cisco

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA Security 210-260

OMAR SANTOS, CISSP NO. 463598
JOHN STUPPI, CCIE NO. 11154

ciscopress.com

CCNA Security 210-260 **Official** Cert Guide

OMAR SANTOS, CISSP 463598
JOHN STUPPI, CCIE NO. 11154

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Security 210-260
Official Cert Guide

Omar Santos

John Stuppi

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

Printed in the United States of America

First Printing June 2015

Library of Congress Control Number: 2015938283

ISBN-13: 978-1-58720-566-8

ISBN-10: 1-58720-566-1

Warning and Disclaimer

This book is designed to provide information about the CCNA Security Implementing Cisco Network Security (IINS) 210-260 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.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Acquisitions Editor: Denise Lincoln

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Senior Project Editor: Tonya Simpson

Copy Editor: Keith Cline

Technical Editors: Scott Bradley, Panos Kampanakis

Editorial Assistant: Vanessa Evans

Cover Designer: Mark Shirar

Composition: Bronkella Publishing

Indexer: Erika Millen

Proofreader: Chuck Hutchinson

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

About the Authors

Omar Santos is the technical leader for the Cisco Product Security Incident Response Team (PSIRT). He mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities in all Cisco products. Omar has been working with information technology and cybersecurity since the mid-1990s. Omar has designed, implemented, and supported numerous secure networks for Fortune 100 and 500 companies and for the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations.

Omar is an active member of the security community, where he leads several industry-wide initiatives and standards bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of several books and numerous white papers, articles, and security configuration guidelines and best practices. Omar has also delivered numerous technical presentations at many conferences and to Cisco customers and partners, in addition to many C-level executive presentations to many organizations.

John Stuppi, CCIE No. 11154 (Security), is a technical leader in the Cisco Security Solutions (CSS) organization at Cisco, where he consults Cisco customers on protecting their network against existing and emerging cybersecurity threats. In this role, John is responsible for providing effective techniques using Cisco product capabilities to provide identification and mitigation solutions for Cisco customers who are concerned with current or expected security threats to their network environments. Current projects include helping customers leverage DNS and NetFlow data to identify and subsequently mitigate network-based threats. John has presented multiple times on various network security topics at Cisco Live, Black Hat, and other customer-facing cybersecurity conferences. In addition, John contributes to the Cisco Security Portal through the publication of white papers, security blog posts, and cyber risk report articles. Before joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (#25525) and holds an Information Systems Security (INFOSEC) professional certification. In addition, John has a BSEE from Lehigh University and an MBA from Rutgers University. John lives in Ocean Township, New Jersey (a.k.a. the “Jersey Shore”) with his wife, two kids, and dog.

About the Technical Reviewers

Scott Bradley is a network engineer dedicated to customer success. He began building knowledge and experience in Cisco technology more than 15 years ago when he first started in the Technical Assistance Center (TAC). Over time, thousands of customers have been assisted by his knowledge of internetworking in routing, switching, and security, and his ability to provide network design, implementation, and troubleshooting service. Scott has enjoyed being an escalation resource to the Catalyst and Nexus switching group, a technical trainer, and an early field trial software and hardware tester.

Currently, he is an active member of the Applied Security Intelligence Team, testing security-related software and hardware and writing applied mitigation bulletins and white papers. He works closely with the Cisco Product Security Incident Response Team (PSIRT), consulting on security advisories.

Scott lives with his wife, Cathy, in Santa Cruz, California, where he enjoys gardening, hiking, and riding bicycles.

Panos Kampanakis is part of the Security Research and Operations teams at Cisco Systems, providing early-warning intelligence, threat, and vulnerability analysis and proven Cisco mitigation solutions to help protect networks. He holds a CCIE and other certifications. He has extensive experience in network and IT security and cryptography. He has written numerous research publications and security-related guides and white papers. Panos has often participated in the development and review of Cisco certification exam material. He also presents in Cisco conferences, teaching customers about security best practices, identification, and mitigation techniques. In his free time, he has a passion for basketball (and never likes to lose).

Dedications

From Omar

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

I also dedicate this book to my father, Jose; and in memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

From John

I would like to dedicate this book to my wife, Diane, and my two wonderful children, Tommy and Allison, who have had to put up with more (than usual!) late night and weekend hours with me on my laptop during the development of this book.

I also want to dedicate this book as a thank you to those friends and family who provided inspiration and support through their genuine interest in the progress of the book.

Finally, I want to thank Omar for convincing me to help him as a co-author on this book. Although the process was arduous at times, it was a blessing to be able to work together on this effort with someone as dedicated, intelligent, and motivated as Omar.

Acknowledgments

We would like to thank the technical editors, Scott Bradley and Panos Kampanakis, for their time and technical expertise. They verified our work and contributed to the success of this book.

We would like to thank the Cisco Press team, especially Denise Lincoln and Christopher Cleveland, for their patience, guidance, and consideration. Their efforts are greatly appreciated.

Finally, we would like to acknowledge the Cisco Security Research and Operations teams. Several leaders in the network security industry work there, supporting our Cisco customers under often very stressful conditions and working miracles daily. They are truly unsung heroes, and we are all honored to have had the privilege of working side by side with them in the trenches when protecting customers and Cisco.

Contents at a Glance

Contents

On the CD

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

Congratulations! If you are reading this, you have in your possession a powerful tool that can help you to

- Improve your awareness and knowledge of network security
- Increase your skill level related to the implementation of that security
- Prepare for the CCNA Security certification exam

When writing this book, we did so with you in mind, and together we will discover the critical ingredients that make up the recipe for a secure network and work through examples of how to implement these features. By focusing on both covering the objectives for the CCNA Security exam and integrating that with real-world best practices and examples, we created this content with the intention of being your personal tour guides as we take you on a journey through the world of network security.

The CCNA Security Implementing Cisco Network Security (IINS) 210-260 exam is required for the CCNA Security certification. The prerequisite for CCNA Security is the CCNA Route/Switch certification (or any CCIE certification). The CCNA Security exam tests your knowledge of securing Cisco routers and switches and their associated networks, and this book prepares you for that exam. This book covers all the topics listed in Cisco's exam blueprint, and each chapter includes key topics and preparation tasks to assist you in mastering this information. The CD that accompanies this book also includes bonus videos to assist you in your journey toward becoming a CCNA in Security. Of course, the CD included with the printed book also includes several practice questions to help you prepare for the exam.

About the CCNA Security Implementing Cisco Network Security (IINS) 210-260 Exam

Cisco's objective of the CCNA Security exam is to verify the candidate's understanding, implementation, and verification of security best practices on Cisco hardware and software. The focus points for the exam (which this book prepares you for) are as follows:

- **Cisco routers and switches**
  - Common threats, including blended threats, and how to mitigate them
  - The lifecycle approach for a security policy
  - Understanding and implementing network foundation protection for the control, data, and management planes
  - Understanding, implementing, and verifying *AAA (authentication, authorization, and accounting)*, including the details of TACACS+ and RADIUS
  - Understanding and implementing basic rules inside of Cisco *Access Control Server (ACS)* Version 5.x, including configuration of both ACS and a router for communications with each other

- Standard, extended, and named access control lists used for packet filtering and for the classification of traffic
- Understanding and implementing protection against Layer 2 attacks, including CAM table overflow attacks, and VLAN hopping

- **Cisco firewall technologies**
  - Understanding and describing the various methods for filtering implemented by firewalls, including stateful filtering. Compare and contrast the strengths and weaknesses of the various firewall technologies.
  - Understanding the methods that a firewall may use to implement *Network Address Translation (NAT)* and *Port Address Translation (PAT)*.
  - Understanding, implementing, and interpreting a zone-based firewall policy through *Cisco Configuration Professional (CCP)*.
  - Understanding and describing the characteristics and defaults for interfaces, security levels, and traffic flows on the *Adaptive Security Appliance (ASA)*.
  - Implementing and interpreting a firewall policy on an ASA through the GUI tool named the *ASA Security Device Manager (ASDM)*.
- **Intrusion prevention systems**
  - Comparing and contrasting *intrusion prevention systems (IPS)* versus *intrusion detection systems (IDS)*, including the pros and cons of each and the methods used by these systems for identifying malicious traffic
  - Describing the concepts involved with IPS included true/false positives/negatives
  - Configuring and verifying IOS-based IPS using CCP
- **VPN technologies**
  - Understanding and describing the building blocks used for *virtual private networks (VPNs)* today, including the concepts of symmetrical, asymmetrical, encryption, hashing, *Internet Key Exchange (IKE)*, *public key infrastructure (PKI)*, authentication, Diffie-Hellman, certificate authorities, and so on
  - Implementing and verifying IPsec VPNs on IOS using CCP and the *command-line interface (CLI)*
  - Implementing and verifying *Secure Sockets Layer (SSL)* VPNs on the ASA firewall using ASDM

As you can see, it is an extensive list, but together we will not only address and learn each of these, but we will also have fun doing it.

You can take the exam at Pearson VUE testing centers. You can register with VUE at http://www.vue.com/cisco/.

CCNA Security Exam

Table I-1 lists the topics of the CCNA Security exam and indicates the parts in the book where these topics are covered.

Table I-1 *CCNA Security Exam Topics*

Exam Topic	Part
1.0 Security Concepts	
1.1 Common Security Principles	
1.1.a Describe Confidentiality, Integrity, Availability (CIA)	Chapter 1
1.1.b Describe SIEM technology	Chapter 1
1.1.c Identify common security terms	Chapter 1
1.1.d Identify common network security zones	Chapter 1
1.2 Common Security Threats	
1.2.a Identify Common network attacks	Chapter 2
1.2.b Describe Social Engineering	Chapter 2
1.2.c Identify Malware	Chapter 2
1.2.d Classify the vectors of Data Loss/Exfiltration	Chapter 2
1.3 Cryptography Concepts	
1.3.a Describe Key Exchange	Chapter 5
1.3.b Describe Hash Algorithm	Chapter 5
1.3.c Compare & Contrast Symmetric and Asymmetric Encryption	Chapter 5
1.3.d Describe Digital Signatures, Certificates and PKI	Chapter 5
1.4 Describe network topologies	
1.4.a Campus Area Network (CAN)	Chapter 1
1.4.b Cloud, Wide Area Network (WAN)	Chapter 1
1.4.c Data Center	Chapter 1
1.4.d Small office/Home office (SOHO)	Chapter 1
1.4.e Network security for a virtual environment	Chapter 1
2.0 Secure Access	
2.1 Secure management	
2.1.a Compare In-band and out of band	Chapter 11
2.1.b Configure secure network management	Chapter 11
2.1.c Configure and verify secure access through SNMP v3 using an ACL	Chapter 11
2.1.d Configure and verify security for NTP	Chapter 11
2.1.e Use SCP for file transfer	Chapter 11

Exam Topic	Part
2.2 AAA Concepts	
2.2.a Describe RADIUS & TACACS+ technologies	Chapter 3
2.2.b Configure administrative access on a Cisco router using TACACS+	Chapter 3
2.2.c Verify connectivity on a Cisco router to a TACACS+ server	Chapter 3
2.2.d Explain the integration of Active Directory with AAA	Chapter 3
2.2.e Describe Authentication & Authorization using ACS and ISE	Chapter 3
2.3. 802.1X Authentication	
2.3.a Identify the functions 802.1X components	Chapter 4
2.4. BYOD	
2.4.a Describe the BYOD architecture framework	Chapter 4
2.4.b Describe the function of Mobile Device Management (MDM)	Chapter 4
3. VPN	
3.1. VPN Concepts	
3.1.a Describe IPSec Protocols and Delivery Modes (IKE, ESP, AH, Tunnel mode, Transport mode)	Chapter 6
3.1.b Describe Hairpinning, Split Tunneling, Always-on, NAT Traversal	Chapter 6
3.2. Remote Access VPN	
3.2.a Implement basic Clientless SSL VPN using ASDM	Chapter 8
3.2.b Verify clientless connection	Chapter 8
3.2.c Implement basic AnyConnect SSL VPN using ASDM	Chapter 8
3.2.d Verify AnyConnect connection	Chapter 8
3.2.e Identify Endpoint Posture Assessment	Chapter 8
3.3 Site-to-Site VPN	
3.3.a Implement an IPSec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls	Chapter 7
3.3.b Verify an IPSec site-to-site VPN	Chapter 7
4.0. Secure Routing & Switching	
4.1 Security on Cisco Routers	
4.1.a Configure multiple privilege levels	Chapter 11
4.1.b Configure IOS Role-based CLI Access	Chapter 11
4.1.c Implement IOS Resilient Configuration	Chapter 11

Exam Topic	Part
4.2 Securing Routing Protocols	
4.2.a Implement routing update authentication on OSPF	Chapter 13
4.3 Securing the Control Plane	
4.3.a Explain the function of Control Plane Policing	Chapter 13
4.4 Common Layer 2 Attacks	
4.4.a Describe STP attacks	Chapter 9
4.4.b Describe ARP Spoofing	Chapter 9
4.4.c Describe MAC spoofing	Chapter 9
4.4.d Describe CAM Table (MAC Address Table) Overflows	Chapter 9
4.4.e Describe CDP/LLDP Reconnaissance	Chapter 9
4.4.f Describe VLAN Hopping	Chapter 9
4.4.g Describe DHCP Spoofing	Chapter 9
4.5 Mitigation Procedures	
4.5.a Implement DHCP Snooping	Chapter 9
4.5.b Implement Dynamic ARP Inspection	Chapter 9
4.5.c Implement Port Security	Chapter 9
4.5.d Describe BPDU Guard, Root Guard, Loop Guard	Chapter 9
4.5.e Verify mitigation procedures	Chapter 9
4.6 VLAN Security	Chapter 9
4.6.a Describe the security implications of a PVLAN	Chapter 9
4.6.b Describe the security implications of a Native VLAN	Chapter 9
5.0 Cisco Firewall Technologies	**Chapter 14**
5.1 Describe operational strengths and weaknesses of the different firewall technologies	Chapter 14
5.1.a Proxy firewalls	Chapter 14
5.1.b Application firewall	Chapter 14
5.1.c Personal firewall	Chapter 14
5.2 Compare Stateful vs. Stateless Firewalls	
5.2.a Operations	Chapter 16
5.2.b Functions of the state table	Chapter 16

Exam Topic	Part
5.3 Implement NAT on Cisco ASA 9.x	
5.3.a Static	Chapter 16
5.3.b Dynamic	Chapter 16
5.3.c PAT	Chapter 16
5.3.d Policy NAT	Chapter 16
5.3 e Verify NAT operations	Chapter 16
5.4 Implement Zone Based Firewall	
5.4.a Zone to zone	Chapter 15
5.4.b Self zone	Chapter 15
5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x	
5.5.a Configure ASA Access Management	Chapter 16
5.5.b Configure Security Access Policies	Chapter 16
5.5.c Configure Cisco ASA interface security levels	Chapter 16
5.5.d Configure Default Modular Policy Framework (MPF)	Chapter 16
5.5.e Describe Modes of deployment (Routed firewall, Transparent firewall)	Chapter 16
5.5.f Describe methods of implementing High Availability	Chapter 16
5.5.g Describe Security contexts	Chapter 16
5.5.h Describe Firewall Services	Chapter 16
6.0 IPS	
6.1 Describe IPS Deployment Considerations	Chapter 17
6.1.a Network Based IPS vs. Host Based IPS	Chapter 17
6.1.b Modes of deployment (Inline, Promiscuous - SPAN, tap)	Chapter 17
6.1.c Placement (positioning of the IPS within the network)	Chapter 17
6.1.d False Positives, False Negatives, True Positives, True Negatives	Chapter 17
6.2 Describe IPS Technologies	
6.2.a Rules/Signatures	Chapter 17
6.2.b Detection/Signature Engines	Chapter 17
6.2.c Trigger Actions/Responses (drop, reset, block, alert, monitor/log, shun)	Chapter 17
6.2.d Blacklist (Static & Dynamic)	Chapter 17

Exam Topic	Part
7.0 Content and Endpoint Security	**Chapter 18**
7.1 Describe Mitigation Technology for Email-based Threats	
7.1.a SPAM Filtering, Anti-Malware Filtering, DLP, Blacklisting, Email Encryption	Chapter 18
7.2 Describe Mitigation Technology for Web-based Threats	
7.2.a Local & Cloud Based Web Proxies	Chapter 18
7.2.b Blacklisting, URL-Filtering, Malware Scanning, URL Categorization, Web Application Filtering, TLS/SSL Decryption	Chapter 18
7.3 Describe Mitigation Technology for Endpoint Threats	
7.3.a Anti-Virus/Anti-Malware	Chapter 19
7.3.b Personal Firewall/HIPS	Chapter 19
7.3.c Hardware/Software Encryption of local data	Chapter 19

About the *CCNA Security 210-260 Official Cert Guide*

This book maps to the topic areas of the CCNA Security exam and uses a number of features to help you understand the topics and prepare for your exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics for 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. This book is designed to assist you in the exam by using the following methods:

- Using a conversational style that reflects the fact that we wrote this book as if we made it just for you, as a friend, discussing the topics with you, one step at a time
- Helping you discover which exam topics you may want to invest more time studying, to really "get it"
- Providing explanations and information to fill in your knowledge gaps
- Supplying three bonus videos (on the CD) to reinforce some of the critical concepts and techniques that you have learned from in your study of this book
- Providing practice questions to assess your understanding of the topics

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 when you finish 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 icon appears 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 "define this term" type of question, the CCNA 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.
  - **Command Reference to Check Your Memory:** Review important commands covered in the chapter.
- **CD-based practice exam:** The companion CD contains an exam engine that enables you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 19 core chapters. Chapter 20 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNA Security exam. The core chapters are organized into parts. They cover the following topics:

Part I: Fundamentals of Network Security

- **Chapter 1, "Networking Security Concepts":** This chapter covers the need for and the building blocks of network and information security, threats to our networks today, and fundamental principles of secure network design.

- **Chapter 2, "Common Security Threats":** This chapter covers the current state of network security in terms of the types of threats organizations face on behalf of malicious actors. It provides coverage of different threat landscape topics and common attacks such as distributed denial-of-service (DDoS) attacks, social engineering, malware identification tools, data loss, and exfiltration.

Part II: Secure Access

- **Chapter 3, "Implementing AAA in Cisco IOS":** This chapter covers the role of Cisco Secure ACS and the Cisco Identity Services Engine (ISE), along with the two primary protocols used for authentication RADIUS and TACACS. It also covers configuration of a router to interoperate with an ACS server and configuration of the ACS server to interoperate with a router. The chapter also covers router tools to verify and troubleshoot router-to-ACS server interactions.
- **Chapter 4, "Bring Your Own Device (BYOD)":** This chapter covers different subjects focused on the topic of BYOD. It provides a description of the BYOD concept and an overview of a BYOD architecture framework. This chapter covers the fundamentals of mobile device management (MDM), its function, and the deployment options.

Part III: Virtual Private Networks (VPN)

- **Chapter 5, "Fundamentals of VPN Technology and Cryptography":** This chapter covers what VPNs are and why we use them and the basic ingredients of cryptography. This chapter also covers the concepts, components, and operations of the *public key infrastructure (PKI)* and includes an example of putting the pieces of PKI to work.
- **Chapter 6, "Fundamentals of IP Security":** This chapter covers the concepts, components, and operations of IPsec and how to configure and verify IPsec.
- **Chapter 7, "Implementing IPsec Site-to-Site VPNs":** This chapter covers planning and preparing to implement an IPsec site-to-site VPN and implementing and verifying the IPsec site-to-site VPN.
- **Chapter 8, "Implementing SSL VPNs Using Cisco ASA":** This chapter covers the functions and use of SSL for VPNs, configuring SSL clientless VPN on the ASA, and configuring the full SSL AnyConnect VPN on the ASA.

Part IV: Secure Routing and Switching

- **Chapter 9, "Securing Layer 2 Technologies":** This chapter covers VLANs and trunking fundamentals, spanning-tree fundamentals, and common Layer 2 threats and how to mitigate them.
- **Chapter 10, "Network Foundation Protection":** This chapter covers securing the network using the network foundation protection (NFP) approach, the management plane, the control plane, and the data plane.
- **Chapter 11, "Securing the Management Plane on Cisco IOS Devices":** This chapter covers management traffic and how to make it more secure and the implementation of security measures to protect the management plane.
- **Chapter 12, "Securing the Data Plane in IPv6":** This chapter covers IPv6 (basics, configuring, and developing a security plan for IPv6).

- **Chapter 13, "Securing Routing Protocols and the Control Plane":** This chapter covers different subjects focused on the control plane of the network device. It provides details on how to secure the control plane of network infrastructure devices. This chapter explains the function of control plane policing (CoPP), control plane protection (CPPr), and how to secure IP routing protocols.

Part V: Cisco Firewall Technologies and Intrusion Prevention System Technologies

- **Chapter 14, "Understanding Firewall Fundamentals":** This chapter covers firewall concepts and the technologies used by them, the function of *Network Address Translation (NAT)*, including its building blocks, and the guidelines and considerations for creating and deploying firewalls.
- **Chapter 15, "Implementing Cisco IOS Zone-Based Firewalls":** This chapter covers the operational and functional components of the IOS zone-based firewall and how to configure and verify the IOS zone-based firewall.
- **Chapter 16, "Configuring Basic Firewall Policies on Cisco ASA":** This chapter covers the *Adaptive Security Appliance (ASA)* family and features, ASA firewall fundamentals, and configuring the ASA.
- **Chapter 17, "Cisco IPS Fundamentals":** This chapter compares intrusion *prevention systems (IPS)* to *intrusion detection systems (IDS)* and covers how to identify malicious traffic on the network, manage signatures, and monitor and manage alarms and alerts.

Part VI: Content and Endpoint Security

- **Chapter 18, "Mitigation Technologies for E-Mail-Based and Web-Based Threats":** This chapter covers the different mitigation technologies for e-mail-based and web-based threats. It covers the Cisco Email Security Appliances (ESA), Cisco cloud e-mail security, Cisco Cloud Web Security (CWS), the Cisco Web Security Appliance (WSA), and the Cisco Content Security Management Appliance (SMA). Cisco has added advanced malware protection (AMP) to the ESA and WSA to enable security administrators to detect and block malware and perform continuous analysis and retrospective alerting. Both the ESA and WSA use cloud-based security intelligence to allow protection before, during, and after an attack. This chapter covers these technologies and solutions in detail. It details mitigation technologies such as spam and antimalware filtering, data loss prevention (DLP), blacklisting, e-mail encryption, and web application filtering.
- **Chapter 19, "Mitigation Technology for Endpoint Threats":** This chapter provides details of the different mitigation technologies available for endpoint threats. It covers introductory concepts of endpoint threats to advanced malware protection capabilities provided by Cisco security products. This chapter covers the different antivirus and antimalware solutions, personal firewalls and host intrusion prevention systems (HIPS), Cisco AMP for endpoints, and hardware and software encryption of endpoint data.

Part VII: Final Preparation

- **Chapter 20, "Final Preparation":** This chapter identifies tools for final exam preparation and helps you develop an effective study plan.

Appendixes

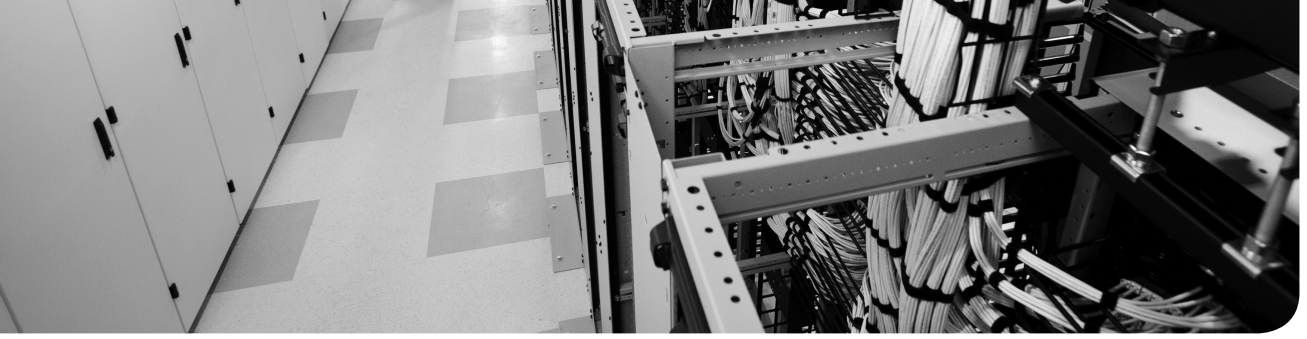
- **Appendix A, "Answers to the 'Do I Know This Already?' Quizzes":** Includes the answers to all the questions from Chapters 1 through 19.
- **Appendix B, "CCNA Security 210-260 (IINS) Exam Updates":** This appendix provides instructions for finding updates to the exam and this book when and if they occur.
- **Glossary:** The glossary contains definitions for all the terms listed in the "Define Key Terms" sections at the conclusions of Chapters 1 through 19.

CD-Only Appendixes

- **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.
- **Appendix E, "Study Planner":** This spreadsheet provides major study milestones where you can track your progress through your study.
- **Glossary:** The glossary contains definitions for all the terms listed in the "Define Key Terms" sections at the conclusions of Chapters 1 through 19.

Premium Edition eBook and Practice Test

This Cert Guide contains a special offer for a 70 percent discount off the companion CCNA Security 210-260 Official Cert Guide Premium Edition eBook and Practice Test. The Premium Edition combines an eBook version of the text with an enhanced Pearson IT Certification Practice Test. By purchasing the Premium Edition, you get access to two eBook versions of the text: a PDF version and an EPUB version for reading on your tablet, eReader, or mobile device. You also get an enhanced practice test that contains an additional two full practice tests of unique questions. In addition, all the practice test questions are linked to the PDF eBook, allowing you to get more detailed feedback on each question instantly. To take advantage of this offer, you need the coupon code included on the paper in the CD sleeve. Just follow the purchasing instructions that accompany the code to download and start using your Premium Edition today.



This chapter covers the following topics:

- Mitigation technology for e-mail-based threats
- Mitigation technology for web-based threats

CHAPTER 18

Mitigation Technologies for E-mail-Based and Web-Based Threats

Efficient e-mail-based and web-based security requires a robust solution that is expanded beyond the traditional perimeter, as new threats are emerging on a daily basis. The Cisco *E-mail Security Appliances (ESA)* and the *Cisco Web Security Appliance (WSA)* provide a great solution designed to protect corporate users against these threats. Cisco has added *advanced malware protection (AMP)* to the ESA and WSA to allow security administrators to detect and block malware and perform continuous analysis and retrospective alerting. Both the ESA and WSA use cloud-based security intelligence to allow protection before, during, and after an attack. This chapter covers these technologies and solutions in detail. You will learn mitigation technologies such as spam and antimalware filtering, *data loss prevention (DLP)*, blacklisting, e-mail encryption, and web application filtering.

"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 18-1 details the major topics discussed in this chapter and their corresponding quiz questions.

Table 18-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Mitigation Technology for E-mail-Based Threats	1–4
Mitigation Technology for Web-Based Threats	5–8

1. Which of the following features does the Cisco ESA provide? (Choose all that apply.)
   a. Network antivirus capabilities
   b. E-mail encryption
   c. Threat outbreak prevention
   d. Support for remote access SSL VPN connections
2. Which of the following Cisco ESA models are designed for mid-sized organizations? (Choose all that apply.)
   a. Cisco C380
   b. Cisco C670
   c. Cisco C680
   d. Cisco X1070

3. What is a spear phishing attack?
   a. Unsolicited e-mails sent to an attacker.
   b. A denial-of-service (DoS) attack against an e-mail server.
   c. E-mails that are directed to specific individuals or organizations. An attacker may obtain information about the targeted individual or organization from social media sites and other sources.
   d. Spam e-mails sent to numerous victims with the purpose of making money.
4. Which of the following e-mail authentication mechanisms are supported by the Cisco ESA? (Choose all that apply.)
   a. Sender Policy Framework (SPF)
   b. Sender ID Framework (SIDF)
   c. DomainKeys Identified Mail (DKIM)
   d. DomainKeys Mail Protection (DMP)
5. Which of the following is the operating system used by the Cisco WSA ?
   a. Cisco AsyncOS operating system
   b. Cisco IOS-XR Software
   c. Cisco IOS-XE Software
   d. Cisco IOS Software
   e. Cisco ASA Software
6. Which of the following connectors are supported by the Cisco CWS service? (Choose all that apply.)
   a. Cisco Security Manager (CSM)
   b. Cisco ASA
   c. Cisco ISR G2 routers
   d. Cisco AnyConnect Secure Mobility Client
   e. Cisco WSA
7. Which of the following features are supported by the Cisco WSA? (Choose all that apply.)
   a. File reputation
   b. File sandboxing
   c. Layer 4 traffic monitor
   d. Real-time e-mail scanning
   e. Third-party DLP integration
8. Cisco WSA can be deployed using the Web Cache Communication Protocol (WCCP) configured in which of the following modes? (Choose all that apply.)
   a. Multiple context mode
   b. Explicit proxy mode
   c. Transparent proxy mode
   d. Virtualized mode

Foundation Topics

Mitigation Technology for E-mail-Based Threats

Users are no longer accessing e-mail from the corporate network or from a single device. Cisco provides cloud-based, hybrid, and on-premises ESA-based solutions that can help protect any dynamic environment. This section introduces these solutions and technologies explaining how users can use threat intelligence to detect, analyze, and protect against both known and emerging threats.

E-mail-Based Threats

Key Topic

There are several types of e-mail-based threats. The following are the most common:

- **Spam:** Unsolicited e-mail messages that can be advertising a service or (typically) a scam or a message with malicious intent. E-mail spam continuous to be a major threat because it can be used to spread malware.
- **Malware attachments:** E-mail messages containing malicious software (malware).
- **Phishing:** An attacker's attempt to fool a user that such e-mail communication comes from a legitimate entity or site, such as banks, social media websites, online payment processors, or even corporate IT communications. The goal of the phishing e-mail is to steal user's sensitive information such as user credentials, bank accounts, and so on.
- **Spear phishing:** Phishing attempts that are more targeted. These phishing e-mails are directed to specific individuals or organizations. For instance, an attacker may perform a passive reconnaissance on the individual or organization by gathering information from social media sites (for example, Twitter, LinkedIn, Facebook) and other online resources. Then the attacker may tailor a more directed and relevant message to the victim increasing the probability of such user being fooled to follow a malicious link, click an attachment containing malware, or simply reply to the e-mail providing sensitive information. There is another phishing-based attack called *whaling*. These attacks specifically target executives and high-profile users within a given organization.

Cisco Cloud E-mail Security

Key Topic

Cisco cloud e-mail security provides a cloud-based solution that allows companies to outsource the management of their e-mail security management. The service provides e-mail security instances in multiple Cisco data centers to enable high availability. Figure 18-1 illustrates the Cisco cloud e-mail security solution.

In Figure 18-1, three organizations (a large enterprise, a university, and a small- to medium-size business) leverage the Cisco hosted (cloud) environment. The solution also supports mobile workers.

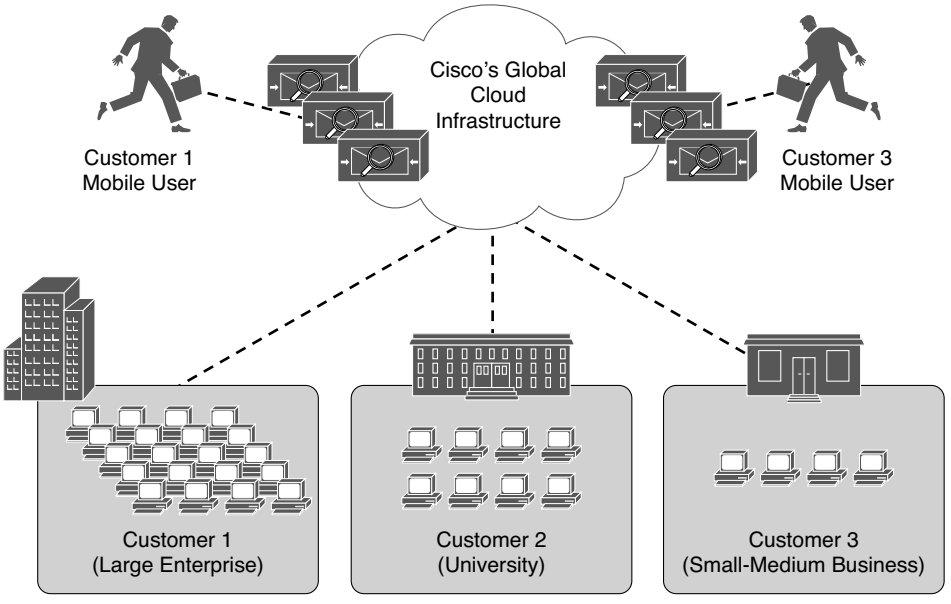


Figure 18-1 *Cisco Cloud E-mail Security Architecture*

Cisco Hybrid E-mail Security

The Cisco hybrid e-mail security solution combines both cloud-based and on-premises ESAs. This hybrid solution helps Cisco customers reduce their on-site e-mail security footprint, outsourcing a portion of their e-mail security to Cisco, while still allowing them to maintain control of confidential information within their physical boundaries. Many organizations need to stay compliant to many regulations that may require them to keep sensitive data physically on their premises. The Cisco hybrid e-mail security solution allows network security administrators to remain compliant and to maintain advanced control with encryption, *data loss prevention (DLP)*, and on-site identity-based integration.

Key Topic

Cisco E-mail Security Appliance

The following are the different ESA models:

- Cisco X-Series E-mail Security Appliances
  - **Cisco X1070:** High-performance ESA for service providers and large enterprises
- Cisco C-Series E-mail Security Appliances
  - **Cisco C680:** The high-performance ESA for service providers and large enterprises
  - **Cisco C670:** Designed for medium-size enterprises
  - **Cisco C380:** Designed for medium-size enterprises
  - **Cisco C370:** Designed for small- to medium-size enterprises
  - **Cisco C170:** Designed for small businesses and branch offices

The Cisco ESA runs the Cisco AsyncOS operating system. The Cisco AsyncOS supports numerous features that will help mitigate e-mail-based threats. The following are examples of the features supported by the Cisco ESA:

- **Access control:** Controlling access for inbound senders according to the sender's IP address, IP address range, or domain name.
- **Antispam:** Multilayer filters based on Cisco SenderBase reputation and Cisco antispam integration. The antispam reputation and zero-day threat intelligence are fueled by Cisco's security intelligence and research group named Talos.
- **Network Antivirus:** Network antivirus capabilities at the gateway. Cisco partnered with Sophos and McAfee, supporting their antivirus scanning engines.
- **Advanced malware protection (AMP):** Allows security administrators to detect and block malware and perform continuous analysis and retrospective alerting.
- **DLP:** The ability to detect any sensitive e-mails and documents leaving the corporation. The Cisco ESA integrates RSA e-mail DLP for outbound traffic.

NOTE If RSA e-mail DLP is configured on a Cisco ESA that is also running antispam and antivirus scanning on inbound traffic, it can cause a performance decrease of less than 10 percent. Cisco ESAs that are only running outbound messages and are not running antispam and antivirus may experience a significant performance decline.

- **E-mail encryption:** The ability to encrypt outgoing mail to address regulatory requirements. The administrator can configure an encryption policy on the Cisco ESA and use a local key server or hosted key service to encrypt the message.
- **E-mail authentication:** A few e-mail authentication mechanisms are supported, including Sender Policy Framework (SPF), Sender ID Framework (SIDF), and DomainKeys Identified Mail (DKIM) verification of incoming mail, as well as DomainKeys and DKIM signing of outgoing mail.
- **Outbreak filters:** Preventive protection against new security outbreaks and e-mail-based scams using Cisco's Security Intelligence Operations (SIO) threat intelligence information.

NOTE Cisco SenderBase is the world largest e-mail and web traffic monitoring network. It provides real-time threat intelligence powered by Cisco *Security Intelligence Operations (SIO)*. The Cisco SenderBase website is located at http://www.senderbase.org.

The Cisco ESA acts as the e-mail gateway to the organization, handling all e-mail connections, accepting messages, and relaying them to the appropriate systems. The Cisco ESA can service e-mail connections from the Internet to users inside your network, and from systems inside your network to the Internet. E-mail connections use *Simple Mail Transfer Protocol (SMTP)*. The ESA services all SMTP connections by default acting as the SMTP gateway.

NOTE Mail gateways are also known as a *mail exchangers* or *MX*.

The Cisco ESA uses listeners to handle incoming SMTP connection requests. A listener defines an e-mail processing service that is configured on an interface in the Cisco ESA. Listeners apply to e-mail entering the appliance from either the Internet or from internal systems.

The following listeners can be configured:

- Public listeners for e-mail coming in from the Internet.
- Private listeners for e-mail coming from hosts in the corporate (inside) network. These e-mails are typically from an internal groupware, Exchange, POP, or IMAP e-mail servers.

Figure 18-2 illustrates the concept of Cisco ESA listeners.

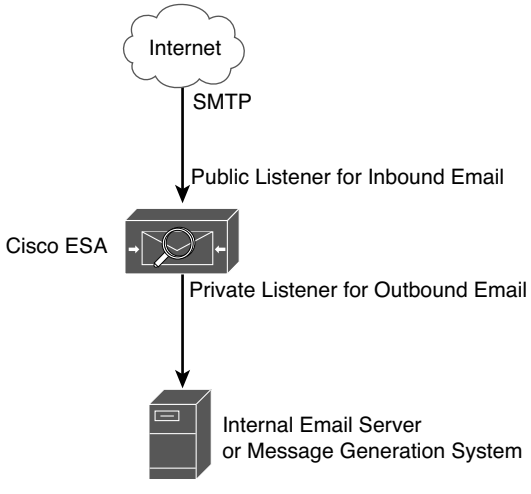


Figure 18-2 *Cisco ESA Listeners*

Cisco ESA listeners are often referred to as *SMTP daemons* running on a specific Cisco ESA interface. When a listener is configured, the following information must be provided:

- Listener properties such as a specific interface in the Cisco ESA and the TCP port that will be used. The listener properties must also indicate whether it is a public or a private listener.
- The hosts that are allowed to connect to the listener using a combination of access control rules. An administrator can specify which remote hosts can connect to the listener.
- The local domains for which public listeners accept messages.

Cisco ESA Initial Configuration

To perform the initial Cisco ESA configuration, complete the following steps:

Step 1. Log in to the Cisco ESA. The default username is admin, and the default password is ironport.

Step 2. Use the **systemsetup** command in the *command-line interface (CLI)* of the Cisco ESA to initiate the System Setup Wizard, as shown in Example 18-1.

Example 18-1 *Initial Setup with the* **systemsetup** *Command*

```
IronPort> systemsetup
WARNING: The system setup wizard will completely delete any existing
'listeners' and all associated settings including the 'Host Access Table' - mail
operations may be interrupted.
Are you sure you wish to continue? [Y]> Y

You are now going to configure how the IronPort C60 accepts mail by
creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):
[]> InboundMail

Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3
Enter the domains or specific addresses you want to accept mail for.
Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
Separate multiple addresses with commas

[]> securemeinc.org
Would you like to configure SMTP routes for example.com? [Y]> y

Enter the destination mail server which you want mail for example.com to be delivered.

Separate multiple entries with commas.
[]> exchange.securemeinc.org
```

```
Do you want to enable rate limiting for this listener? (Rate limiting defines the
maximum

number of recipients per hour you are willing to receive from a remote domain.) [Y]> y

Enter the maximum number of recipients per hour to accept from a remote domain.
[]> 4500

Default Policy Parameters
==========================
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 1,000
Maximum Number Of Messages Per Connection: 1,000
Maximum Number Of Recipients Per Message: 1,000
Maximum Number Of Recipients Per Hour: 4,500
Maximum Recipients Per Hour SMTP Response:
 452 Too many recipients received this hour
Use SenderBase for Flow Control: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Would you like to change the default host access policy? [N]> n
Listener InboundMail created.
Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.
*****

Do you want to configure the C60 to relay mail for internal hosts? [Y]> y

Please create a name for this listener (Ex: "OutboundMail"):
[]> OutboundMail

Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 2

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.
```

```
Separate multiple entries with commas.
[]> .securemeinc.org

Do you want to enable rate limiting for this listener? (Rate limiting defines the
maximum number of recipients per hour you are willing to receive from a remote
domain.)
[N]> n

Default Policy Parameters
==========================
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: No
Virus Detection Enabled: Yes
Allow TLS Connections: No
Would you like to change the default host access policy? [N]> n
Listener OutboundMAil created.
Defaults have been set for a Private listener.
Use the listenerconfig->EDIT command to customize the listener.
*****

Congratulations! System setup is complete. For advanced configuration, please refer to
  the User Guide.
mail3.securemeinc.org >
```


In Example 18-1, the inside (private) and outside (public) listeners are configured. The domain name of securemeinc.org is used in this example.

To verify the configuration, you can use the **mailconfig** command to send a test e-mail containing the system configuration data that was entered in the System Setup Wizard, as shown in Example 18-2.

Example 18-2 *Verifying the Configuration with the* **mailconfig** *Command*

```
mail3.securemeinc.org> mailconfig

Please enter the email address to which you want to send
the configuration file. Separate multiple addresses with commas.

[]> admin@securemeinc.org

The configuration file has been sent to admin@securemeinc.org.

mail3.securemeinc.org>
```

In Example 18-2, the e-mail is sent to the administrator (admin@securemeinc.org).

Mitigation Technology for Web-Based Threats

For any organization to be able to protect its environment against web-based security threats, the security administrators need to deploy tools and mitigation technologies that go far beyond traditional blocking of known bad websites. Nowadays, you can download malware through compromised legitimate websites, including social media sites, advertisements in news and corporate sites, gaming sites, and many more. Cisco has developed several tools and mechanisms to help their customers combat these threats. The core solutions for mitigating web-based threats are the Cisco *Cloud Web Security (CWS)* offering and the integration of *advanced malware protection (AMP)* to the Cisco *Web Security Appliance (WSA)*. Both solutions enable malware detection and blocking, continuous monitoring, and retrospective alerting. The following sections cover the Cisco CWS and Cisco WSA in detail.

Cisco CWS

Cisco CWS is a cloud-based security service from Cisco that provides worldwide threat intelligence, advanced threat defense capabilities, and roaming user protection. The Cisco CWS service uses web proxies in Cisco's cloud environment that scan traffic for malware and policy enforcement. Cisco customers can connect to the Cisco CWS service directly by using a *proxy autoconfiguration (PAC)* file in the user endpoint or through connectors integrated into the following Cisco products:

- Cisco ISR G2 routers
- Cisco ASA
- Cisco WSA
- Cisco AnyConnect Secure Mobility Client

Organizations using the transparent proxy functionality through a connector can get the most out of their existing infrastructure. In addition, the scanning is offloaded from the hardware appliances to the cloud, reducing the impact to hardware utilization and reducing network latency. Figure 18-3 illustrates how the transparent proxy functionality through a connector works.

In Figure 18-3, the Cisco ASA is enabled with the Cisco CWS connector at a branch office. The following steps explain how Cisco CWS protects the corporate users at the branch office:

1. An internal user makes an HTTP request to an external website (securemeinc.org).
2. The Cisco ASA forwards the request to Cisco CWS global cloud infrastructure.
3. It notices that securemeinc.org had some web content (ads) that were redirecting the user to a known malicious site.
4. Cisco CWS blocks the request to the malicious site.

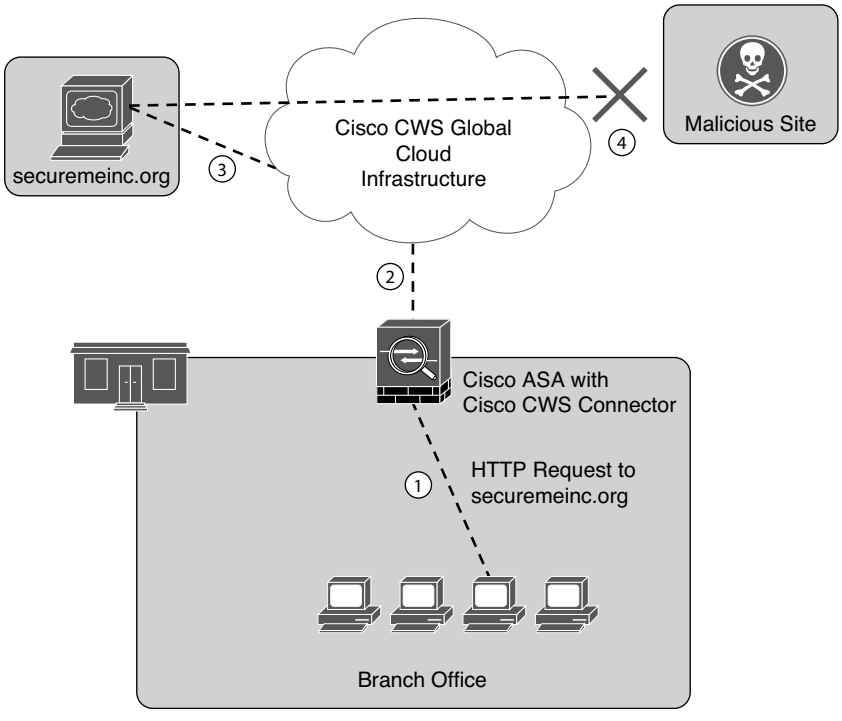


Figure 18-3 *Cisco ASA with Cisco CWS Connector Example*

Key Topic

Cisco WSA

The Cisco WSA uses cloud-based intelligence from Cisco to help protect the organization before, during, and after an attack. This "lifecycle" is what is referred to as the *attack continuum*. The cloud-based intelligence includes web (URL) reputation and zero-day threat intelligence from Cisco's security intelligence and research group named Talos. This threat intelligence helps security professionals to stop threats before they enter the corporate network, while also enabling file reputation and file sandboxing to identify threats during an attack. Retrospective attack analysis allows security administrators to investigate and provide protection after an attack when advanced malware might have evaded other layers of defense.

The Cisco WSA can be deployed in explicit proxy mode or as a transparent proxy using the *Web Cache Communication Protocol (WCCP)*. WCCP is a protocol originally developed by Cisco, but several other vendors have integrated it in their products to allow clustering and transparent proxy deployments on networks using Cisco infrastructure devices (routers, switches, firewalls, and so on).

Figure 18-4 illustrates a Cisco WSA deployed as an explicit proxy.

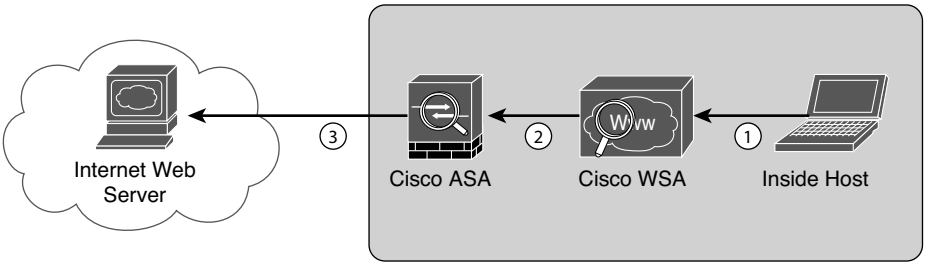


Figure 18-4 *Explicit Proxy Configuration*

The following are the steps illustrated in Figure 18-4:

1. An internal user makes an HTTP request to an external website. The client browser is configured to send the request to the Cisco WSA.
2. The Cisco WSA connects to the website on behalf of the internal user.
3. The firewall (Cisco ASA) is configured to only allow outbound web traffic from the Cisco WSA, and it forwards the traffic to the web server.

Figure 18-5 shows a Cisco WSA deployed as a transparent proxy.

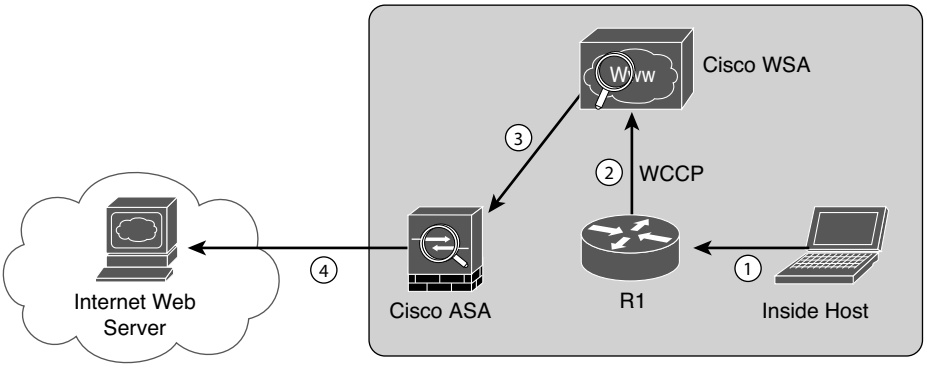


Figure 18-5 *Transparent Proxy Configuration*

The following are the steps illustrated in Figure 18-5:

1. An internal user makes an HTTP request to an external website.
2. The internal router (R1) redirects the web request to the Cisco WSA using WCCP.
3. The Cisco WSA connects to the website on behalf of the internal user.
4. Also in this example, the firewall (Cisco ASA) is configured to only allow outbound web traffic from the WSA. The web traffic is sent to the Internet web server.

Figure 18-6 demonstrates how the WCCS registration works. The Cisco WSA is the WCCP client, and the Cisco router is the WCCP server.

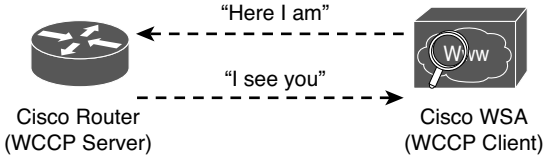


Figure 18-6 *WCCP Registration*

During the WCCP registration process, the WCCP client sends a registration announcement ("Here I am") every 10 seconds. The WCCP server (the Cisco router in this example) accepts the registration request and acknowledges it with an "I See You" WCCP message. The WCCP server waits 30 seconds before it declares the client as "inactive" (engine failed). WCCP can be used in large-scale environments. Figure 18-7 shows a cluster of Cisco WSAs, where internal Layer 3 switches redirect web traffic to the cluster.

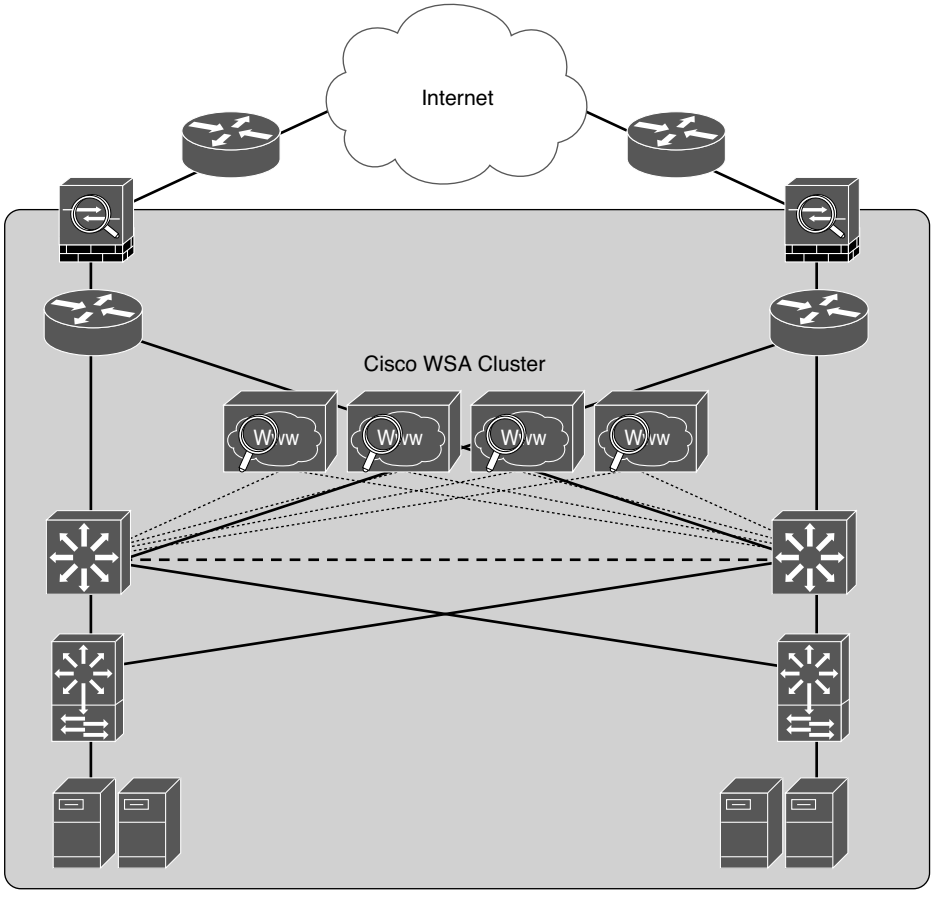


Figure 18-7 *Cisco WSA Cluster Example*

The Cisco WSA comes in different models. The following are the different Cisco WSA models:

- Cisco WSA S680
  - It is a high-performance WSA designed for large organizations with 6000 to 12,000 users.
  - A 2 *rack-unit (RU)* appliance with 16 (2 octa core) CPUs, 32 GB of memory, and 4.8 TB of disk space.
- Cisco WSA S670
  - A high-performance WSA designed for large organizations with 6000 to 12,000 users
  - A 2 RU appliance with 8 (2 octa core) CPUs, 8 GB of memory, and 2.7 TB of disk space.
- Cisco WSA S380
  - Designed for medium-size organizations with 1500 to 6000 users.
  - A 2 RU appliance with 6 (1 hexa core) CPUs, 16 GB of memory, and 2.4 TB of disk space.
- Cisco WSA S370
  - Designed for medium-size organizations with 1500 to 6000 users.
  - A 2 RU appliance with 4 (1 quad core) CPUs, 4 GB of memory, and 1.8 TB of disk space.
- Cisco WSA S170
  - Designed for small- to medium-size organizations with up to 1500 users.
  - A 1 RU appliance with 2 (1 dual core) CPUs, 4 GB of memory, and 500 GB of disk space.

The Cisco WSA runs Cisco AsyncOS operating system. The Cisco AsyncOS supports numerous features that will help mitigate web-based threats. The following are examples of these features:

- **Real-time antimalware adaptive scanning:** The Cisco WSA can be configured to dynamically select an antimalware scanning engine based on URL reputation, content type, and scanner effectiveness. Adaptive scanning is a feature designed to increase the "catch rate" of malware that is embedded in images, JavaScript, text, and Adobe Flash files. Adaptive scanning is an additional layer of security on top of Cisco WSA Web Reputation Filters that include support for Sophos, Webroot, and McAfee.
- **Layer 4 traffic monitor:** Used to detect and block spyware. It dynamically adds IP addresses of known malware domains to a database of sites to block.
- **Third-party DLP integration:** Redirects all outbound traffic to a third-party DLP appliance, allowing deep content inspection for regulatory compliance and data exfiltration protection. It enables an administrator to inspect web content by title, metadata, and size and to even prevent users from storing files to cloud services, such as Dropbox, Google Drive, and others.
- **File reputation:** Using threat information from Cisco Talos. This file reputation threat intelligence is updated every 3 to 5 minutes.

- **File sandboxing:** If malware is detected, the Cisco AMP capabilities can put files in a sandbox to inspect its behavior, combining the inspection with machine-learning analysis to determine the threat level. Cisco Cognitive Threat Analytics (CTA) uses machine-learning algorithms to adapt over time.
- **File retrospection:** After a malicious attempt or malware is detected, the Cisco WSA continues to cross-examine files over an extended period of time.
- **Application visibility and control:** Allows the Cisco ASA to inspect and even block applications that are not allowed by the corporate security polity. For example, an administrator can allow users to use social media sites like Facebook but block micro-applications such as Facebook games.

Cisco Content Security Management Appliance

Cisco *Security Management Appliance (SMA)* is a Cisco product that centralizes the management and reporting for one or more Cisco ESAs and Cisco WSAs. Cisco SMA has consistent enforcement of policy, and enhances threat protection. Figure 18-8 shows a Cisco SMA that is controlling Cisco ESA and Cisco WSAs in different geographic locations (New York, Raleigh, Chicago, and Boston).

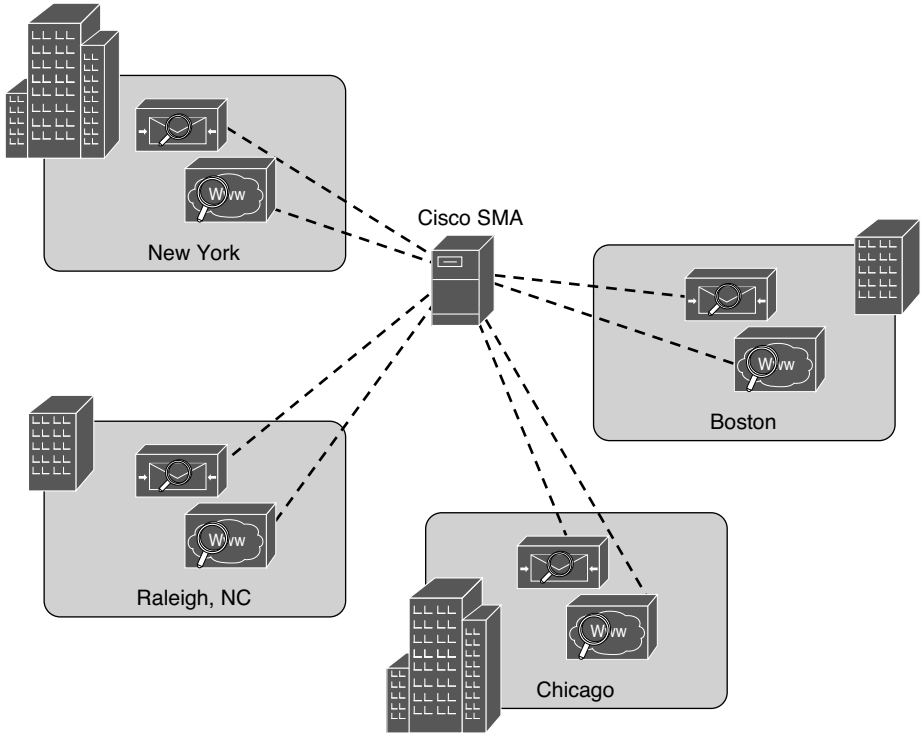


Figure 18-8 *Cisco SMA Centralized Deployment*

The Cisco SMA comes in different models. These models are physical appliances or the Cisco Content *Security Management Virtual Appliance (SMAV)*. The following are the different Cisco SMA models:

- **Cisco SMA M680:** Designed for large organizations with over 10,000 users
- **Cisco SMAV M600v:** Designed for large enterprises or service providers
- **Cisco SMA M380:** Designed for organizations with 1000 to 10,000 users
- **Cisco SMAV M300v:** Designed for organizations with 1000 to 5000 users
- **Cisco SMA M170:** Designed for small business or branch offices with up to 1000 users
- **Cisco SMAV M100v:** Designed for small business or branch offices with up to 1000 users

NOTE Cisco also has a Cisco SMAV M000v that is used for evaluations only.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, denoted with a Key Topic icon. Table 18-2 lists these key topics.

Key Topic

Table 18-2 Key Topics

Key Topic Element	Description	Page Number
Section	E-mail-Based Threats	479
Section	Cisco Cloud E-mail Security	479
Section	Cisco E-mail Security Appliance	480
Section	Mitigation Technology for Web-Based Threats	486
Section	Cisco CWS	486
Section	Cisco WSA	487

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 so that you can check your work. There are no applicable tables in this specific chapter.

Define Key Terms

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

antispam filters, network antivirus, advanced malware protection (AMP), file sandboxing, file retrospection

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. To see how well you have memorized the commands as a side effect of your other studies, cover the left side of Table 18-3 with a piece of paper, read the descriptions on the right side, and see whether you remember the commands.

Table 18-3 Command Reference

Command	Description
systemsetup	Launch the System Setup Wizard to initially configure the Cisco ESA.
mailconfig	Verify the Cisco ESA configuration by sending a test e-mail that contains the system configuration data that was entered in the system setup wizard.

Index

Numbers

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q-R

S

T

U

V

W

X-Y-Z