CISCO.

Official
Cert Guide

Learn, prepare, and practice for exam success

CCNP Security IPS 642-627

- Master **CCNP Security IPS 642-627** exam topics with the official study guides
- Assess your knowledge with **chapter-opening quizzes**
- Review key concepts with **exam preparation tasks**
- Practice with **realistic exam questions** on the CD-ROMs

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

Cisco Press

800 East 96th Street
Indianapolis, IN 46240

CCNP Security IPS 642-627 Official Cert Guide

David Burns

Odunayo Adesina, CCIE No. 26695

Keith Barker, CCIE No. 6783

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

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.

ISBN-13: 978-1-58714-255-0

ISBN-10: 1-58714-255-4

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.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: International Sales international@pearsoned.com

Trademark Acknowledgments

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Kimberley Debus

Senior Project Editor: Tonya Simpson

Copy Editor: John Edwards

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editor: Brandon Anastasoff

Proofreader: Sarah Kearns

Indexer: Tim Wright

Compositor: Mark Shirar

Book Designer: Gary Adair

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.

About the Technical Editor

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

Contents

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*

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

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)

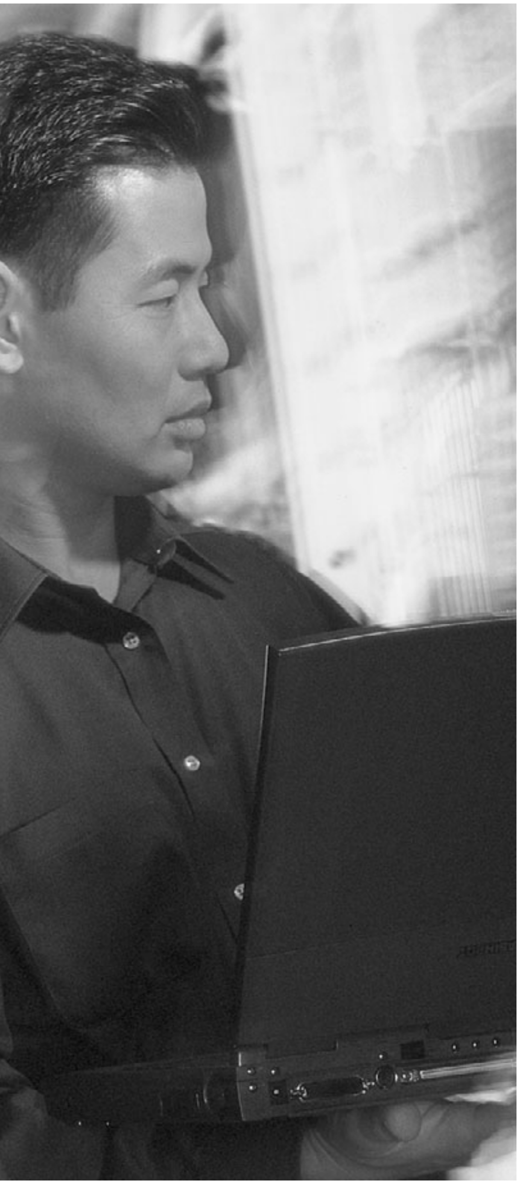
Part I: Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices

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.

CHAPTER 1

Intrusion Prevention and Intrusion Detection Systems

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 1-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions
Intrusion Prevention Terminology	1, 2
Intrusion Detection Versus Intrusion Prevention Systems	3
Intrusion Prevention Approaches	4, 5
Endpoint Security Controls	6–9
A Systems Approach to Security	10

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

Foundation Topics

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

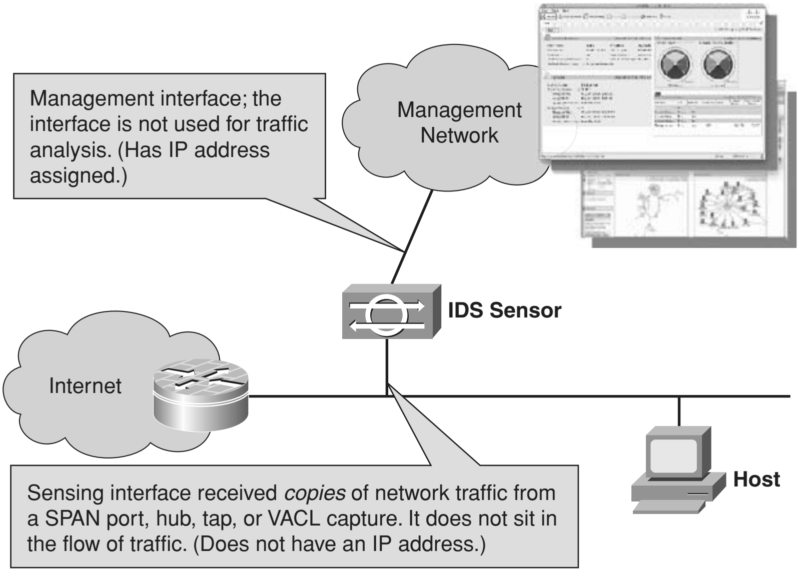

Management interface; the interface is not used for traffic analysis. (Has IP address assigned.)
Management Network
IDS Sensor
Internet
Host
Sensing interface received *copies* of network traffic from a SPAN port, hub, tap, or VACL capture. It does not sit in the flow of traffic. (Does not have an IP address.)

Figure 1-1 *Intrusion Detection System*

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.

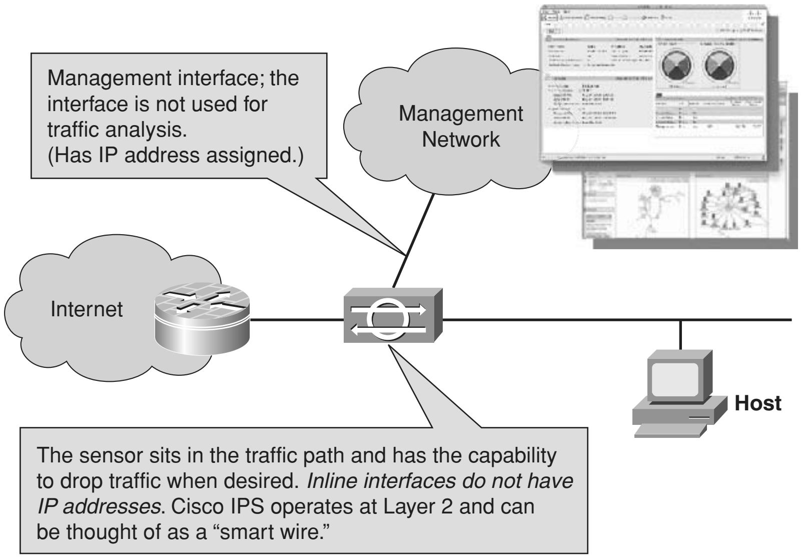
Intrusion Prevention Terminology

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.

Key Topic



Management interface; the interface is not used for traffic analysis. (Has IP address assigned.)
Management Network
Internet
Host
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.

Key Topic

Table 1-2 *Signature-Based Features and Limitations*

Category	Feature	Limitation
Complexity	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).	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.
Susceptibility and Accuracy	Relatively low false positive rate (if the IPS is properly tuned and using well-designed signatures).	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.

Table 1-2 *Signature-Based Features and Limitations*

Category	Feature	Limitation
Reporting	Ability to name attacks and provide the administrator with additional information about a specific attack.	—

- **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 1-3 *Anomaly-Based Features and Limitations*

Key Topic

Features	Limitations
Ability to act on both known and yet-unknown threats.	More susceptible to evasion through complex signatures that are designed to evade an anomaly-based IPS.
	Unable to name individual attacks.
	Statistical approach requires a learning period to establish a normal network profile.
	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.

- **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 1-4 *Policy-Based Features and Limitations*

Key Topic

Features	Limitations
Very focused on the target environment and triggers very few false positives; thus, very accurate and effective in most cases.	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.
Ability to act on both known and yet-unknown threats.	Unable to name individual attacks.

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.

Key Topic

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

Features	Limitations
Identity association, meaning that the endpoint security control can provide the information about the attacker.	Platform flexibility (some operating systems might not support endpoint security controls).
System-specific or customized to protect the system it is protecting and resides on.	Inability to correlate whether a single endpoint or agent is deployed.

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

Features	Limitations
Ability to see malicious network data; consequences of network attacks even if encrypted.	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.
Detection of the success of an attack and can take action after the system is stable.	If an attack is successful in accessing the host prior to the endpoint security reacting, the host is compromised.

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 of 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 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.

Key Topic

Table 1-6 *Host IPS (HIPS) and Network IPS (NIPS)*

Host IPS	Network IPS
CSA can inspect the behavior of applications (encrypted or nonencrypted).	Requires constant updates for new vulnerabilities.
CSA is a behavior-based HIPS.	Can prevent known attacks.
CSA does not need constant updates.	Can protect complete network.
CSA can protect the host (server, desktop, and so on) efficiently, communicate with IPSs, and stop known and unknown (Day Zero) attacks.	—
CSA cannot "name" the attack or protect unsupported platforms.	—

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.

Key Topic

Table 1-7 *Defense-in-Depth: Host-Focused and Network-Focused Technology*

Host-Focused Technology	Network-Focused Technology
Protects the operating system	Detects and prevents DoS attacks
Controls access to local host resources	Detects and prevents network reconnaissance attacks
Protects applications and the data they handle	Detects and prevents attacks against many network-facing applications and operating systems

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*

Key Topic

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

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

Index