31 Days Before Your CCNA Security Exam

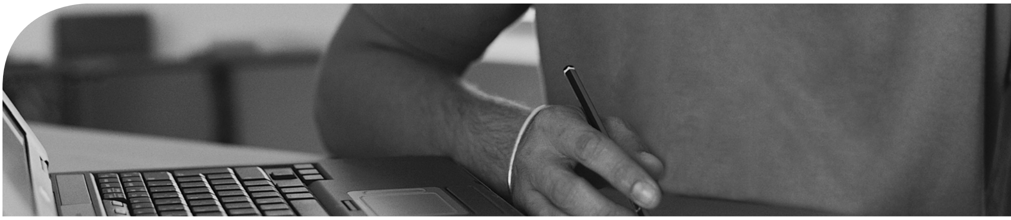
A Day-By-Day Review Guide for the IINS 210-260 Certification Exam

ciscopress.com

Patrick Gargano

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



31 Days Before Your CCNA Security Exam

A Day-By-Day Review Guide for the IINS 210-260 Certification Exam

Patrick Gargano

Cisco Press • 800 East 96th Street • Indianapolis, Indiana 46240 USA

31 Days Before Your CCNA Security Exam

Patrick Gargano

Copyright © 2016 Cisco Systems, Inc.

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

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

Printed in the United States of America

First Printing June 2016

Library of Congress Control Number: 2016936752

ISBN-13: 978-1-58720-578-1

ISBN-10: 1-58720-578-5

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Network Associate Security (CCNA Security) certification 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 author 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 intlcs@pearson.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.

Business Operation Manager, Cisco Press	Jan Cornelssen
Executive Editor	Mary Beth Ray
Managing Editor	Sandra Schroeder
Development Editor	Ellie Bru
Senior Project Editor	Tonya Simpson
Copy Editor	Bill McManus
Technical Editor	John Stuppi
Editorial Assistant	Vanessa Evans
Cover Designer	Chuti Prasertsith
Composition	Bumpy Design
Indexer	Ken Johnson
Proofreader	The Wordsmithery LLC

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.

About the Author

Patrick Gargano has been an educator since 1996 and a Cisco Networking Academy Instructor since 2000. He currently heads the Networking Academy program at Collège La Cité in Ottawa, Canada, where he teaches CCNA/CCNP-level courses. Patrick has twice led the Cisco Networking Academy student Dream Team deploying the wired and wireless networks supporting the U.S. Cisco Live conferences. In 2014 he co-authored *CCNP Routing and Switching Portable Command Guide*. Recognitions of his teaching include prizes from Collège La Cité for innovation and excellence and from the Ontario Association of Certified Engineering Technicians and Technologists for excellence in technology education. Previously, Patrick was a Cisco Networking Academy instructor at Cégep de l'Outaouais (Gatineau, Canada) and Louis-Riel High School (Ottawa, Canada) and a Cisco instructor (CCSI) for Fast Lane UK (London). His certifications include CCNA (R&S), CCNA Wireless, CCNA Security, and CCNP (R&S). He holds Bachelor of Education and Bachelor of Arts degrees from the University of Ottawa. Find him on Twitter @PatrickGargano.

About the Technical Reviewer

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. He is also the co-author of *CCNA Security 210-260 Official Cert Guide* with Omar Santos. Before joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc. John is also a CISSP (No. 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.

Dedications

To my wife Kathryn, who is always happy to explain that when in doubt, “that” is always better than “which,” and to our son Samuel who, at age 7, already knows that (not which) Mummy is usually right but Daddy is usually more fun.

To my father, who can’t read this.

To my mother, who has devoted everything to our family.

To Albert, who has endured with courage.

Acknowledgments

My first thank-you's have to go to Mary Beth Ray for suggesting that I write this book, and to Scott Empson and Hans Roth for making my first Cisco Press project such a thoroughly enjoyable collaboration that I was happy to accept her offer. Mary Beth is a remarkable executive editor, but then everyone at Cisco Press has been fantastic to work with: Ellie Bru, the development editor, has kept the SS Gargano on an even keel, and Tonya Simpson, the project editor, has ensured that everything is shipshape, while Bill McManus, the copy editor, has kept the good ship from sinking under an avalanche of mixed metaphors and grammatical missteps. I confess that I was a bit intimidated when I found out John Stuppi would be the technical editor, because he co-wrote one of my primary sources, the Cisco Press *CCNA Security 210-260 Official Cert Guide*, but in addition to being a true authority, he was a pleasure to work with. Allan Johnson, who initiated the 31 Days series, was my trusty guide on this, and Troy McMillan, who produced the fantastic material used in the Digital Study Guide version of the book, deserves sincere thanks as well.

Alongside the Cisco Press team, I want to offer my sincere gratitude to my colleagues at La Cité, especially Georges Absi, who has been generous with advice, moral support, and his wife's authentic tabbouleh.

My past, present, and future students at La Cité are the inspiration for this book. I had them in mind with every word that I wrote, and if I've produced something that they'll find useful and easy to understand, then I've met my loftiest goal.

Contents at a Glance

Introduction xxii

Digital Study Guide xxvi

Day 31: Common Security Principles 1

Day 30: Common Security Threats 5

Day 29: Cryptographic Technologies 11

Day 28: PKI and Network Security Architectures 21

Day 27: Secure Management Systems 35

Day 26: AAA Concepts 45

Day 25: TACACS+ and RADIUS Implementation 51

Day 24: 802.1X 61

Day 23: BYOD 67

Day 22: IPsec Technologies 73

Day 21: Clientless Remote-Access VPN 85

Day 20: AnyConnect Remote Access VPN 99

Day 19: Site-to-Site VPN 113

Day 18: VPN Advanced Topics 131

Day 17: Secure Device Access 137

Day 16: Secure Routing Protocols 143

Day 15: Control Plane Security 149

Day 14: Layer 2 Infrastructure Security 153

Day 13: Layer 2 Protocols Security 161

Day 12: VLAN Security 171

Day 11: Firewall Technologies 181

Day 10: Cisco ASA NAT Implementation 191

Day 9: Cisco IOS Zone-Based Policy Firewall 209

Day 8: Cisco ASA Firewall Concepts 219

Day 7: ASA Firewall Configuration 227

Day 6: IDS/IPS Concepts 245

Day 5: IDS/IPS Technologies 253

Day 4: Email-based Threat Mitigation 259

Day 3: Web-based Threat Mitigation 269

Day 2: Endpoint Protection 275

Day 1: CCNA Security Skills Review and Practice 281

Exam Day 299

Post-Exam Information 301

Index 303

Contents

Introduction xxii

Digital Study Guide xxvi

Day 31: Common Security Principles 1

CCNA Security 210-260 IINS Exam Topics 1

Key Topics 1

Confidentiality, Integrity, and Availability (CIA) 1

SIEM 1

Common Network Security Terms 2

Security Zones 2

Study Resources 4

Day 30: Common Security Threats 5

CCNA Security 210-260 IINS Exam Topics 5

Key Topics 5

Network Attacks 5
Reconnaissance Attacks 5
Access Attacks 5
DoS and DDoS Attacks 6

Social Engineering 7
Types 7
Defenses 8

Malware 8

Data Loss 9

Study Resources 10

Day 29: Cryptographic Technologies 11

CCNA Security 210-260 IINS Exam Topics 11

Key Topics 11

CIA Triad 11

Key Exchange and Management 11

Hash Algorithms 12
Well-known Hash Functions 12
Authentication Using Hashing 13
Hashing in Cisco Products 14

Symmetric and Asymmetric Encryption 15
Encryption Overview 15
Symmetric Encryption Algorithms 15
Asymmetric Encryption Algorithms 16
Digital Signatures and RSA Certificates 18
Study Resources 19

Day 28: PKI and Network Security Architectures 21
CCNA Security 210-260 IINS Exam Topics 21
Key Topics 21
Public Key Infrastructure 21
PKI Terminology, Components, and Classes of Certificates 22
PKI Topologies 23
PKI Standards 24
PKI Operations 25
Enrollment and Revocation 27
Network Architectures and Topologies 28
Campus-Area Network (CAN) 28
WAN and Branch/SOHO 29
Data Center 31
Cloud and Virtual Networks 31
Study Resources 33

Day 27: Secure Management Systems 35
CCNA Security 210-260 IINS Exam Topics 35
Key Topics 35
In-band and Out-of-band Management 35
Management Plane Security 36
Access Security 36
SSH/HTTPS 38
Syslog 38
Simple Network Management Protocol (SNMP) 39
Network Time Protocol (NTP) 42
Secure Copy Protocol (SCP) 43
Study Resources 44

Day 26: AAA Concepts 45

CCNA Security 210-260 IINS Exam Topics 45

Key Topics 45

AAA 45

RADIUS and TACACS+ 46

RADIUS 46

TACACS+ 47

ACS and ISE 48

ACS 49

ISE 49

Study Resources 50

Day 25: TACACS+ and RADIUS Implementation 51

CCNA Security 210-260 IINS Exam Topics 51

Key Topics 51

Server-based AAA Authentication 51

Server-based AAA Authorization 53

Server-based AAA Accounting 54

Server-based AAA Verification and Troubleshooting 55

Study Resources 58

Day 24: 802.1X 61

CCNA Security 210-260 IINS Exam Topics 61

Key Topics 61

802.1X 61

Terminology and Concepts 61

Configuration and Verification 63

Study Resources 65

Day 23: BYOD 67

CCNA Security 210-260 IINS Exam Topics 67

Key Topics 67

BYOD Architecture 67

BYOD Management 69

Study Resources 72

Day 22: IPsec Technologies 73

CCNA Security 210-260 IINS Exam Topics 73

Key Topics 73

VPNs 73

IPsec Framework 76

IPsec Protocols 77

AH 77

ESP 78

IPsec Modes of Operations 78

Confidentiality 79

Data Integrity 79

Origin Authentication 80

Key Management 80

Suite B Cryptographic Standard 81

IKE 81

IKEv1 Phase 1 82

IKEv1 Phase 2 83

IKEv2 83

Study Resources 84

Day 21: Clientless Remote-Access VPN 85

CCNA Security 210-260 IINS Exam Topics 85

Key Concepts 85

Clientless SSL VPN Concepts 85

Clientless SSL VPN Configuration 87

Task 1: Launch Clientless SSL VPN Wizard from ASDM 88

Task 2: Configure the SSL VPN URL and Interface 88

Task 3: Configure User Authentication 89

Task 4: Configure User Group Policy 90

Task 5: Configure Bookmarks 90

Clientless SSL VPN Verification 95

Study Resources 97

Day 20: AnyConnect Remote Access VPN 99

CCNA Security 210-260 IINS Exam Topics 99

Key Topics 99

AnyConnect SSL VPN Concepts 99

SSL VPN Server Authentication 100

SSL VPN Client Authentication 100
SSL VPN Client IP Address Assignment 100
AnyConnect SSL VPN Configuration and Verification 101
Phase 1: Configure Cisco ASA for Cisco AnyConnect 101
Task 1: Connection Profile Identification 101
Task 2: VPN Protocols and Device Certificate 102
Task 3: Client Image 102
Task 4: Authentication Methods 103
Task 5: Client Address Assignment 103
Task 6: Network Name Resolution Servers 104
Task 7: Network Address Translation Exemption 104
Task 8: AnyConnect Client Deployment and Summary 105
Phase 2: Configure the Cisco AnyConnect VPN Client 106
Phase 3: Verify AnyConnect Configuration and Connection 108
Study Resources 111

Day 19: Site-to-Site VPN 113

CCNA Security 210-260 IINS Exam Topics 113
Key Topics 113
IPsec Negotiation 113
Cisco IOS CLI-based Site-to-Site IPsec VPN 114
Configuration 115
Step 1: ACL Compatibility 115
Step 2: IKE Phase 1—ISAKMP Policy 115
Step 3: IKE Phase 2—IPsec Transform Set 117
Step 4: Crypto ACLs 117
Step 5: IPsec Crypto Map 118
Verification 119
Cisco ASA Site-to-Site IPsec VPN 122
Configuration 123
Step 1: Launch the ASDM Site-to-Site VPN Wizard 123
Step 2: Peer Device Identification 123
Step 3: Traffic to Protect 124
Step 4: Security 124
Step 5: NAT Exempt 125
Verification 125
Study Resources 128

Day 18: VPN Advanced Topics 131

CCNA Security 210-260 IINS Exam Topics 131

Key Topics 131

Hairpinning and Client U-Turn 131

Split Tunneling 132

Always-on VPN 134

NAT Traversal 134

Endpoint Posture Assessment 135

Study Resources 136

Day 17: Secure Device Access 137

CCNA Security 210-260 IINS Exam Topics 137

Key Topics 137

Cisco IOS Authorization with Privilege Levels 137

Authorization with Role-Based CLI 138

Cisco IOS Resilient Configuration 139

Cisco IOS File Authenticity 140

Study Resources 142

Day 16: Secure Routing Protocols 143

CCNA Security 210-260 IINS Exam Topics 143

Key Topics 143

Routing Protocol Authentication 143

OSPF MD5 Authentication 144

MD5 Authentication with Key Chain 144

MD5 Authentication Without Key Chain 145

OSPF SHA Authentication 146

Study Resources 148

Day 15: Control Plane Security 149

CCNA Security 210-260 IINS Exam Topics 149

Key Topics 149

Functional Planes of the Network 149

Control Plane Policing 150

Control Plane Protection 151

Study Resources 152

Day 14: Layer 2 Infrastructure Security 153

CCNA Security 210-260 IINS Exam Topics 153

Key Topics 153

Common Layer 2 Attacks 153
STP Attacks 153
ARP Spoofing 155
MAC Spoofing 156
CAM Table Overflows 157
CDP/LLDP Reconnaissance 157
VLAN Hopping 157
DHCP Spoofing 158

Study Resources 159

Day 13: Layer 2 Protocols Security 161

CCNA Security 210-260 IINS Exam Topics 161

Key Topics 161

DHCP Snooping 161

Dynamic ARP Inspection 163

IP Source Guard 164

Port Security 165

STP Security Mechanisms 167
PortFast 167
BPDU Guard 168
Root Guard 168
Loop Guard 168

Study Resources 169

Day 12: VLAN Security 171

CCNA Security 210-260 IINS Exam Topics 171

Key Topics 171

Private VLANs 171

PVLAN Edge 174

ACLs on Switches 175
PACL Configuration 176
VACL Configuration 177

Native VLAN 178

Study Resources 180

Day 11: Firewall Technologies 181

CCNA Security 210-260 IINS Exam Topics 181

Key Topics 181

Firewall Overview 181

Packet Filtering 183

Proxy and Application Firewalls 185

Stateful Firewalls 187

Next-Generation Firewalls 188

Personal Firewall 189

Study Resources 189

Day 10: Cisco ASA NAT Implementation 191

CCNA Security 210-260 IINS Exam Topics 191

Key Topics 191

NAT Fundamentals 191

NAT on Cisco ASA 193

Static NAT 195

Dynamic NAT 198

Dynamic PAT 201

Policy NAT 203

Study Resources 208

Day 9: Cisco IOS Zone-Based Policy Firewall 209

CCNA Security 210-260 IINS Exam Topics 209

Key Topics 209

ZPF Concepts 209

ZPF Zones and Zone Pairs 210

Introduction to C3PL 211

Class Maps 212

Policy Maps 212

Service Policy 213

Default Policies and Traffic Flows 213

ZPF Configuration and Verification 214

Configuring Class Maps 214
Configuring Policy Maps 215
Configuration and Verification 216
Study Resources 218

Day 8: Cisco ASA Firewall Concepts 219
CCNA Security 210-260 IINS Exam Topics 219
Key Topics 219
Cisco ASA Family 219
ASA Features and Services 221
ASA Deployments 222
ASA High Availability 223
ASA Contexts 225
Study Resources 226

Day 7: ASA Firewall Configuration 227
CCNA Security 210-260 IINS Exam Topics 227
Key Topics 227
ASA Default Configuration 227
ASA Management Access 229
ASA Interfaces 230
ASA Access Rules 232
ASA Objects and Object Groups 234
ASA Modular Policy Framework 240
Study Resources 244

Day 6: IDS/IPS Concepts 245
CCNA Security 210-260 IINS Exam Topics 245
Key Topics 245
IDS vs. IPS 245
Host-based vs. Network-based IPS 247
IPS Deployment Options 248
IPS Placement 249
IPS Terminology 250
Study Resources 251

Day 5: IDS/IPS Technologies 253

CCNA Security 210-260 IINS Exam Topics 253

Key Topics 253

Detection Technologies 253

Signatures 254

Trigger Actions 255

Blacklisting 256

Next-Generation IPS with FirePOWER 256

Study Resources 257

Day 4: Email-based Threat Mitigation 259

CCNA Security 210-260 IINS Exam Topics 259

Key Topics 259

ESA Overview 259

ESA Deployment 260

ESA Features 263

Filtering Spam 263

Fighting Viruses and Malware 264

Email Data Loss Prevention 264

Advanced Malware Protection 264

ESA Mail Processing 265

Incoming Mail Processing 265

Outgoing Mail Processing 266

Study Resources 267

Day 3: Web-based Threat Mitigation 269

CCNA Security 210-260 IINS Exam Topics 269

Key Topics 269

Cisco WSA 269

Cisco CWS 272

Study Resources 274

Day 2: Endpoint Protection 275

CCNA Security 210-260 IINS Exam Topics 275

Key Topics 275

Endpoint Security Overview 275

Personal Firewalls 276

Antivirus 276

Antispyware 277

Antimalware 278

Data Encryption 279

Study Resources 280

Day 1: CCNA Security Skills Review and Practice 281

CCNA Security 210-260 IINS Exam Topics 281

Key Topics 281

CCNA Security Skills Practice 281

Introduction 281

Topology Diagram 281

Addressing Table 282

ISP Configuration 283

Implementation 283

Step 1: Cable the Network As Shown in the Topology 283

Step 2: Configure Initial Settings for R1_BRANCH 283

Step 3: Configure Initial Settings for HQ_SW 284

Step 4: Configure Initial Settings for HQ-ASA 285

Step 5: Configure Clientless SSL VPN 286

Step 6: Configure Site-to-Site IPsec VPN 286

Step 7: Configure a Zone-Based Policy Firewall 288

Answers to CCNA Security Skills Practice 289

Step 1: Cable the Network As Shown in the Topology 289

Step 2: Configure Initial Settings for R1_BRANCH 289

Step 3: Configure Initial Settings for HQ_SW 290

Step 4: Configure Initial Settings for HQ-ASA 291

Step 5: Configure Clientless SSL VPN 293

Step 6: Configure Site-to-Site IPsec VPN 294

Step 7: Configure a Zone-Based Policy Firewall 295

Exam Day 299

What You Need for the Exam 299

What You Should Receive After Completion 299

Summary 300

Post-Exam Information 301

Receiving Your Certificate 301

U.S. Government Recognition 301

Examining Certification Options 302

If You Failed the Exam 302

Summary 302

Index 303

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

If you're reading this Introduction, you've probably already spent a considerable amount of time and energy pursuing your CCNA Security certification. Regardless of how you got to this point in your travels through your networking studies, *31 Days Before Your CCNA Security Exam* most likely represents the last leg of your journey on your way to the destination: to become CCNA Security certified.

However, if you happen to be reading this book at the beginning of your studies, then this book provides you with an excellent overview of the material you must now spend a great deal of time studying and practicing. But, I must warn you: Unless you are extremely well-versed in network security technologies and have considerable experience as a network technician or administrator, this book will not serve you well as the sole resource for CCNA Security exam preparation. I know this first hand. I recently took the CCNA Security exam and was impressed with both the breadth and depth of knowledge required to pass. I have been teaching, writing about, and implementing networks for almost two decades. And yet, there was a moment during the CCNA Security exam where I thought, "Wow, this is really a tough exam!"

You see, Cisco states that for the CCNA Security exam, you must "demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats." You simply cannot just study this content. You must practice it. Although I have a solid understanding of network security concepts and technologies, I also have extensive experience implementing and troubleshooting network security. That's why I was able to successfully pass the exam. There really is no other way to correctly answer the many scenario-based questions a candidate will receive during the exam than to have experienced the same or similar scenario in the real world or a lab simulation.

Now that I've sufficiently challenged you, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press offers an abundance of network security books and resources to serve you well as you learn how to install, troubleshoot, and monitor network devices to maintain the integrity, confidentiality, and availability of data and devices. Most of the resources can be purchased in book form or as eBooks for your tablet reader or mobile device by visiting www.ciscopress.com.

Safari Books Online

All the resources I reference in the book are available with a subscription to Safari Books Online (https://www.safaribooksonline.com). If you don't have an account, you can try it free for ten days.

Primary Resources

First on the list is the *CCNA Security 210-260 Official Cert Guide*, written by Omar Santos and John Stuppi. The authors have done an outstanding job of gathering together and organizing all the material you need to study for the CCNA Security certification exam. It is available in print (ISBN: 978158720568) and Premium Edition eBook (ISBN: 9780134077895) versions. The print version comes with the Pearson IT Certification Practice Test engine and two practice exams, as well as 90 minutes of video training. The Premium Edition eBook version comes with four practice exams, multiplatform accessibility, and performance tracking.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the CCNA Security curriculum and the wildly popular Packet Tracer network simulator. The course provides an introduction to the core security concepts and skills needed for the installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices. The course helps students learn how to secure Cisco routers, implement AAA, configure ACLs, mitigate common Layer 2 attacks, implement Cisco IOS firewall features, implement site-to-site VPNs, and implement remote-access VPNs. To learn more about the CCNA Security course and to find an Academy near you, visit http://www.netacad.com. Cisco Press also produces a printed course booklet (ISBN: 9781587133510) and lab manual (ISBN: 9781587133503) to accompany the CCNA Security Networking Academy course.

Supplemental Resources

In addition to the book you hold in your hands and to those mentioned previously, there are three more supplemental resources I would recommend to augment your final 31 days of review and preparation.

Omar Santos, Aaron Woland, and Mason Haris recorded more than 13 hours of video in their *CCNA Security 210-260 Complete Video Course* (ISBN: 9780134499314), which is available free with your Safari Books Online account. You can also purchase it separately from Cisco Press. The authors talk you through the full range of topics on the CCNA Security exam using a variety of presentation styles, including live instructor whiteboarding, real-world demonstrations, animations of network activity, dynamic KeyNote presentations, and doodle videos. They also demonstrate router, switch, and ASA CLI/ASDM configuration and troubleshooting in real lab environments, enabling you to learn both the concepts and the hands-on application.

Cisco Press has recently published the second edition of the very popular *CCNA Security Portable Command Guide* (ISBN: 9781587205750), by Bob Vachon. This book summarizes all the relevant Cisco IOS Software security commands, keywords, command arguments, and associated prompts, and offers tips and examples for applying these commands to real-world security challenges. Bob also includes ASDM screenshots to help when configuring the Cisco ASA.

The second book I would suggest is *Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services*, Third Edition (ISBN: 9781587143076), written by Jazib Frahim, Omar Santos, and Andrew Ossipov. This is an amazingly detailed resource (1248 pages!) on configuring, monitoring, and troubleshooting the entire Cisco ASA firewall family. True, it goes beyond the CCNA Security exam topics, but if you're a geek like me, you'll enjoy delving more deeply into the ASA with this book.

I occasionally reference other Cisco Press books for more specific topics. The simplest way to access this extra content is with a Safari Books Online subscription.

So, which resources should you buy? That question is largely up to how deep your pockets are or how much you like books. If you're like me, you want it all...online access for mobile and tablet reading, as well as hard copies for intensive study sessions with a pencil in hand. I admit it; my bookcase is a testament to my "geekness." But that's not practical for most students. So if you are on a budget, then choose one of the primary study resources and one of the supplemental resources, such as the *CCNA Security 210-260 Official Cert Guide* and the *CCNA Security Portable*

Command Guide. Whatever you choose, you will be in good hands. Any or all of these authors will serve you well.

Goals and Methods

The main goal of this book is to provide you with a clear and succinct review of the CCNA Security exam objectives. Each day's exam topics are grouped into a common conceptual framework and uses the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CCNA Security IINS 210-260 exam topics to be reviewed
- A Key Topics section to introduce the review material and quickly orient you to the day's focus
- An extensive review section consisting of short paragraphs, lists, tables, examples, and graphics
- A Study Resources section to provide you a quick reference for locating more in-depth treatment of the day's topics (as introduced in the previous section)

The book counts down starting with Day 31 and continues through exam day to provide post-test information. You will also find a calendar and checklist inside the book that you can tear out and use during your exam preparation.

Use the calendar to enter each actual date beside the countdown day and the exact day, time, and location of your CCNA Security exam. The calendar provides a visual for the time that you can dedicate to each CCNA Security exam topic.

The checklist highlights important tasks and deadlines leading up to your exam. Use it to help map out your studies.

Who Should Read This Book?

The audience for this book is anyone finishing their preparation for taking the CCNA Security IINS 210-260 exam. A secondary audience is anyone who needs a refresher review of CCNA Security exam topics, perhaps before attempting to recertify.

Getting to Know the CCNA Security IINS 210-260 Exam

Cisco launched the newest version of the CCNA Security exam, numbered 210-260, on September 1, 2015. The exam tests the candidate's knowledge of secure network infrastructure, core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, and endpoint security. It also validates skills for installation, troubleshooting, and monitoring of a secure network to maintain integrity, confidentiality, and availability of data and devices. As a prerequisite, Cisco states that a candidate must be CCENT or CCNA Routing and Switching certified before attempting the exam.

Currently for the CCNA Security exam, you are allowed 90 minutes to answer 60 to 70 questions. Most recently, a passing score is 860 on a scale of 300 to 1000, but the passing score often rises as the exam matures. If you've never taken a certification exam before with Pearson VUE, there is a 2 minute 45 second video titled What to Expect in a Pearson VUE Test Center that nicely summarizes the experience: https://home.pearsonvue.com/test-taker/security.aspx. You can also search for it on YouTube.

When you get to the testing center and check in, the proctor verifies your identity, gives you some general instructions, and then takes you into a quiet room containing a PC. When you're at the PC, you have a few things to do before the timer starts on your exam. For instance, you can take the tutorial to get accustomed to the PC and the testing engine. Every time I sit for an exam, I go through the tutorial even though I know how the test engine works. It helps me settle my nerves and get focused. Anyone who has user-level skills in getting around a PC should have no problems with the testing environment.

What Topics Are Covered on the CCNA Security

Table I-1 summarizes the seven domains of the CCNA Security exam.

Table I-1 CCNA Security IINS 210-260 Exam Domains and Weightings

Domain	% of Examination
1.0 Security Concepts	12%
2.0 Secure Access	14%
3.0 VPN	17%
4.0 Secure Routing and Switching	18%
5.0 Cisco Firewall Technologies	18%
6.0 IPS	9%
7.0 Content and Endpoint Security	12%
Total	100%

Registering for the CCNA Security IINS 210-260 Exam

If you are starting 31 Days Before Your CCNA Security Exam today, register for the exam right now. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet it's the same for you. Don't worry about unforeseen circumstances. You can cancel your exam registration for a full refund up to 24 hours before taking the exam. So if you're ready, then you should gather the following information and register right now!

- Legal name
- Social Security or passport number
- Company name
- Valid email address
- Method of payment

You can schedule your exam at any time by visiting www.pearsonvue.com/cisco/. I recommend you schedule it now for 31 days from now. The process and available test times will vary based on the local testing center you choose.

Digital Study Guide

Cisco Press offers this book in an online digital format that includes enhancements such as video, activities, and Check Your Understanding questions—plus Packet Tracer activities and a full-length exam.

> *31 Days Before Your CCNA Security Certification Exam Digital Study Guide* is available for a discount for anyone who purchases this book. There are details about redeeming this offer in the back of the book. If you are reading this in eBook format, please see the instructions below to access the companion website to get the discount offer.

- **Read** the complete text of the book on any web browser that supports HTML5, including mobile.
- **Watch** unique embedded videos (totaling more than 5 hours of video instruction) that demonstrate tasks, explain important topics, and visually describe key CCNA Security exam objectives.
- **Reinforce** key concepts with more than 31 dynamic and interactive hands-on exercises, and see the results with the click of a button. Also included are 7 Packet Tracer activities.

To get your copy of Packet Tracer software please go to the companion website for instructions. To access this companion website, follow these steps:

1. Go to www.ciscopress.com/register and log in or create a new account.
2. Enter the ISBN: 9781587205781.
3. Answer the challenge question as proof of purchase.
4. Click on the Access Bonus Content link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Test your understanding of the material at the end of each day with more than 300 fully interactive online quiz questions, PLUS a full-length final quiz of 60 questions that mimic the type you will see in the CCNA Security certification exam.

Throughout this book there are references to the Digital Study Guide enhancements that look like this:

Video: Data Encapsulation Summary

Refer to the Digital Study Guide to view this video.

Activity: Identify the Encapsulation Layer

Refer to the Digital Study Guide to complete this activity.

Check Your Understanding

Refer to the Digital Study Guide to take a 10-question quiz covering the content of this day.

When you are at these points in the Digital Study Guide you can start the enhancement.

Cryptographic Technologies

CCNA Security 210-260 IINS Exam Topics

- 1.3.a Describe key exchange
- 1.3.b Describe hash algorithm
- 1.3.c Compare and contrast symmetric and asymmetric encryption
- 1.3.d Describe digital signatures, certificates, and PKI

Key Topics

Today we will review cryptographic technologies and terminology. In particular, we will look at understanding the challenges of secure key management within a network environment. As well, we will review the different types of hashing algorithms in use today for data integrity. We will compare and contrast symmetric and asymmetric encryption algorithms, and finally delve into digital signatures and certificates. We will review PKI tomorrow.

CIA Triad

Before looking at the different cryptographic technologies in use today, it is important to understand the basic premise of cryptography itself. *Cryptography* is the practice and study of techniques to secure communications in the presence of third parties. Historically, cryptography was synonymous with encryption. Its goal was to keep messages private. Today, cryptography includes other responsibilities:

- **Confidentiality:** Uses encryption algorithms to encrypt and hide data
- **Data integrity:** Uses hashing algorithms to ensure that data is unaltered during any operation
- **Authentication:** Ensures that any messages received were actually sent from the perceived origin

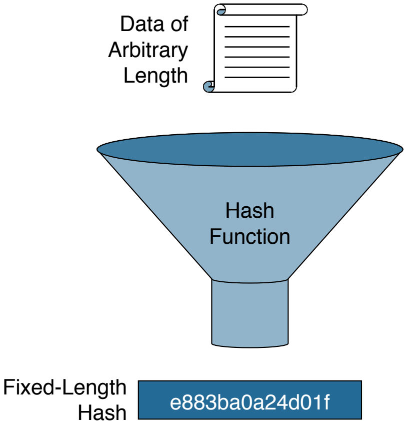
Key Exchange and Management

Key management deals with the secure generation, verification, exchange, storage, and destruction of keys. It is extremely important to have secure methods of key management. Key exchange and management are often considered the most difficult part of designing a cryptosystem. Many cryptosystems have failed because of mistakes in their key management, and all modern cryptographic algorithms require key management procedures. The basic components of any key management system include (1) automated and randomized key generation, (2) key strength verification, (3) encrypted key storage, (4) secure key exchange, (5) short key lifetimes, and (6) revocation and destruction of compromised or expired keys.

Hash Algorithms

Hashing is a mechanism that is used for data integrity assurance. Hashing is based on a one-way mathematical function that is relatively easy to compute but significantly difficult to reverse. Figure 29-1 illustrates how hashing is performed. Data of an arbitrary length is input into the hash function, and the result of the hash function is the fixed-length hash, which is known as the "digest" or "fingerprint."

Figure 29-1 Hash Function



Well-known Hash Functions

Hash functions are helpful when ensuring data is not changed accidentally, such as by a communication error. Although hashing can be used to detect *accidental* changes, it cannot be used to guard against deliberate changes. There is no unique identifying information from the sender in the hashing procedure. Therefore, hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data.

The following are the three most commonly used cryptographic hash functions:

- **Message Digest 5 (MD5):** MD5 is a one-way function that makes it easy to compute a hash from the given input data but makes it very difficult to compute input data given only a hash value. MD5 produces a 128-bit hash and is now considered a legacy algorithm that should be avoided.

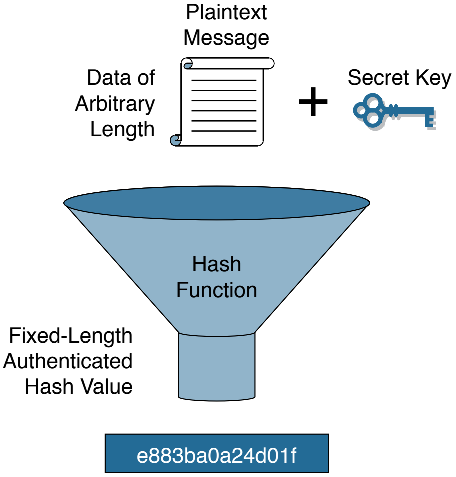
- **Secure Hash Algorithm 1 (SHA-1):** SHA-1 takes a message of up to 2^64 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks. It is now considered legacy and should be avoided when possible.
- **Secure Hash Algorithm 2 (SHA-2):** SHA-2 algorithms are the secure hash algorithms that the U.S. government requires by law for use in certain applications. The SHA-2 family includes 224-bit, 256-bit, 384-bit, and 512-bit functions. When choosing a hashing algorithm, use SHA-256 or higher, as they are currently the most secure.

CAUTION: Security flaws were discovered in SHA-1 and MD5. Therefore, it is now recommended that these algorithms be avoided.

Authentication Using Hashing

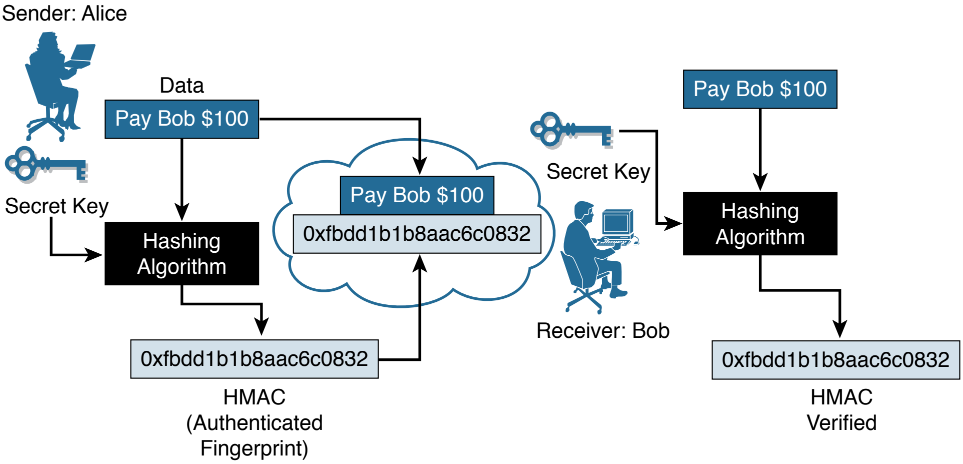
Two systems that have agreed on a secret key can use the key along with a hash function to verify data integrity of communication between them by using a keyed hash. A message authentication code is produced by passing the message data along with the secret key through a hash algorithm. Only the sender and the receiver know the secret key, and the output of the hash function now depends on the message data and the secret key. Figure 29-2 illustrates how the message authentication code is created. Data of an arbitrary length is input into the hash function, together with a secret key. The result is the fixed-length hash that depends on the data and the secret key. This type of authentication is referred to as keyed-hash message authentication code (HMAC) and adds authentication to integrity assurance.

Figure 29-2 HMAC Hashing



HMAC functions can be used with MD5 (HMAC-MD5) or SHA-1 (HMAC-SHA-1).
Figure 29-3 illustrates cryptographic authentication in action. The sender, Alice, wants to ensure that the message is not altered in transit and wants to provide a way for the receiver, Bob, to authenticate the origin of the message.

Figure 29-3 HMAC in Action



Alice inputs data and the secret key into the hashing algorithm and calculates the fixed-length message authentication code, or fingerprint. This authenticated fingerprint is then attached to the message and sent to Bob. Bob removes the fingerprint from the message and uses the received message with his copy of the secret key as input to the same hashing function. If the fingerprint that is calculated is identical to the fingerprint that was received, then data integrity has been verified. Also, the origin of the message is authenticated, because only Alice possesses a copy of the shared secret key.

Hashing in Cisco Products

Cisco products use hashing for entity authentication, data integrity, and data authenticity purposes such as

- IPsec gateways and clients use hashing algorithms to verify packet integrity and authenticity.
- Cisco IOS routers use keyed hashing with secret keys to add authentication information to routing protocol updates.
- Cisco software images that you can download from Cisco.com have MD5 and SHA-512 based checksums available, so that customers can check the integrity of downloaded images.

Symmetric and Asymmetric Encryption

Before diving into the differences between symmetric and asymmetric encryption algorithms, let's first start by reviewing the basic concepts of encryption itself.

Encryption Overview

Encryption is the process of disguising a message in such a way as to hide its original contents. With encryption, the plaintext readable message is converted to ciphertext, which is the unreadable, "disguised" message. Decryption reverses this process. Encryption is used to guarantee confidentiality so that only authorized entities can read the original message.

Encryption can provide confidentiality at different network layers, such as the following:

- Encrypting application layer data, such as encrypting email messages with Pretty Good Privacy (PGP)
- Encrypting session layer data using a protocol such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS)
- Encrypting network layer data using protocols such as those provided in the IP security (IPsec) protocol suite
- Encrypting data link layer data using proprietary link-encrypting devices

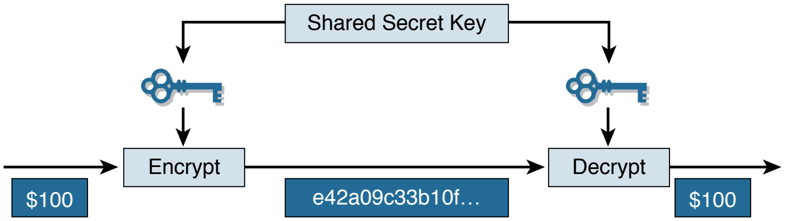
A good cryptographic algorithm is designed in such a way that it resists common cryptographic attacks. Variable key lengths and scalability are also desirable attributes of a good encryption algorithm. A key is a required parameter for encryption algorithms to encrypt and decrypt a message. The key is the link between the plaintext and ciphertext. There are two classes of encryption algorithms, which differ in their use of keys:

- **Symmetric encryption algorithms:** Use the same key to encrypt and decrypt data
- **Asymmetric encryption algorithms:** Use different keys to encrypt and decrypt data

Symmetric Encryption Algorithms

Symmetric, or secret key, encryption is the most commonly used form of cryptography because the shorter key length increases the speed of execution. The typical key-length range of symmetric encryption algorithms is 40 to 256 bits. Figure 29-4 illustrates an example of symmetric encryption in action.

Figure 29-4 Symmetric Encryption Example



In this example, the same key is used to encrypt the data by the sender and decrypt the data by the recipient.

With symmetric encryption, key management can be a challenge. The encryption and decryption keys are the same. The sender and the receiver must exchange the symmetric, secret key using a secure channel before any encryption can occur.

Table 29-1 provides a summary of the types of symmetric encryption algorithms in use today and their respective key lengths.

Table 29-1 Symmetric Encryption Algorithms

Symmetric Encryption Algorithm	Key Length (in bits)
DES	56
3DES	112 and 168
AES	128, 192, and 256
SEAL	160
RC	RC2 (40 and 64)
	RC4 (1 to 256)
	RC5 (0 to 2040)
	RC6 (128, 192, and 256)

DES is considered a legacy algorithm and is vulnerable to brute-force attacks. One way to increase the effectiveness of DES, without changing the well-analyzed algorithm itself, is to use the same algorithm with different keys several times in a row. The technique of applying DES three times in a row to a plaintext block is called *3DES*. Brute-force attacks on 3DES are considered unfeasible today. Because the basic algorithm has been well tested in the field for more than 35 years, it is considered very trustworthy. For several years, it was recognized that DES would eventually reach the end of its usefulness. In 1997, the *AES* initiative was announced. AES was chosen to replace DES and 3DES, because the key length of AES is much stronger than that of DES, and AES runs faster than 3DES on comparable hardware.

Video: Symmetric Encryption Demonstration

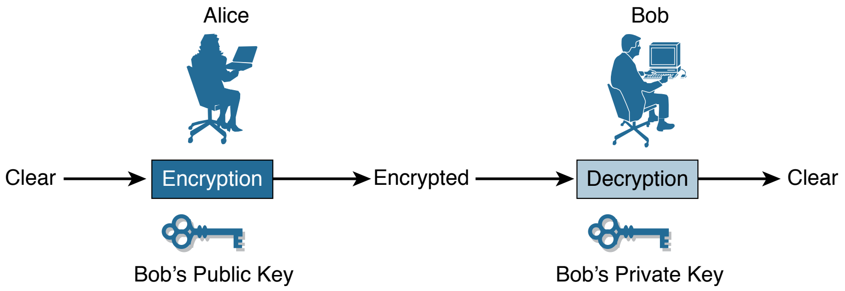
Refer to the Digital Study Guide to view this video.

Asymmetric Encryption Algorithms

Asymmetric encryption algorithms use a pair of keys to encrypt and decrypt data. Secure messages can be exchanged without having to have a pre-shared key. Because neither party has a shared secret, very long key lengths must be used. These algorithms are resource intensive and slower to execute. Most commonly, an entity with a key pair will share one of the keys (the public key) and keep the other key in complete secrecy (the private key). The private key cannot, in any reasonable amount of time, be calculated from the public key. Data that is encrypted with the private key requires the public key to decrypt. Vice versa, data that is encrypted with the public key requires the private key to decrypt. Asymmetric encryption is also known as public key encryption.

Here is one possible scenario of asymmetric encryption in action. In Figure 29-5, imagine that Bob has generated a public/private key pair. Bob keeps the private key totally secret but publishes the public key so it is available to everyone. Alice has a message that she wants to send to Bob in private. If Alice encrypts the message using Bob's public key, only Bob has the private key that is required to decrypt the message, providing confidentiality.

Figure 29-5 Asymmetric Encryption Example



The following table provides a detailed comparison between symmetric and asymmetric encryption algorithms:

Asymmetric Encryption Algorithm	Key Length (in bits)
DH	512, 1024, 2048, 3072, 4096
DSS and DSA	512–1024
RSA	512–2048
ElGamal	512–1024
Elliptical curve techniques	160

Four protocols that use asymmetric encryption algorithms are

- **Internet Key Exchange (IKE):** A fundamental component of IPsec VPNs
- **Secure Sockets Layer (SSL):** Now implemented as IETF standard TLS
- **Secure Shell (SSH):** Provides a secure remote-access connection to network devices
- **Pretty Good Privacy (PGP):** A computer program that provides cryptographic privacy and authentication

Video: Asymmetric Encryption Demonstration

Refer to the Digital Study Guide to view this video.

Activity: Compare Symmetric and Asymmetric Encryption Algorithms

Refer to the Digital Study Guide to complete this activity.

Digital Signatures and RSA Certificates

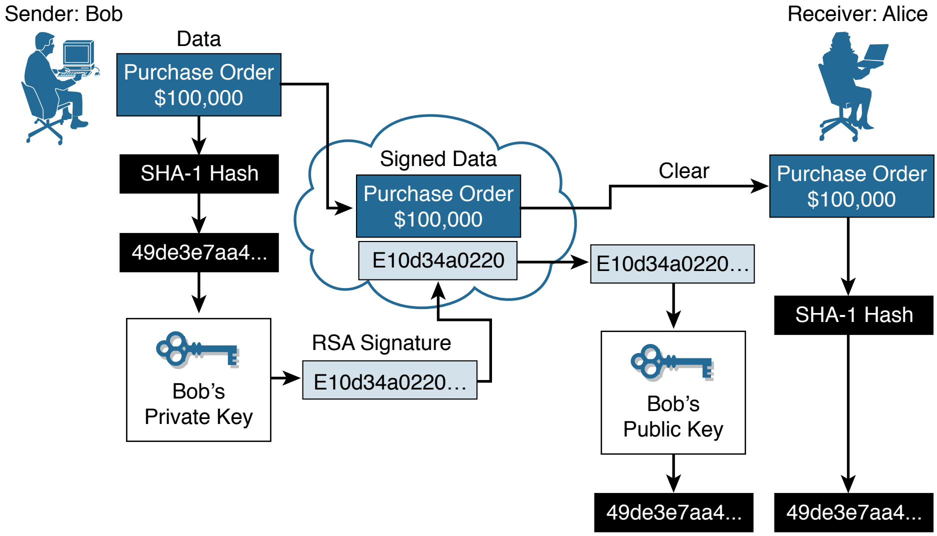
Digital signatures provide the same functionality as handwritten signatures. Specifically, they are a mathematical technique used to provide three basic security services: authenticates a source, proving that a certain party has seen and signed the data in question; guarantees that the data has not changed from the time it was signed; proves to a third party that the data exchange did take place.

Digital signatures are commonly used in code signing (to verify the integrity of downloaded files) and digital certificates (to verify the identity of an organization or individual). The basic four properties of digital signatures are that (1) the signature is authentic, (2) the signature is not forgeable, (3) the signature is not reusable, and (4) the signer cannot claim later that they did not sign it.

Digital certificates are used to authenticate and verify that a user sending a message is who they claim to be. Figure 29-6 shows how an RSA digital certificate or signature is used. RSA is an asymmetric algorithm that is commonly used for generating and verifying digital signatures. In this scenario, Bob is confirming an order with Alice. The steps are as follows:

1. Bob makes a hash, or fingerprint, of the document, which uniquely identifies the document and all its contents.
2. Bob encrypts the hash with only the private key of the signer (i.e., Bob's private key).

Figure 29-6 Using RSA Digital Signatures



3. The encrypted hash, which is known as the signature, is appended to the document.
4. Alice obtains Bob's public key.
5. Alice decrypts the signature using Bob's public key. This step reveals the hash value initially calculated by Bob.
6. Alice makes a hash of the received document, without its signature, and compares this hash to the decrypted signature hash sent by Bob. If the hashes match, the document is authentic. The match means that the document has been signed by Bob and has not changed since it was signed.

Study Resources

For today's exam topics, refer to the following resources for more study.

Resource	**Location**	**Topic**
CCNA Security Official Cert Guide	5	Fundamentals of VPN Technology and Cryptography
CCNA Security (Networking Academy Curriculum)	7	Cryptographic Systems
Supplemental Resources		
CCNA Security Complete Video Course	3	Fundamentals of VPN Technology and Cryptography
CCNA Security Portable Command Guide	14	VPNs and Cryptology
	15	Asymmetric Encryption and PKI

Check Your Understanding

Refer to the Digital Study Guide to take a ten-question quiz covering the content of this day.

This page intentionally left blank

Index

Numbers

3DES encryption algorithm, 16, 79

***31 Days Before Your CCNA Routing and Switching Exam*, 153**

802.1X
- authentication process, 61
- authentication servers, 62
- authenticators, 62
- configuring, 63-64
- end-to-end message exchange, 62
- supplicants, 62-63
- verifying, 64-65

A

AAA
- accounting
  - *server-based AAA, 54–55*
  - *start-stop records, 54*
  - *stop-only records, 54*
- ACS, 49
- authentication
  - *local AAA, 45-46*
  - *server-based AAA, 45-46, 51-53*
- authorization, server-based AAA, 53-54
- deploying, 51
- ISE, 49-50
- RADIUS, 46-48
- TACACS+, 46-48
- troubleshooting, 58
- verifying, 55-58

access
- attacks, 5
  - *baiting, 8*
  - *buffer overflow attacks, 6*
  - *defenses, 8*
  - *DHCP spoofing, 6*
  - *IP spoofing, 6*
  - *MAC spoofing, 6*
  - *malvertising, 8*
  - *man-in-the-middle attacks, 6*
  - *password attacks, 6*
  - *pharming, 7*
  - *phishing, 7*
  - *port redirection, 6*
  - *pretexting, 7*
  - *smishing, 8*
  - *something for something, 8*
  - *spam, 8*
  - *spear phishing, 7*
  - *tailgating, 8*
  - *trust exploitation, 6*
  - *vishing, 8*
  - *whaling, 7*
- control, data loss/exfiltration, 9
- device access
  - *IOS authorization with privilege levels, 137-138*
  - *IOS file authenticity, 140-142*
  - *IOS resilient configuration, 139-140*
  - *RBAC, 138-139*
- privilege levels, 138
- security, configuring, 36-37

accounting, server-based AAA, 54-55

ACL (Access Control Lists)
ASA Firewall, 233-234
Cisco IOS ACL, 175-176
crypto ACL
configuring, 118
IOS CLI-based site-to-site IPsec VPN, 117-118
firewalls
packet filtering, 183-185
stateful firewalls, 187
IOS CLI-based site-to-site IPsec VPN, 115
PACL, 175-177
VACL, 175-176
configuring, 177-178
verifying, 178

ACS (Access Control Servers), 49

active/active failover model (ASA high availability), 223

active/standby failover model (ASA high availability), 223

ActiveX, AnyConnect SSL VPN, 106

addressing schemes skills practice, 282

advertising and malvertising, 8

adware, 9

AES encryption algorithm, 16, 79

Aggressive mode (IKEv1), 83

AH (Authentication Header)
IPsec, 77-79
transport mode, 79
tunnel mode, 79

alerts, IDS/IPS, 255

Always-on VPN, 134

AMP (Advanced Malware Protection), 278-279
ESA, 264
file reputation, 264
file retrospection, 265
file sandboxing, 265
IPS, 256

amplification attacks, 7

anomaly detection (IDS), 247

antimalware
AMP, 256, 278-279
ESA, 264
file reputation, 264
file retrospection, 265
file sandboxing, 265
endpoint security, 275, 278-279
ESA, 264

antiphishing defenses, 8

anti-replay protection, IPsec, 76

antispyware, endpoint security, 275-277

antivirus software, 8
endpoint security, 275-277
ESA, 264-266
McAfee Antivirus, 266
Sophos Antivirus, 266

AnyConnect Secure Mobility Client
AnyConnect SSL VPN, 100
split tunneling, 132
Standalone mode, 100
WebLaunch mode, 100

AnyConnect SSL VPN
authentication, 100
client IP address assignments, 100
configuring
ActiveX, 106
ASA configuration, 101-105
client configuration, 106
Java detection, 106
platform detection, 106
topology sample, 99
troubleshooting connections, 111
verifying configurations, 108-109

application inspection firewalls, 186

ARP spoofing, 155-156

ASA (Adaptive Security Appliance), 219
Always-on VPN, 134
AnyConnect SSL VPN, 99
client authentication, 100
client IP address assignments, 100
configuring, 101-106
server authentication, 100
AVC services, 221
Client U-turns, 132

clientless SSL VPN
configuring, 87-94
verifying configurations, 95-96
components of, 220-221
console ports, 221
contexts, 225
deploying, 222
DHCP server/client integration, 222
features of, 221
FirePOWER, 222
FirePOWER NGIPS, 189
high availability
active/active failover model, 223
active/standby failover model, 223
clustering, 223
with failover, 222-224
hairpinning, 131-132
Host Scan and VPN endpoint posture assessments, 135
identity firewalls, 222
IP routing, 222
IPS deployment, 247-249
lock slots, 221
management ports, 221
NAT, 193-194
process of, 192
static NAT, 195-197
network data ports, 221
power cord sockets, 221
reset buttons, 221
services of, 222
site-to-site IPsec VPN, 122
configuring, 123-125
verifying, 125-128
split tunneling, 132
stateful packet inspection, 221
status LED, 220
USB ports, 221
virtualization, 222, 225

ASA Firewall
access rules, 232-234
ACL, 233-234
ASDM access rules, 233
ASDM object groups, 236-240
configuring, 227-229
FirePOWER, 228
Global configuration mode, 229
interfaces
ASDM DMZ configuration, 231
DMZ configuration, 231
security levels, 230
traffic flows, 231
management access, 229-230
MPF, 240-244
objects/object groups, 235-240
Privileged EXEC mode, 229
ROM monitor mode, 229
specific configuration mode, 229
User EXEC mode, 229

ASAv (Adaptive Security Virtual Appliance), 221

ASDM (Adaptive Security Device Manager)
ASDM site-to-site VPN wizard, 123
NAT
dynamic NAT configuration, 198-200
dynamic PAT configuration, 201-202
policy NAT configuration, 203-206
static NAT configuration, 196-197

assets, defining, 2

assigning views (CLI) to users, 139

asymmetric encryption, 15-17

attachments (email), data loss/exfiltration, 9

authentication
802.1X, 61
authentication process, 61
authentication servers, 62
authenticators, 62
configuring, 63-64
end-to-end message exchange, 62
supplicants, 62-63
verifying, 64-65
AnyConnect SSL VPN, 100
clientless SSL VPN, 89
cryptography and, 11-14
digital signatures, 18-19
ECDSA signatures, IPsec, 80
ESP, 78
hashing
Cisco products, 14
HMAC, 13-14
HMAC, 13-14, 80
IOS files, 140-142

IPsec
ECDSA signatures, 80
HMAC, 80
origin authentication, 76, 80
PSK, 80
RSA encrypted nonces, 80
RSA signatures, 80
keyed hashes (MAC), 143
local AAA, 45-46
MD5 authentication, 144-146
NTP, 43
origin authentication, IPsec, 76, 80
OSPF
MD5 authentication, 144-146
SHA authentication, 146-147
PKI CA, 27
PSK, IPsec, 80
routing protocols, 143
OSPF MD5 authentication, 144-146
OSPF SHA authentication, 146-147
RSA
certificates, 18-19
encrypted nonces, 80
signatures, IPsec, 80
server-based AAA, 45-46, 51-53
SHA authentication, OSPF, 146-147
two-factor authentication, 8

authentication servers (802.1X authentication), 62

authenticators (802.1X authentication), 62

authNoPriv mode (SNMPv3), 40

authorization
IOS, privilege levels, 137-138
RBAC, 138-139
server-based AAA, 53-54

authPriv mode (SNMPv3), 40

Auto NAT (NAT tables), 194

availability, CIA Triad, 1

AVC (Application Visibility and Control)
ASA and, 221
Cisco CWS, 274

B

baiting, 8

bidirectional NAT, 193

blacklisting (IPS), 256

block actions, IDS/IPS, 255

bookmarks, clientless SSL VPN configuration, 90-94

botnets, 6

BPDU guard, 154, 168

Branch/SOHO topologies, 29

buffer overflow attacks, 6

BYOD (Bring Your Own Device)
architecture of, 68-69
collaboration, 68
MDM, 69
cloud-based deployments, 70
onboarding new devices, 72
on-premises deployments, 70
mobile device security, 67
mobility, 67
network intelligence, 68

C

C3PL (Cisco Common Classification Policy Language), 211
class maps, 212-215
policy maps, 212-215
service policies, 213
ZPF configuration, 210, 216-218
class maps, 214-215
policy maps, 215

CA (Certificate Authorities), 21-22
certificates
authentication, 27
enrollment process, 27
retrieving, 26
CRL, 27
cross-certified CA topologies, 24
enrollment, 27
hierarchical CA topologies, 23
OCSP, 28
revocation, 27
SCEP, 27

cabling skills practice, 283

CAM table overflow attacks, 157

CAN (Campus-Area Networks), 28

***CCNA Routing and Switching 200-120 Official Cert Guide Library*, 153**

***CCNA Security 210-260 Official Cert Guide*, 153**

CCNA Security Skills Practice
addressing schemes, 282
cabling, 283
clientless SSL VPN configuration, 286, 293
HQ-ASA configuration, 285, 291-293
HQ_SW configuration, 284-285, 290-291
ISP configuration, 283
R1_BRANCH configuration, 283-284, 289-290
site-to-site IPsec VPN configuration, 286-288, 294-295
topologies, 281
zone-based policy firewall configuration, 288-289, 295-297

CDP (Cisco Discovery Protocol) reconnaissance, 157

CEF (Cisco Express Forwarding)
CEF-exception subinterface (CPPr), 151
FIB tables, 149

certificates, PKI, 22

certification (exams), 299
options of, 302
U.S. government recognition, 301
validation period, 301

change management and social engineering (access attacks), 8

CIA Triad, 1, 11

Cisco CWS (Cloud Web Security), 272-274

Cisco IOS ACL, 175-176

Cisco WSA (Web Security Appliance), 269-272

class maps
CSPL, ZPF configuration, 212-215
MPF, 241

CLI (Command Line Interface)
authorization
parser views, 138-139
RBAC, 138-139
superviews, 138
IOS CLI-based site-to-site IPsec VPN, 114
configuring, 115-119
verifying, 119-122

Client U-turns, 132

clientless SSL VPN, 86
configuring, 87
bookmark configuration, 90-94
interface configuration, 88
skills practice, 286, 293
URL configuration, 88
user authentication, 89
user group policy configuration, 90
SSL/TLS encapsulation, 85
verifying configurations, 95-96

clients, AnyConnect SSL VPN
authentication, 100
configuration, 106
IP address assignments, 100

cloud-computing
security, Cisco CWS, 272-274
storage devices, data loss/exfiltration, 9
topologies, 31

clustering (ASA high availability), 223

collaboration, BYOD deployments, 68

common threats
data loss/exfiltration, 9
malware, 8-9
network attacks
access attacks, 5-8
DDoS attacks, 6
DoS attacks, 6
reconnaissance attacks, 5

community ports (PVLAN), 172

confidentiality
CIA Triad, 1
cryptography and, 11
IPsec, 76, 79

configuring
802.1X, 63-64
access security (management plane), 36-37

ACL
  crypto ACL, 118
  PACL, 176-177
  VACL, 177-178
AnyConnect SSL VPN
  ASA configuration, 101-105
  client configuration, 106
ASA Firewall, 227-229
bookmarks, 90-94
clientless SSL VPN, 87
  bookmark configuration, 90-94
  interface configuration, 88
  skills practice, 286, 293
  URL configuration, 88
  user authentication, 89
  user group policy configuration, 90
CPPr, 151
crypto ACL, 118
crypto maps, 118-119
DAI, 163
DHCP snooping, 161
dynamic NAT, 198-200
dynamic PAT, 201
HQ-ASA skills practice, 285, 291-293
HQ_SW skills practice, 284-285, 290-291
IOS resilient configuration, 139-140
IP PACL, 176-177
IPSG, 165
ISAKMP policies, IOS CLI-based site-to-site IPsec VPN, 116
MAC PACL, 176
NAT
  dynamic NAT, 198-200
  dynamic PAT, 201
  policy NAT, 203-206
  static NAT, 195-197
Native VLAN, 179-180
PACL, 176-177
policy NAT, 203-206
port security, 166
privilege levels, 137-138
PSK, IOS CLI-based site-to-site IPsec VPN, 117
PVLAN, 173
PVLAN Edge, 174
R1_BRANCH skills practice, 283-284, 289-290
RBAC, 138-139
site-to-site IPsec VPN
  ASA site-to-site IPsec VPN, 123-125
  IOS CLI-based site-to-site IPsec VPN, 115-119
  skills practice, 286-288, 294-295
SNMP, 41-42
split tunneling, 133
SSH/HTTPS (management plane), 38
static NAT, 195-197
Syslog (management plane), 38-39
VACL, 177-178
VLAN
  Native VLAN, 179-180
  PVLAN, 173
  PVLAN Edge, 174
zone-based policy firewall skills practice, 288-289, 295-297
ZPL, 210, 216-218
  class maps, 214-215
  policy maps, 215

console ports, ASA, 221

content filtering, ESA, 266

control plane
CoPP, 150
CPPr, 151
defining, 149

CoPP (Control Plane Policing), 150-151

countermeasures, defining, 2

CPPr (Control Plane Protection), 151

CRL (Certificate Revocation Lists), PKI, 27

cross-certified CA PKI topologies, 24

crypto ACL
configuring, 118
IOS CLI-based site-to-site IPsec VPN, 117-118

crypto maps
configuring, 118-119
IOS CLI-based site-to-site IPsec VPN, 118-119
viewing, 120

cryptography
authentication and, 11-14
CIA Triad, 11
confidentiality and, 11

data integrity and, 11
digital signatures, 18-19
encryption
asymmetric encryption, 16-17
symmetric encryption, 15-16
hashing
MD5, 12-14
SHA-1, 13-14
SHA-2, 13
key exchange/management, 11
RSA certificates, 18-19
Suite B cryptographic standard, 81

CSD (Cisco Secure Desktop) and VPN endpoint posture assessments, 135

D

DAI (Dynamic ARP Inspection)
configuring, 163
verifying, 164

DAP (Dynamic Access Policies) and VPN, 135

data center topologies, 31

data encryption, endpoint security, 279

data integrity
CIA Triad, 1
cryptography and, 11
IPsec, 76, 79

data loss/exfiltration, 9

data packets, filtering, 183-185

data plane, 149

data ports (network), ASA, 221

DDoS attacks, 6

deploying
ASA, 222
firewalls, 181-182

DES encryption algorithm, 16, 79

detection technologies
alerts, 255
anomaly-based IDS, 253
anomaly-based IPS, 253
blocks, 255
drops, 255
monitors, 255
policy-based IDS, 253
policy-based IPS, 253
profile-based IDS, 253
profile-based IPS, 253
reputation-based IDS, 254
resets, 255
shuns, 255
signature-based IDS, 253-254
signature-based IPS, 253-254
trigger actions, 255

device access
IOS
authorization, privilege levels, 137-138
file authenticity, 140-142
resilient configuration, 139-140
RBAC, 138-139

DH encryption algorithm, 17

DH (Diffie-Hellman) key agreements, 81-83

DHCP (Dynamic Host Configuration Protocol)
ASA and, 222
snooping, 161-163
spoofing, 6, 158-159

digital signatures, 18-19

discs (hard copy storage) and data loss/exfiltration, 9

DLP (Data Loss Prevention), ESA, 264-266

DMZ (Demilitarized Zones)
ASA Firewall, ASDM DMZ interface configuration, 231
DMZ-private policies, ZPF, 210
security zones and, 3-4
servers, IPS, 250

DoS attacks, 6-7

drop actions, IDS/IPS, 255

DSA encryption algorithm, 17

DSS encryption algorithm, 17

dynamic NAT, 193
configuring, 198-200
verifying, 200

dynamic PAT (NAT Overload), 193
configuring, 201
verifying, 202

E

ECDH key agreements, 81

ECDSA signatures, IPsec authentication, 80

ElGamal encryption algorithm, 17

elliptical curve techniques, 17

email
- attachments, data loss/exfiltration, 9
- ESA
  - *antimalware protection, 264*
  - *antivirus protection, 264*
  - *deploying, 260-262*
  - *DLP, 264-266*
  - *email processing, 265-266*
  - *overview of, 259-260*
  - *spam filtering, 263*
- malware, 259
- phishing attacks, 259
- spam, 259, 265-266
- viruses, 259

encapsulation, ESP, 78

encryption
- asymmetric encryption, 15-17
- cryptography and, 15
  - *asymmetric encryption, 16-17*
  - *symmetric encryption, 15-16*
- endpoint security, 279
- IPsec, 79
- overview of, 15
- symmetric encryption, 15-16

endpoint posture assessments, VPN, 135

endpoint security
- antimalware, 275-279
- antispyware, 275-277
- antivirus software, 275-277
- data encryption, 279
- personal firewalls, 275-276

enterprise campuses (CAN), 28

ESA (Email Security Appliance)
- antimalware protection, 264
- antivirus protection, 264
- deploying, 260-262
- DLP, 264-266
- email processing, 265-266
- overview of, 259-260
- spam filtering, 263

ESP (Encapsulating Security Payload), 78

exams
- certification, 299
  - *options of, 302*
  - *U.S. government recognition, 301*
  - *validation period, 301*
- failing, 302
- preparing for
  - *items needed for exam day, 299*
  - *test proctors, 299*
- retaking, 302
- score reports, 299-301
- skills practice
  - *addressing schemes, 282*
  - *cabling, 283*
  - *clientless SSL VPN configuration, 286, 293*
  - *HQ-ASA configuration, 285, 291-293*
  - *HQ_SW configuration, 284-285, 290-291*
  - *ISP configuration, 283*
  - *R1_BRANCH configuration, 283-284, 289-290*
  - *site-to-site IPsec VPN configuration, 286-288, 294-295*
  - *topologies, 281*
  - *zone-based policy firewall configuration, 288-289, 295-297*

F

failing exams, 302

false positives/negatives (IPS), 250

FIB (Forwarding Information Base) tables and CEF, 149

files, AMP
- reputations, 264
- retrospection, 265
- sandboxing, 265

filtering
- security zone policies, 4
- URL filtering, Cisco CWS, 274

FirePOWER
- ASA, 222, 228
- IPS, 247-249
- NGIPS, 189, 256

firewalls
- application inspection firewalls, 186
- ASA, 219
  - *Access rules, 232-234*
  - *ACL, 233-234*
  - *ASDM access rules, 233*
  - *ASDM object groups, 236-240*
  - *AVC services, 221*
  - *components of, 220-221*
  - *configuring, 227-229*
  - *console ports, 221*
  - *contexts, 225*
  - *deploying, 222*
  - *DHCP server/client integration, 222*
  - *features of, 221*
  - *FirePOWER, 222, 228*
  - *Global configuration mode, 229*
  - *high availability, 223*
  - *high availability with failover, 222-224*
  - *identity firewalls, 222*
  - *interfaces, 230-231*
  - *IP routing, 222*
  - *lock slots, 221*
  - *management access, 229-230*
  - *management ports, 221*
  - *MPF, 240-244*
  - *network data ports, 221*
  - *objects/object groups, 235-240*
  - *power code sockets, 221*
  - *Privileged EXEC mode, 229*
  - *reset buttons, 221*
  - *ROM monitor mode, 229*
  - *services of, 222*
  - *Specific configuration mode, 229*
  - *stateful packet inspection, 221*
  - *status LED, 220*
  - *USB ports, 221*
  - *User EXEC mode, 229*
  - *virtualization, 222, 225*
- ASAv, 221
- benefits of, 182
- defining, 181
- deploying, 181-182
- identity firewalls, ASA, 222
- limitations of, 183
- next-generation firewalls, 188-189
- packet filtering, 183-185
- personal firewalls, 189, 275-276
- proxy servers, 185-186
- requirements of, 182
- security zones, 2
- stateful firewalls, 187
- zone-based policy firewall configuration skills practice, 288-289, 295-297
- ZPF
  - *benefits of, 210*
  - *C3PL and ZPF configuration, 210-211, 214-218*
  - *C3PL and ZPL configuration, 212-213*
  - *DMZ-private policies, 210*
  - *private-DMZ policies, 210*
  - *private-public policies, 210*
  - *public-DMZ policies, 209*
  - *self zones, 211*
  - *traffic flows, 209, 213-214*
  - *verifying, 217-218*
  - *zone pairs, 211, 214*
  - *zones, 211-214*

full tunnel SSL VPN, 87

G

GET messages (SNMP), 40

global addresses (inside/outside), NAT, 192

Global configuration mode (ASA Firewall), 229

GRE (Generic Routing Encapsulation), 73

group policies, clientless SSL VPN configuration, 90

H

hairpinning, 131-132

hard copy storage (paper/discs) and data loss/exfiltration, 9

hashing
- authentication
  - *Cisco products, 14*
  - *HMAC, 13-14*
- Cisco products, 14
- cryptography and, 12-14
- MD5, 12-14
- SHA-1, 13-14
- SHA-2, 13

hierarchical CA PKI topologies, 23

high availability, ASA
- active/active failover model, 223
- active/standby failover model, 223
- clustering, 223
- high availability with failover, 222-224

HMAC (Hash Message Authentication Code), 13-14, 80

Host Scan and VPN endpoint posture assessments, 135

host subinterface (CPPr), 151

HQ-ASA configuration skills practice, 285, 291-293

HQ_SW configuration skills practice, 284-285, 290-291

HTTP (Hypertext Transfer Protocol), 75

HTTPS (HTTP Secure), 38, 75

I

ICMP-type object groups (ASA Firewall), 235

identity firewalls, ASA, 222

IDS (Intrusion Detection Systems)
- alerts, 255
- anomaly-based IDS, 253
- anomaly detection, 247
- blocks, 255
- drops, 255
- IPS versus, 245-249
- monitors, 255
- network tap, 248
- policy-based IDS, 253
- profile-based IDS, 253
- promiscuous (passive) mode, 245
- reputation-based IDS, 254
- resets, 255
- rule-based detection, 247
- shuns, 255
- signature-based IDS, 253-254
- trigger actions, 255

IKE (Internet Key Exchange), 17
- IKEv1
  - *Aggressive mode, 83*
  - *IPsec and, 82-83*
  - *Main mode, 82*
  - *Quick mode, 83*
- IKEv2 and IPsec, 82-83

in-band management (secure management systems), 35-36

information classification/handling and social engineering (access attacks), 8

inline mode (IPS), 245

inside local/global addresses (NAT), 191

integrity (data)
- CIA Triad, 1
- cryptography and, 11
- IPsec, 76, 79

interfaces, clientless SSL VPN configuration, 88

Internet edges (CAN), 28

intranet data centers (CAN), 28

IOS
- authorization, privilege levels, 137-138
- CLI-based site-to-site IPsec VPN, 114
  - *ACL compatibility, 115*
  - *crypto ACL, 117-118*
  - *crypto maps, 118-119*
  - *IPsec transform sets, 117*
  - *ISAKMP policies, 115-117*
  - *verifying, 119-122*
- file authenticity, 140-142
- MD5 checksum, verifying, 140-141
- resilient configuration, 139-140
- ZPF
  - *benefits of, 210*
  - *C3PL and ZPF configuration, 210-218*
  - *C3PL and ZPL configuration, 212-218*
  - *DMZ-private policies, 210*
  - *private-DMZ policies, 210*
  - *private-public policies, 210*
  - *public-DMZ policies, 209*
  - *self zones, 211*
  - *traffic flows, 209, 213-214*
  - *verifying, 217-218*
  - *zone pairs, 211, 214*
  - *zones, 211-214*

IP (Internet Protocol). ***See also*** **IPsec**
- AnyConnect SSL VPN and client IP address assignments, 100
- PACL, configuring, 176-177

routing, ASA, 222
spoofing, 6

IPS (Intrusion Prevention Systems)
alerts, 255
AMP, 256
anomaly-based IPS, 253
blacklisting, 256
blocks, 255
deploying, 247-249
DMZ servers, 250
drops, 255
false positives/negatives, 250
FirePOWER
IPS, 247-249
NGIPS, 256
host-based IPS, 247-248
IDS versus, 245-249
inline mode, 245
inside networks, 250
monitors, 255
network-based IPS, 247-248
outside networks, 250
policy-based IPS, 253
profile-based IPS, 253
resets, 255
shuns, 255
signature-based IPS, 253-254
trigger actions, 255
true positives/negatives, 250

IPsec. *See also* IP
3DES, 79
AES, 79
AH, 77-79
anti-replay protection, 76
authentication
ECDSA signatures, 80
HMAC, 80
origin authentication, 76, 80
PSK, 80
RSA encrypted nonces, 80
RSA signatures, 80
Client U-turns, 132
confidentiality, 76, 79
crypto maps, 118-120
data integrity, 76, 79
DES, 79
encryption, 79
ESP, 78
framework of, 76-77
hairpinning, 131-132
HMAC, 80
IKEv1, 82-83
IKEv2, 82-83
key management, 76, 80-81
operation modes, 78-79
SEAL, 79
site-to-site VPN
ASA site-to-site IPsec VPN, 122-128
IOS CLI-based site-to-site IPsec VPN, 114-122
negotiations, 113-114
Suite B cryptographic standard, 81
transform sets, IOS CLI-based site-to-site IPsec VPN, 117
VPN, 73-74, 286-288, 294-296

IPSG (IP Source Guard), 164-165

ISAKMP (Internet Security Association and Key Management Protocol)
IKE and, 82
IOS CLI-based site-to-site IPsec VPN, 115-117

ISE (Identity Services Engines), 49-50

isolated ports (PVLAN), 171

ISP configuration skills practice, 283

J

Java detection, AnyConnect SSL VPN, 106

Johnson, Allan, 153

K

key exchange/management and cryptography, 11

key management
DH key agreements, 81-83
ECDH key agreements, 81
IPsec, 76, 80-81

keyed hashes (MAC), 143

L

Layer 2 network security
- ARP spoofing, 155-156
- BPDU guard, 154, 168
- CAM table overflow attacks, 157
- CDP reconnaissance, 157
- DAI
  - *configuring, 163*
  - *verifying, 164*
- DHCP
  - *snooping, 161-163*
  - *spoofing, 158-159*
- IPSG, 164-165
- LLDP reconnaissance, 157
- loop guard, 154, 168
- MAC spoofing, 156
- port security, 165-167
- PortFast, 154, 167
- root guard, 154, 168
- STP attacks, 153-154
- VLAN hopping attacks, 157-158

LED (status), ASA, 220

legacy VPN, 74

LLDP (Link-Layer Discovery Protocol) reconnaissance, 157

local AAA authentication, 45-46

local addresses (inside/outside), NAT, 191

lock slots, ASA, 221

loop guard, 154, 168

M

MAC (Message Authentication Code), 143
- MAC addresses
  - *port security, 165-167*
  - *spoofing, 6, 156*
- MAC PACL, 176

Main mode (IKEv1), 82

malvertising, 8

malware
- adware, 9
- AMP, 278-279
  - *ESA, 264*
  - *file reputation, 264*
  - *file retrospection, 265*
  - *file sandboxing, 265*
  - *IPS, 256*
- antimalware, ESA, 264
- email, 259
- endpoint security, 275, 278-279
- ransomware, 9
- scareware, 9
- spyware, 9
- Trojan horses, 9
- viruses, 8
- worms, 9

man-in-the-middle attacks, 6

management consoles, 246

management plane
- access security, configuring, 36-37
- defining, 149
- in-band management, 35-36
- NTP, 42-43
- OOB management, 35-36
- SCP, 43-44
- SNMP
  - *agents, 39*
  - *authNoPriv mode, 40*
  - *authPriv mode, 40*
  - *configuring, 41-42*
  - *GET messages, 40*
  - *managers, 39*
  - *MIB, 40*
  - *noAuthNoPriv mode, 40*
  - *SET messages, 40*
  - *trap messages, 40*
  - *versions of, 40-41*
- SSH/HTTPS, 38
- Syslog, 38-39

management ports, ASA, 221

Manual NAT (NAT tables), 194

Manual NAT after Auto NAT (NAT tables), 195

McAfee Antivirus, 266

MD5 (Message Digest 5), 12-14

MD5 authentication, OSPF authentication, 144-146

MDM (Mobile Device Management) and BYOD, 69
- cloud-based deployments, 70
- onboarding new devices, 72
- on-premises deployments, 70

message filtering, ESA, 265

MIB (Management Information Base) in SNMP, 40

mobile devices and BYOD
deployments, 67
MDM and, 69-72
mobile device security, 67

monitor actions, IDS/IPS, 255

MPF (Modular Policy Frameworks), ASA MPF, 240-244

MPLS VPN (Multiprotocol Label Switching VPN), 73

MQC (Modular QoS CLI), 151

N

NAC (Network Admission Control) and VPN endpoint posture assessments, 135

NAT (Network Address Translation), 191
AnyConnect SSL VPN configuration, 104
ASA NET, 192-197
bidirectional NAT, 193
dynamic NAT, 193
configuring, 198-200
verifying, 200
dynamic PAT (NAT Overload), 193
configuring, 201
verifying, 202
exemptions, ASA site-to-site IPsec VPN, 125
global addresses (inside/outside), 192
local addresses (inside/outside), 191
NAT tables, 194
outside NAT, 193
policy NAT, 193
configuring, 203-206
verifying, 206
process of, 192
reference topology, 195
static NAT, 193
configuring, 195-197
verifying, 197
static PAT, 193

NAT-T (NAT Traversal), 134

Native VLAN, 178-180

network object groups (ASA Firewall), 235

network objects (ASA Firewall), 235

networks
attacks
access attacks, 5-6
DDoS attacks, 6
DoS attacks, 6-7
reconnaissance attacks, 5
botnets, 6
Branch/SOHO topologies, 29
BYOD deployments, 68
CAN, 28
cloud topologies, 31
control plane
CoPP, 150
CPPr, 151
defining, 149
data center topologies, 31
data plane, 149
data ports, ASA, 221
Layer 2 security
ARP spoofing, 155-156
BPDU guard, 154, 168
CAM table overflow attacks, 157
CDP reconnaissance, 157
DAI, 163-164
DHCP snooping, 161-163
DHCP spoofing, 158-159
IPSG, 164-165
LLDP reconnaissance, 157
loop guard, 154, 168
MAC spoofing, 156
port security, 165-167
PortFast, 154, 167
root guard, 154, 168
STP attacks, 153-154
VLAN hopping attacks, 157-158
management plane, defining, 149
taps, IDS, 248
virtual network topologies, 31
WAN topologies, 29

next-generation firewalls, 188-189

noAuthNoPriv mode (SNMPv3), 40

NTP (Network Time Protocol), 42-43

O

OCSP (Online Certificate Status Protocol), PKI, 28

Odom, Wendell, 153

OOB (Out-Of-Band) management (secure management systems), 35-36

origin authentication, IPsec, 76, 80

OSPF (Open Shortest Path First) authentication
- MD5 authentication, 144-146
- SHA authentication, 146-147

outbreak filtering, ESA, 266

outside local/global addresses (NAT), 192

outside NAT, 193

P

packets (data)
- filtering, 183-185
- inspection, ASA, 221

PACL (Port ACL), 175-177

paper (hard copy storage) and data loss/exfiltration, 9

parser views (CLI), 138-139

passive (promiscuous) mode (IDS), 245

passwords
- attacks, 6
- data loss/exfiltration, 9
- managing, 8

personal firewalls, 189, 275-276

PGP (Pretty Good Privacy), 17

pharming attacks, 7

phishing attacks, 7
- antiphishing defenses, 8
- email, 259

ping of death, 7

PKCS (Public-Key Cryptography Standards), 25

PKI (Public Key Infrastructure)
- CA, 21-22
  - *certificate authentication, 27*
  - *certificate enrollment process, 27*
  - *CRL, 27*
  - *cross-certified CA topologies, 24*
  - *enrollment, 27*
  - *hierarchical CA topologies, 23*
  - *OCSP, 28*
  - *retrieving certificates, 26*
  - *revocation, 27*
  - *SCEP, 27*
- components of, 22
- CRL, 27
- cross-certified CA topologies, 24
- hierarchical CA topologies, 23
- OCSP, 28
- operations, 25-27
- PKCS, 25
- RA, 24
- single-root topologies, 23
- X.509 standard, 25

PKIX (PKI X.509), 24

platform detection, AnyConnect SSL VPN, 106

policy maps
- CSPL, ZPF configuration, 212-215
- MPF, 241

policy NAT, 193
- configuring, 203-206
- verifying, 206

PortFast, 154, 167

ports
- authentication. *See* 802.1X
- community ports (PVLAN), 172
- console ports, ASA, 221
- isolated ports (PVLAN), 171
- management ports, ASA, 221
- network data ports, ASA, 221
- promiscuous ports (PVLAN), 171
- PVLAN Edge, 174-175
- redirection, 6
- security, 165-167
- SPAN, 248
- USB ports, ASA, 221

power cord sockets, ASA, 221

practicing skills (exam preparation)
- addressing schemes, 282
- cabling, 283
- clientless SSL VPN configuration, 286, 293

- HQ-ASA configuration, 285, 291-293
- HQ_SW configuration, 284-285, 290-291
- ISP configuration, 283
- R1_BRANCH configuration, 283-284, 289-290
- site-to-site IPsec VPN configuration, 286-288, 294-295
- topologies, 281
- zone-based policy firewall configuration, 288-289, 295-297

preparing for exams
- items needed for exam day, 299
- test proctors, 299

pretexting, 7

principles of security
- CIA Triad, 1
- security zones, 2-4
- SIEM, 1

private-DMZ policies, ZPF, 210

private-public policies, ZPF, 210

privilege levels
- accessing, 138
- configuring, 137-138
- IOS authentication, 137-138
- verifying, 138

Privileged EXEC mode (ASA Firewall), 137, 229

proctors (exams), 299

promiscuous (passive) mode (IDS), 245

promiscuous ports (PVLAN), 171

proxy servers, 185-186

PSK (Pre-Shared Keys)
- IOS CLI-based site-to-site IPsec VPN, 117
- IPsec authentication, 80

public-DMZ policies, ZPF, 209

PVLAN (Private VLAN)
- community ports, 172
- configuring, 173
- isolated ports, 171
- promiscuous ports, 171
- PVLAN Edge, 174-175
- topology, 172
- verifying, 173-174
- VLAN usage, 172

Q

Quick mode (IKEv1), 83

R

R1_BRANCH configuration skills practice, 283-284, 289-290

RA (Registration Authorities), 24

RADIUS, server-based AAA, 46-48
- accounting, 54-55
- authentication, 51-53
- authorization, 53-54
- deploying, 51
- troubleshooting, 58
- verifying, 55-58

ransomware, 9

RBAC (role-based CLI authorization), 138-139

RC encryption algorithm, 16

reconnaissance attacks, 5

reflection attacks, 7

remote-access VPN, 74
- AnyConnect SSL VPN
  - *ActiveX, 106*
  - *client authentication, 100*
  - *client IP address assignments, 100*
  - *configuring, 101-106*
  - *Java detection, 106*
  - *platform detection, 106*
  - *server authentication, 100*
  - *topology sample, 99*
  - *troubleshooting connections, 111*
  - *verifying configurations, 108-109*
- clientless SSL VPN, 86
  - *configuring, 87-94*
  - *SSL/TLS encapsulation, 85*
  - *verifying configurations, 95-96*
- full tunnel SSL VPN, 87
- thin client SSL VPN, 86

removable storage devices, data loss/exfiltration, 9

replays, anti-replay protection, 76

reports, Cisco CWS, 274

reputations (files)
AMP, 264
filtering, ESA, 265-266

requirements for exam day, 299

reset actions, IDS/IPS, 255

reset buttons, ASA, 221

retaking exams, 302

retrospection (files), AMP, 265

risks, defining, 2

ROM monitor mode (ASA Firewall), 229

root guard, 154, 168

routed mode deployments, ASA, 222

routing protocol authentication, OSPF, 143
MD5 authentication, 144-146
SHA authentication, 146-147

RSA encryption algorithm, 17-19, 80

rule-based detection (IDS), 247

S

sandboxing (files), AMP, 265

Santos, Omar, 153

ScanSafe. *See* Cisco CWS

scareware, 9

SCEP (Simple Certificate Enrollment Protocol), 27

score reports (exams), 299-301

SCP (Secure Copy Protocol), 43-44

SEAL encryption algorithm, 16, 79

secure management systems
access security, configuring, 36-37
in-band management, 35-36
NTP, 42
authentication, 43
verifying client synchronization, 43
OOB management, 35-36
SCP, 43-44
SNMP
agents, 39
authNoPriv mode, 40
authPriv mode, 40
configuring, 41-42
GET messages, 40
managers, 39
MIB, 40
noAuthNoPriv mode, 40
SET messages, 40
trap messages, 40
versions of, 40-41
SSH/HTTPS, configuring, 38
Syslog, configuring, 38-39

security
endpoint security
antimalware, 275, 278-279
antispyware, 275-277
antivirus software, 275-277
data encryption, 279
personal firewalls, 275-276
skills practice, 281
addressing schemes, 282
cabling, 283
clientless SSL VPN configuration, 286, 293
HQ-ASA configuration, 285, 291-293
HQ_SW configuration, 284-285, 290-291
ISP configuration, 283
R1_BRANCH configuration, 283-284, 289-290
site-to-site IPsec VPN configuration, 286-288, 294-295
topologies, 281
zone-based policy firewall configuration, 288-289, 295-297
STP
attacks, 153-154
BPDU guard, 154, 168
loop guard, 154, 168
PortFast, 154, 167
root guard, 154, 168
threats
access attacks, 5-8
data loss/exfiltration, 9
DDoS attacks, 6
DoS attacks, 6
malware, 8-9
network attacks, 5-6
reconnaissance attacks, 5
social engineering attacks, 7-8

web security
Cisco CWS, 272-274
Cisco WSA, 269-272
zones
DMZ, 3-4
filtering policies, 4
firewalls, 2

security object groups (ASA Firewall), 235

self zones (ZPL), 211

server-based AAA
accounting, 54-55
authentication, 45-46, 51-53
authorization, 53-54
deploying, 51
troubleshooting, 58
verifying, 55-58

servers
AnyConnect SSL VPN, server authentication, 100
DMZ servers, IPS, 250

service object groups (ASA Firewall), 235

service objects (ASA Firewall), 235

service policies
CSPL, ZPF configuration, 213
MPF, 241

SET messages (SNMP), 40

severity levels (Syslog), 38-39

SHA authentication, OSPF, 146-147

SHA-1 (Secure Hash Algorithm 1), 13-14

SHA-2 (Secure Hash Algorithm 2), 13

shun actions, IDS/IPS, 255

SIEM (Security Information Event Management), 1

signatures, IPsec authentication
ECDSA signatures, 80
RSA signatures, 80

single-root PKI topologies, 23

site-to-site IPsec VPN
ASA site-to-site IPsec VPN, 122
configuring, 123-125
verifying, 125-128
ASDM site-to-site VPN wizard, 123
IOS CLI-based site-to-site IPsec VPN, 114
configuring, 115-119
verifying, 119-122
negotiations, steps of, 113-114
skills practice, 286-288, 294-295

site-to-site VPN, 74

skills practice, 281
addressing schemes, 282
cabling, 283
clientless SSL VPN configuration, 286, 293
HQ-ASA configuration, 285, 291-293
HQ_SW configuration, 284-285, 290-291
ISP configuration, 283
R1_BRANCH configuration, 283-284, 289-290
site-to-site IPsec VPN configuration, 286-288, 294-295
topologies, 281
zone-based policy firewall configuration, 288-289, 295-297

smartphones, data loss/exfiltration, 9

smishing attacks, 8

smurf attacks, 7

SNMP (Simple Network Management Protocol)
agents, 39
authNoPriv mode, 40
authPriv mode, 40
configuring, 41-42
GET messages, 40
managers, 39
MIB, 40
noAuthNoPriv mode, 40
SET messages, 40
trap messages, 40
versions of, 40-41

social engineering (access attacks)
baiting, 8
defenses, 8
malvertising, 8
pharming, 7
phishing, 7
pretexting, 7
smishing, 8
something for something, 8
spam, 8

spear phishing, 7
tailgating, 8
vishing, 8
whaling, 7

software
antimalware
AMP, 264
ESA, 264
antispyware, endpoint security, 275-277
antivirus software
endpoint security, 275-277
ESA, 264-266
McAfee Antivirus, 266
Sophos Antivirus, 266

something for something (social engineering/access attacks), 8

Sophos Antivirus, 266

spam, 8, 259
ESA spam detection, 265-266
ESA spam filtering, 263

SPAN (Switched Port Analyzer), 248

spear phishing, 7

Specific configuration mode (ASA Firewall), 229

split tunneling, 132-133

spoofing attacks
ARP spoofing, 155-156
DHCP spoofing, 6, 158-159
IP spoofing, 6
MAC spoofing, 6, 156

spyware, 9

SSH (Secure Shell), 17, 38

SSL (Secure Sockets Layer), 17
remote-access VPN
AnyConnect SSL VPN, 99-111
clientless SSL VPN, 85-96
full tunnel SSL VPN, 87
thin client SSL VPN, 86
SSL VPN, 73-75, 286, 293

Standalone mode (AnyConnect Security Mobility Client), 100

start-stop records (AAA accounting), 54

stateful firewalls, 187

stateful packet inspection, ASA, 221

static NAT, 193
configuring, 195-197
verifying, 197

static PAT, 193

status LED, ASA, 220

stop-only records (AAA accounting), 54

storage devices (removable), data loss/exfiltration, 9

STP security
attacks, 153-154
BPDU guard, 154, 168
loop guard, 154, 168
PortFast, 154, 167
root guard, 154, 168

Stuppi, John, 153

Suite B cryptographic standard and IPsec, 81

superviews (CLI), 138

supplicants (802.1X authentication), 62-63

switches, ACL
Cisco IOS ACL, 175-176
PACL, 175-177
VACL, 175-178

symmetric encryption, 15-16

Syslog, 38-39

T

TACACS+ (Terminal Access Controller Access Control System Plus), server-based AAA, 46-48
accounting, 54-55
authentication, 51-53
authorization, 53-54
deploying, 51
troubleshooting, 58
verifying, 55-58

tailgating, 8

TCP SYN flood attacks, 7

test proctors, 299

thin client SSL VPN, 86

threats (security)
data loss/exfiltration, 9
defining, 2
malware, 8-9
network attacks
access attacks, 5-6
DDoS attacks, 6
DoS attacks, 6
reconnaissance attacks, 5
social engineering (access attacks)
defenses, 8
types of attacks, 7-8

TLS (Transport Layer Security), SSL/TLS encapsulation and clientless SSL VPN, 85

topologies (networks)
Branch/SOHO, 29
CAN, 28
clouds, 31
data centers, 31
skills practice, 281
virtual networks, 31
WAN, 29

traffic flows
ASA Firewall, 231
ZPF, 209, 213-214

transform sets (IPsec), IOS CLI-based site-to-site IPsec VPN, 117

transit subinterface (CPPr), 151

transparent (bridged) mode deployments, ASA, 222

transport mode
AH, 79
ESP, 78

trap messages (SNMP), 40

trigger actions, IDS/IPS, 255

Trojan horses, 9

troubleshooting
AnyConnect SSL VPN connections, 111
server-based AAA, 58

true positives/negatives (IPS), 250

trust exploitation, 6

tunnel mode
AH, 79
ESP, 78

two-factor authentication, 8

U

unencrypted devices, data loss/exfiltration, 9

URL (Uniform Resource Locators)
clientless SSL VPN configuration, 88
filtering, Cisco CWS, 274

U.S. government recognition of CCNA Security certification, 301

USB memory sticks, data loss/exfiltration, 9

USB ports, ASA, 221

User EXEC mode (ASA Firewall), 137, 229

user object groups (ASA Firewall), 235

V

VACL (VLAN ACL), 175-176
configuring, 177-178
verifying, 178

verifying
802.1X, 64-65
AnyConnect SSL VPN configurations, 108-109
clientless SSL VPN configurations, 95-96
DAI, 164
DHCP snooping, 162-163
dynamic NAT, 200
dynamic PAT, 202
IOS MD5 checksum, 140-141
IOS resilient configuration, 140
IPSG, 165
NAT
dynamic NAT, 200
dynamic PAT, 202
policy NAT, 206
static NAT, 197
NTP client synchronization, 43
parser views (CLI), 139
policy NAT, 206
port security, 166-167
privilege levels, 138
PVLAN, 173-174
PVLAN Edge, 174-175
server-based AAA, 55-58

site-to-site IPsec VPN
ASA site-to-site IPsec VPN, 125-128
IOS CLI-based site-to-site IPsec VPN, 119-122
static NAT, 197
VACL, 178
VLAN
PVLAN, 173-174
PVLAN Edge, 174-175
ZPL, 217-218

views (CLI)
assigning to users, 139
parser views, 138-139
superviews, 138

virtual network topologies, 31

virtualization, ASA, 222, 225

viruses
antivirus defenses, 8
antivirus software, 266
email, 259

vishing, 8

VLAN (Virtual Local Area Networks)
hopping attacks, 157-158
Native VLAN, 178-180
PVLAN
community ports, 172
configuring, 173
isolated ports, 171
promiscuous ports, 171
PVLAN Edge, 174-175
topology, 172
verifying, 173-174
VLAN usage, 172

VLAN maps. *See* VACL

VPN (Virtual Private Networks)
Always-on VPN, 134
AnyConnect SSL VPN
ActiveX, 106
client authentication, 100
client IP address assignments, 100
configuring, 101-106
Java detection, 106
platform detection, 106
server authentication, 100
topology sample, 99
troubleshooting connections, 111
verifying configurations, 108-109
ASDM site-to-site VPN wizard, 123
benefits of, 73
Client U-turns, 132
clientless SSL VPN, 86
configuring, 87-94
SSL/TLS encapsulation, 85
verifying configurations, 95-96
DAP, 135
endpoint posture assessments, 135
full tunnel SSL VPN, 87
GRE, 73
hairpinning, 131-132
IPsec VPN, 73-74
legacy VPN, 74
MPLS VPN, 73
NAT-T, 134
remote-access VPN, 74
AnyConnect SSL VPN, 99-111
clientless SSL VPN, 85-96
full tunnel SSL VPN, 87
thin client SSL VPN, 86
site-to-site IPsec VPN
ASA site-to-site IPsec VPN, 122-128
ASDM site-to-site VPN wizard, 123
IOS CLI-based site-to-site IPsec VPN, 114-122
negotiations, 113-114
site-to-site VPN, 74
split tunneling, 132
SSL VPN, 73-75
types of, 73

vulnerabilities, defining, 2

W

WAN (Wide-Area Network) topologies, 29

web security
Cisco CWS, 272-274
Cisco WSA, 269-272

WebLaunch mode (AnyConnect Security Mobility Client), 100

whaling, 7

worms, 9

X - Y

X.509 standard, 25

Z

zone-based policy firewall
configuration skills practice, 288-289, 295-297

ZPF (Zone-Based Policy Firewalls)
benefits of, 210
C3PL and ZPF configuration, 210-211, 216-218
class maps, 214-215
policy maps, 215
C3PL and ZPL configuration, 216-218
class maps, 212-215
policy maps, 212-215
service policies, 213
DMZ-private policies, 210
private-DMZ policies, 210
private-public policies, 210
public-DMZ policies, 209
self zones, 211
traffic flows, 209, 213-214
verifying, 217-218
zone pairs, 211, 214
zones, 211-214