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
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

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

List of Tables

List of Illustrations

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
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.

15. B. One of the issues with substitution ciphers is that if the message is of sufficient length, patterns in the encryption begin to become noticeable, which makes it vulnerable to a frequency attack. A frequency attack is when the attacker uses these recurring patterns to reverse engineer the message.

16. C. To calculate the number of keys that would be needed in this example, you would use the following formula:

    # of users × (# of users – 1) / 2

    Using our example, you would calculate 5 ×(4) / 2 or 10 needed keys.

17. B. Asymmetric encryption is *more* expensive than symmetric, it is slower than symmetric, it is *easier* to crack than symmetric, and key compromise can occur *less* easily than with symmetric.

18. A. Only RC4 is a stream cipher.

19. B. Some modes of symmetric key algorithms use initialization vectors (IVs) to ensure that patterns are not produced during encryption. These IVs provide this service by using random values with the algorithms.

20. B. A router ID is not a part of the configuration.

21. C. Privilege levels allow you to assign a technician sets of activities that coincide with the level they have been assigned. There are 16 levels from 0 to 15.

22. B. The IOS Resilient Configuration feature can provide a way to easily recover from an attack on the configuration, and it can also help to recover from an even worse attack in which the attacker deletes not only the startup configuration but also the boot image.

23. B. A keychain can be used to hold multiple keys if required.

24. C. When a malicious individual introduces a rogue switch to the switching network and the rogue switch has a superior BPDU to the one held by the current root bridge, the new switch assumes the position of root bridge.

25. A. Gratuitous ARP is called gratuitous because the ARP message sent is an answer to a question that the target never asks and it cause the target to change its ARP cache.

26. C. The result of this attack is that the attacker is now able to receive traffic that he would not have been able to see otherwise because in this condition the switch is basically operating as a hub and not a switch.

27. B. DHCP snooping is implemented on the switches in the network, so it is a Layer 2 solution. The switch ports on the switch are labeled either trusted or untrusted. Trusted ports are those that will allow a DHCP message to traverse.

28. C. Without executing this command the other commands will have no effect.

29. B. The BPDU Guard feature is designed to prevent the reception of superior BPDUs on access ports by preventing the reception of any BPDU frames on access ports.

30. Spanning Tree Protocol (STP), prevents switching loops in redundant switching networks.

Chapter 1
Understanding Security Fundamentals

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.1 Common security principles**
  - Describe confidentiality, integrity, availability (CIA)
  - Identify common security terms
  - Identify common network security zones
- ✓ **1.4 Describe network topologies**
  - Campus area network (CAN)
  - Cloud, wide area network (WAN)
  - Data center
  - Small office/home office (SOHO)
  - Network security for a virtual environment

Securing a network is no easy task. Daily you probably hear about data disclosures and new network attacks. However, you are not defenseless. By properly implementing the security features available in Cisco routers, switches, and firewalls, you can reduce the risk of a security breach to a manageable level. This book is designed to help you understand the issues, identify your security options, and deploy those options in the correct manner. In the process, the book will prepare you for the Cisco CCNA Security certification, which validates the skills and knowledge required to secure a network using Cisco products.

In this chapter, you will learn the following:

- Common security principles
- Network topologies

Goals of Security

When you're securing a network, several important security principles should guide your efforts. Every security measure you implement should contribute to the achievement of one of

three goals. The three fundamentals of security are confidentiality, integrity, and availability (CIA), often referred to as the *CIA triad*.

Most security issues result in a violation of at least one facet of the CIA triad. Understanding these three security principles will help ensure that the security controls and mechanisms implemented protect at least one of these principles.

Every security control that is put into place by an organization fulfills at least one of the security principles of the CIA triad. Understanding how to circumvent these security principles is just as important as understanding how to provide them.

Confidentiality

To ensure *confidentiality*, you must prevent the disclosure of data or information to unauthorized entities. As part of confidentiality, the sensitivity level of data must be determined before putting any access controls in place. Data with a higher sensitivity level will have more access controls in place than data at a lower sensitivity level. Identification, authentication, and authorization can be used to maintain data confidentiality. Encryption is another popular example of a control that provides confidentiality.

Integrity

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.

An access control list (ACL) is an example of a control that helps to provide integrity. Another example is the generation of hash values that can be used to validate data integrity.

Availability

Availability means ensuring that data is accessible when and where it is needed. Only individuals who need access to data should be allowed access to that data. The two main areas where availability is affected are

- When attacks are carried out that disable or cripple a system.
- When service loss occurs during and after disasters. Each system should be assessed on its criticality to organizational operations. Controls are implemented based on each system's criticality level.

Fault-tolerant technologies, such as RAID or redundant sites, are examples of controls that help to improve availability.

Guiding Principles

When managing network security and access to resources, there are some proven principles that should guide your efforts. These concepts have stood the test of time because they

contribute to supporting the CIA triad.

Least Privilege/Need-to-Know

The principle of *least privilege* requires that a user or process is given only the minimum access privilege needed to perform a particular task. Its main purpose is to ensure that users only have access to the resources they need and are authorized to perform only the tasks they need to perform. To properly implement the least privilege principle, organizations must identify all users' jobs and restrict users only to the identified privileges.

The *need-to-know* principle is closely associated with the concept of least privilege. Although least privilege seeks to reduce access to a minimum, the need-to-know principle actually defines what the minimums for each job or business function are. Excessive privileges become a problem when a user has more rights, privileges, and permissions than he needs to do his job. Excessive privileges are hard to control in large environments.

A common implementation of the least privilege and need-to-know principles is when a systems administrator is issued both an administrative-level account and a normal user account. In most day-to-day functions, the administrator should use his normal user account. When the systems administrator needs to perform administrative-level tasks, he should use the administrative-level account. If the administrator uses his administrative-level account while performing routine tasks, he risks compromising the security of the system and user accountability.

Organizational rules that support the principle of least privilege include the following:

- Keep the number of administrative accounts to a minimum.
- Administrators should use normal user accounts when performing routine operations.
- Permissions on tools that are likely to be used by attackers should be as restrictive as possible.

To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as *compartmentalization*.

Default to No Access

During the authorization process, you should configure an organization's access control mechanisms so that the default level of security is to default to no access. This means that if nothing has been specifically allowed for a user or group, then the user or group will not be able to access the resource. The best security approach is to start with no access and add rights based on a user's need to know and least privilege needed to accomplish daily tasks.

Defense in Depth

A *defense-in-depth* strategy refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers. The first layer of a good

defense-in-depth strategy is appropriate access control strategies. Access controls exist in all areas of an information systems (IS) infrastructure (more commonly referred to as an *IT infrastructure*), but a defense-in-depth strategy goes beyond access control. It also considers software development security, cryptography, and physical security. Figure 1.1 shows an example of the defense-in-depth concept.

FIGURE 1.1 Defense in depth

Separation of Duties

Separation of duties is a preventive administrative control to keep in mind when designing an organization's authentication and authorization policies. Separation of duties prevents fraud by distributing tasks and their associated rights and privileges between more than one user. It helps to deter fraud and collusion because when an organization implements adequate separation of duties, collusion between two or more personnel would be required to carry out fraud against the organization. A good example of separation duties is authorizing one person to manage backup procedures and another to manage restore procedures.

Separation of duties is associated with dual controls and split knowledge. With dual controls, two or more users are authorized and required to perform certain functions. For example, a retail establishment might require two managers to open the safe. Split knowledge ensures that no single user has all the information to perform a particular task. An example of a split control is the military requiring two individuals to each enter a unique combination to authorize missile firing.

Separation of duties ensures that one person is not capable of compromising organizational security. Any activities that are identified as high risk should be divided into individual tasks, which can then be allocated to different personnel or departments.

Let's look at an example of the violation of separation of duties. An organization's internal audit department investigates a possible breach of security. One of the auditors interviews three employees.

- A clerk who works in the accounts receivable office and is in charge of entering data into the finance system
- An administrative assistant who works in the accounts payable office and is in charge of approving purchase orders
- The finance department manager who can perform the functions of both the clerk and the administrative assistant

To avoid future security breaches, the auditor should suggest that the manager should only be able to review the data and approve purchase orders.

Job Rotation

From a security perspective, *job rotation* refers to the detective administrative control where multiple users are trained to perform the duties of a position to help prevent fraud by any individual employee. The idea is that by making multiple people familiar with the legitimate functions of the position, the likelihood increases that unusual activities by any one person will be noticed. Job rotation is often used in conjunction with mandatory vacations. Beyond the security aspects of job rotation, additional benefits include the following:

- Trained backup in case of emergencies
- Protection against fraud
- Cross-training of employees

Mandatory Vacation

With *mandatory vacation*s, all personnel are required to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

Some of the security benefits of using mandatory vacations include having the replacement employee do the following:

- Run the same applications as the vacationing employee
- Perform tasks in a different order from the vacationing employee
- Perform the job from a different workstation than the vacationing employee

Replacement employees should avoid running scripts that were created by the vacationing employee. A replacement employee should either develop their own script or manually complete the tasks in the script.

Common Security Terms

The risk management process cannot be discussed without understanding some key terms used in risk management. Security professionals should become familiar with the following terms as they are used in risk management:

- *Assets* include anything that is of value to the organization. Assets can be physical such as buildings, land, and computers, and they can be intangible such as data, plans, and recipes.
- A *vulnerability* is an absence or weakness of a countermeasure that is in place. Vulnerabilities can occur in software, hardware, or personnel. An example of a vulnerability is unrestricted access to a folder on a computer. Most organizations implement a vulnerability assessment to identify vulnerabilities.
- A *threat* is the next logical progression in risk management. A threat occurs when vulnerability is identified or exploited. A threat would occur when an attacker identified the folder on the computer that has an inappropriate or absent ACL.

- A *threat agent* is something that carries out a threat. Continuing with the example, the attacker who takes advantage of the inappropriate or absent ACL is the threat agent. Keep in mind, though, that threat agents can discover and/or exploit vulnerabilities. Not all threat agents will actually exploit an identified vulnerability.
- A *risk* is the probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out. The risk in the vulnerability example would be fairly high if the data residing in the folder is confidential. However, if the folder contains only public data, then the risk would be low. Identifying the potential impact of a risk often requires security professionals to enlist the help of subject-matter experts.
- An *exposure* occurs when an organizational asset is exposed to losses. If the folder with the inappropriate or absent ACL is compromised by a threat agent, the organization is exposed to the possibility of data exposure and loss.
- A *countermeasure* reduces the potential risk. Countermeasures are also referred to as *safeguards* or *controls*. Three things must be considered when implementing a countermeasure: vulnerability, threat, and risk. For this example, a good countermeasure would be to implement the appropriate ACL and to encrypt the data. The ACL protects the integrity of the data, and the encryption protects the confidentiality of the data.

Countermeasures or controls come in many categories and types. The categories and types of controls are discussed later in this chapter.

All the aforementioned security concepts work together in the relationship demonstrated in Figure 1.2.

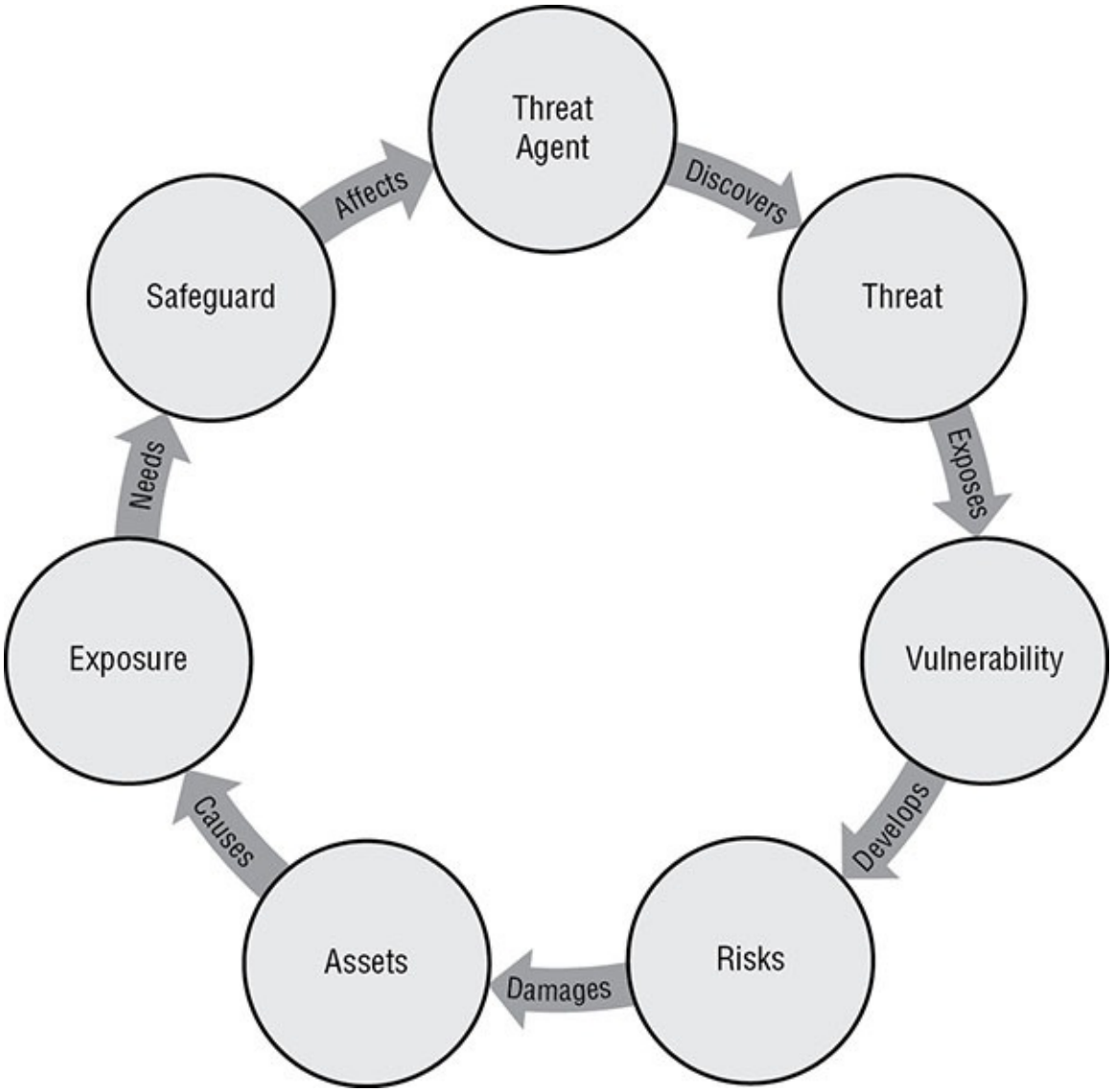

FIGURE 1.2 Security cycle

Risk Management Process

The *risk management* process is composed of a series of operations in which the data from one operation feeds the next operation. According to NIST SP 800-30, common information-gathering techniques used in risk analysis include automated risk assessment tools, questionnaires, interviews, and policy document reviews. Keep in mind that multiple sources should be used to determine the risks to a single asset. NIST SP 800-30 identifies the following steps in the risk management process:

1. Identify the assets and their value.
2. Identify threats.
3. Identify vulnerabilities.
4. Determine likelihood.
5. Identify impact.

6. Determine risk as a combination of likelihood and impact.

The following sections include these processes and two additional ones that relate to the identification of countermeasures and cost-benefit analysis.

Asset Classification

The first step of any risk assessment is to identify the assets and determine the asset value, called *asset classification*. Assets are both tangible and intangible. Tangible assets include computers, facilities, supplies, and personnel. Intangible assets include intellectual property, data, and organizational reputation. The value of an asset should be considered in respect to the asset owner's view. The six following considerations can be used to determine the asset's value:

- Value to owner
- Work required developing or obtaining the asset
- Costs to maintain the asset
- Damage that would result if the asset were lost
- Cost that competitors would pay for the asset
- Penalties that would result if the asset was lost

After determining the value of the assets, you should determine the vulnerabilities and threats to each asset.

Data Assets

Data should be classified based on its value to the organization and its sensitivity to disclosure. Assigning a value to data allows an organization to determine the resources that should be used to protect the data. Resources that are used to protect data include personnel resources, monetary resources, access control resources, and so on. Classifying data allows you to apply different protective measures. Data classification is critical to all systems to protect the confidentiality, integrity, and availability of data.

After data is classified, the data can be segmented based on its level of protection needed. The classification levels ensure that data is handled and protected in the most cost-effective manner possible. An organization should determine the classification levels it uses based on the needs of the organization. Several commercial business and military and government information classifications are commonly used.

The information life cycle should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, or government laws and regulations.

In this section, we will discuss the sensitivity and criticality of data, commercial business classifications, military and government classifications, information life cycle, database maintenance, and data audit.

SENSITIVITY AND CRITICALITY

Sensitivity is a measure of how freely the data can be handled. Some data requires special care and handling, especially when inappropriate handling could result in penalties, identity theft, financial loss, invasion of privacy, or unauthorized access by an individual or many individuals. Some data is also subject to regulation by state or federal laws and requires notification in the event of a disclosure.

Data is assigned a level of sensitivity based on who should have access to it and how much harm would be done if it were disclosed. This assignment of sensitivity is called *data classification*.

Criticality is a measure of the importance of the data. Data considered sensitive may not necessarily be considered critical. Assigning a level of criticality to a particular data set must take into consideration the answers to a few questions:

- Will you be able to recover the data in case of disaster?
- How long will it take to recover the data?
- What is the effect of this downtime, including loss of public standing?

Data is considered essential when it is critical to the organization's business. When essential data is not available, even for a brief period of time, or its integrity is questionable, the organization will be unable to function. Data is considered required when it is important to the organization, but organizational operations would continue for a predetermined period of time even if the data is not available. Data is nonessential if the organization is able to operate without it during extended periods of time.

Once the sensitivity and criticality of data is understood and documented, the organization should then work to create a data classification system. Most organizations will use either a commercial business classification system or a military and government classification system.

COMMERCIAL BUSINESS CLASSIFICATIONS

Commercial businesses usually classify data using four main classification levels, listed from highest sensitivity level to lowest:

1. Confidential
2. Private
3. Sensitive
4. Public

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would be available only to personnel in the organization whose work relates to the data's subject. Access to confidential data usually requires authorization for each access. Confidential data is exempt from disclosure under the Freedom of Information

Act. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

- After signing a confidentiality agreement
- When complying with a court order
- As part of a government project or contract procurement agreement

Data that is private includes any information related to personnel, including human resource records, medical records, and salary information, that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data that would not cause a negative impact on the organization.

MILITARY AND GOVERNMENT CLASSIFICATIONS

Military and governmental entities usually classify data using five main classification levels, listed from highest sensitivity level to lowest:

1. Top secret
2. Secret
3. Confidential
4. Sensitive but unclassified
5. Unclassified

Data that is top secret includes weapon blueprints, technology specifications, spy satellite information, and other military information that could gravely damage national security if disclosed. Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed. Data that is confidential includes patents, trade secrets, and other information that could seriously affect the government if unauthorized disclosure occurred. Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security but could cause citizens to question the reputation of the government. Military and government information that does not fall into any of the other four categories is considered unclassified and usually has to be granted to the public based on the Freedom of Information Act.

OTHER CLASSIFICATION SYSTEMS

Another classification system created by the United Kingdom's National Infrastructure Security Coordination Centre (NISCC, now Centre for Protection of National Infrastructure) and since adopted by the ISO/IEC as part of the Standard on Information security management for intersector and interorganizational communications and by CERT is the Traffic Light Protocol (TLP). This system uses traffic light colors to classify information assets. Table 1.1 shows the four colors and their meanings.

TABLE 1.1 TLP classifications

Color	Meaning
Red	Shared only within a meeting
Amber	Shared only with those in the organization with a need to know
Green	Shared only within a community
White	No restriction but still subject to copyright rules

Vulnerability Identification

When identifying vulnerabilities, the Common Vulnerability Scoring System and the Security Content Automation Protocol are standards used in this process. In this section, you'll learn about these two methods for enumerating vulnerabilities in a common format.

Security Content Automation Protocol (SCAP) is a standard used by the security automation community used to enumerate software flaws and configuration issues. It standardized the nomenclature and formats used. A vendor of security automation products can obtain a validation against SCAP, demonstrating that it will interoperate with other scanners and express the scan results in a standardized way.

Understanding the operation of SCAP requires an understanding of the components of it.

Common Configuration Enumeration (CCE) These are configuration best-practice statements maintained by NIST.

Common Platform Enumeration (CPE) These are methods for describing and classifying operating systems applications and hardware devices.

Common Weakness Enumeration (CWE) These are design flaws in the development of software that can lead to vulnerabilities.

Common Vulnerabilities and Exposures (CVE) These are vulnerabilities in published operating systems and applications software.

The *Common Vulnerability Scoring System (CVSS)* is a system of ranking vulnerabilities that are discovered based on predefined metrics. This system ensures that the most critical vulnerabilities can be easily identified and addressed after a vulnerability test is met. Scores are awarded on a scale of 0 to 10, with the values having the following ranks:

- 0: No issues
- 0.1 to 3.9: Low
- 4.0 to 6.9: Medium
- 7.0 to 8.9: High
- 9.0 to 10.0: Critical

CVSS is composed of three metric groups. These metric groups are described as follows:

- Base includes characteristics of a vulnerability that are constant over time and user environments.
- Temporal includes characteristics of a vulnerability that change over time but not among user environments.
- Environmental includes characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The base metric group includes the following metrics:

- *Access vector (AV)* describes how the attacker would exploit the vulnerability and has three possible values.
  - L stands for Local and means that the attacker must have physical or logical access to the affected system.
  - A stands for Adjacent network and means that the attacker must be on the local network.
  - N stands for Network and means that the attacker can cause the vulnerability from any network.
- *Access complexity (AC)* describes the difficulty of exploiting the vulnerability and has three possible values.
  - H stands for High and means that the vulnerability requires special conditions that are hard to find.
  - M stands for Medium and means that the vulnerability requires somewhat special conditions.
  - L stands for Low and means that the vulnerability does not require special conditions.
- *Authentication (Au)* describes the authentication an attacker would need to get through to exploit the vulnerability and has three possible values.
  - M stands for Multiple and means that the attacker would need to get through two or more authentication mechanisms.
  - S stands for Single and means that the attacker would need to get through one authentication mechanism.
  - N stands for None and means that no authentication mechanisms are in place to stop the exploit of the vulnerability.
- *Availability (A)* describes the disruption that might occur if the vulnerability is exploited and has three possible values.
  - N stands for None and means that there is no availability impact.
  - P stands for Partial and means that system performance is degraded.
  - C stands for Complete and means that the system is completely shut down.

- *Confidentiality (C)* describes the information disclosure that may occur if the vulnerability is exploited and has three possible values.
  - N stands for None and means that there is no confidentiality impact.
  - P stands for Partial and means some access to information would occur.
  - C stands for Complete and means all information on the system could be compromised.
- *Integrity (I)* describes the type of data alteration that might occur and has three possible values.
  - N stands for None and means that there is no integrity impact.
  - P stands for Partial and means some information modification would occur.
  - C stands for Complete and means all information on the system could be compromised.

The CVSS vector will look something like this:

```
CVSS2#AV:L/AC:H/Au:M/C:P/I:N/A:N
```

This vector is read as follows:

`AV:L`

Access Vector: L stands for Local and means that the attacker must have physical or logical access to the affected system.

`AC:H`

Access Complexity: H stands for stands for High and means that the vulnerability requires special conditions that are hard to find.

`Au:M`

Authentication: M stands for Multiple and means that the attacker would need to get through two or more authentication mechanisms.

`C:P`

Confidentiality: P stands for Partial and means some access to information would occur.

`I:N`

Integrity: N stands for None and means that there is no integrity impact.

`A:N`

Availability: N stands for None and means that there is no availability impact.

Control Selection

Once the assets have been classified and their value determined and all vulnerabilities have been identified, controls or mitigations must be selected to address the vulnerabilities. This cannot be done until the level of risk associated with each vulnerability has been determined

through one of two methods, qualitative and quantitative risk assessment.

Qualitative Risk Analysis

Qualitative risk analysis does not assign monetary and numeric values to all facets of the risk analysis process. Qualitative risk analysis techniques include intuition, experience, and best-practice techniques, such as brainstorming, focus groups, surveys, questionnaires, meetings, interviews, and Delphi. Although all of these techniques can be used, most organizations will determine the best technique (or techniques) based on the threats to be assessed. Experience and education on the threats are needed.

Each member of the group who has been chosen to participate in the qualitative risk analysis uses their experience to rank the likelihood of each threat and the damage that might result. After each group member ranks the threat possibility, loss potential, and safeguard advantage, data is combined in a report to present to management. All levels of staff should be represented as part of the qualitative risk analysis, but it is vital that some participants in this process should have some expertise in risk analysis.

Quantitative Risk Analysis

A *quantitative risk analysis* assigns monetary and numeric values to all facets of the risk analysis process, including asset value, threat frequency, vulnerability severity, impact, safeguard costs, and so on. Equations are used to determine total and residual risks. The most common equations are for *single loss expectancy (SLE)* and *annual loss expectancy (ALE)*.

The SLE is the monetary impact of each threat occurrence. To determine the SLE, you must know the *asset value (AV)* and the *exposure factor (EF)*. The EF is the percent value or functionality of an asset that will be lost when a threat event occurs. The calculation for obtaining the SLE is as follows:

$$SLE = AV \times EF$$

For example, an organization has a web server farm with an AV of $10,000. If the risk assessment has determined that a power failure is a threat agent for the web server farm and the exposure factor for a power failure is 25 percent, the SLE for this event equals $2,500.

The *annual loss expectancy (ALE)* is the expected risk factor of an annual threat event. To determine the ALE, you must know the SLE and the annualized rate of occurrence (ARO). The ARO is the estimate of how often a given threat might occur annually. The calculation for obtaining the ALE is as follows:

$$ALE = SLE \times ARO$$

Using the previously mentioned example, if the risk assessment has determined that the ARO for the power failure of the web server farm is 50 percent, the ALE for this event equals $1,250.

Cost-Benefit Analysis

Using the ALE, the organization can decide whether to implement controls. If the annual cost of the control to protect the web server farm is more than the ALE, the organization could easily choose to accept the risk by not implementing the control. If the annual cost of the control to protect the web server farm is less than the ALE, the organization should consider implementing the control.

Handling Risk

Risk reduction is the process of altering elements of the organization in response to risk analysis. After an organization understands its total and residual risk, it must determine how to handle the risk. The following four basic methods are used to handle risk:

Avoidance Terminating the activity that causes a risk or choosing an alternative that is not as risky

Transfer Passing the risk on to a third party, including insurance companies

Mitigation Defining the acceptable risk level the organization can tolerate and reducing the risk to that level

Acceptance Understanding and accepting the level of risk as well as the cost of damages that can occur

Network Topologies

Understanding the types of network topologies that you may see will help you appreciate some of the security measures called for in various scenarios. In this section, you'll learn about some topologies that may exist in your organization.

CAN

The *campus area network* (CAN) comprises the part of the network where data, services, and connectivity to the outside world are provided to those who work in the corporate office or headquarters. It can be further subdivided into the following:

- *Enterprise core* connects the enterprise campus and the intranet data center.
- *Enterprise campus* includes the end devices and provides them access to the outside world and to the intranet data center through the enterprise core.
- *Intranet data center* includes the data center where resources are made available to the enterprise campus and to branch offices though the enterprise core.

Figure 1.3 shows the components of the CAN. It includes two parts that are not part of the enterprise campus (WAN edge and Internet edge) that comprise the networks that are used to connect to the outside world.

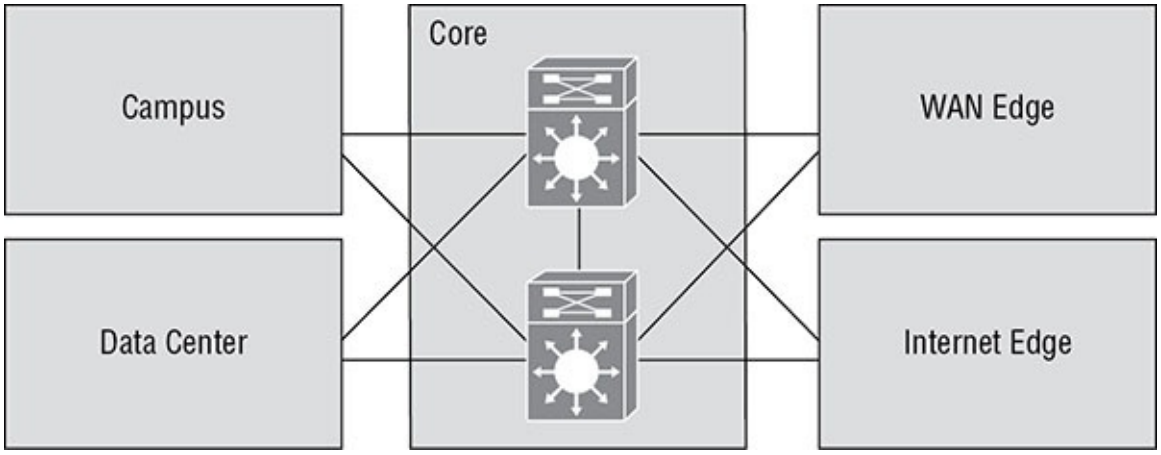

FIGURE 1.3 Campus area network

Security issues in the enterprise core include the following:

- Service disruptions (denial of service [DoS], distributed denial of service [DDoS])
- Unauthorized access (intrusions, routing protocol attacks)
- Data leaks and data modifications (packet sniffing, man in the middle [MITM] attacks)

Security issues in the enterprise campus include the following:

- Service disruptions (botnets, malware, DoS)
- Unauthorized access (intrusions, IP spoofing)
- Data leaks and data modifications (packet sniffing, MiTM attacks)
- Identify theft and fraud (phishing, email spam)

Security issues in the intranet data center include the following:

- Unauthorized access (device access, data access, privilege escalation)
- Service disruptions (botnets, DoS)
- Data leaks and data modifications (MITM, malware, scripting, SQL attacks)

WAN

The WAN connection of the organization is called the *enterprise WAN edge* in the Cisco network model. It is one of two modules that are used to connect the CAN to the outside world, the other being the enterprise Internet edge (shown in Figure 1.3). This comprises the provisioned WAN connections to other offices.

Security issues in the enterprise WAN edge include the following:

- Malicious branch client activity (malware, Trojans, botnets)
- Transmission threats (MITM, sniffing)
- Infrastructure attacks (reconnaissance, DoS, service attacks)

Data Center

While the data center may be located in the campus area network, it may also be located in the cloud. The introductions of cloud environments bring many benefits, but they also bring security threats. These threats include the following:

- Account or service hijacking
- Data loss
- Improper device hardening and patching
- DoS attacks
- Insecure APIs and user interfaces
- Malicious provider insiders
- Improper access from other tenants

SOHO

Many of today's workers operate from home rather than in the main office or headquarters. Other users will be operating from smaller branch offices. When this is the case, the *small office/home office (SOHO)* network will connect to the main office via the WAN edge module in cases where the connection is provisioned and via the Internet edge module when the connection leverages the Internet (such as a VPN connection). These two edge modules were shown in Figure 1.3. Since this module interfaces with those two modules, the security issues in the SOHO network will be the same as those present in the Internet edge and WAN edge modules.

Virtual

Today's data centers are increasingly moving to a virtual environment. When a virtual environment is present, it may reside in the campus data center, or it may reside in a cloud data center. Also, it is not unusual to find that the organization has both a physical data center and a virtual data center. Regardless of the exact configuration, there are challenges to securing a virtual environment.

In a virtual environment there are two traffic pathways, one that is used within the virtual environment and one used between the virtual environment and the physical environment. Physical security devices cannot be used to enforce security on the traffic that never leaves a physical host (traffic between VMs located on the same host) or on traffic that never leaves the virtual environment (traffic between VMs on different hosts). The solution is the deployment of virtual security devices such as the Cisco ASAv firewall, the Cisco CSR1000v router, and the Cisco Nexus 1000v switch.

Common Network Security Zones

One of the most basic design principles for a secure network calls for creating *security zones*. These are logical divisions of the network with access controls applied to control traffic between the zones. By organizing resources in these zones and applying the proper access controls, you can reduce the possibility that unauthorized access to data is allowed. In this section, you'll explore four common security zones.

DMZ

A *demilitarized zone (DMZ)* is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources. This can be accomplished using firewalls to isolate your network.

When establishing a DMZ, you assume that the person accessing the resource isn't necessarily someone you would trust with other information. By keeping the rest of the network from being visible to external users, this lowers the threat of intrusion in the internal network.

Any time you want to separate public information from private information, a DMZ is an acceptable option.

The easiest way to create a DMZ is to use a firewall that can transmit in these three directions:

- To the internal network
- To the external world (Internet)
- To the public information you're sharing (the DMZ)

From there, you can decide what traffic goes where; for example, HTTP traffic would be sent to the DMZ, and email would go to the internal network.

Intranet and Extranet

While DMZs are often used to make assets publicly available, extranets are used to make data available to a smaller set of the public—for example, a partner organization. *Intranet* is a term to describe the interior LAN; an *extranet* is a network logically separate from the intranet, the Internet, and the DMZ (if both exist in the design), where resources that will be accessed from the outside world are made available. Access may be granted to customers, business partners, and the public in general. All traffic between this network and the intranet should be closely monitored and securely controlled. Nothing of a sensitive nature should be placed in the extranet.

Public and Private

The purpose of creating security zones such as DMZs is to separate sensitive assets from those that require less protection. Because the goals of security and of performance and ease of use are typically mutually exclusive, not all networks should have the same levels of security.

Information that is of a public nature, or that you otherwise deem not to be of a sensitive nature, can be located in any of the zones you create. However, you should ensure that private corporate data and especially *personally identifiable information (PII)*—information that can be used to identify an employee or customer and perhaps steal their identity—is located only in secure zones and never in the DMZ or the extranet.

VLAN

Network security zones can also be created at layer 2. *Virtual local area networks (VLANs)* are logical subdivisions of a switch that segregate ports from one another as if they were in different LANs. VLANs offer another way to add a layer of separation between sensitive devices and the rest of the network. For example, if only one device should be able to connect to the finance server, the device and the finance server could be placed in a VLAN separate from the other VLANs. As traffic between VLANs can occur only through a router, ACLs can be used to control the traffic allowed between VLANs.

These VLANs can also span multiple switches, meaning that devices connected to switches in different parts of a network can be placed in the same VLAN regardless of physical location.

Summary

This chapter covered common security principles such as the CIA triad, the goals of which should guide all security initiatives. It also discussed common security terms such as risk, vulnerability, and threat, as well as the proper application of common security zones, such as Intranet, DMZ, and extranets. This chapter also discussed network topologies as seen from the perspective of the Cisco campus area network. Finally, the chapter discussed other methods of network segmentation such as VLANs.

Exam Essentials

Describe the CIA triad. Every security measure you implement should contribute to the achievement of one of three goals. The three fundamentals of security are confidentiality, integrity, and availability (CIA), often referred to as the CIA triad.

Define important security terms. Security professionals should become familiar with terms such as *assets*, *vulnerabilities*, *threats*, *threat agent*, *risk*, *exposure*, and *countermeasures*.

Identify common security zones. Describe *intranet*, *extranet*, *DMZ*, and the *Internet*. Explain their proper use.

Describe common network topologies. Explain various topologies as seen from the perspective of the Cisco campus area network such as the enterprise core, enterprise campus,

intranet data center, WAN edge, and intranet edge. Describe the common security issues found in each.

Review Questions

1. Which of the following is *not* one of the CIA triad?
   A. Confidentiality
   B. Integrity
   C. Availability
   D. Accountability
2. Which of the following requires that a user or process is given only the minimum access privilege needed to perform a particular task?
   A. Least privilege
   B. Separation of duties
   C. Job rotation
   D. Mandatory vacation
3. Which of the following occurs when a vulnerability is identified or exploited?
   A. Risk
   B. Threat
   C. Exposure
   D. Countermeasure
4. According to NIST SP 800-30, what is the first step in the risk management process?
   A. Identify threats
   B. Identify impact
   C. Identify vulnerabilities
   D. Identify the assets and their value
5. Which of the following is a measure of how freely data can be handled?
   A. Criticality
   B. Sensitivity
   C. Integrity
   D. Value
6. Which of the following is not a typical commercial data classification level?

A. Sensitive

B. Confidential

C. Secret

D. Public

7. Which of the following represents data shared only within a meeting in the TLP system?

A. Amber

B. White

C. Red

D. Green

8. Which of the following is a standard used by the security automation community used to enumerate software flaws and configuration issues?

A. TLP

B. CIA

C. SCAP

D. CAN

9. Which of the following is *not* a metric group in the Common Vulnerability Scoring System?

A. Base

B. Access vector

C. Temporal

D. Environmental

10. Which of the following is the monetary impact of each threat occurrence?

A. ALE

B. AV

C. ARO

D. SLE

11. Which method of handling risk involves defining the acceptable risk level the organization can tolerate and reducing the risk to that level?

A. Avoidance

B. Mitigation

C. Acceptance

D. Transfer

12. What part of the campus area network includes the end devices and provides them with access to the outside world and to the Intranet data center through the enterprise core?

    A. Intranet data center

    B. Enterprise campus

    C. Enterprise core

    D. Enterprise WAN edge

13. Which of the following is an area where you can place a public server for access by anyone?

    A. Intranet

    B. DMZ

    C. Internet

    D. Extranet

14. Which of the following is a logical subdivision of a switch that segregates ports from one another?

    A. VLAN

    B. VPN

    C. DMZ

    D. STP

15. Which of the following refers to the data being unaltered by unauthorized individuals?

    A. Confidentiality

    B. Integrity

    C. Availability

    D. Accountability

16. Which of the following refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers?

    A. Default to no access

    B. Defense in depth

    C. Separation of duties

    D. Job rotation

17. Which of the following is the probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out?

    A. Risk

B. Threat

C. Exposure

D. Countermeasure

18. Which of the following is a system that uses traffic light colors to classify information assets?

A. DLP

B. VLAN

C. TLP

D. VTP

19. Which component of SCAP refers to vulnerabilities in published operating systems and applications software?

A. CWE

B. CVE

C. CCE

D. CPE

20. Which of the following is the percent value or functionality of an asset that will be lost when a threat event occurs?

A. SLE

B. AV

C. EF

D. ALE

Chapter 2
Understanding Security Threats

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.2 Common security threats**
  - Identify common network attacks
  - Describe social engineering
  - Identify malware
  - Classify the vectors of data loss/exfiltration

To secure a network, you must have a clear understanding of the threats that the network faces. These threats come from all sorts of sources and have a variety of goals. In this chapter, you will continue your investigation of common security threats and their associated threat vectors.

In this chapter, you will learn the following:

Common security threats

Common Network Attacks

While new attacks and new motivations for those attacks seem to be arriving almost daily, there are some common attacks and common motivations for those attacks. In this chapter, you'll first learn about common motivations for attacks and common attack vectors that are simply various ways in which the attacks are implemented. Following that, you'll learn about some specific attacks that are quite common.

Motivations

Hackers hack for many different reasons. When you really get down to it, they want one of four things:

- Financial gain
- Disruption

- Geopolitical change
- Notoriety

The Federal Bureau of Investigation (FBI) has identified three categories of threat actors.

- Organized crime groups primarily threatening the financial services sector and expanding the scope of their attacks
- State sponsors, usually foreign governments, interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors
- Terrorist groups that want to impact countries by using the Internet and other networks to disrupt or harm the viability of our way of life by damaging our critical infrastructure

While there are other less organized groups out there, these three groups are considered to be the primary threat actors by law enforcement. However, organizations should not totally disregard the threat of any threat actors that fall outside these three categories. Lone actors or smaller groups that use hacking as a means to discover and exploit any discovered vulnerability can cause damage just like the larger, more organized groups.

Hacktivists This includes those who hack not for personal gain but to further a cause. An example is the Anonymous group that hacks from time to time for various political reasons.

Thrill hackers These guys do it for the notoriety. They deface websites and brag about their conquests to their fellow thrill hackers on websites where they share tools and methods.

Hacker and *cracker* are two terms that are often used interchangeably in media but do not actually have the same meaning. Hackers are individuals who attempt to break into secure systems to obtain knowledge about the systems and possibly use that knowledge to carry out pranks or commit crimes. Crackers, on the other hand, are individuals who attempt to break into secure systems without using the knowledge gained for any nefarious purposes.

In the security world, the terms *white hat*, *gray hat*, and *black hat* are more easily understood and less often confused than the terms *hackers* and *crackers*. A white hat does not have any malicious intent. A black hat has malicious intent. A gray hat is considered somewhere in the middle of the two. A gray hat will break into a system, notify the administrator of the security hole, and offer to fix the security issues for a fee.

Classifying Attack Vectors

After assets have been classified with regard to sensitivity and criticality (see Chapter 1), the next step is to identify threats. When determining vulnerabilities and threats to an asset, considering the threat agents first is often easiest. Threat agents can be grouped into the following six categories:

- Human includes both malicious and nonmalicious insiders and outsiders, terrorists, spies, and terminated personnel.

- Natural includes floods, fires, tornadoes, hurricanes, earthquakes, or other natural disaster or weather event.
- Technical includes hardware and software failure, malicious code, and new technologies.
- Physical includes CCTV issues, perimeter measures failure, and biometric failure.
- Operational includes any process or procedure that can affect CIA.

Examples of the threat actors include both internal and external actors and include the following:

- Internal actors
  - Reckless employee
  - Untrained employee
  - Partner
  - Disgruntled employee
  - Internal spy
  - Government spy
  - Vendor
  - Thief
- External actors
  - Anarchist
  - Competitor
  - Corrupt government official
  - Data miner
  - Government cyber warrior
  - Irrational individual
  - Legal adversary
  - Mobster
  - Activist
  - Terrorist
  - Vandal

Spoofing

Spoofing, also referred to as *masquerading*, occurs when communication from an attacker appears to come from trusted sources. The goal of this type of attack is to obtain access by

pretending to be that trusted source. Spoofing can be attempted based on the following:

- IP addresses
- MAC addresses
- Email addressees

Let's look at each one of these types of spoofing.

IP Address Spoofing

IP address spoofing is one of the techniques used by hackers to hide their trail or to masquerade as another computer. The hacker alters the IP address as it appears in the packet. This can sometimes allow the packet to get through an ACL that is based on IP addresses. It also can be used to make a connection to a system that trusts only certain IP addresses or ranges of IP addresses.

MAC Address Spoofing

MAC addresses can also be spoofed and used to get through MAC address filters. These filters are typically applied to control access to wireless access points at layer 2. They can also be used to impersonate another device connected to the same switch. In that scenario, it enables the impersonating device to receive traffic intended for the legitimate device. In Chapters 4 and 5 you will learn about methods to prevent these switch-based attacks.

Email Spoofing

Email spoofing is the process of sending an email that appears to come from one source when it really comes from another. It is made possible by altering the fields of email headers such as From, Return Path, and Reply-to. Its purpose is to convince the receiver to trust the message and reply to it with some sensitive information that the receiver would not have shared unless it was a trusted message.

Often this is one step in an attack designed to harvest usernames and passwords for banking or financial sites. This attack can be mitigated in several ways. One is SMTP authentication, which, when enabled, disallows the sending of an email by a user who cannot authenticate with the sending server.

Another possible mitigation technique is to implement the *Sender Policy Framework (SPF)*. 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.

Password Attacks

A password attack is one that attempts to discover user passwords. The two most popular password threats are dictionary attacks and brute-force attacks.

The best countermeasures against password threats are to implement complex password

policies, require users to change passwords on a regular basis, employ account lockout policies, encrypt password files, and use password-cracking tools to discover weak passwords.

Dictionary Attack

A *dictionary attack* occurs when attackers use a dictionary of common words to discover passwords. An automated program uses the hash of the dictionary word and compares this hash value to entries in the system password file. Although the program comes with a dictionary, attackers also use extra dictionaries that are found on the Internet.

You should implement a security rule that says that a password must *not* be a word found in the dictionary to protect against these attacks.

Brute-Force Attack

Brute-force attacks are more difficult to carry out because they work through all possible combinations of numbers and characters. A brute-force attack is also referred to as an *exhaustive attack*. It carries out password searches until a correct password is found. These attacks are also very time-consuming.

Reconnaissance Attacks

Reconnaissance attacks are carried out to gather information about the organizational network as a prelude to a larger attack. It is also sometimes called *fingerprinting* the network. It is the first step that a penetration tester will take because it mimics the first step of a real attacker. There are several ways in which information can be gathered about the network topology. Let's take a look at the three most common.

Ping Scans

Ping scans involve identifying the live hosts on a network or in a domain namespace. Nmap and other scanning tools (ScanLine, SuperScan) can be used for this. It records responses to pings sent to every address in the network. It can also be combined with a port scan by using the proper arguments to the command.

To execute this scan from nmap, the command is `nmap -sP 192.168.0.0-100` (`0-100` is the range of IP addresses to be scanned in the 192.168.0.0 network). Figure 2.1 shows an example of the output. All devices that are on will be listed. For each the MAC address will also be listed.

FIGURE 2.1 Ping scan with nmap

Port Scans

As operating systems have well-known vulnerabilities, so do common services. By determining the services that are running on a system, the attacker also discovers potential vulnerabilities of the service of which he may attempt to take advantage. This is typically done with *port scans* in which all "open" or "listening" ports are identified. Once again, the lion's share of these issues will have been mitigated with the proper security patches, but that is not always the case, and it is not uncommon for security analysts to find that systems that are running vulnerable services are missing the relevant security patches. Consequently, when performing service discovery, patches should be checked on systems found to have open ports. It is also advisable to close any ports not required for the system to do its job.

Nmap is one of the most popular port scanning tools used today. By performing scans with certain flags set in the scan packets, security analysts (and hackers) can make certain assumptions based on the responses received. These flags are used to control the TCP connection process, so they are present only in those packets. Figure 2.2 shows a TCP header. The flags of which I speak are circled. Normally the flags that are "turned on" will be done as a result of the normal TCP process, but a hacker can craft packets with the flags checked that the hacker desires.

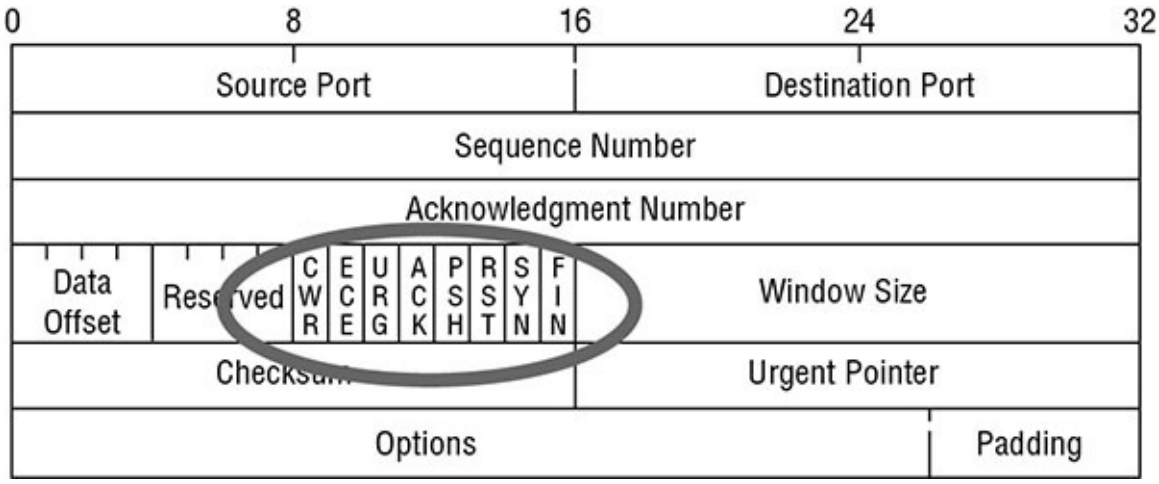

FIGURE 2.2 TCP header

These are the flags shown:

- URG: Urgent pointer field significant
- ACK: Acknowledgment field significant
- PSH: Push function
- RST: Reset the connection
- SYN: Synchronize sequence numbers
- FIN: No more data from sender

By performing scans with certain flags set in the scan packets, security analysts (and hackers) can make certain assumptions based on the responses received

Nmap exploits weaknesses with three scan types.

- A *NULL scan* is a series of TCP packets that contain a sequence number of 0 and no set flags. Because the NULL scan does not contain any set flags, it can sometimes penetrate firewalls and edge routers that filter incoming packets with particular flags. When this packet is sent, these responses are possible:
  - No response: The port is open on the target.
  - RST: The port is closed on the target.

  Figure 2.3 shows the result of this scan using the command `nmap -sN`. In this case, nmap is unable to determine whether the port is open or closed because there was no response, but you don't know if the port is closed or if the firewall is blocking the port. That's why they are listed as open/filtered.
- A *FIN scan* sets the FIN bit set. When this packet is sent, these responses are possible.
  - No response: The port is open on the target.
  - RST/ACK: The port is closed on the target.

The following is sample output of this scan using the command `nmap -sF`. I added `-v` for verbose output. Again, in this case, nmap is unable to determine whether the port is open or closed because there was no response, but you don't know if the port is closed or if the firewall is blocking the port. That's why they are listed as open/filtered.

FIGURE 2.3 NULL scan

```
# nmap -sF -v 192.168.0.7

Starting nmap 3.81 at 2016-01-23 21:17 EDT
Initiating FIN Scan against 192.168.0.7 [1663 ports] at 21:17
The FIN Scan took 1.51s to scan 1663 total ports.
Host 192.168.0.7 appears to be up ... good.
Interesting ports on 192.168.0.7:
(The 1654 ports scanned but not shown below are in state: closed)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
79/tcp   open|filtered finger
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
514/tcp  open|filtered shell
886/tcp  open|filtered unknown
2049/tcp open|filtered nfs
MAC Address: 00:03:47:6D:28:D7 (Intel)

Nmap finished: 1 IP address (1 host up) scanned in 2.276 seconds
               Raw packets sent: 1674 (66.9KB) | Rcvd: 1655 (76.1KB)
```

- An *XMAS scan* sets the FIN, PSH, and URG flags. When this packet is sent, these responses are possible:
  - No response: The port is open on the target.

- RST: The port is closed on the target.

Figure 2.4 shows the result of this scan using the command `nmap -sX`. In this case, nmap is unable to determine whether the port is open or closed because there was no response, but you don't know if the port is closed or if the firewall is blocking the port. That's why they are listed as open/filtered.

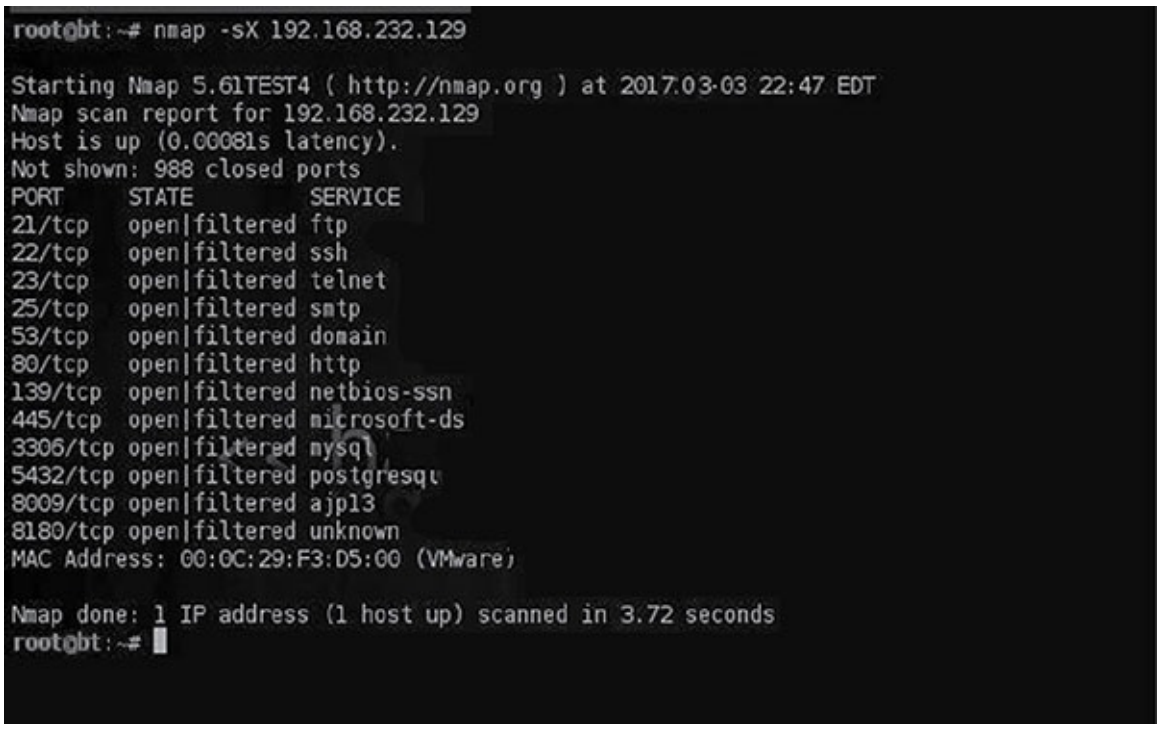

FIGURE 2.4 XMAS scan

These three scans (NULL, FIN, and XMAS) all serve the same purpose (to discover open ports and ports blocked by a firewall) and differ only in the switch used. While there are many more scan types and attacks that can be launched with this tool, these scan types are commonly used during environmental reconnaissance testing to discover what the hacker might discover before the hacker does and take steps to close any gaps in security.

OS Fingerprinting

Operating system fingerprinting is simply the process of using some method to determine the operating system running on a host or a server. Its value to the hacker is that by identifying the OS version and build number, common vulnerabilities of that operating system can be identified using readily available documentation from the Internet. While many of the issues will have been addressed in subsequent service packs and hotfixes, there might be zero-day weaknesses (those that have not been widely publicized or addressed by the vendor) the hacker may be able to leverage in the attack. Moreover, if any of the relevant security patches have not been applied, the weaknesses the patch was intended to address will exist on the machine. Therefore, the purpose of attempting OS fingerprinting during assessment is to assess the relative ease with which it can be done and identifying methods to make it more difficult.

Buffer Overflow

Buffers are portions of system memory that are used to store information. A *buffer overflow* is an attack that occurs when the amount of data that is submitted to data is larger than the buffer can handle. Typically, this type of attack is possible because of poorly written application or operating system code. This can result in an injection of malicious code, primarily either a denial-of-service attack or a SQL injection.

To protect against this issue, organizations should ensure that all operating systems and applications are updated with the latest service packs and patches. In addition, programmers should properly test all applications to check for overflow conditions. Hackers can take advantage of this phenomenon by submitting too much data, which can cause an error or in some cases execute commands on the machine if the hacker can locate an area where commands can be executed. Not all attacks are designed to execute commands. An attack may just lock the computer as in a DoS attack.

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. The key to preventing many buffer overflow attacks is input validation, in which any input is checked for format and length before it is used. Buffer overflows and boundary errors (when input exceeds the boundaries allotted for the input) are a family of error conditions called *input validation errors*.

DoS

A *denial-of-service (DoS)* attack occurs when attackers flood a device with enough requests to degrade the performance of the targeted device. Some popular DoS attacks include SYN floods, pings of death, and smurf attacks. Let's explore how these attacks work.

TCP SYN Flood

To understand a *TCP SYN flood* attack, you must understand the three-way TCP handshake, which occurs whenever a TCP connection is made. Figure 2.5 displays the process.

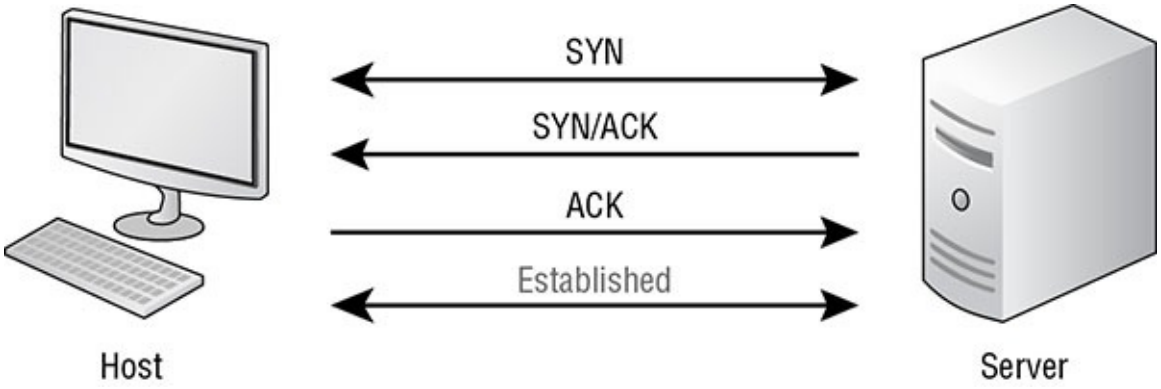

FIGURE 2.5 TCP handshake

One important fact not evident in the figure is that when the recipient of the initial SYN packet

receives that packet and responds by sending a SYN/ACK packet, it will reserve a small piece of memory for the expected response (ACK). In the attack the attacker sends thousands of these SYN packets and *never* answers the SYN/ACK packets with an ACK packet. At some point, the recipient will fill up its memory, reserving space for the responses that never come. Then the target will be unable to do anything and is thus the denial of service. Figure 2.6 shows the attack. At the point in the diagram where it says TCP Queue Full, the target memory is full.

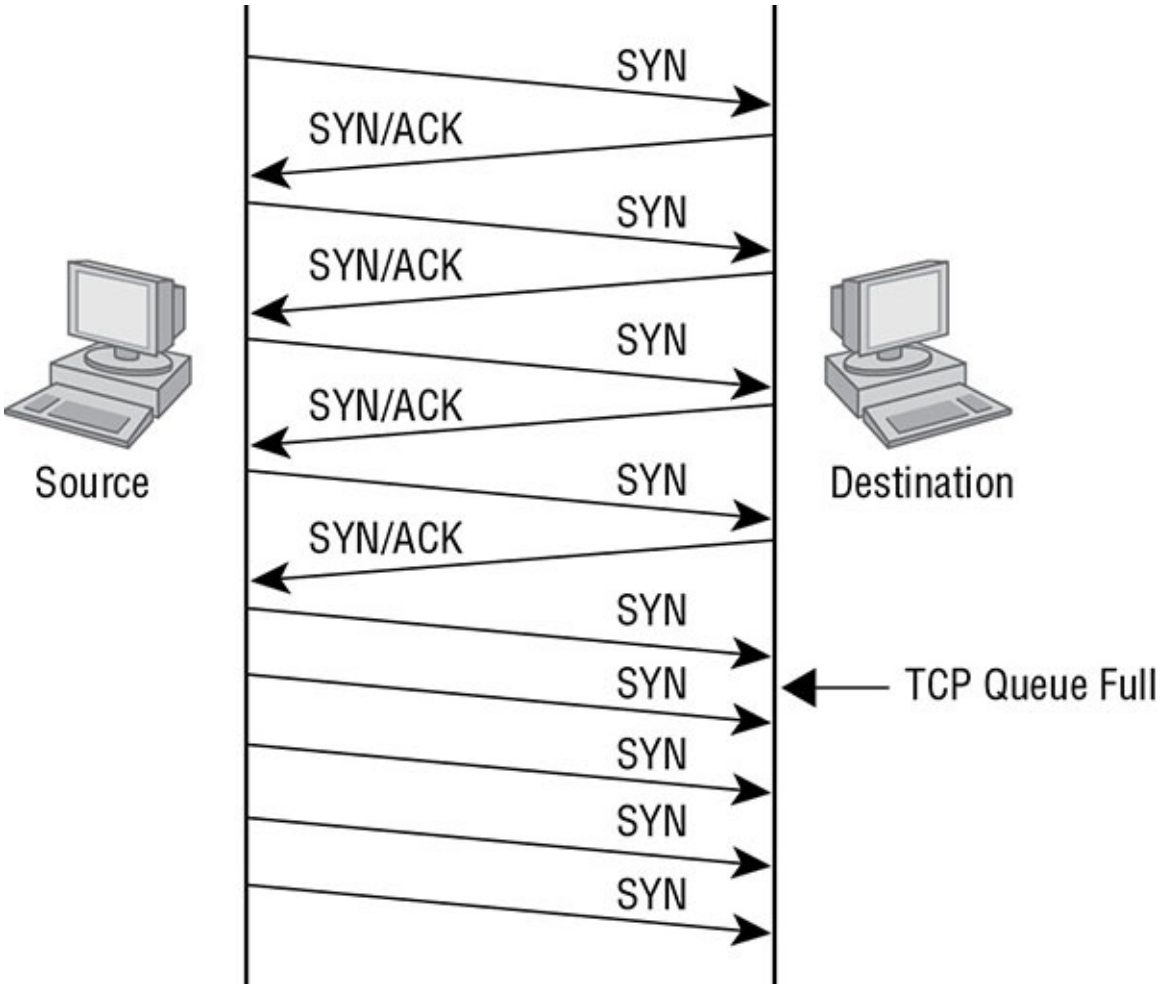

FIGURE 2.6 SYN flood

Ping of Death

A *ping of death* is when an oversized ICMP packet is sent to the target. The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes. An ICMP echo request is an IP packet with a pseudoheader, which is 8 bytes. Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes (65,535 – 20 – 8 = 65,507).

A grossly oversized ICMP packet can trigger a range of adverse system reactions such as DoS, crashing, freezing, and rebooting. Figure 2.7 shows such a packet. The packet will be fragmented en route, and when the target attempts to reassemble the packet, it will crash some systems.

FIGURE 2.7 Ping-of-death packet

DDoS

A *distributed DoS (DDoS)* attack is a DoS attack that is carried out from multiple attack locations. Vulnerable devices are infected with software agents, called *zombies*. This turns the vulnerable devices into botnets, which then carry out the attack.

Because of the distributed nature of the attack, identifying all the attacking botnets is virtually impossible. The botnets also help to hide the original source of the attack. These attacks can be direct, reflected, and amplified. Let's look at examples of each.

Direct DDoS

In a *direct DDoS* attack, the attacker launches the attack by sending the attack signal to the handlers, which in turn signal the zombies to attack, as shown in Figure 2.8 . The attack is greatly amplified by the use of the zombies. So, a direct attack is also an amplified attack.

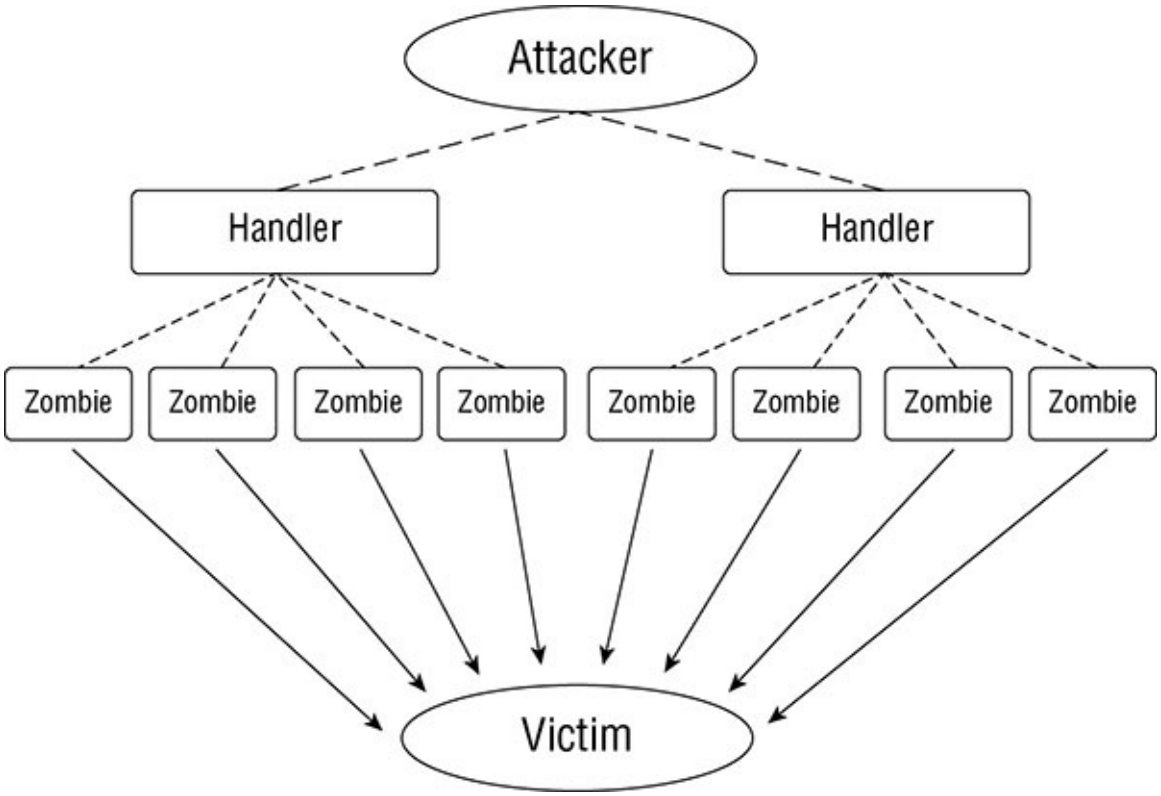

FIGURE 2.8 Direct DDoS

Reflection

In a reflected DDoS attack, the attack is bounced off a large number of devices without actually recruiting the devices as zombies. A good example of the *reflection* type of DDoS is the smurf

attack. In the smurf attack, the attacker sends an ICMP packet to the broadcast address of the network in which the target resides. However, the hacker creates this ICMP packet with a spoofed source address and that spoofed address is that of the target. When every device in the network answers the ping requests, the answers will go to the target. Typically, the hacker will set the number of pings to a very high number so that this continues for some time and uses all the resources of the web server, as shown in Figure 2.9 .

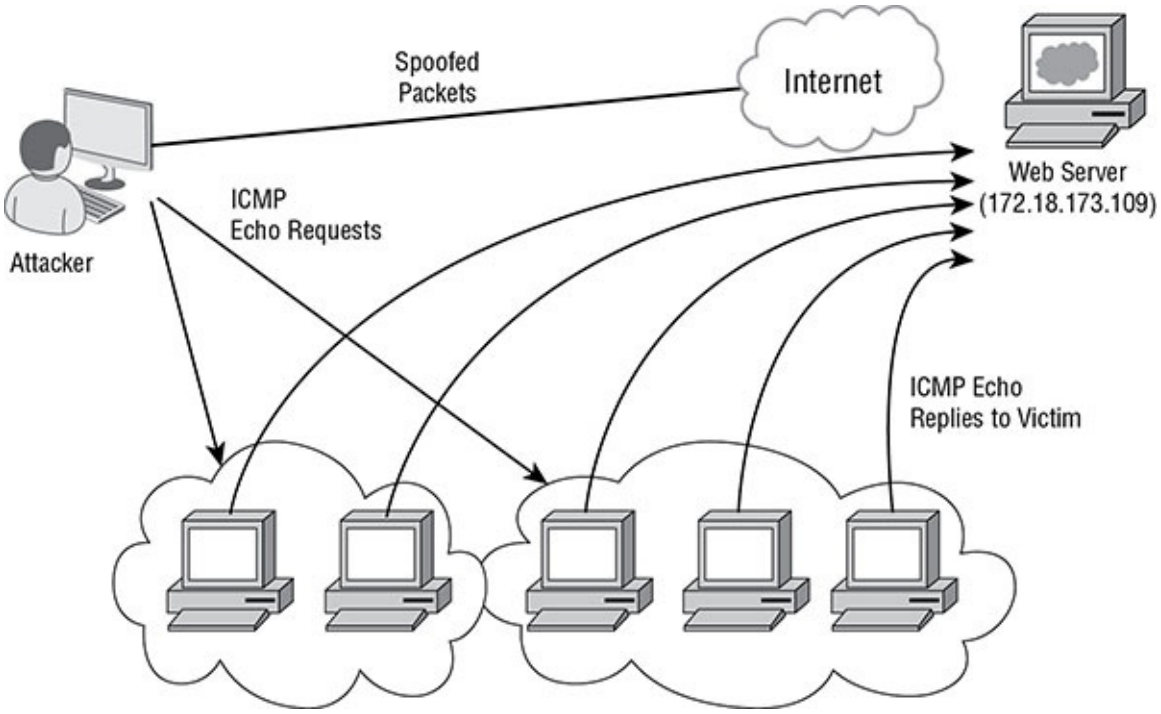

FIGURE 2.9 Smurf attack

Man-in-the-Middle Attack

A *man-in-the-middle (MITM)* attack is when an active attacker listens to the communication between two communicators and changes the contents of this communication. While performing this attack, the attacker pretends to be one of the parties to the other party. The most common type of MITM attack is done at layer 2 and uses the technique described in the next attack to pollute the ARP cache of the targets.

ARP Poisoning

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 *ARP poisoning* by answering ARP requests for another computer's IP address with their 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 the attacker "in the middle."

Two mitigation techniques are available for preventing ARP poisoning on a Cisco switch.

Dynamic ARP Inspection (DAI) This security feature 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. This table is built by also monitoring all DHCP requests for IP addresses and maintaining the mapping of each resulting IP address to a MAC address (which is part of DHCP snooping). If an incorrect mapping is attempted, the switch rejects the packet.

DHCP Snooping The main purpose of DHCP snooping is to prevent a poisoning attack on the DHCP database. This is not a switch attack per se, but one of its features can support DAI. It creates a mapping of IP addresses to MAC addresses from a trusted DHCP server that can be used in the validation process of DAI.

You must implement both DAI and DHCP snooping because DAI depends on DHCP snooping. Both configurations will be covered in Chapter 6.

Social Engineering

Social engineering attacks occur when attackers use believable language and user gullibility to obtain user credentials or some other confidential information. In this section we are going to focus our attention on a social engineering attack that has been in the news quite a bit lately: phishing.

Phishing/Pharming

Phishing is a social engineering attack in which attackers try to learn personal information, including credit card information and financial data. This type of attack is usually carried out by implementing a fake website that very closely resembles a legitimate website. Users enter data, including credentials on the fake website, allowing the attackers to capture any information entered. Spear phishing is a phishing attack carried out against a specific target by learning about the target's habits and likes. Spear phishing attacks take longer to carry out than phishing attacks because of the information that must be gathered.

Pharming is similar to phishing, but pharming actually pollutes the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

Prevention

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.

Caution users against using any links embedded in e-mail messages, even if the message appears to have come from a legitimate entity. Users should also review the address bar any time they access a site where their personal information is required to ensure that the site is correct and that SSL is being used, which is indicated by an HTTPS designation at the beginning of the URL address.

Malware

Malicious software, also called *malware*, is any software that is designed to perform malicious acts. The following are the four classes of malware you should understand:

Virus Any malware that attaches itself to another application to replicate or distribute itself

Worm Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate

Trojan Horse Any malware that disguises itself as a needed application while carrying out malicious actions

Spyware Any malware that collects private user data, including browsing history or keyboard input

The best defense against malicious software is to implement antivirus and anti-malware software. Today most vendors package these two types of software in the same package. Keeping antivirus and anti-malware software up-to-date is vital. This includes ensuring that the latest virus and malware definitions are installed.

Data Loss and Exfiltration

Data exfiltration is the unauthorized transfer of data from a computer or from a storage device. At its most serious level, it is the ultimate goal of advanced persistent threats (APTs), which are those that continue on a long-term basis and are carried out by highly skilled cybercriminals. These groups are not interested in the vacation photos of the receptionist. They are interested in three types of data that they can monetize. Let's look at these data types.

IP

Intellectual property is property that is considered to be a unique creation of the mind and includes books, music, logos, inventions, and slogans. These items can be protected by copyrights, patents, trademarks, and registrations. However, it also includes things that cannot be protected with these mechanisms such as organizational plans, formulas, recipes, customer lists, and other types of data that cannot be disclosed because it might eliminate or reduce the effectiveness of a business advantage. Attack vectors for IP include disgruntled employees, competitors performing corporate espionage, and inadvertent releases though social media.

PII

Personally identifiable information (PII) is any piece of data that can be used alone or with other information to identify a single person. Any PII that an organization collects must be protected in the strongest manner possible. PII includes full name, identification numbers (including driver's license number and Social Security number), date of birth, place of birth, biometric data, financial account numbers (both bank account and credit card numbers), and digital identities (including social media names and tags).

Keep in mind that different countries and levels of government can have different qualifiers for identifying PII. Security professionals must ensure that they understand international, national, state, and local regulations and laws regarding PII. As the theft of this data becomes even more prevalent, you can expect more laws to be enacted that will affect your job.

Credit Card

While PII can be used to perform identity theft, stealing credit card information provides a much quicker path to monetizing malicious activities. Many of the most high-profile data breaches have involved the harvesting of thousands of credit card numbers and the related information that makes them usable. When an organization suffers this type of disclosure, it hurts their reputation because they must inform every user whose data was disclosed. They will also be responsible for any harm suffered by the disclosure, so this is a real nightmare when it occurs. The best mitigation for this is to adopt all recommendations of the Payment Card Industry Data Security Standard (PCI-DSS).

Summary

This chapter covered common network attacks and their motivations. It also discussed various attack vectors, such as malicious and nonmalicious insiders and outsiders, terrorists, spies, and terminated personnel. The chapter also looked at various methods used to perform network reconnaissance, such as ping scans and port scans. Finally, the chapter covered types of malware and the exfiltration of sensitive data such as IP, PII, and credit card data.

Exam Essentials

Describe attack motivations. These include financial gain, disruption, geopolitical change, and notoriety. They may be attempted by organized crime groups, state sponsors, terrorist groups, hacktivists, and thrill hackers.

Identify common network attacks. These include but are not limited to IP address spoofing, MAC address spoofing, and email spoofing. They also include password attacks such as dictionary and brute-force attacks. Finally, explain reconnaissance attacks such as ping scans, port scans, and SYN scans.

Explain social engineering attacks. Describe phishing and pharming attacks and how these attacks can lead to malware such as viruses, worms, and Trojan horses.

Define the types of information most susceptible to data exfiltration. These include personally identifiable information (PII), intellectual property, and credit card information. Provide examples for each type of data.

Review Questions

1. What is the typical motivation of a hacktivist?
   A. Financial gain
   B. Disruption
   C. Geopolitical change
   D. Notoriety
2. Which of the following attacks has as its goal to get through an ACL on a router?
   A. IP address spoofing
   B. MAC address spoofing
   C. Email spoofing
   D. Buffer overflow
3. Which of the following is *not* a form of password attack?
   A. Brute force
   B. Dictionary
   C. Port scan
   D. Social engineering
4. When executing a NULL scan, which response indicates the port is closed on the target?
   A. No response
   B. Destination unreachable
   C. RST
   D. ACK
5. Which of the following is a measure used to prevent buffer overflows?
   A. Input validation
   B. Multifactor authentication
   C. Complex passwords
   D. Sensitivity labels
6. Which of the following is not a DDoS attack?
   A. SYN flood
   B. Ping of death
   C. Smurf attack
   D. Man-in-the-middle

7. Which of the following is typically used to set up a man-in-the-middle attack?
   A. ARP poisoning
   B. Dynamic ARP inspection
   C. Rogue switches
   D. MAC overflow
8. Which of the following is mitigation for ARP poisoning?
   A. Input validation
   B. DAI
   C. Multifactor authentication
   D. Rootguard
9. Which of the following must be implemented to use DAI?
   A. DTP
   B. Authenticated ARP
   C. DHCP snooping
   D. NAT
10. Which of the following attaches itself to another application to replicate or distribute itself?
   A. Worm
   B. Rootkit
   C. Spyware
   D. Virus
11. Which of the following is considered to be a unique creation of the mind?
   A. PII
   B. IP
   C. PHI
   D. IPS
12. Which of the following provides recommendations for securely handling credit card data?
   A. HIPAA
   B. SOX
   C. PCI-DSS

D. GLBA

13. At what OSI layer does MAC address spoofing occur?
    A. 1
    B. 2
    C. 3
    D. 4
14. Which of the following is mitigation for email spoofing?
    A. SPF
    B. DAI
    C. DNSSec
    D. DHCP snooping
15. Which of the following is a common tool used for ping and port scans?
    A. Metasploit
    B. Nmap
    C. Netstat
    D. Snort
16. Which of the following is *not* a flag set in an XMAS scan?
    A. FIN
    B. PSH
    C. SYN
    D. URG
17. Which of the following attacks uses an oversized ICMP packet?
    A. Ping of death
    B. Smurf
    C. Fraggle
    D. SYN flood
18. Which of the following is a reflected DDoS attack?
    A. Ping of death
    B. Smurf
    C. Buffer overflow

D. XXS

19. Which attack type does DAI address?

A. IP spoofing

B. MAC overflow

C. ARP poisoning

D. Ping of death

20. Which of the following pollutes the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site?

A. Phishing

B. Pharming

C. Vishing

D. Whaling

Chapter 3
Understanding Cryptography

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **1.3 Cryptography concepts**
  - Describe key exchange
  - Describe hash algorithm
  - Compare and contrast symmetric and asymmetric encryption
  - Describe digital signatures, certificates, and PKI

Cryptography is the use of mathematical algorithms to scramble data so it cannot be read if captured. In that role cryptography provides confidentiality, but that is not the only security goal it can achieve. Through the use of hash values and digital signatures, it can also provide assurance of data integrity and origin authentication. This chapter will cover the types of cryptography, their strengths and weaknesses, and some of the services that cryptography can provide.

In this chapter, you will learn the following:

Cryptography concepts

Symmetric and Asymmetric Encryption

There are two types of cryptography algorithms that you must understand, symmetric and asymmetric. A bit later in this section you will learn the differences between these two systems and the advantages and disadvantages of both. You'll also learn when to apply these algorithms to secure both data at rest and data in transit.

But first let's look at some basic concepts used in cryptography. First you'll be introduced to some of the various ways algorithms scramble the data. Then you'll learn about two different ways encryption algorithms operate on the data.

Ciphers

Cryptographic algorithms are often called *ciphers* for short, and these ciphers are

mathematical formulas that move the data around in various ways to scramble it. The two main methods are substitution and transposition. I'll cover these in this section, along with a method of addressing shortcomings of substitution. Ciphers also differ in the amount of data that is encrypted at a time. The two main types of algorithms with respect to this issue are block and stream ciphers, which will also be covered in this section.

Substitution

A *substitution cipher* uses a key to substitute characters or character blocks with different characters or character blocks. The Caesar cipher and the Vigenère cipher are two of the earliest forms of substitution ciphers. Figure 3.1 shows the ROT13, which is a Caesar cipher. It rotates the alphabet 13 positions. Therefore, the message "Hello" encrypts to the ciphertext URYYB.

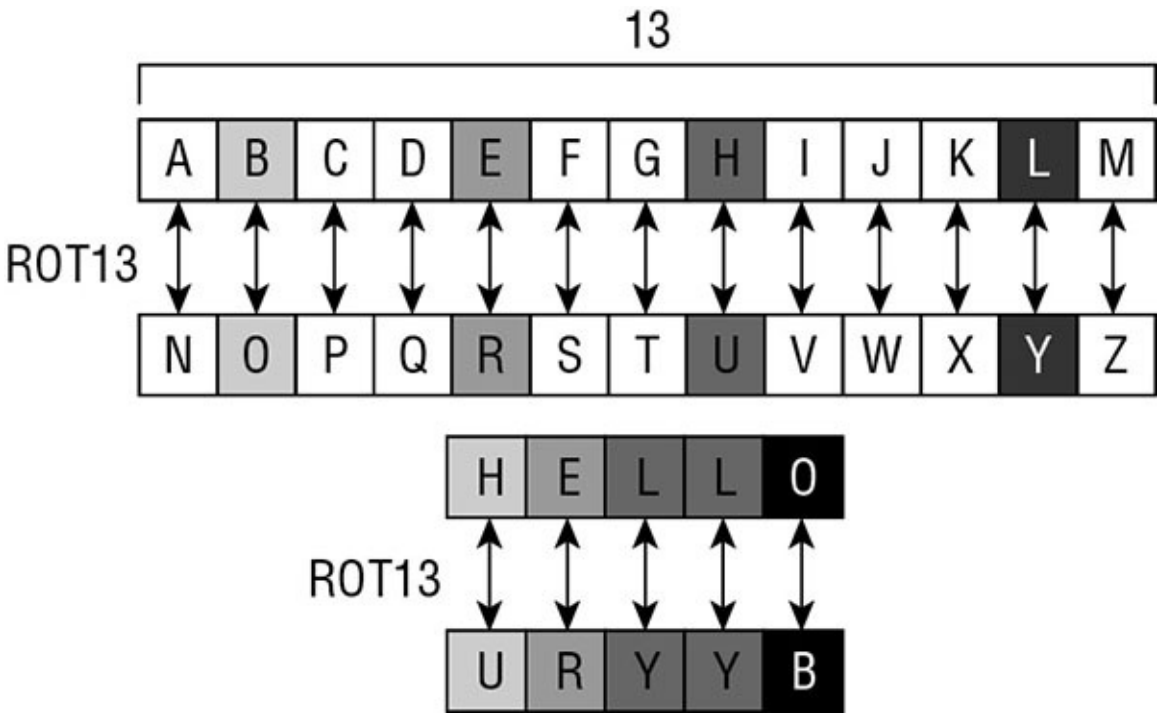

FIGURE 3.1 ROT 13 Caesar cipher

One of the issues with substitution ciphers is if the message is of sufficient length, patterns in the encryption begin to become noticeable, which makes it vulnerable to a frequency attack. A frequency attack is when the attacker uses these recurring patterns to reverse engineer the message. For this reason, the polyalphabetic algorithm was created.

Polyalphabetic

To increase the difficulty of performing a frequency attack, *polyalphabetic algorithms* were created. They use multiple instances of the alphabet shifted in a 26 × 26 table called a *tableau*, shown in Figure 3.2 . The figure shows the Vigenère cipher, an example of a polyalphabetic cipher.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE 3.2 Vigenère cipher

As an example of a message on which the Vigenère cipher is applied, let's use the security key SYBEX and the plaintext message of WE ATTACK AT FIVE. The first letter in the plaintext message is *W*, and the first letter in the key is *S*. We should locate the letter *W* across the headings for the columns. We follow that column down until it intersects with the row that starts with the letter *S*, resulting in the letter *O*. The second letter of the plaintext message is *E*, and the second letter in the key is *Y*. Using the same method, we obtain the letter *C*. We continue in this same manner until we run out of key letters, and then we start over with the key, which would result in the second *A* in the plaintext message working with the letter *S* of the key.

So, applying this technique to the entire message of WE ATTACK AT FIVE, the plaintext message converts to the OCBXQSALEQXGWI ciphertext message.

Transposition

A *transposition cipher* scrambles the letters of the original message in a different order. The key determines the positions to which the letters are moved.

The following is an example of a simple transposition cipher:

```
Original message            SNOWFLAKES WILL FALL
Broken into groups          SNOW   FLAK    ESWI   FALL
Key                         4231   2314    4231   2314
Ciphertext message          WONS   LAFK    IWSE   ALFL
```

With this example, the original message is SNOWFLAKES WILL FALL, and the key is 4231 2314. The ciphertext message is WONS LAFK IWSE ALFL. So, you take the first four letters

of the plaintext message (SNOW) and use the first four numbers (4231) as the key for transposition. The key describes the relative potions of the same characters in the ciphertext. In the new ciphertext, the letters would be WONS. Then you take the next four letters of the plaintext message (FLAK) and use the next four numbers (2314) as the key for transposition. In the new ciphertext, the letters would be LAFK. Then you take the next four letters of the original message and apply the first four numbers of the key because you do not have any more numbers in the key. Continue this pattern until complete.

Algorithms

While cryptographic algorithms can deploy either substitution or transposition, there is another key characteristic that differentiates two main classes of algorithms: symmetric and asymmetric. In the next two sections, I'll talk about how they are different.

Symmetric

Symmetric algorithms use a private or secret key that must remain secret between the two parties. Each party pair requires a separate private key. Therefore, a single user would need a unique secret key for every user with whom she communicates.

Consider an example where there are 10 unique users. Each user needs a separate private key to communicate with the other users. To calculate the number of keys that would be needed in this example, you would use the following formula:

```
# of users × (# of users – 1) / 2
```

Using our example, you would calculate 10 × (10 – 1) / 2, or 45 needed keys.

With symmetric algorithms, the encryption key must remain secure. To obtain the secret key, the users must find a secure out-of-band method for communicating the secret key, including courier or direct physical contact between the users.

A special type of symmetric key called a *session key* encrypts messages between two users during one communication session. Symmetric algorithms can be referred to as *single-key*, *secret-key*, *private-key*, or *shared-key cryptography*.

Symmetric systems provide confidentiality but not authentication or nonrepudiation. If both users use the same key, determining where the message originated is impossible. Symmetric algorithms include DES, AES, 3DES, and RC4. Table 3.1 lists the strengths and weaknesses of symmetric algorithms.

TABLE 3.1 Symmetric algorithm strengths and weaknesses

Strengths	Weaknesses
Cheaper to implement than asymmetric	Key compromise can occur more easily than with asymmetric
Faster than asymmetric	Difficulty in performing secure key distribution
Hard to crack	Key compromise occurs if one party compromised, thereby allowing impersonation

The two broad types of symmetric algorithms are *stream-based ciphers* and *block ciphers*. *Initialization vectors (IVs)* are an important part of block ciphers. These three components will be discussed in the next sections.

Block

Another way in which ciphers can differ is in the amount of data that is encrypted at a time. Block ciphers perform encryption by breaking the message into fixed-length units. A message of 1,024 bits could be divided into 16 blocks of 64 bits each. Each of those 16 blocks is processed by the algorithm formulas, resulting in a single block of ciphertext.

Advantages of block ciphers include the following:

- The implementation is easier than stream-based cipher implementation.
- They are generally less susceptible to security issues.
- They are generally used more in software implementations.

Block ciphers employ both substitution and transposition.

Stream

Stream-based ciphers perform encryption on a bit-by-bit basis and use keystream generators. The keystream generators create a bit stream that is XORed with the plaintext bits. The result of this XOR operation is the ciphertext.

A synchronous stream-based cipher depends only on the key, and an asynchronous stream cipher depends on the key and plaintext. The key ensures that the bit stream that is XORed to the plaintext is random.

An example of a stream-based cipher is RC4.

Advantages of stream-based ciphers include the following:

- They generally have lower error propagation because encryption occurs on each bit.
- They are generally used more in hardware implementation.
- They use the same key for encryption and decryption.
- They are generally cheaper to implement than block ciphers.

- The employ only substitution.

Initialization Vectors

Some modes of symmetric key algorithms use initialization vectors to ensure that patterns are not produced during encryption. These IVs provide this service by using random values with the algorithms. Without using IVs, a repeated phrase within a plaintext message could result in the same ciphertext. Attackers can possibly use these patterns to break the encryption.

Digital Encryption Standard (DES)

Digital Encryption Standard (DES) uses a 64-bit key, 8 bits of which are used for parity. Therefore, the effective key length for DES is 56 bits. DES divides the message into 64-bit blocks. Sixteen rounds of transposition and substitution are performed on each block, resulting in a 64-bit block of ciphertext.

DES has mostly been replaced by 3DES and AES, both of which are discussed later in this chapter.

3DES

Because of the need to quickly replace DES, Triple DES (*3DES*), a version of DES that increases security by using three 56-bit keys, was developed. Although 3DES is resistant to attacks, it is up to three times slower than DES. 3DES did serve as a temporary replacement to DES. However, the National Institute of Standards and Technology (NIST) has actually designated the Advanced Encryption Standard (AES) as the replacement for DES, even though 3DES is still in use today.

DES can operate in a number of different modes, but the two most common are Electronic Code Book (ECB) and Cipher Block Chaining (CBC). In ECB, 64-bit blocks of data are processed by the algorithm using the key. The ciphertext produced can be padded to ensure that the result is a 64-bit block. If an encryption error occurs, only one block of the message is affected. ECB operations run in parallel, making it a fast method.

Although ECB is the easiest and fastest mode to use, it has security issues because every 64-bit block is encrypted with the same key. If an attacker discovers the key, all the blocks of data can be read. If an attacker discovers both versions of the 64-bit block (plaintext and ciphertext), the key can be determined. For these reasons, the mode should not be used when encrypting a large amount of data because patterns would emerge. ECB is a good choice if an organization needs encryption for its databases because ECB works well with the encryption of short messages.

Figure 3.3 shows the ECB encryption process.

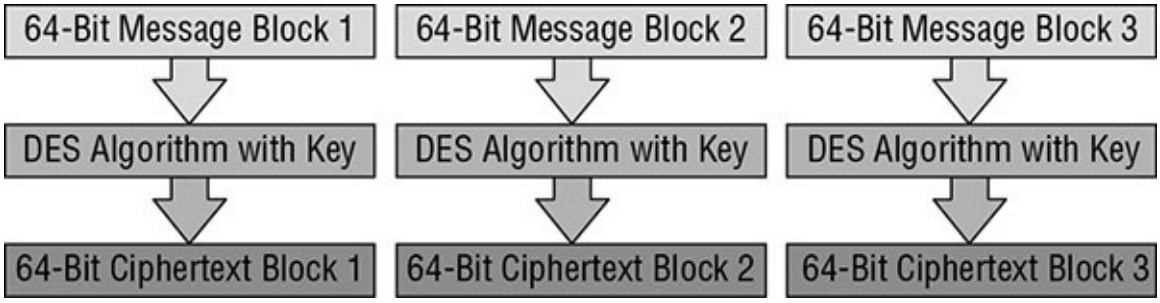

FIGURE 3.3 ECB process

In CBC, each 64-bit block is chained together because each resultant 64-bit ciphertext block is applied to the next block. So, plaintext message block 1 is processed by the algorithm using an IV. The resultant ciphertext message block 1 is XORed with plaintext message block 2, resulting in ciphertext message 2. This process continues until the message is complete.

Unlike ECB, CBC encrypts large files without having any patterns within the resulting ciphertext. If a unique IV is used with each message encryption, the resultant ciphertext will be different every time even in cases where the same plaintext message is used.

Figure 3.4 shows the CBC encryption process.

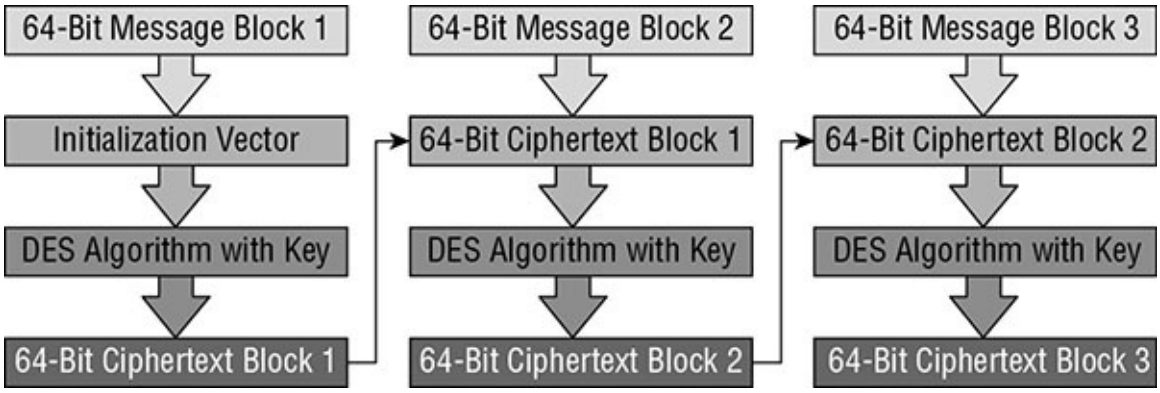

FIGURE 3.4 CBC process

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is the replacement algorithm for DES. Although AES is considered the standard, the algorithm that is used in the AES standard is the Rijndael algorithm. The AES and Rijndael terms are often used interchangeably.

The three block sizes that are used in the Rijndael algorithm are 128, 192, and 256 bits. A 128-bit key with a 128-bit block size undergoes 10 transformation rounds. A 192-bit key with a 192-bit block size undergoes 12 transformation rounds. Finally, a 256-bit key with a 256-bit block size undergoes 14 transformation rounds.

Rijndael employs transformations composed of three layers: nonlinear layer, key addition layer, and linear-maxing layer. The Rijndael design is very simple, and its code is compact, which allows it to be used on a variety of platforms. It is the required algorithm for sensitive but unclassified U.S. government data.

RC4

A total of six RC algorithms have been developed by Ron Rivest. RC1 was never published, RC2 was a 64-bit block cipher, and RC3 was broken before release. RC4, also called ARC4, is one of the most popular stream ciphers. It is used in SSL and WEP. RC4 uses a variable key size of 40 to 2,048 bits and up to 256 rounds of transformation.

Asymmetric

Asymmetric algorithms use both a public key and a private or secret key. The public key is known by all parties, and the private key is known only by its owner. One of these keys encrypts the message, and the other decrypts the message.

In asymmetric cryptography, determining a user's private key is virtually impossible even if the public key is known, although both keys are mathematically related. However, if a user's private key is discovered, the system can be compromised.

Asymmetric algorithms can be referred to as dual-key or public-key cryptography.

Asymmetric systems provide confidentiality, integrity, authentication, and nonrepudiation. Because both users have one unique key that is part of the process, determining where the message originated is possible.

If confidentiality is the primary concern for an organization, a message should be encrypted with the receiver's public key, which is referred to as a secure message format. If authentication is the primary concern for an organization, a message should be encrypted with the sender's private key, which is referred to as an open message format. When using open message format, the message can be decrypted by anyone with the public key.

Perhaps the most widely known and used asymmetric algorithm is RSA. Oher asymmetric algorithms include RSA, El Gamal, DSA, and Elliptic Curve Cryptography (ECC).

RSA

RSA is the most popular asymmetric algorithm and was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA can provide key exchange, encryption, and digital signatures. The strength of the RSA algorithm is the difficulty of finding the prime factors of very large numbers. RSA uses a 1,024- to 4,096-bit key and performs one round of transformation.

As a key exchange protocol, RSA encrypts a DES or AES symmetric key for secure distribution. RSA uses a one-way function to provide encryption/decryption and digital signature verification/generation. The public key works with the one-way function to perform encryption and digital signature verification. The private key works with the one-way function to perform decryption and signature generation. These processes will be covered in detail in the section "Public Key Infrastructure (PKI)."

Hashing Algorithms

A *hash function* runs data through a cryptographic algorithm to produce a one-way message digest. The size of the message digest is determined by the algorithm used. The message digest represents the data but cannot be reversed in order to determine the original data. Because the message digest is unique, it can be used to check data integrity.

A one-way hash function reduces a message to a hash value. A comparison of the sender's hash value to the receiver's hash value determines message integrity. If the resultant hash values are different, then the message has been altered in some way, provided that both the sender and the receiver used the same hash function. Hash functions do not prevent data alteration but provide a means to determine whether data alteration has occurred.

Hash functions do have limitations. If an attacker intercepts a message that contains a hash value, the attacker can alter the original message to create a second invalid message with a new hash value. If the attacker then sends the second invalid message to the intended recipient, the intended recipient will have no way of knowing that he received an incorrect message. When the receiver performs a hash value calculation, the invalid message will look valid because the invalid message was appended with the attacker's new hash value, not the original message's hash value. To prevent this from occurring, the sender should use Message Authentication Code (MAC).

Encrypting the hash function with a symmetric key algorithm generates a keyed MAC. The symmetric key does not encrypt the original message. It is used only to protect the hash value. Figure 3.5 shows the basic steps of a hash function.

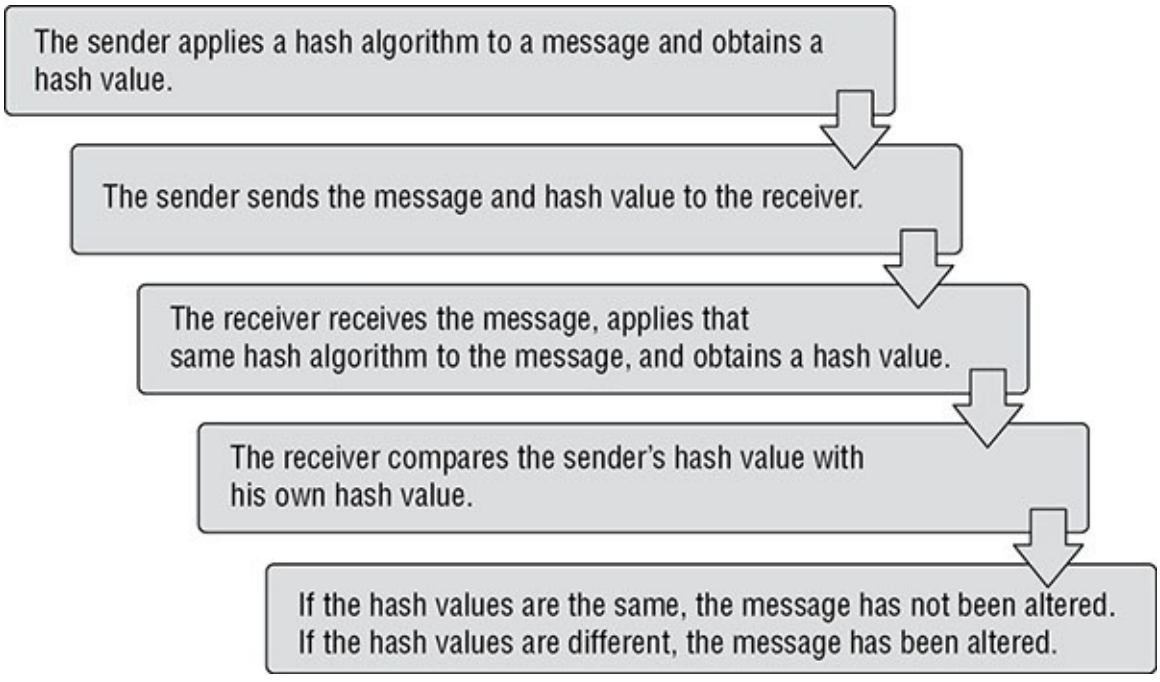

FIGURE 3.5 Hash process

Two major hash function vulnerabilities can occur: collisions and rainbow table attacks. A collision occurs when a hash function produces the same hash value on different messages. A rainbow table attack occurs when rainbow tables are used to reverse a hash by computing all possible hashes and looking up the matching value.

Because a message digest is determined by the original data, message digests can be used to compare different files to see whether they are identical down to the bit level. If a computed message digest does not match the original message digest value, then data integrity has been compromised.

Password hash values are often stored instead of the actual passwords to ensure that the actual passwords are not compromised.

When choosing which hashing function to use, it is always better to choose the function that uses a larger hash value. To determine the hash value for a file, you should use the hash function. As an example, let's suppose you have a document named `crypto.doc` that you need to ensure is not modified in any way. To determine the hash value for the file using the `md5` hash function, you would enter the following command:

```
md5 crypto.doc
```

This command would result in a hash value that you should record. Later, when users need access to the file, they should always issue the `md5` command listed to recalculate the hash value. If the value is the same as the originally recorded value, the file is unchanged. If it is different, then the file has been changed.

MD5

The *MD5 algorithm* produces a 128-bit hash value. It performs four rounds of computations. It was originally created because of the issues with MD4, and it is more complex than MD4. However, MD5 is not collision free. For this reason, it should not be used for SSL certificates or digital signatures. The U.S. government requires the usage of SHA-2 instead of MD5. However, in commercial usage, many software vendors publish the MD5 hash value when releasing software patches so customers can verify the software's integrity after download.

SHA-1

SHA-1 produces a 160-bit hash value after performing 80 rounds of computations on 512-bit blocks. SHA-1 corrected the flaw in SHA-0 that made it susceptible to attacks.

SHA-2

SHA-2 is actually a family of hash functions, each of which provides different functional limits. The SHA-2 family is as follows:

- *SHA-224*: Produces a 224-bit hash value after performing 64 rounds of computations on 512-bit blocks.
- *SHA-256*: Produces a 256-bit hash value after performing 64 rounds of computations on 512-bit blocks.
- *SHA-384*: Produces a 384-bit hash value after performing 80 rounds of computations on 1,024-bit blocks.

- *SHA-512*: Produces a 512-bit hash value after performing 80 rounds of computations on 1,024-bit blocks.
- *SHA-512/224*: Produces a 224-bit hash value after performing 80 rounds of computations on 1,024-bit blocks. The 512 designation here indicates the internal state size.
- *SHA-512/256*: Produces a 256-bit hash value after performing 80 rounds of computations on 1,024-bit blocks. Once again, the 512 designation indicates the internal state size.

HMAC

A *hash MAC (HMAC)* is a keyed-hash Message Authentication Code (MAC) that involves a hash function with symmetric key. HMAC provides data integrity and authentication. Any of the previously listed hash functions can be used with HMAC, with the HMAC name being appended with the hash function name, as in HMAC-SHA-1. The strength of HMAC is dependent upon the strength of the hash function, including the hash value size and the key size.

HMAC's hash value output size will be the same as the underlying hash function. HMAC can help to reduce the collision rate of the hash function. Figure 3.6 shows the basic steps of an HMAC process.

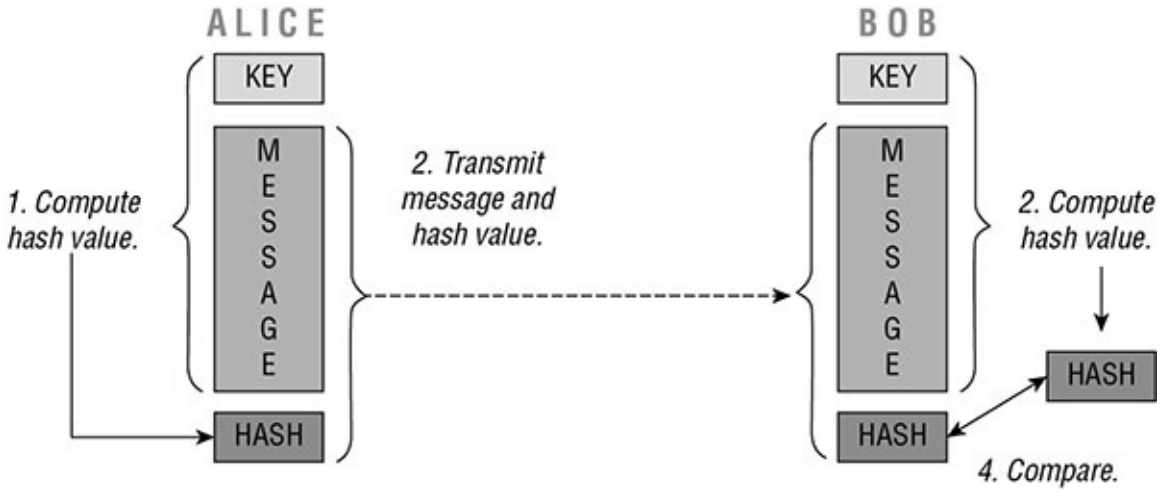

FIGURE 3.6 HMAC process

Digital Signatures

A *digital signature* is a hash value encrypted with the sender's private key. A digital signature provides authentication, nonrepudiation, and integrity. A blind signature is a form of digital signature where the contents of the message are masked before it is signed. Figure 3.7 shows the process.

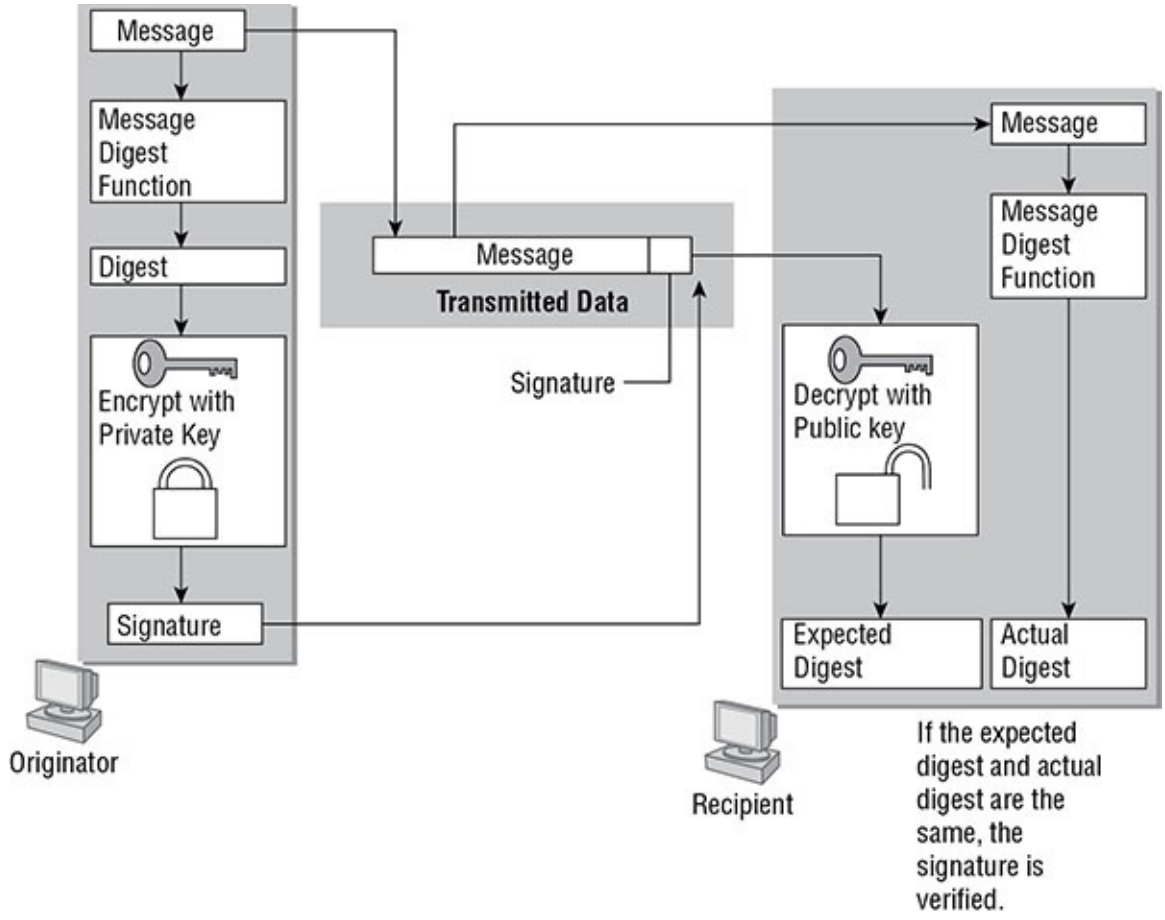

FIGURE 3.7 Digital signature process

The process for creating a digital signature is as follows:

1. The signer obtains a hash value for the data to be signed.
2. The signer encrypts the hash value using his private key.
3. The signer attaches the encrypted hash and a copy of his public key in a certificate to the data and sends the message to the receiver.

The process for verifying the digital signature is as follows:

1. The receiver separates the data, encrypted hash, and certificate.
2. The receiver obtains the hash value of the data.
3. The receiver verifies that the public key is still valid using the PKI.
4. The receiver decrypts the encrypted hash value using the public key.
5. The receiver compares the two hash values. If the values are the same, the message has not been changed.

Public key cryptography, which is discussed later in this chapter, is used to create digital signatures. Users register their public keys with a certification authority (CA), which distributes a certificate containing the user's public key and the CA's digital signature. The digital signature is computed by the user's public key and validity period being combined with

the certificate issuer and digital signature algorithm identifier.

The Digital Signature Standard (DSS) is a federal digital security standard that governs the Digital Security Algorithm (DSA). DSA generates a message digest of 160 bits. The U.S. federal government requires the use of DSA, RSA, or Elliptic Curve DSA (ECDSA) and SHA for digital signatures.

DSA is slower than RSA and provides only digital signatures. RSA provides digital signatures, encryption, and secure symmetric key distribution.

Key Exchange

As you have learned, symmetric key algorithms are significantly more efficient at encrypting and decrypting data than are asymmetric algorithms. However, the best way to illustrate the hybrid cryptosystem is to explore the function of SSH.

Application: SSH

Secure Shell (SSH) is an application and protocol that is used to remotely log in to another computer using a secure tunnel. After a session key is exchanged and a secure channel is established, all communication between the two computers is encrypted over the secure channel. SSH is a solution that could be used to remotely access devices, including switches, routers, and servers.

SSH offers a good illustration of the use of asymmetric algorithms to generate and exchange a symmetric key and thereafter to use that key for data encryption. The steps are as follows:

1. The client connects to the server, and the server presents its public key to the client.
2. The client and server negotiate a group of settings that must match on both ends. It includes the symmetric algorithm they will use.
3. The client creates a random session key and encrypts it with the server’s public key.
4. The client sends this encrypted session key to the server, and the server decrypts it using its private key.

Using the symmetric key, which they both now possess, the two start encrypting everything that goes on from this point, including the authentication process.

Public Key Infrastructure

A *public key infrastructure (PKI)* includes systems, software, and communication protocols that distribute, manage, and control public key cryptography. A PKI publishes digital certificates. Because a PKI establishes trust within an environment, a PKI can certify that a public key is tied to an entity and verify that a public key is valid. Public keys are published through digital certificates.

The X.509 standard is a framework that enables authentication between networks and over the Internet. A PKI includes timestamping and certificate revocation to ensure that certificates are managed properly. A PKI provides confidentiality, message integrity, authentication, and nonrepudiation.

The structure of a PKI includes CAs, certificates, registration authorities, certificate revocation lists, and cross-certification. This section discusses these PKI components as well as a few other PKI concepts.

Public and Private Keys

In public key cryptography, two keys are used, a *public key* and a *private key*. These two keys are not the same, but they are mathematically related in such a way that if you encrypt data with one of them, you can decrypt it with the other. Users and devices are issued public/private key pairs that are bound to a digital document called a *digital certificate*. This certificate (more specifically the keys to which it is bound) can be used for a variety of things including the following:

- Encrypting data
- As a form of authentication
- Encrypting email
- Digitally signing software

Private Key

The private key that is generated as part of the key pair is made available only to the user or device to which it was issued. This key may be stored on software in the user's computer, or it might be stored on a smart card if it is to be used for authentication. At any rate, the key concept here is that it is available *only* to the user or device to which it was issued.

Public Key

The public key that is generated as part of the key pair is made available to anyone to whom the certificate is presented because it is part of the information contained in this digital document. In some cases, public keys may be kept in a repository so they can be requested by an entity if required. Regardless of the method used to obtain the public key, the key concept here is that it is available to anyone.

Putting It Together

These keys work together to perform both encryption and digital signatures. To provide encryption, the data is encrypted with the receiver's public key, which results in ciphertext that only the receiver's private key can decrypt. Figure 3.8 shows this process.

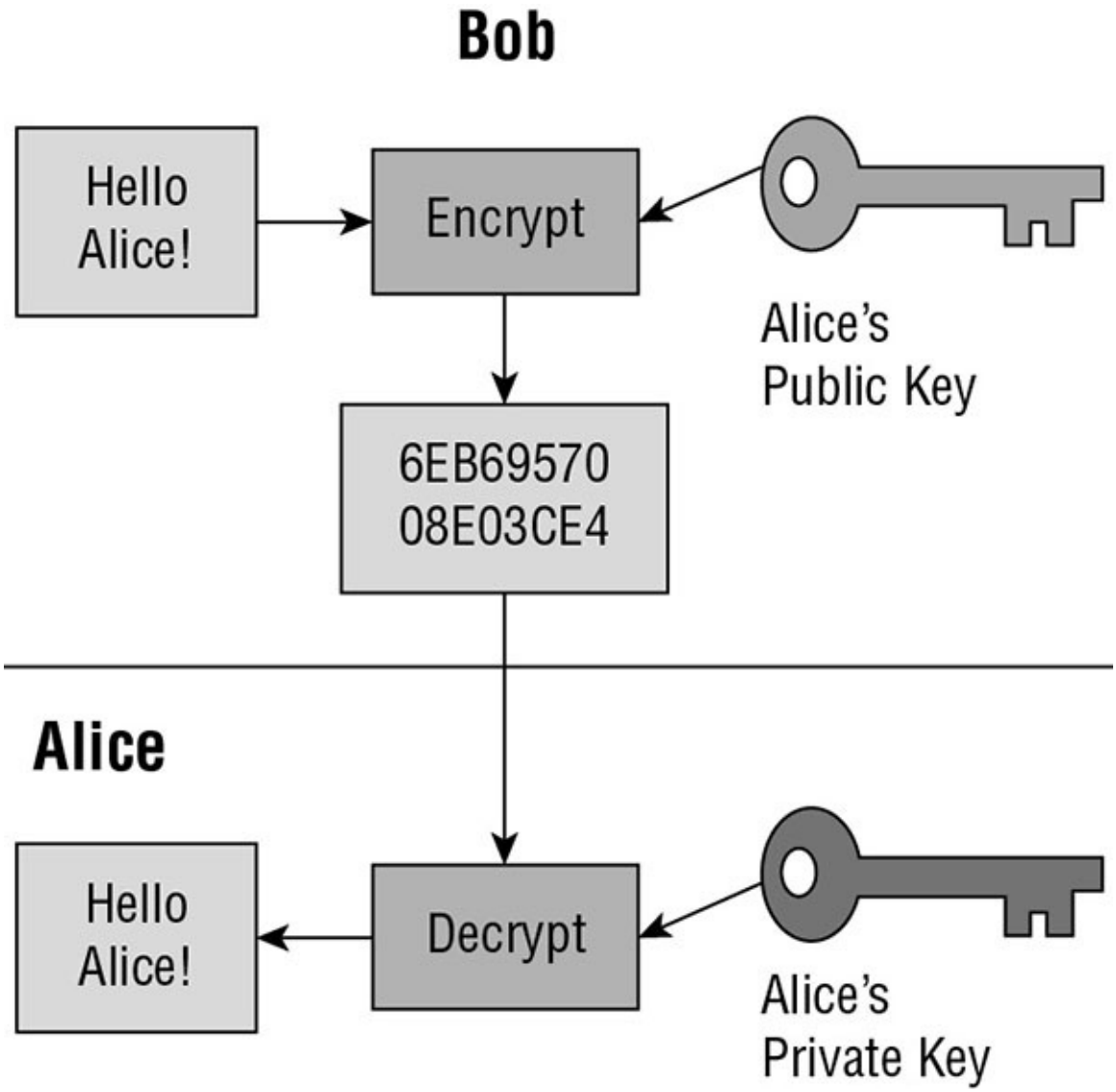

FIGURE 3.8 PKI encryption

To digitally sign a document, the sender creates what is called a *hash value* of the data being sent, encrypts that value with the sender's his private key, and sends this value along with the message. The receiver decrypts the hash using the sender's public key. The receiver then, using the same hashing algorithm, hashes the message. The sender then compares the decrypted hash value to the one just generated. If they are the same, the signature (and the integrity of the data) has been verified. Figure 3.9 shows this process.

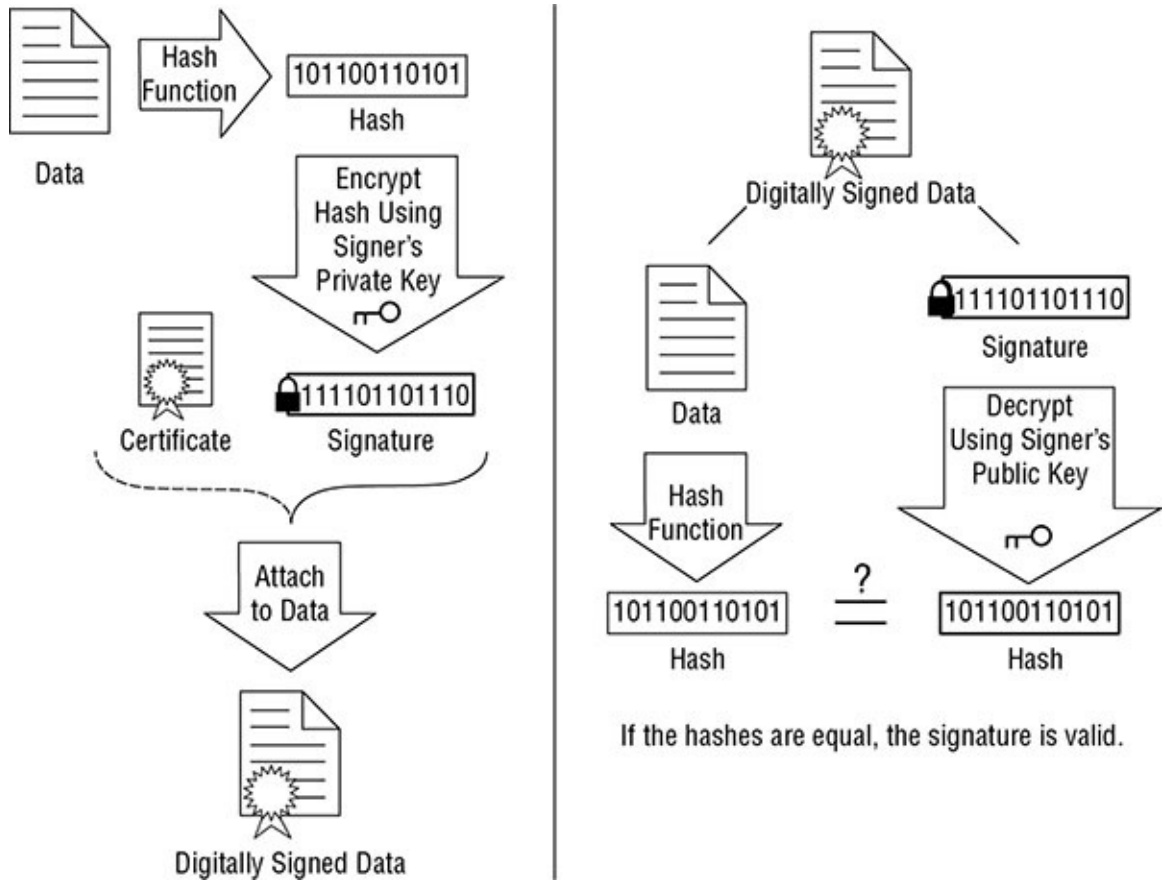

FIGURE 3.9 PKI digital signature

Certificates

A *digital certificate* provides an entity, usually a user, with the credentials to prove its identity and associates that identity with a public key. At minimum, a digital certification must provide the serial number, the issuer, the subject (owner), and the public key.

An X.509 certificate complies with the X.509 standard. An X.509 certificate contains the following fields:

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
- Subject
- Subject Public Key Info
  - Public Key Algorithm
  - Subject Public Key

- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Extensions (optional)

Revocation

Certificates have a defined lifetime. When the validity period ends, the certificate must be renewed to continue to be valid. There are cases when a certificate must be revoked before its lifetime ends. Reasons for certificate revocation include the following:

- Compromise of the associated keys
- Improper issuance
- Compromise of the issuing CA
- Owner of the certificate no longer owning the domain for which it was issued
- Owner of the certificate ceasing operations entirely
- Original certificate being replaced with a different certificate from a different issuer

A *certificate revocation list (CRL)* is a list of digital certificates that a CA has revoked. To find out whether a digital certificate has been revoked, either the browser must check the CRL or the CA must push out the CRL values to clients. This can become quite daunting when you consider that the CRL contains every certificate that has ever been revoked.

One concept to keep in mind is the revocation request grace period. This period is the maximum amount of time between when the revocation request is received by the CA and when the revocation actually occurs. A shorter revocation period provides better security but often results in a higher implementation cost.

Uses

Certificates can be used for variety of operations. This can include authentication, encryption, digital signatures, and email to name a few. VeriSign first introduced the following digital certificate classes:

- *Class 1*: For individuals intended for email. These certificates get saved by web browsers.
- *Class 2*: For organizations that must provide proof of identity.
- *Class 3*: For servers and software signing in which independent verification and identity and authority checking is done by the issuing CA.
- *Class 4*: For online business transactions between companies.
- *Class 5*: For private organizations or governmental security.

Application: SSL/TLS

Certificates are often used when using SSL/TLS. Most modern systems today use TLS, but the

term SSL is often still used to refer to the connection. SSL is used to protect many types of applications, the most common being HTTPS (as HTTP is called when used with SSL).

An SSL session is formed between a web server and the web browser of the client. Figure 3.10 depicts the process.

Certificate Authorities

A *certification authority (CA)* is the entity that creates and signs digital certificates, maintains the certificates, and revokes them when necessary. Every entity that wants to participate in the PKI must contact the CA and request a digital certificate. It is the ultimate authority for the authenticity for every participant in the PKI and signs each digital certificate. The certificate binds the identity of the participant to the public key.

Any participant that requests a certificate must first go through the *registration authority (RA)*, which verifies the requestor's identity and registers the requestor. After the identity is verified, the RA passes the request to the CA. In many cases, the CA and the RA are the same server.

There are different types of CAs. Organizations exist that provide a PKI as a payable service to companies that need them. An example is VeriSign. Some organizations implement their own private CAs so that the organization can control all aspects of the PKI process. If an organization is large enough, it might need to provide a structure of CAs, with the root CA being the highest in the hierarchy.

Because more than one entity is often involved in the PKI certification process, certification path validation allows the participants to check the legitimacy of the certificates in the certification path.

When implementing a PKI, most organizations rely on a hierarchical chain-of-trust model that uses three components at minimum: certificate authorities (CAs), registration authorities (RAs), and a central directory/distribution management mechanism.

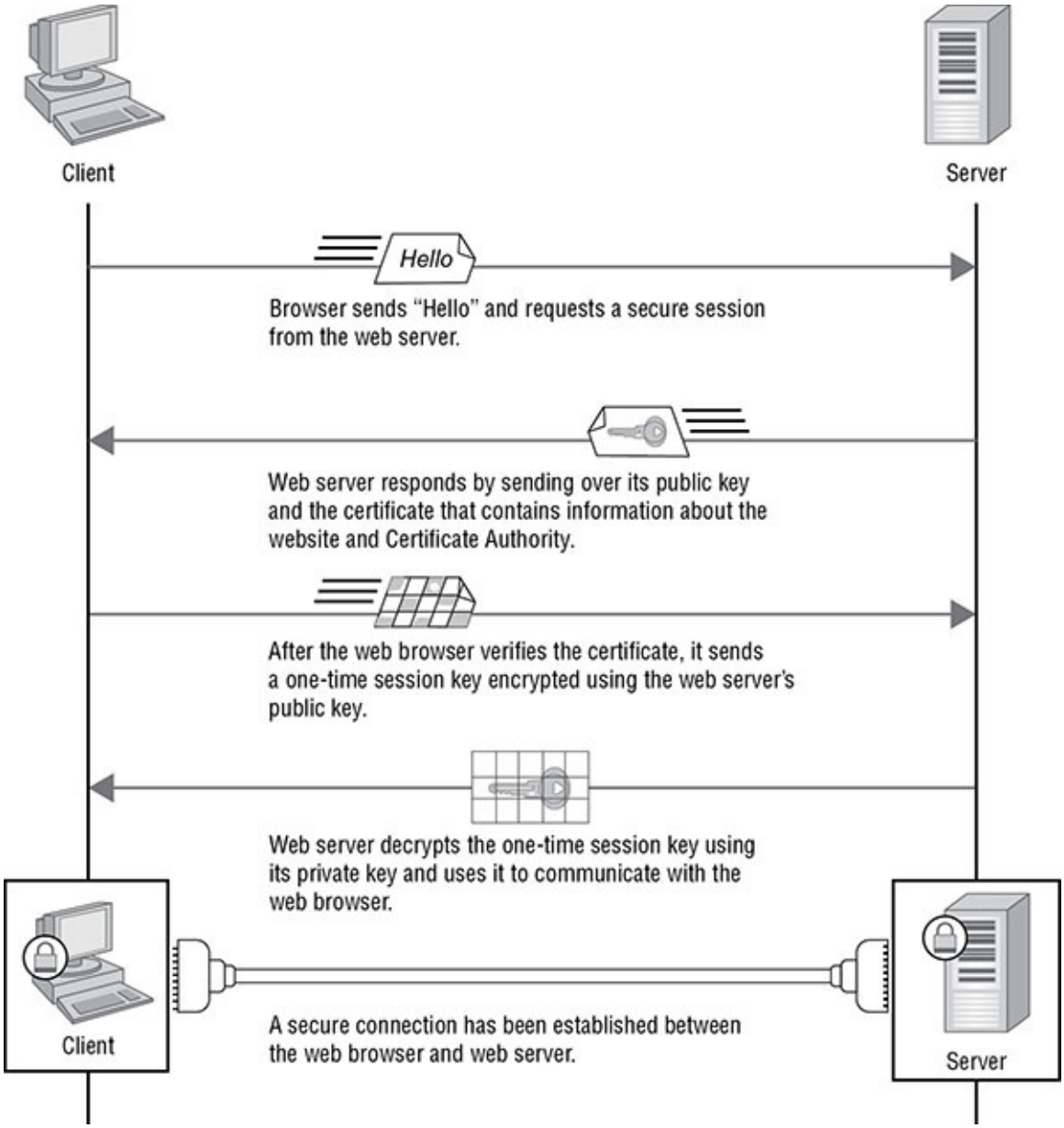

FIGURE 3.10 SSL process

A CA issues certificates that bind a public key to a specific distinguished name (DN) issued to the certificate applicant (user). Before issuing a certificate, however, the CA validates the applicant's identity.

When a subject's public certificate is received, the system must verify its authenticity. Because the certificate includes the issuer's information, the verification process checks to see whether it already has the issuer's public certificate. If not, it must retrieve it.

A root CA is at the top of the certificate signing hierarchy. VeriSign, Comodo, and Entrust are examples of public root CAs. For organizations that maintain their own PKI, the first CA created will be the root CA.

Using the root certificate, the system verifies the issuer signature and ensures that the subject certificate is not expired or revoked. If verification is successful, the system accepts the subject certificate as valid.

Root CAs can delegate signing authority to other entities. These entities are known as *intermediate CAs*. Intermediate CAs are trusted only if the signature on their public key certificate is from a root CA or can be traced directly back to a root. Because a root CA can delegate to intermediate CAs, a lengthy chain of trust can exist.

Any system receiving a subject certificate can verify its authenticity by stepping up the chain of trust to the root.

PKI Standards

Public Key Cryptography Standards (PKCS) were created by RSA Security. While they were created to help promote techniques for which RSA had patents, many of these standards have become standards by the IETF. Table 3.2 shows the standards that have not since been abandoned or obsoleted.

TABLE 3.2 PKI standards

Standard	Version	Name	Description
PKCS #1	2.2	RSA Cryptography Standard	Defines the mathematical properties and format of RSA public and private keys and the basic algorithms and encoding/padding schemes for performing RSA encryption and decryption and for producing and verifying signatures.
PKCS #3	1.4	Diffie-Hellman Key Agreement Standard	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #5	2.0	Password-Based Encryption Standard	Provides recommendations for the implementation of password-based cryptography, covering key derivation functions, encryption schemes, message-authentication schemes, and ASN.1 syntax identifying the techniques.
PKCS #7	1.5	Cryptographic Message Syntax Standard	Used to sign and/or encrypt messages under a PKI. Formed the basis for S/MIME. Often used for single sign-on.
PKCS #8	1.2	Private-Key Information Syntax Standard	Used to carry private certificate key pairs (encrypted or unencrypted).
PKCS #9	2.0	Selected Attribute Types	Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.

PKVS #10	1.7	Certification Request Standard	Format of messages sent to a certification authority to request certification of a public key.
PKCS #11	2.4	Cryptographic Token Interface	Also known as Cryptoki. An API defining a generic interface to cryptographic tokens (see also hardware security module). Often used in single sign-on, public-key cryptography and disk encryption.
PKCS #12	1.1	Personal Information Exchange Syntax Standard	Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.
PKCS #15	1.1	Cryptographic Token Information Format Standard	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API.

PKI Topologies

A PKI can consist of a single server that operates as RA and CA and is the root certificate server. But in very large environments, you may be advised to create a hierarchy of CAs. When this is done, a single CA will be the root CA and the top of the hierarchy. Underneath this would be a number of subordinate CAs that actually issue the certificates to the entities. The root CA creates and signs the certificates of the subordinate CAs, which creates a trust path up to the root. Figure 3.11 shows this arrangement.

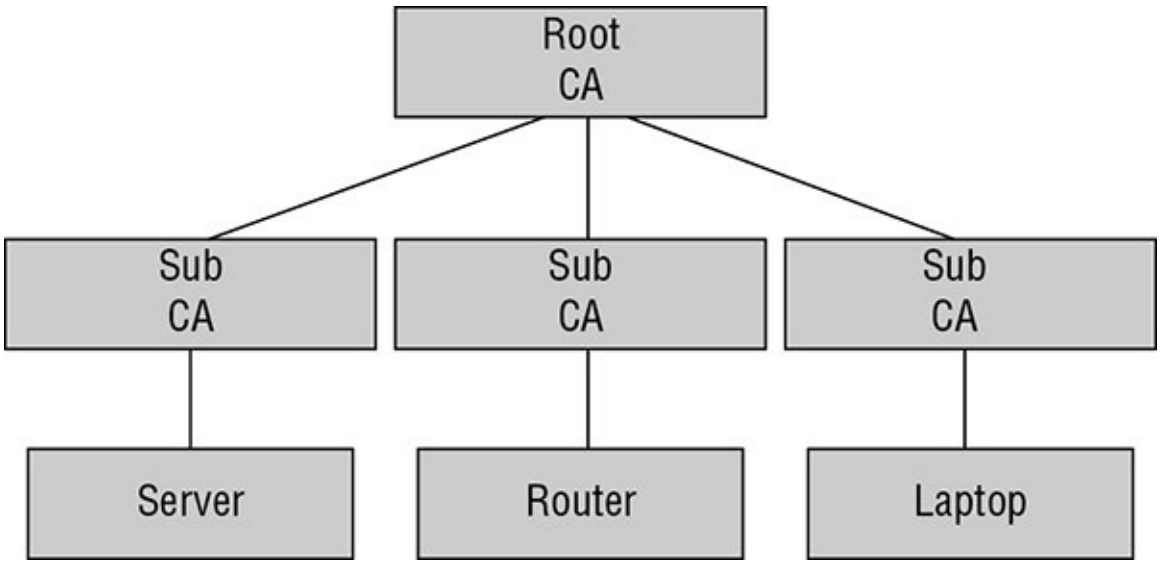

FIGURE 3.11 PKI hierarchy

In some cases, two organizations may have a need to trust one another's certificates. This can

be done by configuring cross certification. In cross certification, a trust is created between the two root CAs, which enable both systems to trust all certificates, as shown in Figure 3.12 .

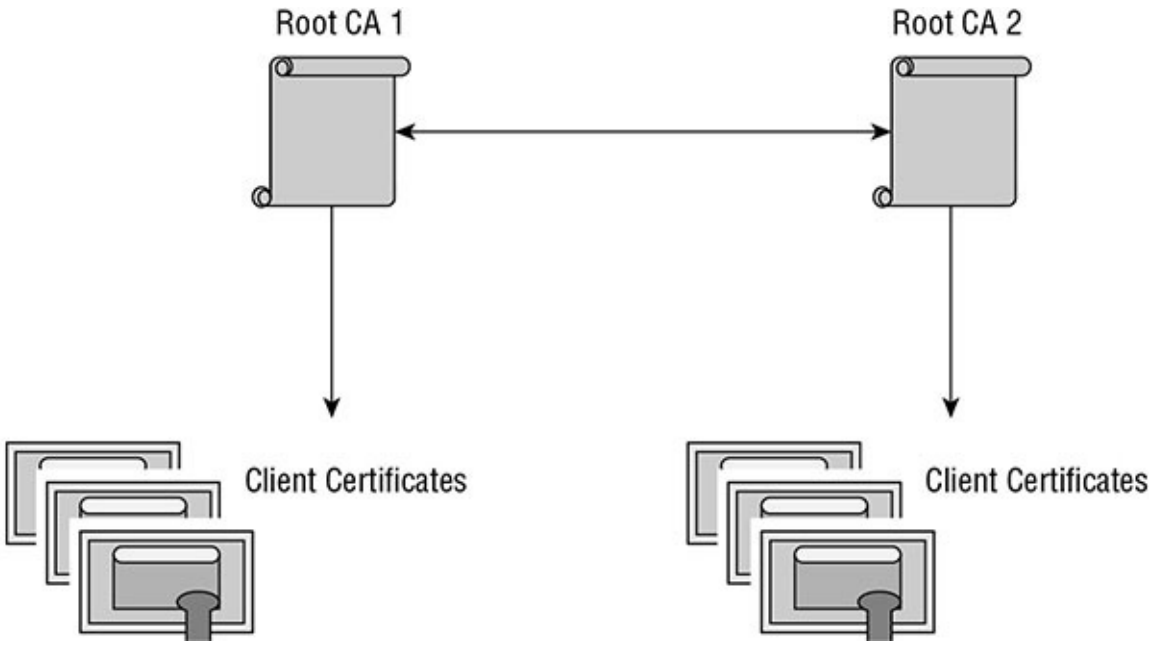

FIGURE 3.12 Cross certification

Certificates in the ASA

The *Cisco Adaptive Security Appliance (ASA)* makes use of certificates and the associated keys to protect the connection of the administrator to the ASA using the Adaptive Security Device Manager (ADSM) and to support SSL VPN clients. In this section, you'll learn about the default certificate that is present in the ASA, the process of adding a certificate and viewing the certificates that are present, and the use of the Simple Certificate Enrollment Protocol (SCEP).

Default Certificate

The ASA has a self-signed default certificate that can be used for the operations listed in the previous section. The issue with a self-signed certificate is that no browsers or devices will have the ASA listed as a trusted CA. Because of this, any HTTPS connections to the ASA will generate a warning message that the certificate being presented is not trusted. To avoid this issue, you can install a root certificate of the CA whose certificate is found in the browsers and devices that will interact with the ASA (either that you own or a public CA).

Viewing and Adding Certificates in the ASDM

To view the current certificates in the ADSM, select Configuration at the top of the ADSM console and Device Management from the tabs on the left side of the console, as shown in Figure 3.13 . As you can see, this ASA currently has no certificates installed other than the default.

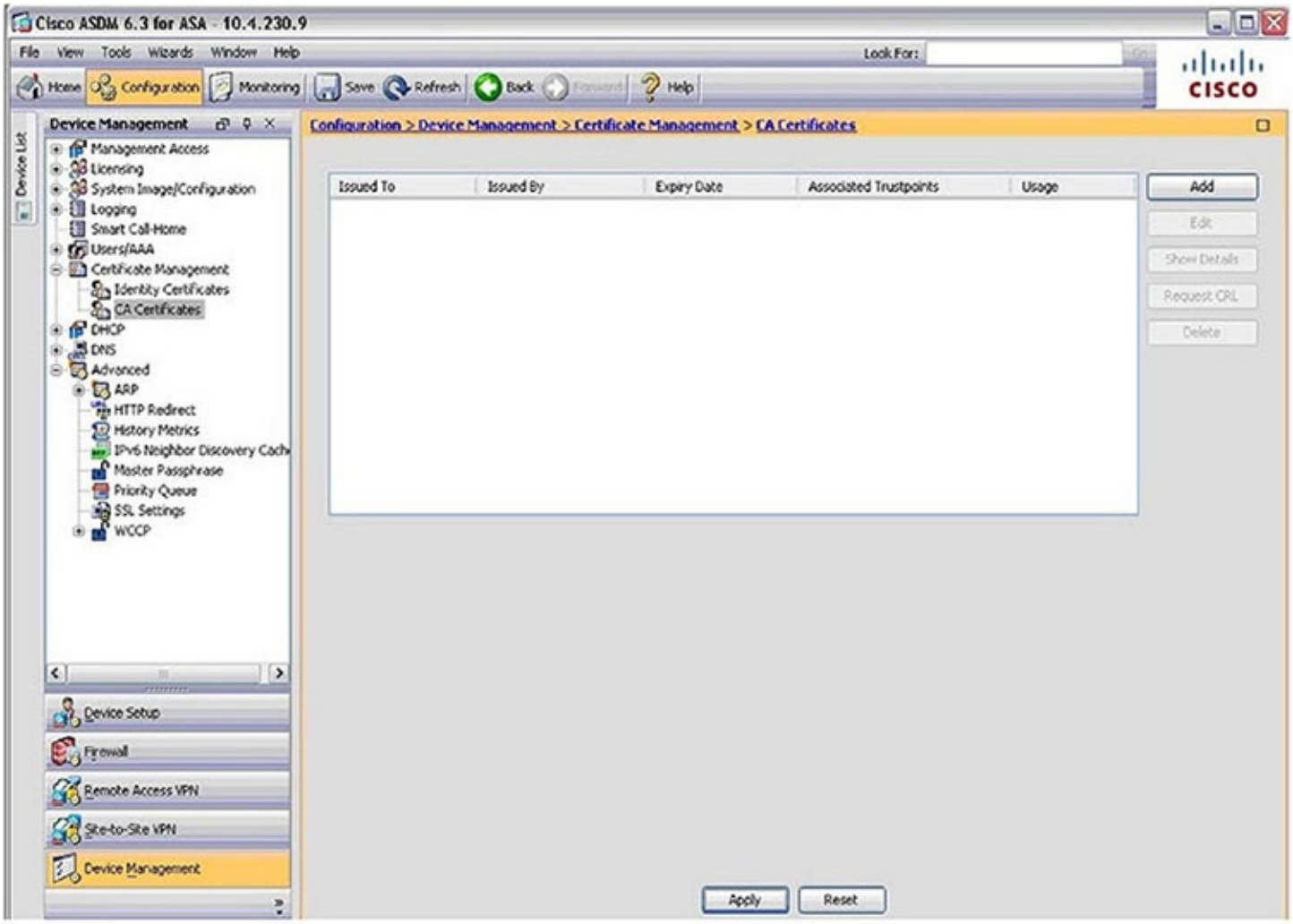

FIGURE 3.13 Viewing certificates

To add a certificate, follow these steps:

1. In the Cisco ASDM Configuration Tool, select Configuration ➢ Device Management ➢ Certificate Management ➢ CA Certificates.
2. Click Add. The Install Certificate dialog box appears. You have three options: install from a file, paste the information, or use SCEP. If the root CA represented by the root certificate supports SCEP, choose that option. Otherwise, use the next two steps.
3. Enter a trustpoint name or use the default name that appears in the box.
4. Click the Install From A File radio button and browse to the location of the `Root.crt` file that you are installing.
5. Click the More Options button, and here you can configure how certificate revocation will be checked, the protocols to be used for certificate verification, and other settings.

SCEP

Simple Certificate Enrollment Protocol is a protocol used for enrollment and other PKI operations. It is supported on most Cisco devices. It simplifies the process of obtaining and

installing both the root and the identity certificates. The process to use SCEP is as follows:

1. Choose Configuration ➢ Device Management ➢ Certificate Management ➢ Identity Certificates and click Add.
2. Click the Add A New Identity Certificate radio button and click the Advanced button.
3. In the Advanced box, on the Enrollment Mode tab, select Request From A CA and then enter the IP address of the CA that supports SCEP. Click OK.
4. In the Add A New Identity Certificate dialog box, select Add Certificate. If the enrollment is successful, you will receive an Enrollment Succeeded message.

Cryptanalysis

In *cryptanalysis*, cryptography attacks are categorized as either passive or active attacks. A passive attack is usually implemented just to discover information and is much harder to detect because it is usually carried out by eavesdropping or packet sniffing. Active attacks involve an attacker actually carrying out steps, such as message alteration or file modification. Cryptography is usually attacked via the key, algorithm, execution, data, or people. But most of these attacks are attempting to discover the key used.

Ciphertext-Only Attack

In a *ciphertext-only attack*, an attacker uses several encrypted messages (ciphertext) to figure out the key used in the encryption process. Although it is a common type of attack, it is usually not successful because so little is known about the encryption used.

Known Plaintext Attack

In a *known plaintext attack*, an attacker uses the plaintext and ciphertext versions of a message to discover the key used. This type of attack implements reverse engineering, frequency analysis, or brute force to determine the key so that all messages can be deciphered.

Chosen Plaintext Attack

In a *chosen plaintext attack*, an attacker chooses the plaintext to get encrypted to obtain the ciphertext. The attacker sends a message hoping that the user will forward that message as ciphertext to another user. The attacker captures the ciphertext version of the message and tries to determine the key by comparing the plaintext version he originated with the captured ciphertext version. Once again, key discovery is the goal of this attack.

Chosen Ciphertext Attack

A *chosen ciphertext attack* is the opposite of a chosen plaintext attack. In a chosen ciphertext attack, an attacker chooses the ciphertext to be decrypted to obtain the plaintext. This attack is more difficult because control of the system that implements the algorithm is needed.

Brute Force

As with a *brute-force attack* against passwords, a brute-force attack executed against a cryptographic algorithm uses all possible keys until a key is discovered that successfully decrypts the ciphertext. This attack requires considerable time and processing power and is difficult to complete.

Birthday Attack

A *birthday attack* uses the premise that finding two messages that result in the same hash value is easier than matching a message and its hash value. Most hash algorithms can resist simple birthday attacks.

Meet-in-the-Middle Attack

In a *meet-in-the middle attack*, an attacker tries to break the algorithm by encrypting from one end and decrypting from the other to determine the mathematical problem used.

Summary

In this chapter, you learned about symmetric and asymmetric key cryptography and how they differ. The chapter gave examples of each type of algorithm, and you learned how they can work together in a hybrid system. You also learned about the hashing process and looked at the major hashing algorithms. There was coverage of PKI and the components that make it function. Finally, you learned about common attacks on cryptography.

Exam Essentials

Differentiate between symmetric and asymmetric key cryptography. This includes the types of keys used, the scenarios in which they are used, and the disadvantages and advantages of each.

Describe the hashing process. This includes how hashing algorithms work, examples of hashing algorithms, and the role of hashing in digital signatures.

Explain the role of a PKI. Describe the components of a PKI, the certificate enrollment process, and the use of public and private keys in the process.

Define cryptanalytic attacks. These include ciphertext-only attack, chosen plaintext, chosen ciphertext, brute force, birthday, and meet-in-the-middle.

Review Questions

1. Which of the following is *not* true of symmetric algorithms?
   A. They use a public key.
   B. They are faster than asymmetric algorithms.

C. They present key exchange issues.

D. They are typically used for data at rest.

2. Which of the following is *not* true of asymmetric algorithms?

   A. They provide automatic key exchange.

   B. They are typically used for data at rest.

   C. They use a private and public key.

   D. They are slower than symmetric algorithms.

3. Which of the following is *not* an advantage of block ciphers?

   A. The implementation is easier than stream-based cipher implementation.

   B. Generally they are less susceptible to security issues.

   C. Generally they are used more in software implementations.

   D. They employ only substitution.

4. Which of the following ciphers perform encryption on a bit-by-bit basis?

   A. Block

   B. Stream

   C. Asymmetric

   D. Polyalphabetic

5. Which of the following is used to ensure that patterns are not produced during encryption?

   A. IVs

   B. HMAC

   C. RC4

   D. Salting

6. In which of the following modes of DES is every 64-bit block encrypted with the same key?

   A. CBC

   B. ECB

   C. ECC

   D. CFB

7. Which of the following is the replacement algorithm for 3DES?

   A. Blowfish

B. AES

C. IDEA

D. RC4

8. Which of the following is the most popular asymmetric algorithm?

A. RSA

B. El Gamal

C. DSA

D. ECC

9. Which of the following occurs when a hash function produces the same hash value on different messages?

A. Birthday attack

B. Key exposure

C. Collision

D. Substitution

10. Which of the following hashing algorithms is required by the U.S. government?

A. MD4

B. MD5

C. SHA1

D. SHA2

11. Which of the following can help to reduce the collision rate of the hash function?

A. MAC

B. HMAC

C. Digital signatures

D. Substitution

12. Which of the following is a hash value encrypted with the sender's private key?

A. Salt

B. Nonce

C. Digital signature

D. HMAC

13. Which of the following is true of a hybrid cryptosystem?

A. Asymmetric algorithms are used for the key exchange.
B. Symmetric keys are used for the key exchange.
C. Asymmetric keys are used for the data encryption.
D. Asymmetric keys are exchange automatically.

14. Which of the following is a digital document binding a key pair to an entity?
A. Certificate
B. Nonce
C. Salt
D. IV

15. Which of the following is the standard for digital certificates?
A. X.500
B. X.509
C. IEEE 509
D. RFC 500

16. Which of the following is a list of digital certificates that a CA has revoked?
A. OSCP
B. CRL
C. SCEP
D. REVC

17. Which of the following certificate classes is for individuals intended for email?
A. 1
B. 2
C. 3
D. 4

18. Which of the following PKI components verifies the requestor's identity?
A. CA
B. RA
C. DN
D. CN

19. Which of the following can be used to allow one root CA to trust another root CA's

certificates?

A. Subordination
B. Cross certification
C. Certlink
D. Trust

20. What type of certificate does the ASA use out of the box?

A. Public
B. Self-signed
C. Globally trusted
D. Locally trusted

Chapter 4
Securing the Routing Process

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.1 Security on Cisco routers**
  - Configure multiple privilege levels
  - Configure Cisco IOS role-based CLI access
  - Implement Cisco IOS resilient configuration
- ✓ **4.2 Securing routing protocols**
  - Implement routing update authentication on OSPF
- ✓ **4.3 Securing the control plane**
  - Explain the function of control plane policing

To provide secure routing and switching, the routers and switches themselves must be secured. Leaving them in a vulnerable state can render all other security implementations useless because unauthorized access can allow a malicious individual to alter all the security settings that are in place. Additionally, when routers are exchanging routing updates, any unauthenticated updates can reveal important information about your network to anyone who convinces your router to perform a routing update. In this chapter, you will explore functionality you should take advantage of to secure access to the devices, to secure routing updates, and to secure the control plane.

In this chapter, you will learn the following:

Securing Cisco routers

Securing routing protocols

Securing Router Access

Securing administrative access to the router is the first step in securing the routing process. This prevents unauthorized access to the router, which will ensure that the configuration of the router cannot be altered. In this section, you'll learn about configuring secure administrative

access using several tools.

First I'll discuss how to configure an encrypted session with the router using SSH rather than Telnet (which transmits in clear text). Next I'll talk about controlling the operations of each individual technician by assigning privilege levels. As privilege levels do not meet the needs of all environments, you'll also look at a way to get more granular with the assignment of tasks by authorizing functions via a command-line interface (CLI) with role-based CLI. Finally, I'll discuss how to protect the configuration of the router using the Cisco IOS resilient configuration feature.

Configuring SSH Access

While Telnet can certainly be used to manage a router, this remote access technology transmits everything in clear text, making it unsuitable in today's environments. For this reason, you should always use *Secure Shell (SSH)* for secure remote access. The SSH server on the router will require an RSA public/private key pair to use in the process of encrypting the traffic. It can generate this key pair but must have certain information configured before it can do so because it uses this information as the label for the key pair.

Therefore, the high-level steps to set up SSH are as follows:

1. Set the router name.
2. Set the router domain name.
3. Generate the RSA key.

Here are the actual commands:

```
Router(config)#hostname R63
R63(config)#ip domain-name mcmillan.com
R63(config)#crypto key generate rsa ?
  encryption    Generate a general purpose RSA key pair for signing and
                encryption
  exportable    Allow the key to be exported
  general-keys  Generate a general purpose RSA key pair for signing and
                encryption
  label         Provide a label
  modulus       Provide number of modulus bits on the command line
  on            create key on specified device.
  redundancy    Allow the key to be synced to high-availability peer
  signature     Generate a general purpose RSA key pair for signing and
                encryption
  storage       Store key on specified device
  usage-keys    Generate separate RSA key pairs for signing and encryption


R63(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R63.mcmillan.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 2 seconds)

R63(config)#
*Mar 28 18:32:09.095: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

In these steps, you can see I created a name, `R63`; set the domain name to `mcmillan.com`; and generated a key. The `modulus` keyword I used sets the length of the key, which in this case is 1,024 bits. Notice the syslog message that indicates SSH version 1.99 has been enabled. This indicates it is a version 2 server, which can accept connections from SSH version 1 devices.

Next you need to do the following:

1. Create a username and password for each user who needs SSH access.
2. Configure `line vty` to only accept SSH connections.

```
R63(config)#username troy secret mac
R63(config)#line vty ?
  <0-1114>  First Line number

R63(config)#line vty 0 1114
R63(config-line)#login local
R63(config-line)#transport input ssh
R63(config-line)#
```

Notice that I created a user named `troy` with a password of `mac`. You can create a single account to be shared by all authorized technicians and name it something like `admin`, or you can create separate accounts for each user. Separate accounts will provide accountability.

Also notice that when I entered `line vty` mode, I checked to see how many vty lines this device has so that when I run the command to enter that mode, the commands I apply will apply to *all* lines. The command `login local` tells the router that all user accounts will be found locally on this router and *not* on a remote server. That's why I needed to create the local account that I did. Finally, I set the router to only accept SSH connections with the last command.

Configuring Privilege Levels in IOS

Privilege levels allow you to assign a technician sets of activities that coincide with the level the technician has been assigned. There are 16 levels, from 0 to 15. When you are in user mode (`router>`), you are at Privilege level 1. When you are in privileged mode (`router#`), you are at level 15.

You can assign levels between 0 and 15, and by linking these levels with commands, you can control the activities of each technician. This can be done on both IOS devices and on the Cisco Adaptive Security Appliance (ASA), although the details of each process are slightly different. Privilege levels are created at the global configuration prompt `router(config)#`. When a level is created, you also add a command at the same time, which means if you are adding multiple commands to the level, you will run the privilege command several times. Once a level is created, access to that level is obtained by entering a password assigned to that

level. From a high level, here are the steps required:

1. Create the level and assign a command to that level.
2. Assign any additional commands to the level.
3. Set a password for the level.
4. Provide the level number and password to the technician (or technicians) who will use it.

First I will create a level numbered 12, and I will assign the `show interfaces` command to it. Notice that when I do this, I have to assign the command to the level where it is usually executed, in this case `privilege exec level`.

```
router(config)#privilege exec level 12 show interfaces
```

To demonstrate how to assign a command that is executed at a different level, I am now going to add the `interface` configuration command, and since that command is executed normally at the global configuration mode, I will use the `configure` keyword when I add it.

```
router(config)#privilege configure level 12 interface
```

My intent is to allow this technician to change IP addresses on interfaces, so I need to assign him that command. Since the `ip` command (along with the parameter `address`) is executed after entering interface configuration mode, I have to reference interface in the command, as shown here:

```
router(config)#privilege interface level 12 ip
```

Now I'm ready to assign a password for level 12 that I just created. That is done the same way any `enable secret` password is created, adding the level to which it applies as shown next (otherwise it will apply to level 15 as it usually does). The password I set is `wordpass`.

```
router(config)#enable secret level 12 wordpass
```

Once I provide the level number and password to the technician, he will use the password to enter the privilege level as shown here, making it possible to use those commands and no others. To verify the application of the level, he can type `show privilege` as is also shown.

```
router#enable 12
password:wordpass
router#show privilege
Current privilege level is 12
```

If he attempts to use any other commands, he will receive the error message shown here:

```
router#show run
          ^
%invalid input detected at '^' marker.
```

Configuring IOS Role-Based CLI

Another option you can use to control the operations of technicians is a *role-based CLI*. Using this approach, you can create roles, implemented as sets of operations called *parser views*. The only view that exists by default is called *root*, which as you would expect allows access to all commands. Access to this view is provided when you submit the `enable secret` password.

Once a parser view is created, you can permit access to the view with a password. This makes it simple to onboard a new technician by assigning him the role he will play in the network. Every technician granted the role will have the same set of operations available.

From a high level, here are the steps required:

1. Create and name the parser view.
2. Assign a password to the parser view.
3. Assign commands to the parser view.
4. Provide the parser view name and password to technicians in the role.

   First I will create a view called OSPFAdmin.

```
R63(config)#parser view OSPFAdmin
R63(config-view)#
```

Notice the prompt has changed, and now any commands I run will affect only this view. At this prompt I can both set a password and assign commands to the view. First I'll assign a password.

```
R63(config-view)#secret OSPFp@$$
R63(config-view)#
```

Now I will assign commands. I won't assign all commands required to manage OSPF, just enough to show you how it's done. You must ensure that you have provided all commands required for the role.

```
R63(config-view)#commands exec include all show
R63(config-view)#commands exec include all debug ip ospf
R63(config-view)#commands exec include all no debug
R63(config-view)#commands exec include all undebug
R63(config-view)#commands configure include router ospf
```

I have allowed access in exec mode to all show commands and to the `debug ip ospf` commands required. Then I allowed access to the `router ospf` command, which will include all command within that context. After a technician has been assigned this role, he will access the role using the following commands. Notice that you can verify the application of the role by using the `show parser view` command.

```
R63#enable view OSPFAdmin
Password: OSPFp@$$
R63#show parser view
R63#current view is 'OSPFAdmin'
```

Implementing Cisco IOS Resilient Configuration

While securing access to the router should be enough to effectively protect the configuration of the router, there is an additional way to prevent unwanted changes to the configuration. The IOS *resilient configuration* feature can provide a way to easily recover from an attack on the configuration, and it can also help to recover from an even worse attack in which the attacker deletes not only the startup configuration but also the boot image.

The configuration of this feature can be done with two commands. One enables protection of the boot image, and the other enables protection of the startup configuration. To enable protection of the boot image, issue the following command:

```
R64(config)#secure boot-image
*April 2 14:24:50.231: %IOS_Resilience-5-IMAGE_RESIL_ACTIVE: Successfully
secured running  image
```

Notice the system message indicating the boot image is protected. To enable protection of the startup configuration, issue the following command:

```
R64(config)#secure boot-config
*April 2 14:24:50.231: %IOS_Resilience-5-CONFIG_RESIL_ACTIVE: Successfully
secured config archive [flash: .runcfg-20140131-14259.ar]
```

Once these two items are secured (called the *secure bootset*), you cannot update the startup configuration without removing the secure configuration long enough to make the change and then resecuring it as was done in the first place. To remove the secure startup configuration, execute the following command:

```
R64(config)#no secure boot-config
*April 2 14:34:50.231: %IOS_Resilience-5-CONFIG_RESIL_INACTIVE: Disabled
secure config archive [removed flash: .runcfg-20140131-14259.ar]
```

When finished making changes, execute the `secure boot-config` command to secure the configuration again.

But what do you do if the worst happens and the startup configuration is deleted? It can be restored, but you must know the location of the secure boot configuration, and you must reference it in the command. To identify its name and location, execute the following command:

```
R64#show secure bootset
IOS resilience router id FTX1125A67x

IOS image resilience version 12.4 activated at 14:24:50 UTC Mon April 2
2017
Secure archive flash:/c2800nm-advipservicesk9-mz.124-25e.bin type is image
(elf) [] Runnable image, entry point 0x8000F000, run from ram
IOS image resilience version 12.4 activated at 14:24:50 UTC Mon April 2
2017
Secure archive flash:.runcfg-20140131-14259.ar type is config
Configuration archive size 4060 bytes
```

With the location of the secure configurations in hand, now run the following command to restore the configuration:

```
R64(config)#secure boot-config restore  flash:.runcfg-20140131-14259.ar
ios resilience: configuration successfully restored as flash: .runcfg-
20140131-14259.ar
```

In case you were already wondering what would stop a hacker from using these commands, it is worth knowing that these commands can be run *only* from the console connection.

Implementing OSPF Routing Update Authentication

One of the ways in which a malicious individual may attempt to gather information about your network is to enable the routing protocol in use on a workstation and convince your routers to allow the workstation to become a routing neighbor, allowing the malicious individual to receive routing updates from your routers. As if this isn't enough to be concerned about, he may also convince your routers to accept a malicious routing update from his workstation, which could pollute the routing tables of your routers. If this occurs, it could result in an inability of the routers to properly route, which would be a form of denial-of-service attack. Moreover, he could inject routes that cause traffic to be directed to him as a prelude to a man-in-the-middle attack.

To prevent this, you can configure the routers to authenticate one another when performing routing updates. In the following two sections, you'll learn how to do this for the two most commonly used interior routing protocols, OSPF and EIGRP.

Implementing OSPF Routing Update Authentication

OSPF routing updates are secured using a hashing algorithm. You can use either MD5 or SHA-256HMAC. Be aware, however, that some devices may support only MD5. The following are the high-level steps to configuring this:

1. Define a keychain (a keychain can be used to hold multiple keys if required).
2. Define a key by number that will reside on the keychain.
3. Specify the key characters of the key.
4. Specify the hashing algorithm.
5. Apply the keychain to an interface.

While keychain names and the key numbers do not have to match on the two routers on either end of the link, the key strings and the hashing algorithms *must* match!

In this following example, I'm going to use MD5 for the configuration. I will first configure

router R64 and then router R65 on the other end of the link. The first step is to configure the keychain as shown here. The keychain on R64 will be **`ospf-keys`**.

```
R64(config)#key-chain ospf-keys
R64(config-keychain)#
```

Notice the prompt has changed, and I am now in keychain configuration mode, which is where I will define the key number as follows. The number I am using is 1.

```
R64(config-keychain)#key 1
R64(config-keychain-key)#
```

Again, the prompt has changed, and I am in key 1 configuration mode, which is where I define the characters in the key, called the *key string*. The string I am using is `troymac`.

```
R64(config-keychain-key)#key-string troymac
R64(config-keychain-key)#
```

The next step is to tell the router the algorithm (MD5) to use for this key, which is done at the same key 1 prompt.

```
R64(config-keychain-key)#cryptographic-algorithm md5
R64(config-keychain-key)#
```

The final step is to apply the keychain to the interface that connects to router R65.

```
R64(config-if)#ip ospf authentication key-chain ospf-keys
R64(config-if)#
```

Keep in mind that while one of the routers is set to use authentication and the other has not yet been configured, routing updates will fail, and the devices will no longer be OSPF neighbors. This will resolve itself as soon as the other router is correctly configured.

The configuration can be the same on router R65, but I'm going to change two of the values that do *not* have to match just to show that they don't have to match, while keeping the values that *do* have to match (the key string and the hashing algorithm) the same. The following is the entire set of commands on R65:

```
R65(config)#key-chain router-keys
R65(config-keychain)#key 2
R65(config-keychain-key)#key-string troymac
R65(config-keychain-key)#cryptographic-algorithm md5
R65(config-keychain-key)#end
R65(config)#int g0/1
R65(config-if)#ip ospf authentication key-chain router-keys
```

Implementing EIGRP Routing Update Authentication

Configuring EIGRP routing update authentication is similar to OSPF. However, OSPF specifies the hashing algorithms in the same mode where you specify the key string, but in EIGRP you specify that on the interface. The following are the commands for R64 and R65. Additionally, when you specify the algorithm, you specify the EIGRP AS number in the same command. In the following examples, that AS number is 66. Notice that, again, the keychain names and key numbers do *not* have to match, while the key string and hashing algorithms *do* have to match.

```
R64(config)#key-chain router-keys
R64(config-keychain)#key 1
R64(config-keychain-key)#key-string troymac
R64(config-keychain-key)#end
R64(config)#int g0/2
R64(config-if)#ip authentication key-chain router-keys
R64(config-if)#up authentication mode eigrp 66 md5

R65(config)#key-chain EIGRP-keys
R65(config-keychain)#key 2
R65(config-keychain-key)# key-string troymac
R65(config-keychain-key)#end
R65(config)#int g0/1
R65(config-if)#ip authentication key-chain EIGRP-keys
R65(config-if)#ip authentication mode eigrp 66 md5
```

Securing the Control Plane

There are four types of packets that a router may encounter, and they operate in four “planes” of the router. The four planes and the types of packets that operate in these planes are as follows:

Data Plane Packets These are end-station, user-generated packets that are always forwarded by network devices to other end-station devices.

Control Plane Packets These are network device–generated or received packets that are used for the creation and operation of the network itself. Examples include protocols such as ARP, BGP, and OSPF.

Management Plane Packets These are network device–generated or received packets or management station–generated or received packets that are used to manage the network. Examples are Telnet, SSH, TFTP, SNMP, FTP, NTP, HTTP, HTTPS and other protocols used to manage the device and/or network.

Services Plane Packets A subset of data plane packets, services plane packets are also user-generated packets that are forwarded by network devices to other end-station devices. Examples include such functions as GRE encapsulation, QoS, MPLS VPNs, and SSL/IPsec encryption/decryption.

The concern in this section is with the protection of access to the control plane, which includes

the hardware and software that supports routing and the management of the device. Packets in the control plane are those that are either destined for the router itself or generated by the router. If access to the control plane is not protected, routing table corruption, changes to the router configuration, and DoS attacks on the router may result.

Control Plane Policing

Control plane policing (CoPP) is a Cisco IOS feature that can be implemented to prevent these issues. Its implementation is an advanced topic not covered in the exam objectives; however, an understanding of its use is included in the exam objectives.

CoPP treats the control plane as a stand-alone entity with its own ingress and egress ports. It allows for the implementation of controls at the ingress port to the control plane. Figure 4.1 shows the relationship between those control plane ingress and egress ports and the physical interfaces. It also shows the paths taken by the four types of traffic discussed in the previous section.

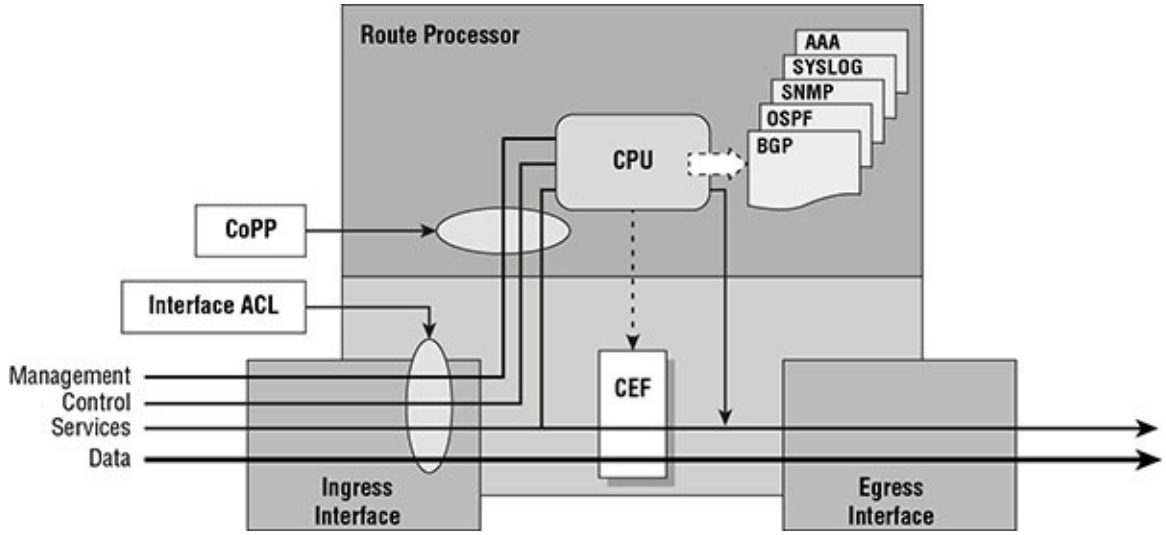

FIGURE 4.1 CoPP

Notice that three types of traffic can be controlled by CoPP, that is, management, control, and services traffic. Also notice that when access control lists (ACLs) are applied to the ingress physical interface and CoPP has also been applied, CoPP comes into play *only* for traffic that was allowed through the ingress physical interface ACL. As you can see, ultimately CoPP is designed to protect the route processor. Controls can be implemented that allow and disallow certain types of traffic and can also be used to rate-limit the traffic so as to prevent a DoS attack.

When CoPP is configured, the configuration follows the Cisco Modular QoS CLI (MQC). In this model, three mechanisms are used.

Class Maps Used to categorize traffic types into classes. ACLs are typically used to define the traffic, and then the ACL is referenced in the class map.

Policy Maps Used to define the action to be taken for a particular class. Actions that can be

specified are allow, block, and rate-limit.

Service Policies Used to specify where the policy map should be implemented.

Figure 4.2 shows the relationship between these mechanisms.

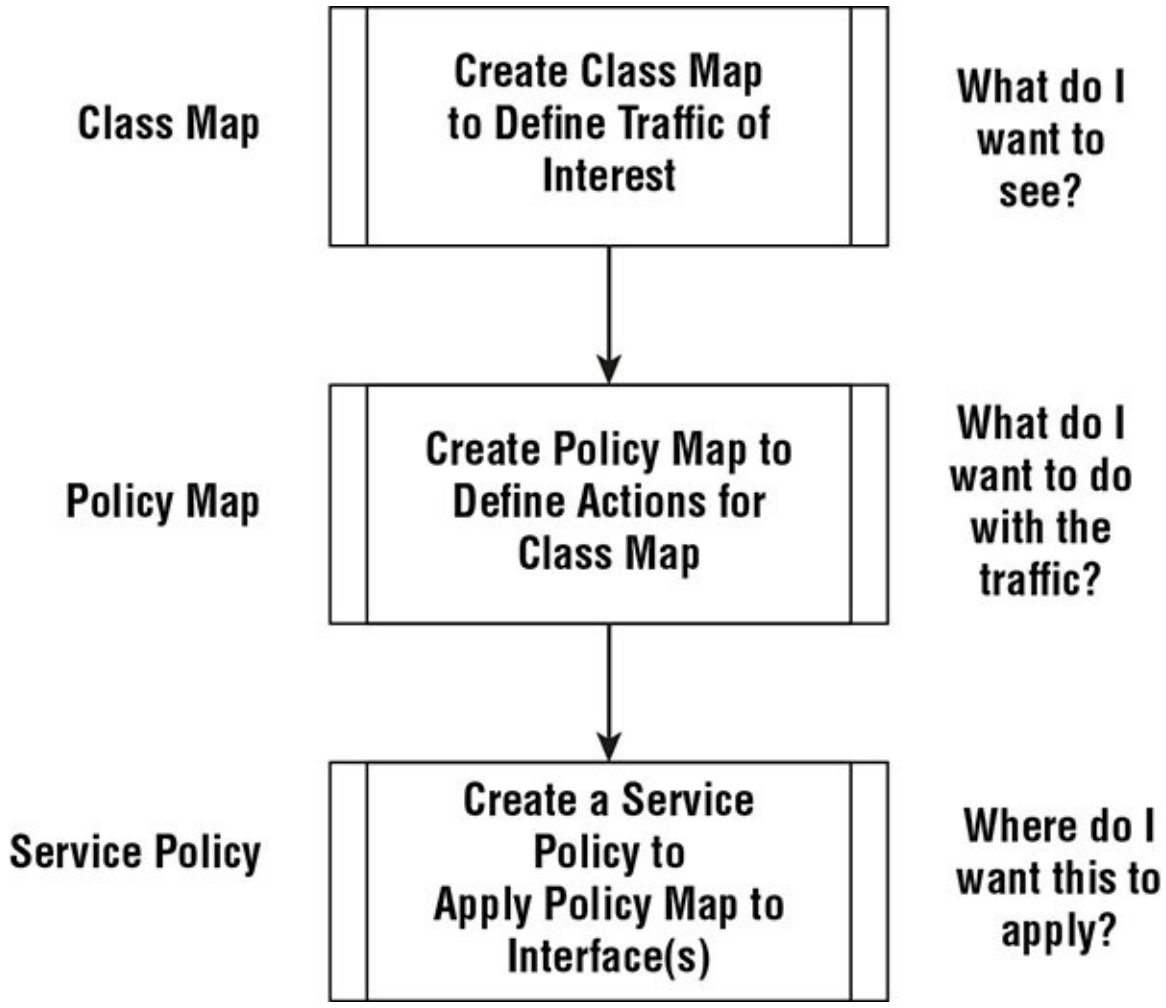

FIGURE 4.2 Modular policy framework

This framework is used for other features as well, such as QoS and traffic shaping.

Summary

In this chapter, you learned about methods for securing administrative access to the router or switch. You also learned how IOS privilege levels and IOS role-based CLI can be used to specify allowed actions. The Cisco IOS resilient configuration feature and its benefits were introduced. You also learned how to configure authentication for router updates for both OSPF and EIGRP. Finally, the chapter discussed how control plane policing can be used to control access to the control plane.

Exam Essentials

Secure administrative access to the router. Complete the steps required to use Secure Shell to administer the router. These steps include setting the router name and domain name and generating the RSA key. It also includes specifying the use of SSH on the vty lines.

Control administrative actions. Configure IOS privilege levels and IOS role-based CLI to specify actions allowed by technicians when maintaining the router.

Implement Cisco IOS resilient configuration. Protect the integrity and availability of both the IOS and the startup configuration by configuring the Cisco IOS resilient configuration feature.

Implement OSPF routing update authentication. Describe the steps involved in configuring authentication between two OSPF routers that is invoked at each routing update.

Implement EIGRP routing update authentication. Describe the steps involved in configuring authentication between two EIGRP routers that is invoked at each routing update.

Describe the benefits of securing the control plane. Understand the dangers that confront the control plane of a router and how control plane policing can be used to control access to the control plane and prevent attacks on it.

Review Questions

1. Which of the following is *not* a required step when configuring a router for SSH access?

   A. Set the router name.

   B. Generate the RSA key.

   C. Set the router domain name.

   D. Set the router loopback IP address.

2. Which of the following statements is true of the following system message?

```
R63(config)#
*Mar 28 18:32:09.095: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

   A. This router will accept connections only from SSH version 1 devices.

   B. This router will accept connections only from SSH version 2 devices.

   C. This router will accept connections from SSH version 1 or SSH version 2 devices.

   D. This router is an SSH version 1 device.

3. Which statement is false with regard to this configuration?

```
R63(config)#line vty 0 1114
R63(config-line)#login local
R63(config-line)#transport input ssh
R63(config-line)#
```

   A. vty line 67 is affected by this configuration.

B. The user accounts for access to the vty lines are contained on this router.

C. Only SSH is allowed to be used on the vty lines.

D. SSH access will be controlled by a TACACS+ server.

4. Which of the following statements is true with regard to privilege levels in the IOS?

   A. There are 16 privilege levels.

   B. Level 16 is user mode.

   C. Level 0 is privileged mode.

   D. Privilege levels can be defined on routers but not ASA devices.

5. Which of the following commands allows the technician to whom the privilege level will be assigned to only change IP addresses?

   A. `privilege exec level 12 show interfaces`

   B. `privilege configure level 12 interface`

   C. `privilege interface level 12 ip`

   D. `enable secret level 12 wordpass`

6. Which of the following is the only parser view that exists by default?

   A. admin

   B. root

   C. exec

   D. priv

7. Which of the statements is true with regard to the following configuration?

```
R64(config)#secure boot-image
*April 2 17:24:50.231: %IOS_Reslience-5-IMAGE_RESIL_ACTIVE: Successfully
secured running image
```

   A. It secures the startup configuration.

   B. It secures the IOS image.

   C. It secures both the IOS image and the startup configuration.

   D. It secures nothing until an additional command is run.

8. Which of the following statements is false with regard to the Cisco IOS resilient configuration?

   A. The IOS image and the startup configuration are called the *secure boot set* when protected.

   B. Once secured, the configuration cannot be removed.

C. To restore the bootset, you must know its location.

D. To restore the bootset, you must know its name.

9. Which of the following can be done only from a console connection?

A. Set up SSH.

B. Remove a secure bootset configuration.

C. Create a privilege level.

D. Generate an SSH key.

10. Which of the following hashing algorithms are used to implement OSPF routing update authentication?

A. MD4

B. MD5

C. SHA1

D. SHA2

11. Which of the following configuration settings must match in the two routers when configuring OSPF routing update authentication?

A. Keychain name

B. Key number

C. Keystring

D. Router passwords

12. To which component is the keychain applied when configuring OSPF routing update authentication?

A. Routing protocol

B. Hashing algorithm

C. Interface

D. Key

13. To which component is the key applied when configuring OSPF routing update authentication?

A. Routing protocol

B. Hashing algorithm

C. Interface

D. Keychain

14. To which component is the hashing algorithm applied when configuring OSPF routing update authentication?

    A. Key

    B. Hashing algorithm

    C. Interface

    D. Keychain

15. How is configuring EIGRP routing update authentication different from OSPF?

    A. OSPF specifies the hashing algorithms in the same mode where you specify the key string; in EIGRP, that is specified on the interface.

    B. EIGRP specifies the hashing algorithms in the same mode where you specify the key string; in OSPF, that is specified on the interface.

    C. OSPF specifies the keychain in the same mode where you specify the key string: in EIGRP, that is specified on the interface.

    D. OSPF specifies the keychain in the same mode where you specify the key string; in EIGRP, that is specified on the hashing algorithm.

16. When you specify the algorithm for EIGRP route update authentication, you also specify what value in the same command?

    A. Process ID

    B. AS number

    C. Area ID

    D. Interface number

17. Which packet type comes from end stations to be forwarded by the router?

    A. Data plane

    B. Control plane

    C. Management plane packets

    D. Services plane packets

18. Which of the following is an example of control plane packets?

    A. Data to be routed

    B. OSPF updates

    C. Telnet packets

    D. Packets forwarded by network devices to other end-station devices

19. Packets that are either destined for the router itself or generated by the router are in which

plane?

A. Data plane

B. Services plane

C. Control plane

D. Services plane

20. When CoPP is configured, the configuration follows the Cisco Modular QoS CLI (MQC). In this model, which mechanism specifies the actions to be taken on the specified traffic type?

A. Class map

B. Policy map

C. Service policy

D. Action map

Chapter 5
Understanding Layer 2 Attacks

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.4 Common Layer 2 attacks**
  - Describe STP attacks
  - Describe ARP spoofing
  - Describe MAC spoofing
  - Describe CAM table (MAC address table) overflows
  - Describe CDP/LLDP reconnaissance
  - Describe VLAN hopping
  - Describe DHCP spoofing

To prevent a certain type of attack, you must understand the attack. Attacks can occur at a number of different layers of the TCP/IP model. When I discuss layer 2 attacks, I am talking about attacks that use layer 2 addresses (MAC addresses) or that are aimed at protocols that operate at layer 2. Finally, some layer 2 attacks take advantage of layer 3 services such as DHCP, but they do so within a local subnet and thus are also called layer 2 attacks. In this chapter, I'll describe how a number of layer 2 attacks occur. In the next chapter, I'll discuss mitigations for these attacks.

In this chapter, you will learn the following:

Common layer 2 attacks

Understanding STP Attacks

Spanning Tree Protocol (STP) is used to prevent switching loops that can occur when there is redundancy built into the switching network. Since redundancy is a desirable design concept, STP is a feature that you cannot live without. Unfortunately, there is an attack on the switching network that takes advantage of the operations of STP. The good news is that Cisco has developed several responses to these attacks, but you must understand the attacks and how the features address the vulnerabilities to properly implement these safeguards. In this chapter, I'll

discuss the attacks and how they work, and in Chapter 6 I'll cover the implementation of the mitigations.

STP attacks target the loop-free switching topology that is created by the switches using the *bridge protocol data units* (BPDUs) upon which STP is based. These BPDUs are used by the switches to select the root bridge and thereafter to select the switch ports that are forwarding and those that are blocking. These BPDUs are also used when a change in the topology occurs (such as a link going down) to establish a new loop-free topology based upon the remaining links.

While link issues can cause a change in the topology, another event can cause this as well, and that is the introduction of a new switch in the network that possesses a higher bridge priority (sometimes called a *superior BPDU*) than the current root bridge. When a malicious individual introduces a rogue switch to the switching network and the rogue switch has a superior BPDU than the one held by the current root bridge, the new switch assumes the position of root bridge.

Since the topology of the switching network depends on the position of the root bridge and the relative position of the other switches to the root bridge, this alters the topology in ways that not only may impact performance but may cause all traffic to traverse the new rogue switch, which will be under the management of the attacker. To see how this can impact the topology, look at Figure 5.1 .

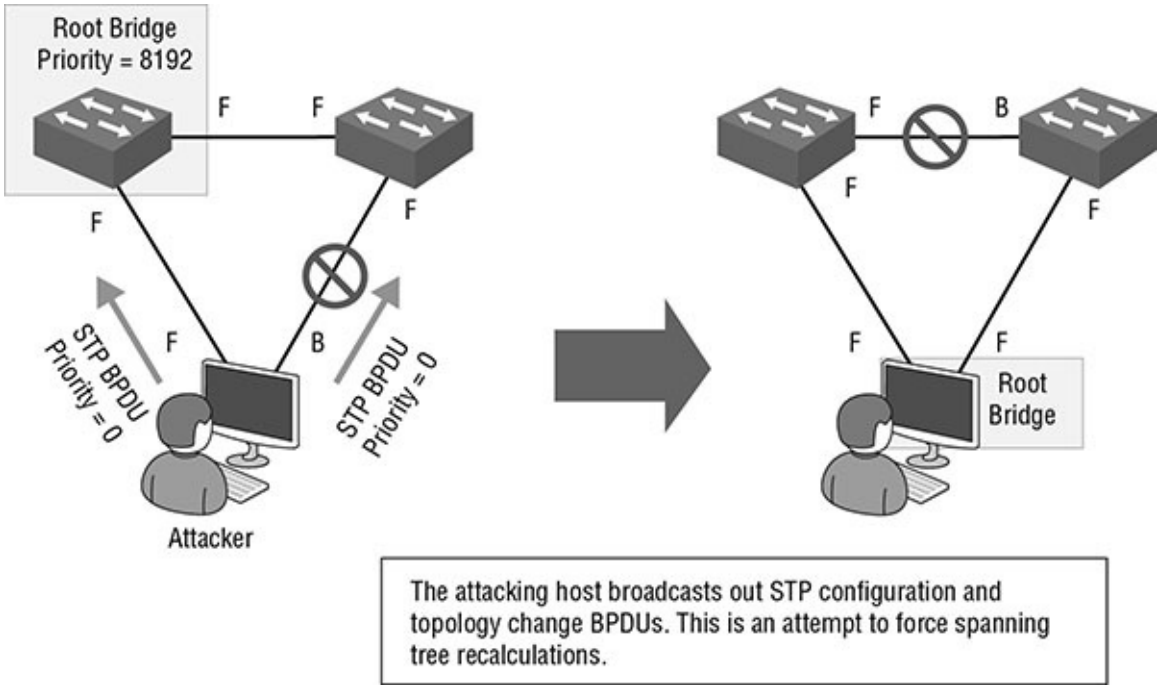

FIGURE 5.1 STP attack

Again, mitigations to this attack will be covered in Chapter 6.

Understanding ARP Attacks

An *ARP poisoning attack* is one that takes advantage of the normal process that devices use to learn an unknown MAC address that a device with a known IP address possesses. Before I cover the ARP poisoning attack, I'll review the ARP broadcast process.

Address Resolution Protocol (ARP), one of the protocols in the TCP/IP suite, operates at layer 3 of the OSI model. The information it derives is utilized at layer 2, however. ARP's job is to resolve the destination IP address placed in the header by IP to a layer 2 or MAC address. Remember, when frames are transmitted on a local segment, the transfer is done in terms of MAC addresses, not IP addresses, so this information must be known.

Whenever a packet is sent across the network, at every router hop and again at the destination subnet the source and destination MAC address pairs change, but the source and destination IP addresses do not. The process that ARP uses to perform this resolution is called an *ARP broadcast*.

First an area of memory called the ARP cache is consulted. If the MAC address has been recently resolved, the mapping will be in the cache, and a broadcast is not required. If the record has aged out of the cache, ARP sends a broadcast frame to the local network that all devices will receive. The device that possesses the IP address responds with its MAC address. Then ARP places the MAC address in the frame and sends the frame. Figure 5.2 illustrates this process.

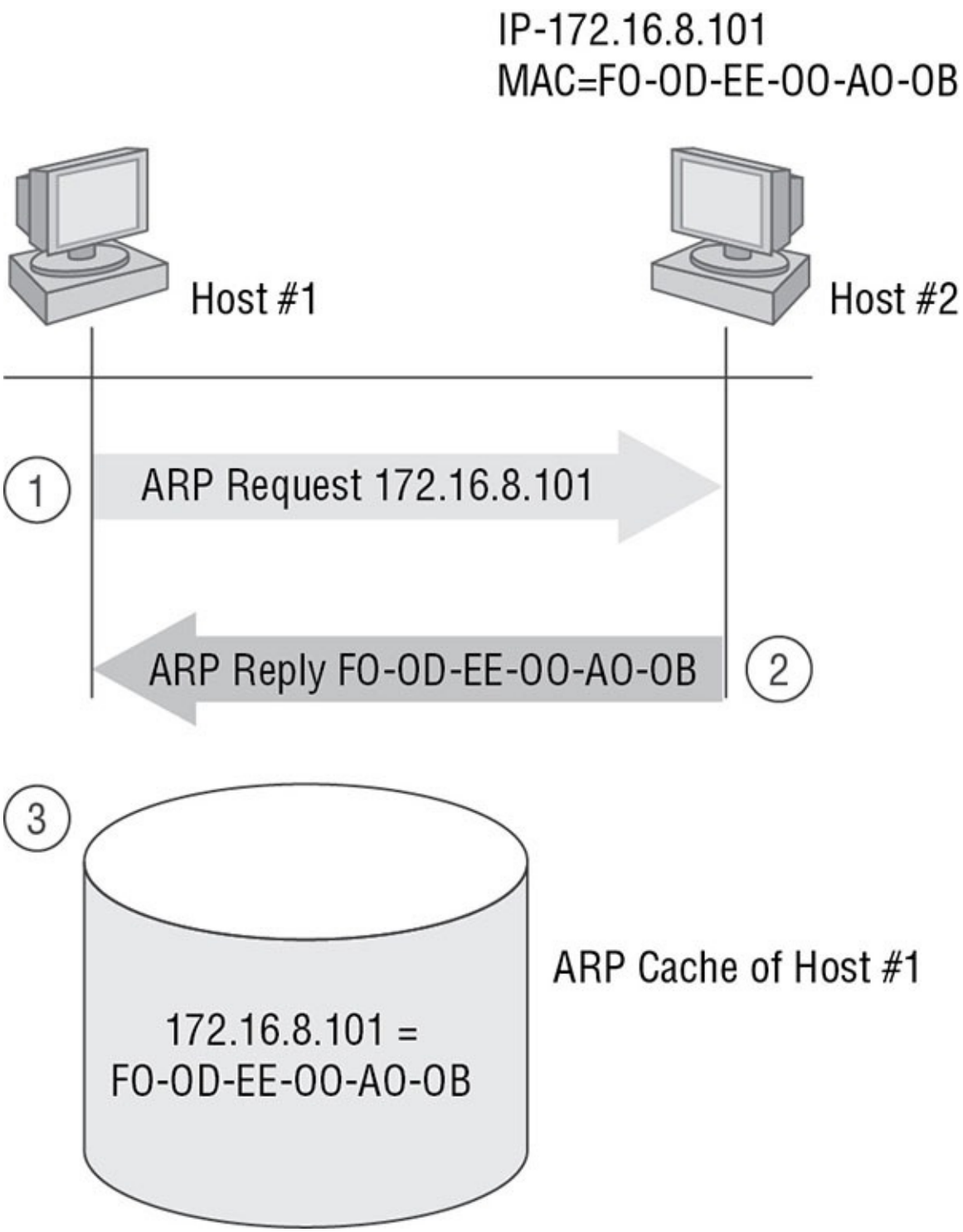

FIGURE 5.2 ARP process

In an ARP poisoning attack, the attacker sends a packet type called a *gratuitous ARP* to the target device with an incorrect IP address to MAC address mapping.

What's a Gratuitous ARP?

A *gratuitous ARP* is called *gratuitous* because the ARP message sent is an answer to a question that the target never asks. In the normal ARP process, a device never announces its MAC address to another device unless asked to do so. This means there is an ARP request that goes from device A to device B and then an ARP reply from device B to device A. In the case of the gratuitous ARP, the ARP message is a reply to a request never sent by the target that causes a malicious (and incorrect) update to the receiver's ARP cache.

In a classic man-in-the middle attack, the attacker will send these gratuitous ARP requests to the two target devices between which he would like to be "in the middle." In the scenarios shown in Figure 5.3 , the two targets are the Victim laptop and the default gateway of the Victim laptop.

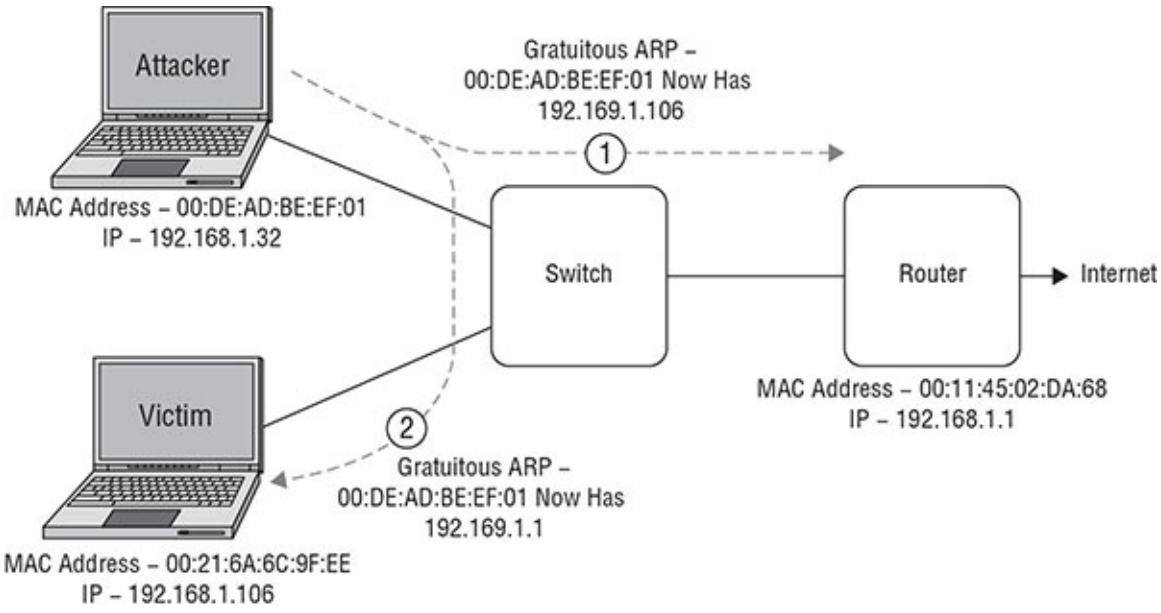

FIGURE 5.3 ARP cache poisoning

After the gratuitous ARP messages are sent and processed by the two targets, the Victim laptop and the router interface would be sending traffic to the attacker while both thinking they are sending to one another. Mitigations for this attack will be presented in Chapter 6. Stayed tuned!

Understanding MAC Attacks

MAC spoofing attacks occur when an attacker changes his MAC address so that his device appears to be another device. As is the case with all spoofing attacks, the ultimate aim is to receive something intended for the real device or to get past access controls based on a MAC address.

A MAC address attack is also considered a switch attack because it leverages the MAC

address table in the switch to accomplish the goal of receiving traffic destined for another device. As you know, the MAC address table is populated as frames are sent and received by the switch. On the left side of Figure 5.4 , the MAC table prior to the attack is shown.

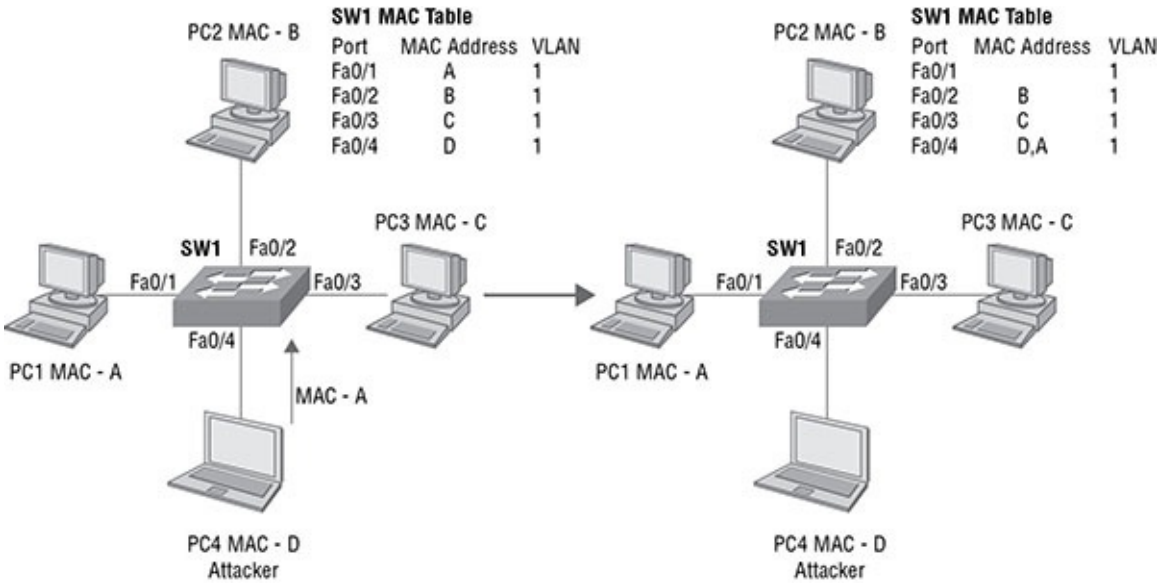

FIGURE 5.4 MAC spoofing

Prior to the attack, the switch has the MAC address A (shortened for simplicity) recorded on port Fa0/1 where the real holder of that MAC address resides. When the attacker sends a frame with a spoofed MAC address of A, then the switch does what a switch is supposed to do. It removes the MAC address from its current listing of port Fa0/1 and moves it to port Fa0/4, where the attacker resides. Now the attacker will receive all traffic destined for the device on port Fa0/1. This will continue until the device on port Fa0/1 sends a frame. However, by continually sending frames, the attacker will be able to continually update the table to his advantage. But fear not! There are ways to deal with this, and I will cover them in Chapter 6. You'll get there soon. Don't peek!

Understanding CAM Overflows

As you know, the MAC address table, also called the *content addressable memory (CAM) table*, is populated by the switch as frames are switched through it. The switch records the source MAC address of every frame entering each port. There is a limited amount of memory space that is available for this table. In a *CAM overflow* attack, the attacker floods the switch with frames that have invalid source MAC addresses. This is easier than it sounds by using a tool such as `macof`.

At some point, the CAM table is full and can hold no other MAC addresses. Any MAC addresses that were in the table prior to the attack will still be there, and those devices will still be able to receive traffic. However, it is not the aim of the attacker to prevent access to these devices. When the table is full and frames destined to MAC addresses that are not currently in the table are received, they will be flooded out all ports. If you think about it, this is the normal operation of a switch when it receives a frame with an unknown destination

MAC address. Figure 5.5 shows this attack, with the steps in the process numbered.

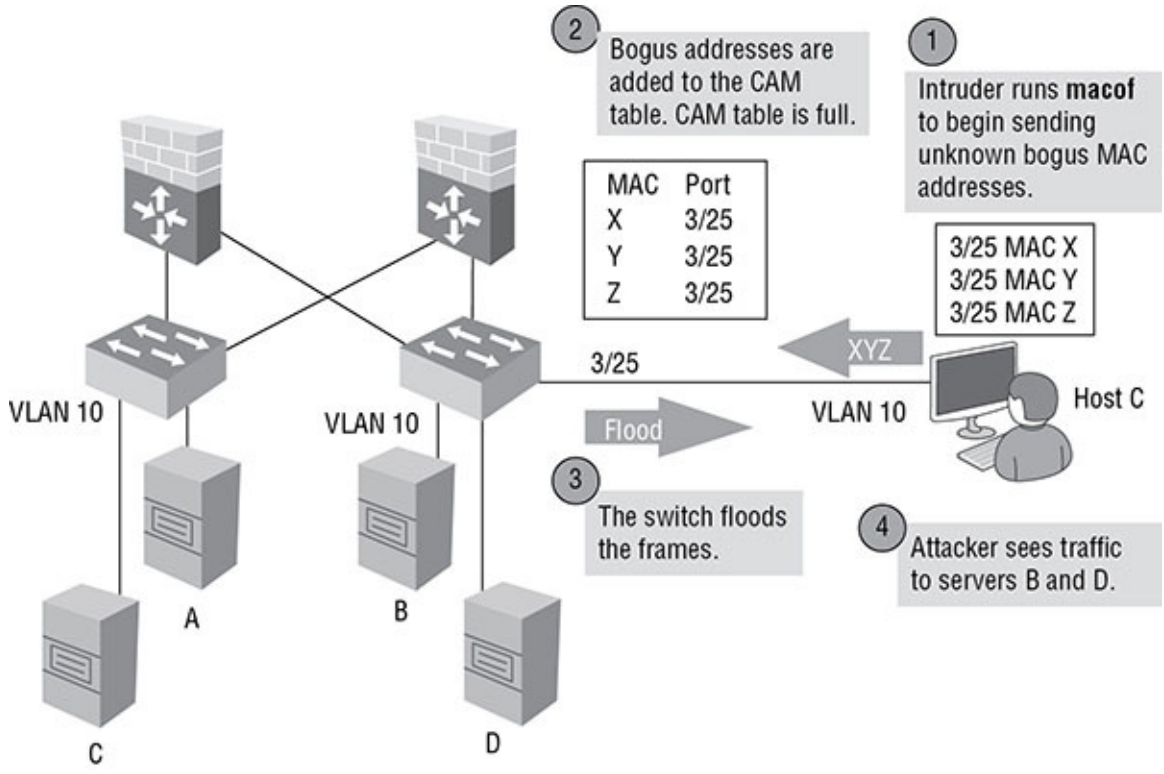

FIGURE 5.5 CAM overflow

The result of this attack is that the attacker is now able to receive traffic that he would not have been able to see otherwise because in this condition the switch is basically operating as a hub, not a switch. In Chapter 6 I'll discuss how to prevent this attack.

Understanding CDP/LLDP Reconnaissance

Cisco Discovery Protocol (CDP) and its standards-based alternative *Link Layer Discovery Protocol (LLDP)* are useful tools. They can be used to display information about directly connected devices. This can be especially useful when you have no layer 3 connectivity to a neighboring device because the protocols operate at layer 2 and thus can be used to extract information even when IP is not functional. Unfortunately, as is often the case, there is a dark side to these tools.

When a malicious individual is attempting to hack your network, the first thing the hacker does is perform network reconnaissance. This operation admits to gathering all information possible about the layout of the network and the devices in the network. By capturing the CDP or LLDP packets that are used by Cisco devices to exchange information, a wealth of information can be obtained.

For this reason, many organizations choose to forgo the advantages of using CDP and LLDP and disable the operation of both on Cisco devices. Disabling these features can be done on an interface basis or globally on all interfaces. This time I won't make you wait until Chapter 6 for the solution.

To disable CDP on an interface, use the following command in interface configuration mode:

```
Router67(config-if)#no cdp enable
```

To disable CDP globally, run the following command in global configuration mode:

```
Router67(config)#no cdp run
```

To disable LLDP on an interface, run the following commands in interface configuration mode:

```
Router67(config-if)#no lldp receive
Router67(config-if)#no lldp transmit
```

To disable LLDP globally, run the following command in global configuration mode:

```
Router67(config)#no lldp run
```

Understanding VLAN Hopping

A virtual LAN (VLAN) security issue you should be aware of is called *VLAN hopping*. By default, a switch port is an access port, which means it can be a member of only a single VLAN. Ports that are configured to carry the traffic of multiple VLANs, called *trunk ports*, are used to carry traffic between switches and routers. A VLAN hopping attack's aim is to receive traffic from a VLAN of which the hacker's port is not a member. This can be done in two ways, covered next.

Switch Spoofing

Switch ports can be set to use a protocol called Dynamic Trunking Protocol (DTP) to negotiate the formation of a trunk link. If an access port is left configured to use DTP, it is possible for hackers to set their interface to spoof a switch and use DTP to create a trunk link. If this occurs, they can capture traffic from all VLANs. Figure 5.6 shows a *switch spoofing* attack.

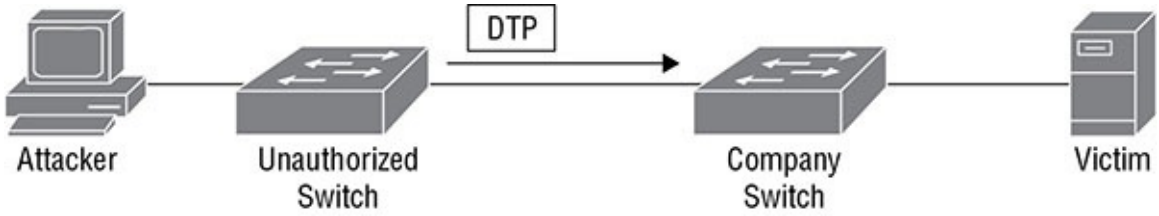

FIGURE 5.6 Switch spoofing

The prevention of this attack will be covered in Chapter 6.

Double Tagging

Trunk ports use an encapsulation protocol called 802.1q to place a VLAN tag around each frame to identify the VLAN to which the frame belongs. When a switch at the end of a trunk link receives an 802.1q frame, it strips this off and forwards the traffic to the destination device. In a *double tagging* attack, the hacker creates a special frame that has two tags. The

inner tag is the VLAN to which the hacker wants to send a frame (perhaps with malicious content), and the outer tag is the real VLAN of which the hacker is a member. If the frame goes through two switches (which is possible since VLANs can span switches), the first tag gets taken off by the first switch, leaving the second, which allows the frame to be forwarded to the target VLAN by the second switch.

Figure 5.7 shows this process. In this example, the native VLAN number between the Company Switch A and Company Switch B switches has been changed from the default of 1 to 10.

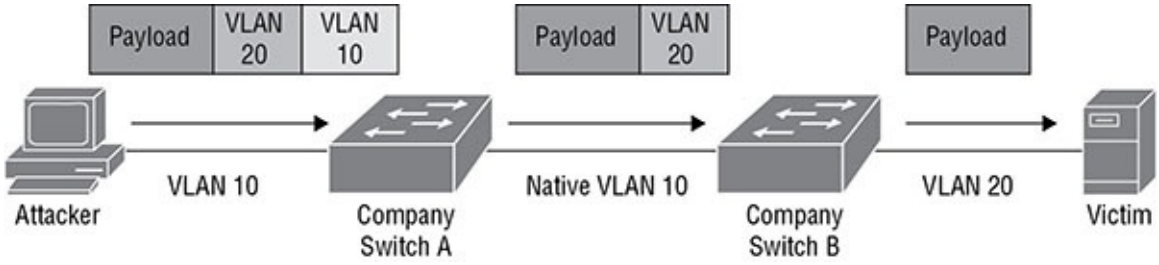

FIGURE 5.7 Double tagging

Double tagging is only an issue on switches that use "native" VLANs. A native VLAN is used for any traffic that is still a member of the default VLAN, or VLAN 1. The mitigation of this attack will be covered in Chapter 6.

Understanding DHCP Spoofing

Dynamic Host Configuration Protocol (DHCP) is used to automate the process of assigning IP configurations to hosts. When configured properly, it reduces administrative overload, reduces the human error inherent in manual assignment, and enhances device mobility. But it introduces a vulnerability that when leveraged by a malicious individual can result in an inability of hosts to communicate (constituting a DoS attack) and can result in peer-to-peer attacks.

When an illegitimate DHCP server (called a *rogue* DHCP server) is introduced to the network, unsuspecting hosts may accept DHCP offer packets from the illegitimate DHCP server, rather than the legitimate DHCP server. When this occurs, the rogue DHCP server will not only issue the host an incorrect IP address, subnet mask, and default gateway address (which makes a peer-to-peer attack possible) but can also issue an incorrect DNS server address, which will lead to the host relying on the attacker's DNS server for the IP addresses of websites (such as major banks) that lead to phishing attacks. Figure 5.8 shows an example of how this can occur.

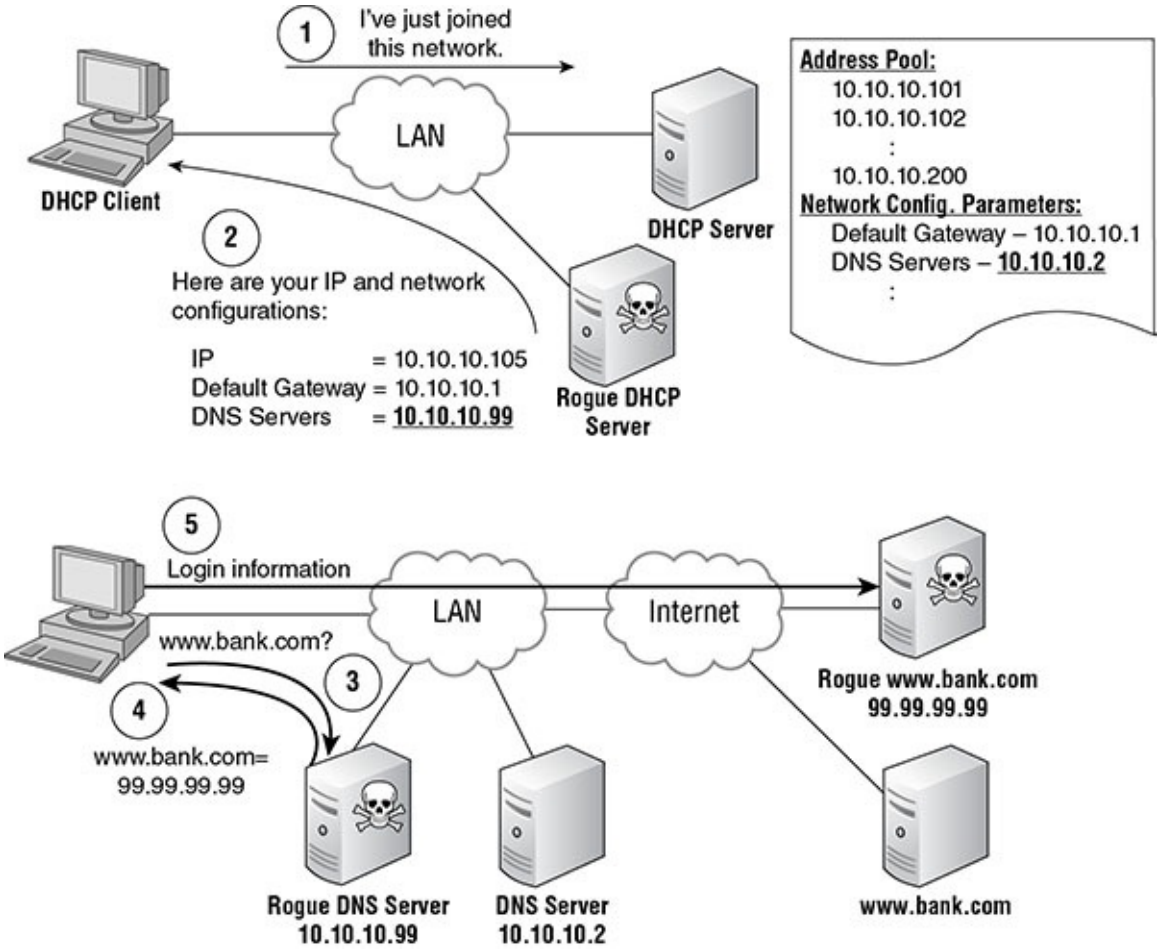

FIGURE 5.8 DHCP spoofing

In Figure 5.8 , after receiving an incorrect IP address, subnet mask, default gateway, and DNS server address from the rogue DHCP server, the DHCP client uses the attacker's DNS server to obtain the IP address of his bank. This leads him to unwittingly connect to the attacker's copy of the bank's website. When the client enters his credentials to log in, the attacker now has his bank credentials and can proceed to empty out his account. It sounds scary, but luckily I will cover mitigation for this attack in Chapter 6!

Summary

In this chapter, you learned about STP attacks such as rogue switches. The chapter discussed how an ARP spoofing attack works and how it leads to a man-in-the-middle attack. MAC spoofing and its use in accessing traffic to which an attacker is not authorized was also covered. You learned how a CAM overflow attack works and its effect on a switch. You looked at both the value and the danger of using CDP and LLDP. Finally, you learned how VLAN hopping attacks are performed.

Exam Essentials

Explain STP attacks. Describe how an attacker can introduce a rogue switch into the network

and alter the loop-free switching topology created by STP.

Describe ARP spoofing attacks. Explain how an ARP spoofing attack is set up and what the end result of a successful ARP spoofing attack can be.

Understand MAC spoofing. Describe the purpose of a MAC spoofing attack and how it might enable an attacker to receive traffic to which she is not authorized.

Explain the CAM overflow attack. List the steps that can cause a CAM overflow and describe the potential benefit to a malicious individual.

Understand the issues with CDP and LLDP. Describe the reason for disabling CDP and LLDP and explain how to implement this.

Describe a VLAN hopping attack. List the ways to accomplish a VLAN hopping attack and explain the purpose of this attack.

Explain DHCP snooping. Describe a DHCP spoofing attack and understand the attacks to which it can lead.

Review Questions

1. Which of the following is true of an STP attack?
   A. It occurs with the introduction of a new switch in the network that is more powerful than the current root bridge.
   B. It occurs with the introduction of a new switch in the network that possesses an inferior BPDU than the current root bridge.
   C. It occurs with the introduction of a new switch in the network that possesses a superior BPDU than the current root bridge.
   D. It may cause all traffic to bypass the new rogue switch, which will be under the management of the attacker.
2. Which of the following takes advantage of the normal process that devices use to learn an unknown MAC address that a device with a known IP address possesses?
   A. CAM overflow
   B. ARP poisoning attack
   C. DHCP spoofing
   D. STP attack
3. Which of the following is used by an attacker to pollute the ARP cache of hosts?
   A. Gratuitous ARP
   B. Superior BPDU

C. Inferior BPDU

D. DTP

4. Which of the following is checked prior to a host performing an ARP broadcast?

   A. CAM table

   B. Host file

   C. ARP cache

   D. LMhosts file

5. Which of the following occurs when an attacker changes his physical address so that his device appears to be another device?

   A. DHCP spoofing

   B. CAM overflow

   C. MAC spoofing

   D. Switch spoofing

6. Which of the following is also considered a switch attack?

   A. MAC spoofing

   B. DHCP spoofing

   C. Rogue DHCP

   D. ARP spoofing

7. The content addressable memory table is also known as which of the following?

   A. ARP cache

   B. DNS resolver cache

   C. MAC table

   D. DHCP scope

8. Which of the following attacks floods the switch with frames that have invalid source MAC addresses?

   A. Smurf attack

   B. CAM overflow

   C. SYN flood

   D. Fraggle attack

9. Which of the following attacks causes a switch to basically operate as a hub and not a switch?

A. Smurf attack

B. CAM overflow

C. SYN flood

D. Fraggle attack

10. Which of the following is standards based?

A. LLDP

B. CDP

C. EIGRP

D. DTP

11. Which of the following commands disables CDP on all interfaces when applied at the global configuration prompt?

A. `cdp disable`

B. `no cdp enable`

C. `no cdp run`

D. `no cdp receive`

12. Which of the following commands disables LLDP reception on an interface when applied at the interface configuration prompt?

A. `lldp disable`

B. `no lldp enable`

C. `no lldp run`

D. `no lldp receive`

13. Which attack's aim is to receive traffic from a VLAN of which the hacker's port is not a member?

A. CDP reconnaissance

B. VLAN hopping

C. DHCP snooping

D. STP attack

14. Which of the following is an example of a VLAN hopping attack?

A. Switch spoofing

B. Man-in-the-middle

C. LLDP reconnaissance

D. ARP spoofing

15. What protocol does the attacker leverage in a switch spoofing attack used to perform VLAN hopping?

A. CDP

B. LLDP

C. DTP

D. STP

16. Which attack is only an issue on switches that use “native” VLANs?

A. Switch spoofing

B. Double tagging

C. ARP pollution

D. CAM overflow

17. Which service introduces a vulnerability that when leveraged by a malicious individual can result in an inability of hosts to communicate (constituting a DoS attack) and peer-to-peer attacks?

A. DHCP

B. DNS

C. DTP

D. NAT

18. Which of the following attacks can lead to a phishing attack?

A. DHCP spoofing

B. CAM overflow

C. Double tagging

D. Switch spoofing

19. Which attack occurs on trunk links?

A. Double tagging

B. ARP pollution

C. CAM overflow

D. DHCP spoofing

20. What protocol is used to negotiate the formation of a trunk link?

A. CDP

B. NTP

C. DTP

D. VTP

Chapter 6
Preventing Layer 2 Attacks

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.5 Mitigation procedures**
  - Implement DHCP snooping
  - Implement Dynamic ARP Inspection
  - Implement port security
  - Describe BPDU guard, root guard, loop guard
  - Verify mitigation procedures

Now that you understand some of the layer 2 attacks that can be aimed at your switching infrastructure, you are ready to learn about the mitigations that are available to address each of these attacks. This chapter will discuss how to prevent STP attacks, ARP pollution, MAC spoofing, and CAM overflows. The chapter will also discuss the prevention of VLAN hopping attacks and rogue DHCP servers. Finally, the chapter will discuss how to verify the proper application of the mitigations discussed in the chapter.

In this chapter, you will learn the following:

Mitigations for common layer 2 attacks

Configuring DHCP Snooping

In Chapter 5 you learned that a rogue DHCP server can create significant security issues for your environment. When a rogue DHCP server issues an incorrect IP address, an incorrect subnet mask, and incorrect default gateway information to the host, it can prevent proper communications for those hosts, amounting to a DoS attack. Moreover, it can also result in traffic being directed through this device so that it captures all traffic. Finally, if the rogue DHCP server issues an incorrect DNS server address, it can result in a rogue DNS server responding to queries for sensitive website IP addresses such as banks with incorrect information that, when used by unsuspecting users, can lead to the capture of user credentials.

There is a way to prevent all of this, however, by implementing a feature called *DHCP*

snooping. This feature works by filtering the DHCP messages sent by the rogue DHCP server so that they are never received by the unsuspecting hosts. It also uses the messages sent to and from the legitimate DHCP server to build a binding database that maps the MAC addresses of hosts to the IP addresses they received from the legitimate DHCP server.

DHCP snooping is implemented on the switches in the network, so it is a layer 2 solution. The switch ports on the switch are labeled either trusted or untrusted. Trusted ports are those that will allow a DHCP message to traverse. The only access ports on the switch that should be labeled as trusted are those leading to legitimate DHCP servers.

All interswitch ports should also be labeled as trusted since they might be used to send the DHCP message from the legitimate server to hosts located on a switch to which the legitimate DHCP server is not committed. All other access ports on the switches should be labeled as untrusted (or left unlabeled, in which case they will be considered untrusted). This prevents a rogue DHCP server connected to one of these ports from responding to the DHCP discover packets sent by the hosts. As a matter of fact, any server response packets (DHCPOFFER, DHCPACK, or DHCPNACK) will be dropped by these interfaces.

Figure 6.1 shows an example of how these ports should be configured in a sample network containing both a legitimate and rogue DHCP server. Notice in this scenario that the legitimate DHCP server is located on the other side of a network of layer 3 switches; therefore, all ports leading from the layer 2 switches toward the legitimate DHCP server are labeled as trusted so that any of these ports can be used for communication by the legitimate DHCP server. Also notice that all access ports on the two layer 2 switches have been left unlabeled, which makes them untrusted. This prevents the rogue DHCP server from responding to any DHCP discover packets.

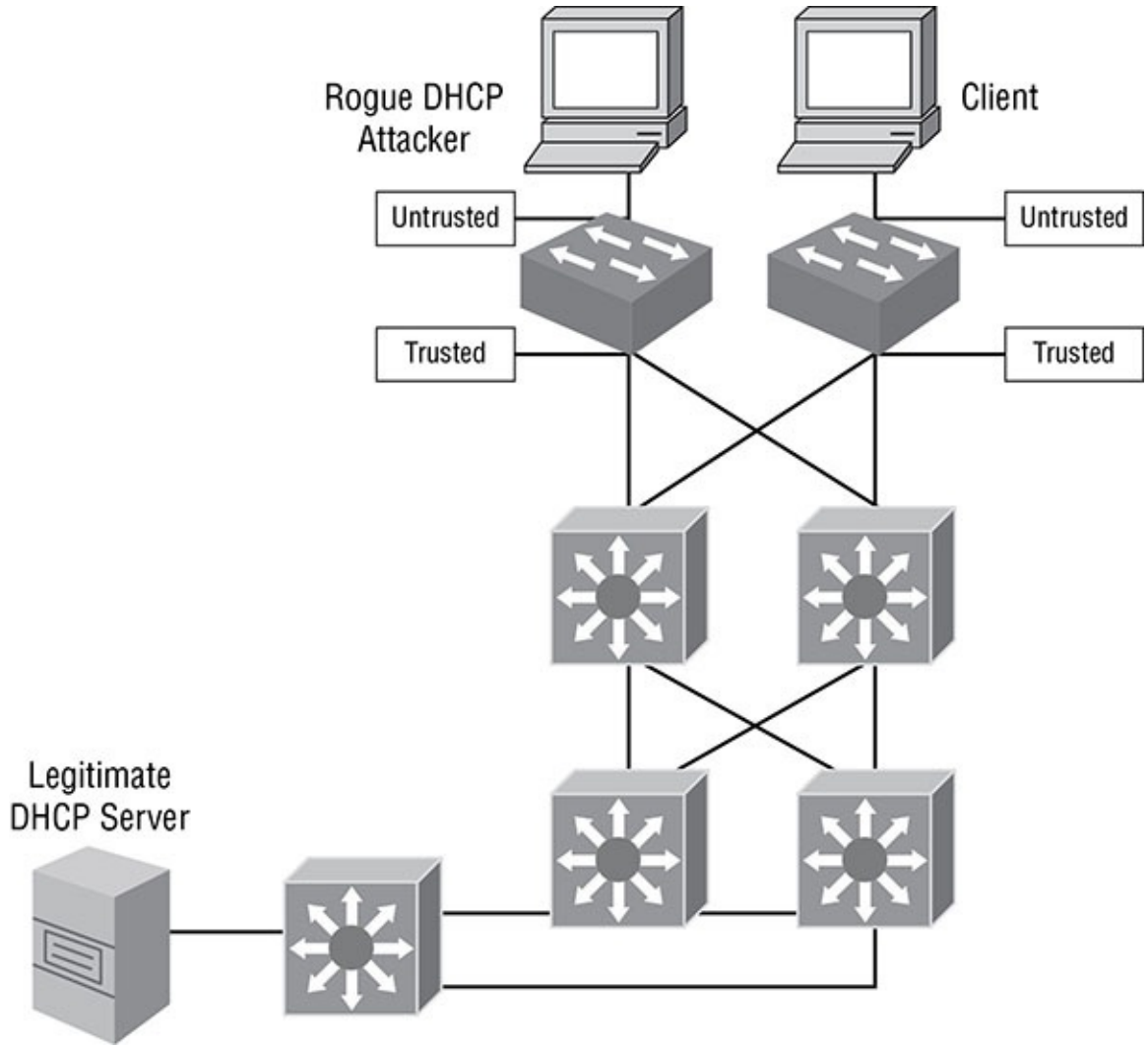

FIGURE 6.1 DHCP snooping

From a high level, the steps that are required to implement DHCP snooping are as follows:

1. Enable DHCP snooping globally on each switch.
2. Enable DHCP snooping explicitly for each VLAN with members on the switch.
3. Label all access ports that connect to legitimate DHCP servers as trusted.
4. Leave all other access ports unlabeled, which makes them untrusted.
5. Label any interswitch ports as trusted.

An optional step you may want to take is to specify a file in flash memory to hold the DHCP snooping database that is created by "snooping" on legitimate DHCP server traffic. In the absence of doing this, the database will be stored in RAM. So, if you want the database to persist through a switch reload, configure a file in flash for this purpose.

Let's go over each of these steps using Figure 6.1 as our guide. First let's enable DHCP snooping globally on the layer 2 switches. I'll call them SW67 and SW68.

```
SW67(config)#ip dhcp snooping
SW68(config)#ip dhcp snooping
```

This is not indicated on the diagram, but let's assume you have four VLANs, VLANs 2–5, on the two switches. Now let's explicitly enable DHCP snooping on those VLANs.

```
SW67(config)#ip dhcp snooping vlan 2-5
SW68(config)#ip dhcp snooping vlan 2-5
```

There are no access ports on the two layer 2 switches that contain legitimate DHCP servers, so you can leave them all unlabeled, which will make them untrusted by default. However, you will need to mark all four of the interfaces leading from the layer 2 switches to the layer 3 switches as trusted. While not labeled on the diagram, let's identify this as `gi0/1` and `gi0/2` on SW67 and `gi0/3` and `gi0/4` on SW68.

```
SW67(config)#int gi0/1 - 2
SW67(config-if-range)#ip dhcp snooping trust

SW68(config)#int gi0/3 - 4
SW68(config-if-range)#ip dhcp snooping trust
```

Finally, just to see how it's done, let's configure a file in flash for the DHCP snooping database. Then if the switches reload for some reason, they will retain this database. Call the file `mysnooper` on both devices.

```
SW67(config)#ip dhcp snooping database flash:/mysnooper
SW68(config)#ip dhcp snooping database flash:/mysnooper
```

In the next section, I'll show you an additional use for the DHCP snooping database. Stay tuned!

Configuring Dynamic ARP Inspection

As you learned in Chapter 5, ARP attacks are targeted at the ARP cache that is used by all devices to store recently resolved IP address to MAC address mappings. These mappings become known to the hosts through the ARP broadcast process and stored in the ARP cache for a short period of time to eliminate the need to repeat the ARP broadcast process for every packet in a large stream of packets. Each time an entry in the cache is used, the timer that ages it out of the cache is updated. ARP pollution attacks use gratuitous ARP packets to force incorrect entries into the ARP cache, with the aim of sending traffic to the attacker that should be sent elsewhere.

The attack can be prevented by implementing a feature on the switches called *Dynamic ARP Inspection (DAI)*. This feature requires that DHCP snooping also be enabled because it depends on the DHCP snooping database that is created when DHCP snooping is enabled. When enabled, it allows the switch to intercept ARP packets on ports that you designate as untrusted and will verify that each intercepted packet has a valid MAC to IP address mapping before updating the ARP cache and forwarding the packet. This validation is performed by using the DHCP snooping database.

When properly configured, DAI operates as shown in Figure 6.2 . An attacker sends a

gratuitous ARP message to pollute the ARP cache of the host at 10.1.1.2. When the switch receives this message, it consults the DHCP snooping database, and when discovering that the packet contains an incorrect MAC to IP address mapping, it drops the packet.

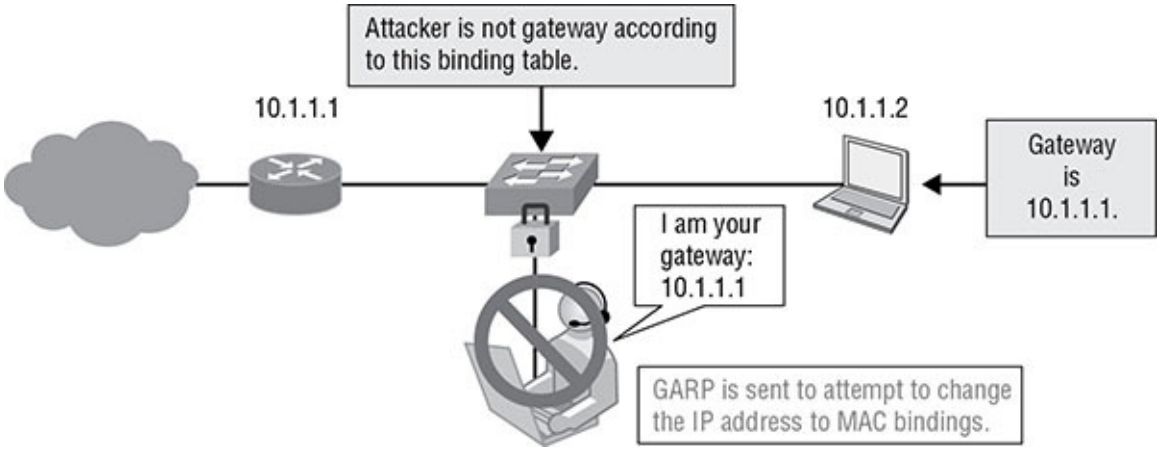

FIGURE 6.2 DAI in action

In the scenario shown in Figure 6.2 , the DAI implementation would require that the ports on the switch connected to the hosts be labeled as untrusted (for the purposes of DAI) and all interswitch ports be labeled as trusted. Bypassing the security check between switches is safe if DAI is enabled on all of the switches because the switches will only be sending packets to one another that have already been checked when received by the switch.

In cases where interfaces with static IP addresses are present (such as default gateways on routers), additional steps are required because those interfaces and their IP to MAC address mappings will not be found in the DHCP snooping database because that's not how those interfaces got their IP addresses. These interfaces will require that you create a type of ACL on the switch called an ARP ACL. This ACL identifies the correct IP to MAC address mapping for the interface, and the ACL is referenced as a filter in the DAI configuration. This makes the ACL available to the DAI process as an addition to the DHCP snooping database.

To enable DAI, the high-level steps are as follows:

1. Enable DAI for each VLAN.
2. Specify interswitch ports as trusted.
3. Leave all other ports to the default of untrusted.
4. For any interfaces such as default gateways that have static IP addresses, create an ARP ACL that maps the IP address of the interface to its MAC address of the interface.
5. Reference any ARP ACLs that have been created when enabling DAI.

Using the diagram in Figure 6.2 , let's perform each step. First let's enable DAI on the switch for VLAN 3.

```
SW69(config)ip arp inspection vlan 3
```

While not shown in the diagram, let's pretend the switch has an uplink called `gi/04`, which

connects to another switch. You need to mark this interface as trusted, so let's do it.

```
SW69(config)#int gi0/4
SW69(config-if)#ip arp inspection trust
```

All other ports need to be labeled untrusted, which is the default, so you can leave them as they are. Since the default gateway on the router has a static IP address of 10.1.1.1, you need to create an ARP ACL that creates the IP to MAC address mapping. Let's do this and use the MAC address aaaa.bbbb.cccc. Its name will be `Static-IP-VLAN3`. Notice that this is an instance where an ACL is used not to allow or block traffic but to identify an item (in this case the IP to MAC address mapping) for special treatment.

```
SW69(config)#arp access-list StaticIP-VLAN3
SW69(config-arp-acl)#permit ip host 10.1.1.1 mac host aaaa.bbbb.cccc
```

The last item you need to take care of is to reference the name of the ARP ACL in the DAI configuration. When you do this, you also have to reference the VLAN to which it applies.

```
SW69(config)#ip arp inspection filter StaticIP-VLAN3 vlan 3
```

While you used the VLAN number in the name of the ACL, that is not what ties it to VLAN. It is the explicit reference to VLAN 3 at the end of the command that does it.

Configuring Port Security

In Chapter 5 you learned how a malicious individual could use a CAM overflow attack to fill the CAM table of the switch, resulting in the switch flooding all traffic out all ports. This basically turns the switch into a hub and thereby allows the attacker to receive all traffic, regardless of the VLAN to which the frame belongs. However, you can prevent this by using a feature called *port security*. This feature can control the following:

- The maximum number of MAC addresses that can be seen on a port (which will solve the *CAM overflow* issue)
- Exactly which MAC addresses can transmit on a port (preventing unauthorized access to the network)

Let's look at how you might prevent a CAM overflow attack by limiting the number of MAC addresses that can be seen on an interface. From a high level, these are the steps required. The commands will follow later.

1. Specify the port as an access port (if not already done).
2. Enable port security on the port.
3. Specify the maximum number of MAC addresses allowed on the port.
4. Specify the action to be taken when a violation occurs.

Let's configure these steps on a Cisco switch. First specify the port `gi0/2` as an access port.

```
SW70(config)#int gi0/2
SW70(config-if)#switchport mode access
```

The next step is to enable port security on the interface. That is done with the following command:

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

To specify the maximum number of MAC addresses that can be seen on the port, use the following command. In this case, you are allowing two because the user has both a PC and an IP phone connected to the same port.

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

Finally, let's specify that if a violation occurs, the port will be shut down. You can also choose the following actions using alternative keywords to the `shutdown` keyword:

- `protect`: The offending frame will be dropped.
- `restrict`: The frame is dropped and an SNMP trap and a syslog message are generated.

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

With this configuration in place, the port will be protected by a CAM overflow attack. If one occurs, the port will be shut down.

Port security can also be used to specify the exact MAC addresses that are allowed on the port. This will prevent an unauthorized device from using the port. You can specify the MAC address (or addresses) manually, or you can use a cool command option called `mac-address sticky` that tells the port to learn the MAC addresses of the devices currently connected to the port and make those MAC addresses the *only* ones allowed on the port. Assuming you have specified the port as an access port and enabled port security on the port, this is easily done with this single command:

```
SW70(config-if)# switchport port-security mac-address sticky
```

With the port configured like this, the port is protected both from unauthorized devices and from CAM overflow attacks.

Configuring STP Security Features

In Chapter 5 you were introduced to an attack aimed at the Spanning Tree Protocol (STP). When a malicious individual introduces a rogue switch to the switching network and the rogue switch has a superior BPDU compared to the one held by the current root bridge, the new switch assumes the position of root bridge.

Since the topology of the switching network depends on the position of the root bridge and the relative position of the other switches to the root bridge, this alters the topology in ways that not only may impact performance but may cause all traffic to traverse the new rogue switch,

which will be under the management of the attacker. To prevent this from occurring, you can make use of three features: BPDU Guard, Root Guard, and Loop Guard. Let's look at all three features.

BPDU Guard

The *BPDU Guard* feature is designed to prevent the reception of superior BPDUs on access ports by preventing the reception of any BPDU frames on the access port. It should be implemented *only* on access ports, because if implemented on trunks, it would interfere with the normal operation of STP, which depends on these frames for its operation. However, it should be implemented on all access ports. When implemented, it has the effect shown in Figure 6.3 . By blocking the superior BPDU sent by the attacker, the STP topology remains unchanged.

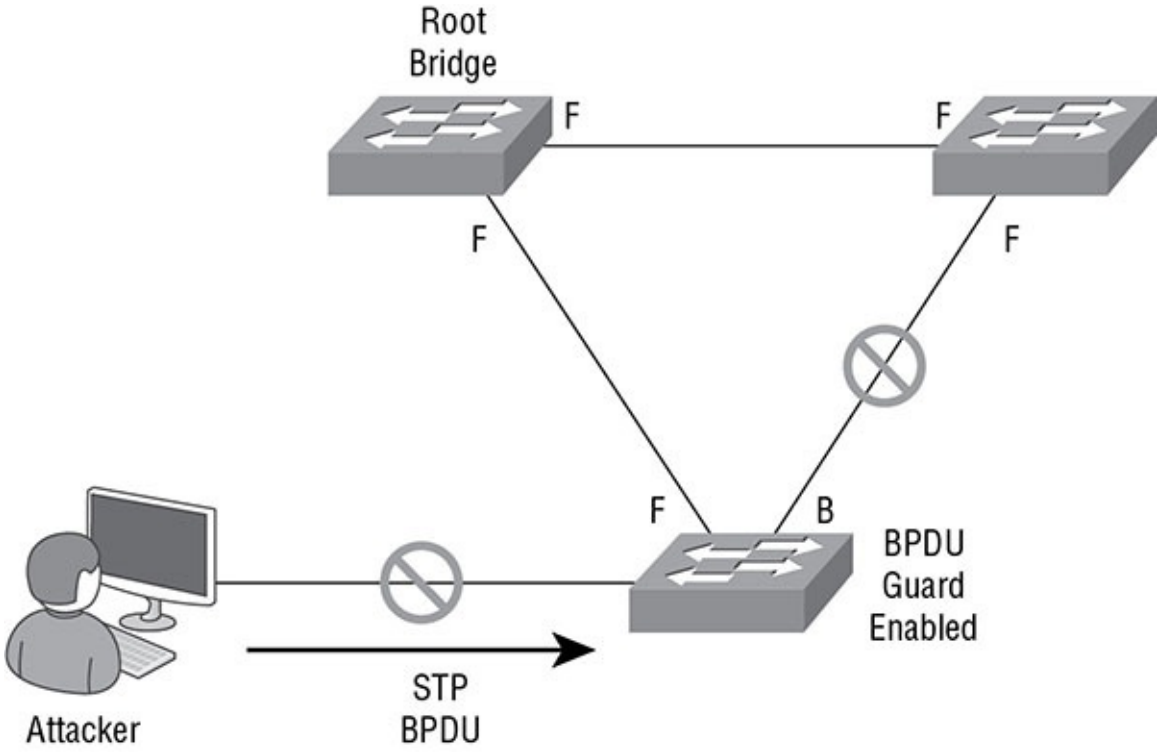

FIGURE 6.3 BPDU Guard in action

The implementation of BPDU Guard can be done at the interface level or it can be done globally, which will implement the feature on all access ports on the switch. Let's implement it first at the interface level. This is done with the following command:

```
SW71(config)#int gi0/5
SW71(config-if)#spanning-tree bpduguard enable
```

To enable this feature on all access ports, execute the following command at the global configuration prompt. You must ensure before you run this command that all access ports are configured with PortFast. This feature allows access ports to immediately proceed to the forwarding state without going through the interim port states of STP as would be done on a trunk port.

The following command will enable both PortFast and BPDU Guard on all access ports:

```
SW71(config)#spanning-tree portfast bpduguard default
```

When a violation occurs, the port will be placed in an err-disabled state and will not pass traffic until it is enabled again manually.

Root Guard

Another feature that is designed to prevent a change in the root bridge is *Root Guard*. This feature is also implemented on access ports. It is implemented on all ports of the root bridge. It prevents the reception of superior BPDUs *only*, not all BPDUs. Moreover, when a violation occurs, the port is not err-disabled as in the case with BPDU Guard. Rather, it is placed in an inconsistent state and will recover and return to a normal state when the reception of superior BPDUs ceases. This feature is implemented only at the interface level, as shown here:

```
SW71(config)#int gi0/5
SW71(config-if)#spanning-tree guard root
```

Loop Guard

An STP loop can be created when a blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The STP Loop Guard feature provides additional protection against layer 2 forwarding loops (STP loops).

To prevent this anomaly from altering the STP topology, use the *Loop Guard* feature. This feature makes additional checks if BPDUs are not received on a nondesignated port. With Loop Guard enabled, that port moves into the STP loop-inconsistent blocking state, instead of the listening/learning/forwarding state. Without the Loop Guard feature, the port assumes the designated port role, moves to the STP forwarding state, and creates a loop.

To enable Loop Guard, use the following command:

```
SW77(config)#interface gigabitEthernet 1/1
SW77(config-if)#spanning-tree guard loop
```

Disabling DTP

In Chapter 5 you learned that a rogue switch added to your network by a malicious individual can alter your STP topology and may even cause the rogue switch to become the root bridge. If *Dynamic Trunking Protocol (DTP)* is enabled on your switch interfaces and if the interface is set to either dynamic desirable or dynamic auto, it is possible for a rogue switch connected to such a configured interface to become part of the STP topology. By setting the port state of the rogue switch to dynamic desirable, a trunk link will automatically be formed.

To prevent this, disable DTP on all switch interfaces. Set the port states of all interfaces to

either trunk or access as required by setting their port states to trunk or access. To disable DTP on all ports, use the following command:

```
SW71(config)#int fa0/1 - 24
SW71(config-if)#switchport nonegotiate
```

Verifying Mitigations

When using the configurations covered in this chapter, it is always a good idea to verify the successful application of each. It is also helpful to know how to check for these configurations when you are unfamiliar with a specific switch. This section will cover these verifications.

DHCP Snooping

To verify the configuration of DHCP snooping, use the `show ip dhcp snooping` command, as shown here. The output is truncated to show the critical parts.

```
SW72#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1-200
Insertion of option 82 is enabled
Interface              Trusted         Rate limit (pps)
————————               ———               ——————
FastEthernet0/1         yes                unlimited
SW72#
```

Note the following:

- DHCP snooping is globally enabled.
- It is operational on VLANs 1–200.
- FastEthernet 0/1 is the trusted interface.

DAI

To verify the configuration of DAI, use the `show ip arp inspection` command, as shown here:

```
Switch73# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan     Configuration    Operation   ACL Match          Static ACL
----     -------------    ---------   ---------          ----------

   10     Enabled          Active

Vlan     ACL Logging      DHCP Logging      Probe Logging
```

```
----     -----------      ------------      -------------

   10     Deny             Deny               Off

Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
----      ---------        -------     ----------      ---------
   10               0               10          10               0

Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
----   ------------    -----------  -------------   -------------------

   10              0              0              0                     0

Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
----   -----------------   ----------------------   ---------------------
   10                   0                        0                      0
```

Note the following:

- It is enabled for VLAN 10.
- Ten packets have been dropped by DAI.

Port Security

To verify the configuration of port security, use the `show port security` command, as shown here:

```
SW74# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
               (Count)    (Count)    (Count)
-------------------------------------------------------------------------

     Fa5/1           11            11            0            Shutdown
     Fa5/5           15            5             0            Restrict
     Fa5/11          5             4             0            Protect
-------------------------------------------------------------------------



Total Addresses in System: 21
Max Addresses limit in System: 128
```

Note the following:

- Ports security is enabled on the Fa5/1, Fa5/5, and Fa5/11 interfaces.
- There have been no violations thus far.
- If a violation occurs, the fa5/1 interface will not forward the offending traffic, will shut down, will send an SNMP trap and syslog message, and will increment the violation counter.
- If a violation occurs, the fa5/5 interface will not forward the offending traffic, will send an

SNMP trap and syslog message, and will increment the violation counter, but it will still pass legitimate traffic.

- If a violation occurs, the fa5/5 interface will not forward the offending traffic, will *not* send an SNMP trap or syslog message, and will *not* increment the violation counter, but it will still pass legitimate traffic.

STP Features

In this section, you'll learn how to verify the proper application of BPDU Guard, Root Guard, Loop Guard, and DTP.

BPDU Guard

To verify that BPDU Guard has been configured correctly, execute the `show spanning-tree summary totals` command. Note that PortFast BPDU Guard is enabled globally on this switch.

```
SW75# show spanning-tree summary totals
Root bridge for: none. PortFast BPDU Guard is enabled

UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------

  1 VLAN                    0         0         0         1          1
```

Root Guard

To verify that Root Guard has been configured correctly, execute the `show spanning-tree interface <int id > detail` command. Note that Root Guard is enabled on this port.

```
SW76#show spanning-tree int fa0/22 detail
 Port 24 (FastEthernet0/22) of VLAN0001 is broken (Root Inconsistent)
   Port path cost 19, Port priority 128, Port Identifier 128.24.
   Designated root has priority 4097, address 000d.bc51.6d00
   Designated bridge has priority 24577, address 0018.1820.2700
   Designated port id is 128.24, designated path cost 57
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 2
   Link type is point-to-point by default
   Root guard is enabled on the port

   BPDU: sent 502, received 1701
```

Loop Guard

To verify that Loop Guard has been configured correctly, execute the `show spanning-tree`

`summary` command. Note that Loop Guard is enabled.

```
Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled Loopguard Default            is
enabled

UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------

Total                         0         0        0          0          0
```

DTP

To verify that Dynamic Trunking Protocol has been properly disabled, execute the `show interfaces switchport` command, as shown here:

```
SW1#show interfaces fastEthernet 0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native Negotiation of Trunking: Off
```

Note the following:

- DTP negotiation is disabled (see the last line).
- This is an access port.

Summary

In this chapter, you learned to configure DHCP snooping to prevent the introduction of rogue DHCP servers. The chapter also discussed how, when combined with DHCP snooping, DAI can prevent ARP poisoning attacks. You learned how to prevent MAC overflow attacks and learned about how unauthorized devices can switch ports by using port security. Finally, the chapter discussed BPDU Guard, Root Guard, and Loop Guard, all STP features designed to prevent changes to the STP topology.

Exam Essentials

Implement DHCP snooping. Configure and verify DHCP snooping to prevent the issues caused by a rogue DHCP server and to support the application of Dynamic ARP Inspection.

Deploy DAI. Implement Dynamic ARP Inspection to prevent ARP pollution, which can lead to a man-in-the-middle attack.

Configure port security. Prevent MAC overflow attacks and the introduction of unauthorized devices to switch ports by securing the port using the port security feature.

Describe the benefits of STP security features. These features include BPDU Guard, Root Guard, and Loop Guard.

Review Questions

1. Which of the following is true of DHCP snooping?
   A. It prevents the introduction of rogue switches.
   B. It is implemented on routers.
   C. It builds a binding database that maps the MAC addresses of hosts to the IP addresses they received from the legitimate DHCP server.
   D. When implementing it, all ports should be untrusted.
2. Which DHCP packet types are dropped on untrusted interfaces protected by DHCP snooping?
   A. DHCPACK
   B. DHCPOFFER
   C. DHCPNACK
   D. All of the above
3. Which of the following features must be configured for the operation of DAI?
   A. Loop Guard
   B. DHCP snooping
   C. Root Guard
   D. BPDU Guard
4. What is required to enable DAI on an interface with a static IP address?
   A. An ACL
   B. Loop Guard
   C. PortFast
   D. Root Guard

5. Which of the following commands causes the switch to drop the offending traffic when a violation occurs but neither shuts down the interface nor sends syslog messages?

   A. `switchport port-security violation shutdown`

   B. `switchport port-security violation restrict`

   C. `switchport port-security violation deny`

   D. `switchport port-security violation protect`

6. Which attack does the `switchport port-security maximum 2` command prevent?

   A. MAC spoofing

   B. CAM overflow

   C. Rogue DHCP

   D. ARP spoofing

7. Which of the following should be implemented only on access ports?

   A. BPDU Guard

   B. Root Guard

   C. Loop Guard

   D. DTP

8. Which type of traffic is prevented on ports where Root Guard is enabled?

   A. All traffic

   B. All BPDUs

   C. Superior BPDUs

   D. Inferior BPDUs

9. What state does a port configured with Loop Guard enter when the reception of BPDUs stops?

   A. Shutdown

   B. Loop-inconsistent

   C. Err-disabled

   D. Blocking

10. Which feature is disabled with the command `switchport nonegotiate`?

    A. STP

    B. DTP

    C. VTP

D. CDP

11. In the following configuration, which port will not forward the offending traffic, will *not* send an SNMP trap or syslog message, and will *not* increment the violation counter but will still pass legitimate traffic?

```
SW74# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                 (Count)     (Count)      (Count)

    Fa5/1           11           11           0           Shutdown
    Fa5/5           15            5           0           Restrict
    Fa5/11           5            4           0           Protect
    Fa5/12           3            2           0           Shutdown
-----------------------------------------------------------------------


Total Addresses in System: 21
Max Addresses limit in System: 128
```

A. Fa5/1

B. Fa5/5

C. Fa5/11

D. Fa5/12

12. Which of the following features prevents the introduction of a rogue switch?

A. BPDU Guard

B. DAI

C. DHCP snooping

D. Loop Guard

13. Which command should be configured on a port where the legitimate DHCP server resides?

A. `ip dhcp snooping trust`

B. `ip dhcp snooping enable`

C. `ip dhcp snooping`

D. `ip dhcp snooping untrust`

14. What is the purpose of the command `ip dhcp snooping database flash:/mysnooper`?

A. The switch will retain the database through a reboot.

B. The switch will share the database with directly connected switches.

C. The switch will apply the database to all VLANs.

D. The switch will delete the file during a reboot.

15. What is the default state of a port with respect to DAI?
    A. Trusted
    B. Untrusted
    C. Null
    D. Nonegotiate
16. In the following command, what is the name of the ACL?

```
SW69(config)#ip arp inspection filter StaticIP-VLAN3 vlan 3
```

    A. vlan 3
    B. 3
    C. StaticIP-VLAN3
    D. filter StaticIP
17. Which command enables port security on an interface?
    A. `switchport port-security`
    B. `switchport port-security maximum 2`
    C. `switchport port-security violation shutdown`
    D. `switchport port-security mac-address sticky`
18. Which of the following is not a mitigation to STP attacks?
    A. Root Guard
    B. BPDU Guard
    C. Disabling DTP
    D. DAI
19. When a violation occurs on a BPDU Guard–enabled port, in what state is the port placed?
    A. Shutdown
    B. Port inconsistent
    C. Err-disabled
    D. Restrict
20. Which ports should have DTP disabled?
    A. Access ports
    B. Trunk ports

C. Etherchannels

D. All ports

Chapter 7
VLAN Security

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **4.6 VLAN security**
  - Describe the security implications of a PVLAN
  - Describe the security implications of a native VLAN

VLANs can be used to segment a LAN and can span multiple switches, providing both security and the ability to locate users in the same VLAN in physically dispersed locations. There are security issues with VLANs, as you learned in Chapter 5. This chapter will expand your knowledge of VLAN issues by introducing private VLANs (PVLANs) and the security implications of deploying them. I will also talk about security issues with native VLANs. I'll wrap up the chapter by introducing how to use access lists on switches.

In this chapter, you will learn the following:

Security implications of a PVLAN

Security implications of a native VLAN

Switch ACLs

Native VLANs

In Chapter 5 you learned about double tagging and how an attacker can craft a packet with two 802.1q tags with the inner tag set to the VLAN to which he would like to send traffic. This attack takes advantage of the native VLAN. If the attacker's access port is set to the same VLAN as the native VLAN, this attack becomes possible.

Mitigation

The solution is to set the native VLAN (number 1 by default) to one in which *none* of the access ports resides. This is done only on the trunk ports. To change the native VLAN of the trunk port `gi 0/1` to 78, use the following command:

```
Switch79(config)#int gi 0/1
Switch79(config-if)#switchport trunk native vlan 78
```

After changing the native VLAN from 1 to 78, simply ensure that no access ports are members of VLAN 78.

PVLANs

When hosts are segregated into VLANs, they are also placed into separate IP subnets. Service providers often find this arrangement to be problematic, especially when there is need for additional security across a VLAN being shared by multiple customers and perhaps by the ISP servers themselves. While a separate VLAN for each customer is an option, it presents the following challenges:

- The requirement of a high number of interfaces on service provider devices to support the subnets
- The increased management complexity of dividing the network address space and the potential wasting of address space
- The management of multiple ACLs to maintain security across the VLANs

A feature that can be a solution in these cases is the implementation of *private VLANs*. These provide separation within a VLAN at layer 2, while still leaving all members of the original VLAN (called the primary VLAN) in the same subnet. Communication between ports in the primary VLAN is controlled not with ACLs but with the proper assignment of one of three port types.

Promiscuous ports These are ports that can communicate with a port of any other type. Typical candidates for this port assignment are those ports leading to the router or firewall that act as the default gateway for the primary VLAN.

Isolated portsThese are ports that *only* communicate with a promiscuous port. These ports are used to isolate a single host from all other hosts in the primary VLAN. Since these ports can only communicate with promiscuous ports, the only way another host can communicate with an isolated port is through the router, where an ACL might be applied for control.

Community ports These are ports that can communicate with other members of the same community and with promiscuous ports. Therefore, hosts connected to community ports can communicate with other communities and with isolated ports *only* through the router.

Figure 7.1 shows an example of a primary VLAN that has been divided into PVLANs. In this example, keep in mind that all hosts connected to the switch are in the same primary VLAN and the same IP subnet. Port `Ge0/1` is a promiscuous port, while the ports leading to SRV1 and SRV2 are community ports that are members of PVLAN 101. Notice they can communicate with one another and with the default gateway since it is a promiscuous port.

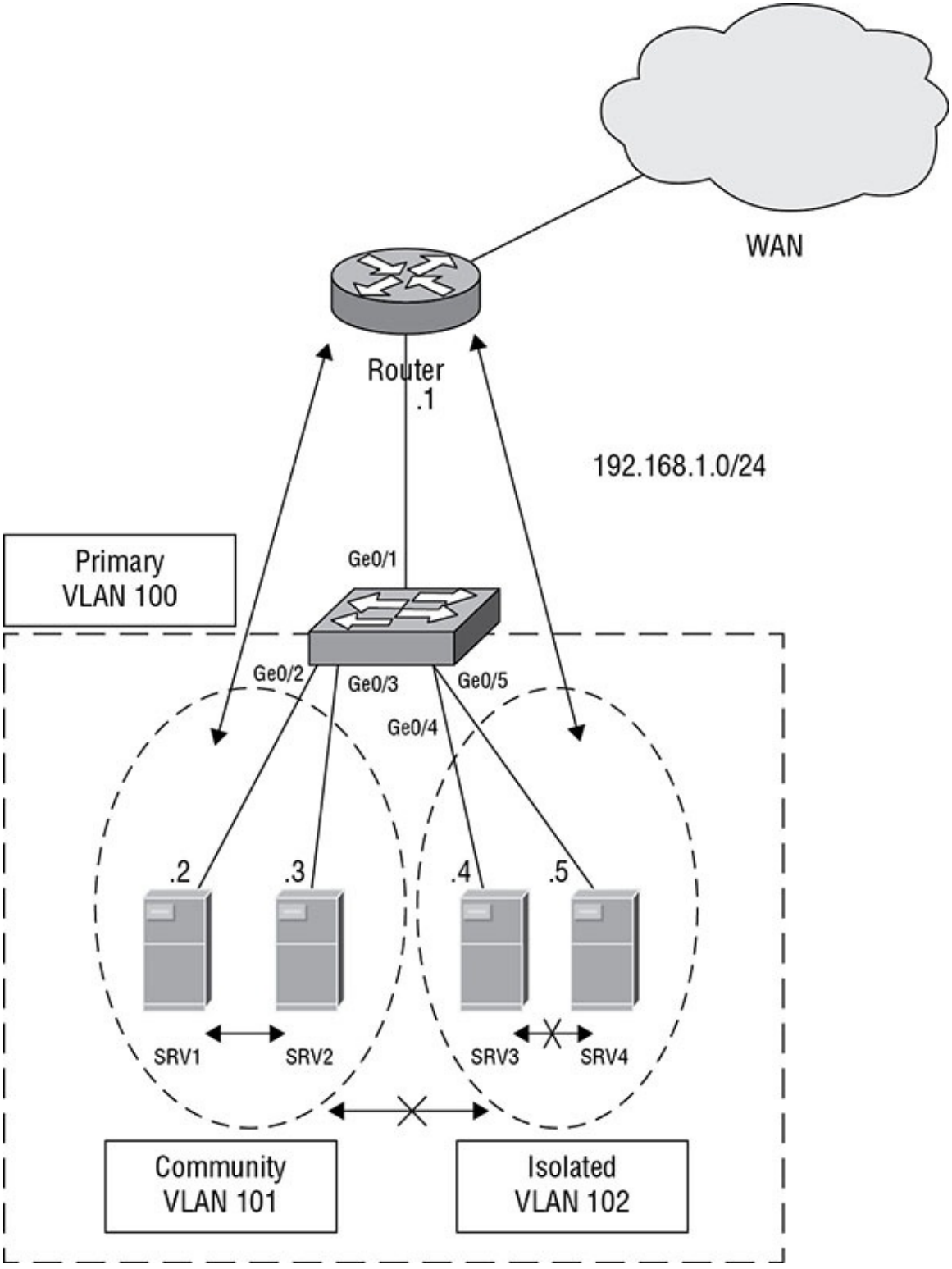

FIGURE 7.1 PVLANs

Also notice that the ports leading to SRV3 and SRV4 are isolated ports that are members of PVLAN 102. Notice that even though SRV3 and SRV4 reside in the same primary VLAN and the same secondary VLAN (102), they cannot communicate with one another because isolated ports can *only* communicate with the promiscuous port, which in this case is the default gateway.

To set up PVLANs, the steps include the following:

1. Configure the *primary VLAN*, specifying it as a primary PVLAN.
2. Configure any required secondary PVLANs, specifying the type.
3. Specify each interface as a private VLAN host port and associate it with a private VLAN pair.

The following are the steps to configure VLAN 10 as a primary VLAN, VLAN 201 as an isolated VLAN, and VLANs 202 and 203 as community VLANs; to associate them in a private VLAN; and to verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 203
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan association 201-203
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- -----------------
----------------------------------------

10      201       isolated
10      202       community
10      203       community
10      204       non-operational
```

Notice that the last command, `private-vlan association 201-203`, executed under the VLAN 10 configuration is what ties the PVLANs to the primary VLAN.

To set a port to its proper type and PVLAN, use this command:

```
Switch# configure terminal
Switch(config)# interface gigatibethernet0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 10 202
Switch(config-if)# end
```

In the previous configuration, port `Gi0/22` was assigned to primary VLAN 10 and PVLAN 202. Since PVLAN 202 was created as a community VLAN, port `Gi0/22` will be a community port.

PVLAN Edge

In some cases, you may find there is no reason for any communication between ports connected to the same switch. When that is the case, it may be beneficial to take advantage of another feature called the *PVLAN Edge* feature. Preventing communications between ports when possible can both prevent attacks such as ARP poisoning attacks and impair the ability of a hacker to move from a compromised host to other hosts.

When a port has been designated as a PVLAN Edge port (called a *protected port*), it has the following features:

- No traffic will be sent from one protected port to another protected port on the same switch. Any data traffic must go through the router first.
- Forwarding behavior between a protected port and unprotected ports proceeds as usual.
- There is no isolation between protected ports located on different switches.

While PVLAN Edge is only effective between ports on the same switch, it is simpler to configure than PVLANs and can be the solution in certain cases. To specify a port as "protected," use the following command:

```
Switch(config)#interface fa0/1
Switch(config-if-range)#switchport protected
```

PVLAN Proxy Attack

As with many features, malicious individuals have figured out a way to attack PVLAN configurations. In a *PVLAN proxy attack*, an attacker sends a packet (using the promiscuous port) with the source IP and MAC address of the attacker, a destination IP address of the target, and the MAC address of the router. When the router receives the packet, the router rewrites the destination MAC address to that of the target and sends the packet to the target. It is the presence of the MAC address of the router in the packet, rather than that of the target, that causes this to be possible. This causes the packet to be coming from the router, which is allowed since the router is on a promiscuous port. Since the router is being used as the source MAC, the router is considered a "proxy." Figure 7.2 shows the attack.

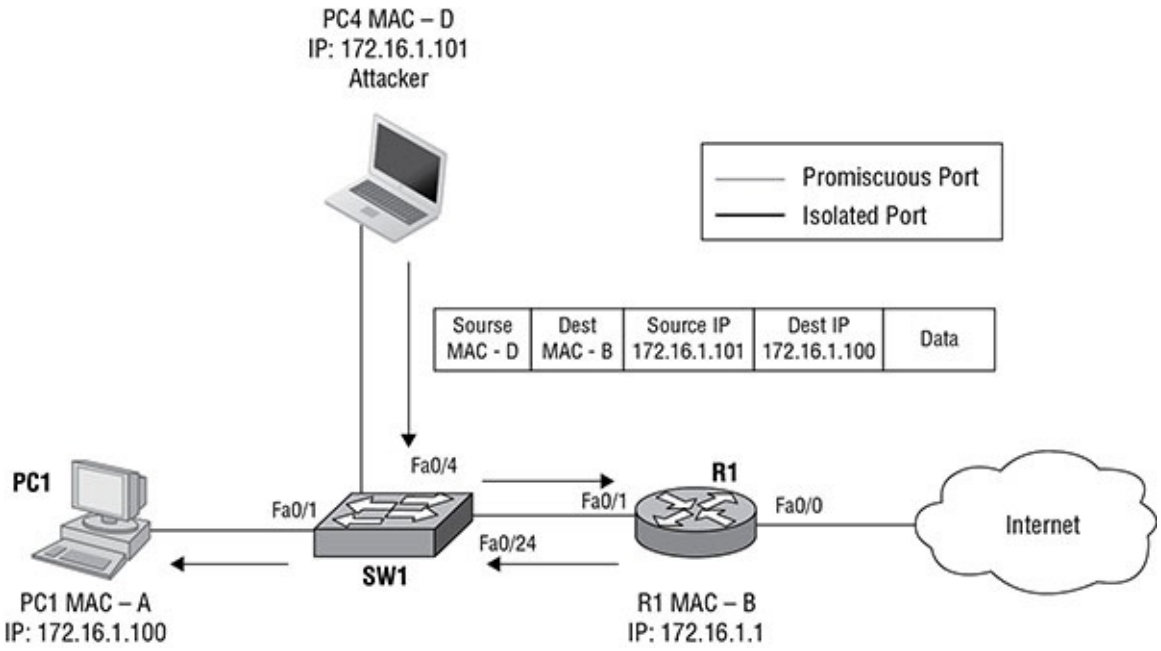

FIGURE 7.2 PVLAN proxy attack

Mitigation

To prevent PVLAN proxy attacks, implement ACLs on the router interface that deny traffic from the local subnet to the local subnet. An example of such an access list, applied to the router interface, would solve the issue shown in Figure 7.2 .

```
Router(config)#access-list 101 deny ip 172.16.0.0 0.0.255.255 172.16.0.0
0.0.255.255
Router(config)#access-list 101 permit ip any any
Router(config)#int fa0/1
Router(config)#ip access-group 101 in
```

ACLs on Switches

Access lists can be applied not only to router interfaces but can also be used on layer 2 interfaces on switches. When used on switches, there are three types of access lists that can be used.

Port access lists (PACLs) These are applied to layer 2 interfaces either on a layer 2 switch or on a multilayer switch. When applied to a layer 2 interface on a multilayer switch, they can be applied only inbound. These lists can be either IP ACLs or MAC ACLs.

VLAN access lists (VACLs) These use maps to control traffic on a VLAN. They can be applied either to traffic routed into or out of a VLAN or to all traffic bridged within a VLAN.

Router ACLs Used to control traffic between VLANs, router ACLs can be applied either to a router interface or to a switched virtual interface (SVI) on a multilayer switch.

First let’s look at configuring port ACLs.

Port ACLs

Ports ACLs can be applied either as IP access lists or as MAC access lists. The procedure to create and apply both types is as follows:

```
Switch(config)#ip access-list extended simple-ip-acl
Switch(config-ext-nacl)#permit host 10.0.0.1 any
Switch(config)#int gi0/22
Switch(config-if)#ip access-group simple-ip-acl in

Switch(config)#mac access-list extended simple-mac-acl
Switch(config-ext-nacl)#permit host 0000.aaaa.bbbb any
Switch(config)#int gi0/22
Switch(config-if)#mac access-group simple-ip-acl in
```

VLAN ACLs

VLAN access lists apply to all traffic in a VLAN and are not configured with a direction. These access lists use maps to define both the traffic in question and the action to be taken. The maps can reference other access lists when specifying these values. From a high level, the steps to set up a VACL are as follows:

1. Create an ACL that defines the specified traffic type.
2. Create a map that references the access list and specifies an action.
3. Apply the access map to the appropriate VLAN.

Here is the creation of an access list defining the traffic as HTTPS (port 443):

```
Switch(config)ip access-list extended permit_HTTPS
Switch(config-ext-nacl)#permit tcp any any eq 443
```

The next step is to create the map referencing the ACL and specifying an action:

```
Switch(config)#vlan access-map Allow_HTTPS
Switch(config-access-map)#match ip address permit_HTTPS
Switch(config-access-map)#action forward
```

Finally, here is the command to apply the access map to a VLAN, in this case VLAN 403:

```
Switch(config)#vlan filter Allow_HTTPS vlan-list 403
```

Note that you use a VLAN list to specify the VLANs to which the map applies, even when the list consists of only one VLAN.

Summary

In this chapter, you learned about preventing VLAN hopping attacks that take advantage of the native VLAN. You also looked at how to break up a VLAN into private VLANs. You learned that configuring PVLANs is a matter of setting ports as promiscuous, community, and isolated.

The chapter discussed the PVLAN Edge feature as another way of providing isolation between switch ports. Finally, you learned how to use ACLs to prevent a PVLAN proxy attack.

Exam Essentials

Mitigate native VLAN security issues. Prevent VLAN hopping attacks that use double tagging by setting the native VLAN number to one in which *none* of the access ports reside.

Describe the benefits of PVLANs. These include the ability to segregate within a primary VLAN, while saving IP address space, decreasing management complexity, and reducing the need for multiple ACLs to maintain security across the VLANs.

Identify the port types used in PVLANs. These include promiscuous, community, and isolated ports. They allow for grouping devices with a VLAN (community), for isolating devices within a VLAN (isolated), and for providing access to all devices back to the router (promiscuous).

Explain the functionality of the PVLAN Edge feature. This feature is used to provide isolation between protected ports located on the same switch.

Mitigate a PVLAN proxy attack. To prevent PVLAN proxy attacks, implement ACLs on the router interface that deny traffic from the local subnet to the local subnet.

Review Questions

1. Which of the following attacks takes advantage of the native VLAN?
   A. Double tagging
   B. ARP poisoning
   C. Buffer overflow
   D. PVLAN proxy
2. How should the native VLAN be configured to thwart a double tagging attack?
   A. It should be disabled.
   B. It should be the same VLAN number where hosts reside.
   C. It should be the same as the management VLAN.
   D. It should be set to a VLAN number in which *none* of the access ports reside.
3. Which of the following is *not* true about service providers providing a separate VLAN per customer?
   A. It requires a high number of interfaces on service provider devices to support the subnets.

B. It increases management complexity of dividing the network address space and the potential wasting of address space.

C. Multiple ACLs must be managed to maintain security across the VLANs.

D. It decreases security.

4. What feature allows for providing layer 2 separation within a VLAN?

A. PVLANs

B. Loop Guard

C. DAI

D. Root Guard

5. Which of the following commands changes the native VLAN from 1 to 78?

A. `switchport trunk native vlan 78`

B. `switchport native vlan 78`

C. `switchport native vlan trunk 78`

D. `switchport vlan 78`

6. Which type of PVLAN port can communicate with a port of any other type?

A. Promiscuous

B. Isolated

C. Community

D. Private

7. Which of the following is *not* a step in setting up PVLANs?

A. Configuring the primary VLAN, specifying it as a primary PVLAN

B. Specifying each interface as a private VLAN host port and associating it with a private VLAN pair

C. Configuring any required secondary PVLANs, specifying the type

D. Setting the native VLAN number to one in which *none* of the access ports resides

8. Which of the following commands configures the primary PVLAN?

A. `primary-vlan primary`

B. `private-vlan private`

C. `private-vlan primary`

D. `vlan primary`

9. To what port state should the default gateway port be set?

A. Promiscuous

B. Isolated

C. Community

D. Private

10. Which command associates two private VLANs with the primary VLAN?

A. `vlan association 501-503`

B. `private-vlan 501-503`

C. `private-vlan association 501-503`

D. `private-vlan 501-503 associate`

11. Which command sets a port as a PVLAN port?

A. `switchport mode private-vlan host`

B. `switchport private-vlan host-association 10 202`

C. `switchport host-association 10 202`

D. `switchport mode host-association 10 202`

12. Which of the following commands assigns a PVLAN port to its PVLAN?

A. `switchport mode private-vlan host`

B. `switchport private-vlan host-association 10 202`

C. `switchport host-association 10 202`

D. `switchport mode host-association 10 202`

13. Which type of attack can be prevented by the PVLAN Edge feature?

A. Double tagging

B. ARP poisoning

C. Buffer overflow

D. PVLAN proxy

14. What is the purpose of the following set of commands?

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan association 501
```

A. Ties the PVLAN 10 to the primary VLAN 501

B. Ties the PVLAN 501 to the PVLAN 10

C. Ties PVLAN 501 to the primary VLAN 10

D. Ties the PVLAN 10 to the secondary VLAN 501

15. What statement is false about the PVLAN Edge feature?

A. No traffic will be sent from one protected port to another protected port on the same switch.

B. Forwarding behavior between a protected port and unprotected ports proceeds as usual.

C. There is no isolation between protected ports located on different switches.

D. Forwarding between a protected port and unprotected ports is not permitted.

16. What is a port protected by the PVLAN Edge feature called?

A. Isolated

B. Protected

C. Hidden

D. Promiscuous

17. Which command specifies a port as PVLAN Edge?

A. `switchport protected`

B. `switchport edge`

C. `switchport security edge`

D. `switchport protected edge`

18. Which of the following describes a packet sent by an attacker attempting the PVLAN proxy attack?

A. It contains a source IP and MAC address of the attacker, a destination IP address of the target, and a destination MAC address of the router.

B. It contains a source MAC address of the attacker and source IP address of the target, a destination IP address of the target, and the IP address and MAC address of the router.

C. It contains a source IP address of the attacker and source MAC address of the target, a destination IP address of the target, and the MAC address of the router.

D. It contains a source IP and MAC address of the attacker, a destination IP address of the target, and the MAC address of the router.

19. In a PVLAN proxy attack, which device is acting as the proxy?

A. The target

B. The attacker

C. The router

D. The switch

20. How are VLAN proxy attacks prevented?

A. Implement ACLs on the router interface that allow traffic from the local subnet to the local subnet

B. Implement ACLs on the router interface that deny traffic from remote subnets to the local subnet

C. Implement ACLs on the router interface that deny traffic from the local subnet to remote subnets

D. Implement ACLs on the router interface that deny traffic from the local subnet to the local subnet

Chapter 8
Securing Management Traffic

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.1 Secure management**
  - Compare in-band and out-of-band
  - Configure secure network management
  - Configure and verify secure access through SNMP v3 using an ACL
  - Configure and verify security for NTP
  - Use SCP for file transfer

Controlling access to the management interface of a router or switch is critical to ensuring that there is no unauthorized access that can introduce malicious changes to the configuration of the device. Moreover, when network management and time synchronization protocols such as SMTP and NTP are in use, access to this information must be secured. Finally, as a technician, you should use secure protocols when performing file transfers. This chapter will cover all of these secure management topics.

In this chapter, you will learn the following:

Comparing in-band and out-of-band

Configuring secure network management

Configuring and verifying secure access through SNMP v3 using an ACL

Configuring and verifying security for NTP

Using SCP for file transfer

In-Band and Out-of-Band Management

Many options are available to connect to a Cisco device for managing the device. Methods can be classified as either in-band or out-of-band. An *in-band* connection is one that uses the network as its transmission medium. In-band connection types include SNMP, virtual terminal (VTY), and HTTPS connections. *Out-of-band* connections include the console port and the

AUX port, both physical connections that do not use the network as the transmission medium. It is good practice to have both in-band and out-of-band methods available for redundancy.

AUX Port

The AUX port comprises a direct serial connection to the device and is considered an out-of-band method of managing the device. One option is to connect a modem to the AUX port and dial into the modem when access to the CLI is required and when network access is not available. To set up the AUX port for this and to also set a password for the AUX port, you need to know the line number used by the AUX port. This can be determined with the `show line` command, as shown here:

```
R1#show line
   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                  -    -      -    -     -     0       0     0/0
-
    65 AUX  9600/9600  -    -      -    -    -     0     1      0/0
-
    66 VTY                 -    -      -    -     -     0       0     0/0
-
    67 VTY                 -    -      -    -     -     0       0     0/0
-
```

In the previous output, the AUX port is using line 65, which you will need to reference in the following set of commands, which set the AUX port to use a modem with a speed of 1115200. The commands also set the flow control to hardware and set the password to `cisco`. Don't forget the `login` command, which is the command that specifies asking for a password at connection time!

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
```

VTY Ports

The virtual terminal (VTY) ports are considered an in-band method as these connections use the network as the transmission medium. These ports can use several protocols, among them Telnet and SSH. While you will learn later in the chapter to configure the secure alternative to clear-text Telnet, here I will cover securing the lines with passwords and adding physical redundancy to the connections by setting a loopback address. When a loopback address is configured and used as the management IP address, *any* physical interface on the device can accept the connection attempt if the loopback address is included in dynamic routing advertisements or advertised via a static route. When management access is tied to a physical

IP address, the device will be unreachable when that physical interface is down.

To configure a loopback address for management, use the following command:

```
R1(config)# int loopback0
R1(config-if)#ip address 192.168.5.5 255.255.255.0
R1(config-if)#no shut
```

To include the IP address in EIGRP or OSPF routing advertisements, use the following commands. This will ensure that you can reach this address from a remote network.

```
R1(config)#router eigrp 10
R1(config-rtr)#network 192.168.5.0 0.255.255.255
R1(config)#router ospf 1
R1(config-rtr)#network 192.168.5.0 0.255.255.255
```

Before setting a password on the VTY lines, you should determine how many of these lines exist on the device (which varies) so that you secure them all. Use this command to learn the number of VTY lines:

```
R1(config)#line vty ?
R1(c0nfig)#line vty <0 15>
```

Now you know there are 16 lines on this device, so refer to 16 lines when you execute any command designed to apply to all VTY lines. To set a password on the VTY lines, use the following set of commands:

```
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
```

HTTPS Connection

Many Cisco devices offer the option of managing the device from a GUI interface. This would be considered an in-band connection as it uses the network. While the initial configuration must be completed at the CLI, once an interface has been assigned an IP address and is functional and the HTTP or HTTPS server has been enabled, these devices can be managed using this interface. While the HTTP server is certainly functional, when managing the device, you should always use a secure connection as provided with HTTPS.

Later in this chapter, you will learn how to configure HTTPS.

SNMP

Another option for configuration management is SNMP. As with other methods that use the network as a transmission medium, it is also considered an in-band method. SMTP stores the settings in a MIB. This is a repository with a hierarchical structure with standardized locations for each piece of configuration or status information. These locations and their associated data are called OIDs. The OID number describes the path through the tree-like structure where the specific piece of information is located. Figure 8.1 shows a portion of the MIB. An example of

an OID would be 1.3.6.1.2.1.1.5 (system name), which would be one of the subsections of sysDescr (1.3.6.2.1.1).

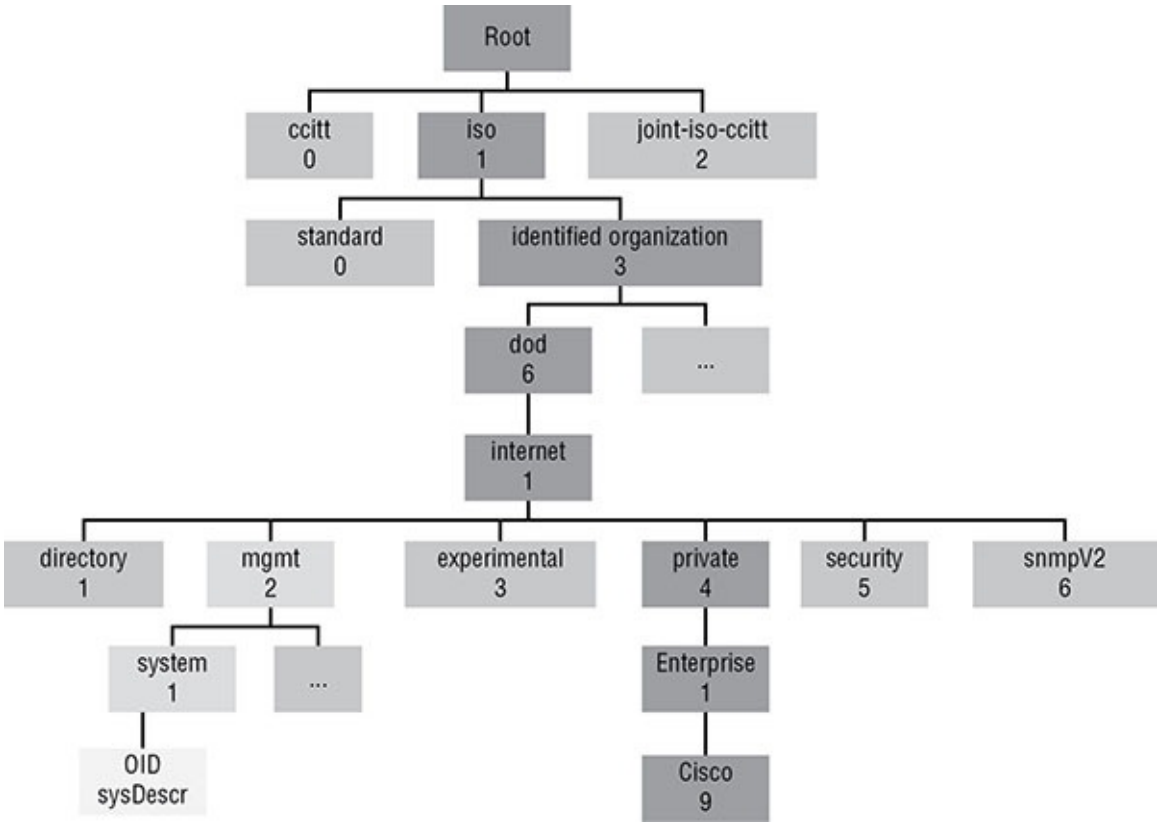

FIGURE 8.1 Partial MIB

Notice also that there is a private branch in the tree where vendors can include settings and status information that might be unique to their products. Therefore, the path to Cisco-specific data is 1.3.6.1.4.1.9. Access to information stored by an individual device is done using `get` or `set` commands, while referencing the OID. `get` commands retrieve information, while `set` commands make configuration changes to IODs that can be changed. SNMP also allows for the creation of traps on devices, which can trigger a message to the management station when a threshold is met or an event occurs. In SMTP version 2, these trap messages are called *informs*.

SNMP has undergone three version changes over the years. Versions 1 and 2 used the knowledge of a community string as the access control mechanism to the MIBs of the devices. As this is quite a flimsy security system, version 3 adopted a user-based security model that provides for authentication, integrity hashing, and encryption of transmissions. These functions can be configured using three modes that represent various combinations of these capabilities.

- *noAuthNoPriv*: No hashing to secure authentication or encryption of data (referenced as `noauth` in the command)
- *AuthNoPriv*: Hashing to secure authentication but no encryption of data (referenced as `auth` in the command)
- *AuthPriv*: Hashing to secure authentication and encryption of data (referenced as `priv` in

the command)

Later in this chapter, you will learn how to configure SNMPv3.

Console Port

The *console port* also comprises a serial connection that is considered an out-of-band connection. Access control can be applied to this interface by using the `line console 0` command. For example, here I have applied a password in this single line and by using the `login` command have specified that the password is required:

```
R83(config)line console 0
R83(config-line)#password cisco
R83(config-line)#login
```

Securing Network Management

Regardless of the interface with which you manage a Cisco device, you should ensure that the method used is secure. In this section, you'll look at securing VTY ports and HTTP connections and using ACLs as a further line of defense in protecting these critical management interfaces. Finally, I'll discuss banner messages and the role they can play in securing management interfaces.

SSH

When accessing a device using the VTY ports, you should always configure and use SSH rather than Telnet for the connection. For more information on configuring SSH, see Chapter 4.

HTTPS

To disable the HTTP server and enable the HTTPS server, execute the following commands:

```
R81(config)#no ip http server
R81(config)#ip https secure-server
R81(config)#copy run start
```

Once these commands are executed, the device will generate an RSA key and will use the key to encrypt all transmissions.

ACLs

An additional layer of security that can be applied to any management interface is the application of ACLs. After the ACL has been created, it can be applied to the VTY, HTTPS, and SNMPv3 processes. For example, consider the following access list that allows access only to and from hosts in the 192.168.5.0/24 network (presumably one that contains only management stations).

```
R84(config)#access-list 99 permit 192.168.5.0 0.0.0.255
```

This ACL can be applied to each of these management interfaces as follows:

- SSH

```
R84(config)#line vty 0 15
R84(config-line)#access-class 99 in
```

- HTTPS

```
R84(config)#ip http access-class 99
```

SNMPv3

To apply ACL 99 at the group level, use this command, which refers to the group `test-group` using the `priv` security policy with write access to a view called `write-view`:

```
R84(config)#snmp-server group test-group v3 priv write write-view access 99
```

To apply ACL 99 at the user level, use the following command, which refers to a user named `nms-user` who is a member of the group `nms-group` using the `auth` security policy. This policy uses SHA hashing for authentication with a shared secret of `auth-pass`. It uses 128-bit AES for encryption using a shared secret of `priv-pass`. The 99 at the end of the command is the reference to controlling access with ACL 99.

```
R84(config)#snmp-server user nms-user nms-group v3 auth sha auth-pass priv
aes 128 priv-pass 99
```

Banner Messages

While *banner messages* will never prevent unauthorized access to a device, they should be implemented to provide legal notice to unauthorized individuals that they are breaking the law when attempting to achieve unauthorized access. While the specific wording required for this varies from jurisdiction to jurisdiction, there are some general guidelines regarding this wording.

- Use of words such as *Welcome* may be used later as a defense that access was encouraged.
- If you plan to use AAA accounting records in any subsequent legal proceeding, you must inform intruders they are being audited.
- You should always state the owner of the system so there will be no later defense that the intruder was unaware of the system owner.
- To prevent any future defense that permission was implied, always state “authorized access only.”

There are three types of banner message, and they differ in when they are displayed. Let’s look at configuring each type and discuss when they will appear. The messages used do *not* constitute any recommendations as to wording.

Message of the Day (MOTD)

A *message of the day (MOTD)* appears at connection time and before the login banner (if configured). They may be used to communicate scheduled maintenance windows or other general information. To create a message that says “We will be down for 2 hours at 12 p.m.,” use the following command. The message can be surrounded with any character (in this case ') as long as that character does not appear in the message.

```
R85(config)#banner motd '
Enter text message , End with character '''
We will be down for 2 hours at 12 PM.'
```

EXEC Banner

This banner appears after successful authentication but before the first command prompt appears. To configure the *EXEC banner* to say “This is your last chance to leave if you are unauthorized,” use this command:

```
R85(config)#banner exec '
Enter text message, End with character '''
This is your last chance to leave if you are unauthorized.'
```

Login Banner

This banner appears after the MOTD banner (if configured), before the login prompt, and before the EXEC banner (if configured). To configure the *login banner* to say “This is your first chance to leave if you are unauthorized,” use this command:

```
R85(config)#banner login '
Enter text message, End with character '''
This is your first chance to leave if you are unauthorized.'
```

Verification

To check your work, let’s connect from R86 using Telnet and see what you get:

```
R86#telnet 10.10.10.10
Trying 10.10.10.10 ... Open
We will be down for 2 hours at 12 PM
This is your first chance to leave if you are unauthorized
Username:Admin
Password: <hidden>
This is your last chance to leave if you are unauthorized
```

As you can see, you received the messages as configured in the order you expected.

Securing Access through SNMP v3

Configuring SNMP requires you to set an engine ID for any device used to manage SNMP. This is an ID number composed of 24 hex characters. When inform messages are sent to stations, it is the engine ID that identifies the station. It is entered as a 12-character string. Setting the SNMPv3 engine ID for the management station on a router is done as follows:

```
R82(config)#snmp-server engineID local 000010000203
```

Once the engine ID has been defined, the high-level steps to control access to SNMP are as follows:

1. Define an SNMP group and specify the cryptographic policy to be used by the group. In this same command, you can assign an MIB view.
2. Define SNMP users and assign them a user group, a view, an authentication hashing algorithm and shared secret, and when used an encryption algorithm.
3. Define SNMP views, each of which will control the information that can be accessed by users who have been assigned the view.
4. Define the SNMP host that will be the recipient of traps. You will also specify in the same command the user account (and the algorithms and keys associated with that account) under whose security context the traps will be sent.

First let's define an SMTP group named `snmp-group`, specify version 3, and set it to use the `priv` security policy and to have read-only access to the view named `read-view` (to be created in a later step).

```
R82(config)#snmp-server group snmp-group v3 priv read read-view
```

Next let's define an SNMP user named `read-user`, assign the user to the group `snmp-group`, set the version as version 3, configure SHA as the authentication algorithm using a shared key of `troy-key`, and configure 128-bit AES as the encryption algorithm using `mac-key` as the shared key for AES.

```
R82(config)#snmp-server user read-user snmp-group v3 auth sha troy-key priv
aes 128 mac-key
```

Now let's define the view that you referenced in the command creating the group. The view will only allow read access to the OID 1.3.6.1.2.1 and below.

```
R82(config)#snmp-server view read-view 1.3.6.1.2.1 included
```

Finally, let's set the IP address of the management station to which any traps should be sent along with the version number, a cryptographic policy of auth, and a user account named `test-user` under whose security context the traps will be sent. This is an account you did not create in this example.

```
R82(config)#snmp-server host 10.10.10.10 version 3 priv test-user
```

Securing NTP

Synchronization of time among infrastructure devices has become more and more critical to the proper operation of networks. Digital certificates have explicit validity periods, certain Windows operations require strict time synchronization, and analysis of integrated log files

becomes a nightmare when the devices from which the log files come have not been synchronized. Moreover, some compliance standards call for strict time synchronization.

While the need to use NTP is without question, network attacks leveraging NTP have appeared that now require you to secure the operation of NTP to prevent such attacks. These attacks can be prevented by configuring NTP authentication. This involves setting a shared secret between the NTP clients and the NTP server that will be used to compute a hash value of the update sent to the client. The client will perform a hash calculation of the update using the same shared key and will compare the results. A match serves as assurance that the update came from the legitimate NTP server. It is important to note that this does not encrypt the update; it only verifies its origin and trustworthiness. Figure 8.2 shows the process.

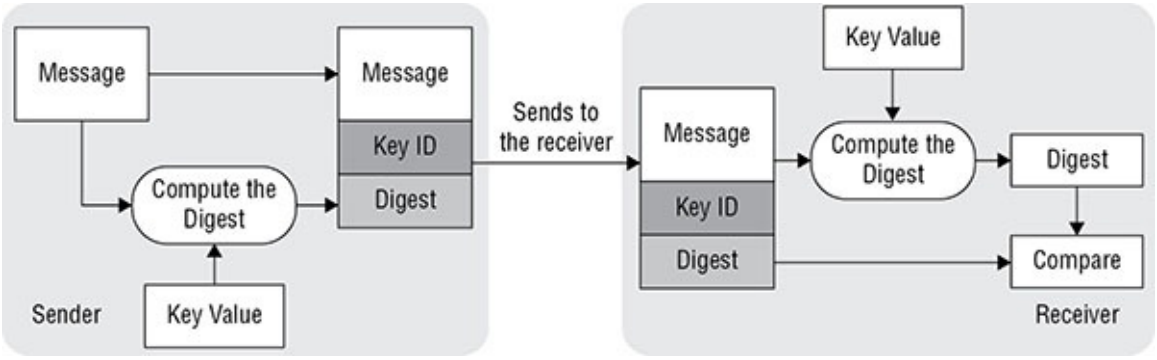

FIGURE 8.2 NTP authentication process

To configure NTP authentication, the high-level steps (to be performed on both server and client) are as follows:

1. Configure an NTP authentication key number and MD5 string (shared secret).
2. Specify at least one trusted key number referencing the key number in step 1.
3. Enable NTP authentication.

For the first step, let's configure an NTP key numbered 87 with an associated MD5 string (the shared secret) of `mykey` on two routers.

```
R88(config)#ntp authentication-key 87 md5 mykey

R89(config)#ntp authentication-key 87 md5 mykey
```

Now let's specify the use of key number 87 and its associated MD5 string to be used for NTP authentication.

```
R88(config)#ntp trusted-key 87

R89(config)#ntp trusted-key 87
```

Finally, all you need do is enable NTP authentication.

```
R88(config)#ntp authenticate
R89(config)#ntp authenticate
```

Using SCP for File Transfer

While FTP and TFTP can be used to transfer configurations and IOS images across the network, these protocols lack the ability to encrypt the transmission. A better alternative is *Secure Copy Protocol (SCP*). This is an implementation of the Remote Copy Protocol (RCP) that operates over an SSH connection. The server that is used to store images and configurations must be configured as an SCP server with a key that can be validated by the Cisco devices. That setup is beyond the scope of this book; however, we will cover the commands to be used on the Cisco devices to perform an SCP transfer.

With the server setup in place, you simply reference the SCP server by URL in the `copy` command. For example, if the server were named `scp-srv` and you wanted to copy the running configuration to it under the security context of an account named Admin with a password of `mypass`, while naming the file `R88-config.txt`, you would use the following command:

```
R88#copy run scp://scp-srv/admin:mypass/r88-config.txt
```

To restore that file to the startup configuration, you would use the following command:

```
R88#copy scp://scp-srv/admin:mypass/r88-config.txt start
```

Summary

In this chapter, you learned about the security differences in managing devices from in-band and out-of-band interfaces. You also learned that in-band interfaces include HTTP, VTY, and the physical interfaces on the device and that out-of-band interfaces include the console and AUX ports. The chapter also discussed 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. Among the other topics covered in this chapter were the types of banner message that can be configured and the securing of the NTP protocol.

Exam Essentials

Identify in-band and out-of-band interfaces. In-band interfaces include HTTP, VTY, and the physical interfaces on the device. Out-of-band interfaces include the console and AUX ports.

Describe methods to secure management interfaces. These include disabling the HTTP server and enabling the HTTPS server, securing SNMP v3 with a security policy, applying passwords to all management interfaces, and using SSH for remote management rather than Telnet. It also includes applying ACLs to all management interfaces.

Identify the types of banner messages and their use. These include the message of the day banner, which appears when a connection is made, and login banners, which appear after authentication, after the MOTD and EXEC banners that appear.

List the three security policies that can be applied to SNMPv3. These include AuthNoPriv, which is no hashing to secure authentication or encryption of data; AuthNoPriv, which is hashing to secure authentication but no encryption of data; and AuthPriv, which is hashing to secure authentication and encryption of data.

Describe the steps to configure NTP authentication. These steps are configuring an NTP authentication key number and MD5 string (shared secret), specifying at least one trusted key number referencing the key number in the first step, and enabling NTP authentication.

Review Questions

1. Which of the following is an out-of-band connection?
   A. HTTP
   B. Con0
   C. Gi0/1
   D. VTY
2. What information is required to set up a modem on the AUX port?
   A. Line number
   B. AUX password
   C. Transmission rate
   D. Modem model
3. Which of the following is a valid reason for configuring a loopback interface as the management interface?
   A. It is more secure.
   B. It provides better performance.
   C. It is always up.
   D. It is preconfigured.
4. What command enables you to identify the total number of VTY ports in the device?
   A. `R1(config)#line ?`
   B. `R1(config)#line vty ?`
   C. `R1#line ?`
   D. `R1#line vty ?`
5. How are the locations of information contained in SNMP identified?
   A. MIB

B. OID

C. Informs

D. Traps

6. Which SNMP security policy provides hashing to secure authentication but no encryption of data?

   A. noAuthNoPriv

   B. AuthNoPriv

   C. AuthPriv

   D. Priv

7. Which interfaces should be protected by passwords?

   A. VTY

   B. Console

   C. HTPS

   D. All of the above

8. Which of the following commands enables encryption of HTTP transfers?

   A. `R81(config)#ip https secure`

   B. `R81(config)#ip https server`

   C. `R81(config)#ip https secure-server`

   D. `R81(config-line)#ip https secure-server`

9. Which command applies ACL 99 at the group level, while referring to the group `test-group` using the `priv` security policy with write access to a view called `write-view`?

   A. `R84#snmp-server group test-group v3 priv write write-view access 99`

   B. `R84(config)#snmp-server test-group v3 priv write write-view access 99`

   C. `R84(config)#snmp-server group test-group v3 priv write-view access 99`

   D. `R84(config)#snmp-server group test-group v3 priv write write-view access 99`

10. Which of the following is *not* a recommendation for banner message wording?

    A. Use of words such as *Welcome* should be encouraged.

    B. If you plan to use AAA accounting records in any subsequent legal proceeding, you must inform intruders they are being audited.

    C. You should always state the owner of the system so there will be no later defense that the intruder was unaware of the system owner.

D. To prevent any future defense that permission was implied, always state “authorized access only.”

11. Which of the following is *not* a banner type?
    A. MOTD
    B. EXEC
    C. Login
    D. Maintenance
12. Which of the following banner messages appears at connection time?
    A. MOTD
    B. EXEC
    C. Login
    D. Maintenance
13. When SNMP inform messages are sent to stations, what value identifies the station?
    A. Process ID
    B. MAC address
    C. Engine ID
    D. Router ID
14. Which of the following steps in configuring SNMP v3 security is optional?
    A. Define an SNMP group
    B. Assign an MIB view
    C. Specify the cryptographic policy to be used by the group
    D. Define SNMP users and assign them a user group
15. What statement is false with regard to the following command?

```
R82(config)#snmp-server view read-view 1.3.6.1.2.1 included
```

    A. The view is name `read-view`.
    B. `read-view` is the group name.
    C. 1.3.6.1.2.1 is the OID.
    D. This command defines a view.
16. How is MD5 used in NTP authentication?
    A. Encrypts the data
    B. Hashes the update

C. Hashes the password

D. Encrypts the shared secret

17. Which step is not part of configuring NTP authentication?

A. Configure an NTP authentication key number and MD5 string

B. Specify at least one trusted key number referencing the key number

C. Encrypt the key number

D. Enable NTP authentication

18. Which of the following should be used as a secure alternative to TFTP or FTP?

A. SCP

B. RTP

C. VTP

D. STP

19. When using SCP to copy files to an SCP server, how do you reference the SCP server in the `copy` command?

A. MAC address

B. IP address

C. URL

D. Port number

20. In what repository is SNMP data contained?

A. OID

B. MIB

C. Registry

D. Hardware register

Chapter 9
Understanding 802.1x and AAA

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.2 AAA concepts**
  - Describe RADIUS and TACACS+ technologies
  - Configure administrative access on a Cisco router using TACACS+
  - Verify connectivity on a Cisco router to a TACACS+ server
  - Explain the integration of Active Directory with AAA
  - Describe authentication and authorization using ACS and ISE
- ✓ **2.3 802.1x authentication**
  - Identify the functions of 802.1x components

While access to the network and to network resources can be controlled by performing user authentication at the point of entry into the network, this approach creates a larger and larger management headache as the number of network entry devices grows. In fact, creating and managing user accounts and user passwords across multiple wireless access points, RAS servers, and VPN servers becomes almost unworkable. The 802.1x standard was created to address this issue. In this chapter, you'll explore 802.1x and two closely related technologies that make it possible.

In this chapter, you will learn the following:

Understanding AAA 802.1x components

Using RADIUS and TACACS+ technologies

Configuring administrative access with TACACS+

Verifying router connectivity to TACACS+

Integrating Active Directory with AAA

Performing authentication and authorization using ACS and ISE

802.1x Components

The *802.1x* standard defines a framework for centralized port-based authentication. It can be applied to both wireless and wired networks and uses three components.

- *Supplicant*: The user or device requesting access to the network
- *Authenticator*: The device through which the supplicant is attempting to access the network
- *Authentication server*: The centralized device that performs authentication

The role of the authenticator can be performed by a wide variety of network access devices, including remote access servers (both dial-up and VPN), switches, and wireless access points. The role of the authentication server can be performed by a Remote Authentication Dial-in User Service (RADIUS) or Terminal Access Controller Access Control System + (TACACS+) server. The authenticator requests credentials from the supplicant and, upon receipt of those credentials, relays them to the authentication server, where they are validated. Upon successful verification, the authenticator is notified to open the port for the supplicant to allow network access.

Figure 9.1 illustrates this process.

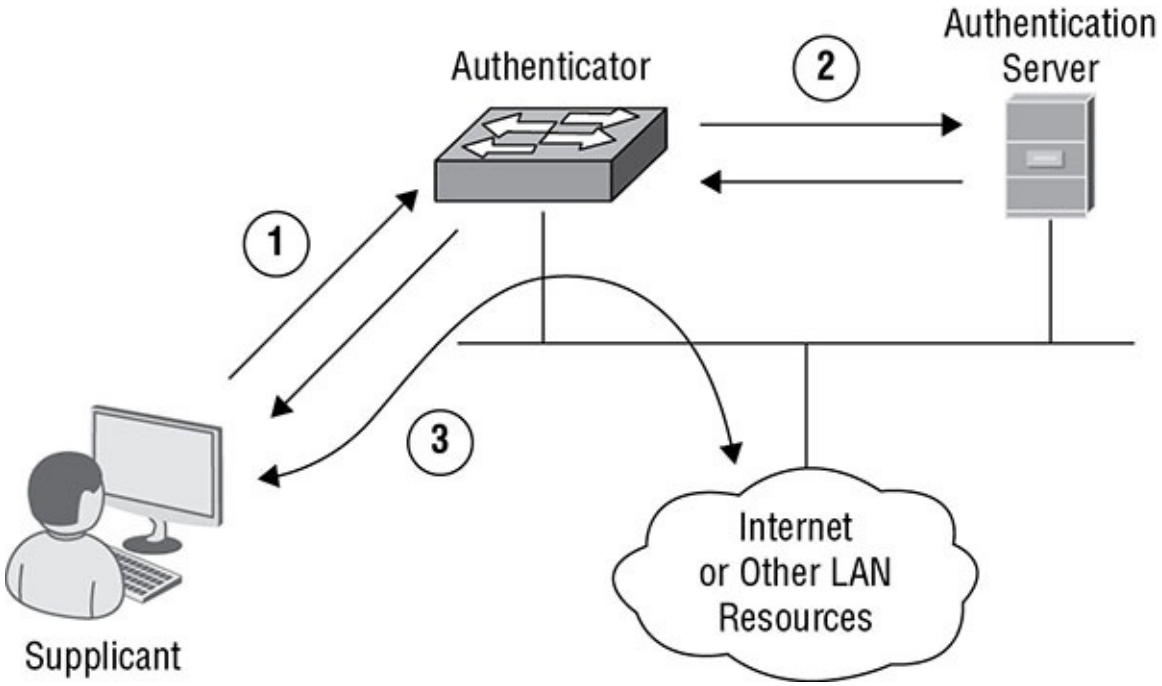

FIGURE 9.1 802.1x

RADIUS and TACACS+ Technologies

While *RADIUS* and *TACACS+* perform the same roles, they have different characteristics. These differences must be taken into consideration when choosing a method. Keep in mind also that while RADIUS is a standard, TACACS+ is Cisco proprietary. Table 9.1 compares them.

TABLE 9.1 RADIUS and TACACS+

Protocol	Transport Protocol	Confidentiality	Authentication, Authorization, and Accounting	Supported Layer 3 Protocols	Devices	Traffic
RADIUS	UDP	Password only	Combines the three processes	All but RAS, NetBIOS, or X.25	No support for securing Cisco commands	Less
TACACS+	TCP	Entire body except TACACs+ header	Separates the three processes	All	Support for securing Cisco commands	More

Many consider enabling 802.1x authentication on all devices to be the best protection you can provide a network.

Configuring Administrative Access with TACACS+

Earlier you learned how to secure administrative access to a Cisco device using SSH over the VTY lines. You also learned how to control the activities of those with administrative access using privilege levels. Both operations can also be done using AAA services. As you now know, the usernames and passwords can be located on an AAA server rather than on the local device. Having said that, it is also possible to take advantage of these services while locating the usernames and password on the local device. Regarding controlling the activities of those with administrative access, using user accounts rather than privilege levels provides more accountability. In this section, you'll look at how using AAA services changes these configurations.

Local AAA Authentication and Accounting

Local AAA authentication and accounting is a form of AAA in which the user accounts are located on the device rather than on an AAA server. To use AAA services for any type of authentication, it must be enabled on the device. Including this step, the high-level steps to configure local AAA authentication and accounting are as follows:

1. Create user accounts with an assigned privilege level and password.
2. Enable AAA services.
3. Configure an authentication method that specifies local authentication.
4. Configure an authorization method for access to the CLI that specifies local authentication.

Let's begin by creating a user account named `adminsr` that has a privilege level of 7 with an encrypted (secret) password of `srpass`.

```
R89(config)#username adminsr privilege 7 secret srpass
```

Now let's enable AAA services on the router.

```
R89(config)# aaa new-model
```

To configure an authentication method that specifies local authentication on all lines (by adding the `default` keyword), use this command:

```
R89(config)#aaa authentication login default local
```

Finally, let's configure an authorization method that provides access to the CLI (by including the `exec` keyword) on all lines (by adding the `default` keyword).

```
R89(config)#aaa authorization exec default local
```

The configuration will apply all lines except for the `Con0`. This gives you a fallback method to access the CLI if a misconfiguration of authorization locks you out.

SSH Using AAA

In Chapter 8, you learned how to configure SSH access on the VTY lines. When you did that, you created local accounts and passwords to authenticate those connecting with SSH. You also learned in Chapter 8 how to assign privilege levels to user accounts. If you use AAA authentication for SSH, then you can use AAA to authorize the assigned privilege level of the same account when authentication occurs. Later in this chapter, you will learn how to use a TACACS+ server as the authentication method. In this example, you will continue to use a local AAA database. To do this, complete the following tasks:

1. Enable AAA services.
2. Configure an authentication method that specifies local authentication.
3. Configure an authorization method for access to the CLI that specifies local authentication.

These commands are executed much the same as when you were setting up local AAA authentication and accounting in the previous section.

To enable AAA services on the router, use this command:

```
R89(config)# aaa new-model
```

To configure an authentication method that specifies local authentication on all lines (by adding the `default` keyword), use this command:

```
R89(config)#aaa authentication login default local
```

To configure an authorization method that provide access to the CLI (by including the `exec` keyword) on all lines (by adding the `default` keyword), use this command:

```
R89(config)#aaa authorization exec default local
```

Again, the configuration will apply all lines except for the `Con0`. This gives you a fallback method to access the CLI if a misconfiguration of authorization locks you out.

Understanding Authentication and Authorization Using ACS and ISE

To fully realize the benefits of the 802.1x security solution, user accounts and the security polices surrounding those accounts should be in a centralized database available to all devices operating as authenticators. The device operating as the authentication server in the 802.1x framework is the AAA server.

Cisco offers two AAA servers that can fulfill the role of authenticating server. The *Cisco Secure Access Control Server (ACS)* can operate either as a RADIUS server or as a TACACS+ server. The *Cisco Identity Services Engine (ISE)* supports only RADIUS at the time of this writing. However, it supports functionality not present in the Cisco ACS. Additional features include the following:

- Profiling to determine the type of device from which a network access request originates and to apply a set of access policies specific to the profile attached to that device. This means a user might have multiple profiles each attached to the various devices they use.
- Posture assessment to verify the minimum security requirements of a device before allowing access. If issues arise such as missing OS or security updates, the device may be either remediated or denied entry.
- Centralized web access for guest access to the network.

Understanding the Integration of Active Directory with AAA

Both Cisco AAA offerings support the centralization of user accounts and credentials on the AAA server. However, in most cases, doing so would constitute a duplication of efforts since this same information is already contained in a directory services server such as Microsoft Active Directory. Both Cisco ACS and Cisco ISE can consult other databases for information.

The ability of these two offerings to utilize an external enterprise user ID repository is a key feature. While some Cisco devices, such as the Cisco Adaptive Security Appliance (ASA), can communicate directly with LDAP repositories or Active Directory for authentication purposes, most do not. Therefore, the deployment of an AAA server serves as an important link between the authenticators in the 802.1x framework and the external enterprise directory service. In the next section, you'll learn how an authenticator might speak to an external enterprise database through the AAA server, and you'll discover how to set up a Cisco router to use a TACACs+-based AAA server.

TACACS+ on IOS

While an AAA server can be populated with usernames and credentials, an AAA server can also utilize the same information that resides in an enterprise directory service such as Active Directory. When this is the case, the process that occurs during a request for network access occurs as follows. In this case, a TACACS + server is in use.

1. The supplicant establishes a connection with the authenticator (router, WAP, VPN server).
2. The authenticator challenges the supplicant for credentials.
3. The suppliant responds with credentials.
4. The authenticator passes the credentials to the authentication server (AAA server).
5. The TACACS+ server consults the LDAP server.
6. The LDAP server performs authentication.
7. The authenticator passes the result to the supplicant.

Configuring a Router to Use a TACACS+ Server

The steps to configure a router to use a TACACS+ server are as follows:

1. Enable AAA authentication.
2. Specify the TACACs+ server name.
3. Specify the TACACs+ server IP address and type (IPv4 or IPv6).
4. Specify the key string used as a shared secret between the router and the TACACS+ server.
5. Specify the use of TACACS+ in the method list for authentication and authorization, while also specifying a backup method.
6. Create local usernames and credentials for use in case of loss of access to the TACACS+ server.
7. Enable per-command authorization (optional).
8. Enable accounting of administrative sessions and of the use of specific commands (optional).

First, let's enable AAA as you have done before.

```
R90(config#)AAA new-model
```

Next, you must do the following:

```
R90(config)#tacacs server servertac
R90(config-server-tacacs)#address ipv4 192.168.56.6
R90(config-server-tacacs)#key mysecetkey
R90(config-server-tacacs)#exit
```

Next, let's specify the use of TACACS+ in the method list for authentication and authorization, while also specifying a backup method. In this case, the backup is local authentication.

```
R90(config)#aaa authentication login default group tacacs+ local
R90(config)#aaa authorization exec default group tacacs+ local
```

As you are using local authentication as a backup, you need to create an account for that process should it be necessary. This process is the same as you learned earlier.

```
R90(config)#username adminsr privilege 7 secret srpass
```

Optionally, you can enable per-command authorization. In the following example, the router will consult the TACACS+ server whenever an administrator enters any privilege level 15 commands or any configuration commands. If the account lacks the authorization, it will be denied, and an error message will appear. Again, you have specified local as the backup method here.

```
R90(config)#aaa authorization commands 15 default group tacacs+  local
R90(config)#aaa authorization config-commands
```

Optionally, you can also enable accounting of administrative sessions and of the use of specific commands. In the following example, an accounting record will be sent at the start of an administrative session to the `EXEC` process, and another will be sent at the end of the session.

```
R90(config)#aaa accounting exec default start-stop group tacacs+
```

Finally (again optionally), the following command causes an accounting record to be sent for every privilege level 15 command and every configuration command:

```
R90(config)# aaa accounting commands 15 default stop-only group tacacs+
```

Verify Router Connectivity to TACACS+

Once you have configured the router with the IP address of the TACACS+ server, you should verify that you have connectivity between the devices. This can be done by using the `test` command to test an authentication using the TACACS+ server. For example, to test the username `mytest` with a password of `mypass`, use the following command:

```
R99(config)#test aaa group tacacs mytest mypass new-code
Sending password
User sucessfully authenticated
USER ATTRIBUTES
Username      0     "mytest"
Reply-message 0     "Password:  "
```

As you can see, the authentication succeeded, which indicates that you have connectivity to the TACACS+ server.

Summary

In this chapter, you learned about the AAA service that can be provided by TACACS+ and RADIUS servers. You also looked at configuring administrative access to a router using

TACACS+. You learned how AAA can be integrated with Active Directory. You looked at the Cisco implementations of a RADIUS server including the Cisco Secure Access Control Server (ACS) and the Cisco Identity Services Engine (ISR). Finally, you learned about the functions of various 802.1x components.

Exam Essentials

Describe the RADIUS and TACACS+ technologies. Understand the benefits of these technologies, which include centralization of authentication and reduction of administrative overhead. Also identify the differences between these technologies, which include the ports used and the way in they handle authentication, authorization, and accounting functions.

Configure and verify administrative access to a router using TACACS+. This includes enabling AAA services, specifying the TACACs+ server name, specifying the TACACs+ server IP address and type (IPv4 or IPv6), specifying the key string used as a shared secret between the router and the TACACS+ server, and specifying the use of TACACS+ in the method list for authentication and authorization, while also specifying a backup method.

Explain the integration of Active Directory with AAA. Describe how an Active Directory server can be used by an AAA server as a repository for usernames and credentials.

Identify Cisco implementations of AAA servers. These include the Cisco Secure Access Control Server (ACS), which can operate either as a RADIUS server or as a TACACS+ server. The Cisco Identity Services Engine (ISR) supports only RADIUS at the time of this writing. However, it supports functionality not present in the Cisco ACS.

Identify the functions of 802.1x components. These include the supplicant (the device requesting access), the authenticator (the network access device to which you are connecting), and the authentication server (AAA server).

Review Questions

1. Which of the following is an example of the authenticator in the 802.1x standard?
   A. Wireless AP
   B. TACACS+ server
   C. User laptop
   D. AAA server
2. Which of the following is true about TACACs+?
   A. Encrypts only the password
   B. Separates the three AAA processes
   C. Uses UDP

D. Creates less traffic than RADIUS

3. Which of the following commands enables AAA services on a router?

   A. `aaa enable`

   B. `aaa new-model`

   C. `enable aaa`

   D. `aaa authentication`

4. What command configures an authentication method that specifies local authentication?

   A. `aaa authentication default local`

   B. `aaa authentication login local default`

   C. `aaa authentication login default local`

   D. `aaa login default local`

5. When configuring an authorization method that provides access to the CLI, to which line does the configuration *not* apply?

   A. VTY0

   B. CON0

   C. AUX0

   D. VTY1

6. Which of the following is a Cisco implementation of an AAA server?

   A. SDM

   B. ACS

   C. PIX

   D. ASA

7. Which device can communicate directly with LDAP repositories or Active Directory for authentication purposes?

   A. SDM

   B. VTP

   C. PIX

   D. ASA

8. Which of the following commands specifies the TACACS+ server for a router?

   A. `tacacs server` *`servername`*

   B. `server` *`servername`*

C. `tacacs server ip address`

D. `server ip address`

9. Which command tests the authentication process and verifies connectivity to the TACACS+ server?

A. `test aaa group tacacs username passwordnew-code`

B. `test aaa group tacacs password new-code`

C. `test aaa group tacacs username new-codepassword`

D. `test aaa group tacacs username password`

10. Which of the following commands specifies the use of TACACS+ in a method list for authorization while also specifying a backup method?

A. `aaa authorization default group tacacs+ local`

B. `aaa authorization exec default group tacacs+ local`

C. `aaa authorization exec default tacacs+ local`

D. `aaa authorization exec group tacacs+ local`

11. Which of the following steps in configuring a router to use a TACACS+ server is optional?

A. Enable AAA authentication

B. Specify the TACACs+ server name

C. Enable per-command authorization

D. Specify the TACACs+ server IP address and type

12. When AAA services make use of an LDAP server, which component performs the authentication?

A. AAA server

B. LDAP server

C. Network access device

D. Supplicant

13. Which of the following is the ability to verify minimum security requirements of a device before allowing access?

A. Profiling

B. Posture assessment

C. Supplication

D. Authorization

14. Which of the following commands configures a local authorization method that provides access to the CLI on all lines?

    A. `aaa authorization default local`

    B. `aaa authorization default exec local`

    C. `aaa authorization exec default local`

    D. `aaa authorization exec default`

15. Which command creates a user account named `adminsr` that has a privilege level of 7 with an encrypted (secret) password of `srpass`?

    A. `username adminsr privilege 7 secret srpass`

    B. `username adminsr privilege secret 7 srpass`

    C. `username adminsr privilege srpass 7 secret`

    D. `username privilege 7 adminsr secret srpass`

16. Regarding controlling the activities of those with administrative access, why should you use user accounts rather than privilege levels?

    A. Better performance

    B. More accountability

    C. Simpler configuration

    D. Encrypted processes

17. Which of the following is false of RADIUS?

    A. Industry standard

    B. Uses UDP

    C. Supports Cisco commands

    D. Protects only the password

18. Which standard provides a security framework that includes a supplicant, authenticator, and authentication server?

    A. 802.11

    B. 802.3

    C. 802.1x

    D. 802.5

19. In the 802.1x framework, which device can operate as the authentication server?

    A. RADIUS

B. Wireless AP

C. User laptop

D. VPN server

20. Which of the following is the ability to determine the type of device from which a network access request is originating?

A. Posture assessment

B. Profiling

C. Classification

D. Contextual awareness

Chapter 10
Securing a BYOD Initiative

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **2.4 BYOD**
  - The BYOD architecture framework
  - Describe the function of mobile device management (MDM)

Despite the security challenges, users are increasingly demanding the right to use their personal mobile devices in the enterprise. Somewhat like the clamor for wireless access witnessed more than a decade ago, this outcry for a *bring your own device (BYOD)* initiative has reached the point where it can no longer be ignored. It has given rise to the development of mobile management software to gain control over these personal devices.

In this chapter, you will learn the following:

The BYOD architecture framework

The function of mobile device management (MDM)

The BYOD Architecture Framework

To enable the secure deployment of a BYOD initiative, Cisco has created an architectural framework that provides the components required to allow use of personal devices while ensuring that these devices are secure and free from malware every time they access the network. The framework may include the following functions:

- The 802.1x framework
- *Mobile device management* software
- The Cisco Integrated Services Engine
- The *Cisco TrustSec* provisioning and management platform

While you already understand the role that the 802.1x framework plays, in the following sections, the role that each of the other features plays in the Cisco BYOD architectural framework will be discussed.

Cisco ISE

The Cisco Integrated Services Engine (ISE) is a centralized identity-based policy platform that provides context-based access control for wired, wireless, and VPN connections. It combines AAA, posture assessment and profiling, and guest access management. The network access devices (NADs) can be wired switches, VPN servers, wireless access points, and controllers and routers.

ISE can take many items into account when assessing a connection request. Moreover, it can take the same context-based item into account when accessing authorization requests. As shown in Figure 10.1 , the following can be considered during both the access request and the authorization request:

- Who is the individual?
- What device are they using?
- Where are they connecting from?
- When are they connecting?
- How are they connecting?

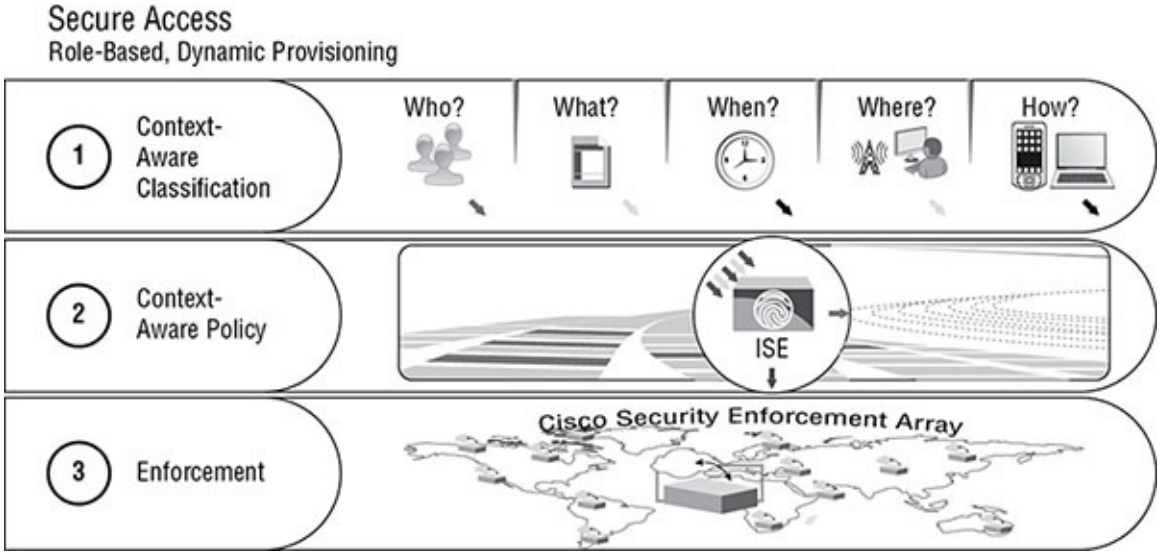

FIGURE 10.1 ISE context-based access

The ISE can make use of several advanced features to provide granular and dynamic access control policies. Among these are the following:

- *Downloadable ACLs (dACLs)*: IP-based ACLs that are implemented on devices when the policy calls for it
- *Automatic VLAN assignment*: To an employee, guest, or, in the case of a failed health check, a remediation VLAN
- *Security Group Access (SGAs)*: Applies a security group tag (SGT) that uniformly enforces the security group policy regardless of topology

- *Change of authorization (COA) updates*: The ability of ISE to change the authorization policy in real time after the administrator makes a change without requiring a log-off for the change to take effect
- *Posture assessment*: Can check the health of a device before allowing access and if the check fails can remediate the device

Finally, the ISE can accept many authentication mechanisms, including the following:

- *802.1x*: The ISE is a fully functional AAA server.
- *MAC authentication bypass (MAB)*: This is a port-based access control using the MAC address of the endpoint.
- *Web authentication (WebAuth)*: This enables network access for end hosts that do not support IEEE 802.1X authentication.

Later in this chapter, you'll see how ISE integrates with mobile device management to make successful and secure BYOD possible.

Cisco TrustSec

Another component in the Cisco BYOD architecture framework is Cisco TrustSec. It works in concert with ISE and other security devices to use security group tags and security group ACLs (SACLs) to provide improved visibility into an access request. It uses logical policy groupings to define policies that control both access and authorization. The three main functions of TrustSec are to do the following:

- Classify each device by assigning a security group tag (SGT) to its IP address.
- Transport or communicate this classification information throughout the network using a process called inline tagging (for those networking devices that support inline tagging) or by using the *SGT eXchange Protocol (SXP)* for those networking devices that do not.
- Enforcement of access rules through the examination of the SGTs.

Let's look at how TrustSec does this.

SGT Classification

Classification of a device is done through the *SGT classification* using SGT tags. These tags, which are 16 bits in length, can be applied dynamically or statically. Dynamic tagging is applied through the Cisco ISE. *Dynamic tagging* is possible when the authentication method is 802.1x, MAC bypass, or through web authentication. In dynamic tagging, the ISE pushes the SGT to the network access device (NAD).

Static tagging can also be performed, and when done, it can be done either on the ISE or directly in the NAD. Examples of this could be to map an entire subnet to an SGT or to map a VLAN to an SGT.

Inline SGT Transport

For those devices that support the feature, *inline SGT transport* can be used to propagate SGTs throughout the network. The sending device will embed the SGT into the Ethernet frame on egress. This tag will be read by the receiving device and propagated to the next device. The SGT will be in a new section of the Ethernet header called the *Cisco Metadata (CMD) header*. Its location is shown in Figure 10.2 . As you can see, the CMD holds other information besides the SGT. Overall, this adds 20 bytes to the size of the header.

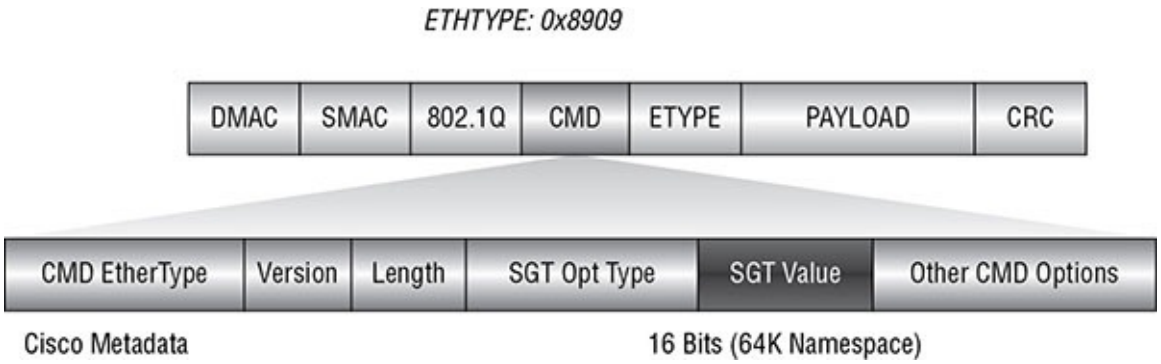

FIGURE 10.2 CMD

One thing to note is that in cases where two networking devices are also using *802.1ae security (MACSec)*, the addition of the 802.1ae header and ICV field will result in a total addition to the Ethernet header of 40 bytes.

SGT Exchange Protocol

For those devices that do not support inline SGT transport, the SGT eXchange Protocol (SXP) can be used to transport the SGT mappings. The goal is to get the classification information (in the form of SGTs) applied to the traffic to the upstream devices that must enforce the security.

SXP connections are used for this purpose and are point-to-point TCP-based connections created between two endpoints, one of which must be designated as the speaker and the other as the listener (any other combination of the two roles will fail). In Figure 10.3 , the 2960 switch on the left is capable of SXP and uses it to send the SGT information and an upstream device (the 3750 switch) that is SGT capable, so when the 3560 sends to the CAT 6500 (which is also SGT capable), the traffic is tagged as described in the previous section.

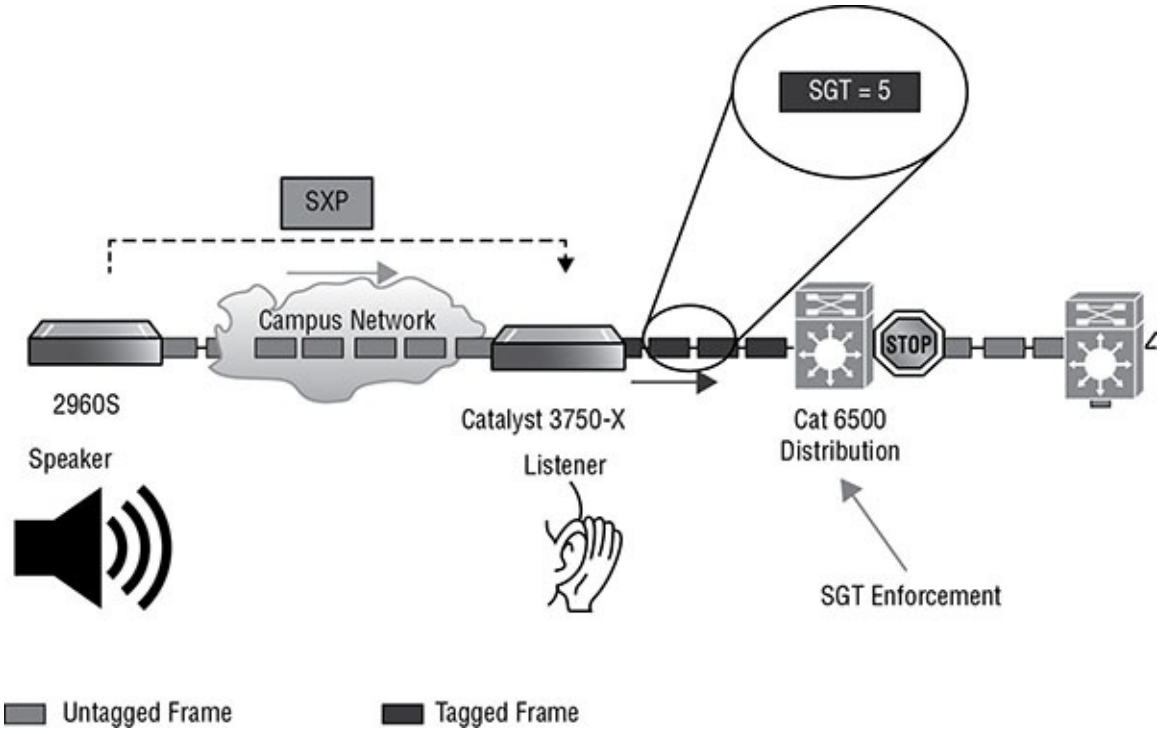

FIGURE 10.3 SXP and SGT

Also notice in Figure 10.3 that at the CAT 6500 an enforcement action has occurred, blocking traffic at that point as result of the SGT information. The four versions of SXP can be described as follows:

- *Version 1*: Supports only IPv4 binding propagation.
- *Version 2*: Supports both IPv4 and IPv6 binding propagation.
- *Version 3*: Adds support for subnet to SGT mappings. If speaking to a lower-version listener, the speaker will expand the subnet.
- *Version 4*: Adds loop detection and prevention, capability exchange, and a built-in keep-alive mechanism.

Enforcing SGACLs

TrustSec maintains a permission matrix with source group numbers (SGTs) on one axis and destination group numbers (SGTs) on the other. Each cell or intersection of a row and column contains an ordered list of rules (SAGLs) controlling the access between those two entities. The security group access lists (SGACLs) do *not* contain references to the SGTs. The action listed in each cell is incorporated into the access list for application. This allows a single ACL to be applied to many cells with a potentially different result based on the cell contents. Figure 10.4 shows an example of a permission matrix.

	SGT10	SGT11	SGT12	SGT40	SGT50
SGT10	✓	✗	✗	✓	✓
SGT11	✗	✓	✗	✓	✓
SGT12	✗	✗	✓	✓	✗
SGT40	✓	✓	✓	✓	✓
SGT50	✓	✓	✗	✓	✓

FIGURE 10.4 Permission matrix

Enforcement Using SGFW

The Cisco Adaptive Security Appliance and several other routing platforms use a different method to enforce TrustSec. While ISE manages SGACLs centrally, these devices are configured individually with ACLs that reference the SGT numbers or security group names. For the ASA to be able to use these SGTs or security group names, the ASA must also be configured with a security group table to map security group names to tags, and an SGT to IP address mapping exists.

Benefits

In the absence of TrustSec technology, access control lists (ACLs) must be updated whenever the following events occur:

- New building on the campus
- New branch office
- New business partner
- Expansion of wireless coverage
- Addition of new servers

Since these ACLs are each tied to a device and must be written from the network perspective of that device, keeping these ACLs updated and maintained can be a nightmare. This is all easier to manage with the TrustSec technology.

Using TrustSec, any new devices must simply be classified at the ingress point of the network, and the security for that device is maintained throughout the network by the associated security group ACL (SAGL). In cases where the introduction of a new device might require the creation of a new security group, rather than the addition to an existing group, a new row and column are added to the access matrix. This matrix is updated and maintained by the ISE, and changes are dynamically propagated across the TrustSec domain.

The Function of Mobile Device Management

Mobile device management software is designed to make it possible to exert control over personal mobile devices that users want to use on the enterprise network. When used in conjunction with ISE, the combination can be a powerful and secure identity and authentication solution for both company-owned and non-company-owned devices.

In the context of a BYOD architecture, the ISE when working in combination with a mobile management policy ties together the provisioning of mobile devices along with a health check of the device at each connection request, as shown in Figure 10.5 .

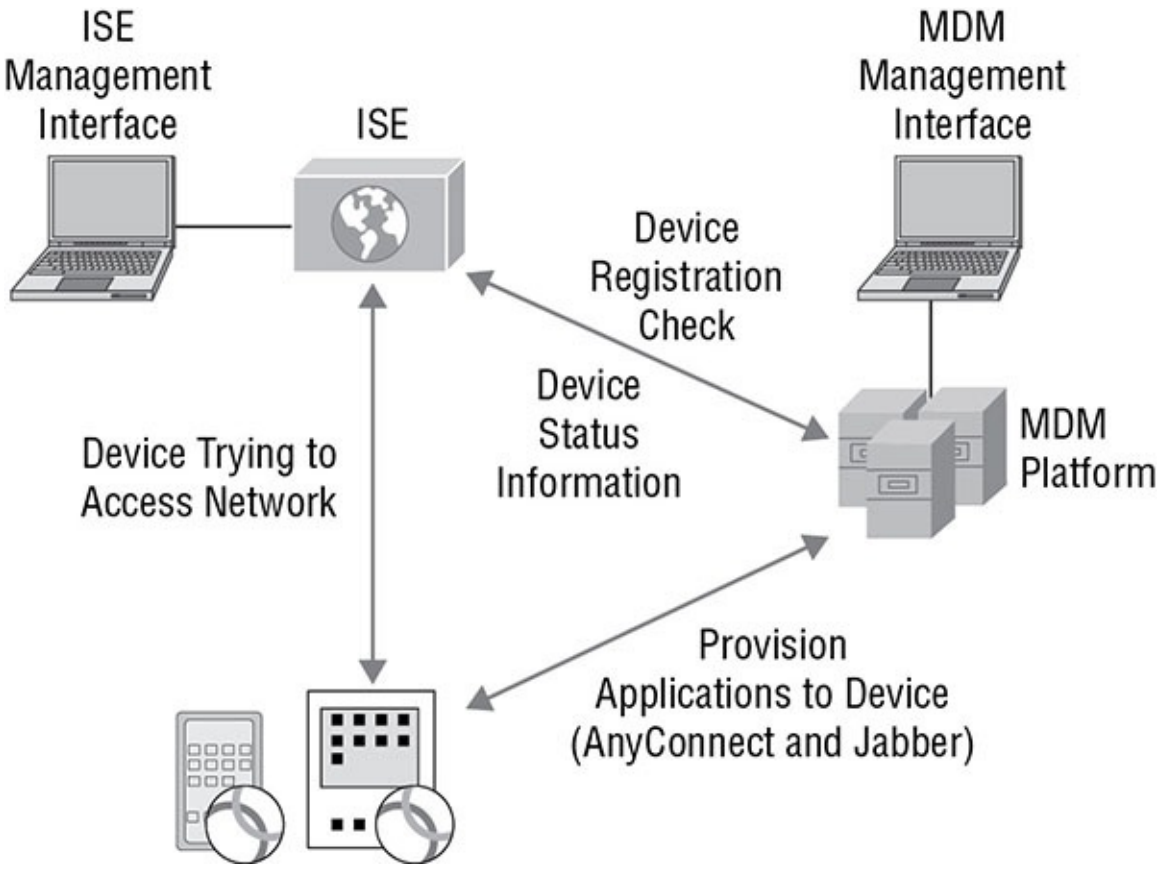

FIGURE 10.5 MDM with IDE

Integration with ISE Authorization Policies

Beyond the health check that can be performed, as described in the previous section, an MDM solution can integrate with ISE authorization policies. For example, let's consider a scenario where an organization uses EAP-TLS for the authentication of company-owned devices. As EAP-TLS is a mechanism that requires a certificate on both the authentication server and the supplicant, company-owned devices will possess such a certificate while employee-onboarded devices will not.

Using this information, ISE can perform an assessment (as shown in Figure 10.6), identify the device type, and apply a unique authorization profile for both groups of devices.

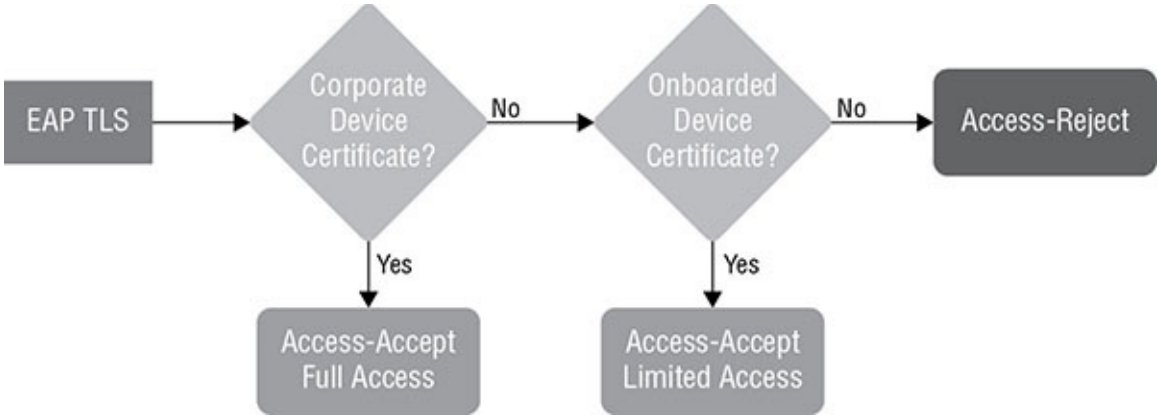

FIGURE 10.6 ISE authorization policy integration

Summary

In this chapter, you learned about the challenges involved in supporting a BYOD initiative. The chapter discussed the components provided by Cisco for this, including the Cisco Integrated Services Engine (ISE) and the Cisco TrustSec provisioning and management platform. You also learned about the advanced features of Cisco ISE, including downloadable ACLs (dACLs), automatic VLAN assignment, security group access (SGA), change of authorization (COA), and posture assessment. Further, the chapter discussed the authentication mechanisms ISE can accept, including 802.1x, MAC authentication bypass (MAB), and web authentication (WebAuth). Finally, the chapter ended by covering the three main functions of TrustSec.

Exam Essentials

Identify the possible components of a BYOD architectural framework. The framework may include the following functions: the 802.1x framework, mobile device management software, the Cisco Integrated Services Engine (ISE), and the Cisco TrustSec provisioning and management platform.

Describe the advanced features of Cisco ISE. These services include downloadable ACLs (dACLs), automatic VLAN assignment, security group access (SGAs), change of authorization (COA), and posture assessment.

Identify the authentication mechanisms ISE can accept. The ISE can accept many authentication mechanisms, including 802.1x, MAC authentication bypass (MAB), and web authentication (WebAuth).

Identify the three main functions of TrustSec. The three main functions of TrustSec are to classify each device by assigning a security group tag (SGT) to its IP address, to transport or communicate this classification information throughout the network using a process called inline tagging (for networking devices that support inline tagging) or using the SGT eXchange Protocol (SXP) for those networking devices that do not, and to enforce access rules through the examination of the SGTs.

Review Questions

1. Which of the following is a centralized identity-based policy platform that provides context-based access control for wired, wireless, and VPN connections?
   A. BYOD
   B. TACACS+ server
   C. ISE
   D. TrustSec
2. Using ISE, which of the following *cannot* be considered during both the access request and the following authorization request?
   A. Why are they connecting?
   B. What device are they using?
   C. Who is the individual?
   D. Where are they connecting from?
3. Which of the following are implemented on devices when a policy calls for it?
   A. dACLs
   B. SAGs
   C. COA
   D. Posture assessment
4. Which ISE feature applies a security group tag (SGT) that uniformly enforces the security group policy regardless of topology?
   A. dACLs
   B. SAGs
   C. COA
   D. Posture assessment
5. Which ISE feature provides the ability of ISE to change the authorization policy in real time?
   A. dACLs
   B. SAGs
   C. COA
   D. Posture assessment
6. Which of the following ISE features checks the health of a device before allowing access

and, if the check fails, can remediate the device?

A. dACLs

B. SAGs

C. COA

D. Posture assessment

7. Which ISE authentication mechanism enables network access for end hosts that do not support IEEE 802.1X authentication?

A. WebAuth

B. MAC bypass

C. WEP

D. WPA

8. Which of the following is *not* a main function of TrustSec?

A. Classification of devices

B. Assessment of devices

C. Transport of classification information

D. Enforcement of access rules

9. Which of the following is used to classify a device?

A. SGA

B. SGT

C. SXP

D. NAD

10. Which of the following is used to transport or communicate classification information for those networking devices that do not support inline tagging?

A. SXP

B. SGA

C. SGT

D. SGFW

11. With which of the following authentication methods is dynamic tagging not possible?

A. WEP

B. 802.1x

C. WebAuth

D. MAC bypass

12. Where is the SGT found when using inline transport?

A. CMD header

B. IP header

C. 802.1ae header

D. ICV

13. How much does the CMD add to the size of the Ethernet header?

A. 16 bytes

B. 18 bytes

C. 20 bytes

D. 22 bytes

14. In cases where two networking devices are also using 802.1ae security (MACSec), what will be the total addition to the Ethernet header?

A. 20 bytes

B. 28 bytes

C. 30 bytes

D. 40 bytes

15. Which is the following is the *only* combination of SXP roles that will result in a successful SXP connection between two devices?

A. Speaker and speaker

B. Listener and speaker

C. Transmitter and receiver

D. Speaker and receiver

16. Which SXP version added support for subnet to SGT mappings?

A. 1

B. 2

C. 3

D. 4

17. Which method of enforcement does the ASA use?

A. SGFW

B. Inline

C. SXP

D. 802.1x

18. Which of the following makes it possible to exert control over personal mobile devices that users want to use on the enterprise network?

A. MDM

B. 802.11i

C. VTP

D. DTP

19. What additional functionality does the addition of ISE to MDM provide for devices connecting?

A. Posture assessment

B. IP identification

C. TACACS+

D. NAT

20. Which of the following is examined to enforce access rules?

A. NAT

B. SGT

C. SXP

D. MAC

Chapter 11
Understanding VPNs

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**3.1 VPN concepts**

- Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
- Describe hairpinning, split tunneling, always-on, NAT traversal

Virtual private network (VPN) connections are widely used to provide a secure method of remote access to the enterprise network. As the sophistication of these connection types has evolved, many additional uses have been found for this concept. Today we use these connections between offices in the place of WAN connections for which we once paid. In this chapter, we will introduce the underlying concepts that make VPNs functional and secure.

In this chapter, you will learn the following:

The protocols that comprise IPsec and the delivery modes in which IPsec can be configured

Advanced features of VPN connections including hairpinning, split tunneling, and always-on VPNs and NAT traversal

Understanding IPsec

While *IPsec* is a protocol, it is also a framework that provides many choices to people configuring an IPsec connection. The framework does not lock one into a certain encryption algorithm, hashing algorithm, or authentication mechanism. Depending on the choice of components that are part of the IPsec protocol suite, you can get several different security services. In this section, you'll learn about those services and the protocols and components that make them possible. You'll also learn about the possible delivery modes of IPsec and about IPsec's relationship to the IPv6 protocol.

Security Services

The security services offered by IPsec are impressive, which is why it has become so widely embraced. One of its more frequent implementations is its use in VPN connections. These connections can be of two types: remote access VPNs in which the traditional dial-up connection is updated to create a secure (and free) pathway through the most untrusted network there is (the Internet), and site-to-site VPNs, which can replace WAN connections that cost money with secure (and free) tunnels for all traffic traversing the sites. Let's look at the security services that have made IPsec so ubiquitous.

Confidentiality

Confidentiality can be provided with IPsec and represents one of the choices that can be made when setting up a connection. As you will learn later in the chapter, when you choose to use ESP, one of the protocols in the suite, at the least the data payload will be encrypted, and, depending on the delivery mode, the entire packet including the header may be encrypted.

Data Integrity

IPsec will always provide data integrity, which means you can be assured that the data has not been changed or corrupted in transit. It does this by using the hashing algorithm you select during implementation. This is called *hash-based message authentication* (HMAC).

Origin Authentication

IPsec will also always provide this security service as well. *Origin authentication* means that you can be assured it came from who it appears to come from. IPsec will authenticate the connection by using the following:

- PSKs
- Digital certificates
- RSA-encrypted nonces

While these processes authenticate the system connecting, extended authentication provides authentication of the user behind the system and is optional.

Anti-Replay

IPsec supports *anti-replay*. To prevent the replay of authentication packets, IPsec examines sequence numbers in the packets. If a packet arrives late or is a duplicate of an earlier packet, it will be dropped.

Key Management

The key management process in IPsec provides for the dynamic generation of keys to be used for encryption and for their secure exchange over an untrusted network, such as the Internet. If the *Diffie-Hellman key exchange* algorithm is used, an asymmetric algorithm is used to create and exchange symmetric keys for this process. This is part of a larger process called the Internet Key Exchange (IKE). Figure 11.1 shows a simplified version of the key generation and

exchange process. A formula is used to generate both Bob and Alice's secret integer base numbers (the first step, which they perform independent of one another). They exchange those values and use them with an algorithm in the second step, which results in them generating keys to be used for encryption.

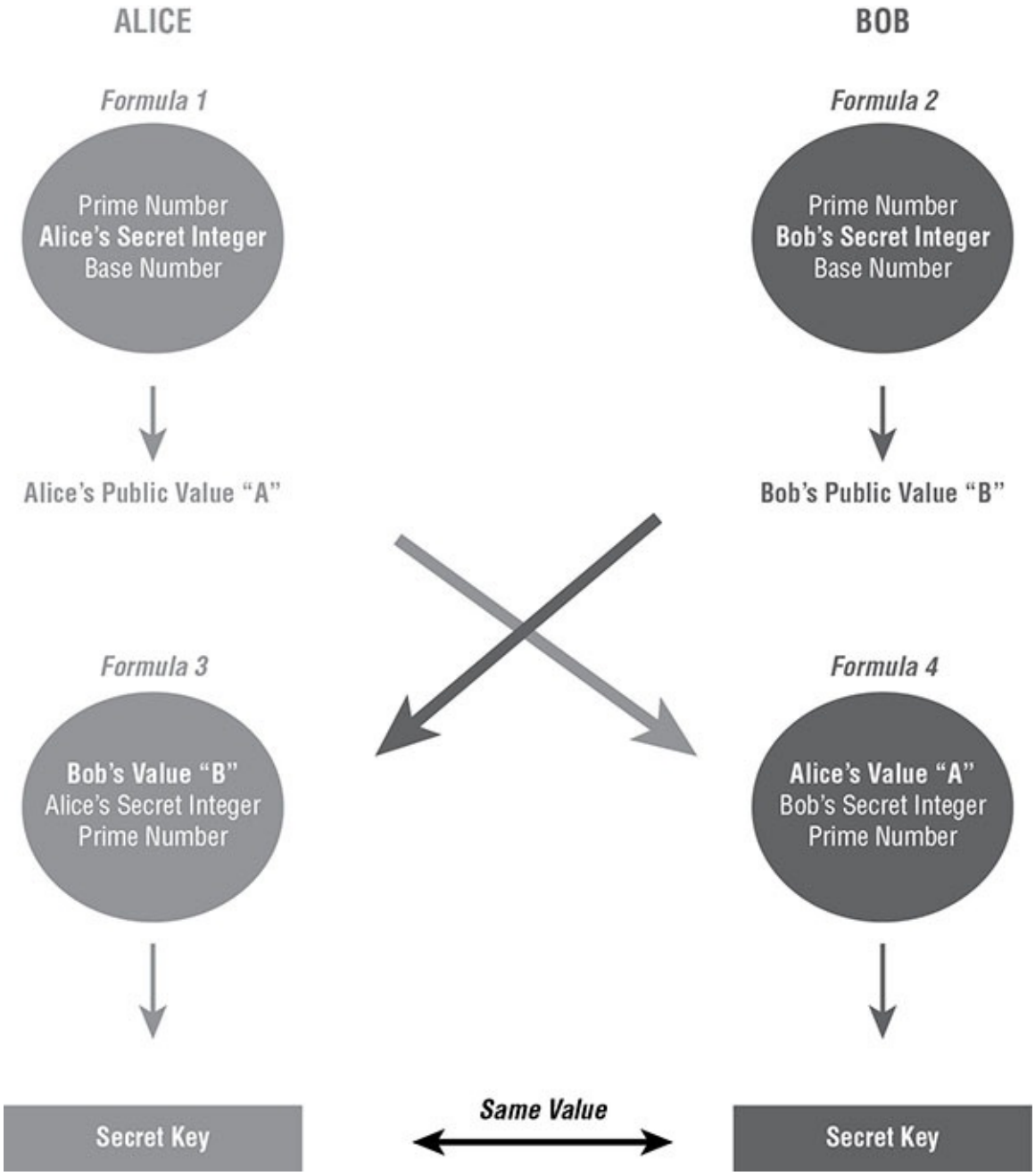

FIGURE 11.1 Diffie-Hellman

A variant of this process called the *Elliptical Curve digital signature algorithm (ECDSA)* is also available and is part of the Suite B standard.

Suite B Cryptographic Standard

In 2005, the NSA identified a set of cryptographic algorithms that are the preferred method for security of information. It called these algorithms *Suite B*. These algorithms use a minimum key

length of at least 128 bits. The use of these algorithms helps to ensure compliance with many standards such as PCI-DSS, HIPAA, and FIPS.

Suite B cryptography uses the following algorithms:

- AES encryption with either 128- or 256-bit keys
- SHA-2 hashing
- *Elliptical Curve digital signature algorithm (ECDSA)* for digital signatures using 256- and 384-bit prime moduli
- Key exchange using ECDHECDSA

Protocols

There are four protocols used in the IPsec process. One of them, the Internet Key Exchange, has two versions. In the next sections, we will discuss each of these protocols and the role each plays in the process.

IKE v1

The *Internet Key Exchange (IKE) protocol* is used for many functions in the IPsec framework.

- *Automatic key generation*: This happens as discussed earlier with Diffie-Hellman.
- *Automatic key refresh*: This includes the generation of new keys periodically.
- *Negotiation of the security association (SA)*: A security association is negotiated successfully if certain configuration selections match on both ends of the connection.

There are two versions of IKE. IKEv2 was designed to overcome limitations inherent in IKEv1. IKEv2 will be covered later in this section. IKE operates in two phases.

Phase 1

In phase 1, IKE negotiates the policy sets (the configuration selections made on either end), authenticates the peer devices to one another, and sets up a secure channel. This phase can be performed in two different modes, Main and Aggressive. A choice must be made between the two, and usually this choice is based on whether the main concern is performance or security. While Main mode requires more messages, it does not expose the identity of the peers. While Aggressive mode requires fewer messages, peer identities are exposed before the secure channel is created.

Main Mode

Main mode consists of three exchanges.

- Peers negotiate the encryption and hashing algorithms to be used.
- The Diffie-Hellman protocol is used to generate a shared symmetric key.

- The *SA* is built, and then the peers authenticate one another within the SA.

Figure 11.2 shows this process.

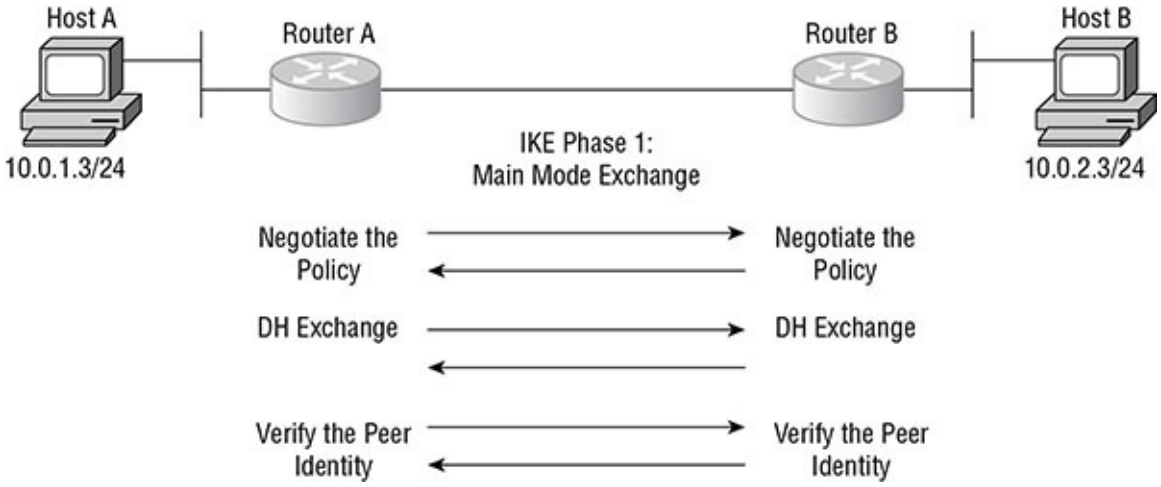

FIGURE 11.2 IKE phase 1

Aggressive Mode

In Aggressive mode, there are only two messages. The initiator passes all information required for the SA, and the responder sends the proposal key material and ID and performs authentication in the next message. This makes negotiation quicker. While Aggressive mode requires fewer messages, peer identities are exposed before the secure channel is created.

Phase 2

While the purpose of phase 1 is to create a secure channel for the phase 2 operations; in phase 2, the parameters that define the IPsec connection are negotiated. In phase 2, the following functions are performed:

- The IPsec transform set is negotiated.
- The SA is established.
- Periodically the SA is renegotiated.
- Optional DH key exchanges that have been configured will be perfumed.

There will be two SAs created because these are unidirectional.

IKEv2

The enhancements provided with *IKEv2* are as follows:

- Fewer transactions, which results in increased speed
- Incorporates extensions such as NAT traversal and dead peer detection
- Stronger security through denial-of-service protection
- More reliability using sequence numbers and acknowledgments

- Supports mobility through the IKEv2 Mobility and Multihoming Protocol (MOBIKE)

ISAKMP

Internet Security Association Key Management Protocol (ISAKMP) is the framework within which IKE performs the dynamic generation of keys. Using IKE and Diffie-Hellman, the result is a security association. This association is based on the successful negotiation of security parameters. In Figure 11.3 , the parameters that must match between two devices, R1 and R2, are shown, and in this case, they match.

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key distribution method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption algorithm	DES, 3DES, or AES	AES	AES
Hash algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication method	Pre-shared keys or RSA	pre-share	pre-share
Key exchange	DH Group 1, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		vpnpa55	vpnpa55

FIGURE 11.3 Matching ISAKMP parameters

AH

When confidentiality of an IPsec connection is not required, the *Authentication Headers (AH) protocol* can be used. While it does provide data integrity and origin authentication and anti-replay protection, the data is sent in clear text. To provide these features, the following steps are used:

1. The immutable fields of the IP header, the data, and the shared key are sent through a hashing algorithm.
2. The resulting hash value is prepended to the original packet.
3. The packet is transmitted to the peer.
4. The peer calculates a hash value from the received packet and compares this value to the one received. If they match data integrity and origin, authentication is validated.

Figure 11.4 shows this process.

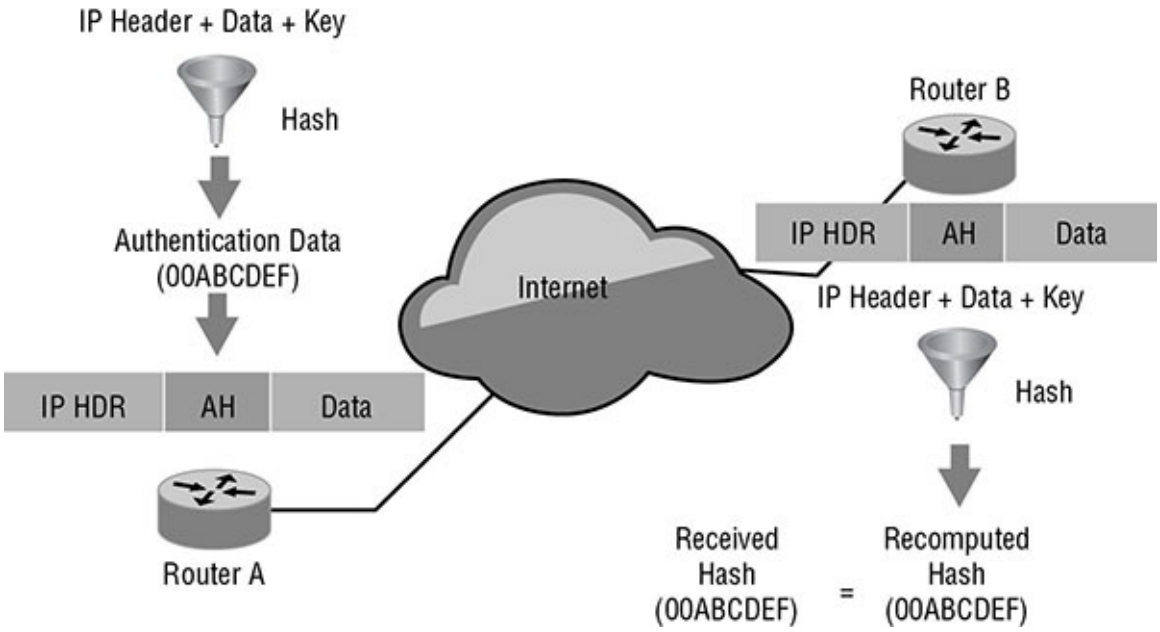

FIGURE 11.4 AH process

ESP

When *Encrypting Security Payload (ESP)* is selected, you get all the protections provided by AH plus encryption. The extent of this encryption depends on the delivery mode selected.

Delivery Modes

There are two modes of delivery available with IPsec, and the difference between the two modes is with parts of the packet that are protected by AH and ESP. Let's look at how these two modes operate in both AH and ESP.

Tunnel Mode

In *tunnel mode*, the entire original packet is protected by either encryption or authentication. In addition, in both AH and ESP, when tunnel mode is used, a new IP header is created that includes the tunnel source and destination address. First let's see how tunnel mode looks when using AH.

AH

When AH is used in tunnel mode, the entire packet is authenticated, and a new IP header is added, as shown in Figure 11.5 .

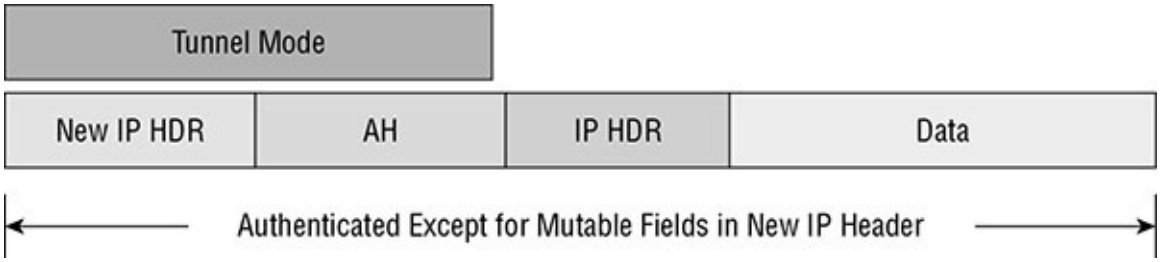

FIGURE 11.5 AH in tunnel mode

ESP

When ESP is used in tunnel mode, the entire packet is encrypted, and a new IP header is added, as shown in Figure 11.6 . A new ESP header is added and encapsulated with the original packet. Finally, a new IP header is added. Notice that all but the new IP header is also authenticated.

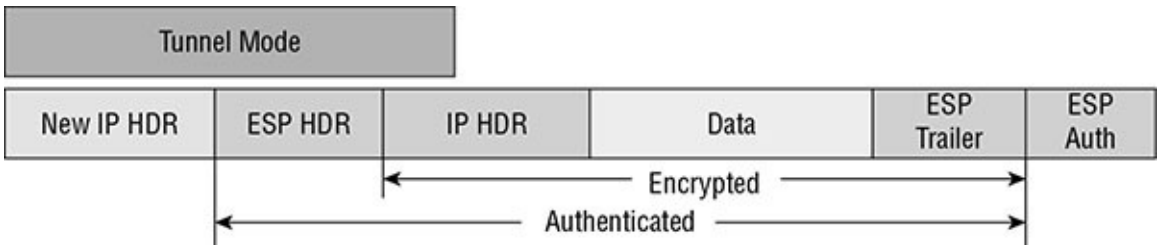

FIGURE 11.6 ESP in tunnel mode

Transport Mode

In *transport mode*, only the payload is protected by either encryption or authentication. First let's see how transport mode looks when using AH.

AH

When AH is used in transport mode, only the payload is authenticated, as shown in Figure 11.7 .

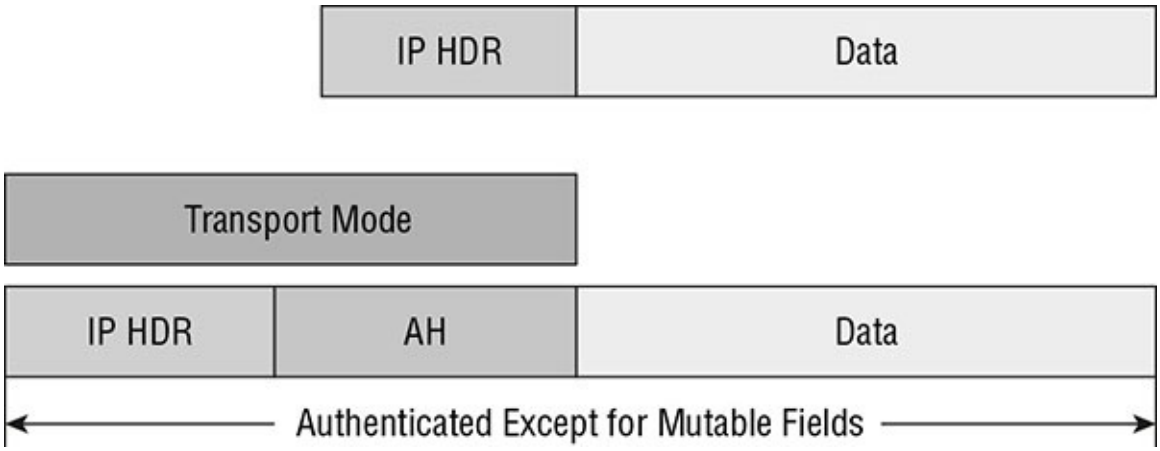

FIGURE 11.7 AH in transport mode

ESP

When ESP is used in transport mode, only the payload is encrypted, as shown in Figure 11.8 . Notice again that all but the IP header is also authenticated.

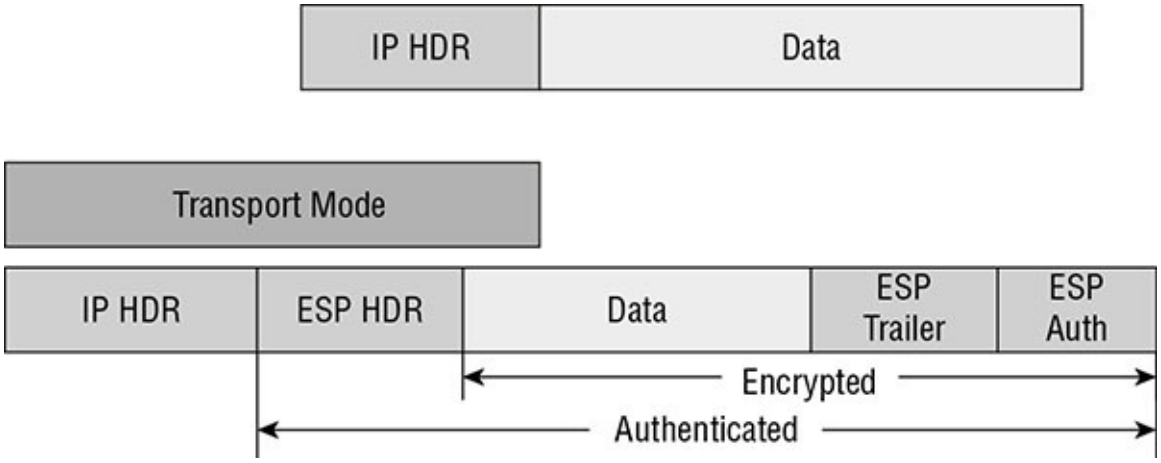

FIGURE 11.8 ESP in transport mode

IPsec with IPV6

While the use of IPsec is not required when using IPv6, the IPv6 packet structure was redesigned to accommodate its use. In IPv4, AH and ESP were implemented as IP protocol headers. In IPv6, extension headers are used instead. These headers, when used, come after the original IPv6 header. The next header field in the original IPv6 header is used to indicate whether the extension header is AH or ESP. It uses the protocol value of 50 for ESP and 51 for AH. Figure 11.9 shows the IPv6 header. Note the next header field. Also note that the extension header lies between the IPv6 header and the payload.

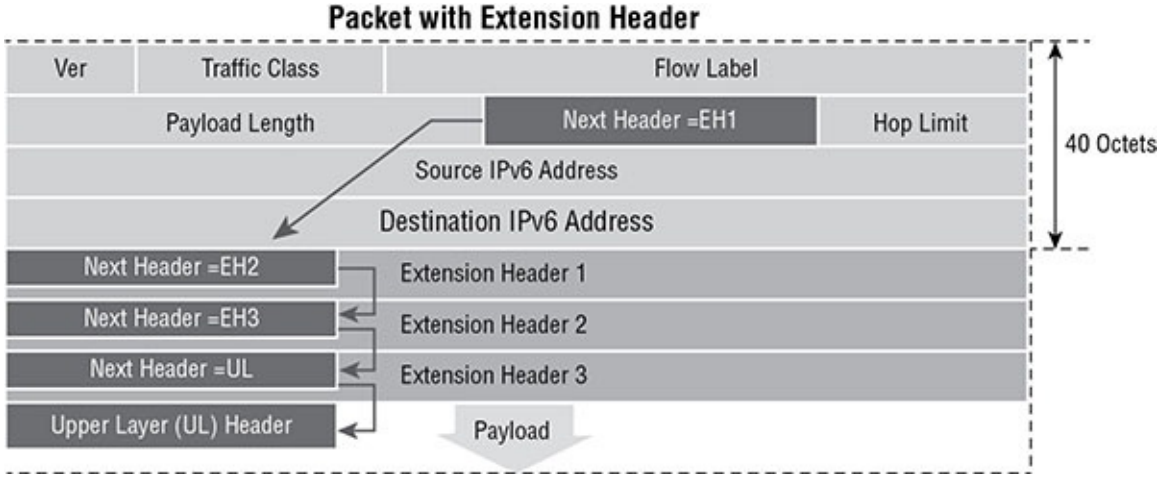

FIGURE 11.9 IPv6 header with extensions

Understanding Advanced VPN Concepts

When implementing IPsec, some scenarios may present challenges. In this section, you'll learn how to overcome specific issues and learn about some additional advanced configurations

topics.

Hairpinning

When using a remote access VPN, two default behaviors can cause issues.

- Once a tunnel is operational, all traffic leaving the VPN client must pass through the tunnel.
- By default, an ASA will not forward packets back out the same interface in which it was received.

This can cause connectivity issues. In the scenario shown in Figure 11.10 , there is a VPN tunnel between the R1 and the ASA1. Because of these two rules, the Internet PC cannot reach SRV1 (because of rule 2) or resources in site 3 (because of rule 1 forcing the traffic through the end of the tunnel and rule 2 because it cannot reenter that interface).

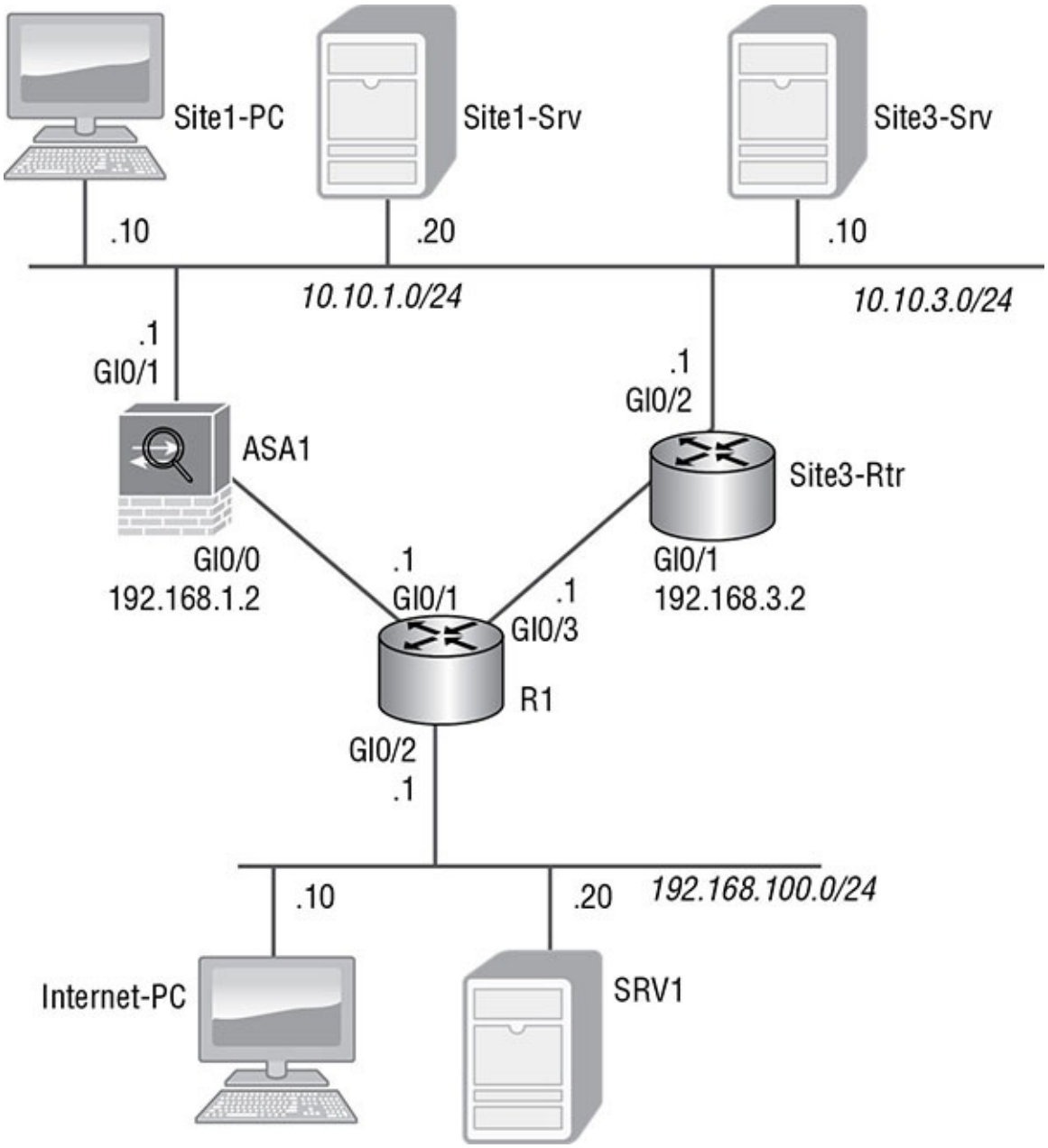

FIGURE 11.10 The need for hairpinning

To solve this issue, you must enable an option called Enable Traffic Between Two Or More Hosts Connected To The Same Interface. This is commonly referred to as *hairpinning*. This option is found by navigating in the ASDM to Configuration ➢ Device Setup ➢ Interfaces. This selection must be made on the ASA that terminates the VPN connection. You'll find this selection at the bottom of the Interface page, as shown in Figure 11.11 . You should have the interface in question highlighted when you make the selection.

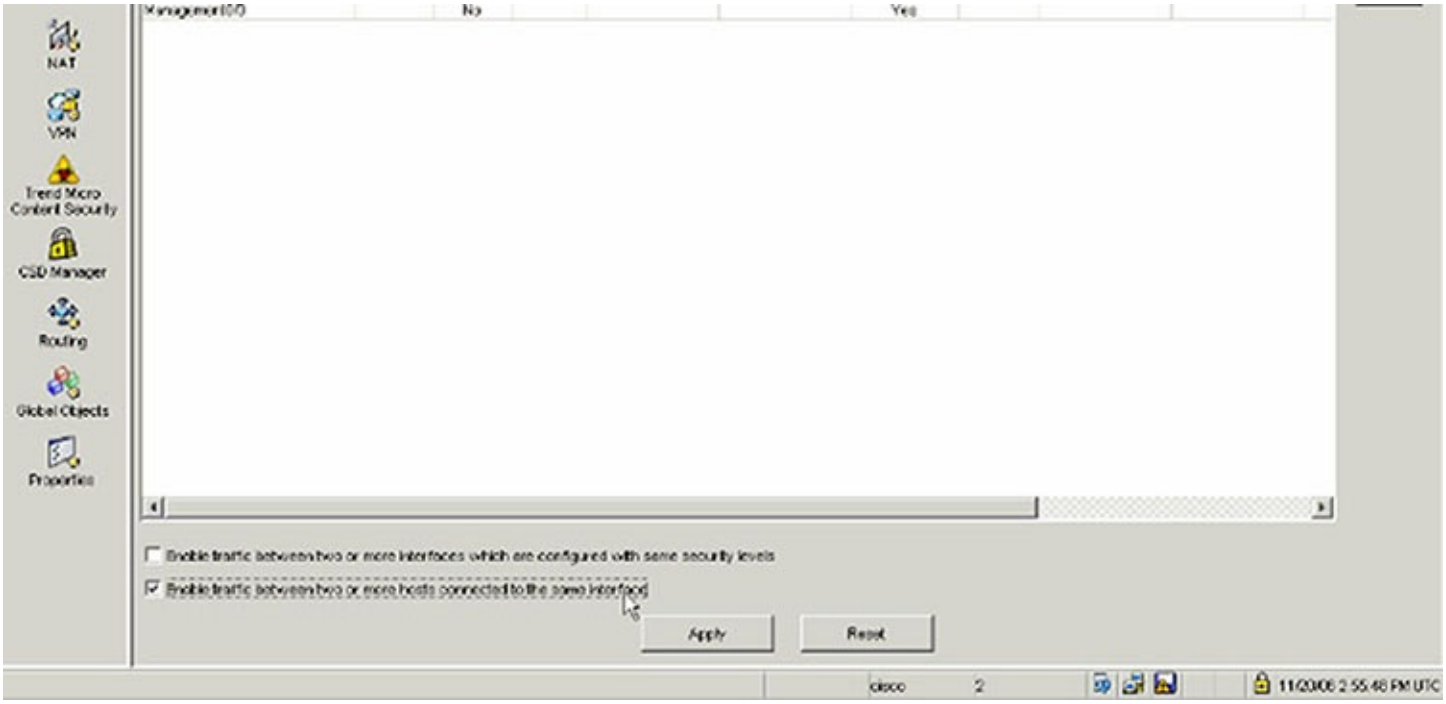

FIGURE 11.11 Hairpin configuration

Split Tunneling

Another advanced option you can enable is called *split tunneling*. When enabled, it allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel. When this is done, an ACL is used to determine the traffic that goes through the tunnel (all traffic except for Internet traffic) and the traffic that does not go through the tunnel (Internet).

To make this possible, follow these steps:

1. Navigate in the ADSM to Configuration ➢ Remote Access VPN ➢ Network (Client) Access ➢ Group Policies. The policies that have been defined will appear. Select the policy that was created when you set up the remote access VPN connection and select Edit.
2. In the Edit Internal Group Policy window, navigate to Advanced ➢ Split Tunneling. Deselect the Inherit box for the Network List field. This prevents the policy from inheriting the current policy. Next click the Management button to the right of the field. The ACL Manager window will appear.
3. Select the Standard ACL tab and then select Add ➢ Add ACL.
4. In the Add ACL box, give this ACL a name, such as RA-split-tunnel.
5. Click OK and then highlight the ACL and select Add ➢ Add ACE. Here add the network ID of the destination LAN and select Permit.

That defines the traffic to go through the tunnel. All undefined traffic will not go through the tunnel and will therefore not be impacted by the two rules discussed earlier. From a conceptual view, what will now be allowed is shown in Figure 11.12 .

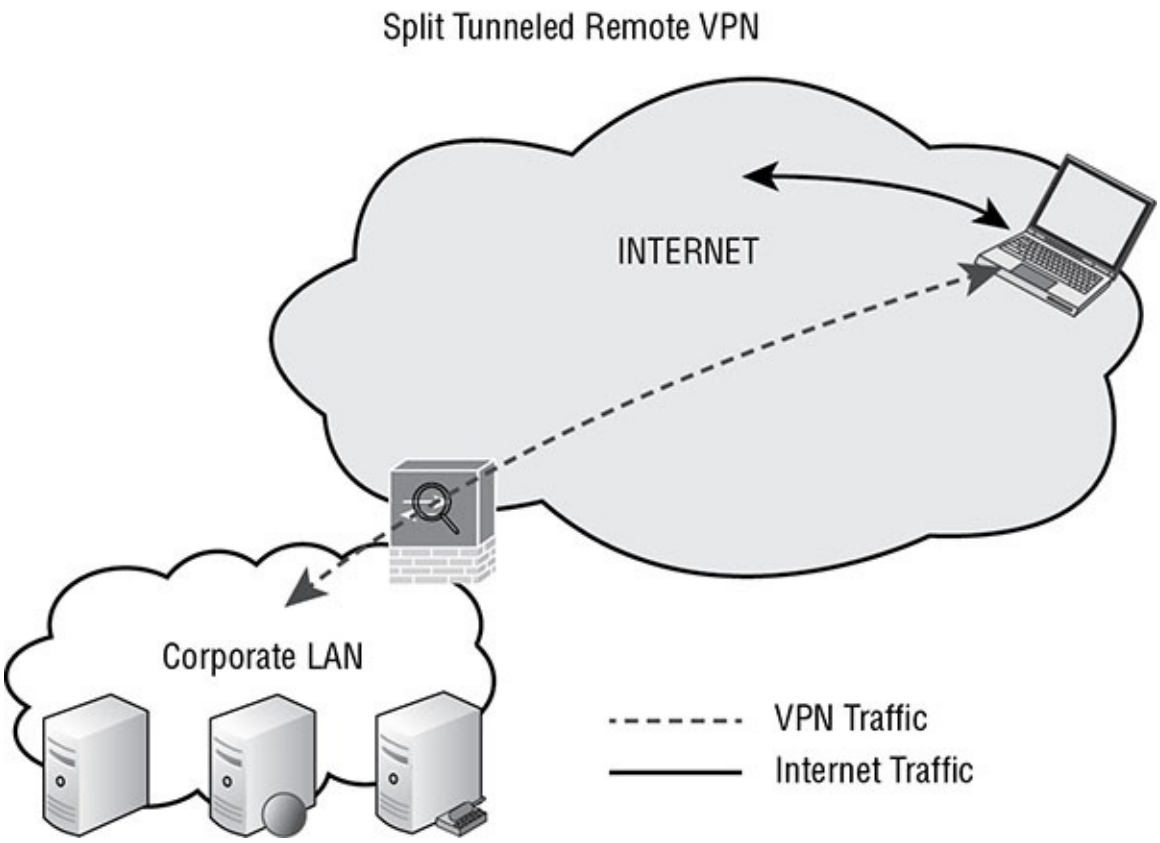

FIGURE 11.12 Split tunneling

Always-on VPN

When the Cisco AnyConnect is used to create a VPN connection, it is possible to have the connection brought up any time the user logs on to his device. This is called *Always-On VPN*.

To enable Always-On VPN, you must first enable Trusted Network Detection in a profile that applies to the user. This feature enables the device to know when it is connected to the corporate LAN and when it is not. Then you specify that when not connected to the corporate LAN, the VPN connection should be started.

1. In the ASDM, navigate to Configuration ➢ Remote Access VPN ➢ Network ➢ AnyConnect Client Profile. In this configuration mode, you can add a new AnyConnect profile. Click the Add button and choose a profile name and profile location. You can also apply this profile to a Group Policy. But this could be also added later with the command. Click OK and Apply.
2. Select the new profile and then on the left select Preferences Part2. You will see the screen shown in Figure 11.13 .
3. Check Automatic VPN Policy and select Disconnect on Trusted Network Policy and Connect on Untrusted Network Policy. You must also enter the DNS domain name for your trusted network, and you should also add DNS servers.

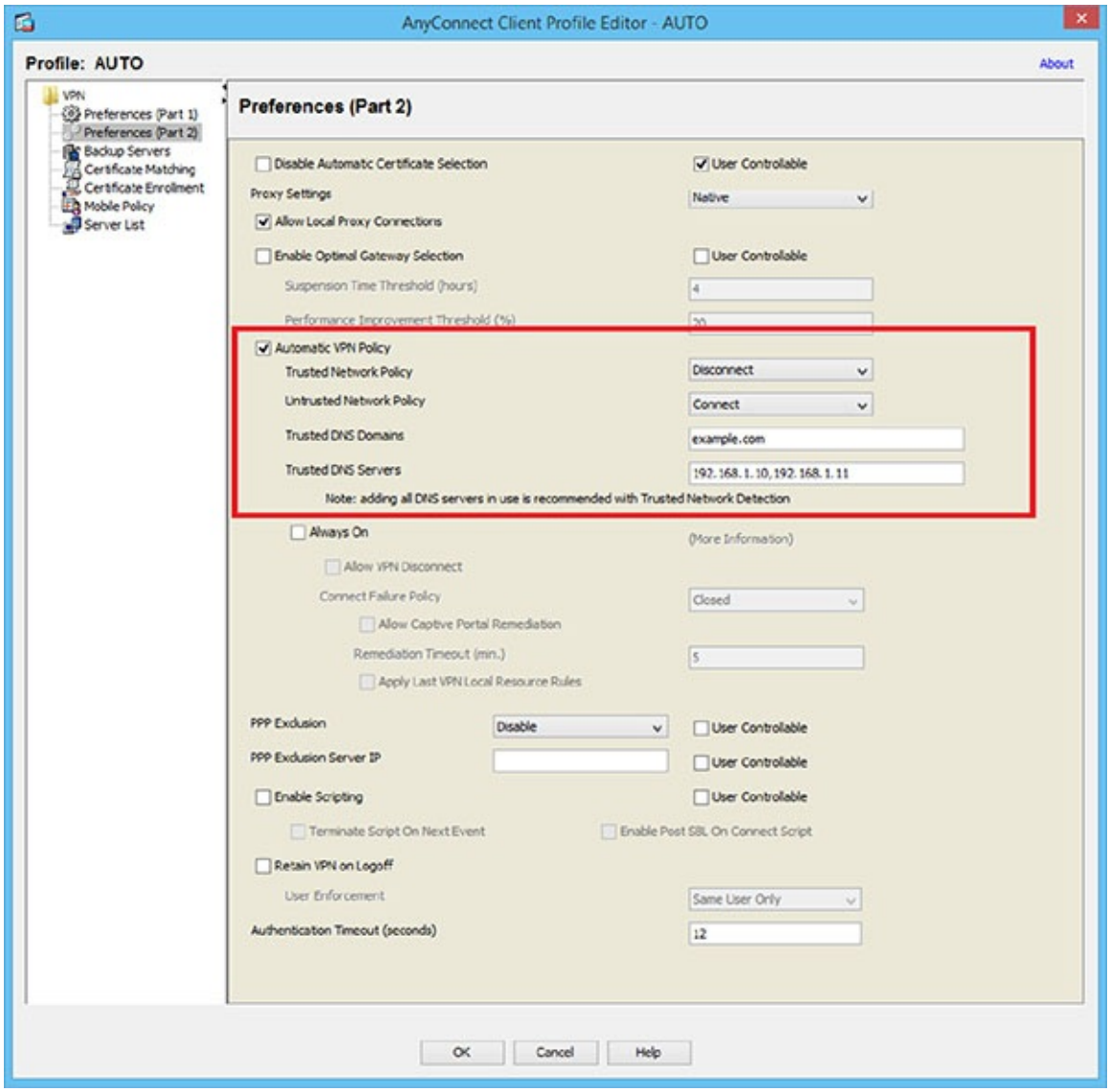

FIGURE 11.13 Preferences (Part 2) window

NAT Traversal

As ESP does not utilize the concept of source and destination ports, NAT has difficulty operating when IPsec traffic arrives at the NAT device. *NAT traversal* encapsulates IPsec within UDP, providing the requisite ports for NAT.

Configuring NAT traversal or NAT-T is done with a simple check box found in the Global Parameters section of IKE in the ASDM. Navigate to Configuration ➢ VPN ➢ IKE ➢ Global Parameters in the ASDM.

Select the interface in the enable IKE box and then select Enable IPSec Over NAT-T, as shown in Figure 11.14 .

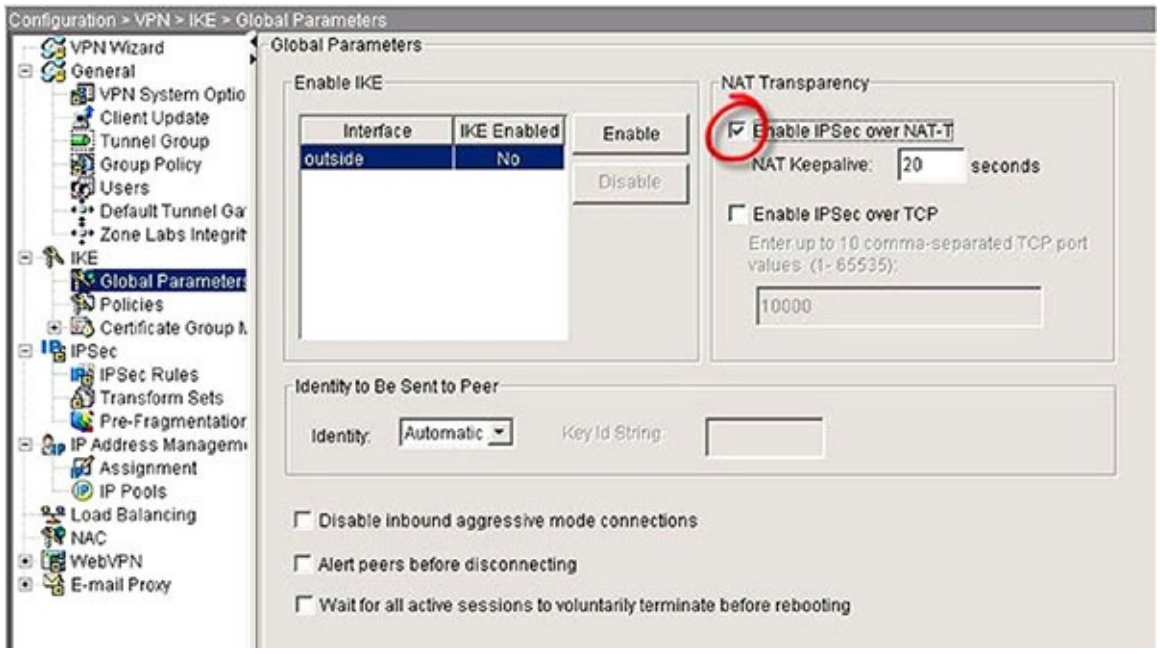

FIGURE 11.14 NAT traversal

Summary

In this chapter, you learned about IPsec and the security services it provides. The chapter discussed the components of IPsec such as ISAKMP, IKE, AH, and ESP. You also learned how to use hairpinning to allow traffic between two hosts to connect to the same VPN interface. Finally, split tunneling and its benefits were discussed.

Exam Essentials

Identify the security services provided by IPsec. They include confidentiality, integrity, origin authentication, anti-replay, and key management.

List the components and delivery modes of IPsec. These include ISAKMP, IKE, AH, and ESP. Delivery modes include transport and tunnel mode.

Describe the operation of hairpinning. Hairpinning can be used to allow traffic between two hosts to connect to the same VPN interface. It is required because of the default rule that an ASA will not forward packets back out the same interface in which they were received.

Describe the operation of split tunneling. When enabled, it allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel.

Review Questions

1. Which IPsec component provides confidentiality?
   A. AH

B. IKE

C. ESP

D. ISAKMP

2. Which IPsec component provides integrity?

A. HMAC

B. IKE

C. ESP

D. ISAKMP

3. Which IPsec component provides only data integrity, origin authentication, and anti-replay protection?

A. HMAC

B. AH

C. ESP

D. ISAKMP

4. Which IPsec component provides key exchange?

A. HMAC

B. AH

C. Diffie-Hellman

D. ISAKMP

5. What is the minimum key length for Suite B algorithms?

A. 64-bit

B. 80-bit

C. 128-bit

D. 160-bit

6. What hashing algorithm is required by the Suite B standard?

A. MD5

B. SHA-1

C. SHA-2

D. AES

7. Which of the following is not a function of IKE?

A. Automatic key generation
B. Automatic key refresh
C. key exchange
D. Negotiation of the security association (SA)

8. Which of the following does not occur in phase 1 of IKE?
A. Negotiates the policy sets.
B. Sets up a secure channel.
C. Authenticates the peer devices to one another.
D. The IPsec transform set is negotiated.

9. Which of the following is true of the Main and Aggressive IKE modes?
A. Main mode uses two messages, and Aggressive mode uses three.
B. Main mode uses three messages, and Aggressive mode uses two.
C. Both modes use three messages.
D. Both modes use two messages.

10. Which of the following is *not* performed during IKE phase 2?
A. Periodic renegotiation of the SA.
B. The SA is established.
C. The IPsec transform set is negotiated.
D. The Diffie-Hellman protocol is used to generate a shared symmetric key.

11. Which of the following is *not* true of IKEv2 when compared with IKEv1?
A. More transactions that result in decreased speed
B. Stronger security through denial-of-service protection
C. Supports EAP as an authentication method
D. Incorporates extensions such as NAT traversal and dead peer detection

12. When using AH in transport mode, which parts of the packet are authenticated?
A. Only the header
B. Only the payload
C. Header and payload
D. None

13. When using ESP in tunnel mode, which parts of the packet are encrypted?

A. Only the header

B. Only the payload

C. Header and payload

D. None

14. Which if the following is *not* true of IPsec in IPv6 and IPv4?

A. IPsec is required in IPv6.

B. In IPv4, AH and ESP are implemented as IP protocol headers.

C. In IPv6, extension headers are used to implement IPsec.

D. In IPv6, the extension header lies between the IPv6 header and the payload.

15. Which of the following is true?

A. By default, an ASA will not forward packets back out the same interface in which it was received.

B. By default, an ASA will forward packets back out the same interface in which it was received.

C. Once a tunnel is operational, all traffic leaving the VPN client need not pass through the tunnel.

D. In IPv4, AH and ESP are implemented as IP protocol headers.

16. Which of the following features can be used to allow traffic to re-enter the end of an IPsec tunnel?

A. Split horizon

B. Hairpinning

C. Split tunnel

D. Poison reverse

17. Which feature, when enabled, allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel?

A. Split horizon

B. Hairpinning

C. Split tunnel

D. Poison reverse

18. Which additional feature must be enabled to use Always-on VPN?

A. MDM

B. Trusted network detection

C. Hairpinning

D. STP

19. What feature encapsulates IPsec within UDP?

A. NAT-T

B. DNSSec

C. Split tunnel

D. Trusted network detection

20. What protocol number is used for ESP?

A. 48

B. 49

C. 50

D. 51

Chapter 12
Configuring VPNs

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**3.2 Remote access VPN**

- Implement basic clientless SSL VPN using ASDM
- Verify clientless connection
- Implement basic AnyConnectSSL VPN using ASDM
- Verify AnyConnectconnection
- Identify endpoint posture assessment

✓**3.3 Site-to-site VPN**

- Implement an IPsec site-to-site VPN with preshared key authentication on Cisco routers and ASA firewalls
- Verify an IPsec site-to-site VPN

Virtual private network (VPN) connections can be configured in two basic forms, as remote access VPNs or as site-to-site VPNs. While one is designed to provide a secure remote access connection for a telecommuter or remote user, the other is designed to provide a secure tunnel to carry all traffic between two locations. In this chapter, you'll learn how to configure and verify both VPN types. Moreover, you'll learn about two different ways to implement the remote access VPN.

In this chapter, you will learn the following:

How to configure and verify a clientless SSL VPN using ASDM

How to implement and verify an AnyConnect SSL VPN using ASDM

How a Cisco endpoint posture assessment can help protect the network from malware and other types of attacks

How to implement and verify an IPsec site-to-site VPN with preshared key authentication on Cisco routers and ASA firewalls

Configuring Remote Access VPNs

Cisco *remote access VPNs* can be deployed either by installing the *AnyConnect client* on the user's device or by configuring the clientless SSL VPN solution in which no client is required on the user device. Additionally, you can use a Cisco clientless connection to deploy the AnyConnect client to the user device. Finally, when combined with a Cisco endpoint posture assessment, the security posture of the device can be verified before allowing the remote device to access the network, helping to protect the network from malware and other threats. In this section, you'll learn how to implement these two types of remote access solutions and examine the benefits of utilizing a Cisco endpoint posture assessment.

Basic Clientless SSL VPN Using ASDM

While the *clientless SSL VPN* can be deployed on the Cisco Adaptive Security Appliance using the command line, it is simpler to do so using the Cisco Adaptive Security Device Manager (ASDM). Before diving into the configuration, it is helpful to look at the protocol that provides confidentiality, integrity, and authentication services for the connection.

SSL/TLS

Transport Layer Security (TLS) is used to provide security services for both the clientless SSL VPN and the AnyConnect VPN. While its predecessor is *Secure Sockets Layer (SSL)*, the term SSL VPN has persisted and is still used to describe the connection even though most modern systems use TLS. These protocols use public key cryptography and digital certificates in their operation. While certificates can be deployed on both the client and the server to enable mutual authentication, in most cases a certificate is deployed only on the server because that can secure the connection as well as when certificates are deployed on both ends.

SSL/TLS has a great deal of flexibility regarding the encryption algorithms, hashing algorithms, authentication mechanisms, and key management protocols that can be used. Figure 12.1 depicts the choices available for each of these components.

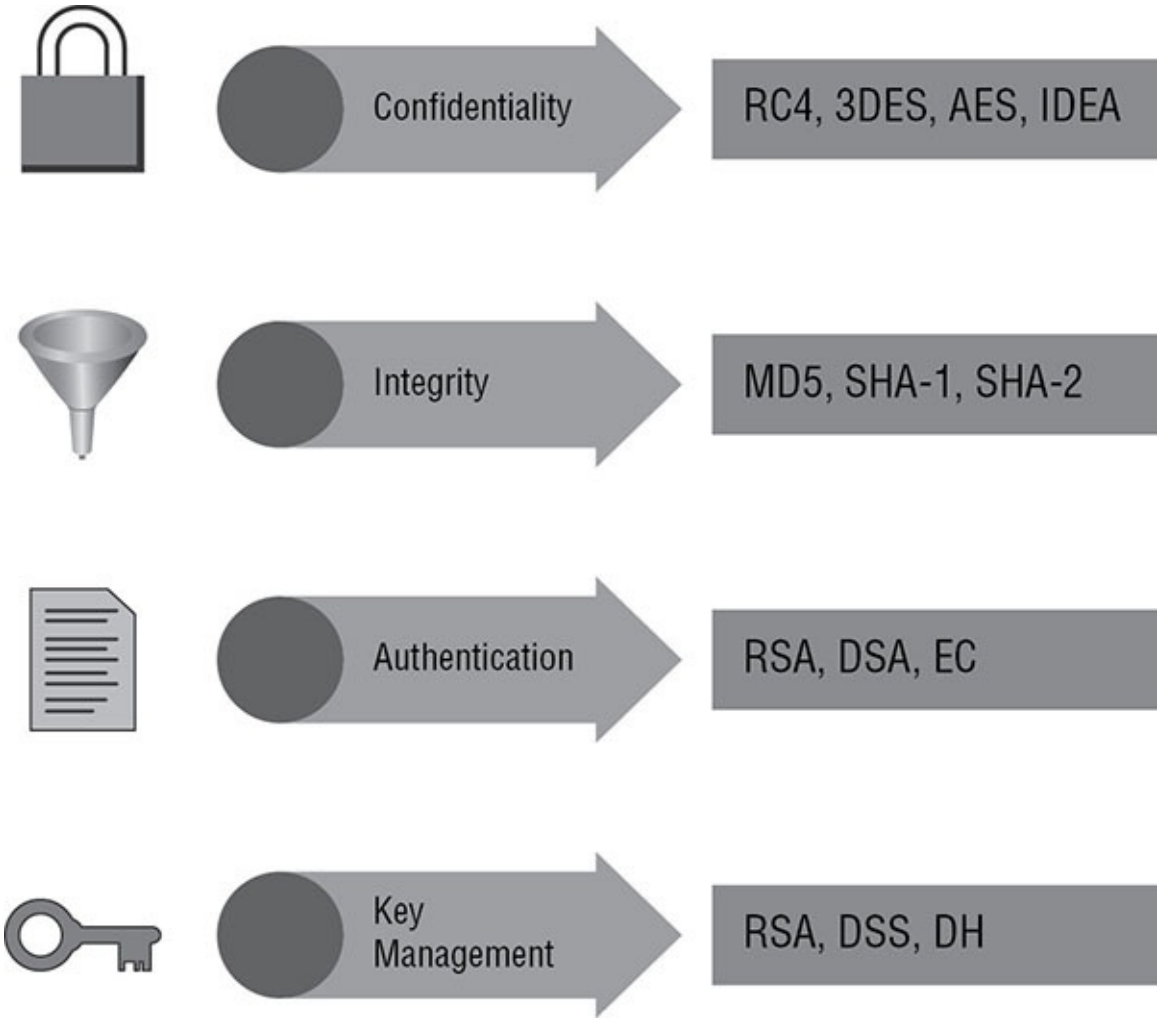

FIGURE 12.1 Supported SSL/TLS algorithms

It is also helpful to understand the process that occurs when one of these connections is established between the client and the server. The steps that occur are as follows:

1. The client initiates the process by starting the exchange of hello packets between the client and the VPN gateway (the ASA). This step allows the two to negotiate and agree on the encryption algorithms, hashing algorithms, authentication mechanisms, and key management protocols to be used.
2. The server transmits its certificate to the client (which will include its public key). If the RSA key exchange algorithm is in use, the client sends a premaster key to the server using the public key of the server to protect the transmission.
3. If mutual authentication is required, the client then sends its certificate to the server, a session key is calculated, and the cipher suite is activated. Integrity will be provided by the selected hashing algorithm (MD5 or SHA-1), and encryption will be provided by the selected cipher (RC4, 3DES, AES, or IDEA).
4. Once the session keys are exchanged, the data transfer begins. When the traffic gets beyond the ASA, the information will be in clear text but will be encrypted between the client and the ASA.

Configuration

When using the Cisco clientless SSL VPN, the remote device uses the browser to connect to an SSL-enabled website on the ASA or on a Cisco router. Once the security appliance has authenticated the user, the server certificate is used to establish the SSL tunnel. Then the security appliance presents the user with a web portal that contains a link to the internal resources that have been made available.

From a high level, the steps to be completed to configure the Cisco clientless SSL VPN are as follows:

1. Enable clientless SSL VPN traffic termination on an ASA interface.
2. Configure clientless SSL server authentication by provisioning an identity certificate and attaching it to the interface.
3. Configure user authentication, which comprises three subtasks.
    a. Create accounts for the VPN users.
    b. Configure a group policy for the VPN users specifying in the policy clientless SSL VPN as the tunneling protocol.
    c. Create a connection profile for the VPN users and connect the policy to the profile.
4. Set up bookmarks that will appear when the users connect to the web portal.

Configuring Clientless SSL VPN

In this procedure, you will configure a clientless SSL VPN using the local user database of the ASA.

1. In the ASDM, navigate to Wizards ➢ VPN Wizards ➢ Clientless SSL VPN Wizard.
2. On the Step 1 page of the wizard, provide an informational description for the connection and click Next.
3. When the Step 2 page appears, give the connection profile a name in the Connection Profile Name box. Just below that, select the interface that will host the connection and click Next.
4. In the Step 3 dialog box, select the Authenticate Using The Local User Database radio button. Click the Add button and create a user account for the user, specifying both a username and a password. Then click Next.
5. On the Step 4 page of the wizard, create a group policy for the user by selecting the Create A New Group Policy radio button and give the policy a name. Then click Next.
6. In the Step 5 dialog box, you will create a bookmark list and then add bookmarks to the list. Just to the right of the Bookmarks List field, click the Manage button. The Configure GUI customization dialog box appears. Click the Add button, and when the Add Bookmark List dialog box appears, give the bookmark list a name. Then click the Add button in this dialog box. When the Select Bookmark Type dialog box appears, accept the URL with the GET or POST method option and click OK.
7. Now you will add a bookmark for a web resource you will make available. In the Add Bookmark dialog box, give the bookmark a name, select the HTTP protocol, and enter the IP address of the server providing this resource. When you have added all the bookmarks you need on this page, click OK.
8. On the Configure GUI Customization page, click OK.
9. In the Step 5 window, ensure that your bookmark list is selected and click Next.
10. Review the summary Page 6 window and click Finish.

Verify a Clientless Connection

Naturally the most effective way to verify the proper configuration of the clientless SSL VPN is to ensure that a connection can be made. This involves the following:

1. Connecting to the site URL
2. Specifying the group configured for the user
3. Entering the name and the password for the user
4. Verifying that the bookmarks appear when authentication is complete

5. Testing the bookmarks to ensure that they connect to the correct resource

Basic AnyConnect SSL VPN Using ASDM

To utilize a *Cisco AnyConnect SSL VPN*, a VPN client called the *AnyConnect client* must be installed on the user device. When configuring the connection, you will make this client available to be downloaded and installed on the user device the first time the user connects, making a manual installation of the client unnecessary.

From a high level, the steps to be completed to configure the Cisco AnyConnect SSL VPN are as follows:

1. Create a connection profile and attach it to the external interface of the ASA.
2. Generate a self-signed certificate for the ASA (or use an existing one if it exists already).
3. Make the AnyConnect client available for download when the user connects.
4. Create an account and password for the user on the ASA.
5. Create a pool of IP addresses that can be issued to AnyConnect clients.
6. Exempt the internal network from the NAT process.
7. Select to allow the web launch of the AnyConnect client.
8. Create a group policy for the remote access connection and assign it to the user.

Configuring AnyConnect SSL VPN

In this procedure, you will configure an AnyConnect SSL VPN using the local user database of the ASA.

1. In the ASDM window, navigate to Wizards ➢ VPN Wizards ➢ AnyConnect VPN Wizard. When the wizard opens, click Next on the first page.
2. Next, on the Connection Profile Identification page, enter a profile name for the connection profile and ensure that VPN Access Interface is set to the Internet interface.
3. On the VPN Protocol page, select SSL. In the Device Certificate With RSA Key drop-down box, select an existing certificate or click Manage and generate a certificate.
4. On the Client Images page, click the Add button. In the Add AnyConnect Client Image window, click the Upload button. Browse to the location of the AnyConnect image file and select the `.pkg` version. Verify the selection by clicking Select, Upload File, OK, and OK.
5. On the Authentication Methods page, create a username and password for the user.
6. On the Client Address Assignment page, click New and create a scope of IP addresses to be available to the AnyConnect clients.
7. On the Network Resolution page, enter the IP address of a DNS server.
8. On the NAT Exempt page, if the ASA is also performing NAT, select the Exempt VPM Traffic From Network Address Translation check box. Click Next.
9. For the AnyConnect Client Deployment step, select Allow Web Launch.
10. On the Summary page, review your settings and click Finish.

Verify an AnyConnect Connection

Again, the most effective way to verify the proper configuration of the AnyConnect SSL VPN is to ensure that a connection can be made and that the client installs and allows full VPN access. This involves the following:

1. Connecting to the site URL
2. Specifying the group configured for the user
3. Entering the name and the password for the user
4. Ensuring that the user is offered the option to install the AnyConnect client
5. Ensuring the client successfully installs
6. Ensuring that the user is given full tunnel VPN access to the network

Endpoint Posture Assessment

The Cisco AnyConnect client also includes modules that can enhance its capabilities. Two of these modules are the ASA Posture module and ISE Posture module. Both modules offer the ability to access an endpoint's compliance with requirements regarding operating system version, antivirus updates, and other security-related issues through an *endpoint posture assessment*. This gives you the ability to verify the security posture before allowing the device access to the network.

While the ASA module performs a server-side assessment, ISE sends the policy requirements to the endpoint, where the assessment then occurs. The ASA module collects the health information in the form of attributes and sends them to the ASA, where the assessment occurs.

Both systems can deny access to the endpoints that fail the assessment, and both offer remediation capabilities as well. Remediation with the ASA module is limited to working with the software present on the endpoint, meaning it can enable, disable, or update that software. ISE quarantines the device and directs it to servers that remediate the issues. Only then is the endpoint allowed full access to the network.

Configuring Site-to-Site VPNs

Site-to-site VPN connections have an endpoint in one location or office and another endpoint in another office. While both SSL and IPsec can be used for these VPNs, this section will focus on the IPsec site-to-site VPN. Also, while the authentication can be done with other means, we will focus on the use of a preshared key.

Implement an IPsec Site-to-Site VPN with Preshared Key Authentication

A Cisco IPsec site-to-site VPN can be configured on an ASA using the ASDM, or it can be set up on a Cisco router. You will learn about both methods in the following sections. Following this, you will learn how to verify the configuration. For both processes, the high-level steps required are as follows:

1. Ensure that all ACLs are compatible with IPsec.
2. Configure an ISAKMP policy that contains the ISAKMP parameters.
3. Define the IPsec transform set, which includes the encryption and integrity algorithms.
4. Create a crypto ACL that defines the traffic types to be sent and protected through the tunnel.
5. Create a crypto map that defines the peers, applies the parameters of the crypto ACL to them, and applies the crypto ACL to the interface.

Cisco Routers

Here you will learn how to do the implementation.

Implement an IPsec Site-to-Site VPN with Preshared Key Authentication with a Cisco Router

In this procedure, you will implement an IPsec site-to-site VPN with preshared key authentication with a Cisco router.

1. Execute the `show run` command and locate the section for the interface where the connection will be configured. Examine the ACL applied to that interface if one exists. Ensure that the following `permit` statements are present and, if not present, apply them to the list, taking care to sequence them in the proper location:

   ```
   permit ahp host ip address of the peer router host ip address of the
   local router

   permit esp host ip address of the peer router host ip address of the
   local router
   permit udp host ip address of the peer router host ip address of the
   local router eq isakmp

   permit udp host ip address of the peer router host ip address of the
   local router eq non500-isakmp
   ```

2. Now define an ISAKMP policy and number it 111. When you are done, the prompt will change, and the next commands will be part of the policy.

   ```
   Router70(config)#crypto isakmp policy 111
   ```

3. Now complete the policy specifying the following settings:

   Authentication: preshared key

   Encryption algorithm 128-bit AES

   1024-bit Diffie-Hellman for key exchange (specify group 5)

   SHA algorithm for integrity

   Security Association lifetime 1 day (86400 seconds)

   Use the following commands for this:

   ```
   Router70(config-isakmp)#authentication pre-share
   Router70(config-isakmp)#encryption aes 128
   Router70(config-isakmp)#group 5
   Router70(config-isakmp)#hash sha
   Router70(config-isakmp)#lifetime 86400
   ```

   Ensure that the peer router has at least one ISAKMP policy that incudes these settings. Remember that policy names and PSKs are case-sensitive.

4. Specify the `ISAKMP` key and the IP address of the peer router at the global configuration prompt. In this case, the peer is at 102.168.5.3, and the PSK is MAC321.

```
Router70(config)#crypto isakmp MAC321 102.168.5.3
```

5. Configure the IPsec transform set by specifying the following:

   Transform set name: AES_SHA

   Mechanism for payload authentication: ESP HMAC

   Mechanism for payload encryption: ESP

   IPsec mode: tunnel (defaults to tunnel)

   Use the following commands for this:

```
Router70(config)#crypto ipsec transform-set AES_SHA esp-aes esp-sha-
hmac
```

6. Create a crypto ACL (an extended access list) that specifies the inbound and outbound traffic that IPsec should protect. In this case, protect all TCP traffic. It will be specified using the source network ID and the destination network ID using wildcard masks. The source network is 10.0.2.0/24, and the destination is 10.0.1.0/24.

```
Router70(config)#access-list 110 permit tcp 10.0.2.0 0.0.0.255
10.0.1.0 0.0.0.255
```

7. Create a crytpo map that specifies the ACL number 110, the transform set name, and the IPsec peer. Use a map name of mymap and set the SA lifetime to 86400.

```
Router70(config)#crypto map mymap 10 ipsec-isakmp
Router70(config-crypto-map)#match address 110
Router70(config-crypto-map)#set peer 102.168.5.3
Router70(config-crypto-map)#set transform-set AES_SHA
Router70(config-crypto-map)#set security-association lifetime 86400
```

8. Apply the crypto map to the interface Serial0/1.

```
Router70(config)#int s0/1
Router70(config)#crypto map mymap
```

ASA Firewalls

When configuring a site-to-site VPN between two *ASA firewalls*, you will in most cases make use of the ASDM. Therefore, you will learn the procedure for doing this.

Implement an IPsec Site-to-Site VPN with Preshared Key Authentication on ASA with the ASDM

In this procedure, you will implement an IPsec site-to-site VPN with preshared key authentication on ASA.

1. In the ASDM, navigate to Wizards ➢ VPN Wizards ➢ Site-to-Site VPN Wizard. On the Introduction screen, click Next.
2. On the Peer Device Identification screen, enter the IP address of the peer ASA device and select the external interface leading to the peer. Click Next.
3. On the Traffic To Protect screen, enter the network ID of the local network in the Local Network field and the network ID of the remote network in the Remote Network field. Click Next.
4. In the Security panel, select Simple Configuration and enter the preshared key for the connection.
5. On the NAT Exempt page, if the ASA is also performing NAT, select the Exempt VPN Traffic From Network Address Translation check box. Then click Next.
6. In the Summary window, verify your selections. When satisfied, select Finish.

Verify an IPsec Site-to-Site VPN

Regardless of the method used to set up the site-to-site VPN, the verification method is the same. You need to generate interesting traffic from one of the sites to the other and verify that the connection is functional. In these two examples, all traffic is interesting traffic, so all you need do is ping from a device in one location to a device in the other location. If the ping succeeds, the connection is working. If the first ping fails, try again and keep in mind that it takes some time to negotiate the security of the SA.

Summary

In this chapter, you learned the value of the Cisco clientless SSL VPN and the steps required to configure it. The chapter also discussed an alternative to this VPN type, the Cisco AnyConnect SSL VPN, which provides a full-table experience but requires client software on the user's device. You also learned about modules in the Cisco AnyConnect client that can provide endpoint posture assessment. Finally, the chapter covered how to implement an IPsec site-to-site VPN with preshared key authentication.

Exam Essentials

Identify the steps to be completed to configure the Cisco clientless SSL VPN. These steps are first to enable clientless SSL VPN traffic termination on an ASA interface and then to

configure clientless SSL server authentication by provisioning an identity certificate and attaching it to the interface. Next configure user authentication and finally create bookmarks for the links to the resources that will appear when the users connect to the web portal.

List the steps to be completed to configure the Cisco AnyConnect SSL VPN. These steps include the following: Create a connection profile and attach it to the external interface of the ASA. Generate a self-signed certificate for the ASA (or use an existing one if it exists already). Generate an identity certificate for the ASA and attach it to the key pair. Make the AnyConnect client available for download when the user connects. Create an account and password for the user on the ASA. Create a pool of IP addresses that can be issued to AnyConnect clients. Exempt the internal network from the NAT process. Select to allow the web launch of the AnyConnect client. Create a group policy for the remote access connection and assign it to the user.

Describe the components that provide endpoint posture assessment. The Cisco AnyConnect client also includes modules that can enhance its capabilities. Two of these modules are the ASA Posture module and the ISE Posture module. Both modules offer the ability to access an endpoint's compliance with requirements regarding operating system version, antivirus updates, and other security-related issues. This gives you the ability to verify the security posture before giving the device access to the network.

List the steps to implement an IPsec site-to-site VPN with preshared key authentication. These steps include the following: Ensure that all ACLs are compatible with IPsec. Configure an ISAKMP policy that contains the ISAKMP parameters. Define the IPsec transform set, which includes the encryption and integrity algorithms. Create a crypto ACL that defines the traffic types to be sent and protected through the tunnel. Create a crypto map that defines the peers, applies the parameters of the crypto ACL to them, and applies the crypto ACL to the interface.

Review Questions

1. Which confidentiality algorithm is not supported for an SSL/TLS VPN?
   A. DES
   B. 3DES
   C. AES
   D. RC4
2. In an SSL/TLS VPN, what function can the DSA algorithm be used for?
   A. Authentication
   B. Integrity
   C. Confidentiality

D. Key management

3. In the SSL connection process, which step occurs last?
   A. Session keys are exchanged.
   B. The server transmits its certificate to the client.
   C. The client sends hello packets.
   D. The client sends its certificate to the server.
4. Which of the following is not a subtask of configuring user authentication for a Cisco clientless SSL VPN connection?
   A. Create a connection profile for the VPN users
   B. Configure a group policy for the VPN users
   C. Create accounts for the VPN users
   D. Create bookmarks for the links to the resources
5. Which of the following is false regarding an endpoint posture assessment?
   A. The ISE module performs a server-side assessment.
   B. Both ISE and ASA posture modules offer the ability to access an endpoint's compliance.
   C. Both systems can deny access to the endpoints that fail the assessment, and both offer remediation capabilities.
   D. The ISE quarantines a noncompliant device and directs it to servers that remediate the issues.
6. When implementing an IPsec site-to-site VPN, in which step are the encryption and integrity algorithms defined?
   A. Creating a crypto map
   B. Creating a crypto ACL
   C. Defining the IPsec transform set
   D. Specifying the ISAKMP key
7. Which of the following commands specified the details of the key exchange algorithm?
   A. `Router70(config-isakmp)#lifetime 86400`
   B. `Router70(config-isakmp)#encryption aes 128`
   C. `Router70(config-isakmp)#group 5`
   D. `Router70(config-isakmp)#authentication pre-share`
8. In the following command, what does the number 10 represent?

```
Router70(config)#crypto map mymap 10 ipsec-isakmp
```

A. Sequence number

B. ACL number

C. Map name

D. SA lifetime

9. Which of the following is possible when certificates are present on both the client and the server?

A. Hairpinning

B. Mutual authentication

C. Online certificate verification

D. Split tunneling

10. Which of the following is *not* a possible authentication mechanism available in the SSL VPN?

A. RSA

B. CHAP

C. DSA

D. EC

11. Which of the following will be included in the certificate the server presents to the client?

A. PSK

B. Private key

C. Transform set

D. Public key

12. What step makes secure data exchange possible?

A. Exchange of hellos

B. Exchange of session keys

C. Exchange of certificates

D. Exchange of credentials

13. In which type of VPN does the user use the browser to connect to an SSL-enabled website?

A. AnyConnect

B. Clientless

C. IPsec with preshared key

D. IPsec site-to-site

14. What is the function of the MD5 algorithm in the SSL VPN process?
    A. Authentication
    B. Integrity
    C. Confidentiality
    D. Key exchange
15. Which of the following defines the traffic types to be sent and protected through the tunnel?
    A. Crypto map
    B. Crypto ACL
    C. IPsec transform set
    D. ISAKMP key
16. What does the following command control?

```
Router70(config-isakmp)#lifetime 86400
```

    A. Authentication timeout
    B. SA lifetime
    C. PSK lifetime
    D. Inactivity timer
17. In the following command, what does AES_SHA define?

```
Router70(config)#crypto ipsec transform-set AES_SHA esp-aes esp-sha-hmac
```

    A. The name of the transform set
    B. The mechanism for the payload authentication
    C. The mechanism for the payload encryption
    D. The tunnel mode
18. Which of the following is *not* a supported key management algorithm in an SSL VPN?
    A. MD5
    B. Quantum
    C. DH
    D. ECC
19. What VPN method requires software on the user device?
    A. IPsec site-to-site

B. AnyConnect

C. Clientless

D. IPsec with PSK

20. What statement is false regarding endpoint posture assessment?

A. The ISE module quarantines a noncompliant device and directs it to servers that remediate the issues.

B. The ISE module is limited to working with the software present on the endpoint.

C. Both systems can deny access to the endpoints that fail the assessment.

D. The ASA module performs a server-side assessment.

Chapter 13
Understanding Firewalls

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**5.1 Describe operational strengths and weaknesses of the different firewall technologies**

- Proxy firewalls
- Application firewall
- Personal firewall

✓**5.2 Compare stateful vs. stateless firewalls**

- Operations
- Function of the state table

Firewalls are part of the foundation of security in a network. They protect the network perimeter and control access between security zones within your networks. You will also typically deploy firewalls in layers, meaning you will place firewalls on each device. Firewalls differ in the way they examine the traffic they are designed to control and in the effect they have on network performance.

In this chapter, you will learn the following:

The operational strengths and weaknesses of the different firewall technologies

The functions of stateful and stateless firewalls

Understanding Firewall Technologies

Firewalls come with a range of abilities and go about their jobs in different ways depending on the job for which they were designed. They can differ in the OSI layer on which they operate and in the types of actions they can take and the attack types they can mitigate. In this section, you'll learn about a variety of these devices. In the section following this one, you'll look at one firewall capability that deserves a section all its own.

Packet Filtering

Packet filtering firewalls are the least detrimental to throughput because they only inspect the header of the packet for allowed IP addresses or port numbers. Although even performing this function will slow traffic, it involves only looking at the beginning of the packet and making a quick allow or disallow decision.

Although packet filtering firewalls serve an important function, they cannot prevent many attack types. They cannot prevent IP spoofing, attacks that are specific to an application, attacks that depend on packet fragmentation, or attacks that take advantage of the TCP handshake. More advanced inspection firewall types are required to stop these attacks.

Proxy Firewalls

Proxy firewalls stand between each connection from the outside to the inside and make the connection on behalf of the endpoints. Therefore, there is no direct connection. The proxy firewall acts as a relay between the two endpoints. Proxy firewalls can operate at two different layers of the OSI model. Both are discussed shortly.

Circuit-level proxies operate at the Session layer (layer 5) of the OSI model. They make decisions based on the protocol header and Session layer information. Because they do not do deep packet inspection (at layer 7 or the Application layer), they are considered application-independent and can be used for wide ranges of layer 7 protocol types.

A *SOCKS firewall* is an example of a circuit-level firewall. This requires a SOCKS client on the computers. Many vendors have integrated their software with SOCKS to make using this type of firewall easier.

A kernel proxy firewall is an example of a fifth-generation firewall. It inspects the packet at every layer of the OSI model but does not introduce the performance hit that an Application layer firewall will because it does this at the kernel layer. It also follows the proxy model in that it stands between the two systems and creates connections on their behalf.

Proxy servers can be appliances, or they can be software that is installed on a server operating system. These servers act like a proxy firewall in that they create the web connection between systems on their behalf, but they can typically allow and disallow traffic on a more granular basis. For example, a proxy server might allow the Sales group to go to certain websites while not allowing the Data Entry group access to these same sites. The functionality extends beyond HTTP to other traffic types, such as FTP and others.

Proxy servers can provide an additional beneficial function called *web caching*. When a proxy server is configured to provide web caching, it saves a copy of all web pages that have been delivered to internal computers in a web cache. If any user requests the same page later, the proxy server has a local copy and need not spend the time and effort to retrieve it from the Internet. This greatly improves web performance for frequently requested pages.

Application Firewall

Application-level proxies perform deep packet inspection. This type of firewall understands

the details of the communication process at layer 7 for the application of interest. An application-level firewall maintains a different proxy function for each protocol. For example, for HTTP the proxy will be able to read and filter traffic based on specific HTTP commands. Operating at this layer requires each packet to be completely opened and closed, making this firewall the most impactful on performance.

Personal Firewall

Personal firewalls may be those that come with an operating system like the Windows Firewall, or they may be third-party host firewalls such as Kaspersky Internet Security or Zone Alarm Pro Firewall. These firewalls, called either *host* or *personal* firewalls, protect only the device on which the software is installed.

While never a replacement for properly positioned network firewalls, they are an excellent complement to the protection provided by the network firewalls, and installing both types of firewalls is an example of exercising the concept of *defense in depth*. This concept prescribes that you should always deploy multiple barriers to unauthorized access.

One key feature that a personal firewall can provide (although in many cases this is not configured by default) is the ability to control egress traffic. This is traffic leaving the device and can help to prevent malware that "calls home" to a command-and-control server from functioning. These firewalls can also help protect systems from other systems inside the network perimeter.

Stateful vs. Stateless Firewalls

One key type of firewall that we saved for the end of this chapter is a *stateful firewall*. Stateful firewalls are those that are aware of the proper functioning of the TCP handshake, keep track of the state of all connections with respect to this process, and can recognize when packets are trying to enter the network that don't make sense in the context of the TCP handshake. Just as a review, Figure 13.1 shows the process.

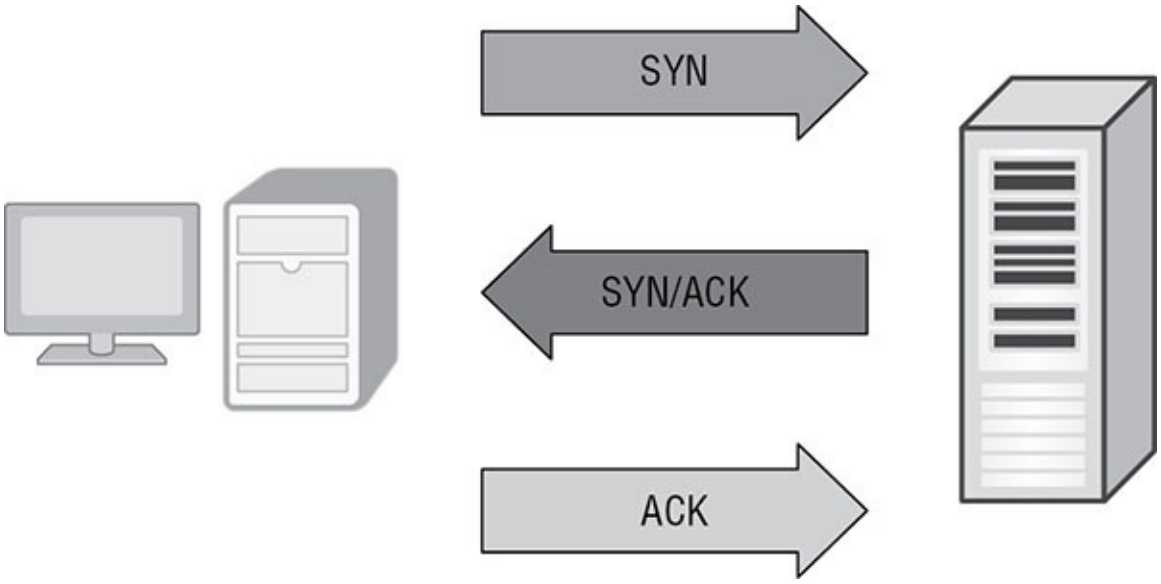

FIGURE 13.1 *TCP three-way handshake*

In this process, a packet should never arrive at a firewall for delivery that has both the *SYN flag* and the *ACK flag* set unless it is part of an existing handshake process, and it should be in response to a packet sent from inside the network with the SYN flag set. This is the type of packet that the stateful firewall would disallow. It also can recognize other attack types that attempt to misuse this process. It does this by maintaining a state table about all current connections and the status of each connection process. This allows it to recognize any traffic that doesn't make sense with the current state of the connection. Of course, maintaining this table and referencing the table causes this firewall type to have more of an effect on performance than a packet filtering firewall.

Operations

Figure 13.2 shows the operation of a stateful firewall.

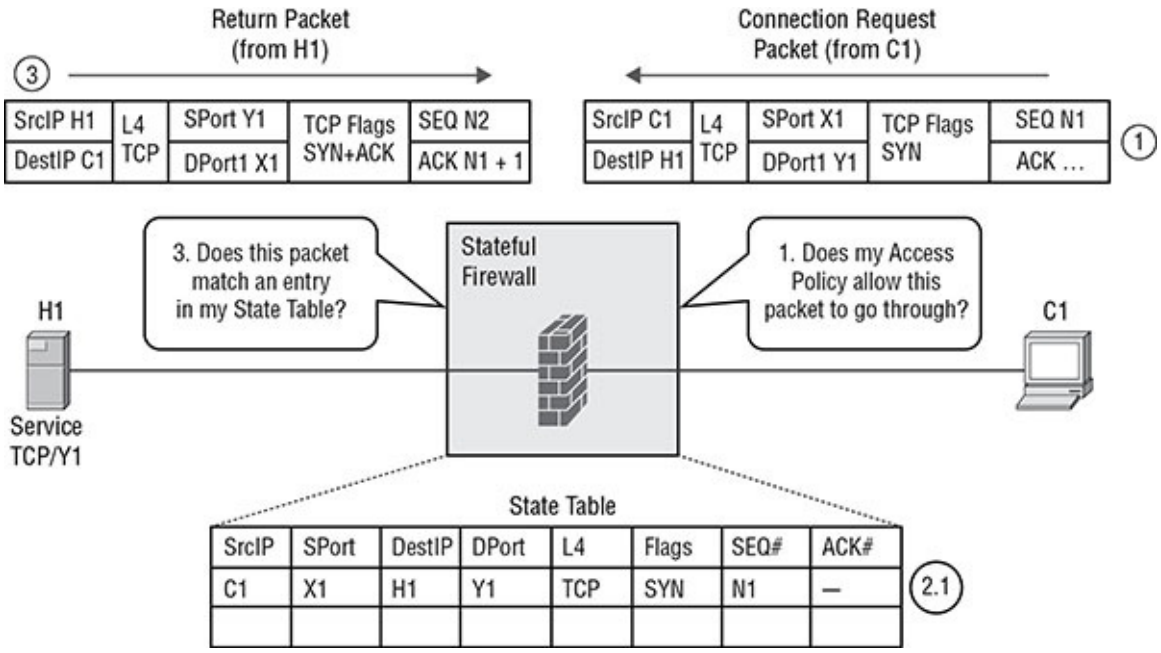

FIGURE 13.2 Stateful firewall operation

The device C1 on the right is sending a SYN packet to the device H1. The firewall permitted and recorded that operation in its state table and will monitor that table whenever a packet arrives at the firewall to ensure that any packets permitted either are connection requests from the inside (SYN packets only) or are part of an existing connection and that all rules of the handshake are enforced. For example, in the scenario, a packet from the outside destined for C1 from H1 with an ACK flag set would be rejected because the next expected packet type in the handshake would be a packet with the SYN and ACK flags set.

State Table

The *state table* is used to monitor all allowed connections. The following are the key items that are typically recorded by a stateful firewall with respect to each connection:

- Source IP address
- Source port number
- Destination IP address
- Destination port number
- IP Protocol
- Flags
- Timeout

Summary

In this chapter, you learned about various firewall technologies such as proxy, application, personal, and stateful firewalls. You learned their strength and weaknesses. You also learned

about stateful firewalls in greater detail and described the relationship between the operation of these firewalls and the TCP three-way handshake. Finally, you learned what is contained in the state table of a stateful firewall.

Exam Essentials

Identify the operational strength and weaknesses of firewall technologies. These include proxy, application, personal, and stateful firewalls. Describe each technology's impact on performance and the features that each provides.

Describe the relationship between the TCP three-way handshake and stateful firewalls. Stateful firewalls understand the three-way handshake and can recognize illegal packets that don't make sense in the TCP connection process.

Identify contents of a state table. Key items that are typically recorded by a stateful firewall with respect to each connection are source port number, destination IP address, destination port number, IP protocol, flags, and timeout.

Review Questions

1. Which firewall technology is the least detrimental to performance?
   A. Proxy
   B. Stateful
   C. Packet filtering
   D. SOCKS
2. Which firewall type operates at the session layer?
   A. Circuit-level proxy
   B. Stateful
   C. Packet filtering
   D. SOCKS
3. Which statement is true of a kernel-level proxy?
   A. Operates at the Transport layer
   B. Considered a fifth-generation firewall
   C. Maintains a state table
   D. Examines only the header
4. Which of the following is not a proxy firewall?

A. Kernel

B. Circuit-level

C. SOCKS

D. Application

5. Which type of firewall is Zone Alarm Pro Firewall?

A. Personal

B. Stateful

C. Packet filtering

D. SOCKS

6. Which value for each connection is not contained in the state table of a stateful firewall?

A. Destination MAC address

B. Source IP address

C. Destination IP address

D. Flags

7. You have selected a firewall that performs deep packet inspection but also creates a performance hit on throughput. What type did you select?

A. Personal

B. Application level

C. Packet filtering

D. SOCKS

8. Which also offers the benefit of web page caching?

A. Personal firewalls

B. Application-level firewalls

C. Proxy servers

D. SOCKS firewalls

9. At what layer of the OSI model do circuit-level proxies operate?

A. Network

B. Transport

C. Application

D. Session

10. Which of the following is most susceptible to IP spoofing attacks?
    A. Packet-filtering firewalls
    B. Application-level firewalls
    C. Proxy servers
    D. SOCKS firewalls
11. Which of the following will be able to read and filter traffic based on specific HTTP commands?
    A. Packet-filtering firewalls
    B. Application-level firewalls
    C. Proxy servers
    D. SOCKS firewalls
12. What is the only legitimate response to a packet with the SYN flag set?
    A. SYN/FIN
    B. ACK
    C. SYN/ACK
    D. FIN
13. A packet was just received with the SYN/ACK flags set. What data structure will a stateful firewall use to determine whether this packet is allowed?
    A. ARP cache
    B. Routing table
    C. DNS resolver cache
    D. State table
14. Installing both personal and network firewalls is an example of exercising what concept?
    A. Defense in depth
    B. Separation of duties
    C. Least privilege
    D. Need to know
15. A SOCKS firewall is an example of which firewall technology?
    A. Packet-filtering firewalls
    B. Circuit-level firewall
    C. Proxy servers

D. Stateful firewalls

16. Which traffic type would be accepted by a stateful firewall?
    A. A SYN/ACK packet that is not related to a current connection
    B. An ACK packet that is in response to a SYN packet in a current connection setup
    C. A SYN/ACK packet in response to a SYN packet in a current connection setup
    D. An ACK packet that is not related to a current connection
17. Which of the following is *not* a proxy firewall?
    A. SOCKS firewalls
    B. Circuit-level firewalls
    C. Stateful firewalls
    D. Kernel-level firewalls
18. Which statement is *not* true of personal firewalls?
    A. May be those that come with an operating system like the Windows Firewall or may be third-party hosted firewalls
    B. Protect only the device on which the software is installed
    C. Can control egress traffic
    D. Can be a replacement for properly positioned network firewalls
19. Which firewall technology is the most detrimental to performance?
    A. Application level
    B. Stateful
    C. Packet filtering
    D. SOCKS
20. Which firewall type operates at the Network and Transport layers?
    A. Circuit-level proxy
    B. Packet filtering
    C. Stateful
    D. SOCKS

Chapter 14
Configuring NAT and Zone-Based Firewalls

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**5.3 Implement NAT on Cisco ASA 9.*x***

- Static
- Dynamic
- PAT
- Policy NAT
- Verify NAT operations

✓**5.4 Implement zone-based firewall**

- Zone to zone
- Self-zone

Network Address Translation (NAT) is a feature found in firewalls and many router platforms that allows for the translation of private IP addresses to public IP addresses at the network edge. While one of the driving forces behind the development of NAT was the conservation of public IPv4 address space, NAT also has a security component in that the process helps to hide the interior addressing scheme. Zone-based firewalling is an approach that makes traffic filtering decisions between *zones* rather than by specific IP addresses. In this chapter, you will learn how to implement several types of NAT and configure zone-based firewalling.

In this chapter, you will learn the following:

How to implement NAT on Cisco ASA 9.*x* platforms

How to implement zone-based firewalls

Implementing NAT on ASA 9.*x*

There are three types of NAT that can be implemented. This section discusses how these three types operate, and you'll learn how to implement each type on the Adaptive Security

Appliance (ASA).

In static NAT, each private IP address is mapped to a public IP address. While this does not save any of the public IPv4 address space, it does have the benefit of hiding your internal network address scheme from the outside world.

In dynamic NAT, a pool of public IP addresses is obtained that is at least equal to the number of private IP addresses that require translation. However, rather than mapping the private IP addresses to the public IP addresses, the NAT device maps the public IP addresses from the pool on a dynamic basis much like a DHCP server does when assigning IP addresses.

Finally, *Port Address Translation (PAT)* is a form of NAT in which all private IP addresses are mapped to a single public IP address. This provides both benefits of saving the IPv4 address space and hiding the network address scheme. This system is called PAT because the ephemeral port numbers that devices choose as the source port for a connection (which are chosen randomly from the upper ranges of the port numbers) are used to identify each source computer in the network. This is required since all devices are mapped to the same public IP address.

When configuring NAT on the ASA, you need to understand that it uses an object-oriented approach. In other words, an object is created for each host, for each translated address, and for each service that is used in the translation process. Translations are configured as network objects. A network object is defined as a single address or as a network ID.

The resulting host or network defined in a network object is used to represent the private IP address prior to translation. When ACLs are used to define traffic allowed from a lower-security interface to a higher-security interface, these pretranslation objects are referenced.

The ASA uses a NAT table to hold the translations. This table has three sections. When an outgoing packet arrives at the ASA, the sections are read from top to bottom, and the first translation match is applied. The three sections are as follows:

Manual NAT This contains translations that have been defined to be applied by the appliance before the other sections are consulted. These translations are typically very specific and may indicate a translation on both the source and destination IP addresses.

Auto NAT In this section, also called *object NAT*, translations that are defined on the object itself are contained. These translations, one for each object, are typically either static translations for servers that must be reached from the outside world (and require the same public IP address always) or dynamic translations for clients trying to reach the Internet.

Manual NAT after Auto NAT This contains more general translations not handled by the first two sections. These are used only when no translation matches in the first two sections.

If a packet doesn’t match any of the mappings found in any of the three tables, the packets are sent untranslated.

Static

To configure a *static NAT* translation, follow the steps in the next procedure.

Configuring Static NAT

In this procedure, you will create a static NAT mapping for a device.

1. Connect to the ASA using the Adaptive Security Device Manager (ASDM).
2. Navigate to Configuration ➢ Firewall ➢ Network Objects ➢ Groups. Select Add Network Object. Define the parameters of this object. Enter the type and the IP address of the device to be translated with the static mapping. Ensure that this is the pretranslation IP address.
3. In the NAT section of the Add Network Object dialog box, select the Add Automatic Address Translation Rules check box and select Static as the type in the drop-down box just below the Add Automatic Address Translation Rules check box.
4. Just below the drop-down box where you select Static is the Translated Addr field. In the Translated Addr field, click the Browse button. You can browse for objects that have been created here, but you will be creating a new object, so click the Add button at the top of the page.
5. When the Add Network Object dialog box appears, enter a name for the translated object and the address type and public IP address to which the device should be translated. Then click OK.
6. Back on the Add Network Object page where you defined the pretranslation information, click the Advanced button in the NAT section. In the Advanced NAT Settings dialog box, select the source interface for the translation and the destination interface. These will be network objects that would need to have been created previously to represent the internal and external interfaces on the ASA. You will choose these from a drop-down box.
7. Click OK and then Apply. The configuration is now complete.

Dynamic

To configure dynamic NAT translation, follow the steps in the next procedure.

Configuring Dynamic NAT

1. Connect to the ASA using the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Network Objects ➢ Groups. Select Add Network Object. Define the parameters of this object. Enter the type and the IP address of the device to be translated with the static mapping. Ensure that this is the pretranslation IP address.
3. In the NAT section of the Add Network Object dialog box, select the Add Automatic Address Translation Rules check box and select Dynamic as the type in the drop-down box just below the Add Automatic Address Translation Rules check box.
4. Just below the drop-down box where you select Static is the Translated Addr field. In the Translated Addr field, click the Browse button. You can browse for objects that have been created here, but you will be creating a new object, so click the Add button at the top of the page.
5. In this case, the object you will be creating will be a range of public IP addresses, which you will name Translated Pool. Enter a range of addresses using the Start Address and End Address fields. While you are creating only one mapping to the pool in this exercise, in the real world ensure that you have enough public IP addresses in the pool for the private address to be translated.
6. Back on the Add Network Object page where you defined the pretranslation information, choose the new network object by double-clicking it and then click the Advanced button in the NAT section. In the Advanced NAT Settings dialog box, select the source interface for the translation and the destination interface. These will be network objects that would need to have been created previously to represent the internal and external interfaces on the ASA. You will choose these from a drop-down box.
7. Click OK and then Apply. The configuration is now complete.

PAT

To configure PAT translation, follow the steps in the next procedure.

Configuring PAT

1. Connect to the ASA using the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Network Objects ➢ Groups. Select Add Network Object. Define the parameters of this object. Enter the type and the IP address of the device to be translated with the static mapping. Ensure that this is the pretranslation IP address.
3. In the NAT section of the Add Network Object dialog box, select the Add Automatic Address Translation Rules check box and select Dynamic PAT (Hide) as the type in the drop-down box just below the Add Automatic Address Translation Rules check box.
4. In this case, you are not mapping to an individual IP address or to a pool of IP addresses; you will be mapping to the Internet-facing interface of the ASA. When you do this with PAT (Hide) selected, *all* mappings will use the public address configured on that Internet interface. Use the Browse button to browse to the Internet-facing interface on the ASA. If an object has not been created for the interface, do so now by specifying its public IP address.
5. Back on the Add Network Object page where you defined the pretranslation information, choose the new network object by double-clicking it and then clicking the Advanced button in the NAT section. In the Advanced NAT Settings dialog box, select the source interface for the translation and the destination interface. These will be network objects that would need to have been created previously to represent the internal and external interfaces of the ASA. You will choose these from a drop- down box.
6. Click OK and then Apply. The configuration is now complete.

Policy NAT

In some scenarios, you may need more options than are available with Auto NAT (as you will see in the next procedure), or you may need to specify exceptions to the Auto NAT rules. By using the Manual NAT section, these options will be available to you. This section also has the advantage of being checked for a translation match before the other two sections. When you do this, it is also called *Policy NAT*. It is also sometimes called *Twice NAT* because the same rule can perform translation in both directions (translating not only the address in the device inside the network outgoing but also the IP address of the exterior device incoming).

In the scenario you will use in the next procedure, you will use Policy NAT to create a mapping for an internal device that is effective *only* when the internal device is communicating with one specific exterior device and *not* effective otherwise.

To configure Policy NAT to support this scenario, follow the steps in the next procedure.

Configuring Policy NAT

1. Connect to the ASA using the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Objects ➢ Network Objects/Groups. Select Add Network Object.
3. Create three network objects: one for the private IP address of the internal device, one for the public IP address to which the internal device will be mapped, and one for the private IP address to which the external device will be mapped incoming. Define the parameters of each object. When you are finished, click Apply.
4. Now you will define the manual translation that will apply *only* between these two systems. Navigate to Configuration ➢ Firewall ➢ NAT Rules.
5. The NAT Rules table appears. When you configure manual NAT entries, they can be applied either before or after Network Object NAT rules such as those you configured in the earlier procedures. In this case, you want this rule to apply before those rules do, so click Add and then Add NAT Rule before "Network Object" NAT Rules. The Add NAT Rule box appears.
6. The top section of the Add NAT Rule dialog box is where you configure how the packet will be identified for transition using this rule. In the Source Interface field, select Any from the drop-down box, and in the Source Address field use the drop-down box to select the object you created in step 3 representing the private IP address of the internal device.
7. In the Destination Interface field, select Any from the drop-down box, and in the Destination Address field use the drop-down box to select the object you created in step 3 representing the public IP address of the external device.
8. Now that you have defined the match parameters for the translation, you need to configure the translation. In the Action: Translation Packet section in the Source NAT Type drop-down box, select Static. In the Source Address drop-down box, select the object you created in step 3 representing the public IP address to which the internal device should be translated. In the Destination Address field, select Original from the drop-down box.
9. Select OK and then Apply. The configuration is now complete.

Verifying NAT Operations

There are several ways to verify that NAT is operating correctly. They include viewing the NAT translations in the translation table using the `show xlate` command, and in cases where

you are not getting any NAT translations, you can view the configuration and check for errors using the `show nat` command.

Viewing Translations

Using the `show xlate` command on an ASA on which PAT has been configured, you can see in the following output that three translations have occurred. As PAT is in use, all three have received the same public IP address.

```
hostname# show xlate

3 in use, 3 most used
PAT Global 103.61.3.9(0) Local 10.1.1.15 ICMP id 340
PAT Global 103.61.3.9(1024) Local 10.1.1.15(1028)
PAT Global 103.61.3.9(1024) Local 10.1.1.15(516)
```

The following is sample output from the `show xlate detail` command. It shows the translation type and interface information with three active PATs.

The `r` flag indicates that the translation is PAT. The `i` flag indicates that the translation applies to the inside address port.

```
hostname# show xlate detail

3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:103.61.3.9/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:103.61.3.9/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:103.61.3.9/0 flags ri
```

Viewing the Configuration

Using the `show nat` command, you can view the configuration. In the following output, there is a single static translation configured in the inside interface that translates the host at 192.168.5.6 to 128.10.6.2. You can also see that there have been no translations (hits) in either direction using this configuration.

```
hostname(config)# show nat

NAT policies on Interface inside:
  match ip inside host 192.168.5.6 outside any
    static translation to 128.10.6.2
    translate_hits = 0, untranslate_hits = 0
```

Configuring Zone-Based Firewalls

Zones are collections of networks reachable over a router interface. Zone pairs are used to define a unidirectional firewall policy. The direction is indicated by specifying the source and destination zones. There is one special type of zone that will be covered in the next section.

When zone-based firewalling is used, each interface (including both physical and virtual interfaces) is assigned to a zone, and a policy is applied to traffic moving between zones. These configurations use a syntax known as the *Cisco Common Classification Policy Language*. When using the Cisco Common Classification Policy Language, *class maps* are used to define traffic classes, and *policy maps* are used to apply policies (actions) to these traffic classes. Finally, *service policies* are used to activate policy maps on zone pairs.

While only a single service policy can be used on a zone pair, the policy maps within can include multiple class maps. These class maps will be checked for a traffic match in the order in which they are configured. If a match is not found in the first map, the second will be consulted. When there are no matches, the default policy will be applied to the traffic. Figure 14.1 shows this logic.

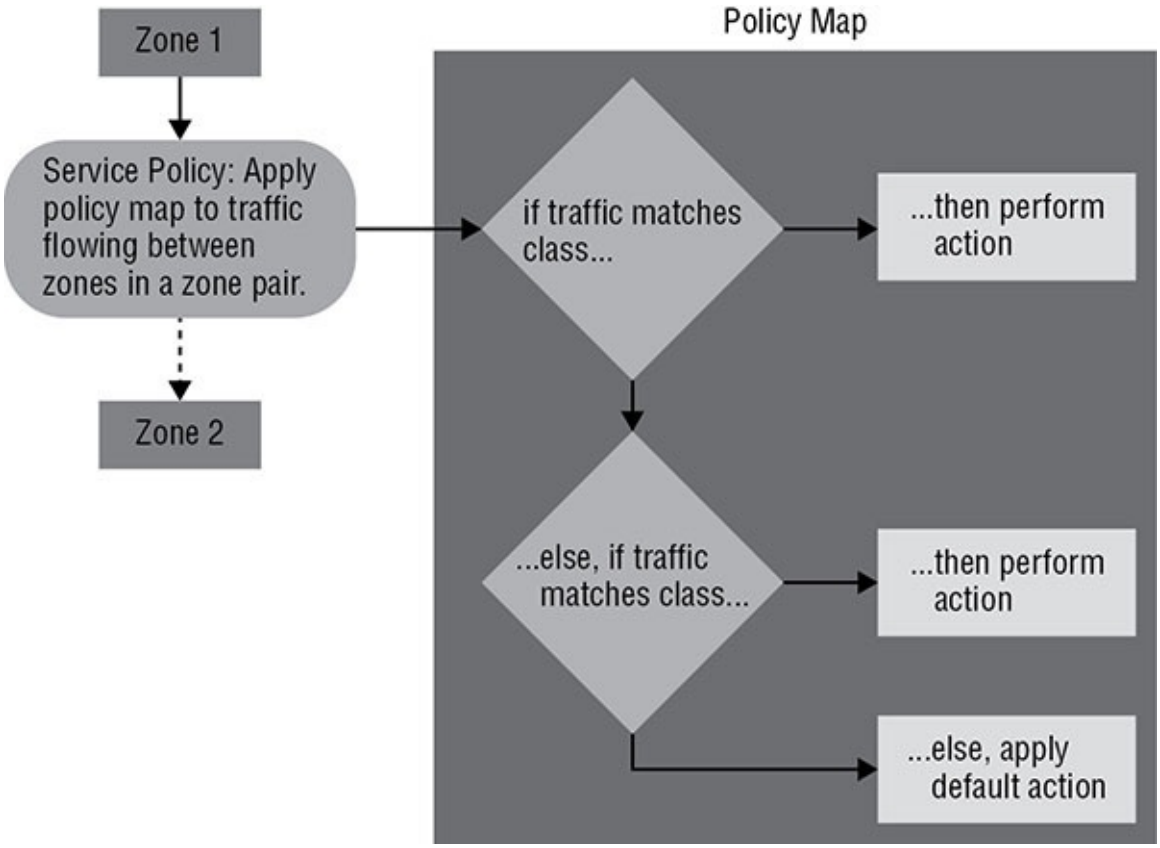

FIGURE 14.1 Multiple class maps

Moreover, these class maps can be used in more than one service policy. In Figure 14.2 , two class maps have been created, and they have both been used in two different service polices.

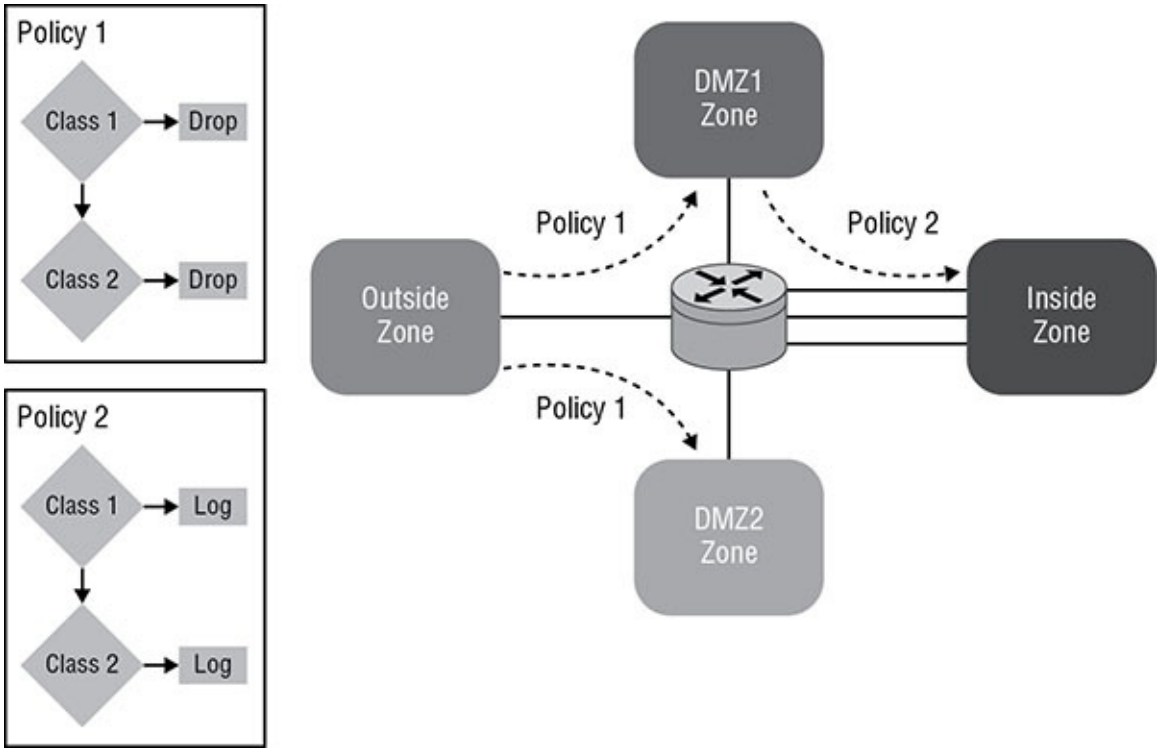

FIGURE 14.2 Reuse of class maps

Class Maps

Class maps have two parts; the first identifies the traffic, and the second specifies an action. A *match* statement is used to specify the traffic and can match traffic based on the following:

- An ACL
- A protocol
- Another class map

The actions that can be defined using *action* statements. The actions can be as follows:

- *Inspect*: Triggers stateful packet inspection
- *Drop*: Denies traffic
- *Pass*: Permits traffic

Default Policies

When no class map matches the traffic type, the *default policy* is invoked. This policy's actions depend on whether the interface has been assigned to a zone and, if so, what policy is currently in effect for that zone pair if it exists. Sound complicated? It can be. Figure 14.3 shows the rules.

Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy exists?	Result
No	No	N/A	N/A	No impact of zoning or policy
Yes	No	N/A	N/A	DROP
No	Yes	N/A	N/A	DROP
Yes (zone 1)	Yes (zone 1)	No	N/A	PASS
Yes	Yes	No	N/A	DROP
Yes	Yes	Yes	No	DROP
Yes	Yes	Yes	Yes	Policy Actions
*Intrazone policy support was introduced in Cisco IOS release 15.0(1)M				

FIGURE 14.3 Default policies

Figure 14.3 applies to traffic that is *not* coming from or destined to the router (self-zone). When that is the case, the rules are as shown in Figure 14.4 .

Source interface member of zone?	Destination interface member of zone?	Zone pair exists?	Policy exists?	Result
Self	Yes	No	—	PASS
Self	Yes	Yes	No	PASS
Self	Yes	Yes	Yes	Policy actions
Yes	Self	No	—	PASS
Yes	Self	Yes	No	PASS
Yes	Self	Yes	Yes	Policy actions

FIGURE 14.4 Default policies (self-zone)

Understanding the Self-Zone

The *self-zone* is a special zone that has no interface members. It applies to any traffic destined for the router rather than traffic that the router is routing. An example of this type of traffic would be traffic to manage the device using SSH. It also applies to traffic generated by the router. The traffic going from the router back to the device making the SSH connection to manage the device would be an example of such router-generated traffic.

Configuring Zone-to-Zone Access

The firewall you will use in the following procedure has three interfaces: one connected to the Internet, one connected to the LAN, and another connected to the DMZ. To configure zone-

based policies to support this scenario, follow the steps in the next procedure.

Configuring Zone-Based Firewall

In this procedure, you will configure a policy that performs stateful inspection of HTTP and FTP traffic coming to the DMZ from the Internet.

1. Define three security zones: Inside, Outside, and DMZ. Use the following commands to do so:

```
RTR64(config)#zone security inside
RTR64(config)#zone security outside
RTR64(config)#zone security dmz
```

2. Assign each interface to its proper zone.

```
RTR64(config)#int gi0/1
RTR64(config-if)#zone-member inside
RTR64(config)#int gi0/2
RTR64(config-if)#zone-member outside
RTR64(config)#int gi0/3
RTR64(config-if)#zone-member dmz
```

3. Create a class map that defines the traffic. In this case, that traffic will be HTTP or FTP. The map will be named HTTP_FTP_filter and will perform stateful inspection of the HTTP traffic.

```
RTR64(config)#class-map type inspect match-any HTTP_FTP_filter
RTR64(config-cmap)#match protocol http
RTR64(config-cmap)#match protocol ftp
```

4. Define a policy map named DMZ_inspect that specifies traffic that matches the HTTP_FTP_filter class map.

```
RTR64(config)#policy-map type inspect DMZ_inspect
RTR64(config-pmap)#class type inspect HTTP_FTP_filter
RTR64(config-pmap-c)#inspect
```

5. Define a zone pair called outside_to_DMZ with the outside zone being the source and the DMZ zone being the destination.

```
RTR64(config)#zone-pair security outside_to_DMZ source outside
destination dmz
```

6. Apply the DMZ_inspect policy to the zone pair called outside_to_DMZ.

```
RTR64(config-sec-zone-pair)#service-policy type inspect DMZ_inspect
```

The configuration is now complete.

Summary

In this chapter, you learned about the three forms of NAT: static NAT, dynamic NAT, and PAT. You also learned about the NAT options available in the ASA. You learned about the benefits of NAT and how to configure it and verify its operation. Class maps, policy maps, and service policies and their respective functions in a zone-based firewall were covered as well. Finally, the steps to configure and verify a zone-based firewall ended the chapter.

Exam Essentials

Identify the forms of Network Address Translation (NAT). These include static NAT, dynamic NAT, and Port Address Translation (PAT).

Describe the three sections of the NAT table in the ASA. The Manual NAT section represents translations that have been defined to be applied by the appliance before the other sections are consulted. The Auto NAT section represents translations that are defined on the object itself. The Manual NAT After Auto NAT section contains more general translations not handled by the first two sections.

Identify benefits of policy NAT. In some scenarios, you may need more options than are available with Auto NAT, or you may need to specify exceptions to the Auto NAT rules. By using the Manual NAT section, these options will be available to you. This section also has the advantage of being checked for a translation match before the other two sections.

Verify NAT operations. There are several ways to verify that NAT is operating correctly. They include viewing the NAT translations in the translation table using the `show xlate` command, and in cases where you are not getting any NAT translations, you can view the configuration and check for errors using the `show nat` command.

Describe the components of a zone-based firewall configuration. *Class maps* are used to define traffic classes, *and policy maps* are used to apply policies (actions) to these traffic classes. Finally, *service policies* are used to activate policy maps on zone pairs.

List the steps to configure zone-to-zone access. From a high level, to configure zone-to-zone access, the following steps must be performed: 1) define zones, 2) define zone pairs, 3) define class maps that define traffic, 4) define policy maps that apply actions to the class maps, 5) apply policy maps to zone pairs, and 6) assign interfaces to zones.

Review Questions

1. In which type of NAT is each private IP address manually mapped to a public IP address?
   A. Dynamic
   B. Static
   C. PAT

D. SAT

2. Which section of the NAT table in the ASA is read last?

   A. Auto NAT

   B. Manual NAT

   C. Dynamic NAT

   D. Manual NAT After Auto NAT

3. You need to create a mapping for an internal device that is effective *only* when the internal device is communicating with one specific exterior device and *not* effective otherwise. What type of NAT must you use?

   A. Auto NAT

   B. Static NAT

   C. Dynamic NAT

   D. Policy NAT

4. What command generated the following output?

```
3 in use, 3 most used
PAT Global 103.61.3.9(0) Local 10.1.1.15 ICMP id 340
PAT Global 103.61.3.9(1024) Local 10.1.1.15(1028)
PAT Global 103.61.3.9(1024) Local 10.1.1.15(516)
```

   A. `show nat`

   B. `show nat detail`

   C. `show xlate`

   D. `show pat`

5. In the following command output, what does the `r` stand for?

```
TCP PAT from inside:10.1.1.15/1026 to outside:103.61.3.9/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:103.61.3.9/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:103.61.3.9/0 flags ri
```

   A. Routed

   B. Remote

   C. Port Address Translation

   D. Reverse

6. Which of the following are collections of networks?

   A. Zone pairs

   B. Zones

C. Policy maps

D. Class maps

7. A match statement can be based on all of the following except which one?

A. An ACL

B. Protocol

C. Another class map

D. Device name

8. Which of the following actions triggers stateful inspection of the traffic?

A. Drop

B. Permit

C. Inspect

D. Pass

9. Which zone has no interface members?

A. DMZ

B. Self

C. Inside

D. Outside

10. In which type of NAT are all private IP addresses mapped to a single public IP address?

A. Dynamic

B. Static

C. PAT

D. SAT

11. In the following command output, what does the value 21505 represent?

```
TCP PAT from inside:10.1.1.15/1026 to outside:103.61.3.9/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:103.61.3.9/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:103.61.3.9/0 flags ri
```

A. Destination port number

B. Sequence number

C. Source port number

D. Acknowledgment number

12. Which of the following is used to define traffic classes?

A. Service policy
B. Zones
C. Policy maps
D. Class maps

13. What command defines a security zone?
A. Zone member
B. Zone security
C. Set zone
D. Zone

14. Traffic to manage the device using SSH would belong to what zone?
A. Inside
B. DMZ
C. Self
D. Outside

15. What command assigns an interface to a zone?
A. `zone-member`
B. `zone-security`
C. `set zone`
D. `zone`

16. Which of the following is used to apply actions to traffic classes?
A. Service policy
B. Zones
C. Policy maps
D. Class maps

17. Which of the following is used to define a unidirectional firewall policy?
A. Zone pairs
B. Zones
C. Policy maps
D. Class maps

18. In the following command output, what does the `i` stand for?

```
TCP PAT from inside:10.1.1.15/1026 to outside:103.61.3.9/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:103.61.3.9/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:103.61.3.9/0 flags ri
```

A. Inside address port

B. Interior

C. IGP

D. Static NAT

19. In which sections of the NAT table in the ASA are translations defined on the object itself?

A. Auto NAT

B. Manual NAT

C. Dynamic NAT

D. Manual NAT After Auto NAT

20. In which type of NAT is a pool of public IP addresses obtained that is at least equal to the number of private IP addresses that require translation?

A. Dynamic

B. Static

C. PAT

D. SAT

Chapter 15
Configuring the Firewall on an ASA

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x**

- Configure ASA access management
- Configure security access policies
- Configure Cisco ASA interface security levels
- Configure default Cisco Modular Policy Framework (MPF)
- Describe modes of deployment (routed firewall, transparent firewall)
- Describe methods of implementing high availability
- Describe security contexts
- Describe firewall services

There are many additional firewall concepts you also should understand beyond configuring zone-based firewalling and network address translation. In this chapter we'll look at some other firewall services as well as discuss the difference between a routed and a transparent firewall. Moreover, we'll cover security contexts and configuring ASA management access. Finally, toward the end of this chapter the *Modular Policy Framework* approach to configuration will be covered.

In this chapter, you will learn the following:

- Configuring ASA access management
- Configuring security access policies
- Configuring Cisco ASA interface security levels
- Configuring the default Cisco Modular Policy Framework (MPF)
- Modes of deployment (routed firewall, transparent firewall)
- Methods of implementing high availability
- Security contexts

- Firewall services

Understanding Firewall Services

The Cisco ASA 9.x firewall series (which is the firewall tested in the CCNA Security exam) has a rich set of features to offer. While it certainly can perform the firewall duties we have come to expect from any enterprise-level firewall, such as traffic filtering and control, it also offers many other functions. Among these are:

Application Inspection Control (AIC)—Also called application protocol control, this feature verifies the conformance of major application layer protocol operations to RFC standards. It can help prevent many of the tunneling attempts and application layer attacks that violate protocol specifications.

Network Address Translation (NAT)—As you learned in Chapter 14, the ASA supports many implementations of NAT including policy NAT, inside and outside NAT, one-to-one and one-to-many NAT, and port forwarding (static NAT)

IP Routing—The ASA has routing capabilities including static and dynamic routing with support for all major routing protocols such as EIGRP, RIP, OSPF, and BGP.

IPv6 support—The ASA supports IPv6 networking natively and can control access between IPv6 security domains.

DHCP—The ASA can be integrated as either a DHCP server or a DHCP client.

Multicast support—The ASA natively integrates with multicast networks supporting Internet Group Management Protocol (IGMP) and both Protocol Independent Multicast Sparse Mode (PIM-SM) and bidirectional Protocol Independent Multicast (PIM).

Understanding Modes of Deployment

The ASA can be deployed in one of two modes, routed and transparent. The mode you choose will depend on requirements and needs. In this section, we differentiate these two modes of operation.

Routed Firewall

In router mode, the ASA is serving as a router and thus each of its interfaces will reside in a separate IP subnet. It can use all major routing protocols including RIP, EIGRP, OSPF, and BGP. In environments where static routing is in use, it can use IP SLA to perform static route tracking to detect when one static route is unavailable and therefore switch to a second static route.

Transparent Firewall

In transparent mode, the ASA is not acting as a router and assumes a layer 2 identity much as a

switch does. This makes the ASA transparent to devices on either side (from a layer 3 perspective); thus the name *transparent mode*. As with a switch, however, it is possible to configure the ASA with a management IP address for connecting to and managing the ASA.

Understanding Methods of Implementing High Availability

Regardless of whether the ASA is operating in routed or transparent mode, it is providing valuable services to the network. Therefore, providing high availability for the ASA and thus for the services it provides is highly desirable. The ASA has several redundancy options available to satisfy this need. In this section we'll cover three ways that multiple ASAs can be deployed to provide this redundancy.

Active/Standby Failover

In *Active/Standby failover* two security appliances are deployed with only one of the appliances processing traffic while the second one serves as a hot standby. This deployment model is shown in Figure 15.1 .

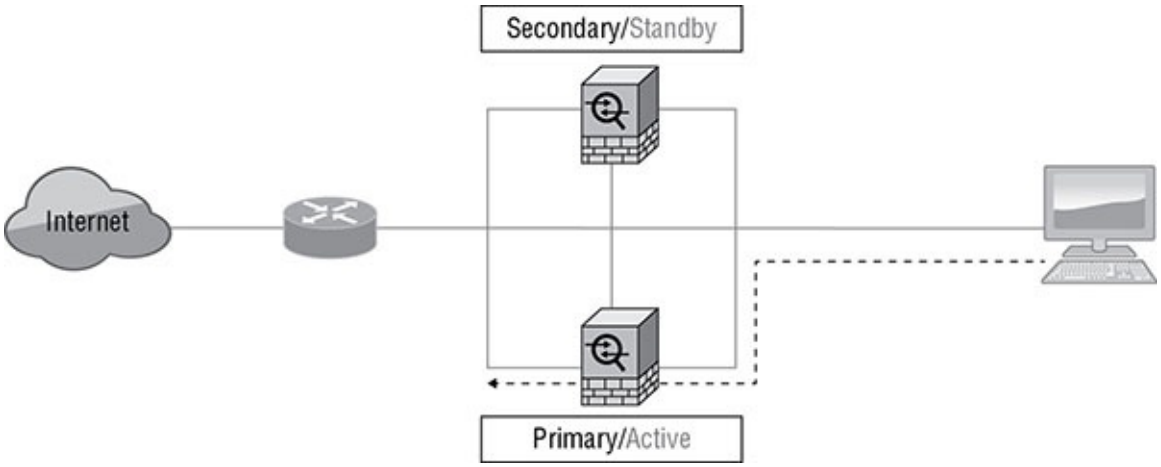

FIGURE 15.1 Active/Standby failover

Active/Active Failover

In *Active/Active failover* two security appliances are deployed with both appliances processing traffic with the ability to survive a single device failure. This deployment model is shown in Figure 15.2 .

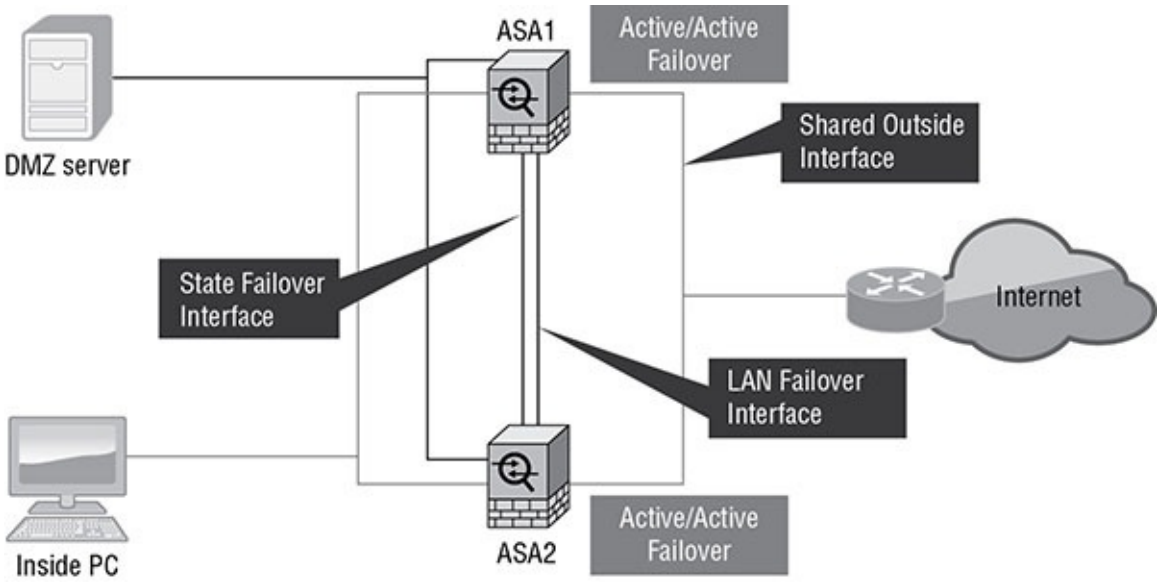

FIGURE 15.2 Active/Active failover

Clustering

In *Clustering*, three or more security appliances are deployed as a single logical device. This allows for the management of the multiple ASAs as a unit. It provides increased throughput and redundancy. This deployment model is shown in Figure 15.3 .

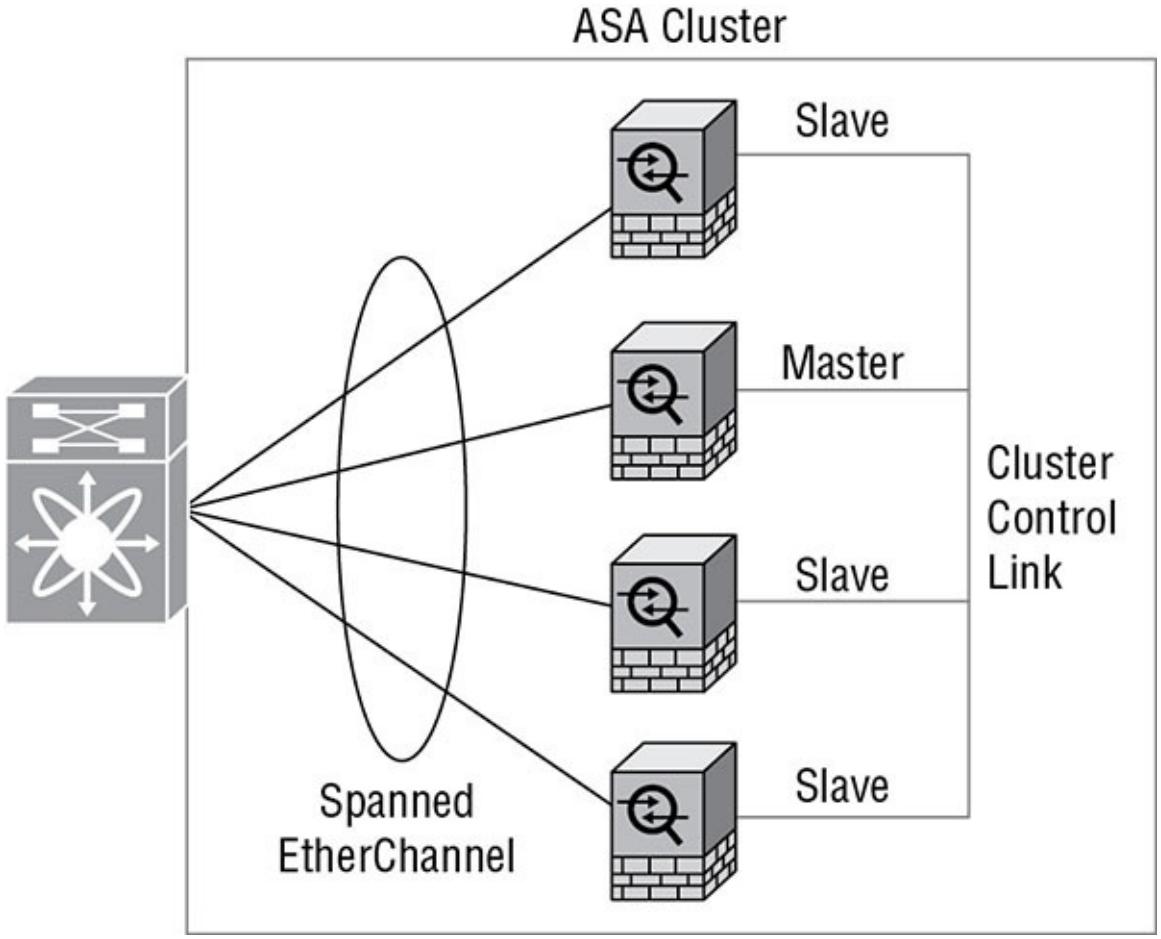

FIGURE 15.3 Clustering

Understanding Security Contexts

The ASA can be partitioned into multiple virtual firewalls or security contexts. Each context can have its own interfaces, policies, and administrators. This results functionally in multiple virtual firewalls as shown in Figure 15.4 , where multiple contexts are being used to support multiple customers.

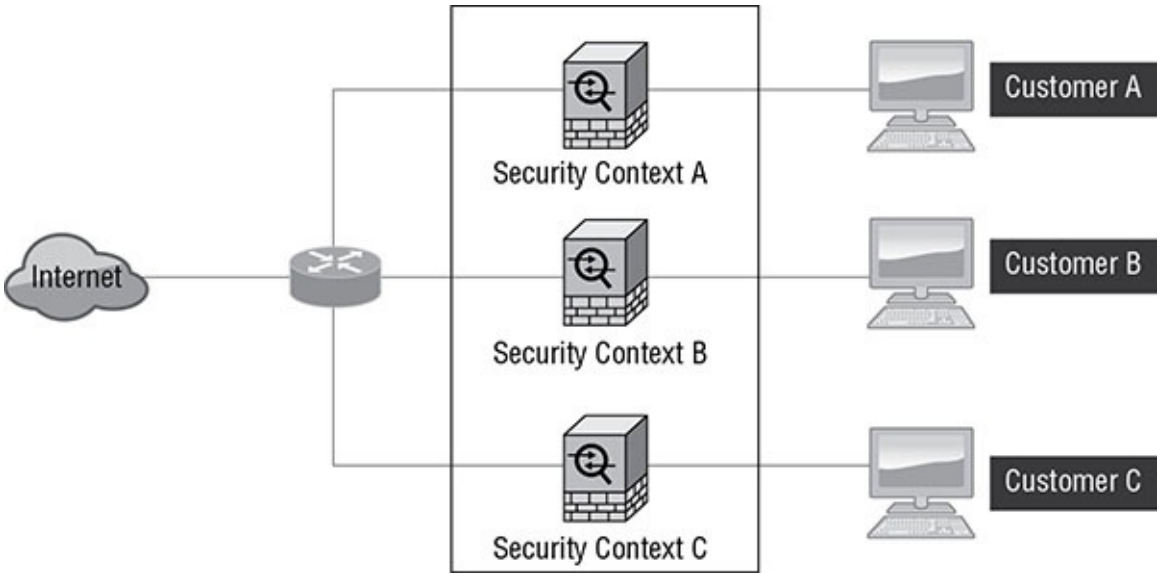

FIGURE 15.4 Security contexts

Configuring ASA Management Access

While many administrators choose to manage and configure the ASA using the *Adaptive Security Device Manager (ASDM)*, when you deploy a new ASA you will have to begin by setting up the ASA using the CLI. Only after an interface with an IP configuration is enabled will you be able to connect to the device using the ASDM. We will first cover this initial configuration and will then follow with the commands required to allow connections for the ASDM.

Initial Configuration

To perform the initial configuration of the ASA, connect to the device from the console port and perform the operations covered in the next procedure.

Initial Configuration of the ASA

In this procedure, you will configure the interfaces of the ASA with IP addresses, subnet masks, and security levels. Finally, you will enable those interfaces.

1. Connect to the ASA using a console cable.
2. Enter interface configuration mode for the external (Internet facing) interface.

```
asa70(config)#int Gi0/1
asa70(config-if)#
```

3. Configure an IP address and subnet mask for the interface.

```
asa70(config-if)#ip address 201.16.5.5 255.255.255.0
```

4. Give the interface a name. In this case, name it *outside*.

```
asa70(config-if)#nameif outside
```

5. Enable the interface.

```
asa70(config-if)#no shutdown
```

6. Using the same commands configure and enable two other interfaces, naming the interface leading to the DMZ as *dmz* and the interface leading to the private network (the LAN) *inside*.

```
asa70(config)#int gi0/2
asa70(configif)#ip address 172.168.5.5 255.255.255.0
asa70(configif)#nameif dmz
asa70(configif)#no shutdown
asa70(config)#int gi0/3
asa70(configif)#ip address 192.168.5.5 255.255.255.0
asa70(configif)#nameif inside
asa70(configif)#no shutdown
```

7. Now we need to enable the HTTP server on the ASA, which is required to connect to the device using the ASDM.

```
asa70(config)#http server enable
```

8. Now we will define an IP address on the inside network that will be allowed to connect to the ASA using either SSH or HTTP to manage the ASA.

```
asa70(config)#http 192.168.5.20 255.555.255.255 inside
asa70(config)#ssh 192.168.5.20 255.555.255.255 inside
```

9. Finally we'll create a local account on the ASA for the technician who will connect using HTTP or SSH and enable local authentication on the ASA. The username will be *Bob* and the password *passbob*. Give him level 15 (admin) access.

```
asa70(config)#username bob password passbob encrypted privilege 15
```

10. Normally at this point one would also configure a security level. We will do that in the next exercise after we discuss security levels.

Configuring Cisco ASA Interface Security Levels

Before we get into interface configuration we need to discuss a concept that may be new to you

if you have only configured routers. In the ASA interfaces have *security levels*. These security levels are one of the ways the ASA controls access from one interface to another. Security levels define the trustworthiness of the interface. The higher the level the more trusted the interface.

Security Levels

The most common configuration is to set the exterior interface (Internet) to a level of zero (or something very low in relation to the other interfaces) and the interior interface (LAN) to a very high security level value. Any other interfaces (such as a DMZ) can be set to a level that properly reflects the trust placed in that interface. With this configuration in place the typical traffic flows in your network will be as follows:

- Inbound traffic will flow from a low-security interface to a high-security interface. Another way of saying this is that it will flow from a less trusted interface to a more trusted interface.
- Outbound traffic will flow from a high-security interface to a low-security interface. Another way of saying this is that it will flow from a more trusted interface to a less trusted interface.

By default, the ASA uses these rules to control traffic between interfaces:

- There is an implicit permit for traffic flowing from a high-security interface to a low-security interface.
- There is an implicit deny for traffic flowing from a low-security interface to a high-security interface.
- There is an implicit deny for traffic flowing between two interfaces with the same security level.

Of course, these defaults can be changed and often are changed. Figure 15.5 shows how this would work using security level values 0, 50, and 100. Green lines represent allowed traffic while the red lines represent denied traffic.

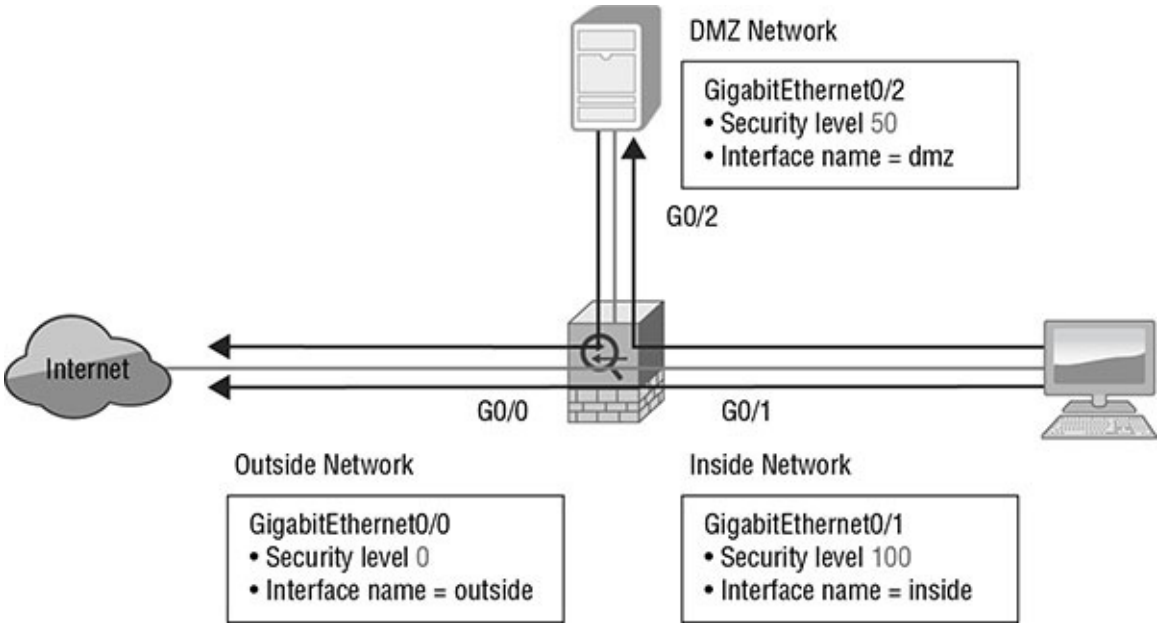

FIGURE 15.5 Security levels in action

Setting Security Levels

In this procedure, you will configure the interfaces of the ASA security levels reflecting the relative trustworthiness of the inside, outside, and dmz interfaces. The interfaces in this procedure align with the last procedure, NOT with Figure 15.5, which is a different example.

1. Enter interface configuration mode for the inside, outside, and dmz interfaces and assign the security levels 100, 50, and 0 respectively.

```
asa70(config)#int gi0/3
asa70(config)#security-level 100
asa70(config)#int gi0/2
asa70(config)#security-level 50
asa70(config)#int gi0/3
asa70(config)#security-level 0
```

At this point you should be able to connect to the ASA using the ASDM as Bob from the machine at 192.168.5.20.

Configuring Security Access Policies

In its role as a firewall the ASA uses security access policies to control traffic types allowed to flow from one interface to another. These access policies can be configured as interface access rules (much like the ACLs you may have experience with on a router) or by creating and linking object groups. In this section, we'll discuss both methods.

Interface Access Rules

If you apply no interface access rules on the ASA the default rules (as covered earlier) are:

- There is an implicit permit for traffic flowing from a high-security interface to a low-security interface.
- There is an implicit deny for traffic flowing from a low-security interface to a high-security interface.
- There is an implicit deny for traffic flowing between two interfaces with the same security level.

This means that you will need to create an access rule to allow traffic in each of the following scenarios:

- Between interfaces of the same security level
- Traffic from a lower-security interface to a higher-security interface

When Using NAT!

ACLs that permit traffic from a lower-security interface to a higher-security interface must reference the "real" or non-translated IP address of the inside host rather than the translated or mapped IP address.

While interface rules operate like ACLs you may (depending on your CLI experience with the ASA) find it easier to create these rules in the ASDM rather than at the command line. In the next procedure, you will see how this is done in the ASDM.

Creating Interface Access Rules in ASDM

In this procedure, you will configure two interface access rules in the ASDM. The ASA you manage has three interfaces that you have labeled inside (LAN), outside (Internet), and dmz. The security levels you have assigned are 100, 0, and 50 respectively. Currently the only rules in place are the global default rules discussed in the first set of bullet points in the section “Interface Access Rules” earlier in this section.

You need to configure the following rules:

- Allow only HTTP access from the outside interface to the dmz.
- Allow only HTTP from the inside to the dmz.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Access Rules.
3. Click Add, and choose Add Access Rule.
4. We will first create the rule allowing only HTTP access from the outside interface to the dmz. In the Add Access Rule dialog box, select outside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select ANY. In the drop-down box for destination IP address, select ANY. In the Service box, type or select HTTP. Click OK. On the ASDM main page, click Apply.
5. Click Add, and choose Add Access Rule.
6. We will next create the rule allowing only HTTP access from the inside interface to the dmz. In the Add Access Rule dialog box, select inside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select ANY. In the drop-down box for destination IP address, select ANY. In the Service box, type or select HTTP. Click OK. On the ASDM main page, click Apply.

The configuration is now complete.

Object Groups

While the previous procedure used the keyword ANY to select source and destination and HTTP for service, not very many configurations are that simple. In many cases we need to allow only a select group of devices rather than all devices, or we need only allow devices on a specific network to send traffic on an interface when there are multiple networks that might be traversing that interface. To make the creation and application of rules easier, the ASA can also use an object-based model for certain rules.

Objects can be created to represent any of the following:

- Networks
- Individual hosts
- Groups of services
- Resources

Once these objects have been created, they can be linked together to create rules as we did in the previous procedure and simply use the browse button next to each of the drop-down boxes in the Add Access Rule dialog box to link them together. In the next procedure, you will create objects and then use them in an access rule.

Creating and Using Objects in an Access Rule

In this procedure, you will create three objects and use them in an access rule. You need to allow HTTP traffic from the 192.168.5.0/24 network inside the LAN to a web server with the IP address of 201.3.3.3 in the DMZ. Therefore, you will

- Create a network object to represent the 192.168.5.0/24 network
- Create a service object to represent HTTP
- Create a host object to represent the server at 201.3.3.3
- Link these objects in an access rule and apply it to the inside interface

Note: interface objects have been created and named inside, outside, and dmz with security levels of 100, 0, and 50.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Objects ➢ Network Objects/Groups.
3. Select Add, then Network Object.
4. In the Name field, enter HTTP_group_internal.
5. In the IP address and network mask sections, enter 192.168.5.0 and 255.255.255.0. Then select OK.
6. Select Add, then Network Objects/Groups.
7. In the Name field, enter DMZ_web.
8. In the IP address section, enter 201.3.3.3. Then select OK.
9. Select Object, then Service Objects/Groups and finally Add Service Group.
10. In the Add Service Group dialog box, enter a name for DMZ_services.
11. In the Existing service group section, select TCP-HTTP and TCP-HTTPS and select Add. Then click OK.

12. In the main ASDM window, select Apply to create the objects.
13. Navigate to Configuration ➢ Firewall ➢ Access Rules.
14. Click Add, and choose Add Access Rule.
15. In the Add Access Rule dialog box, select inside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select the object you created called HTTP_group_internal. In the drop-down box for destination IP address, select the object you created called DMZ_web. In the Service box, select the object you created called DMZ_services. Click OK. On the ASDM main page, click Apply.

The configuration is now complete.

Configuring Default Cisco Modular Policy Framework (MPF)

In Chapters 4 and 14 you learned about the Cisco Modular Policy Framework (MPF). As review, there are three components that are used as building blocks to implement policies in this framework:

- Class maps are used to categorize traffic types into classes. ACLs are typically used to define the traffic and then the ACL is referenced in the class map.
- Policy maps are used to define the action to be taken for a particular class. Actions that can be specified are allow, block, and rate-limit.
- Service policies are used to specify where the policy-map should be implemented.

In the next procedure, you will use this framework to create a new policy by creating a class map that identifies Telnet as the traffic and a policy map that identifies an action of deny and apply the two to all interfaces with a service policy.

Configuring Default Cisco Modular Policy Framework (MPF)

In this exercise, you will create a new policy by creating a class map that identifies Telnet as the traffic and a policy-map that identifies an action of deny and apply the two to all interfaces with a service policy.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Service Policy Rules and click Add, then Service Policy rule.
3. Name the service policy `No_telnet` and select the Global radio button (which applies it to all interfaces). Click Next.
4. In the Traffic Class Criteria dialog box, select Create A New Traffic Class. Name the class `Telnet_deny`.
5. In the Traffic Match Criteria section, check the box for TCP Or UDP Destination Port and select Next.
6. In the service field of the next box enter **TCP/23** in both the Source and Destination fields. Click Next.
7. Select Finish. The configuration is complete.

Summary

In this chapter, you learned how to set up the ASA so you can remotely administer it using the ASDM. You also learned the default security policies that are in place and how the default global policy interacts with configured policies. You also learned about interface security levels and the effect they have on traffic flows. The chapter reviewed the Cisco Modular Policy framework and how it is used to create policies. It also discussed the difference between a transparent and routed firewall. Finally, high-availability solutions were introduced including active-active, active-passive, and clustering approaches.

Exam Essentials

Identify firewall services provided by the ASA. These include Application Inspection Control (AIC), Network Address Translation (NAT), IP Routing, IPv6 support, DHCP, and Multicast support.

Describe the two modes of deploying the ASA. The ASA can be deployed in one of two modes, routed and transparent. In router mode, the ASA is serving as a router and thus each of its interfaces will reside in a separate IP subnet. In transparent mode, the ASA is not acting as a router and assumes a layer 2 identity much as a switch does.

Identify ASA high-availability methods. These include Active/Standby failover,

Active/Active failover, and clustering.

Define security contexts in the ASA. The ASA can be partitioned into multiple virtual firewalls or security contexts. Each context can have its own interfaces, policies, and administrators.

Describe the steps required for initial setup of the ASA. These steps include assigning an IP address and mask to interfaces, enabling interfaces, and enabling the HTTP server. They also include permitting the remote management traffic generated when connecting with the ASDM.

List the default traffic rules in the ASA. By default, the ASA uses these rules to control traffic between interfaces: there is an implicit permit for traffic flowing from a high-security interface to a low-security interface, there is an implicit deny for traffic flowing from a low-security interface to a high-security interface, and there is an implicit deny for traffic flowing between two interfaces with the same security level.

Identify examples of items for which objects can be created in the ASA. Objects can be created to represent any of the following: networks, individual hosts, groups of services, or resources.

Describe the components of the Cisco Modular Policy Framework (MPF). There are three components that are used as building blocks to implement policies in this framework: class maps, used to categorize traffic types into classes (ACLs are typically used to define the traffic and then the ACL is referenced in the class map); policy maps, used to define the action to be taken for a particular class (actions that can be specified are allow, block, and rate-limit); and service policies, used to specify where the policy map should be implemented.

Review Questions

1. Which firewall feature can help prevent many tunneling attempts and application layer attacks?
   A. AIC
   B. NAT
   C. DHCP
   D. PIM-SIM
2. In which mode does the ASA assume a layer 2 identity?
   A. Switch
   B. Transparent
   C. Active/Standby
   D. Routed
3. In which high-availability approach are three or more security appliances deployed as a

single logical device?

A. Active/Active

B. Stackwise

C. Clustering

D. Active/Standby

4. What is it called when the ASA is partitioned into multiple virtual firewalls?

A. security contexts

B. security domains

C. security realms

D. security areas

5. Which command is used to apply the name *outside* to an interface on the ASA?

A. `asa70(config-if)#name outside`

B. `asa70(config-if)#nameif outside`

C. `asa70(config-if)#outside`

D. `asa70(config)#nameif outside`

6. Which command is required to connect to the device using the ASDM?

A. `asa70(config)#http server`

B. `asa70(config)#http enable`

C. `asa70(config)#http server enable`

D. `asa70(config)#enable http server`

7. Which command defines an IP address on the inside network that will be allowed to connect to the ASA using HTTP to manage the ASA?

A. `asa70(config)#http 192.168.5.20 255.555.255.255`

B. `asa70(config)#http 192.168.5.20/32 inside`

C. `asa70(config)#http 192.168.5.20 inside`

D. `asa70(config)#http 192.168.5.20 255.555.255.255 inside`

8. What value is used to determine the allowed traffic flows between the interfaces in the ASA?

A. security level

B. IP address

C. MAC address

D. name

9. There is an implicit permit for traffic flowing from a _____ security interface to a security _____ interface.

   A. low, low

   B. high, low

   C. high, high

   D. low, high

10. Which command assigns the security level 100 to an interface?

   A. `asa70(config)#security 100`

   B. `asa70(config)#100 security-level`

   C. `asa70(config)#security-level 100`

   D. `asa70(config)#level 100`

11. In which of the following scenarios will you need to create an access rule to allow traffic?

   A. between interfaces of the same security level

   B. traffic to the self-zone

   C. traffic from a higher-security interface to a lower-security interface

   D. in all scenarios

12. Which of the following is used to represent a select group of devices rather than all devices in a network?

   A. service policy

   B. object group

   C. policy map

   D. security group

13. Which of the following is used to categorize traffic types in the MPF?

   A. zone pairs

   B. zones

   C. policy maps

   D. class maps

14. You would like to apply a service policy to all interfaces of the ASA. What radio button do you choose for this in the ASDM?

   A. global

B. composite

C. self

D. all

15. You need to allow HTTP traffic from the 192.168.5.0/24 network inside the LAN to a web server with the IP address of 201.3.3.3 in the DMZ. What type of object do you create to represent the HTTP traffic?

A. network object

B. service object

C. host object

D. resource object

16. Which of the following is used to specify where a policy map should be implemented in the MPF?

A. zone pairs

B. zones

C. service policy

D. class maps

17. The ASA you manage has three interfaces that you have labeled *inside* (LAN), *outside* (Internet), and *dmz*. The security levels you have assigned are 100, 0, and 50 respectively. Currently the only rules in place are the global default rules. Which traffic is allowed?

A. inside to outside

B. outside to dmz

C. dmz to outside

D. inside to dmz

18. In the following command output what does inside represent?

```
asa70(config)#ssh 192.168.5.20 255.555.255.255 inside
```

A. ACL name

B. security level

C. interface IP address

D. traffic direction

19. Which of the following is used to define the action to be taken for a traffic type in the MPF?

A. zone pairs

B. zones

C. policy maps

D. class maps

20. There is an implicit deny for traffic flowing from a _____ security interface to a _____ interface.

A. low, low

B. high, low

C. high, high

D. low, high

Chapter 16
Intrusion Prevention

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓**6.1 Describe IPS deployment considerations**

- Network-based IPS vs. host-based IPS
- Modes of deployment (inline, promiscuous - SPAN, tap)
- Placement (positioning of the IPS within the network)
- False positives, false negatives, true positives, true negatives

✓**6.2 Describe IPS technologies**

- Rules/signatures
- Detection/signature engines
- Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
- Blacklist (static and dynamic)

It is no longer acceptable to sit and wait for the next attack and react afterward. In today's threat-filled landscape, security professionals must take a proactive approach to preventing intrusions. Intrusion prevention systems are designed to identify and prevent attacks in real time. In this chapter, you will explore the intrusion prevention capabilities of the ASA.

In this chapter, you will learn the following:

Deployment options of an IPS

Advantages and disadvantages of an HIPS and an NIPS

Proper positioning of an IPS

Management of false positives and negatives

Threat identification methods

Methods of implementing high availability

Trigger actions

IPS Terminology

To begin this chapter, you'll learn a number of terms and concepts that apply to the process of intrusion prevention. A clear understanding of these will help support the rest of the chapter.

Threat

A *threat* is an identified security weakness to which any specific environment may or may not be vulnerable. For example, a threat might exist in the form of a new attack on Oracle database servers, but if you use Microsoft SQL Server, it is a threat to which you are not vulnerable. Risk is present only when a threat and a vulnerability to the threat both exist.

Risk

Risk is created when a threat exists to which a system is vulnerable. Unless these two conditions are both present, no risk exists.

Vulnerability

A *vulnerability* is any susceptibility to an external threat that a device or system may possess. A threat becomes a vulnerability only when the threat target is present in your environment and is in the state required to take advantage of the vulnerability. For example, if a threat to a file server exists only if the file server is lacking a security patch and your file server has the patch installed, the threat is not a vulnerability. Examples of vulnerabilities include the following:

- Weak passwords
- Missing security patches
- Lack of input validation

Exploit

An *exploit* occurs when a threat and a vulnerability both exist and a threat actor takes advantage of the situation. The term *exploit* also refers to the specific tool or attack methodology used. Some examples include the following:

- Scripts
- Malware
- Password crackers

Zero-Day Threat

A *zero-day threat* is any threat not yet remediated by malware vendors or software vendors. This type of threat cannot be detected through attack signature-based methods and is usually discovered only by malware or IPS/IDS software that uses heuristics. This approach identifies attacks by identifying traffic that is consistent with an attack rather than using a signature.

Actions

Actions refer to the operations that an intrusion prevention system (IPS) can take when an attack is recognized. Some examples of these actions are as follows:

- *Drops* means the IPS quietly drops the packets involved.
- *Reset* sends a packet with the RST flag that ends any TCP connection.
- *Shun* accomplishes the same purpose as a reset for non-TCP connections.
- *Block* is when the IPS directs another device (a router or firewall) to block the traffic.

Network-Based IPS vs. Host-Based IPS

The most common way to classify an IPS is based on its information source: network based and host based. A *host-based intrusion detection system (HIPS)* is installed on the device (for the purposes of this discussion, a server), and the system focuses solely on identifying attacks on that device only. This is in contrast to a network-based system, which monitors all traffic that goes through it looking for signs of attack on any machine in the network.

Host-Based IPS

An HIPS can be configured to also focus on attacks that may be relevant to the role that the server is performing (for example, looking for DNS pollution attacks on DNS servers). But there are drawbacks to these systems.

- A high number of false positives can cause a lax attitude on the part of the security team.
- Constant updating of signatures is needed.
- There's a lag time between the release of the attack and the release of the signature.
- An HIPS cannot address authentication issues.
- Encrypted packets cannot be analyzed.
- In some cases, IPS software is susceptible itself to attacks.

Despite these shortcomings, an HIPS can play an important role in a multilayer defense system.

Network-Based IPS

A *network-based IPS (NIPS)* monitors network traffic on a local network segment. This is in contrast to a host-based IPS (HIPS) that monitors a single machine.

One of the disadvantages of an NIPS (which is an advantage of an HIPS) is that it cannot monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal.

Most IPSs are programmed to react in certain ways in specific situations. Event notification and alerts are crucial to IPSs. These notifications and alerts inform administrators and security

professionals when and where attacks are detected.

Promiscuous Mode

To monitor traffic on the network segment, the network interface card (NIC) must be operating in *promiscuous mode*. Moreover, an NIPS is affected by a switched network because generally an NIPS monitors only a single network segment, and each switch port is a separate collision domain.

Detection Methods

These systems can use several methods of detecting intrusions. The two main methods are as follows:

Signature Based Analyzes traffic and compares patterns, called *signatures*, that reside within the IDS database. This means it requires constant updating of the signature database.

Anomaly Based Analyzes traffic and compares it to normal traffic to determine whether the traffic is a threat. This means any traffic out of the ordinary will set off an alert.

Evasion Techniques

While IPSs can do some amazing things, they are not infallible. Several techniques have been developed over the years by malicious individuals that allow them to get malicious code past the IPS. Some of the more common approaches are covered in this section.

Packet Fragmentation

Packet fragmentation is the process of breaking a packet that is larger than the *maximum transmission unit (MTU)* into smaller pieces called *fragments* that abide by the size limits of the MTU. Various networking technologies enforce different MTUs. For example, while the MTU in Ethernet is 1,500 bytes, in an FDDI network the MTU is 4,470 bytes.

Routers on the network enforce the MTU and perform fragmentation of packets as needed to meet the MTU. When the fragments arrive at the destination, they are reassembled. To communicate exactly how the reassembly should occur, several header fields are used in the IP header. Figure 16.1 shows the IP header.

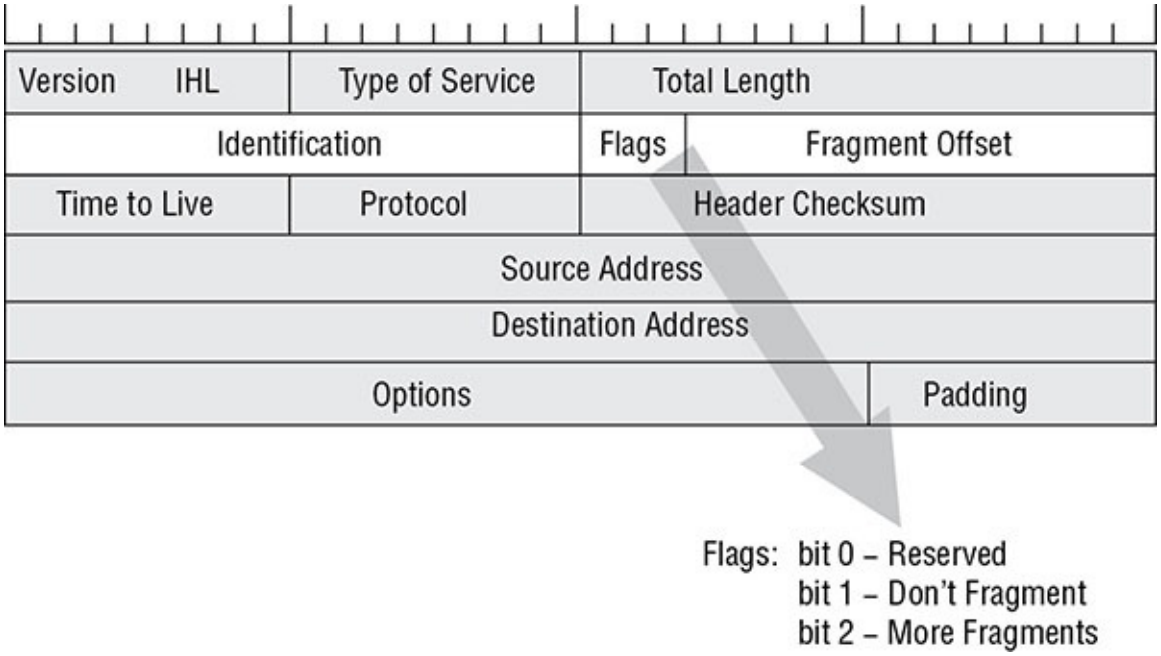

FIGURE 16.1 IP header fragmentation flags

Three fields are of interest.

- *Identification* provides a number that identifies packets that belong to the same transmission that need to be reassembled.
- *Flag* is a field consisting of three bits. As shown in Figure 16.1 , the first bit position 0 is reserved and not used in the fragmentation process; the second position when checked means don't fragment this packet, in which case if the packet is oversized, an ICMP message will be sent to the source indicating it cannot be sent without fragmentation. The third position when checked means this packet is part of a series of fragments and there are more to come. If this is the last fragment in a series of fragments, this bit will not be checked.
- *Fragment Offset values* indicates to the reassembling host where this fragment belongs. It does so by indicating how many bytes away from the beginning of the payload the fragment is.

The fragmentation process follows this sequence:

1. A router makes the decision that a packet must be fragmented.
2. The router splits the packet into fragments, each with an identical IP header apart from the flag bits and the offset values.
3. The destination reassembles the fragments. It recognizes the first fragment because it has an offset value of 0. It then uses the offset values of each fragment to properly position the fragments. It recognizes the last fragment because the More Fragments bit is off.

This process is illustrated in Figure 16.2 , where an MTU of 3,300 bytes is enforced on a packet that is 11,980 bytes. As you can see, the first fragment is given an Offset of 0 and the More Fragments bit is on, indicating more fragments to the receiver. The second packet has an

Offset value of 410 and has the More Fragments bit on. The third and final fragment has an Offset value of 820, and since it is the last fragment, the More Fragments bit is off.

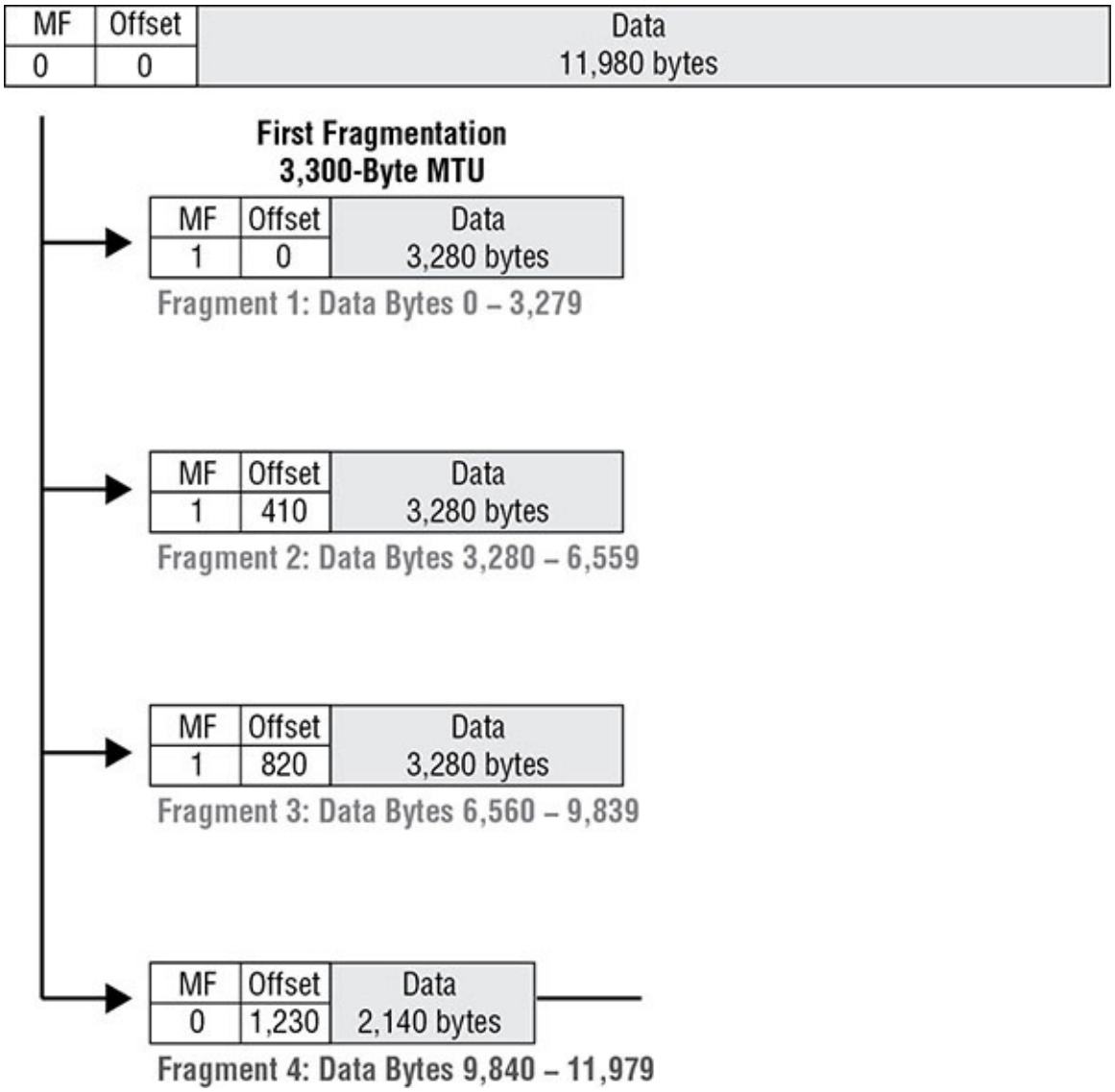

FIGURE 16.2 Fragmentation process

So, how does the fragmentation attack work? The attacker fragments the packet containing the malicious code so that it becomes difficult for the IPS to recognize the code in such a fragmented fashion. This process is shown in Figure 16.3 , where a malicious CGI script that, as shown in the original IP packet at the top, would probably be recognized by the IPS is split into fragments that may *not* be recognized by the IPS. (It is not important to understand the script.) In this case, a tool called `fragroute` was used to split the packet into fragments.

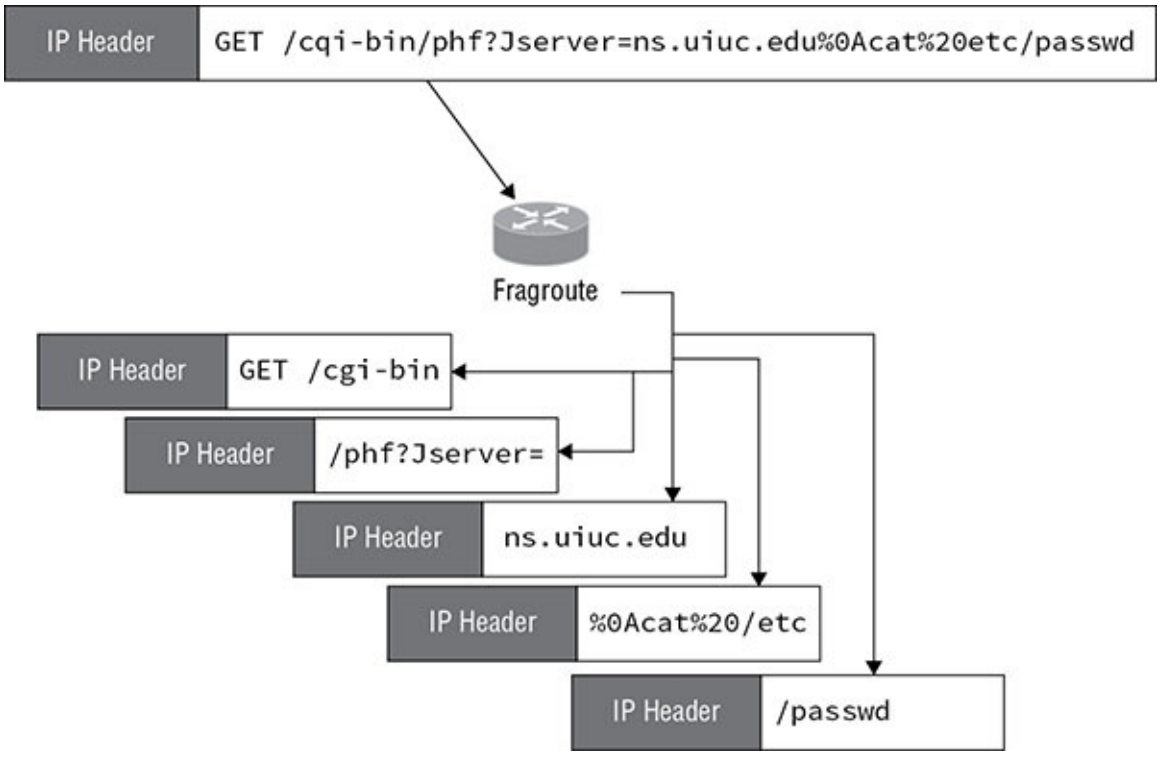

FIGURE 16.3 Fragmentation attack

The mitigations to this attack are to do the following:

- Use an IPS that performs signature analysis against the entire packet rather than individual fragments. This requires the ability to perform stream reassembly.
- Use protocol analysis to evaluate the entire packet for violation of protocol standards.

Injection Attacks

In an *injection attack*, the attacker inserts data that will be accepted by the IPS but will be ignored by the target system. One approach takes advantage of the TTL feature of IP and fragmentation. The time-to-live (TTL) value is used in IP to prevent a packet from looping endlessly. When a packet's TTL value goes to zero (decremented at each hop), it gets dropped by the router.

In the attack (as shown in Figure 16.4), the attacker injects a bogus string into the attack code and then breaks the attack into three fragments. Then he manipulates the TTL value of the fragment containing the bogus string in such a way that the fragment dies (and never gets delivered) before it reaches the destination. If the IPS does not consider the fragment offset values or TTL values, it will detect the bogus string rather than the actual payload. The result is that after inspection by the IPS, the bogus string does not get delivered. The attack payload does.

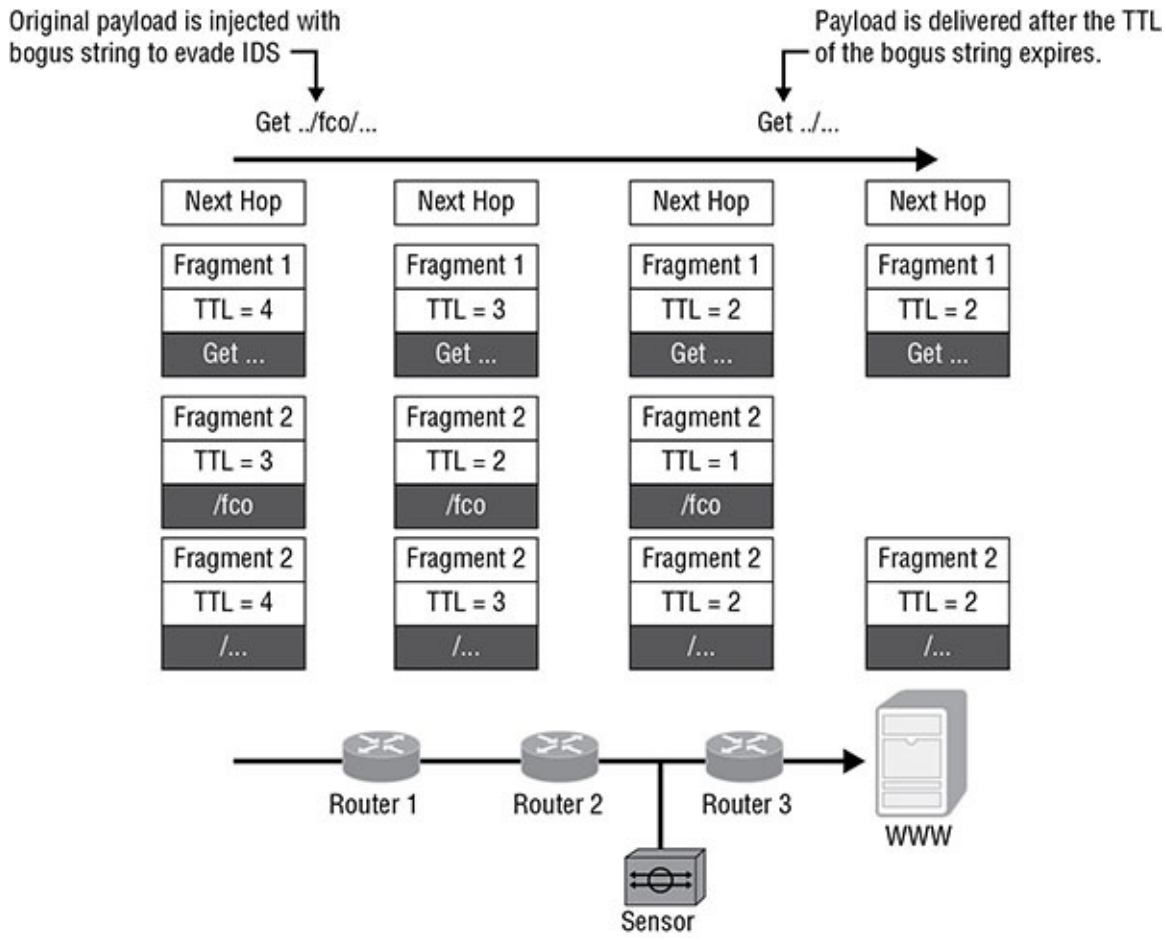

FIGURE 16.4 Injection attack

Mitigations to this attack are as follows:

- Use an IPS that performs stream reassembly, which allows the IPS to recognize the attack.
- Use an IPS that performs TTL value assessment, which allows the IPS to recognize the lower TTL for the fragment containing the bogus string.

Alternate String Expressions

In many protocols, information can be communicated or expressed in multiple ways. For example, HTTP can accept strings expressed in hexadecimal, Unicode, or standard text expressions. Attackers can use this to evade an IPS sensor. If the IPS cannot perform protocol normalization (which decodes the payload to discover its significance), this attack may succeed.

Mitigations to this attack are as follows:

- Protocol analysis
- Protocol normalization

Introducing Cisco FireSIGHT

Cisco FireSIGHT offers threat protection capabilities that go beyond most IPSs. It not only detects and takes action to prevent attacks, it enables a better understanding of the exposures your environment may possess and helps you to take corrective actions to eliminate them. This section surveys the capabilities of FireSIGHT and the role it can play at various stages of an attack.

Capabilities

There are four categories of functions of which FireSIGHT is capable.

- *Detection*: Attack detection technologies include the following:
  - *IPS*: Monitors for malicious and suspicious activity.
  - *Discovery*: Enables visibility into all hosts, services, and applications running on the network. This includes traffic discovery in which you can identify the ways in which resources are being utilized.
- *Learning*: Reports on the state of the environment and detects when changes occur in real time.
- *Adapting*: When changes are detected, FireSIGHT can adapt its configuration to mitigate new risks.
- *Acting*: Actions that are available include the following:
  - Block, alert, or modify suspicious traffic
  - Remediate through custom responses such as blocking a downstream router or scanning a device
  - Automate response and reporting

FireSIGHT is managed using the FireSIGHT Management Center. This application can be hosted on a FireSIGHT Management Center appliance or hosted on a virtual appliance on a VMware server.

Protections

The operations and features of FireSIGHT are best described in terms of how they would be utilized during an attack. Therefore, you will look at these protections in this way.

Before an Attack

The best way to mitigate attacks is to address them before they occur. FireSIGHT provides the following preventative technologies for this:

- *Blacklisting*: Traffic to and from specific IP addresses can be blacklisted, which means that your traffic will be neither sent to nor received from the IP address. When you identify problematic IP addresses, this is an action you take. Moreover, the FireSIGHT Management Center can dynamically download at configurable intervals a collection of IP

addresses that have been identified by a threat intelligence team called Talos (https://www.talosintelligence.com/) as having a bad reputation in this regard. You can choose to add these to this list if desired.

- *Advanced Malware Protection (AMP)*: Two AMP products are included. Cisco AMP for Endpoints is composed of connectors installed on endpoints. It uses a cloud-based detection process that offloads the detection burden to the cloud. Cisco AMP for Networks uses FirePOWER (covered in detail later in this chapter) appliances to detect malware in transit. It also can utilize the cloud for the latest malware. The system can also store detected files for submission to the Cisco Collective Security Intelligence Cloud for dynamic analysis.

During an Attack

While FireSIGHT uses the aforementioned methods to prevent attacks, prevention is not always possible. Once an attack is underway, the FireSIGHT IPS primarily takes actions by identifying and blocking malicious traffic. The IPS is a policy-based feature that allows for monitoring and blocking or altering malicious traffic when the IPS is deployed inline (deployment options are covered in the next section of this chapter).

FireSIGHT uses Snort technology (an IDS). This technology makes use of preprocessors, which examine traffic and in some cases modify the traffic in such a way that attacks that cannot be recognized by the signature can be recognized. For example, one preprocessor helps to recognize malicious code hidden by an IP fragmentation attack.

An IPS policy consists of the following:

- Rules that inspect the header content, packet size, and payload
- Rule state configuration based on FireSIGHT recommendations
- Preprocessors and other detection features

FireSIGHT also generates intrusion event information in a log that includes details such as the following:

- Date and time
- Event priority
- Brief description
- Name of the device
- Source IP address and port for the event
- Destination IP address and port for the event
- Name of the logged-in user
- Impact flag

After an Attack

After the attack, FireSIGHT provides an assessment of the attack, contains the attack, and helps bring the network back into a normal state. To do this, it uses several features:

- *FireSIGHT discovery and awareness*: This collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities that is used to report indicators of compromise.
- *Dynamic file analysis*: Captured files can be submitted to the Cisco Collective Security Intelligence Cloud for analysis. The cloud runs a test and returns a threat score to the FireSIGHT Management Center.
- *Connection data and summaries*: Connection data is information about detected sessions, including timestamps, IP addresses, geolocation, and applications.

Understanding Modes of Deployment

The FireSIGHT Management Center can also manage other monitoring devices such as appliances, virtual appliances, and ASA firewalls running software release ASA 9.2 and later. It is also commonly deployed in branch offices in the form of the FireSIGHT module in the ASA.

The devices managed by the FireSIGHT Management Center acting in the same role as legacy IPS sensors can be deployed in two modes.

Passive

The sensor receives a copy of the network traffic to analyze while the original traffic flows through the network. Because the sensor only receives a copy, and because by the time the copy is analyzed, the original traffic is long gone, FireSIGHT can only function as an intrusion detection system (IDS) when deployed in this mode. There are two ways to implement passive mode.

SPAN

Figure 16.5 illustrates this mode. The sensor is connected to a port on the switch to which all traffic has been mirrored by making the port a SPAN port. Notice that the traffic flow from the device inside the network to a device on the Internet (black dashed line) and then back (gray dashed line) is not interrupted.

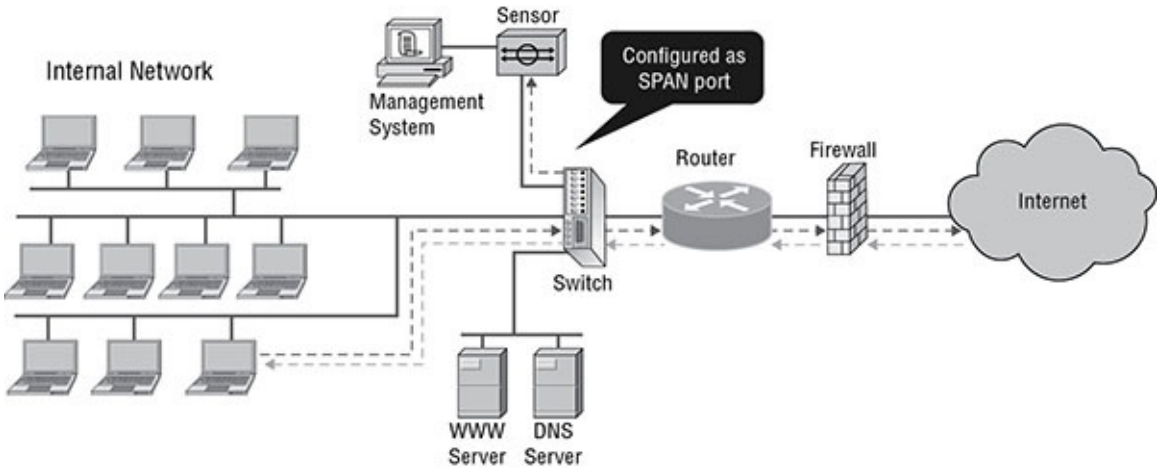

FIGURE 16.5 SPAN

Tap

In this deployment mode, the sensor is implemented as a network *tap*, as shown in Figure 16.6 . The tap is placed between the router and the layer 3 switch. It provides full-duplex connectivity between the devices and splits off two simplex mirrors of the full-duplex traffic. All traffic between the two devices must traverse the sensor.

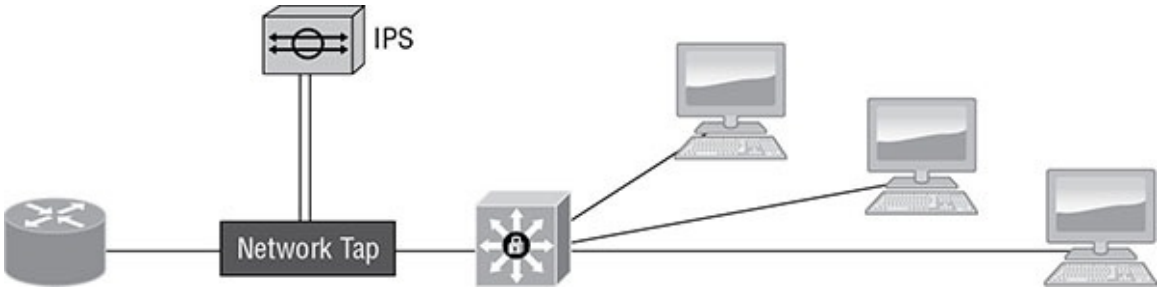

FIGURE 16.6 Tap

Inline

In this mode, the sensing device is placed in the line of traffic and analyzes the original traffic, not a copy in real time. Therefore, it can take actions on the traffic that allow it to operate as a true IPS. Figure 16.7 shows this mode's operation.

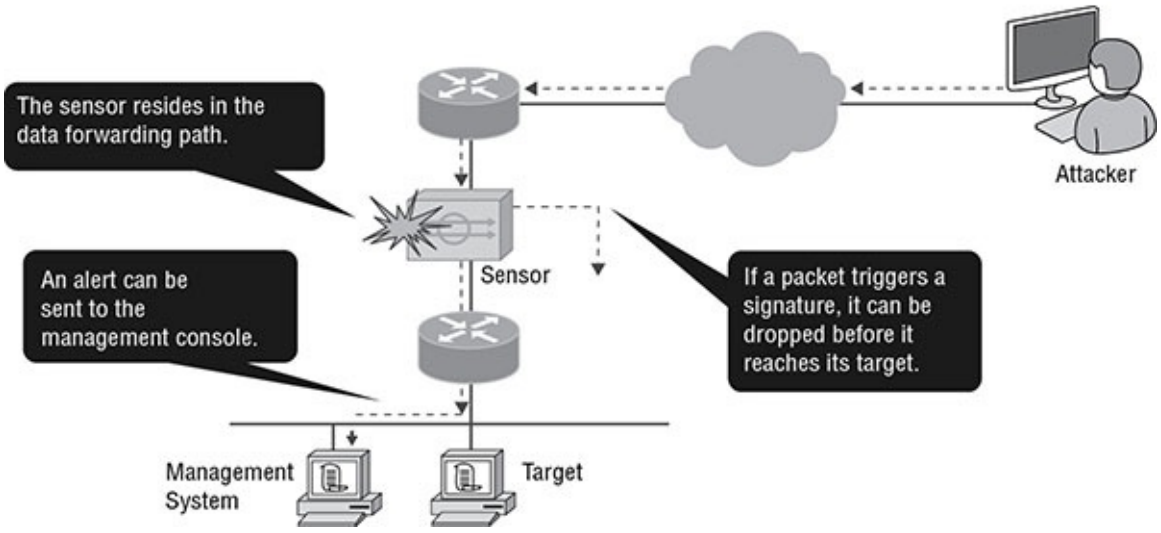

FIGURE 16.7 Inline mode

Positioning of the IPS within the Network

When making this key decision, consider the following factors:

- The features you are utilizing (attack detection, policy enforcement, surveillance, anomaly detection, etc.)
- Location of critical assets
- Bandwidth utilization
- Topology

Outside

One of the options is to place the sensor outside the perimeter firewall (ASA). When placed here, the sensor will generate a very high number of alarms because this is an exposure to the most untrusted network, the Internet. It will also generate many alarms that you will assess to be false positives (more on false positives in the final section of this chapter) because it will be composed of traffic that the ASA would have never allowed into the network. Figure 16.8 shows this option.

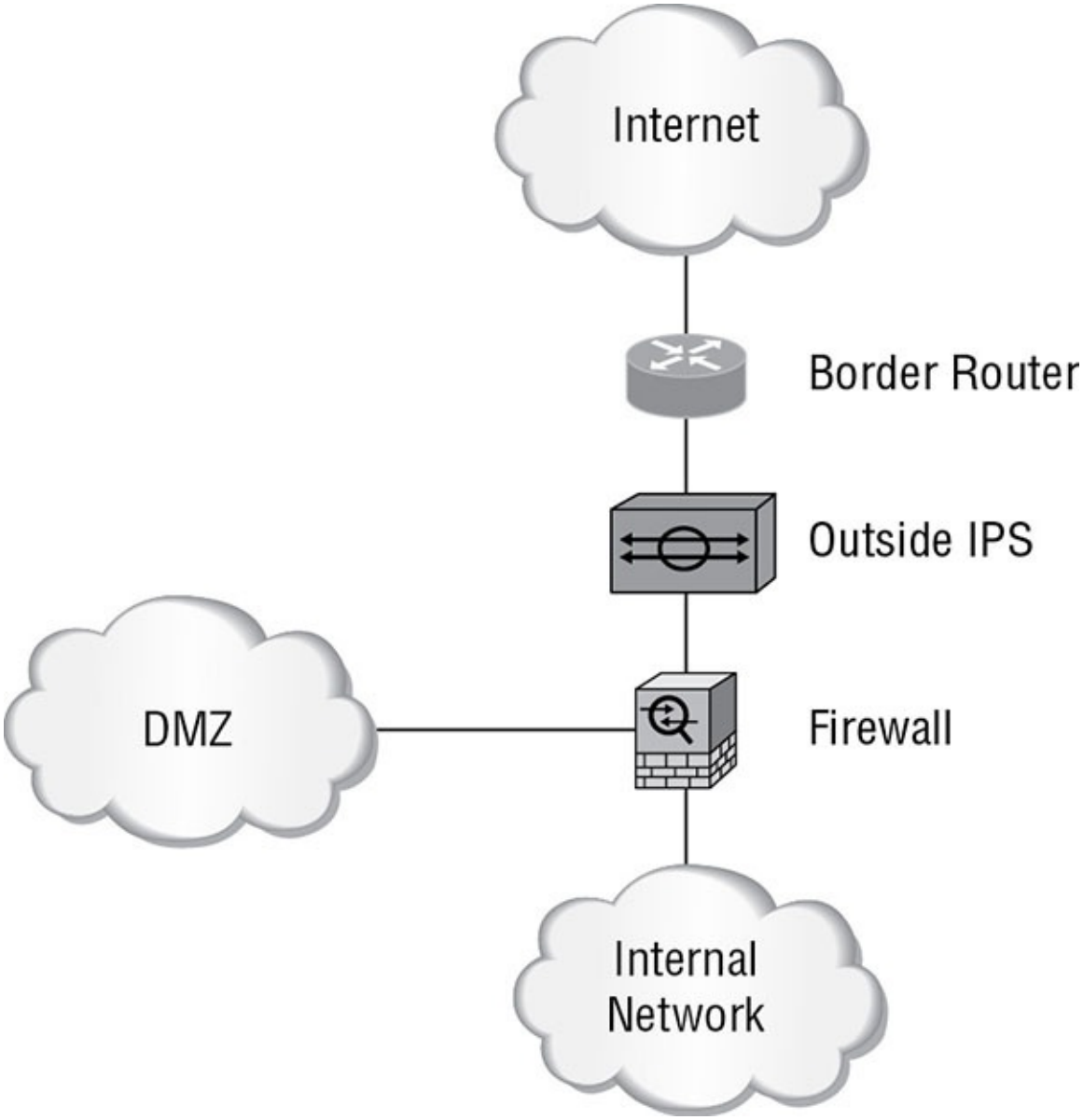

FIGURE 16.8 Outside deployment

DMZ

Servers in the DMZ are exposed to the Internet by design. While placing a sensor here will help to identify attacks on these exposed devices, keep in mind that if these servers are being deployed according to best practices, they will contain no sensitive information and will have been significantly hardened. Figure 16.9 shows this option.

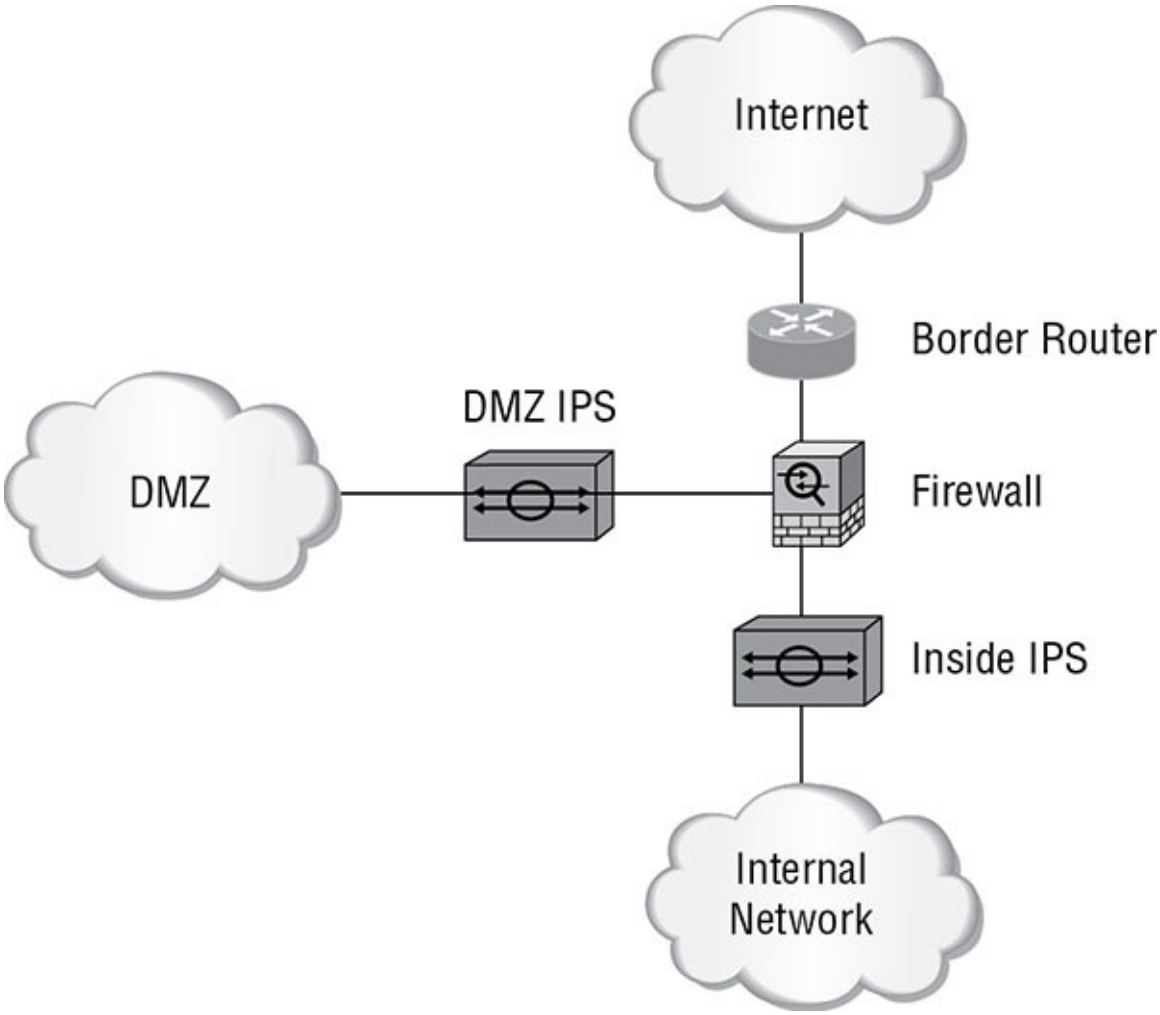

FIGURE 16.9 DMZ deployment

Inside

This is a positioning that yields the most benefit. While the perimeter ASA can provide protection, keep in mind that the users of these interior devices have varying levels of security expertise. This is also where all critical data will be located. Therefore, this will be the best place to deploy a single sensor. Figure 16.10 shows this option. In this option, FireSIGHT is deployed as a module in the ASA and is examining traffic destined for the internal network.

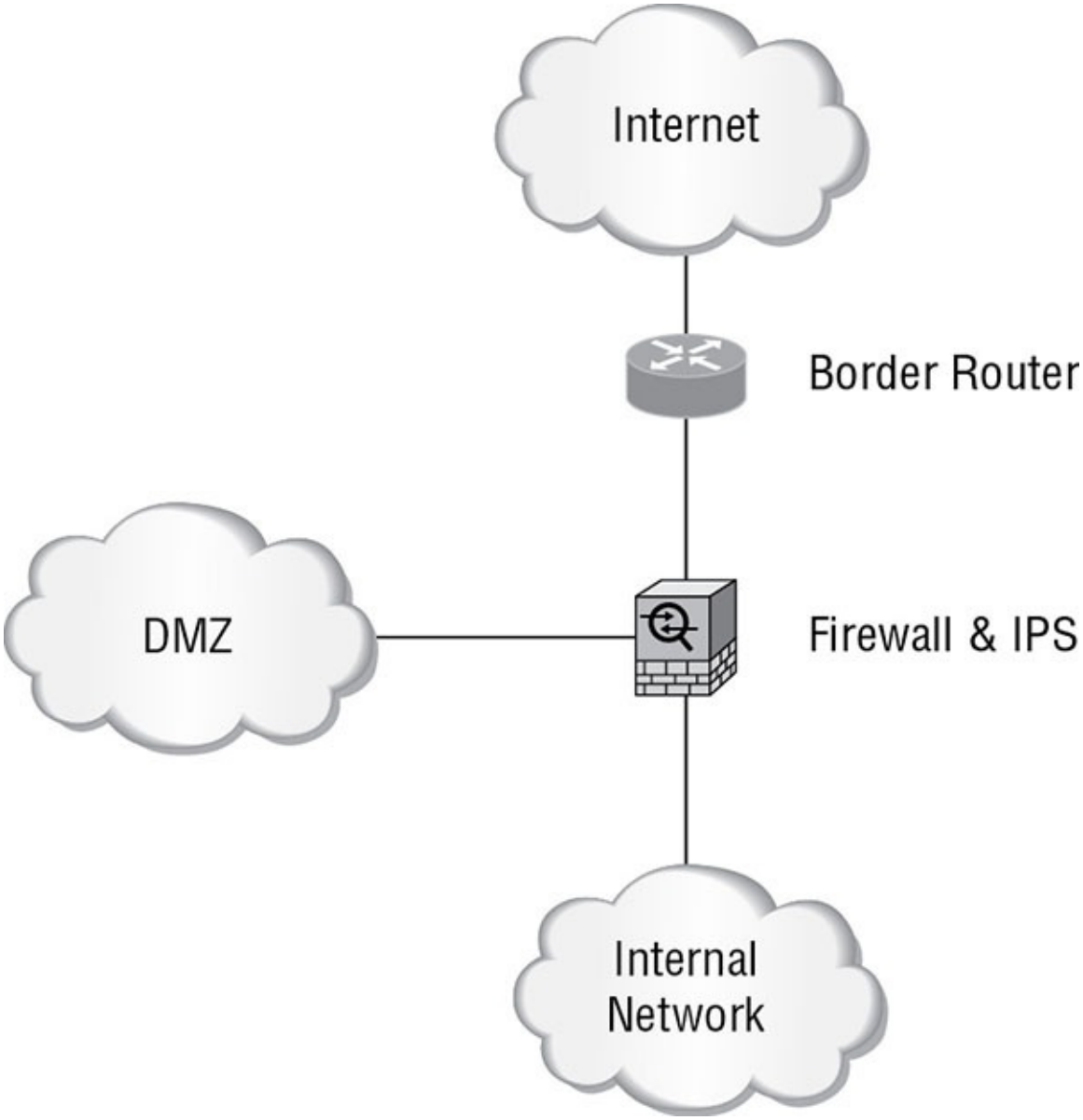

FIGURE 16.10 Inside deployment

Understanding False Positives, False Negatives, True Positives, and True Negatives

All IPSs and IDSs, including FireSIGHT, make incorrect assessments. In some cases, they fail to identify attacks or malicious traffic. In other cases, they alert you that an attack is under way when that is not the case. They also make correct assessments, alerting you to a real attack or ignoring traffic that is *not* an attack. There are terms used to describe all four of these scenarios. Table 16.1 identifies these terms. Keep in mind that *true* means the IPS was correct in its assessment and *false* means it was incorrect in its assessment.

TABLE 16.1 Assessment terms

Term	Meaning
True positive	The IPS alerted you to an attack that is real.
True negative	The IPS did not alert you to a nonexistent attack.
False positive	The IPS alerted you to an attack that is nonexistent.
False negative	The IPS did not alert you to a real attack.

Summary

In this chapter, you learned about some general IPS concepts, such as network-based and host-based deployments; modes of deployment such as inline, SPAN, and tap; and the positioning options available. You also were introduced to false positives and false negatives and the interpretation of these. The chapter covered how both rules and signatures are used in the process of identifying potential attacks. Finally assessment terms (false positive, false negative, etc.) were discussed.

Exam Essentials

Define IPS terminology. These terms include threat, risk, vulnerability, exploit, and zero-day threat.

Describe the actions of which an IPS is capable. Some examples of these actions are drops, which means the IPS quietly drops the packets involved; reset, which sends a packet with the RST flag, which ends any TCP connection; shun, which accomplishes the same purpose as a reset for non-TCP connections; and block, where the IPS directs another device (a router or firewall) to block the traffic.

Differentiate network-based and host-based IPS. A host-based intrusion prevention system (HIPS) is installed on the device (for the purposes of this discussion, a server), and the system focuses solely on identifying attacks on that device only. This is in contrast to a network-based system, which monitors all traffic that goes through it looking for signs of attack on any machine in the network.

Identify evasion techniques employed to defeat an IPS. These include packet fragmentation, injection attacks, and alternate string expressions.

List four categories of functions of which FireSIGHT is capable. These functions include detection, learning, adapting, and acting.

Describe the deployment modes of an IPS. These include passive modes, such as SPAN and tap, where the device can only operate an IDS. It also includes inline mode, in which the device can take actions on traffic as a true IPS.

Review Questions

1. Which of the following is an identified security weakness to which any specific environment may or may not be vulnerable?
   A. Threat
   B. Risk
   C. Vulnerability
   D. Exploit
2. Using which action does the IPS quietly drop the packets involved?
   A. Drop
   B. Reset
   C. Shun
   D. Block
3. Which of the following is *not* a drawback of a host-based IPS?
   A. A high number of false positives can cause a lax attitude on the part of the security team.
   B. Encrypted packets cannot be analyzed.
   C. It cannot monitor any internal activity that occurs within a system.
   D. It cannot address authentication issues.
4. Which evasion technique divides the packet into smaller pieces containing the malicious code so that it becomes difficult for the IPS to recognize the code?
   A. Packet fragmentation
   B. Injection attacks
   C. Injection attacks
   D. Cross-site scripting
5. Which of the following is *not* one of the four categories of functions of which FireSIGHT is capable?
   A. Detection
   B. Learning
   C. Adapting
   D. Block
6. Which of the following is any threat not yet remediated by malware vendors or software

vendors?

A. Zero-day attack

B. Risk

C. Vulnerability

D. Exploit

7. Which capability of FireSIGHT is aimed at malware?

A. Blacklisting

B. AMP

C. SNORT technology

D. Discovery and awareness

8. Which deployment mode has the sensor connected to a port on the switch to which all traffic has been mirrored?

A. SPAN

B. Tap

C. Inline

D. Promiscuous

9. Which evasion technique relies on the fact that many protocols' information can be communicated or expressed in multiple ways?

A. Packet fragmentation

B. Buffer overflows

C. Injection attacks

D. Cross-site scripting

10. Which of the following is susceptible to an external threat that a device or system may possess?

A. Zero-day attack

B. Risk

C. Vulnerability

D. Exploit

11. Using which action does the IPS accomplish the same purpose as a reset for non-TCP connections?

A. Drop

B. Reset

C. Shun

D. Block

12. In which deployment mode is the sensor placed in the line of traffic to analyze the original traffic, not a copy in real time?

A. SPAN

B. Tap

C. Inline

D. Promiscuous

13. In which positioning option will the IPS sensor generate a very high number of alarms?

A. Outside

B. DMZ

C. Inside

D. Remote

14. Which of the following occurs when a threat and a vulnerability both exist and a threat actor takes advantage of the situation?

A. Zero-day attack

B. Risk

C. Vulnerability

D. Exploit

15. Using which action does the IPS direct another device (a router or firewall) to block the traffic?

A. Drop

B. Reset

C. Shun

D. Block

16. In which deployment mode is the sensor placed between two layer 3 devices providing full-duplex connectivity between the devices and splitting off two simplex mirrors of the full-duplex traffic?

A. SPAN

B. Tap

C. Inline

D. Promiscuous

17. Which evasion technique inserts data that will be accepted by the IPS but will be ignored by the target system?

A. Packet fragmentation

B. Buffer overflow

C. Injection attacks

D. Cross-site scripting

18. Which of the following is a drawback of network-based IPS?

A. A high number of false positives can cause a lax attitude on the part of the security team.

B. Encrypted packets cannot be analyzed.

C. It cannot monitor any internal activity that occurs within a system.

D. It cannot address authentication issues.

19. Using which action does the IPS end any TCP connection?

A. Drop

B. Reset

C. Shun

D. Block

20. Which of the following is created when a threat exists to which a system is vulnerable?

A. Zero-day attack

B. Risk

C. Mitigation

D. Exploit

Chapter 17
Content and Endpoint Security

CISCO CCNA SECURITY EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓**7.1 Describe mitigation technology for email-based threats**
  - Spam filtering, anti-malware filtering, DLP, blacklisting, email encryption
- ✓**7.2 Describe mitigation technology for web-based threats**
  - Local and cloud-based web proxies
  - Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption
- ✓**7.3 Describe mitigation technology for endpoint threats**
  - Anti-virus/anti-malware
  - Personal firewall/HIPS
  - Hardware/software encryption of local data

Endpoint devices in the network such as laptops, printers, workstations, scanners, cameras, and other such devices represent one of our biggest challenges in securing the environment. First, there are so many more of these than there are infrastructure devices. Moreover, these devices are most likely in the hands of users who either lack security knowledge or just don't care about it. In this chapter, you'll learn how to overcome these challenges and secure the endpoints in the environment.

In this chapter, you will learn the following:

Mitigation technology for email-based threats, including SPAM filtering, anti-malware filtering, data loss prevention (DLP), blacklisting, and email encryption

Mitigation technology for web-based threats, including local and cloud-based web proxies, blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS/SSL decryption

Mitigation technology for endpoint threats, including antivirus/anti-malware, personal firewall/HIPS, and hardware/software encryption of local data

Mitigating Email Threats

Threats to email strike at the very heart of your enterprise communication system. It has become evident that even tech-savvy users can fall prey to these threats. In this section, you'll learn about a few methods you can use to mitigate these threats. These methods are not mutually exclusive, and when deployed together, they stand as a good example of exercising the principle of a layered defense or *defense in depth*. Following that, you'll learn about the ways the Cisco Email Security Appliance (ESA) can address these threats.

Spam Filtering

Spam is both an annoyance to users and an aggravation to email administrators who must deal with the extra space the spam takes up on the servers. Spam filters are designed to prevent spam from being delivered to mailboxes. The issue with spam filters is that often legitimate email is marked as spam. Finding the right setting can be challenging. Users should be advised that no filter is perfect and that they should regularly check quarantined email for legitimate emails.

Reputation-based filtering relies on the identification of email servers that have become known for sending spam. When a system can do this, it must rely on some service for developing these "reputations." As you will see later, an example is the *Cisco SenderBase*. This is the system the *Cisco Email Security Appliance (ESA)* uses. This repository manages reputation "scores" for servers based on any malicious activity in which the server is reported to have been involved.

Context-Based Filtering

Context-based filtering filters the message and attachments for sender identities, message content, embedded URLs, and email formatting. These systems use algorithms to examine these items to identify spam.

Anti-malware Filtering

Email can also introduce malware into the environment through both malicious attachments and deceptive links in emails. While user training is the best approach to preventing email-based malware, we know that it doesn't always work. Even security professionals have inadvertently clicked malicious links and attachments by mistake. To augment training, the examination of all email for malware and the filtering of such malicious mail should be parts of providing secure email.

DLP

Data leakage occurs when sensitive data is disclosed to unauthorized personnel either intentionally or inadvertently. *Data loss prevention (DLP)* software attempts to prevent data leakage. It does this by maintaining awareness of actions that can and cannot be taken with respect to a document. For example, it might allow printing of a document but only at the

company office. It might also disallow sending the document through email. DLP software uses ingress and egress filters to identify sensitive data that is leaving the organization and can prevent such leakage. Another scenario might be the release of product plans that should be available only to the sales group. The policy you could set for that document is as follows:

- It cannot be emailed to anyone other than sales group members.
- It cannot be printed.
- It cannot be copied.

There are two locations at which DLP can be implemented.

Network DLP Installed at network egress points near the perimeter, network DLP analyzes network traffic.

Endpoint DLP Endpoint DLP runs on end-user workstations or servers in the organization.

You can use both precise and imprecise methods to determine what is sensitive.

Precise methods These methods involve content registration and trigger almost zero false-positive incidents.

Imprecise methods These can include keywords, lexicons, regular expressions, extended regular expressions, metadata tags, Bayesian analysis, and statistical analysis.

The value of a DLP system resides in the level of precision with which it can locate and prevent the leakage of sensitive data.

Blacklisting

Blacklisting identifies bad senders. Whitelisting occurs when a list of acceptable e-mail addresses, Internet addresses, websites, applications, or other identifiers are configured as good senders or as allowed. Graylisting is somewhere in between the two when an entity cannot be identified as a whitelist or blacklist item. In the case of graylisting, the new entity must pass through a series of tests to determine whether it will be whitelisted or blacklisted. Whitelisting, blacklisting, and graylisting are commonly used with spam filtering tools.

Email Encryption

Email traffic, like any other traffic type, can be captured in its raw form with a protocol analyzer. If the email is clear text, it can be read. For this reason, encryption should be used for all emails of a sensitive nature. While this can be done using the digital certificate of the intended recipient, this is typically possible only if the recipient is part of your organization and your company has a public key infrastructure (PKI). Many email products include native support for digital signing and encryption of messages using digital certificates.

While it is possible to use email encryption programs like *Pretty Good Privacy (PGP)*, it is confusing for many users to use these products correctly without training. Another option is to use an encryption appliance or service that automates the encryption of email. Regardless of

the specific approach, encryption of messages is the only mitigation for information disclosure from captured packets.

Cisco Email Security Appliance

The Cisco Email Security Appliance can address each of these concerns. The features that address email issues in the ESA are covered in this section. At the end of the section is a discussion of the message flow when using ESA.

Reputation and Context-Based Filtering

ESA performs both types of filtering. When utilizing the Cisco SenderBase, the actions taken by ESA depend on the reputation score of the source. If the sender score is between –1 and +10, the email is accepted. If it is –1 and –3, the email is accepted but additional emails are throttled. If it is between –10 and –3, it is blocked.

Viruses and Anti-malware

ESA uses a multilayer approach to this issue. The three layers of defense are as follows:

Outbreak Filters Downloaded from the Cisco SenderBase. These filters are generated by watching global email traffic patterns and looking for signs of an outbreak. When an email is received from a server on the list, it is quarantined until antivirus signatures are updated that address the risk.

Antivirus Signatures Used in the same way any anti-malware product uses them: to identify the presence of malware in the email.

Outbound Scanning Scans email that is leaving for the presence of malware.

Email Data Loss Prevention and Encryption

ESA's DLP features use rules for identifying classes of sensitive information such as personally identifiable information (PII), payment card numbers, bank routing numbers, financial account information, government ID numbers, personal names, addresses and phone numbers, and healthcare records. Moreover, you can design your own classes that include data not in these categories. Encryption is also possible to protect any sensitive information that must be sent.

Advanced Malware Protection

Advanced Malware Protection (AMP) is the malware component in ESA that uses a combination of several technologies to protect you from email-based malware.

File Reputation A fingerprint of every file that traverses the Cisco email security gateway is sent to AMP's cloud-based intelligence network for a reputation verdict. Based on these results, you can block malicious files identified as having a bad reputation.

File Retrospection Sometimes files enter the network and are later identified as being a threat.

This allows for the identification and removal of these files later. If malicious behavior is spotted later, AMP sends a retrospective alert so that you can contain and remediate the malware. This process is depicted in Figure 17.1 .

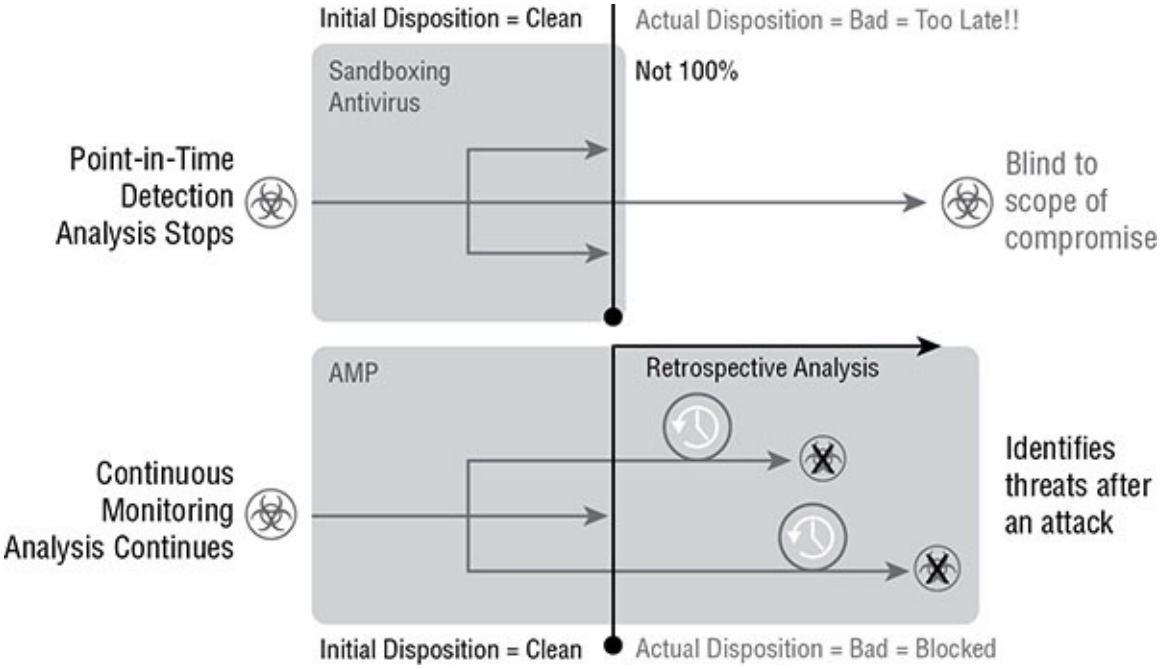

FIGURE 17.1 File retrospection

File Sandboxing This provides the ability to analyze files that traverse the gateway. Then in the safe sandboxed environment, AMP can obtain details about the threat level of the malware and communicate that information to the Cisco Talos intelligence network to update the AMP cloud data for all.

ESA Message Flow

ESA performs its job by acting as a message transfer agent (MTA) in the email system. Another name for this function is *email relay*. Figure 17.2 shows a normal inbound message flow.

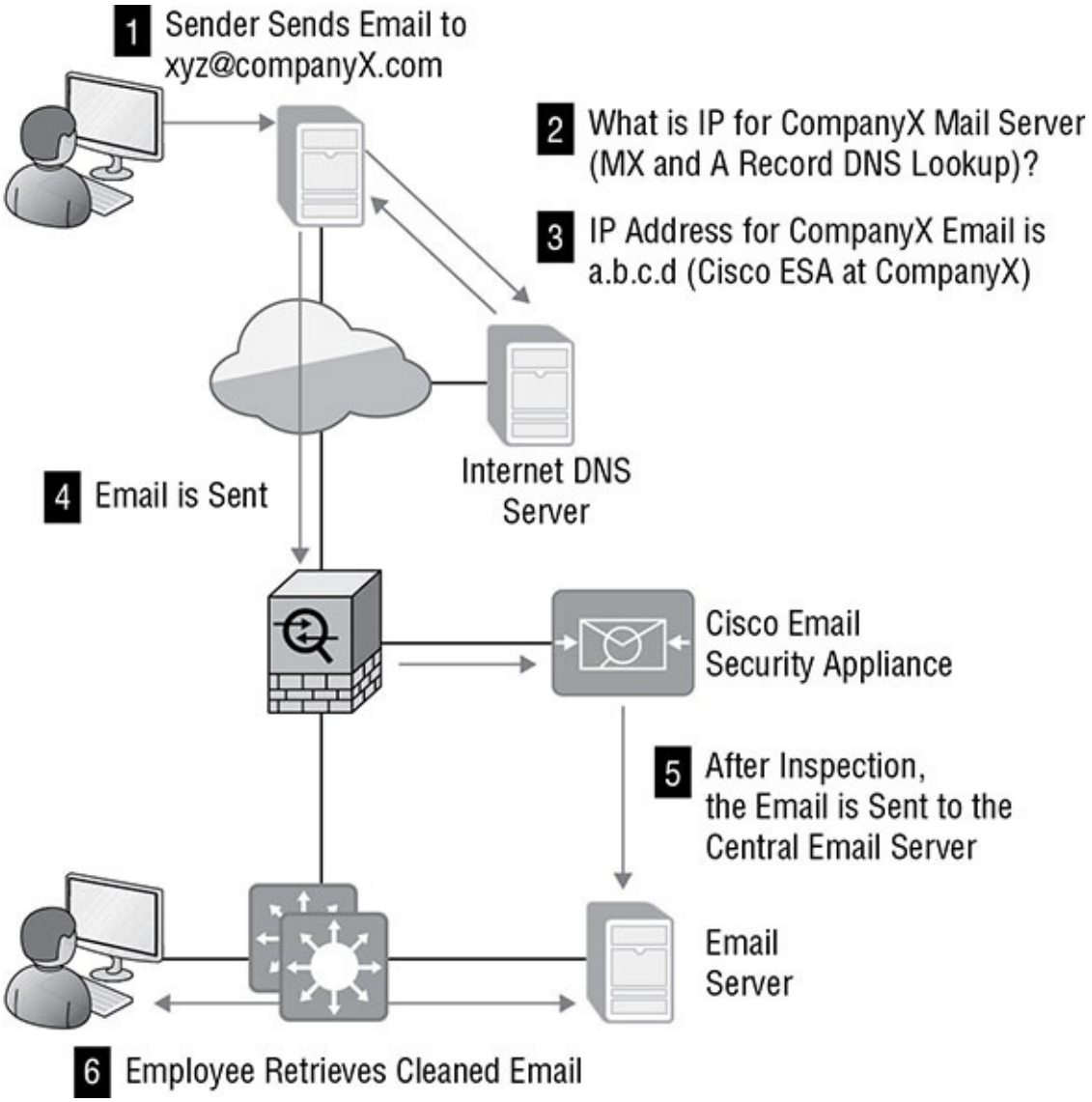

FIGURE 17.2 ESA inbound

Figure 17.3 shows a normal outbound message flow.

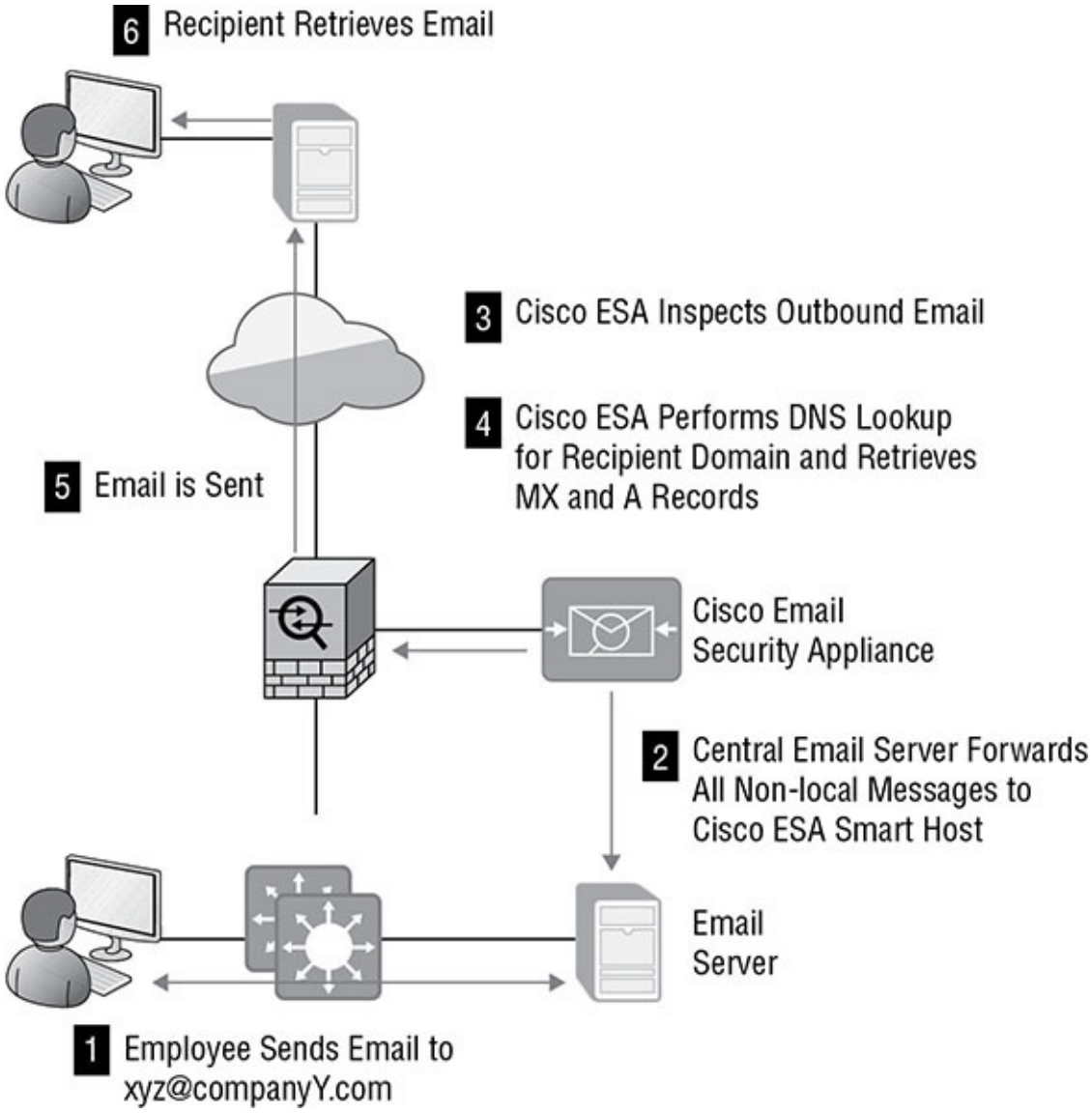

FIGURE 17.3 ESA outbound

Putting the Pieces Together

The various components that ESA brings to bear in its role as an email security utility work together in an integrated fashion, as shown in Figure 17.4 , which is how ESA operates against incoming email.

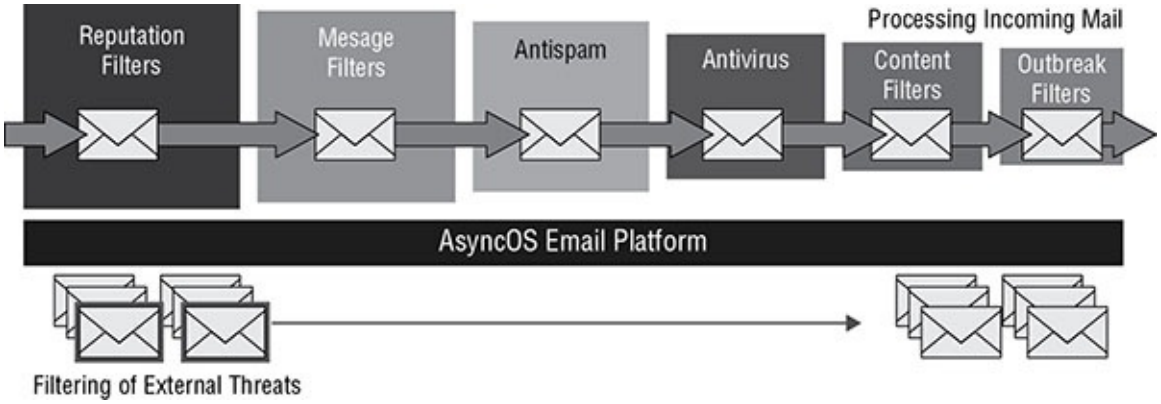

FIGURE 17.4 Incoming mail processing

Regarding email that is leaving the organization, the operations of these components are depicted in Figure 17.5 .

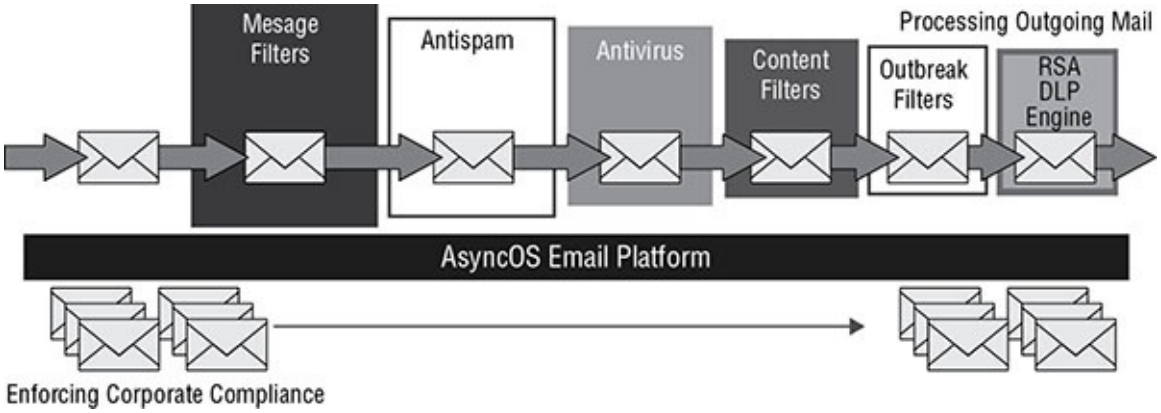

FIGURE 17.5 Outgoing mail processing

Mitigating Web-Based Threats

Another threat that presents itself to most enterprises is aimed at their web services. While not every organization has the need for an e-commerce server, almost every organization has a website or some type of web presence. Even a defacing of a public website, while not costly from a monetary standpoint, hurts the reputation and image of an organization.

One of the common ways of addressing threats against web applications and the web server software upon which they operate is a web proxy. Proxy servers in general stand between internal users or internal applications and potentially malicious requests coming from the Internet. *Web proxies* are a type of proxy that stands between a web application and web request coming from the Internet. This section discusses web proxies and the functions they perform.

Understanding Web Proxies

Proxy servers can be appliances, or they can be installed on a server operating system. These servers act like a proxy firewall in that they create the web connection between systems on

their behalf, but they can typically allow and disallow traffic on a more granular basis. For example, a proxy server may allow the sales group to go to certain websites while not allowing the data entry group access to those same sites. The functionality extends beyond HTTP to other traffic type, such as FTP traffic.

Proxy servers can provide an additional beneficial function called *web caching*. When a proxy server is configured to provide web caching, it saves a copy of all web pages that have been delivered to internal computers in a web cache. If any user requests the same page later, the proxy server has a local copy and need not spend the time and effort to retrieve it from the Internet. This greatly improves web performance for frequently requested pages.

From a deployment perspective, web proxies can be implemented in two ways.

Local

A *local proxy* is one that is installed on the premises in which all of the processing occurs on the local web proxy.

Cloud-Based

A *cloud-based web proxy* is one that transmits the traffic to a cloud location where all the operations that would occur on a local web proxy occur in the cloud. In some cases, this offers the advantage of additional intelligence services that can aggregate and analyze telemetry data from billions of web requests, malware samples, and emerging attack methods.

Cisco Web Security Appliance

The *Cisco Web Security Appliance (WSA)* is a web proxy that integrates with other network components to monitor and control outbound requests for web content. Traffic can be directed to the WSA explicitly on the end host or by using Web Cache Control Protocol on an inline device like the perimeter router. The features it provides are covered in this section and will be followed by a description of traffic flow when using a WSA.

Blacklisting

Blacklisting and whitelisting can be used to create and support the acceptable use policy (AUP) of the organization. Moreover, it helps to prevent malware from malicious sites from entering the network.

URL Filtering

The WSA reputation filters operate much like the reputation filters used in ESA, with the difference being that they operate against web domains rather than email sources. By leveraging Cisco Security Intelligence Operations (SIO), Cisco Ironport reputation filters analyze more than 50 web and network parameters to evaluate a website’s trustworthiness.

Malware Scanning

The WSA anti-malware system uses multiple scanning engines in a single appliance. It uses the Dynamic Vectoring and Streaming Engine and verdict engines from both WebRoot and McAfee.

URL Categorization

The Cisco URL filters can also be managed using access policies based on 52 predefined categories and an unlimited number of customer categories of sites. These can be used along with time-based polices to add additional flexibility.

Web Application Filtering

WSA uses *Application Visibility and Control (AVC)* to allow for the control of the use of web applications. Granular policy control allows administrators to permit the use of applications such as Dropbox or Facebook while blocking users from activities such as uploading documents or clicking the Like button.

TLS/SSL Decryption

In Cisco AsyncOS 9.0.0-485, the operating system in WSA, you can now enable and disable SSL v3 and various versions of TLS for several services. Disabling SSL v3 for all services is recommended for best security. You also can enable a protocol fallback option.

Mitigating Endpoint Threats

This section discusses the protection of endpoints. Many of the items discussed in this section can be managed manually or with third-party tools, but many of the items can be managed automatically using the Identity Services Engine (ISE). Before we discuss the security measures in this section and their potential relationship with ISE, let's take a brief look at ISE.

Cisco Identity Services Engine (ISE)

Finally, if the organization is implementing a BYOD policy, it can streamline this with self-service onboarding and management. While many of these features are beyond the scope of this book, we are going to discuss how it can handle the settings in this section.

Antivirus/Anti-malware

The Cisco ISE posture service interrogates a device requesting access for information regarding the presence of and proper configuration of antivirus and/or anti-malware software. It also checks for the presence of the latest available updates. Only when the machine is fully compliant is it allowed full access to the network.

Personal Firewall

While the Cisco ISE posture service verifies the presence of and proper configuration of antivirus and/or anti-malware software, it doesn't stop there. It can also verify the function and

settings of the personal firewall. It can compare this with a baseline for compliance in the same way it verifies the antivirus and/or anti-malware software.

Hardware/Software Encryption of Local Data

Finally, sensitive data located in endpoints should be secured with either hardware or software encryption. Cisco ISE can be used to implement a mobile management solution that can require encryption of the storage in both easily stolen mobile devices and other devices that may contain sensitive information.

HIPS

While not a function that can be controlled through ISE or TrustSec, a *host-based IPS (HIPS)* monitors traffic on a single system. Its primary responsibility is to protect the system on which it is installed. An HIPS typically works closely with anti-malware products and host firewall products. They generally monitor the interaction of sites and applications with the operating system and stop any malicious activity or, in some cases, ask the user to approve changes that the application or site would like to make to the system.

These systems can use several methods of detecting intrusions. The two main methods are as follows:

- *Signature based*: Analyzes traffic and compares patterns, called *signatures*, that reside within the IDS database. This requires constant updating of the signature database.
- *Anomaly based*: Analyzes traffic and compares it to normal traffic to determine whether the traffic is a threat. This means any traffic out of the ordinary will set off an alert.

Summary

In this chapter, you learned mitigation techniques available when using the Cisco Email Security Appliance. This included reputation and context-based filtering. You also were introduced to the Cisco Web Security Appliance, which can use blacklisting, URL filtering, and malware scanning to secure web traffic and web applications. Finally, the chapter discussed endpoint protection provided by the Cisco Identity Services Engine and Cisco TrustSec technology.

Exam Essentials

Identify the processes used by Cisco ESA to protect email. These processes include spam filtering, reputation-based filtering, context-based filtering, anti-malware filtering, data loss prevention, blacklisting, and email encryption.

Describe the actions of which the Cisco Web Security Appliance is capable. Some examples of these actions are blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS/SSL decryption.

Differentiate endpoint threats. These threats include viruses and malware, data disclosure, peer-to-peer attacks, and unauthorized access.

Identify techniques employed by the Cisco Identity Services Engine. These include access management, 802.1x, health and patch assessment, and verification of settings in the personal firewall.

Review Questions

1. Which of the following relies on the identification of email servers that have become known for sending spam?
   A. Context-based filtering
   B. Reputation-based filtering
   C. Data-based filtering
   D. Domain-based filtering
2. Which of the following occurs when sensitive data is disclosed to unauthorized personnel either intentionally or inadvertently?
   A. Data leakage
   B. Data egress
   C. Information corruption
   D. Unintended release
3. Which of the following is installed at network egress points near the perimeter?
   A. Client DLP
   B. Network DLP
   C. Endpoint DLP
   D. Composite DLP
4. Which of the following trigger almost zero false-positive incidents?
   A. Precise methods
   B. Complete methods
   C. Imprecise methods
   D. Sparse methods
5. With which sender score does ESA accept an email?
   A. Between –1 and +10

B. Between –1 and –3

C. Between –10 and –3

D. Between +10 and +20

6. Which of the following is the malware component in ESA?

A. AMP

B. MAP

C. CMP

D. EMP

7. Which capability of AMP sends a fingerprint of every file that traverses the Cisco email security gateway to AMP's cloud-based intelligence network?

A. File reputation

B. File retrospection

C. File sandboxing

D. File examination

8. Which of the following uses real-time analysis on a vast, diverse, and global dataset to detect URLs that contain some form of malware?

A. SPAN

B. WBRS

C. WCCP

D. SIO

9. Which of the following is a web proxy that integrates with other network components to monitor and control outbound requests for web content?

A. ESA

B. AMP

C. WSA

D. ISE

10. Which component analyzes more than 50 web and network parameters to evaluate a website's trustworthiness?

A. Cisco Ironport

B. Dynamic Vectoring and Streaming Engine

C. Web Cache Control Protocol

D. Message Transfer Agent (MTA)

11. With which sender score does ESA block the email?
    A. Between –1 and +10
    B. Between –1 and –3
    C. Between –10 and –3
    D. Between +10 and +20
12. Which capability of AMP provides the ability to analyze files that traverse the gateway?
    A. File reputation
    B. File retrospection
    C. File sandboxing
    D. File examination
13. Which of the following uses the Dynamic Vectoring and Streaming Engine?
    A. ESA
    B. AMP
    C. WSA
    D. ISE
14. Which of the following allows administrators to permit the use of applications such as Dropbox or Facebook?
    A. ESA
    B. AMP
    C. WSA
    D. AVC
15. Which of the following can provide AAA services so that you can deploy 802.1x security?
    A. ESA
    B. ISE
    C. WSA
    D. AVC
16. Which capability of AMP allows for the identification and removal of these files after they are accepted?
    A. File reputation
    B. File retrospection

C. File sandboxing

D. File examination

17. With which sender score does ESA accept the email but additional emails are throttled?

A. Between –1 and +10

B. Between –1 and –3

C. Between –10 and –3

D. Between +10 and +20

18. Which of the following can include keywords, lexicons, and regular expressions?

A. Precise methods

B. Complete methods

C. Imprecise methods

D. Sparse methods

19. Which of the following is installed on end-user workstations?

A. Client DLP

B. Network DLP

C. Endpoint DLP

D. Composite DLP

20. Which of the following filters the message and attachments for sender identities, message content, embedded URLs, and email formatting?

A. Context-based filtering

B. Reputation-based filtering

C. Data-based filtering

D. Domain-based filtering

Appendix
Answers to Review Questions

Chapter 1: Understanding Security Fundamentals

1. D. Accountability, although important, is not part of the CIA triad. The CIA triad includes confidentiality, integrity, and availability.
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. Its main purpose is to ensure that users have access only to the resources they need and are authorized to perform only the tasks they need to perform.
3. B. A threat occurs when vulnerability is identified or exploited. A threat would occur when an attacker identified the folder on the computer that has an inappropriate or absent access control list.
4. D. NIST SP 800-30 identifies the following steps in the risk management process:
    1. Identify the assets and their value.
    2. Identify threats.
    3. Identify vulnerabilities.
    4. Determine likelihood.
    5. Identify impact.
5. B. Sensitivity is a measure of how freely the data can be handled. Some data requires special care and handling, especially when inappropriate handling could result in penalties, identity theft, financial loss, invasion of privacy, or unauthorized access by an individual or many individuals.
6. C. These are typical commercial classifications:
    1. Confidential
    2. Private
    3. Sensitive
    4. Public
7. C. The Traffic Light Protocol classifications are:

Color	**Meaning**
Red	Shared only within a meeting
Amber	Shared only with those in the organization with a need to know
Green	Shared only within a community
White	No restriction but still subject to copyright rules

8. C. Security Content Automation Protocol (SCAP) is a standard used by the security automation community used to enumerate software flaws and configuration issues. It

standardized the nomenclature and formats used.

9. B. These metric groups are described as follows:

   Base: Characteristics of a vulnerability that are constant over time and user environments

   Temporal: Characteristics of a vulnerability that change over time but not among user environments

   Environmental: Characteristics of a vulnerability that are relevant and unique to a particular user's environment

10. D. The SLE is the monetary impact of each threat occurrence. To determine the SLE, you must know the asset value (AV) and the exposure factor (EF). The EF is the percent value or functionality of an asset that will be lost when a threat event occurs. The calculation for obtaining the SLE is as follows:

    SLE = AV × EF

11. B. Mitigation is the process of selecting a control that will reduce the risk to an acceptable level.

12. B. The enterprise campus includes the end devices and provides them with access to the outside world and to the Intranet data center through the enterprise core.

13. B. A demilitarized zone (DMZ) is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network.

14. A. Network security zones can also be created at layer 2. Virtual local area networks (VLANs) are logical subdivisions of a switch that segregate ports from one another as if they were in different LANs.

15. B. 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.

16. B. A defense-in-depth strategy refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers. The first layer of a good defense-in-depth strategy is appropriate access control strategies.

17. A. A risk is the probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out. The risk in the vulnerability example would be fairly high if the data residing in the folder is confidential. However, if the folder contains only public data, then the risk would be low.

18. C. This classification system created by the United Kingdom's National Infrastructure Security Coordination Centre (NISCC, now Centre for Protection of National Infrastructure) and since adopted by the ISO/IEC as part of the Standard on Information security management for intersector and interorganizational communications and by CERT is the Traffic Light Protocol (TLP). This system uses traffic light colors to classify

information assets.

19. B. Common Vulnerabilities and Exposures (CVE) is a compilation of common vulnerabilities found in operating systems and applications.

20. C. The exposure factor (EF) is the percent value or functionality of an asset that will be lost when a threat event occurs.

Chapter 2: Understanding Security Threats

1. C. Hacktivists include those who hack not for personal gain but to further a cause. An example is the Anonymous group that hacks from time to time for various political reasons.
2. A. IP address spoofing is one of the techniques used by hackers to hide their trail or to masquerade as another computer. The hacker alters the IP address as it appears in the packet. This can sometimes allow the packet to get through an ACL that is based on IP addresses.
3. C. Port scanning is not a password attack. By determining the services that are running on a system, the attacker also discovers potential vulnerabilities of the service of which the attacker may attempt to take advantage. This is typically done with a port scan in which all "open" or "listening" ports are identified.
4. C. When this packet is sent, these responses are possible:

   No response: The port is open on the target.

   RST: The port is closed on the target.
5. A. 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. The key to preventing many buffer overflow attacks is input validation, in which any input is checked for format and length before it is used.
6. D. A man-in-the-middle attack is launched from a single malicious individual, while DDoS attacks come from multiple devices.
7. A. 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 the attacker's 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 the attacker "in the middle."
8. 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. This table is built by also monitoring all DHCP requests for IP addresses and maintaining the mapping of each resulting IP address to a MAC address (which is part of DHCP snooping). If an incorrect mapping is attempted, the switch rejects the packet.
9. C. The main purpose of DHCP snooping is to prevent a poisoning attack on the DHCP database. This is not a switch attack per se, but one of its features can support DAI. It creates a mapping of IP addresses to MAC addresses from a trusted DHCP server that can be used in the validation process of DAI.

10. D. A virus is any malware that attaches itself to another application to replicate or distribute itself.

11. B. Intellectual property is property that is considered to be a unique creation of the mind and includes books, music, logos, inventions, and slogans.

12. C. The best mitigation for credit data theft is to adopt all recommendations of the Payment Card Industry Data Security Standard (PCI-DSS).

13. B. MAC addresses can also be spoofed and used to get through MAC address filters. These filters are typically applied to control access to wireless access points at layer 2.

14. A. A possible mitigation technique is to implement the Sender Policy Framework (SPF). 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.

15. B. Nmap is one of the most popular port scanning tools used today. By performing scans with certain flags set in the scan packets, security analysts (and hackers) can make certain assumptions based on the responses received.

16. C. An XMAS scan sets the FIN, PSH, and URG flags. When this packet is sent, these responses are possible:

    No response: The port is open on the target.

    RST: The port is closed on the target.

17. A. The ping-of-death attack is one in which an oversized ICMP packet is sent to the target. The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes. An ICMP echo request is an IP packet with a pseudoheader, which is 8 bytes. Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes (65,535 – 20 – 8 = 65,507).

18. B. In a reflected DDoS attack, the attack is bounced off a large number of devices without actually recruiting the devices as zombies. A good example of this type of DDoS is the smurf attack.

19. C. The dynamic ARP inspection security feature 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. This prevents ARP poisoning attacks.

20. B. Pharming is similar to phishing, but pharming actually pollutes the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.

Chapter 3: Understanding Cryptography

1. A. A symmetric key algorithm does not use a public key. It uses a matching or private key for both encryption and decryption.
2. B. Asymmetric algorithms are *not* typically used for data at rest because they are very slow in relation to symmetric algorithms at this task. Asymmetric algorithms are used for data in transit.
3. D. Block ciphers employ both substitution and transposition.
4. B. Stream-based ciphers perform encryption on a bit-by-bit basis and use keystream generators. The keystream generators create a bit stream that is XORed with the plaintext bits. The result of this XOR operation is the ciphertext.
5. A. Some modes of symmetric key algorithms use initialization vectors (IVs) to ensure that patterns are not produced during encryption. These IVs provide this service by using random values with the algorithms.
6. B. Although Electronic Code book (ECB) is the easiest and fastest mode to use, it has security issues because every 64-bit block is encrypted with the same key. If an attacker discovers the key, all the blocks of data can be read.
7. B. AES is the replacement algorithm for 3DES and DES. Although AES is considered the standard, the algorithm that is used in the AES standard is the Rijndael algorithm. The AES and Rijndael terms are often used interchangeably.
8. A. RSA is the most popular asymmetric algorithm and was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA can provide key exchange, encryption, and digital signatures. The strength of the RSA algorithm is the difficulty of finding the prime factors of very large numbers.
9. C. A collision occurs when a hash function produces the same hash value on different messages.
10. D. The U.S. government requires the usage of SHA-2 instead of MD5.
11. B. A hash MAC (HMAC) is a keyed-hash MAC that involves a hash function with a symmetric key. HMAC can help reduce the collision rate of the hash function.
12. C. A digital signature is a hash value encrypted with the sender’s private key. A digital signature provides authentication, nonrepudiation, and integrity.
13. A. To use symmetric key algorithms for encrypting data, the two parties must share an identical symmetric key. This means we need some secure way to get identical symmetric keys on the two endpoints. This is done by using asymmetric algorithms for the key exchange and, once the keys are generated and exchanged, using the symmetric keys and a symmetric key algorithm for the encryption of the data. This is often called a hybrid cryptosystem.

14. A. Users and devices are issued public/private key pairs that are bound to a digital document called a digital certificate. This certificate (more specifically the keys to which it is bound) can be used for a variety of things including:

    Encrypting data

    As a form of authentication

    Encrypting email

    Digitally signing software

15. B. An X.509 certificate complies with the X.509 standard.

16. B. A CRL is a list of digital certificates that a CA has revoked. To find out whether a digital certificate has been revoked, the browser must either check the CRL or push out the CRL values to clients.

17. A. VeriSign first introduced the following digital certificate classes:

    Class 1: For individuals intended for e-mail. These certificates get saved by web browsers.

    Class 2: For organizations that must provide proof of identity.

    Class 3: For servers and software signing in which independent verification and identity and authority checking is done by the issuing CA.

    Class 4: For online business transactions between companies.

    Class 5: For private organizations or governmental security.

18. B. Any participant that requests a certificate must first go through the registration authority (RA), which verifies the requestor's identity and registers the requestor. After the identity is verified, the RA passes the request to the CA. In many cases, the CA and the RA are the same server.

19. B. In some cases, two organizations may have a need to trust one another's certificates. This can be done by configuring cross certification. In cross certification, a trust is created between the two root CAs, which enables both systems to trust all certificates.

20. B. The ASA has a self-signed default certificate that can be used, although in most cases it will be desirable to install a certificate from your PKI.

Chapter 4: Securing the Routing Process

1. D. While configuring a loopback IP address to be used for management access is certainly advisable, it is not required when configuring a router for SSH access.
2. C. The syslog message indicates that SSH version 1.99 has been enabled. This indicates that it is a version 2 server that can accept connections from SSH version 1 devices.
3. D. The line in the configuration that says `login local` specifies that the user accounts will be local to this router.
4. A. Privilege levels allow you to assign a technician sets of activities that coincide with the level the technician has been assigned. There are 16 levels, from 0 to 15. When you are in user mode (`router>`), you are at privilege level 0. When you are in privileged mode (router#), you are at level 15.
5. C. If the intent is to allow this technician to change IP addresses on interfaces, assign him that command. Since the `ip` command (along with the parameter address) is executed after entering interface configuration mode, you have to reference `interface` in the command, as shown here:

   ```
   router(config)#privilege interface level 12 ip
   ```
6. B. The only view that exists by default is called *root*, which as you would expect allows access to all commands. Access to this view is provided when you submit the `enable secret` password.
7. B. To enable the protection of the boot image, issue the following command:

   ```
   R64(config)#secure boot-image
   ```

   ```
   *April 2 14:24:50.231: %IOS_Reslience-5-IMAGE_RESIL_ACTIVE: Successfully
   secured running image
   ```

   Notice the system message indicating the boot image is protected.
8. B. A secure configuration can be removed. Once these two items are secured (called the *secure bootset*), you cannot update the startup configuration without removing the secure configuration long enough to make the change and resecuring it as was done in the first place.
9. B. Commands that remove a secure bootset configuration can be run *only* from the console connection.
10. B. OSPF routing updates are secured using a hashing algorithm. You can use either MD5 or SHA-256HMAC. Be aware, however, that some devices may support only MD5.
11. C. While keychain names and the key numbers do not have to match on the two routers on either end of the link, the key strings and the hashing algorithms *must* match!
12. C. The final step is to apply the keychain to the interface that connects to the neighboring router.

13. A. Keychain configuration mode is the mode in which you will define the key number as follows. The number I am using is 1.

```
R64(config-keychain)#key 1
R64(config-keychain-key)#
```

14. A. Telling the router the algorithm (MD5) to use for this key is done at the same key prompt as follows:

```
R64(config-keychain-key)#cryptographic-algorithm md5
R64(config-keychain-key)#
```

15. A. Configuring EIGRP routing update authentication is similar to OSPF. However, OSPF specifies the hashing algorithms in the same mode where you specify the key string, but in EIGRP, that is specified on the interface.

16. B. When you specify the algorithm, you also specify the EIGRP AS number in the same command as follows, where 66 is the AS number:

```
R64(config-if)#up authentication mode eigrp 66 md5
```

17. A. There are four types of packets that a router may encounter. Data plane packets are end-station, user-generated packets that are always forwarded by network devices to other end-station devices.

18. B. There are four types of packets that a router may encounter. Control plane packets are network device–generated or received packets that are used for the creation and operation of the network. Examples include protocols such as ARP, BGP, and OSPF.

19. C. Packets in the control plane are those that are either destined for the router itself or packets generated by the router.

20. B. In this model, three mechanisms are used. Class maps are used to categorize traffic types into classes. ACLs are typically used to define the traffic, and then the ACL is referenced in the class map. Policy maps are used to define the action to be taken for a particular class. Actions that can be specified are allow, block, and rate-limit. Service policies are used to specify where the policy map should be implemented.

Chapter 5: Understanding Layer 2 Attacks

1. C. When a malicious individual introduces a rogue switch to the switching network and the rogue switch has a superior BPDU to the one held by the current root bridge, the new switch assumes the position of root bridge.
2. B. An ARP poisoning attack is one that takes advantage of the normal process that devices use to learn an unknown MAC address that a device with a known IP address possesses. By using a gratuitous ARP, the ARP cache of other devices can be poisoned.
3. A. In an ARP poisoning attack, the attacker sends a packet type called a gratuitous ARP to the target device with an incorrect IP address to MAC address mapping.
4. C. First an area of memory called the ARP cache is consulted. If the MAC address has been recently resolved, the mapping will be in the cache, and a broadcast is not required. If the record has aged out of the cache, ARP sends a broadcast frame to the local network that all devices will receive.
5. C. MAC spoofing attacks occur when an attacker changes his MAC address so that he appears to be another device, and as is the case with all spoofing attacks, the ultimate aim is to receive something intended for the real device or to get past access controls based on a MAC address.
6. A. A MAC address attack is also considered a switch attack because it leverages the MAC address table in the switch to accomplish the goal of receiving traffic destined for another device.
7. C. The MAC address table is also called the content addressable memory (CAM) table and is populated by the switch as frames are switched through it.
8. B. There is a limited amount of memory space that is available for the CAM table. In a CAM overflow attack, the attacker floods the switch with frames that have invalid source MAC addresses. This is easier than it sounds by using a tool such as `macof`.
9. B. The result of this attack is that the attacker is now able to receive traffic that he would not have been able to see otherwise because in this condition the switch is basically operating as a hub and not a switch.
10. A. Cisco Discovery Protocol (CDP) and its standards-based alternative Link Layer Discovery Protocol (LLDP) are useful tools. They can be used to display information about directly connected devices.
11. C. To disable CDP globally, run the following command in global configuration mode:

    ```
    Router67(config)#no cdp run
    ```

12. D. To disable LLDP on an interface, run the following command in interface configuration mode:

    ```
    Router67(config-if)#no lldp receive
    ```

13. B. A VLAN hopping attack's aim is to receive traffic from a VLAN of which the hacker's port is not a member.

14. A. A VLAN hopping attack's aim is to receive traffic from a VLAN of which the hacker's port is not a member. It can be done two ways: switch spoofing and double tagging.

15. C. Switch ports can be set to use a protocol called Dynamic Trunking Protocol (DTP) to negotiate the formation of a trunk link. If an access port is left configured to use DTP, it is possible for hackers to set their interface to spoof a switch and use DTP to create a trunk link. If this occurs, they can capture traffic from all VLANs.

16. B. Double tagging is only an issue on switches that use "native" VLANs. A native VLAN is used for any traffic that is still a member of the default VLAN, or VLAN 1.

17. A. When configured properly, DHCP reduces administrative overload, reduces the human error inherent in manual assignment, and enhances device mobility. But it introduces a vulnerability that when leveraged by a malicious individual can result in an inability of hosts to communicate (constituting a DoS attack) and can result in peer-to-peer attacks.

18. A. After receiving an incorrect IP address, subnet mask, default gateway, and DNS server address from the rogue DHCP server, the DHCP client might use the attacker's DNS server to obtain the IP address of his bank. This leads him to unwittingly connect to the attacker's copy of the bank's website. When the client enters his credentials to log in, the attacker now has his bank credentials and can proceed to empty out his account.

19. A. Trunk ports use an encapsulation protocol called 802.1q to place a VLAN tag around each frame to identity the VLAN to which the frame belongs. When a switch at the end of a trunk link receives an 802.1q frame, it strips this off and forwards the traffic to the destination device. In a double tagging attack, the hacker creates a special frame that has two tags. The inner tag is the VLAN to which the hacker wants to send a frame (perhaps with malicious content), and the outer tag is the real VLAN of which the hacker is a member. If the frame goes through two switches (which is possible since VLANs can span switches), the first tag gets taken off by the first switch, leaving the second, which allows the frame to be forwarded to the target VLAN by the second switch.

20. C. Switch ports can be set to use a protocol called Dynamic Trunking Protocol (DTP) to negotiate the formation of a trunk link. If an access port is left configured to use DTP, it is possible for hackers to set their interface to spoof a switch and use DTP to create a trunk link. If this occurs, they can capture traffic from all VLANs.

Chapter 6: Preventing Layer 2 Attacks

1. C. This feature works by filtering the DHCP messages sent by the rogue DHCP server so that they are never received by the unsuspecting hosts. It also uses the messages sent to and from the legitimate DHCP server to build a binding database that maps the MAC addresses of hosts to the IP addresses they received from the legitimate DHCP server.
2. D. As a matter of fact, any server response packets (DHCPOFFER, DHCPACK, or DHCPNACK) will be dropped by these interfaces.
3. B. The DAI feature requires that DHCP snooping also be enabled because it depends on the DHCP snooping database that is created when DHCP snooping is enabled.
4. A. These interfaces will require that you create a type of ACL on the switch called an ARP ACL. This ACL identifies the correct IP to MAC address mapping for the interface, and the ACL is referenced as a filter in the DAI configuration. This makes the ACL available to the DAI process as an addition to the DHCP snooping database.
5. D. You can also choose the following actions using alternative keywords to the `shutdown` keyword:

   `protect`: The offending frame will be dropped.

   `restrict`: The frame is dropped, and an SNMP trap and a syslog message are generated.
6. B. By limiting the number of MAC addresses that can be seen on a port, CAM overflow attacks can be prevented.
7. A. BPDU Guard should be implemented *only* on access ports because if implemented on trunks, it would interfere with the normal operation of STP, which depends on these frames for its operation.
8. C. Root Guard prevents the reception of superior BPDUs *only*, not all BPDUs.
9. B. This feature makes additional checks if BPDUs are not received on a nondesignated port. With Loop Guard enabled, that port moves into the STP loop-inconsistent blocking state, instead of the listening/learning/forwarding state.
10. B. To disable DTP on all ports, use the following command:

    ```
    SW71(config)#int fa0/1 - 24
    SW71(config-if)#switchport nonegotiate
    ```
11. C. With the Restrict setting, if a violation occurs, the fa5/5 interface will not forward the offending traffic, will *not* send an SNMP trap or syslog message, and will *not* increment the violation counter, but will still pass legitimate traffic.
12. A. The BPDU Guard feature is designed to prevent the reception of superior BPDUs on access ports by preventing the reception of any BPDU frames on the access port. By doing so, it prevents the introduction of a rogue switch.

13. A. The port where the legitimate DHCP server resides must be marked as trusted so that DHCP server responses are allowed on that port.
14. A. If you configure a file in flash memory for the DHCP snooping database and the switches reload for some reason, they will retain this database.
15. B. The default state is untrusted.
16. C. While the VLAN number is used in the name of the ACL (StaticIP-VLAN3), that is not what ties it to VLAN. It is the explicit reference to VLAN3 at the end of the command that does it.
17. A. Before the other commands become effective, you must enable port security with the `switchport port-security` command.
18. D. While DAI can prevent ARP attacks, it cannot prevent STP attacks.
19. C. When a violation occurs, the port will be placed in an err-disabled state and will not pass traffic until it is enabled again manually.
20. D. DTP should be disabled on all ports, both trunk and access.

Chapter 7: VLAN Security

1. A. In a double tagging attack, the attacker crafts a packet with two 802.1q tags, with the inner tag set to the VLAN to which he would like to send traffic. This attack takes advantage of the native VLAN. If the attacker's access port is set to the same VLAN as the native VLAN, this attack becomes possible.
2. D. The solution is to set the native VLAN number to one in which *none* of the access ports resides. This is done only on the trunk ports. To change the native VLAN of the trunk port `Gi 0/1` to 78, use the following command:

   ```
   Switch79(config)#int gi 0/1
   Switch79(config-if)#switchport trunk native vlan 78
   ```
3. D. There are many challenges to providing a separate VLAN per customer, but a decrease in security is not one of them.
4. A. Private VLANs provide separation within a VLAN at layer 2, while still leaving all members of the original VLAN (called the primary VLAN) in the same subnet.
5. A. To change the native VLAN of the trunk port `Gi 0/1` to 78, use the following command:

   ```
   Switch79(config)#int gi 0/1
   Switch79(config-if)#switchport trunk native vlan 78
   ```
6. A. Promiscuous ports can communicate with a port of any other type. Typical candidates for this port assignment are those ports leading to the router or firewall that act as the default gateway for the primary VLAN.
7. D. While a good idea to prevent double tagging attacks, setting the native VLAN number to one in which *none* of the access ports resides is *not* a step in setting up PVLANs.
8. C. To configure the primary VLAN as 10, specifying it as a primary PVLAN, use the following commands:

   ```
   Switch# configure terminal
   Switch(config)# vlan 10
   Switch(config-vlan)# private-vlan primary
   ```
9. A. Typical candidates for this port assignment are those ports leading to the router or firewall that act as the default gateway for the primary VLAN.
10. C. To associate private VLANs 501, 502, and 503 with a primary VLAN 10, use the following commands:

    ```
    Switch(config)# vlan 10
    Switch(config-vlan)# private-vlan association 501-503
    ```
11. A. The command `switchport mode private-vlan host` makes the port a PVLAN port.
12. B. The command `switchport private-vlan host-association 10 202` assigns a

port to primary VLAN 10 and PVLAN 202.

13. B. In some cases, you may find there is no reason for any communication between ports connected to the same switch. When that is the case, it may be beneficial to take advantage of another feature called the PVLAN Edge feature. Preventing communications between ports when possible can prevent attacks such as ARP poisoning attacks and can impair the ability of a hacker to move from a compromised host to other hosts.
14. C. The command `private-vlan association 501` executed under the VLAN 10 configuration is what ties the PVLAN 501 to the primary VLAN 10.
15. D. Forwarding behavior between a protected port and unprotected ports proceeds as usual.
16. B. When a port has been designated as a PVLAN Edge port, it is called a protected port.
17. A. To specify a port as "protected," use the following command:

```
Switch(config)#interface fa0/1
Switch(config-if-range)#switchport protected
```

18. D. In a PVLAN proxy attack, an attacker sends a packet (using the promiscuous port) with the source IP and MAC address of the attacker, a destination IP address of the target, and the MAC address of the router. When the router receives the packet, the router rewrites the destination MAC address to that of the target and sends the packet to the target. It is the presence of the MAC address of the router in the packet, rather than that of the target, that causes this to be possible.
19. C. Since the router is being used as the source MAC, the router is considered a "proxy."
20. D. To prevent PVLAN proxy attacks, implement ACLs on the router interface that deny traffic from the local subnet to the local subnet.

Chapter 8: Securing Management Traffic

1. B. In-band connection types include SNMP, virtual terminal (VTY), and HTTPS connections. Out-of-band connections include the console port and the AUX port, both physical connections that do not use the network as the transmission medium.
2. A. To set up the AUX port, you need to know the line number used by the AUX port. This can be determined with the `show line` command.
3. C. When a loopback address is configured and used as the management IP address, *any* physical interface on the device can accept the connection attempt if the loopback address is included in dynamic routing advertisements or advertised via a static route. When management access is tied to a physical IP address, the device will be unreachable when that physical interface is down.
4. B. Before setting a password on the VTY lines, you should determine how many of these lines exist on the device (which varies) so that you secure them all. Use this command to learn the number of VTY lines:

   ```
   R1(config)#line vty ?
   R1(c0nfig)#line vty <0 15>
   ```

5. B. These locations and their associated data are called OIDs. The OID number describes the path through the tree-like structure where the specific piece of information is located.
6. B. These functions can be configured using three modes, which represent various combinations of these capabilities: noAuthNoPriv, which is no hashing to secure authentication or encryption of data (referenced as `noauth` in the command); AuthNoPriv, which is hashing to secure authentication but no encryption of data (referenced as `auth` in the command); and AuthPriv, which is hashing to secure authentication and encryption of data (referenced as `priv` in the command).
7. D. All management interfaces should be protected by passwords.
8. C. To disable the HTTP server and enable the HTTPS server, execute the following commands:

   ```
   R81(config)#no http server
   R81(config)#ip https secure-server
   ```

9. D. The command syntax is as follows and is executed at the global configuration prompt:

   `snmp-server group` *`group-name`* `v3` *`security policy access-type view-name access-list number`*

10. A. Use of words such as *Welcome* may be used later as a defense that access was encouraged.
11. D. There are three types of banner messages: message of the day, EXEC, and login.
12. A. MOTD messages appear at connection time and before the login banner (if configured).

13. C. Configuring SNMP requires you to set an engine ID for any device used to manage SNMP. This is an ID number composed of 24 hex characters. When inform messages are sent to stations, it is the engine ID that identifies the station.

14. B. Assigning views is optional. In the absence of this, users will be able to view the entire MIB.

15. C. `read-view` is the name of the view that is created by the command, not the group name.

16. B. MD5 will be used to compute a hash value of the update sent to the client. The client will perform a hash calculation of the update using the same shared key and will compare the results. A match in results serves as assurance that the update came from the legitimate NTP server.

17. A. To configure NTP authentication, the high-level steps (to be performed on both the server and client) are configuring an NTP authentication key number and MD5 string (shared secret), specifying at least one trusted key number referencing the key number in the first step, and enabling NTP authentication.

18. A. While FTP and TFTP can be used to transfer configurations and IOS images across the network, these protocols lack the ability to encrypt the transmission. A better alternative is the Secure Copy Protocol (SCP). This an implementation of the Remote Copy Protocol (RCP) that operates over an SSH connection.

19. C. With the server setup in place, you simply reference the SCP server by putting the URL in the `copy` command. For example, if the server were named `scp-srv` and you wanted to copy the running configuration to it under the security context of an account named Admin with a password of `mypass`, while naming the file `R88-config.txt`, you would use the following command:

```
R88#copy run scp://scp-srv/admin:mypass/r88-config.txt
```

20. B. SMTP stores the settings in a MIB. This is a repository with a hierarchical structure, with standardized locations for each piece of configuration or status information.

Chapter 9: Understanding 802.1x and AAA

1. A. The 802.1x standard defines a framework for centralized port-based authentication. It can be applied to both wireless and wired networks and uses these three components:

   Supplicant: The user or device requesting access to the network

   Authenticator: The device through which the supplicant is attempting to access the network

   Authentication server: The centralized device that performs authentication

2. B. While TACACS+ does separate the three AAA processes, it uses TCP rather than UDP; it creates more traffic than RADIUS and encrypts the entire body except the TACACs+ header.

3. B. The command `aaa new-model` enables AAA services.

4. C. To configure an authentication method that specifies local authentication on all lines (by adding the `default` keyword), use this command:

   ```
   aaa authentication login default local
   ```

5. B. The configuration will apply all lines except for the `Con0`. This gives you a fallback method to access the CLI if a misconfiguration of authorization locks you out.

6. B. The Cisco Secure Access Control Server (ACS) can operate either as a RADIUS server or as a TACACS+ server.

7. D. While some Cisco devices, such as the Cisco Adaptive Security Appliance (ASA), can communicate directly with LDAP repositories or Active Directory for authentication purposes, most do not.

8. C. Specify a name for the TACACS+ server. This name does not need to match the actual name of the server and is only locally significant. When you execute this command, the prompt will change at the ensuing prompt where you will enter the IP address and type and the shared secret.

9. A. This can be done by using the `test` command to test an authentication using the TACACS+ server. For example, to test the username `mytest` with a password of `mypass`, use the following command:

   ```
   R99(config)#test aaa group tacacs mytest mypass new-code
   Sending password
   User successfully authenticated
   USER ATTRIBUTES
   Username 0 "mytest"
   Reply-message 0 "Password: "
   ```

10. B. To specify the use of TACACS+ in the method list for authorization while also specifying a backup method, use the following command:

```
aaa authorization exec default group tacacs+ local
```

In this case, the backup is local authentication.

11. C. Enabling per-command authorization is optional to the process.
12. B. The TACACS+ server consults the LDAP server, the LDAP server performs authentication, and the AAA server passes the result to the supplicant.
13. B. Posture assessment is the ability to verify the minimum security requirements of a device before allowing access. If issues arise such as missing OS or security updates, the device may be either remediated or denied entry.
14. B. This command provides access to the CLI (by including the `exec` keyword) on all lines (by adding the `default` keyword).
15. A. This command creates a user account named `adminsr` that has a privilege level of 7 with an encrypted (secret) password of `srpass`.
16. B. Controlling the activities of those with administrative access by using user accounts rather than privilege levels provides more accountability.
17. C. While TACACS+ supports Cisco commands, RADIUS does not.
18. C. 802.1x is a standard that defines a framework for centralized port-based authentication. It can be applied to both wireless and wired networks and uses three components.
    - Supplicant: The user or device requesting access to the network
    - Authenticator: The device through which the supplicant is attempting to access the network
    - Authentication server: The centralized device that performs authentication
19. A. The role of the authentication server can be performed by a Remote Authentication Dial-in User Service (RADIUS) or Terminal Access Controller Access Control System + (TACACS+) server.
20. B. Profiling is the ability to determine the type of device from which a network access request is originating and to apply a set of access policies specific to the profile attached to that device. This means a user might have multiple profiles each attached to the various devices they use.

Chapter 10: Securing a BYOD Initiative

1. C. The Cisco Integrated Services Engine (ISE) is a centralized identity-based policy platform that provides context-based access control for wired, wireless, and VPN connections. It combines AAA, posture assessment and profiling, and guest access management.
2. A. The following can be considered during both the access request and the following authorization request:
   - Who is the individual?
   - What device are they using?
   - Where are they connecting from?
   - When are they connecting?
   - How are they connecting?
3. A. The ISE can make use of several advanced features to provide granular and dynamic access control policies. Among these are downloadable ACLs (dACLs), which are IP-based ACLs that are implemented on devices when the policy calls for it.
4. B. Security group access (SGAs) applies a security group tag (SGT) that uniformly enforces the security group policy regardless of topology.
5. C. Change of authorization (COA) updates provide the ability of ISE to change the authorization policy in real time after the administrator makes a change without requiring a log-off for the change to take effect.
6. D. Posture assessment can check the health of a device before allowing access and, if the check fails, can remediate the device.
7. A. Web authentication (WebAuth) enables network access for end hosts that do not support IEEE 802.1x authentication.
8. C. The three main functions of TrustSec are to classify each device by assigning a security group tag (SGT) to its IP address, to transport or communicate this classification information throughout the network using a process called inline tagging (for those networking devices that support inline tagging) or using the SGT eXchange Protocol (SXP) for those networking devices that do not, and to enforce access rules through the examination of the SGTs.
9. B. Classification of a device is done through the application of an SGT. These tags, 16 bits in length, can be applied dynamically or statically.
10. A. Transportation or communication of this classification information throughout the network uses a process called inline tagging (for networking devices that support inline tagging) or using the SGT eXchange Protocol (SXP) for those networking devices that do not.

11. A. Dynamic tagging is possible when the authentication method is 802.1x, MAC bypass, or through web authentication. In dynamic tagging, the ISE pushes the SGT to the network access device (NAD).

12. A. The SGT will be in a new section of the Ethernet header called the Cisco Metadata (CMD) header.

13. C. The CMD holds other information besides the SGT. Overall, this adds 20 bytes to the size of the header.

14. D. One thing to note is that in cases where two networking devices are also using 802.1ae security (MACSec), the addition of the 802.1ae header and ICV field will result in a total addition to the Ethernet header of 40 bytes.

15. A. SXP connections are point-to-point TCP-based connections created between two endpoints; one must be designated as the speaker and the other as the listener (any other combination of the two roles will fail).

16. C. Version 1 only supports IPv4 binding propagation. Version 2 supports both IPv4 and IPv6 binding propagation. Version 3 added support for subnet to SGT mappings. If speaking to a lower-version listener, the speaker will expand the subnet. Version 4 added loop detection and prevention, capability exchange, and a built-in keep-alive mechanism.

17. A. The Cisco Adaptive Security Appliance and several other routing platforms use a different method to enforce TrustSec. While ISE manages SGACLs centrally, these devices are configured individually with ACLs that reference the SGT numbers or security group names. This is called Security Group Firewall (SGFW).

18. A. Mobile device management software is designed to make it possible to exert control over personal mobile devices that users want to use on the enterprise network. When used in conjunction with ISE, the combination can be a powerful and secure identity and authentication solution for both company-owned and non-company-owned devices.

19. A. In the context of a BYOD architecture, the ISE when working in combination with mobile management ties together the provisioning of mobile devices along with a health check of the device at each connection request.

20. B. One of the three main functions of TrustSec is the enforcement of access rules through the examination of the SGTs.

Chapter 11: Understanding VPNs

1. C. When the choice is made to use ESP, one of the protocols in the suite, at the least the data payload will be encrypted, and depending on the delivery mode, the entire packet including the header may be encrypted.
2. A. It does this by using the hashing algorithm you select during implementation. This is hash-based message authentication (HMAC).
3. B. When confidentiality of an IPsec connection is not required, the Authentication Headers (AH) protocol can be used. While it does provide data integrity and origin authentication and anti-replay protection, the data is sent in clear text.
4. C. The key management process in IPsec provides for the dynamic generation of keys to be used for encryption and for their secure exchange over an untrusted network, such as the Internet. The Diffie-Hellman key exchange algorithm is used, and an asymmetric algorithm is used to create and exchange symmetric keys for this process.
5. C. In 2005, the NSA identified a set of cryptographic algorithms that are the preferred method for securing information. It called these algorithms Suite B. These algorithms use a minimum key length of at least 128 bits.
6. C. Suite B cryptography uses the following algorithms:
   - AES encryption with either 128- or 256-bit keys
   - SHA-2 hashing
   - Elliptical Curve digital signature algorithm (ECDSA) for digital signatures using 256-bit and 384-bit prime moduli
   - Key exchange using Elliptic Curve Diffie-Hellman Exchange (ECDHE)
7. C. The key exchange is performed by the Diffie-Hellman algorithm.
8. D. The IPsec transform set is negotiated in phase 2 of IKE.
9. B. Main mode consists of three exchanges.
   - Peers negotiate the encryption and hashing algorithms to be used.
   - The Diffie-Hellman protocol is used to generate a shared symmetric key.
   - The SA is built, and then the peers authenticate one another within the SA.
10. D. The Diffie-Hellman protocol is used to generate a shared symmetric key in the Main mode of phase 1.
11. A. IKEv2 has fewer transactions; this results in increased speed.
12. B. When AH is used in transport mode, only the payload is authenticated.
13. C. When ESP is used in tunnel mode, the entire packet is encrypted, and a new IP header is added.

14. A. While the use of IPsec is not required when using IPv6, the IPv6 packet structure was redesigned to accommodate its use.

15. A. When using a remote access VPN, there are two default behaviors that can cause issues. The two behaviors are as follows:

    - Once a tunnel is operational, all traffic leaving the VPN client must pass through the tunnel.
    - By default, an ASA will not forward packets back out the same interface in which it was received.

16. B. To solve this issue, you must enable an option called Enable Traffic Between Two Or More Hosts Connected To The Same Interface. This is commonly referred to as *hairpinning*. This option is found by navigating in the ASDM to Configuration ➢ Device Setup ➢ Interfaces.

17. C. Another advanced option you can enable is called *split tunneling*, and when enabled, it allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel. When this is done, an ACL is used to determine the traffic that goes through the tunnel (all traffic except for Internet) and the traffic that does not go through the tunnel (Internet).

18. B. To enable Always-On, you must first enable Trusted Network Detection in a profile that applies to the user. This feature enables the device to know when it is connected to the corporate LAN and when it is not.

19. A. As ESP does not utilize the concept of source and destination ports, NAT has difficulty operating when IPsec traffic arrives at the NAT device. NAT traversal encapsulates IPsec within UDP, providing the requisite ports for NAT.

20. C. In IPv6, extension headers are used. These headers, when used, come after the original IPv6 header. The next header field in the original IPv6 header is used to indicate whether the extension header is AH or ESP. It uses the protocol value of 50 for ESP and 51 for AH.

Chapter 12: Configuring VPNs

1. A. The supported algorithms are 3DES, IDEA, RC4, and AES.
2. A. An SSL/TLS VPN can use RSA, DSA, and ECC for authentication.
3. A. The steps are as follows:
    1. The client initiates the process by starting the exchange of hello packets between the client and the VPN gateway (the ASA).
    2. The server transmits its certificate to the client (which will include its public key).
    3. If mutual authentication is required, the client sends its certificate to the server.
    4. Session keys are exchanged, and the data transfer begins.
4. D. Configuring user authentication comprises three subtasks: creating accounts for the VPN users, configuring a group policy for the VPN users specifying in the policy clientless SSL VPN as the tunneling protocol, and creating a connection profile for the VPN users and connecting the policy to the profile.
5. A. The ISE module performs a client-side assessment.
6. C. Defining the IPsec transform set includes specifying the encryption and integrity algorithms.
7. C. The `group 5` command specifies 1024-bit Diffie-Hellman for key exchange.
8. A. The number 10 refers to the sequence number of the line in the crypto map. The name of the map is `mymap`.
9. B. While certificates can be deployed on both the client and the server to enable mutual authentication, in most cases a certificate is deployed only on the server because that can secure the connection as well as when certificates are deployed on both ends.
10. B. The possible authentication mechanisms available are DSA, ECC, and RSA.
11. D. In the second step, the server transmits its certificate to the client (which will include its public key).
12. B. Once the session keys are exchanged, the data transfer begins. When the traffic gets beyond the ASA, the information will be in clear text but will be encrypted between the client and the ASA.
13. B. When using the Cisco clientless SSL VPN, the remote device uses the browser to connect to an SSL-enabled website on the ASA or on a Cisco router.
14. B. MD5 is one of three integrity algorithms that can be used, including SHA1 and SHA2.
15. B. A crypto ACL defines the traffic types to be sent and protected through the tunnel.
16. B. It defines a security association lifetime of 1 day (86400 seconds).

17. A. `AES_SHA` is the name of the transform set. The mechanism for payload authentication is ESP HMAC. The mechanism for payload encryption is ESP, and the IPsec mode is tunnel (defaults to tunnel).

18. B. The key exchange management algorithms available in an SSL VPN are DH, DSS, and RSA.

19. B. To utilize a Cisco AnyConnect SSL VPN, a VPN client called the AnyConnect client must be installed on the user device.

20. B. Remediation with the ASA module, not the ISE module, is limited to working with the software present on the endpoint, meaning it can enable, disable, or update that software.

Chapter 13: Understanding Firewalls

1. C. Packet filtering firewalls are the least detrimental to throughput because they only inspect the header of the packet for allowed IP addresses or port numbers.
2. A. Circuit-level proxies operate at the Session layer (layer 5) of the OSI model. They make decisions based on the protocol header and Session layer information.
3. B. A kernel proxy firewall is an example of a fifth-generation firewall. It inspects the packet at every layer of the OSI model but does not introduce the performance hit that an Application layer firewall will because it does this at the kernel layer.
4. D. Application firewalls operate at the application layer and are *not* considered proxy firewalls.
5. A. Personal firewalls either may be those that come with an operating system like the Windows Firewall or may be third-party host firewalls such as Kaspersky Internet Security or Zone Alarm Pro Firewall. These firewalls are called either *host* or *personal* firewalls and protect only the device on which the software is installed.
6. A. The contents of the state table include the following for each connection: source IP address, source port number, destination IP address, destination port number, IP protocol, flags, and timeout.
7. B. Application-level proxies perform deep packet inspection. Operating at this layer requires each packet to be completely opened and closed, making this firewall the most impactful on performance.
8. C. Proxy servers can provide an additional beneficial function called *web caching*. When a proxy server is configured to provide web caching, it saves a copy of all web pages that have been delivered to internal computers in a web cache. If any user requests the same page later, the proxy server has a local copy and need not spend the time and effort to retrieve it from the Internet. This greatly improves web performance for frequently requested pages.
9. D. Circuit-level proxies operate at the Session layer (layer 5) of the OSI model. They make decisions based on the protocol header and Session layer information.
10. A. Although packet filtering firewalls serve an important function, they cannot prevent many attack types. They cannot prevent IP spoofing, attacks that are specific to an application, attacks that depend on packet fragmentation, or attacks that take advantage of the TCP handshake.
11. B. An application-level firewall maintains a different proxy function for each protocol. For example, for HTTP the proxy will be able to read and filter traffic based on specific HTTP commands.
12. C. A packet should never arrive at a firewall for delivery that has both the SYN flag and the ACK flag set unless it is part of an existing handshake process, and it should be in

response to a packet sent from inside the network with the SYN flag set.

13. D. The firewall records all operations in its state table and will monitor that table whenever a packet arrives at the firewall to ensure that any packets permitted either are connection requests from the inside (SYN packets only) or are part of an existing connection and that all rules of the handshake are enforced.

14. A. While never a replacement for properly positioned network firewalls, personal firewalls are an excellent complement to the protection provided by the network firewalls, and installing both types of firewalls is an example of exercising the concept of defense in depth. This concept prescribes that you always deploy multiple barriers to unauthorized access.

15. B. A SOCKS firewall is an example of a circuit-level firewall. This requires a SOCKS client on the computers. Many vendors have integrated their software with SOCKS to make using this type of firewall easier.

16. B. A SYN/ACK packet in response to a SYN packet in a current connection setup is normal and would be allowed.

17. C. Proxy firewalls include SOCKS firewalls, circuit-level firewalls, and kernel-level firewalls.

18. D. While never a replacement for properly positioned network firewalls, they are an excellent complement to the protection provided by the network firewalls, and installing both types of firewalls is an example of exercising the concept of defense in depth.

19. A. Operating at the Application layer requires each packet to be completely opened and closed, making this firewall the most impactful on performance.

20. B. Packet filtering firewalls inspect the header of the packet for allowed IP addresses or port numbers. Since these values reside at the Network and Transport layers, respectively, these firewalls operate at those layers.

Chapter 14: Configuring NAT and Zone-Based Firewalls

1. B. In static NAT, each private IP address is mapped to a public IP address. While this does not save any of the public IPv4 address space, it does have the benefit of hiding your internal network address scheme from the outside world.
2. D. The Manual NAT After Auto NAT is read last and contains more general translations not handled by the first two sections. These are used only when no translation matches in the first two sections.
3. D. In some scenarios, you may need more options than are available with Auto NAT, or you may need to specify exceptions to the Auto NAT rules. By using the Manual NAT section, these options will be available to you.
4. C. The `show xlate` command on an ASA shows the translations that have occurred.
5. C. The `r` flag indicates that the translation is a PAT. The `i` flag indicates that the translation applies to the inside address port.
6. B. Zones are collections of networks reachable over a router interface.
7. D. A match statement is used to specify the traffic and can match traffic based on an ACL, protocol, or another class map.
8. C. The actions can be defined using action statements. The actions can be inspect (triggers stateful packet inspection), drop (denies traffic), or pass (permits traffic).
9. B. The self-zone is a special zone that has no interface members. It applies to any traffic destined for the router rather than traffic that the router is routing.
10. C. In PAT, each private IP address is mapped to a public IP address. While this does not save any of the public IPv4 address space, it does have the benefit of hiding your internal network address scheme from the outside world.
11. C. The value 21505 is the source port number selected by the device at 10.1.1.15 for the ICMP session.
12. D. When using the Cisco Common Classification Policy Language, class maps are used to define traffic classes.
13. B. Use the following commands to create the zone called `inside`.

    ```
    RTR64(config)#zone security inside
    ```

14. C. The self-zone is a special zone that has no interface members. It applies to any traffic destined for the router rather than traffic that the router is routing. An example of this type of traffic would be traffic to manage the device using SSH. It also applies to traffic generated by the router. The traffic going from the router back to the device making the SSH connection to manage the device would be an example of such router-generated traffic.
15. A. Applied at the interface configuration prompt, the command to assign an interface to the outside zone is as follows:

```
RTR64(config-if)#zone-member inside
```

16. C. When using the Cisco Common Classification Policy Language, class maps are used to define traffic classes, and policy maps are used to apply policies (actions) to these traffic classes.

17. A. Zone pairs are used to define a unidirectional firewall policy. The direction is indicated by specifying the source and destination zone.

18. A. The `r` flag indicates that the translation is a PAT. The `i` flag indicates that the translation applies to the inside address port.

19. A. In this section, also called object NAT, translations that are defined on the object itself are contained. These translations, one for each object, are typically either static translations for servers that must be reached from the outside world (and require the same public IP address always) or dynamic translations for clients trying to reach the Internet.

20. A. In dynamic NAT, a pool of public IP addresses is obtained that is at least equal to the number of private IP addresses that require translation. However, rather than mapping the private IP addresses to the public IP addresses, the NAT device maps the public IP addresses from the pool on a dynamic basis much like a DHCP server does when assigning IP addresses.

Chapter 15: Configuring the Firewall on an ASA

1. A. Application Inspection Control (AIC) or application protocol control as it is also called verifies the conformance of major application layer protocols operations to RFC standards.
2. B. In transparent mode, the ASA is not acting as a router and assumes a layer 2 identity much as a switch does. This makes the ASA transparent to devices on either side (from a layer 3 perspective); thus the name transparent mode.
3. C. In Clustering, three or more security appliances are deployed as a single logical device. This allows for the management of the multiple ASAs as a unit. It provides increased throughput and redundancy.
4. A. The ASA can be partitioned into multiple virtual firewalls or security contexts. Each context can have its own interfaces, policies, and administrators.
5. B. The `nameif` command is used at the interface configuration prompt.
6. C. The http server enable command is required to start the HTTP service on the ASA.
7. D. The command http ip address mask interface is used to define an IP address on the specified network that will be allowed to connect to the ASA using HTTP to manage the ASA.
8. A. Security levels define the trustworthiness of the interface. The higher the level the more trusted the interface.
9. B. There is an implicit permit for traffic flowing from a high-security interface to a low-security interface. High and low are defined by the security value assigned.
10. C. The command security-level value is used at the interface configuration prompt.
11. A. You will need to create an access rule to allow traffic in each of the following scenarios: between interfaces of the same security level, and traffic from a lower-security interface to a higher-security interface.
12. B. In many cases we need to allow only a select group of devices rather than all devices, or we need only allow devices on a specific network to send traffic on an interface when there are multiple networks that might be traversing that interface. To make the creation and application of rules easier, the ASA can also use an object-based model for certain rules.
13. D. In the Cisco Modular Policy Framework, class-maps are used to categorize traffic types into classes.
14. A. On the Service Policy rule page, the Global radio button applies the policy to all interfaces.
15. B. You will need to create a network object to represent the 192.168.5.0/24 network, create a service object to represent HTTP, and create a host object to represent the server at 201.3.3.3.

16. C. In the Cisco Modular Policy Framework, service policies are used to specify where the policy map should be implemented.

17. B. Since outside has a security level of 0 and the dmz has a level of 50, traffic from the lower level (0) to the higher level (50) will be disallowed.

18. C. The command defines an IP address on the inside network (defined by the interface name) that will be allowed to connect to the ASA using either SSH or HTTP to manage the ASA.

19. C. In the Cisco Modular Policy Framework, policy maps are used to define the action to be taken for a class. Actions that can be specified are allow, block and rate-limit.

20. D. There is an implicit deny for traffic flowing from a low-security interface to a high-security interface. High and low are defined by the security value assigned.

Chapter 16: Intrusion Prevention

1. A. A threat is an identified security weakness to which any specific environment may or may not be vulnerable. For example, a threat might exist in the form of a new attack on Oracle database servers, but if you use Microsoft SQL Server, it is a threat to which you are not vulnerable.
2. A. Actions refer to the operations an intrusion prevention system (IPS) can take when an attack is recognized to block the traffic. Drops means the IPS quietly drops the packets involved.
3. C. The ability to monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal, is a strength of host-based IPS and a weakness of network-based IPS.
4. A. The attack fragments the packet containing the malicious code so that it becomes difficult for the IPS to recognize the code in such a fragmented fashion.
5. D. There are four categories of functions of which FireSIGHT is capable. They include detection, learning, adapting, and acting. Blocking is a form of acting.
6. A. A zero-day threat is any threat not yet remediated by malware vendors or software vendors. This type of threat cannot be detected through attack signature-based methods and is usually only discovered by malware or IPS/IDS software that uses heuristics.
7. B. Cisco AMP for Endpoints is composed of connectors installed on endpoints. It uses a cloud-based detection process that offloads the detection burden to the cloud. Cisco AMP for Networks uses FirePOWER appliances to detect malware in transit.
8. A. The sensor is connected to a port on the switch to which all traffic has been mirrored by making the port a SPAN port.
9. C. Many protocols' information can be communicated or expressed in multiple ways. For example, HTTP can accept strings expressed in hexadecimal, Unicode, or standard text expressions. Attackers can use this to evade an IPS sensor. If the IPS cannot perform protocol normalization (decoding the payload to discover its significance), this attack may succeed.
10. C. A vulnerability is any susceptibility to an external threat that a device or system may possess. A threat only becomes a vulnerability when the threat target is present in your environment and is in the state required to take advantage of the vulnerability.
11. C. Actions refer to the operations an intrusion prevention system (IPS) can take when an attack is recognized. Shun sends a packet with the RST flag when a non-TCP connection is encountered.
12. C. In this mode, the sensing device is placed in the line of traffic and analyzes the original traffic, not a copy in real time. Therefore, it can take actions on the traffic, allowing it to operate as a true IPS.

13. A. One of the options is to place the sensor outside the perimeter firewall (ASA). When placed here, the sensor will generate a very high number of alarms because this is an exposure to the most untrusted network, the Internet.

14. D. An exploit occurs when a threat and vulnerability both exist and a threat actor takes advantage of the situation. The term *exploit* also refers to the specific tool or attack methodology used.

15. D. Actions refer to the operations an intrusion prevention system (IPS) can take when an attack is recognized. When blocking, the IPS directs another device (a router or firewall) to block the traffic.

16. B. The tap is placed between the router and the layer 3 switch. It provides full-duplex connectivity between the devices and splits off two simplex mirrors of the full-duplex traffic. All traffic between the two devices must traverse the sensor.

17. A. The attacker injects a bogus string into the attack code and breaks the attack into fragments. Then he manipulates the TTL value of the fragment containing the bogus string in such a way that the fragment dies (and never gets delivered) before it reaches the destination. If the IPS does not consider the fragment offset values or TTL values, it will detect the bogus string rather than the actual payload. The result is that after inspection by the IPS, the bogus string does not get delivered; the attack payload does.

18. C. The inability to monitor any internal activity that occurs within a system, such as an attack against a system that is carried out by logging on to the system's local terminal, is a strength of host-based IPS and a weakness of network-based IPS.

19. B. Actions refer to the operations an intrusion prevention system (IPS) can take when an attack is recognized. Reset sends a packet with the RST flag that ends any TCP connection.

20. B. A risk is created when a threat exists to which a system is vulnerable.

Chapter 17: Content and Endpoint Security

1. B. Reputation-based filtering relies on the identification of email servers that have become known for sending spam. When a system can do this, it must rely on some service for developing these “reputations.”
2. A. Data leakage occurs when sensitive data is disclosed to unauthorized personnel either intentionally or inadvertently. Data loss prevention (DLP) software attempts to prevent data leakage.
3. B. Network DLP is installed at network egress points near the perimeter, where it analyzes network traffic.
4. A. Precise methods involve content registration and trigger almost zero false-positive incidents.
5. A. If the sender score is between −1 and +10, the email is accepted. If it is between −1 and −3, the email is accepted, but additional emails are throttled. If it is between −10 and −3, it is blocked.
6. A. Advanced Malware Protection (AMP) is the malware component in ESA that uses a combination of several technologies to protect you from email-based malware.
7. A. File reputation sends a fingerprint of every file that traverses the Cisco email security gateway to AMP’s cloud-based intelligence network for a reputation verdict. Based on these results, you can block malicious files identified as having a bad reputation.
8. B. The Cisco Web Reputation System (WBRS) uses real-time analysis on a vast, diverse, and global dataset to detect URLs that contain some form of malware. WBRS is a critical part of the Cisco security database, which protects customers from blended threats from email or web traffic.
9. C. The Cisco Web Security Appliance (WSA) is a web proxy that integrates with other network components to monitor and control outbound requests for web content. Traffic can be directed to the WSA explicitly on the end host or by using the Web Cache Control Protocol on an inline device like the perimeter router.
10. A. By leveraging Cisco Security Intelligence Operations (SIO), Cisco Ironport reputation filters analyze more than 50 web and network parameters to evaluate a website’s trustworthiness.
11. C. If the sender score is between −1 and +10, the email is accepted. If it is between −1 and −3, the email is accepted, but additional emails are throttled. If it is between −10 and −3, it is blocked.
12. C. In the safe sandboxed environment, AMP can obtain details about the threat level of the malware and communicate that information to the Cisco Talos intelligence network to update the AMP cloud data for all.
13. C. The WSA anti-malware system uses multiple scanning engines in a single appliance.

It uses the Dynamic Vectoring and Streaming Engine and verdict engines from both WebRoot and McAfee.

14. D. WSA uses Application Visibility and Control (AVC) to allow for the control of the use of web applications. Granular policy control allows administrators to permit the use of applications such as Dropbox or Facebook while blocking users from activities such as uploading documents or clicking the Like button.

15. B. The main task of Cisco ISE is to manage access to the network, but its abilities go beyond that. It can provide AAA services so that you can deploy 802.1x security. Using Cisco TrustSec technology, it also can enforce endpoint security policies that ensure that many of the security measures in this section are compliant with the policy.

16. B. File retrospection allows for the identification and removal of these files later. If malicious behavior is spotted later, AMP sends a retrospective alert so that you can contain and remediate the malware.

17. B. If the sender score is between −1 and +10, the email is accepted. If it is between −1 and −3, the email is accepted, but additional emails are throttled. If it is between −10 and −3, it is blocked.

18. C. Imprecise methods can include keywords, lexicons, regular expressions, extended regular expressions, metadata tags, Bayesian analysis, and statistical analysis.

19. C. Endpoint DLP runs on end-user workstations or servers in the organization.

20. A. Context-based filtering filters the message and attachments for sender identities, message content, embedded URLs, and email formatting. These systems use algorithms to examine these items to identify spam.

Comprehensive Online Learning Environment

Register to gain one year of FREE access to the online interactive learning environment and test bank to help you study for your CCNA Security certification exam—included with your purchase of this book!

The online test bank includes the following:

- **Assessment Test** to help you focus your study to specific objectives
- **Chapter Tests** to reinforce what you've learned
- **Practice Exams** to test your knowledge of the material
- **Digital Flashcards** to reinforce your learning and provide last-minute test prep before the exam
- **Searchable Glossary** to define the key terms you'll need to know for the exam

Register and Access the Online Test Bank

To register your book and get access to the online test bank, follow these steps:

1. Go to bit.ly/SybexTest.
2. Select your book from the list.
3. Complete the required registration information including answering the security verification proving book ownership. You will be emailed a pin code.
4. Go to http://www.wiley.com/go/sybextestprep and find your book on that page and click the "Register or Login" link under your book.
5. If you already have an account at testbanks.wiley.com, login and then click the "Redeem Access Code" button to add your new book with the pin code you received. If you don't have an account already, create a new account and use the PIN code you received.

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.

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