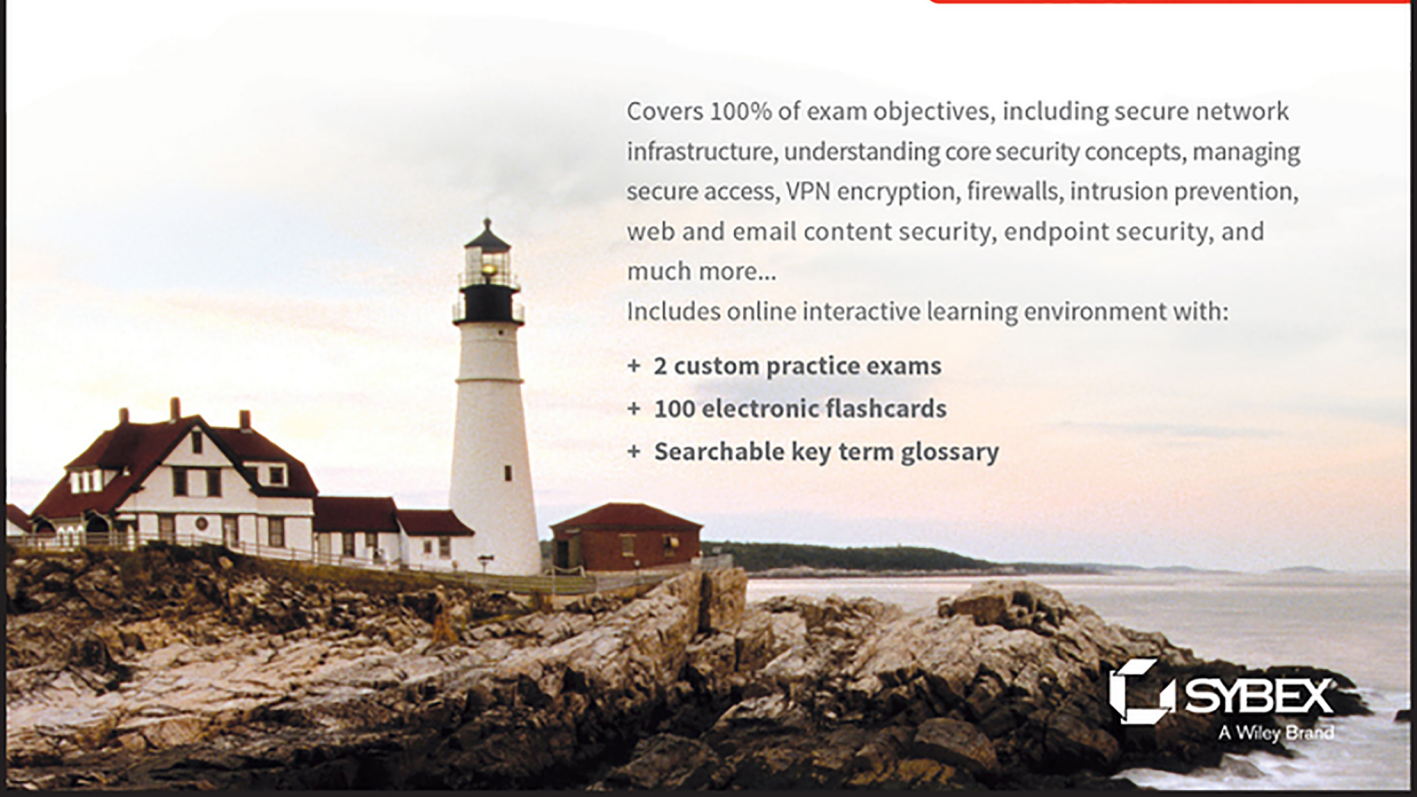
Troy McMillan

CCNA®

Security

STUDY GUIDE

EXAM 210-260



Covers 100% of exam objectives, including secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, endpoint security, and much more...

Includes online interactive learning environment with:

+ **2 custom practice exams**
+ **100 electronic flashcards**
+ **Searchable key term glossary**

SYBEX
A Wiley Brand

CCNA®

Security

Study Guide

CCNA®

Security

Study Guide

Exam 210-260

Troy McMillan

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: David Clark
Technical Editors: Jon Buhagiar and Mark Dittmer
Production Manager: Kathleen Wisor
Copy Editor: Kim Wimpsett
Editorial Manager: Mary Beth Wakefield
Executive Editor: Jim Minatel
Book Designer: Judy Fung and Bill Gibson
Proofreader: Amy Schneider
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: @Jeremy Woodhouse/Getty Images, Inc.

Published simultaneously in Canada

ISBN: 978-1-119-40993-9
ISBN: 978-1-119-40991-5 (ebk.)
ISBN: 978-1-119-40988-5 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2017962360

10 9 8 7 6 5 4 3 2 1

For my best friend, Wade Long, for just being a good friend.

Acknowledgments

Special thanks go to David Clark for keeping me on schedule and ensuring all the details are correct. Also, I'd like to thank Jon Buhagiar for the excellent technical edit that saved me from myself at times. Finally, as always, I'd like to acknowledge Kenyon Brown for his continued support of all my writing efforts.

About the Author

Troy McMillan writes practice tests, study guides, and online course materials for Kaplan IT Training, while also running his own consulting and training business. He holds more than 30 industry certifications and also appears in training videos for OnCourse Learning and Pearson Press. Troy can be reached at mcmillantroy@hotmail.com.

Contents at a Glance

Introduction *xxi*

Assessment Test *xxxi*

Chapter 1 Understanding Security Fundamentals 1

Chapter 2 Understanding Security Threats 25

Chapter 3 Understanding Cryptography 45

Chapter 4 Securing the Routing Process 73

Chapter 5 Understanding Layer 2 Attacks 91

Chapter 6 Preventing Layer 2 Attacks 107

Chapter 7 VLAN Security 127

Chapter 8 Securing Management Traffic 141

Chapter 9 Understanding 802.1x and AAA 157

Chapter 10 Securing a BYOD Initiative 171

Chapter 11 Understanding VPNs 185

Chapter 12 Configuring VPNs 203

Chapter 13 Understanding Firewalls 219

Chapter 14 Configuring NAT and Zone-Based Firewalls 229

Chapter 15 Configuring the Firewall on an ASA 245

Chapter 16 Intrusion Prevention 263

Chapter 17 Content and Endpoint Security 285

Appendix Answers to Review Questions 301

Index *331*

Contents

Introduction *xxi*

Assessment Test *xxxi*

Chapter 1 Understanding Security Fundamentals 1

Goals of Security 2
- Confidentiality 2
- Integrity 3
- Availability 3
- Guiding Principles 3
- Common Security Terms 6
- Risk Management Process 7

Network Topologies 15
- CAN 15
- WAN 16
- Data Center 16
- SOHO 17
- Virtual 17

Common Network Security Zones 17
- DMZ 17
- Intranet and Extranet 18
- Public and Private 18
- VLAN 18

Summary 19
Exam Essentials 19
Review Questions 20

Chapter 2 Understanding Security Threats 25

Common Network Attacks 26
- Motivations 26
- Classifying Attack Vectors 27
- Spoofing 28
- Password Attacks 29
- Reconnaissance Attacks 30
- Buffer Overflow 34
- DoS 34
- DDoS 36
- Man-in-the-Middle Attack 37
- ARP Poisoning 37

Social Engineering 38
- Phishing/Pharming 38
- Prevention 38

Malware 39
Data Loss and Exfiltration 39
Summary 40
Exam Essentials 40
Review Questions 42

Chapter 3 Understanding Cryptography 45

Symmetric and Asymmetric Encryption 46
Ciphers 46
Algorithms 48
Hashing Algorithms 53
MD5 54
SHA-1 54
SHA-2 54
HMAC 55
Digital Signatures 55
Key Exchange 57
Application: SSH 57
Public Key Infrastructure 57
Public and Private Keys 58
Certificates 60
Certificate Authorities 61
PKI Standards 63
PKI Topologies 64
Certificates in the ASA 65
Cryptanalysis 67
Summary 68
Exam Essentials 68
Review Questions 69

Chapter 4 Securing the Routing Process 73

Securing Router Access 74
Configuring SSH Access 74
Configuring Privilege Levels in IOS 76
Configuring IOS Role-Based CLI 77
Implementing Cisco IOS Resilient Configuration 79
Implementing OSPF Routing Update Authentication 80
Implementing OSPF Routing Update Authentication 80
Implementing EIGRP Routing Update Authentication 82
Securing the Control Plane 82
Control Plane Policing 83
Summary 84
Exam Essentials 85
Review Questions 86

Chapter 5 Understanding Layer 2 Attacks 91

Understanding STP Attacks 92
Understanding ARP Attacks 93
Understanding MAC Attacks 95
Understanding CAM Overflows 96
Understanding CDP/LLDP Reconnaissance 97
Understanding VLAN Hopping 98
Switch Spoofing 98
Double Tagging 99
Understanding DHCP Spoofing 99
Summary 101
Exam Essentials 101
Review Questions 102

Chapter 6 Preventing Layer 2 Attacks 107

Configuring DHCP Snooping 108
Configuring Dynamic ARP Inspection 110
Configuring Port Security 112
Configuring STP Security Features 114
BPDU Guard 114
Root Guard 115
Loop Guard 115
Disabling DTP 116
Verifying Mitigations 116
DHCP Snooping 116
DAI 117
Port Security 118
STP Features 118
DTP 120
Summary 120
Exam Essentials 121
Review Questions 122

Chapter 7 VLAN Security 127

Native VLANs 128
Mitigation 128
PVLANs 128
PVLAN Edge 131
PVLAN Proxy Attack 132
ACLs on Switches 133
Port ACLs 133
VLAN ACLs 133
Summary 134
Exam Essentials 134
Review Questions 136

Chapter 8 Securing Management Traffic 141

In-Band and Out-of-Band Management 142
AUX Port 142
VTY Ports 143
HTTPS Connection 144
SNMP 144
Console Port 145
Securing Network Management 146
SSH 146
HTTPS 146
ACLs 146
Banner Messages 147
Securing Access through SNMP v3 149
Securing NTP 150
Using SCP for File Transfer 151
Summary 151
Exam Essentials 152
Review Questions 153

Chapter 9 Understanding 802.1x and AAA 157

802.1x Components 158
RADIUS and TACACS+ Technologies 159
Configuring Administrative Access with TACACS+ 160
Local AAA Authentication and Accounting 160
SSH Using AAA 161
Understanding Authentication and Authorization Using ACS and ISE 161
Understanding the Integration of Active Directory with AAA 162
TACACS+ on IOS 162
Verify Router Connectivity to TACACS+ 164
Summary 164
Exam Essentials 165
Review Questions 166

Chapter 10 Securing a BYOD Initiative 171

The BYOD Architecture Framework 172
Cisco ISE 172
Cisco TrustSec 174
The Function of Mobile Device Management 177
Integration with ISE Authorization Policies 177
Summary 178
Exam Essentials 179
Review Questions 180

Chapter 11 Understanding VPNs 185

Understanding IPsec 186
Security Services 186
Protocols 189
Delivery Modes 192
IPsec with IPV6 194
Understanding Advanced VPN Concepts 195
Hairpinning 195
Split Tunneling 196
Always-on VPN 197
NAT Traversal 198
Summary 199
Exam Essentials 199
Review Questions 200

Chapter 12 Configuring VPNs 203

Configuring Remote Access VPNs 204
Basic Clientless SSL VPN Using ASDM 204
Verify a Clientless Connection 207
Basic AnyConnect SSL VPN Using ASDM 207
Verify an AnyConnect Connection 209
Endpoint Posture Assessment 209
Configuring Site-to-Site VPNs 209
Implement an IPsec Site-to-Site VPN with Preshared Key Authentication 209
Verify an IPsec Site-to-Site VPN 212
Summary 212
Exam Essentials 213
Review Questions 214

Chapter 13 Understanding Firewalls 219

Understanding Firewall Technologies 220
Packet Filtering 220
Proxy Firewalls 220
Application Firewall 221
Personal Firewall 221
Stateful vs. Stateless Firewalls 222
Operations 222
State Table 223
Summary 224
Exam Essentials 224
Review Questions 225

Chapter 14 Configuring NAT and Zone-Based Firewalls 229

Implementing NAT on ASA 9.x 230
Static 231
Dynamic 232
PAT 233
Policy NAT 233
Verifying NAT Operations 235
Configuring Zone-Based Firewalls 236
Class Maps 237
Default Policies 237
Configuring Zone-to-Zone Access 239
Summary 240
Exam Essentials 240
Review Questions 241

Chapter 15 Configuring the Firewall on an ASA 245

Understanding Firewall Services 246
Understanding Modes of Deployment 247
Routed Firewall 247
Transparent Firewall 247
Understanding Methods of Implementing High Availability 247
Active/Standby Failover 248
Active/Active Failover 248
Clustering 249
Understanding Security Contexts 249
Configuring ASA Management Access 250
Initial Configuration 250
Configuring Cisco ASA Interface Security Levels 251
Security Levels 251
Configuring Security Access Policies 253
Interface Access Rules 253
Object Groups 254
Configuring Default Cisco Modular Policy Framework (MPF) 256
Summary 257
Exam Essentials 257
Review Questions 259

Chapter 16 Intrusion Prevention 263

IPS Terminology 264
Threat 264
Risk 264

Vulnerability 265
Exploit 265
Zero-Day Threat 265
Actions 265
Network-Based IPS vs. Host-Based IPS 266
Host-Based IPS 266
Network-Based IPS 266
Promiscuous Mode 266
Detection Methods 267
Evasion Techniques 267
Packet Fragmentation 267
Injection Attacks 270
Alternate String Expressions 271
Introducing Cisco FireSIGHT 271
Capabilities 271
Protections 272
Understanding Modes of Deployment 273
Inline 275
Positioning of the IPS within the Network 275
Outside 275
DMZ 276
Inside 277
Understanding False Positives, False Negatives, True Positives, and True Negatives 277
Summary 278
Exam Essentials 278
Review Questions 280

Chapter 17 Content and Endpoint Security 285

Mitigating Email Threats 286
Spam Filtering 286
Context-Based Filtering 287
Anti-malware Filtering 287
DLP 287
Blacklisting 288
Email Encryption 288
Cisco Email Security Appliance 288
Putting the Pieces Together 290
Mitigating Web-Based Threats 292
Understanding Web Proxies 292
Cisco Web Security Appliance 293

Mitigating Endpoint Threats 294
Cisco Identity Services Engine (ISE) 294
Antivirus/Anti-malware 294
Personal Firewall 294
Hardware/Software Encryption of Local Data 294
HIPS 295
Summary 295
Exam Essentials 295
Review Questions 296

Appendix Answers to Review Questions 301

Chapter 1: Understanding Security Fundamentals 302
Chapter 2: Understanding Security Threats 304
Chapter 3: Understanding Cryptography 305
Chapter 4: Securing the Routing Process 307
Chapter 5: Understanding Layer 2 Attacks 309
Chapter 6: Preventing Layer 2 Attacks 311
Chapter 7: VLAN Security 312
Chapter 8: Securing Management Traffic 314
Chapter 9: Understanding 802.1x and AAA 316
Chapter 10: Securing a BYOD Initiative 317
Chapter 11: Understanding VPNs 319
Chapter 12: Configuring VPNs 321
Chapter 13: Understanding Firewalls 322
Chapter 14: Configuring NAT and Zone-Based Firewalls 324
Chapter 15: Configuring the Firewall on an ASA 325
Chapter 16: Intrusion Prevention 327
Chapter 17: Content and Endpoint Security 328

Index *331*

Introduction

The CCNA Security certification program is one of the elective paths you can take when achieving the CCNA. It requires passing the CCENT exam (100-105) and then passing the CCNA Security exam (210-260).

The Cisco Security exam objectives are periodically updated to keep the certification applicable to the most recent hardware and software. This is necessary because a technician must be able to work on the latest equipment. The most recent revisions to the objectives—and to the whole program—were introduced in 2016 and are reflected in this book.

This book and the Sybex *CCNA Security+ Complete Study Guide* (both the Standard and Deluxe editions) are tools to help you prepare for this certification—and for the new areas of focus of a modern server technician's job.

What Is the CCNA Security Certification?

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies; the installation, troubleshooting, and monitoring of network devices to maintain integrity, confidentiality, and availability of data and devices; and competency in the technologies that Cisco uses in its security structure.

The CCNA Security certification isn't awarded until you've passed the two tests. For the latest pricing on the exams and updates to the registration procedures, call Pearson VUE at (877) 551-7587. You can also go to Pearson VUE's website at `www.vue.com` for additional for information or to register online. If you have further questions about the scope of the exams, see `https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-security.html`.

What Does This Book Cover?

Here is a glance at what's in each chapter.

Chapter 1: Understanding Security Fundamentals covers common security principles such as the CIA triad; common security terms such as risk, vulnerability, and threat; the proper application of common security zones, such as intranet, DMZ, and extranets; a discussion of network topologies as seen from the perspective of the Cisco Campus Area network; and methods of network segmentation such as VLANs.

Chapter 2: Understanding Security Threats covers common network attacks and their motivations; attack vectors such as malicious and non-malicious insiders and outsiders, terrorists, spies, and terminated personnel; various methods used to perform

network reconnaissance such as ping scans and port scans; types of malware; and the exfiltration of sensitive data such as IP, PII, and credit card data.

Chapter 3: Understanding Cryptography covers symmetric and asymmetric key cryptography, the hashing process, major hashing algorithms, PKI and the components that make it function, and common attacks on cryptography.

Chapter 4: Securing the Routing Process covers methods of securing administrative access to the router, IOS privilege levels, IOS role-based CLI access, Cisco IOS resilient configuration, authentication for router updates for both OSPF and EIGRP, and control plane policing.

Chapter 5: Understanding Layer 2 Attacks covers STP attacks such as rogue switches, ARP spoofing, MAC spoofing, and CAM overflow. It also discusses both the value and the danger in using CDP and LLDP. Finally, you will learn how VLAN hopping attacks are performed.

Chapter 6: Preventing Layer 2 Attacks covers DHCP snooping, DAI and how it can prevent ARP poisoning attacks, preventing MAC overflow attacks and the introduction of unauthorized devices to switch ports by using port security, and the use of BPDU Guard, Root Guard, and Loop Guard, all STP features designed to prevent changes to the STP topology.

Chapter 7: VLAN Security covers preventing VLAN hopping attacks that take advantage of the native VLAN; private VLANs; setting ports as promiscuous, community, and isolated; the PVLAN Edge feature; and using ACLs to prevent a PVLAN proxy attack.

Chapter 8: Securing Management Traffic covers managing devices in-band and out-of-band, methods of securing management interfaces including enabling the HTTPS server, securing SNMP v3 with a security policy, applying passwords to all management interfaces, and using SSH for remote management, types of banner message, and securing the NTP protocol.

Chapter 9: Understanding 802.1x and AAA covers AAA service that can be provided by TACACS+ and RADIUS servers, configuring administrative access to a router using TACACS+, how AAA can be integrated with Active Directory, the Cisco implementations of a RADIUS server including the Cisco Secure Access Control Server (ACS) and the Cisco Identity Services Engine (ISR), and the functions of various 802.1X components.

Chapter 10: Securing a BYOD Initiative covers challenges involved in supporting a BYOD initiative, components provided by Cisco for this including the Cisco Integrated Services Engine (ISE), and the Cisco TrustSec provisioning and management platform. It also covers advanced features of Cisco ISE, including downloadable ACLs (dACLs), automatic VLAN assignment, security group access (SGAs), change of authorization (COA), and posture assessment. Further we discuss the authentication mechanisms ISE

can accept, including 802.1x, MAC authentication bypass (MAB), and web authentication (WebAuth). Finally, we end the chapter covering the three main functions of TrustSec.

Chapter 11: Understanding VPNs covers IPsec and the security services it provides; the components of IPsec such as ISAKMP, IKE, AH, and ESP; how to use hairpinning to allow traffic between two hosts to connect to the same VPN interface; and split tunneling and its benefits.

Chapter 12: Configuring VPNs covers the value of the Cisco clientless SSL VPN and the steps required to configure it, the Cisco AnyConnect SSL VPN, modules in the Cisco AnyConnect client that can provide endpoint posture assessment, and how to implement an IPsec site-to-site VPN with preshared key authentication.

Chapter 13: Understanding Firewalls covers various firewall technologies such as proxy, application, personal, and stateful firewalls, with stateful firewalls covered in greater detail and described in relation to the operation of these firewalls and the TCP three-way handshake. Finally you learn what is contained in the state table of a stateful firewall.

Chapter 14: Configuring NAT and Zone-Based Firewalls covers three forms of NAT: static NAT, dynamic NAT, and PAT; the NAT options available in the ASA, the benefits of NAT; and how to configure it and verify its operation. You will learn about class maps, policy maps, and service policies and their respective functions in a zone-based firewall. Finally, the steps to configure and verify a zone-based firewall end the chapter.

Chapter 15: Configuring the Firewall on an ASA covers how to set up the ASA so you can remotely administer it using the ASDM, the default security policies that are in place, how the default global policy interacts with configured policies, how interface security levels affect traffic flows, how the Cisco Modular Policy framework is used to create policies; the difference between a transparent and route firewall; and high availability solutions including active-active, active-passive, and clustering approaches.

Chapter 16: Intrusion Prevention covers general IPS concepts such as network-based and host-based deployments; modes of deployment such as inline, SPAN, and tap; the positioning options available; false positives and false negatives; how rules and signatures are used in the process of identifying potential attacks; and trigger actions of which an IPS might be capable, such as dropping, resetting, and alerting.

Chapter 17: Content and Endpoint Security covers mitigation techniques available when using the Cisco Email Security Appliance, including reputation and context-based filtering, and the Cisco Web Security Appliance, which uses blacklisting, URL filtering, and malware scanning to secure web traffic and web applications. Finally, the chapter discusses endpoint protection provided by the Cisco Identity Services Engine and Cisco TrustSec technology.

Interactive Online Learning Environment and Test Bank

We've put together some really great online tools to help you pass the CCNA Security exam. The interactive online learning environment that accompanies the CCNA Security exam certification guide provides a test bank and study tools to help you prepare for the exam. By using these tools you can dramatically increase your chances of passing the exam on your first try.

The online test bank includes the following:

Sample Tests Many sample tests are provided throughout this book and online, including the Assessment Test, which you'll find at the end of this introduction, and the Chapter Tests that include the review questions at the end of each chapter. In addition, there are two bonus practice exams. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

Flashcards The online text bank includes 100 flashcards specifically written to hit you hard, so don't get discouraged if you don't ace your way through them at first! They're there to ensure that you're really ready for the exam. And no worries—armed with the review questions, practice exams, and flashcards, you'll be more than prepared when exam day comes! Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Resources A glossary of key terms from this book and their definitions are available as a fully searchable PDF.

Go to `http://www.wiley.com/go/Sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools.

Who Should Read This Book

If you want to acquire a solid foundation in managing security on Cisco devices or your goal is to prepare for the exams by filling in any gaps in your knowledge, this book is for you. You'll find clear explanations of the concepts you need to grasp and plenty of help to achieve the high level of professional competency you need in order to succeed in your chosen field.

If you want to become certified as a CCNA Security professional, this book is definitely what you need. However, if you just want to attempt to pass the exam without really understanding the basics of personal computers, this guide isn't for you. It's written for people who want to acquire skills and knowledge of servers and storage systems.

How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Cisco CCNA Security exam, then look no further. We've spent hundreds of hours putting together this book with the sole intention of helping you to pass the exam as well as really learn about the exciting field of network security!

This book is loaded with valuable information, and you will get the most out of your study time if you understand why the book is organized the way it is.

So, to maximize your benefit from this book, I recommend the following study method:

1. Take the assessment test that's provided at the end of this introduction. (The answers are at the end of the test.) It's okay if you don't know any of the answers; that's why you bought this book! Carefully read over the explanations for any questions you get wrong and note the chapters in which the material relevant to them is covered. This information should help you plan your study strategy.
2. Study each chapter carefully, making sure you fully understand the information and the test objectives listed at the beginning of each one. Pay extra-close attention to any chapter that includes material covered in questions you missed.
3. Complete all hands-on labs in each chapter, referring to the text of the chapter so that you understand the reason for each step you take.
4. Answer all of the review questions related to each chapter. (The answers appear in Appendix.) Note the questions that confuse you, and study the topics they cover again until the concepts are crystal clear. And again—do not just skim these questions! Make sure you fully comprehend the reason for each correct answer. Remember that these will not be the exact questions you will find on the exam, but they're written to help you understand the chapter material and ultimately pass the exam!
5. Try your hand at the practice questions that are exclusive to this book. The questions can be found at `http://www.sybex.com/go/ccnasecuritystudyguide`.
6. Test yourself using all the flashcards, which are also found at the download link. These are brand-new and updated flashcards to help you prepare for the CCNA Security exam and a wonderful study tool!

To learn every bit of the material covered in this book, you'll have to apply yourself regularly, and with discipline. Try to set aside the same time period every day to study, and select a comfortable and quiet place to do so. I'm confident that if you work hard, you'll be surprised at how quickly you learn this material!

If you follow these steps and really study in addition to using the review questions, the practice exams, and the electronic flashcards, it would actually be hard to fail the CCNA Security exam. But understand that studying for the Cisco exams is a lot like getting in shape—if you do not go to the gym every day, it's not going to happen!

According to the Cisco website the Cisco CCNA Security exam details are as follows:

Exam code: 210-260

Exam description: This exam tests the candidate's knowledge of secure network infrastructure, understanding core security concepts, managing secure access, VPN encryption, firewalls, intrusion prevention, web and email content security, and endpoint security using Cisco routers and the ASA 9x.

Number of questions: 60–70

Type of questions: multiple choice, drag and drop, testlet, simulation

Length of test: 90 minutes

Passing score: 860 (on a scale of 100–900)

Language: English

How Do You Go About Taking the Exam?

When the time comes to schedule your exam you will need to create an account at `http://www.pearsonvue.com/cisco/` and register for your exam. Cisco testing is provided by their global testing partner Pearson VUE. You can locate your closest testing center at `https://home.pearsonvue.com/`. You can schedule at any of the listed testing centers.

To purchase the exam, you will need to buy an exam voucher from Cisco. The voucher is a code they provide you to use to schedule the exam. Information on purchasing a voucher can be found at: `http://www.pearsonvue.com/vouchers/pricelist/cisco.asp`.

When you have a voucher and have selected a testing center, you can schedule the Cisco 210-260 exam by following this link: `http://www.pearsonvue.com/cisco/`. This will take you to the Pearson VUE website and from here you can also locate a testing center or purchase vouchers if you have not already done so.

When you have registered for the CCNA Security certification exam you will receive a confirmation e-mail that supplies you with all of the information you will need to take the exam. Remember to take a printout of this e-mail with you to the testing center.

Certification Exam Policies

For the most current information regarding Cisco exam policies, it is recommended that you follow the `https://www.cisco.com/c/en/us/training-events/training-certifications/exams/policies.html` link to become familiar with Cisco policies. It contains a large amount of useful information regarding:

- Exam policy requirements
  - Age requirements and policies concerning minors
  - Certification and confidentiality agreement
  - Candidate identification and authentication
  - Candidate rights and responsibilities
  - Confidentiality and agreements

  - Embargoed country policy
  - Privacy
- Exam and testing policies
  - Conduct
  - Confidentiality and agreements
  - Exam discounts, vouchers, and promotional codes
  - Exam violations
  - Preliminary score report
  - Retaking exams
- Post exam policies
  - Certification tracking system
  - Correspondence
  - Exam recertification
  - Exam retirement
  - Exam scoring
  - Logo guidelines

Tips for Taking Your Exam

The Cisco CCNA Security exam contains 60–90 multiple choice, drag and drop, testlet, and simulation item questions, and must be completed in 90 minutes or less. This information may change over time and it is advised to check `www.cisco.com` for the latest updates.

Many questions on the exam offer answer choices that at first glance look identical—especially the syntax questions! So remember to read through the choices carefully because close just doesn't cut it. If you get information in the wrong order or forget one measly character, you may get the question wrong. So, to practice, do the practice exams and hands-on exercises in this book's chapters over and over again until they feel natural to you; also, and this is very important, do the online sample test until you can consistently answer all the questions correctly. Relax, read the question over and over until you are 100% clear on what it is asking, and then you can usually eliminate a few of the obviously wrong answers.

Here are some general tips for exam success:

- Arrive early at the exam center so you can relax and review your study materials.
- Read the questions *carefully*. Don't jump to conclusions. Make sure you're clear about *exactly* what each question asks. "Read twice, answer once!"
- Ask for a piece of paper and pencil if it is offered to take down quick notes and make sketches during the exam.
- When answering multiple-choice questions that you're not sure about, use the process of elimination to get rid of the obviously incorrect answers first. Doing this greatly improves your odds if you need to make an educated guess.

After you complete an exam, you'll get immediate notification of your pass or fail status, a printed examination score report that indicates your pass or fail status, and your exam results by section. (The test administrator will give you the printed score report.) Test scores are automatically forwarded to Cisco after you take the test, so you don't need to send your score to them. If you pass the exam, you'll receive confirmation from Cisco and a package in the post with a nice document suitable for framing showing that you are now a Cisco certified engineer.

Exam Objectives

Cisco goes to great lengths to ensure that its certification programs accurately reflect the IT industry's best practices. The company does this by establishing Cornerstone Committees for each of its exam programs. Each committee comprises a small group of IT professionals, training providers, and publishers who are responsible for establishing the exam's baseline competency level and who determine the appropriate target audience level.

Once these factors are determined, Cisco shares this information with a group of hand-selected subject-matter experts (SMEs). These folks are the true brainpower behind the certification program. They review the committee's findings, refine them, and shape them into the objectives you see before you. Cisco calls this process a *job task analysis* (JTA).

Finally, Cisco conducts a survey to ensure that the objectives and weightings truly reflect the job requirements. Only then can the SMEs go to work writing the hundreds of questions needed for the exam. And, in many cases, they have to go back to the drawing board for further refinements before the exam is ready to go live in its final state. So, rest assured, the content you're about to learn will serve you long after you take the exam.

Cisco also publishes relative weightings for each of the exam's objectives. The following table lists the objective domains and the extent to which they're represented on each exam.

210-260 Exam Domains	% of Exam
1.0 Security Concepts	12%
2.0 Secure Access4.0 Security	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%**

210-260 Sub Domains	Chapters
1.2 Common security threats	2
1.3 Cryptography concepts	2
1.4 Describe network topologies	3
2.1 Secure management	8
2.2 AAA concepts	9
2.3 802.1x authentication	9
2.4 BYOD	10
3.1 VPN concepts	11
3.2 Remote access VPN	12
3.3 Site-to-site VPN	12
4.1 Security on Cisco routers	4
4.2 Securing routing protocols	4
4.3 Securing the control plane	4
4.4 Common Layer 2 attacks	5
4.5 Mitigation procedures	6
4.6 VLAN security	7
5.1 Describe operational strengths and weaknesses of the different firewall technologies	13
5.2 Compare stateful vs. stateless firewalls	13
5.3 Implement NAT on Cisco ASA 9.x	14
5.4 Implement zone-based firewall	14
5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x	15

210-260 Sub Domains	Chapters
6.1 Describe IPS deployment considerations	16
6.2 Describe IPS technologies	16
7.1 Describe mitigation technology for email-based threats	17
7.2 Describe mitigation technology for web-based threats	17
7.3 Describe mitigation technology for endpoint threats	17

Assessment Test

1. When you are concerned with preventing data from unauthorized edits you are concerned with which of the following?
   - **A.** integrity
   - **B.** confidentiality
   - **C.** availability
   - **D.** authorization
2. When a systems administrator is issued both an administrative-level account and a normal user account and uses the administrative account *only* when performing an administrative task, it is an example of which concept?
   - **A.** least privilege
   - **B.** split knowledge
   - **C.** dual control
   - **D.** separation of duties
3. What is the purpose of mandatory vacations?
   - **A.** cross training
   - **B.** fraud prevention
   - **C.** improves morale
   - **D.** employee retention
4. Which of the following occurs when an organizational asset is exposed to losses?
   - **A.** risk
   - **B.** threat
   - **C.** exposure
   - **D.** vulnerability
5. Which of the following is a standard used by the security automation community to enumerate software flaws and configuration issues?
   - **A.** CSE
   - **B.** SCAP
   - **C.** CVE
   - **D.** CWE
6. Which hacker type hacks for a political cause?
   - **A.** black hats
   - **B.** white hats
   - **C.** script kiddies
   - **D.** hacktivists

7. Which of the following is an email validation system that works by using DNS to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator?
   - **A.** PGP
   - **B.** S/MIME
   - **C.** SMTP
   - **D.** SPF

8. What does the following command do?

   ```
   nmap -sP 192.168.0.0-100
   ```

   - **A.** port scan
   - **B.** ping scan
   - **C.** vulnerability scan
   - **D.** penetration test

9. You just executed a half open scan and got no response. What does that tell you?
   - **A.** the port is open
   - **B.** the port is closed
   - **C.** the port is blocked
   - **D.** it cannot be determined

10. Which of the following is a mitigation for a buffer overflow?
    - **A.** antivirus software
    - **B.** IOS updates
    - **C.** input validation
    - **D.** encryption

11. Which of the following is a Layer 2 attack?
    - **A.** buffer overflow
    - **B.** DoS
    - **C.** ARP poisoning
    - **D.** IP spoofing

12. Which of the following is *not* intellectual property?
    - **A.** designs
    - **B.** advertisements
    - **C.** recipes
    - **D.** contact lists

13. What is the best countermeasure to social engineering?
    - **A.** training
    - **B.** access lists

C. HIDS

D. encryption

14. Which of the following is a mitigation for ARP poisoning?

A. VLANs

B. DAI

C. DNSSec

D. STP

15. In which cryptographic attack does the attacker use recurring patterns to reverse engineer the message?

A. side channel

B. frequency

C. plaintext only

D. ciphertext only

16. You have five users in your department. These five users only need to encrypt information with one another. If you implement a symmetric encryption algorithm, how many keys will be needed to support the department?

A. 5

B. 8

C. 10

D. 12

17. Which statement is true with regard to asymmetric encryption?

A. less expensive than symmetric

B. slower than symmetric

C. harder to crack than symmetric

D. key compromise can occur more easily than with symmetric

18. Which of the following is a stream-based cipher?

A. RC4

B. DES

C. 3DES

D. AES

19. What is the purpose of an IV?

A. doubles the encryption

B. adds randomness

C. performs 16 rounds of transposition

D. hashes the message

20. Which step is not required to configure SSH on a router?

- **A.** Set the router name
- **B.** Set the router ID
- **C.** Set the router domain name
- **D.** Generate the RSA key

21. Which of the following allows you to assign a technician sets of activities that coincide with the level they have been assigned?

- **A.** access levels
- **B.** job parameters
- **C.** privilege levels
- **D.** rules

22. Which of the following is a way to prevent unwanted changes to the configuration?

- **A.** router lockdown
- **B.** resilient configuration
- **C.** secure IOS
- **D.** config-sec

23. Which of the following is used to hold multiple keys used in OSPF Routing Update Authentication?

- **A.** key store
- **B.** keychain
- **C.** keydb
- **D.** keyauth

24. Which of the following characteristics of a rogue switch could cause it to become the root bridge?

- **A.** higher MAC address
- **B.** higher IP address
- **C.** a superior BPDU
- **D.** lower router ID

25. Which of the following is used by a malicious individual to pollute the ARP cache of other machines?

- **A.** ping of death
- **B.** buffer overflow
- **C.** bound violation
- **D.** gratuitous ARP

26. What happens when the CAM table of a switch is full of fake MAC addresses and can hold no other MAC addresses?

A. it gets dumped

B. the switch shuts down

C. the switch start forwarding all traffic out of all ports

D. all ports are shut down

27. Which switch feature uses the concept of trusted and untrusted ports?

A. DAI

B. DHCP snooping

C. STP

D. Root Guard

28. Which command enables port security on the switch?

A. `SW70(config-if)#switchport mode access`

B. `SW70(config-if)# switchport port-security maximum 2`

C. `SW70(config-if)#switchport port-security`

D. `SW70(config-if)# switchport port-security violation shutdown`

29. Which switch feature prevents the introduction of a rogue switch to the topology?

A. Root Guard

B. BPDU Guard

C. Loop Guard

D. DTP

30. What prevents switching loops?

A. DAI

B. DHCP snooping

C. STP

D. Root Guard

Answers to Assessment Test

1. A. Integrity, the second part of the CIA triad, ensures that data is protected from unauthorized modification or data corruption. The goal of integrity is to preserve the consistency of data, including data stored in files, databases, systems, and networks.

2. A. The principle of least privilege requires that a user or process is given only the minimum access privilege needed to perform a particular task.

3. B. With mandatory vacations, all personnel are required to take time off, allowing other personnel to fill their position while gone. This detective administrative control enhances the opportunity to discover unusual activity.

4. C. An exposure occurs when an organizational asset is exposed to losses.

5. B. Security Content Automation Protocol (SCAP) is a standard used by the security automation community to enumerate software flaws and configuration issues. It standardized the nomenclature and formats used.

6. D. Hacktivists are those who hack not for personal gain, but to further a cause. For example, the Anonymous group hacks from time to time for various political reasons.

7. D. Sender Policy Framework (SPF) is an email validation system that works by using DNS to determine whether an email sent by someone has been sent by a host sanctioned by that domain's administrator. If it can't be validated, it is not delivered to the recipient's box.

8. B. 0–100 is the range of IP addresses to be scanned in the 192.168.0.0 network.

9. C. If you receive no response the port is blocked on the firewall.

10. C. With proper input validation, a buffer overflow attack will cause an access violation. Without proper input validation, the allocated space will be exceeded, and the data at the bottom of the memory stack will be overwritten.

11. C. One of the ways a man-in-the-middle attack is accomplished is by poisoning the ARP cache on a switch. The attacker accomplishes this poisoning by answering ARP requests for another computer's IP address with his own MAC address. Once the ARP cache has been successfully poisoned, when ARP resolution occurs, both computers will have the attacker's MAC address listed as the MAC address that maps to the other computer's IP address. As a result, both are sending to the attacker, placing him "in the middle."

12. B. An advertisement would be publicly available.

13. A. The best countermeasure against social engineering threats is to provide user security awareness training. This training should be required and must occur on a regular basis because social engineering techniques evolve constantly.

14. B. Dynamic ARP inspection (DAI) is a security feature that intercepts all ARP requests and responses and compares each response's MAC address and IP address information against the MAC–IP bindings contained in a trusted binding table.