources (RADIUS, TACACS, and so on). The local system of user or process privileges and permissions on the discretion of the logical owner/administrator is known as Discretionary Access Control (DAC). Another local system access control that extends the functionality by using the user’s role in the organization is known as Role-Based Access Control (RBAC) capability. Access control lists (ACL) are often used to define which systems or networks have access and in which direction. Audit trails (system logs) can aid in the detection of system misuse and attacks to protected objects. The same access control mechanism that decides whether to permit or deny access usually provides this audit trail, showing successful and unsuccessful access attempts. Buffer and heap overflow protection is critical for local applications that contain input-validation vulnerabilities. Protection against buffer and heap overflow attacks is often embedded into hardware and operating systems that provide specialized protection against this specific class of threats. Table 1-5 summarizes the features and limitations of endpoint security.

<table>
<thead>
<tr>
<th>Features</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity association, meaning that the endpoint security control can provide the information about the attacker.</td>
<td>Platform flexibility (some operating systems might not support endpoint security controls).</td>
</tr>
<tr>
<td>System-specific or customized to protect the system it is protecting and resides on.</td>
<td>Inability to correlate whether a single endpoint or agent is deployed.</td>
</tr>
</tbody>
</table>
Chapter 1: Intrusion Prevention and Intrusion Detection Systems

Host-Based Firewalls

Endpoint security isn’t complete without a form of host-based firewall. There are two basic implementations, which include packet filtering and socket filtering (also known as API call filtering):

- **Packet filtering:** Host firewalls use stateful and stateless packet filtering, and typically support dynamic applications such as HTTPS, FTP, and so on. Filtering is based on Open Systems Interconnection (OSI) Layer 3 and 4 information, so it can control connections based on host addresses, protocols, and port numbers. Similar in behavior to a network firewall.

- **Socket filtering (API call filtering):** Controlling application requests to either create an outgoing or accept an incoming connection by filtering network-related API calls. API call filtering is applications aware, so there is no need to require intelligence to support dynamic sessions.

### API and System Call Interception

Secondary Security Reference Monitor (SSRM) is an operating system security extension that provides a “second opinion” or layered approach of security by extending and duplicating the functionality of the native operating security model. SSRMs are often third-party extensions for the operating system kernel. They use API interception to insert themselves into the access control path. API interception has a low performance impact while consuming less than 5 percent of additional CPU resources; therefore, most today’s HIPS products implement SSRM functionality. API interception (also called *API hooking*) is when an API call is intercepted and the SSRM registers itself as the replacement handler code for the API call it considers important enough to intercept. This allows the SSRM to enforce its own security policy. The SSRM can act as the host firewall, now controlling all applications’ access to the network.

### Cisco Security Agent

The Cisco HIPS is Cisco Security Agent (CSA), which complements the Cisco NIPS, protecting the integrity of applications and operating systems. Malicious activity is blocked before damage is done by using behavior-based technology that monitors application behaviors. CSA protects against known and new/unknown attacks. Residing between the

---

**Table 1-5  Features and Limitations of Endpoint Security**

<table>
<thead>
<tr>
<th>Features</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to see malicious network data; consequences of network attacks even if encrypted.</td>
<td>Every host requires an agent. Thus, the cost of endpoint security controls can become quite large in some environments and also be quite challenging to manage with only a single or a few administrators to manage the hosts.</td>
</tr>
<tr>
<td>Detection of the success of an attack and can take action after the system is stable.</td>
<td>If an attack is successful in accessing the host prior to the endpoint security reacting, the host is compromised.</td>
</tr>
</tbody>
</table>
kernel and applications, CSA enables maximum application visibility with little impact to the performance and stability of the underlying operating system. A few of the numerous network security benefits CSA offers are as follows:

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses.
- Visibility and control of sensitive data protect against loss from both user actions and targeted malware.
- Predefined compliance and acceptable use policies allow efficient management, reporting, and auditing of activities.
- System is protected at all times, even when users are not connected to the corporate network or lack the latest patches. This is often referred to as “always vigilant” security.

As stated in the previous paragraph, host IPSs and network IPSs are complementary. Table 1-6 illustrates this point.

<table>
<thead>
<tr>
<th>Key Topic</th>
<th>Table 1-6 Host IPS (HIPS) and Network IPS (NIPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host IPS</strong></td>
<td><strong>Network IPS</strong></td>
</tr>
<tr>
<td>CSA can inspect the behavior of applications (encrypted or nonencrypted).</td>
<td>Requires constant updates for new vulnerabilities.</td>
</tr>
<tr>
<td>CSA is a behavior-based HIPS.</td>
<td>Can prevent known attacks.</td>
</tr>
<tr>
<td>CSA does not need constant updates.</td>
<td>Can protect complete network.</td>
</tr>
<tr>
<td>CSA can protect the host (server, desktop, and so on) efficiently, communicate with IPSs, and stop known and unknown (Day Zero) attacks.</td>
<td>—</td>
</tr>
<tr>
<td>CSA cannot “name” the attack or protect unsupported platforms.</td>
<td>—</td>
</tr>
</tbody>
</table>

**Antimalware Agents**

Antivirus and antispyware are primarily designed to find file-based malware threats and scan the content to identify known patterns of malware. This tends to be a permissive security approach. File and memory content can both contain traces of known malware, and fortunately antimalware scanners can examine both. Some antimalware scanners can perform scanning using the following methods or approaches:

- Using on-demand scanning when the user initiates a thorough system scan.
- Using real-time scanning, which in some cases isn’t as thorough as offline/on-demand, especially if executable code is populated in memory and the files being scanned are busy writing or reading from the file system.
- Using scanning in a scheduled manner in which all files are scanned thoroughly on the endpoint.
Viruses, spyware, adware, Trojan horses, worms that use file-based infections, rootkit software, and general attack tools can all be detected using file-based antimalware software, as long as that type of malware is known (through the malware database) and can be located using the file and memory scanning.

Typically, the antimalware scans files and memory for known patterns of virus code. This is compared to a database of known malware signatures. In some instances for accuracy, a lot of antivirus scanners today require content matching through multiple, independent detectors for the same virus. Scanners that analyze content for suspicious coding tricks, runtime attributes, structure, and behavior associated with malicious code use heuristic antimalware. Heuristics are not that reliable for new viruses and often will use various techniques that weight malicious features to determine whether the code should be classified as malicious. A common antimalware scanning technique is known as code emulation. In code emulation, the antimalware software executes suspicious code in a simple virtual machine that is isolated or sandboxed from the rest of the system. The antimalware scanner can (or attempts to) determine the behavior and actions that the suspicious code performs. The learned behavior is then stored in a database of executable signatures that can detect known patterns of execution to detect the virus in the future.

Data Loss Prevention Agents

Another form of endpoint security is known as Data Loss Prevention (DLP) extensions. DLP controls mobile data distributed on users’ systems to prevent users from accidentally or deliberately transferring sensitive data to uncontrolled systems. Examples of uncontrolled systems would be paper (using printers), open network systems (file sharing), and mobile storage (USB keys, portable hard disks, and so on). There are different forms of implementation when it comes to DLPs, but two common examples would be using content scanning to identify sensitive content (assuming that the content is labeled appropriately with a standardized labeling systems identifying sensitive material) and controlling transfer of data off the system using interception of users’ and applications’ actions.

Cryptographic Data Protection

One of the most discussed and well-known approaches to endpoint security today is file integrity checking to detect unauthorized changes to sensitive files or the system itself. Integrity-checking software calculates a secure fingerprint (HMAC [Hash Message Authentication Code]) for every important file on the system with a secret key. These fingerprints are created when the file(s) are known to be trusted and not modified from their original states. There are periodic rescans of the files and file fingerprints compared to a database of known good fingerprints, which identify whether they have been tampered with.

Integrity checkers rescan files in a specified interval or time, so they can only provide detection of attacks rather than provide real-time detection. It’s important to note that integrity checkers can be compromised with the system, given that they are usually a user-mode application.

Encryption is also an important method to prevent data from being stolen or compromised physically from a system, disk drive, third-party add-on, or file system. The user
holds the decryption keys with Windows EFS (Encrypting File System) that are transparently linked to user credentials and provide access to encrypted information. Lost cryptographic keys can lead to sensitive data loss, which is why many security policies require the creation of a backup decryption key. Key generation might be left to the user, which substantially weakens cryptography protection of data if operated poorly. If stolen, an attacker must attempt to decrypt protected information; however, this is very difficult to do if cryptographic implementation and key management are done properly.

A Systems Approach to Security

Multiple layers of protection increase the probability of detection and prevention of malicious activity. As we’ve discussed, there are multiple approaches to detection and prevention, but it’s important to understand that what one security control detects, another type can overlook. Proper correlation results in more accurate or trustworthy data about system behavior or incidents when network and endpoint security controls are used together.

A defense-in-depth security solution attempts to protect assets by providing layers of security. Applying security controls at the network and host levels provides this defense-in-depth concept. Table 1-7 summarizes and compares the defense-in-depth technology approaches. It’s important to understand that one isn’t preferred over the other, but they both complement each other.

<table>
<thead>
<tr>
<th>Host-Focused Technology</th>
<th>Network-Focused Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protects the operating system</td>
<td>Detects and prevents DoS attacks</td>
</tr>
<tr>
<td>Controls access to local host resources</td>
<td>Detects and prevents network reconnaissance attacks</td>
</tr>
<tr>
<td>Protects applications and the data they handle</td>
<td>Detects and prevents attacks against many network-facing applications and operating systems</td>
</tr>
</tbody>
</table>
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from the chapter, noted with the Key Topic icons in the margin of the page. Table 1-8 lists a reference of these key topics and the page numbers on which each is found.

Table 1-8   Key Topics for Chapter 1

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1-1</td>
<td>Intrusion Detection System</td>
<td>9</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Security Controls Classifications</td>
<td>9</td>
</tr>
<tr>
<td>Figure 1-2</td>
<td>Intrusion Prevention System</td>
<td>10</td>
</tr>
<tr>
<td>Table 1-2</td>
<td>Signature-Based Features and Limitations</td>
<td>14</td>
</tr>
<tr>
<td>Table 1-3</td>
<td>Anomaly-Based Features and Limitations</td>
<td>15</td>
</tr>
<tr>
<td>Table 1-4</td>
<td>Policy-Based Features and Limitations</td>
<td>15</td>
</tr>
<tr>
<td>Table 1-5</td>
<td>Features and Limitations of Endpoint Security</td>
<td>16</td>
</tr>
<tr>
<td>Table 1-6</td>
<td>Host IPS and Network IPS</td>
<td>18</td>
</tr>
<tr>
<td>Table 1-7</td>
<td>Defense-in-Depth: Host-Focused and Network-Focused Technology</td>
<td>20</td>
</tr>
</tbody>
</table>

Complete the Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

- vulnerability
- exploit
- risk
- threat
- signature
- anomaly
Symbols & Numerics

? (question mark), accessing CLI help information, 116
2SX interface card, 34
4GE bypass interface card, 33
10GE interface card, 33
624-627 IPS v7.0 exam
   preparing for, Pearson IT Certification Practice Test Engine, 585-587
   prerequisites, 114-121
   topics, 121-153
6500 Series Catalyst switches, IDSM-2 module, 35

A

accessing
   AIP SSM, 523-525
   Cisco IPS Sensor CLI, 114
   CLI help information, 116
ACLs (access control lists), remote blocking, 207
acting on events with Cisco IME, 405-407
actions, 201-206
   aggressive responses, removing, 317-319
   configuration strategy, selecting, 228-229
detective actions, implementing, 205
   event action filters, 226-228
   overrides, configuring, 223-226
preventive actions
   configuring, 202-205
   implementing, 206
signature detective actions, configuring, 201-202
SNMP traps, configuring, 202
activating signatures, 200-201
adding
   gadgets to dashboard, 129
   sensors
      to Cisco Security MARS, 432-434
      to CSM, 429-430
   sensors to IPS, reasons for, 13
   virtual sensors, 470-471
advanced setup, sensors, 126
aggressive responses to actions, removing from sensors, 317-319
AIC (Application Inspection and Control) engines, deploying, 253
AIM (Advanced Integration Module)
   IPS sensors, 36-37
AIM-IPS
   heartbeat operation, 547-548
   initializing, 543-546
   inline operation, 540
   promiscuous mode, 540
   rebooting, 548-549
redirecting traffic to, 546-547
router communication, 541-542
router support, 538-539
troubleshooting, 547-550
AIP SSC-5 (Advanced Inspection and Prevention Security Services Card-5), 34-35
accessing, 523-525
comparing with AIP SSM, 510
configuring, 520-523
deploying, 512
redirecting traffic to, 525-530
troubleshooting, 530-531
AIP SSM, 34-35, 508-509
accessing, 523-525
comparing with AIP SSC, 510
configuring, 520-523
console session, starting, 114-115
deploying, 512
initializing, 512-520
inline operation, 510
promiscuous mode, 510
redirecting traffic to, 525-530
troubleshooting, 530-531
alarm summarization, 244
alerts, 9-10, 193-197
Cisco Security IntelliShield Alert Manager Service, 47-48
in event logs, examining, 229-232
false positives, reducing, 322-325
verbose alerts, configuring, 319-322
Alerts page (SIAM), 452-453
analyzing alerts in event logs, 229-232
anomaly-based detection, 259-274
components, 260-262
histograms, 261
learning, 261-262
zones, 261
configuring, 262-271
troubleshooting, 274
verifying, 271-274
worms, 259-260
anomaly-based intrusion prevention, 15
anomaly-based signatures, 12
answer key to “Do I Know This Already?” quizzes, 595-606
API interception, 17
application partition (IDSM-2), upgrading, 572-576
application-layer decoding, 335
architecture
Cisco IPS software architecture, 38-41
architecture, Cisco IPS software architecture
CollaborationApp, 40
MainApp, 39-40
SensorApp, 39
archiving events, 408-409
ARR (Attack Relevancy Rating), 345
ASA selective capture, IPS
promiscuous mode deployment, 98-99
ASR (attack severity rating), 342-343
assigning traffic sources to vs0, 176-177
Atomic IP Advanced engine, 182
ATOMIC signature engines, deploying, 245-246
atomic signatures, 12
attacks, 8
buffer overflow attacks, 16
denied attackers, managing, 205
heap overflow attacks, 16
insertion attacks, 60
timing attacks as evasion technique, 58
authentication
HMAC, 19
sensors, managing, 153-154

back panel
Cisco IPS 4240 sensors, 28-29
Cisco IPS 4255 sensors, 29-30
Cisco IPS 4260 sensors, 31
Cisco IPS 4270 sensors, 33
batch scripts, 11
behavior-based signatures, 12
blocking
with ACLs, 207
configuring, 208-214
buffer overflow attacks, 16
bypassing network detection, evasion techniques, 57-62
encryption and tunneling, 58
protocol-level misinterpretation, 59-60
resource exhaustion, 58-59
timing attacks, 58
traffic fragmentation, 59
traffic substitution and insertion, 60-62

C

calculating RR, 219-221, 341-342
ARR, 345
TVRs, 343-345
case sensitivity of commands, 117
categories of reports, 415
CDP (Cisco Discovery Protocol) policies, configuring, 134
centralized campus, sensor placement, 79-81
choosing action configuration strategy, 228-229
CIDEE (Cisco Intrusion Detection Event Exchange), 41
Cisco AIM (Advanced Integration Module) IPS sensor, 36-37
Cisco ASA 5500 Series, AIP SSM, 34-35
Cisco ASA-based sensor high availability, 489-490
Cisco IDM (IPS Device Manager), 42
and Cisco IME, 365-366
configuring, 126-130
events, viewing, 232-233
gadgets, adding to dashboard, 129
home page, customizing, 128
network settings, configuring, 146-147
Cisco IME (IPS Manager Express), 42
and Cisco IDM, 365-366
event management, 391-401
Event Monitoring views, 391-393
saving/deleting events, 400-401
Event Monitoring views, customizing, 395-397

events
acting on, 405-407
exporting, 408-409
importing, 408-409
investigating, 401-404

filters, creating, 398-400
installing, 366-368
integrating with Cisco IPS sensors, 370-374
notifications, 418-420
reporting, 415-417
reports, configuring, 416-417
RSS feeds, 382-385
supported Cisco IPS hardware, 366-367
tasks, 364-365
user interface
customizing, 376-378
dashboards, 378-380
gadgets, 380-382

Cisco IPS 4200 Series sensors, 27-28
Cisco IPS 4240 sensors, 28-29
Cisco IPS 4255 sensors, 29-30
Cisco IPS 4260 sensors, 30-32
Cisco IPS 4270 sensors, 32-34
Cisco IPS 4240 sensors, 28-29
Cisco IPS 4255 sensors, 29-30
Cisco IPS 4260 sensors, 30-32
Cisco IPS 4270 sensors, 32-34
Cisco IPS NME (Network Module Enhanced), 36-37
heartbeat operation, 547-548
initializing, 543-546
inline operation, 540
promiscuous mode, 540
rebooting, 548-549
redirecting traffic to, 546-547
router communication, 542-543
router support, 538-539
troubleshooting, 547-550

Cisco IPS Sensor CLI
accessing, 114
authentication, managing, 153-154
editing keys, 118
features, 116-118
help information, accessing, 116
interface modes, 119-122
global configuration mode, 121
privileged EXEC mode, 120
service mode, 122
service signature definition mode, 122
remote management access rules, managing, 154-155
sensor licensing, managing, 155-157
user accounts, managing, 151-153
uses of, 119

Cisco IPS Sensor software, IPv6 support, 182-183
Cisco Learning Network, 587-588
Cisco Malware Research Lab, 46
Cisco Security IntelliShield Alert Manager Service, 47-48
Cisco Security Management Suite, 425
Cisco Security Manager 4.1, 427
Cisco Security MARS (Monitoring, Analysis, and Response System), 43-44, 425
and CSM cross-launch capability, 435-436
event feed verification, 434
integration, configuring, 431-432
Cisco SIO (Security Intelligence Operations), 45-47
Cisco Threat Operations Center, 45-46
Cisco.com Design Zone for Security, 81, 107
class-map command, 98
CollaborationApp, 40
command and control access, configuring IDSM-2 module, 568
commands
case sensitivity, 117
class-map, 98
CLI history, recalling, 116
exit command, 120
ips command, 99
policy-map command, 98-99
show events alert, 195-196
show version, 164
syntax, 101-108
comparing
AIP SSM and SSC, 510
Cisco IME and Cisco IDM, 365-366
IDSM-2 module and IPS 4200 Series, 558-559
IPSs and IDSs, 8-9
components of anomaly-based detection, 260-262
histograms, 261
learning, 261-262
zones, 261
configuring
actions, overrides, 223-226
AIP SSM, 520-523
alerts, verbose alerts, 319-322
anomaly-based detection, 262-271
CDP policies, 134
global correlation, 351-353
IDM, 126-130
IDSM-2 module, command and control access, 568
inline VLAN group mode, 133-134
interface modes
  inline interface pair mode, 133
  inline VLAN pair mode, 133
IP logging, 214-218
notifications in Cisco IME, 418-420
packet capture, 214-218
promiscuous mode
  IP fragment reassembly, 179
  TCP stream reassembly, 180
remote blocking, 208-214
reports in Cisco IME, 416-417
sensors
data and time, 147-149
interface modes, 130-136
network settings, 146-147
reboots, 150
software bypass,
  135-136, 183-184
TCP session tracking, 181
traffic flow notification, 134-135
signatures
  actions, 201-206
  detective actions, 201-202
  preventive actions, 202-205
  properties, 197-200
  SNMP traps, 202
traffic flow notification, 492-493
traffic normalization, 177-178
virtual sensors, 471-473
vs0, 176-177
console sessions, starting
  AIP SSM, 114-115
  IDSM-2 module, 115
  NME-IPS, 115-116
creating
custom signatures, 283-284
   with Custom Signature Wizard, 285-305
   without Custom Signature Wizard, 306-308
filters in Cisco IME, 398-400
reports in Cisco IME, 415-417
cross-launch capability, CSM and MARS, 435-436
CSA (Cisco Security Agent), 17-18
CSM (Cisco Security Manager), 43, 425-430
device management, 428-429
features, 426-427
and MARS cross-launch capability, 435-436
sensors, adding, 429-430
Custom Signature Wizard, 127
custom signatures, creating, 285-305
custom signatures, 192, 283-308
creating, 283-284
   with Custom Signature Wizard, 285-305
   without Custom Signature Wizard, 306-308
matching criteria, selecting, 284
regular expressions, 284-285
customizing
Cisco IME user interface, 376-378
Event Monitoring views, 395-397
Event Monitoring views (Cisco IME), 393
IDM home page, 128
dashboard
   Cisco IME, 378-380
   IDM, adding gadgets, 129
data centers, sensor placement, 78-79
date and time, sensor configuration, 147-149
deep-packet inspection, 11
default sensor settings, restoring, 138
default signatures, 192
default virtual sensor
   normalizer mode, configuring, 177-178
   TCP session tracking, configuring, 181
   traffic sources, assigning, 176-177
defense in-depth
   IPSs, 8
   systems approach to security, 20
deleting events in Cisco IME, 400-401
denied attackers, managing, 205
deobfuscation, 335
deploying sensors
   AIP SSM/SSC, 512
   inline analysis mode, 105-107
   inline interface pair mode, 100-102
   inline VLAN group mode, 103-105
   performance considerations, 71-72
   prevention versus detection mode considerations, 70-71
   in promiscuous mode, 90-100
   security considerations, 70
   virtualization requirements, 72
detecting sensor performance issues, 492
detective actions, implementation guidelines, 205
disabling signatures, 200
displaying sensors, 163-165
DLP (Data Loss Prevention), 19
DMZ (demilitarized zone), 73
“Do I Know This Already?” quizzes, answers, 595-606
downloading
   IP logs, 218
   practice exam, 586-587
dropped packets, checking for, 495-496
dynamic alarm summarization, 244-245
dynamic updates, SIO, 46

E

editing
   signature properties, 331
   virtual sensors, 473
editing keys (CLI), 118
enabling signatures, 200
encryption, 20
   as evasion technique, 58
endpoint security controls, 16-20
   antimalware agents, 18-19
   cryptographic data protection, 19-20
   CSA, 17-18
   DLP, 19
   host-based firewalls, 17
   Kernel mode, 16
   SSRM, 17
enterprise or provider Internet edge, sensor placement, 73-75
EtherChannel-based high-availability, 485-486
   guidelines, 486-487
evasion techniques, 57-62
   encryption and tunneling, 58
   protocol-level misinterpretation, 59-60
   resource exhaustion, 58-59
   timing attacks, 58
   traffic fragmentation, 59
   traffic substitution and insertion, 60-62
   event action filters, 226-228
   event correlation, 12, 57
   event logs
      alerts, examining, 229-232
      viewing, 150-151
   Event Monitoring views, 391-393
      custom signatures, 395-397
      customizing, 393
      settings, 393-395
   Event Store, 39
   events, 164-165
      acting on with Cisco IME, 405-407
      archiving, 408-409
      CIDEE, 41
      deleting, 400-401
      exporting from Cisco IME, 408-409
      importing to Cisco IME, 408-409
      investigating with Cisco IME, 401-404
      managing with Cisco IME, 391-401
      Event Monitoring views, 391-393
      saving, 400-401
      viewing in IDM, 232-233
   exam, test prerequisites, 114-121
   examining alerts in event logs, 229-232
   executable code, 11
   exit command, 120
   exploits, 11
   exporting events from Cisco IME, 408-409

F

failures, handling, 483-484
false negatives
   identifying, 313
   reducing, 329-336
false positives, 10, 71
  identifying, 313
  reducing, 314-328
features
  of Cisco IPS Sensor CLI, 116-118
  of CSM (Cisco Security Manager), 426-427
  of IDSM-2, 557-558
  of IPSs, 13
fields, show events alert command, 195-196
filename structure, signatures, 160
filters
  Cisco IME, creating, 398-400
  event action filters, 226-228
  reputation-based filters, 351
fingerprinting operating systems, 346-350
firewalls
  host-based, 17
  packet filtering, 17
  socket filtering, 17
FLOOD signature engines, deploying, 249
flow-based signatures, 12
FSPAN (Flow-Based SPAN), 94

G

gadgets
  adding to Cisco IME, 380-382
  adding to IDM dashboard, 129
  performance-related, inspecting, 493-494
global configuration mode (CLI), 121
  global correlation, configuring, 351-353

H

handling sensor failure, 483-484
hardware, troubleshooting sensors, 138
health of sensors, monitoring, 165-167
heap overflow attacks, 16
heartbeat operation (AIM-IPS), 547-548
high availability
  Cisco ASA-based, 489-490
  EtherChannel-based, 485-486
    guidelines, 486-487
  routing-based, 488-489
  sensor failure, handling, 483-484
  software bypass, 483
  STP-based, 487-488
  switching-based, 484-488
HIPS (host intrusion prevention system), 16-20
  antimalware agents, 18-19
  cryptographic data protection, 19-20
  CSA, 17-18
  DLP, 19
  host-based firewalls, 17
  Kernel mode, 16
histograms, 261
HMAC (Hash Message Authentication Code), 19
home page (IDM), customizing, 128
home pages
  SIAM, 451
  SIO, 443
  host-based firewalls, 17
hubs, IPS promiscuous mode deployment, 90-91
IDAPI (Intrusion Detection Application Programming Interface), 38

identifying
false negatives, 313
false positives, 313

IDM (Cisco IPS Device Manager), 42
Cisco IPS Sensor software, recovering, 157-159
configuring, 126-130
data and time
  sensor configuration, 147-149
  event log, viewing, 150-151
  events, viewing, 232-233
  home page, customizing, 128
  network settings, configuring, 146-147
  remote management access rules, managing, 154-155
  sensor licensing, managing, 155-157
  sensor reboots, configuring, 150
  sensors
    health, monitoring, 165-167
    interfaces, configuring, 130-136
  signatures, updating, 160-162
  system passwords, recovering, 162-163

IDSM-2 module, 35
application partition, upgrading, 572-576
command and control access, configuring, 568
comparing promiscuous and inline mode, 560
console session, starting, 115
features, 557-558
initializing, 562-568
inline mode, 560
installing, 562-564
and IPS 4200 Series, 558-559
maintaining, 572-577
maintenance partition, re-imaging, 577
passwords, recovering, 577-578
ports, 558
promiscuous mode, 561-562
recovery procedure, 572
redirecting traffic to, 568-572
troubleshooting, 577-578
upgrading, 572

IDSs (intrusion detection systems)
alerts, 8-9
anomaly-based detection, 259-274
  configuring, 262-271
  histograms, 261
  learning, 261-262
  troubleshooting, 274
  verifying, 271-274
  worms, 259-260
  zones, 261
attacks detected by, 8
comparing with IPSs, 8-9

IME (Cisco IPS Manager Express), 42
implementing
detective actions, 205
preventive actions, 206
importing events from Cisco IME, 408-409

inbox (SIAM), 455-456
increasing performance
  with load sharing, 497-498
  with traffic reduction, 498-499
indicator lights
  Cisco IPS 4240 sensors, 28
  Cisco IPS 4255 sensors, 29
  Cisco IPS 4260 sensors, 30
  Cisco IPS 4270 sensors, 32
initial sensor configuration,
troubleshooting, 136-137
initializing
  AIP SSM, 512-520
  Cisco IPS NME, 543-546
  IDSM-2 module, 562-568
  IPS AIM, 543-546
  sensors, 123-126
inline analysis mode, sensor deployment, 105-107
inline interface pair mode
  configuring, 133
  sensor deployment, 100-102
inline mode, 12
inline operation
  AIP SSM, 510
  Cisco IPS NME, 540
  IDSM-2, 560
inline traffic normalization, 177-178
inline VLAN group mode
  configuring, 133-134
  sensor deployment, 103-105
inline VLAN pair mode
  configuring, 133
  sensor deployment, 102
insertion attacks, 60
inspecting performance-related gadgets, 493-494
installing
  Cisco IME, 366-368
  IDSM-2 module, 562-564
  Pearson IT Certification Practice Test Engine, 586
integrating Cisco IME with Cisco IPS sensors, 370-374
integration, configuring with Cisco Security MARS, 431-432
integrity checking, 19
IntelliShield, 46
  Cisco Security IntelliShield Alert Manager Service, 47-48
interface modes (CLI), 119-122
  global configuration mode, 121
  privileged EXEC mode, 120
  service mode, 122
  service signature definition mode, 122
interfaces
  Cisco IPS 4240 sensors, 29
  Cisco IPS 4255 sensors, 30
investigating events with Cisco IME, 401-404
IP fragment reassembly, configuring, 179
IP logging, configuring, 214-218
ips command, 99
IPS Signatures page (SIAM), 454
IPS Threat Defense Bulletin, 448-449
IPSs (intrusion prevention systems), 8, 12-14
  alerts, 8-9
  Cisco IPS software architecture, 38-41
    CollaborationApp, 40
    MainApp, 39-40
    SensorApp, 39
  Cisco NME-IPS, 36-37
  comparing with IDSs, 8-9
evasion techniques, 57-62
  encryption and tunneling, 58
  protocol-level misinterpretation, 59-60
  resource exhaustion, 58-59
timing attacks, 58
traffic fragmentation, 59
traffic substitution and insertion, 60-62
features, 13
HIPS, 16-20
  antimalware agents, 18-19
cryptographic data protection, 19-20
IPv6 support in Cisco IPS sensors, 182-183

ISRD (Infrastructure Security Research & Development), 46

J-K-L

Kernel mode, 16

layers of OSI model, anomalies detected by IDSs, 8

learning, 261-262

licensing of sensors, managing, 155-157

limitations

of IPSs, 14

of packet correlation, 55

of sensor virtualization, 470

load sharing, increasing performance with, 497-498

M

MainApp, 39-40

maintaining IDSM-2 module, 572-577

maintenance partition (IDSM-2), re-imaging, 577

malware

antimalware agents, 18-19

Cisco Malware Research Lab, 46

worms, 259-260

managing

denied attackers, 205

events with Cisco IME, 391-401

   Event Monitoring views, 391-393

sensors

   authentication, 153-154

   licensing, 155-157

   remote management access rules, 154-155

   user accounts, 151-153
matching criteria, selecting for custom signatures, 284
memory, IPSs, 13
META signature engine, deploying, 251-252
metacharacters, 284
meta-event generator, 12
modules, accessing CLI, 114-116
monitoring sensors, health, 165-167

N

network analysis methods
  event correlation, 57
  packet content matching, 56
  packet header matching, 56
  protocol decoding, 55
  rate analysis, 55-56
  stateful content matching, 54
  statistical modeling, 57
  traffic correlation, 55

network intrusion prevention approaches
  anomaly-based, 15
  policy-based, 15
  signature-based, 14-15

network settings, configuring with IDM, 146-147

NICs (network interface cards)
  2SX interface card, 34
  4GE bypass interface card, 33
  10GE interface card, 33
  for IPSs, 13

NME-IPS, starting console session, 115-116

normalizer mode, configuring, 177-178
NORMALIZER signature engine, deploying, 252

notifications
  in Cisco IME, 418-420
  SIAM, 459-460

NTP (Network Time Protocol), configuring sensor data and time, 147-149

O

obfuscation, 335
online security resources, 47
operating systems
  fingerprinting, 346-350
  HIPS, 16-20
    CSA, 17-18
    SSRM, 17
OSI (Open Systems Interconnection) layers
  application-layer decoding, 335
  IDSs, anomalies detected by, 8

P

packet capture, configuring, 214-218
packet content matching, 56
packet filtering, 17
packet flow through Cisco IPS sensors, 40
packet header matching, 56
parameters
  for signatures
    Summary Key, 244
parameters for signatures, 242-243
passive OS fingerprinting, enabling, 347
password-guessing tools, 11
passwords, recovering, 162-163
Pearson IT Certification Practice Test Engine, installing, 586
performance

dropped packets, checking for, 495-496
increasing
  *with load sharing*, 497-498
  *with traffic reduction*, 498-499

sensors, 491
  *deployment considerations*, 71-72
  *issues, detecting*, 492
  *traffic flow notification, configuring*, 492-493
  *tuning*, 374-376

SPAN sessions, scaling, 496

physical dimensions
  *of Cisco IPS 4240 sensors*, 29
  *of Cisco IPS 4255 sensors*, 30
  *of Cisco IPS 4260 sensors*, 31-32
  *of Cisco IPS 4270 sensors*, 33

PID (product identifier), 164

placement of sensors
  *centralized campus*, 79-81
  *data centers*, 78-79
  *enterprise or provider Internet edge*, 73-75
  *WANs*, 75-77

policy-based intrusion prevention, 15

ports, IDSM-2 module, 558

post-block ACLs, 207

practice exam, downloading, 586-587

pre-block ACLs, 207

preferences, SIAM, 461

Premium Edition eBook and Practice Test, 587

preparing for exam
  *Cisco Learning Network*, 587-588
  *memory tables*, 588
  *Pearson IT Certification Practice Test Engine*, 585-587

suggested final review plan, 588-591

prerequisites for 624-627 IPV v7.0 exam, 114-121

preventive actions
  *configuring*, 202-205
  *implementation guidelines*, 206

prioritizing tuning process, 314

privileged EXEC mode (CLI), 120

processors for IPSs, 13

product sets (SIAM), 456-459

promiscuous mode, 12

  *AIP SSM*, 510
  *Cisco NME-IPS*, 540
  *configuring*, 132
  *IDSM-2 module*, 561-562
  *sensor deployment*, 90-100
    *ASA selective capture*, 98-99
    *hubs*, 90-91
    *SPAN*, 91-94
    *VACL capture*, 95-98

traffic reassembly options
  *IP fragment reassembly, configuring*, 179
  *TCP stream reassembly, configuring*, 180

properties of signatures, 192
  *configuring*, 197-200
  *editing*, 331

protocol decoding, 55

protocol-level misinterpretation, 59-60

provider Internet edge, sensor placement, 73-75

PSIRT (Cisco Products Security Incident Response Team), 46
Q-R

rate analysis, 55-56
reassembly options (promiscuous mode)
  IP fragment reassembly, configuring, 179
  TCP stream reassembly, configuring, 180
rebooting AIM-IPS, 548-549
reboots (sensor), configuring, 150
recalling CLI command history, 116
recovering
  Cisco IPS Sensor software, 157-159
  system passwords, 162-163
redirecting traffic to IDSM-2 module, 568-572
reducing
  false negatives, 329-336
  false positives, 314-328
regular expressions, 284-285
re-imaging the maintenance partition (IDSM-2), 577
remote blocking
  ACLs, 207
  configuring, 208-214
remote management access rules, managing, 154-155
reports
  configuring in Cisco IME, 416-417
  creating in Cisco IME, 415-417
  SIAM, 460
reputation-based filters, 351
resource exhaustion as evasion technique, 58-59
resources
  Cisco.com Design Zone for Security, 107
  for IPS design and implementation, 81
Resources section (SIO), 446-448
restoring sensor default settings, 138
retiring signatures, 197, 200-201
risks, 11
RMS (Remote Management Services), 46
routing-based sensor high availability, 488-489
RR (risk rating), 11
  calculating, 219-221, 341-342
    ARR, 345
    TVRs, 343-345
  system components, 220
  variables, 220-221
RSPAN (Remote SPAN), 93
RSS feeds for Cisco IME, 382-385

S

saving
  events in Cisco IME, 400-401
  IP logs, 218
scaling SPAN sessions, 496
scanning worms, 259-260
security
  sensor deployment considerations, 70
  systems approach to, 20
Security Alerts section (SIO), 444
selecting
  action configuration strategy, 228-229
  matching criteria for custom signatures, 284
SensorApp, 39
sensors, 13
  adding
    to Cisco Security MARS, 432-434
    to CSM, 429-430
  advanced setup, 126
  aggressive responses, removing, 317-319
  alerts, 193-197
authentication, managing, 153-154
Cisco AIM-IPS sensor, 36-37
Cisco IPS 4200 Series sensors, 27-28
Cisco IPS 4240 sensors, 28-29
Cisco IPS 4255 sensors, 29-30
Cisco IPS 4260 sensors, 30-32
Cisco IPS 4270 sensors, 32-34
Cisco IPS software architecture, 38-41
CollaborationApp, 40
MainApp, 39-40
SensorApp, 39
data and time
configuring, 147-149
default settings, restoring, 138
deployment considerations
performance, 71-72
prevention versus detection mode, 70-71
security, 70
virtualization requirements, 72
displaying, 163-165
event log, viewing, 150-151
failures, handling, 483-484
hardware
troubleshooting, 138
health, monitoring, 165-167
high availability
Cisco ASA-based, 489-490
EtherChannel-based, 485-486
routing-based, 488-489
STP-based, 487-488
switching-based, 484-488
initial configuration, troubleshooting, 136-137
initializing, 123-126
inline analysis mode, 105-107
inline interface pair mode, 100-102
inline VLAN group mode, 103-105
inline VLAN pair mode, 102
integrating with Cisco IME, 370-374
IP logging, configuring, 214-218
IPv6 support, 182-183
licensing, managing, 155-157
network analysis methods
event correlation, 57
packet content matching, 56
packet header matching, 56
protocol decoding, 55
rate analysis, 55-56
stateful content matching, 54
statistical modeling, 57
traffic correlation, 55
network settings, configuring, 146-147
packet capture, configuring, 214-218
packet flow, 40
performance
issues, detecting, 492
traffic flow notification, configuring, 492-493
placement
centralized campus, 79-81
data centers, 78-79
enterprise or provider Internet edge, 73-75
WANs, 75-77
promiscuous mode, 90-100
ASA selective capture, 98-99
hubs, 90-91
SPAN, 91-94
VACL capture, 95-98
reasons for adding to IPS, 13
reboots, configuring, 150
SensorApp, 39
signature engines, 193
signatures
activating, 200-201
custom signatures, 283-308
disabling, 200
enabling, 200
filename structure, 160
parameters, 242-243
properties, 192
properties, configuring, 197-200
remote blocking, configuring, 208-214
retiring, 197, 200-201
trigger counting, 243-244
updating, 160-162
software bypass, configuring, 135-136, 183-184
TCP session tracking
configuring, 181
traffic flow notification, configuring, 134-135
troubleshooting, 163-165
tuning, 314, 374-376
false negatives, reducing, 329-336
false positives, reducing, 314-328
user accounts, managing, 151-153
vs0, assigning traffic sources, 176-177
service mode (CLI), 122
service signature definition mode (CLI), 122
SERVICE signature engines, deploying, 247-248
severity levels of alerts, 194-196
SFR (Signature Fidelity Rating), 342-343
show events alert command, 195-196
show version command, 164
SIAM (Cisco Security IntelliShield Alert Manager) Service, 449-461
Alerts page, 452-453
inbox, 455-456
notifications, 459-460
preferences, 461
product sets, 456-459
reports, 460
signature engines, 12, 193, 239
AIC engines, deploying, 253
ATOMIC signature engines, deploying, 245-246
FLOOD signature engines, deploying, 249
META signature engines, deploying, 251-252
NORMALIZER signature engine, deploying, 252
SERVICE signature engines, deploying, 247-248
STRING signature engines, deploying, 246-247
SWEET signature engines, deploying, 250
signature-based intrusion prevention, 14-15
signatures, 12, 192-233
actions
configuring, 201-206
overrides, configuring, 223-226
activating, 200-201
alerts, 193-197
anomaly-based, 12
atomic, 12
behavior-based, 12
blocking, configuring, 208-214
Custom Signature Wizard, 127
custom signatures, 283-308
creating, 283-284
denied attackers, managing, 205
detective actions
configuring, 201-202
implementing, 205
disabling, 200
enabling, 200
filename structure, 160
flow-based, 12
malware, 18-19
parameters, 242-243
  Summary Key, 244
preventive actions
    configuring, 202-205
    implementing, 206
properties, 192
    configuring, 197-200
    editing, 331
remote blocking, ACLs, 207
retiring, 197, 200-201
RR
    calculating, 219-221
    system components, 220
SNMP traps, configuring, 202
threat rating, 221-222
trigger counting, 243-244
tuning, 327-328, 330-331
updating, 160-162
SIO (Cisco Security Intelligence Operations), 45-47, 443-449
dynamic updates, 46
IPS Signatures page, 454
IPS Threat Defense Bulletin, 448-449
online security resources, 47
Products and Services Updates section, 448
Resources section, 446-448
Security Alerts section, 444
Virus Watch section, 445
SNMP (Simple Network Management Protocol), 166
  traps, configuring, 202
socket filtering, 17
software
  Cisco IPS Sensor software, recovering, 157-159
  Cisco IPS software architecture, 38-41
    CollaborationApp, 40
    MainApp, 39-40
    SensorApp, 39
software bypass, 483
  configuring, 135-136, 183-184
SPAN (Switched Port Analyzer)
  IPS promiscuous mode deployment, 91-94
  sessions, scaling, 496
SSCs (Security Services Cards), AIP
  SSC-5, 34-35
SSH (Secure Shell), accessing CLI,
  114-116
SSMs (Security Services Modules),
  34-35
  AIP SSM, 34-35, 508-509
    initializing, 512-520
SSRM (Secondary Security Reference Monitor), 17
standalone performance sensor
  characteristics, 491
starting console sessions
  for AIP SSM, 114-115
  for IDSM-2 module, 115
  for NME-IPS, 115-116
STAT (Strategic Assessment Technology Team), 46
stateful content matching, 54
statistical modeling, 57
stopping IP logs, 218
STP-based high availability, 487-488
STRING signature engines, deploying, 246-247
subscription-based service, IntelliShield Alert Manager Service, 461
suggested final review plan, 588-591
summarization
  alarm summarization, 244
dynamic alarm summarization, 244-245
Summary Key parameter, 244
SWEEP signature engines, deploying, 250
switching-based high availability, 484-488
  inline mode redundant IPS sensor deployment, 486
  promiscuous mode redundant IPS sensor deployment, 486
syntax, commands, 101-108
system passwords, recovering, 162-163
systems approach to security, 20

T

tab completion (CLI), 116
taps, IPS promiscuous mode deployment, 90-91
TCP session tracking, configuring, 181
TCP stream reassembly, configuring, 180
Telnet, accessing CLI, 114-116
threat rating, 221-222
threats, 11
  Cisco Threat Operations Center, 45-46
time zones, sensor configuration, 147-149
timing attacks as evasion technique, 58
topics, 624-627 IPS v7.0 exam, 121-153
traffic correlation, 55
traffic flow notification
  configuring, 134-135, 492-493
traffic fragmentation as evasion technique, 59
traffic normaliza-tion
  configuring, 177-178
tuning, 334
traffic reduction, increasing performance with, 498-499
traffic substitution and insertion, 60-62
Trend Micro, 160
trigger counting, 243-244
troubleshooting
  AIM-IPS, 547-550
  AIP SSM, 530-531
  anomaly-based detection, 274
  IDSM-2 module, 577-578
  initial sensor configuration, 136-137
  sensors, 163-165
    hardware, 138
true negatives, 10
true positives, 9
tuned signatures, 192
tuning
  sensors, 314, 374-376
    false negatives, reducing, 329-336
    false positives, reducing, 314-328
  signatures, 327-328
  traffic normalization, 334
tunneling as evasion technique, 58
TVRs (Target Value Ratings), 343-345

U

UDI (Unique Device Identifier), 163
Unicode deobfuscation, 60-61
updating
  exam updates, 609-610
  signatures, 160-162
upgrading ISDM-2, 572
user accounts (sensors), managing, 151-153
user interactive prompts (CLI), 116
user interface (Cisco IME)
    customizing, 376-378
dashboards, 378-380
    gadgets, adding, 380-382

V

VACL capture, IPS promiscuous mode
deployment, 95-98
variables for RR, 220-221
verbose alerts, configuring, 319-322
verifying
    anomaly-based detection, 271-274
    virtual sensor operation, 475-477
VID (version identifier), 164
viewing
    events in IDM, 232-233
    RSS feeds in Cisco IME, 383
    sensor event log, 150-151
virtual IPS, 469-470
virtual sensors, 469
    adding, 470-471
    editing, 473
    verifying operation, 475-477
virtualization requirements, sensors, 72
Virus Watch section (SIO), 445
vs0
    normalizer mode, configuring, 177-178
    TCP session tracking, configuring, 181
    traffic sources, assigning, 176-177
vulnerabilities, 11

W

WANs, sensor placement, 75-77
watch list rating, 346
wizards (IDM), Custom Signature
    Wizard, 127
    custom signatures, creating, 285-305
worms, 259-260

X-Y-Z

zones, 261