

EXAM CRAM

The Smart Way to Study™

IINS Exam **640-553**

CCNA® Security



CD Features Multiple
Practice Exams

Eric Stewart

CCNA Security Exam Cram

Copyright © 2009 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-3800-4

ISBN-10: 0-7897-3800-7

Library of Congress Cataloging-in-Publication Data

Stewart, Eric L.

CCNA security exam cram / Eric L. Stewart.
p. cm.

Includes bibliographical references and index.

ISBN-13: 978-0-7897-3800-4 (pbk. w/cd)

ISBN-10: 0-7897-3800-7 (pbk. w/cd)

1. Computer networks--Security measures--Examinations--Study guides.
2. Cisco Systems, Inc. I. Title.
TK5105.59.S758 2009
005.8076--dc22

2008038852

Printed in the United States of America

First Printing: October 2008

Trademarks

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

Cisco, Cisco Systems, and CCNA are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this book are the property of their respective owners.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside the United States, please contact

International Sales

international@pearson.com

Associate Publisher

David Dusthimer

Executive Editor

Brett Bartow

Development Editor

Andrew Cupp

Managing Editor

Patrick Kanouse

Project Editor

Mandie Frank

Copy Editor

Water Crest
Publishing

Indexer

Ken Johnson

Proofreader

Leslie Joseph

Technical Editors

William G. Huisman
Ryan Lindfield

Publishing Coordinator

Vanessa Evans

Multimedia Developer

Dan Scherf

Book Designer

Gary Adair

Composition

TnT Design, Inc.

Introduction

Welcome to *CCNA Security Exam Cram*! The fact that you are reading this means that you are interested in the CCNA Security certification that Cisco announced in July of 2008. Cisco has done a thorough job of revamping the certification path for the Cisco Certified Security Professional (CCSP), with the CCNA Security certification being the cornerstone upon which the CCSP certification depends. Implementing Cisco IOS Network Security (IINS) is the recommended training course for CCNA Security certification. If you already hold the prerequisite valid CCNA certification, passing the 640-553 IINS exam enables you to obtain the CCNA Security certification—likely to become one of the hottest certifications in IT. This book helps prepare you for that exam. The book assumes that you already have your CCNA certification or an equivalent level of knowledge. If you do not have a CCNA level of knowledge, you should consider putting down this book and first pursuing more robust fundamental training, such as a full CCNA course book or a recommended CCNA course. And remember that CCNA is a prerequisite to CCNA Security certification.

This book is a synthesized, distilled, and pared-down effort, with only enough information as is necessary to provide context for the information you need to pass the exam. This is not to say that this book is not a good read, but it is a fair reflection of the type of material that you will need to master in order to be successful with the exam. Read this book, understand the material, and drill yourself with the practice exams, and you stand a very good chance of passing the exam. That said, it's possible that in the course of working through this book, depending on your prior CCNA Security training or on-the-job experience, you might identify topics you are struggling with and might require you to look up more fundamental resources to deal with. This book discusses all the topics on the exam and tests you on all of them, but it does not always provide detailed coverage of all those topics.

Organization and Elements of This Book

When designing a secure network infrastructure, the workflow moves from the perimeter of the network to the inside of the network. After the perimeter is properly secured, the security architect can turn his or her attention to securing devices on the inside of the network perimeter where the endpoints reside. This structured approach is mimicked in the basic organization of this book.

The chapters of this book are organized into four major parts, with each part encapsulating a major idea in the field of network security:

- ▶ Part I: Network Security Architecture
- ▶ Part II: Perimeter Security
- ▶ Part III: Augmenting Depth of Defense
- ▶ Part IV: Security Inside the Perimeter

You can use this book's organization to your advantage while studying for the CCNA Security 640-553 IINS exam because each part of the book is self-contained. Although it is recommended that you follow the parts sequentially, there are frequent cross-references to content contained in other chapters if you choose to follow your own path through this book.

Each chapter follows a uniform structure, with graphical cues about especially important or useful material. The structure of a typical chapter is as follows:

- ▶ **Terms You'll Need to Understand:** Each chapter begins with a list of the terms you'll need to understand, which define the concepts that you'll need to master before you can be fully conversant with the chapter's subject matter.
- ▶ **Exam Topics Covered in This Chapter:** Cisco publishes a list of exam topics for the 640-553 IINS exam. Each chapter of this book begins by listing the exam topics covered in that chapter. See the following "Self Assessment" element for a complete list of the topics and the chapters where they are covered.
- ▶ **Exam Alerts:** Throughout the topical coverage, Exam Alerts highlight material most likely to appear on the exam by using a special layout that looks like this:

EXAM ALERT

This is what an Exam Alert looks like. An Exam Alert stresses concepts, terms, or activities that will most likely appear in one or more certification exam questions. For that reason, any information found offset in Exam Alert format is worthy of unusual attentiveness on your part.

Even if material isn't flagged as an Exam Alert, *all* content in this book is associated in some way with test-related material. What appears in the chapter content is critical knowledge.

- **Notes:** This book is an overall examination of basic Cisco network security concepts and practice. As such, there are a number of side excursions into other aspects of network security and prerequisite networking knowledge. So that these do not distract from the topic at hand, this material is placed in notes.

NOTE

Cramming for an exam will get you through a test, but it won't make you a competent network security practitioner. Although you can memorize just the facts you need to become certified, your daily work in the field will rapidly put you in water over your head if you don't know the underlying principles behind a Cisco Self-Defending Network.

- **Practice Questions:** This section presents a short list of test questions (most chapters have 10 of these) related to the specific chapter topics. Each question has a follow-on explanation of both correct *and* incorrect answers—this is very important because it is more important to know *why* you were wrong. Computers are binary and will accept right or wrong as answers, but we aren't, so we don't!

In addition to the topical chapters, this book also provides the following:

- **Practice Exams:** Part V contains the sample tests that are a very close approximation of the types of questions you are likely to see on the current CCNA Security exam.
- **Answer Keys for Practice Exams:** Part V also contains detailed answers to the practice exam questions. Like the questions at the end of the chapters, these explain both the correct answers and the incorrect answers and are therefore very helpful to go through thoroughly as you grade your practice exam. Knowing the topics you struggle with and why you got a question wrong is crucial.
- **Cram Sheet:** This appears as a tear-away sheet inside the front cover of the book. It is a valuable tool that represents a collection of the most difficult-to-remember facts and numbers that the author thinks you should memorize before taking the test.
- **CD:** The CD that accompanies this book features an innovative practice test engine powered by MeasureUp, including 100 practice questions. The practice exam contains question types covering all the topics on the CCNA Security exam, providing you with a challenging and realistic exam simulation environment.

Contacting the Author

I've tried to create a real-world tool and clearly written book that you can use to prepare for and pass the CCNA Security certification exam. That said, I am interested in any feedback that you have that might help make this Exam Cram better for future test-takers. Constructive and reasonable criticism is always welcome and will most certainly be responded to. You can contact the publisher, or you can reach me by email at eric@breezy.ca.

Please also share your exam experience. Did this book help you pass this exam? Did you feel better prepared after you read the book? Was it a confidence booster? Would you recommend this book to your colleagues?

Thanks for choosing me as your personal trainer, and enjoy the book!

—Eric Stewart

4

CHAPTER FOUR

Implementing Secure Management and Hardening the Router

Terms You'll Need to Understand:

- ✓ Syslog Protocol (syslog)
- ✓ Out-of-band (OOB)
- ✓ In-band
- ✓ Simple Network Management Protocol (SNMP)
- ✓ Secure Shell (SSH) daemon
- ✓ Network Time Protocol (NTP)
- ✓ Simple Network Time Protocol (SNTP)
- ✓ Gratuitous Address Resolution Protocol (GARP)
- ✓ Proxy Address Resolution Protocol (ARP)
- ✓ AutoSecure

Exam Topics Covered in This Chapter:

- ✓ Secure Cisco routers using the SDM Security Audit feature
- ✓ Use the One-Step Lockdown feature in SDM to secure a Cisco router
- ✓ Secure the Cisco IOS image and configuration file
- ✓ Use CLI and SDM to configure SSH on Cisco routers to enable secured management access
- ✓ Use CLI and SDM to configure Cisco routers to send Syslog messages to a Syslog server

NOTE

These exam topics are from cisco.com. Check there periodically for the latest exam topics and info.

Secure management and reporting is an integral part to a comprehensive security policy. This chapter outlines some methods to protect the confidentiality of remote sessions to the router, either by encrypting the communication or ensuring that these remote administrative sessions do not cross the cables of a hostile network. In security terms, we look at methods to separate the *data plane* from the *management plane*. We also look at ways to implement reporting in such a way as to guarantee the integrity and confidentiality of the events logged.

In the last chapter, Chapter 3, “Security at the Network Perimeter,” we took a large step toward securing the login system on the IOS router from both access and DoS attacks. We assumed that because the router was a perimeter device and, therefore, the first device that an attacker would see as they tried to crack the network, that security would start there. We didn’t finish the tasks necessary to completely harden the router from attack, choosing to defer these steps until now. Using an analogy, if our router is a knight that we deploy on the battlements of a fortress to ward against attack, doesn’t it make sense that we equip him with armor so he can protect himself as well? If he is felled by the first arrow that an attacker fires at him, we should rethink our security architecture. To that end, we will look at interactive and automated ways to both audit the router for security vulnerabilities and, more importantly, fix them based on best practices and Cisco’s recommendations.

Planning for Secure Management and Reporting

Secure management and reporting is too often applied on top of a secure architecture as an afterthought rather than being designed into the solution from the beginning. Some hard questions need to be asked early on in the design because they bear on the implemented secure architecture. These questions are typically asked during the *Initiation* phase and answered during the *Acquisition and Development* phase of the Cisco Secure Network Life Cycle first introduced in Chapter 2, “Building a Secure Network Using Security Controls.” In general, what types of activity need to be logged and what protocols and devices are required to perform these functions will determine the technology deployed during the *Implementation* phase of the Cisco Secure Network Life Cycle.

EXAM ALERT

The context of this discussion, as well as others throughout this book, is determined by the Cisco Secure Network Life Cycle. The steps of the lifecycle are listed next with the secure management and reporting topics to be discussed (in parentheses beside it):

Initiation (What to log? How to log?).

Acquisition and Development (Guidelines for secure management and reporting).

Implementation (Cisco solutions for secure management and reporting).

Operations and Maintenance.

Disposition.

Use the Cisco Secure Network Life Cycle as a framework for memorizing this information for the exam. For example, syslog as a management protocol is presented as a possible answer to the question, “How to log?” (Initiation). Recommendations are then made as to how to use syslog (Acquisition and Development), followed by outlining Cisco products that use syslog as a centerpiece for secure management and reporting (Implementation).

Planning for secure management and reporting is based on guidelines set out by the comprehensive security policy. Several questions need to be answered before secure management and reporting can be integrated into the network security architecture design and then configured. The questions that need to be answered can be grouped into two broad categories, as follows:

- ▶ “What to log (or report)?” questions.
- ▶ “How to log (or report)?” questions.

Let’s break this down a bit further.

What to Log

Issues that bear heavily on the first question would be whether the data collected might be used for forensic purposes in investigating a possible network compromise or possibly for criminal prosecution. Rules of evidence, chain of custody, timestamps on log entries, and so on would need to be laid out. The answers to these questions will lead to administrative controls. Some helpful questions include the following:

- ▶ What are the most critical events to log?
- ▶ What are the most important logs?
- ▶ What log data may be required for forensic investigation and prosecution?

The answers to these questions are specific to the organization and thus vary. For example, an organization that is planning to prosecute a possible network compromise in criminal court would be well advised to log all successful and unsuccessful network login attempts, as well as users' activity once logged on and place timestamps on the events logged with a common clock synchronized from a recognized time source. On the other hand, an Internet Service Provider (ISP) that simply needs to keep track of login activities for billing purposes might simply need logs that reflect accurate network login and logoff by users.

How to Log

After the administrative controls have been put in place that set out what needs to be logged, then the mostly technical controls that define how the events will be logged can be laid out.

We saw in Chapter 2, "Building a Secure Network Using Security Controls," that Cisco has a number of solutions as part of the Cisco Integrated Security Portfolio. These solutions include security management products for multiple devices like Cisco Security MARS, with integral logging and report generation facilities for large networks. Here are some useful questions to ask when deciding on the technical controls needed to report and log events in the network:

- ▶ How can the integrity of both the logs, as well as the communication channels in which the log messages flow, be assured?
- ▶ How can the confidentiality of both the logs, as well as the communication channels in which the log messages flow, be assured?
- ▶ How do you deal with the copious amounts of log messages?
- ▶ How do you ensure that logs all use timestamps from the same clock to properly correlate events with logs, as well as logs with other logs?
- ▶ How can messages be prioritized so that critical messages are separated from routine messages?
- ▶ How can changes be reported when network outages or attacks occur?
- ▶ How do you log events from several devices in one central place?

These questions will be answered in the subsequent sections using the Cisco Secure Life Cycle as a guideline.

Reference Architecture for Secure Management and Reporting

So many questions! Nevertheless, these types of questions must be answered before the acquisition and integration of technology is considered. We will not try to answer these questions now, so we will take a shortcut and assume that they have been adequately answered in the reference architecture that we will be using for the subsequent sections in this chapter.

Figure 4.1 represents a typical architecture for secure management and reporting. It leverages on technologies that the reader would have examined in their CCNA studies, particularly in its use of VLANs to separate the traffic inside the network perimeter into different planes. It will serve as a simple visual tool to provide context for several of the *Implementation* phase guidelines that will be recommended presently.

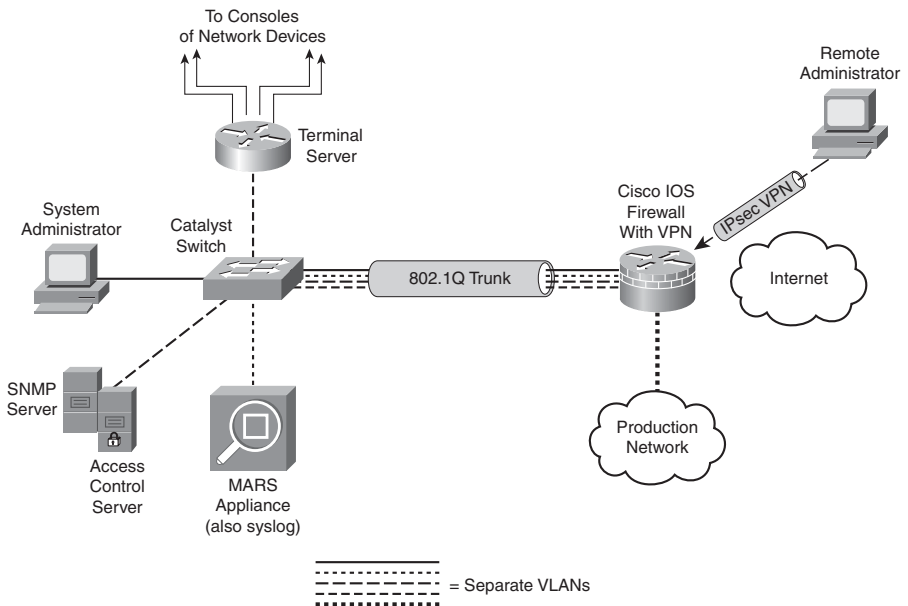


FIGURE 4.1 Reference architecture for secure management and reporting.

The following is a quick explanation of the reference architecture in Figure 4.1. A Cisco IOS firewall with VPN is protecting an organization's network.

The firewall has three interfaces on it. The interfaces are connected to the following:

- ▶ The Internet
- ▶ An inside production network
- ▶ An IEEE 802.1Q trunk to a Cisco Catalyst layer 2 Ethernet switch

Here is an explanation of some of the other security features found in the reference architecture:

- ▶ Ports on the Cisco Catalyst switch are configured in several VLANs (four pictured).
- ▶ The Cisco IOS firewall is routing among these VLANs (router-on-a-stick).
- ▶ ACLs on the Cisco IOS firewall manage traffic between the different VLANs. (See Chapter 5, “Using Cisco IOS Firewalls to Implement a Network Security Policy.”)
- ▶ The firewall is stateful (see Chapter 5) and supports a remote access IPsec VPN for management (see Chapter 7, “Virtual Private Networks with IPsec”).
- ▶ Deployed in different VLANs are the following:
 - ▶ Cisco Security MARS Appliance
 - ▶ SNMP Server
 - ▶ Cisco Secure Access Control Server (ACS)
 - ▶ System Administrator PC
 - ▶ Terminal Server (Used to connect to the console ports of all the network devices.)
 - ▶ Production Network

NOTE

This is a simplified secure network design for the sake of the discussion of the secure management and reporting topics throughout this chapter. It will serve the purpose of demonstrating secure management and reporting but it is lacking depth-of-defense for one thing and intrusion prevention/detection for another. IPS and IDS are discussed in Chapter 8, “Network Security Using Cisco IOS IPS.”

EXAM ALERT

The communication between management hosts and the devices they manage can take two different paths, either by accident or design:

- ▶ **Out-of-band (OOB).** The traffic flows within a network separate from the production network. It is not in the data plane.

Example: A management VLAN.

- ▶ **In-band.** The traffic flows across the production network, the Internet (or other hostile network), or both. It is in the data plane.

Solution: Protect it inside a VPN, either site-to-site or remote access.

Secure Management and Reporting Guidelines

Recall the five steps of the Cisco Secure Network Life Cycle. Clearly, we had some productive meetings and answered the “how to log” and “what to log” questions during the *Initiation* and *Acquisition and Development* phases. Here are some of the guidelines that will be followed in the *Implementation* phase of Cisco’s Secure Network Life Cycle:

- ▶ **General Management Guidelines:**
 - ▶ Synchronize clocks on hosts and network devices.
 - ▶ Document changes and make backups of configurations.
- ▶ **OOB Management Guidelines:**
 - ▶ Find solutions that mitigate the risk of transmitting unsecure management protocols over production networks.
- ▶ **In-Band Management Guidelines:**
 - ▶ Only manage devices that require monitoring or managing
 - ▶ Use encryption (IPsec, SSL, SSH) whenever possible.
 - ▶ Determine if management channel has to be open at all times.

The remaining material in this section addresses these guidelines in detail.

Logging with Syslog

Referring to Figure 4.1, you could deploy a syslog server in one of the private VLANs on the inside of the network. The *syslog server* would accept messages from any device that is configured as a *syslog client*—the Cisco IOS firewall, for example. Other network devices and other IP hosts like a public web server or a mail server could be set up to be syslog clients. There are several advantages to having a central syslog server logging events from a number of different sources. As previously discussed, care has to be taken to ensure that the integrity of the log files is assured, and that the communication path between the syslog server and its clients is not compromised. This is where OOB management and in-band management decisions are made. Also, best practices dictate that the devices’ clocks should be synchronized to a recognized time source using the Network Time Protocol (NTP).

NOTE

If the syslog server is accepting messages from several clients, it is crucial that all the devices' clocks are synchronized from the same source. For example, if an IPS detects an attempted privilege escalation attack on a web server and sends a message to the log server, it might be necessary to correlate this event with the login logs on the web server itself. If the timestamps on the logs cannot be correlated because the devices' clocks are not synchronized, it might be difficult to prove that the two events are linked.

Device synchronization is covered in the section, "Configuring Time Features," later in this chapter.

Cisco Security MARS

Logging to a central syslog server is not only part of the solution but potentially also part of the problem. The biggest issue is the enormity of the task of sifting through the resulting information, correlating the events from several different network devices and application servers and taking different types of actions based on a vulnerability assessment of the incident.

This is what Cisco Security MARS can do. Because Cisco Security MARS understands the complete network topology, MARS can intelligently analyze security events and help focus security staff's efforts in solving the potential problems. For example, false positives are more accurately detected. For example, MARS is used as a reporting and event correlation tool in Chapter 8, "Network Security Using Cisco IOS IPS." MARS sees the entire security architecture and thus sees security events in their complete context. It is a very complex and useful tool for reporting on security events. MARS is introduced in Chapter 2, "Building a Secure Network Using Security Controls."

EXAM ALERT

The MARS appliance is examined only at a high level in this Exam Cram. It is, however, a pivotal device in Cisco's comprehensive Self-Defending Network blueprint for network security. Memorizing MARS's features is recommended!

Where to Send Log Messages

Syslog is a key security policy component, but routers should also be configured to send log messages to one or more of these items:

- ▶ **Console.** Physical terminal lines.
- ▶ **Vtys.** Virtual terminal lines.

- ▶ **Buffered Logging.** Internal router circular buffer.
- ▶ **SNMP Traps.** Event-triggered messages to SNMP server.
- ▶ **Syslog.** External syslog server.

Log Message Levels

Not all messages are as important as others. Some messages are simple system level warnings, whereas others may denote real system emergencies that require immediate human intervention as the system is unusable. For example, an attacker may craft an attack that creates a DoS on a router system, resulting in emergency log messages. If no one's listening, no one knows!

Table 4.1 lists and explains the log severity levels. The “Log String” denotes how the log level appears in a log message.

NOTE

When you specify a level of syslog messages that you want to log, all levels below that level will be logged as well. For example, if the logging level specified is 4 (Warnings), levels 0–3 will also be sent.

TABLE 4.1 Cisco Log Severity Levels

Level	Log String	Name	Description
0	LOG_EMERG	Emergencies	Router unusable
1	LOG_ALERT	Alerts	Immediate action required
2	LOG_CRIT	Critical	Condition critical
3	LOG_ERR	Errors	Error condition
4	LOG_WARNING	Warnings	Warning condition
5	LOG_NOTICE	Notifications	Normal but important event
6	LOG_INFO	Informational	Informational message
7	LOG_DEBUG	Debugging	Debug message

EXAM ALERT

Memorize Table 4.1. Memorization tip: The lower the level number, the more severe the event.

Log Message Format

See Figure 4.2 for the log message format. The example is a level 4 syslog message from an IOS IPS, indicating that a user is attempting to communicate using the MSN Messenger instant messenger (IM) application. The organization's security policy might forbid the use of IM from its workstations, in which case this potential breach may constitute useful evidence for disciplinary purposes.

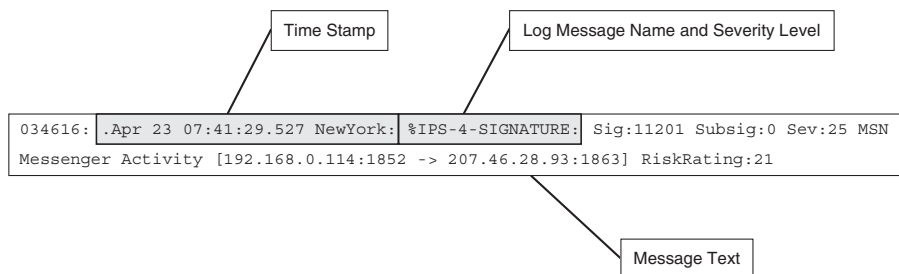


FIGURE 4.2 Log message format.

Enabling Syslog Logging in SDM

Cisco Security Device Manager (SDM) is introduced and examined in Chapter 3, “Security at the Network Perimeter.” Figure 4.3 illustrates how to navigate to the screen to configure syslog on the router.

Starting at the Cisco SDM homepage, follow these steps to enable and configure syslog logging on the Cisco IOS router:

1. Choose **Configure->Additional Tasks->Router Properties->Logging**.
2. Click **Edit** in the logging pane.
3. Check the **Enable Logging Level** check box in the Logging Window and choose the logging level desired from the Logging Level list box.
4. Click **Add**. In the resulting IP Address/Hostname field, enter the IP address of a logging host (syslog server).
5. Click **OK** and then **OK** again to return to the Logging pane.

NOTE

The CLI commands that result are as follows:

```
logging buffered 4096
logging trap debugging
logging host 192.168.99.130
logging on
```

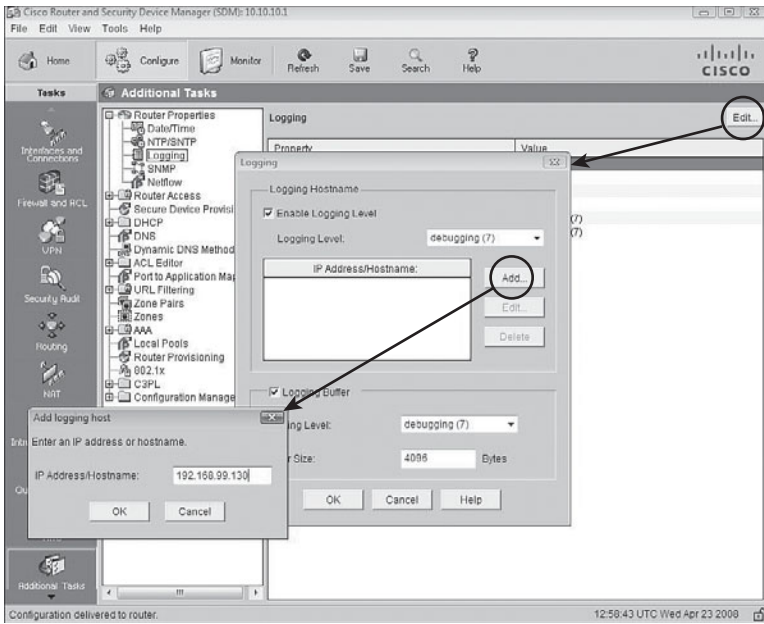



FIGURE 4.3 Enabling Syslog logging in SDM.

You can use Cisco SDM to monitor the internal buffer log, as well as messages that have been sent to syslog servers by choosing **Monitor->Logging** and selecting the **Syslog** tab in the Logging window.

NOTE

You can accomplish the same task by using the **show logging** CLI command.

Using SNMP

The Simple Network Management Protocol (SNMP) has long been deployed in networks to provide for central management of many types of network devices. There are, however, some notable security flaws in the original implementations of this very important protocol, SNMP version 1 and version 2. The protocol remains a valuable tool, and there will likely be a business case for its use. The vulnerabilities of the protocol will be outlined and discussed, as well as strategies for mitigating them, including the use of (the much newer) SNMP version 3.

SNMP Version 1 and 2 Architecture

The Simple Network Management Protocol (SNMP) enables an administrator to configure, manage, and view information on devices and IP hosts. One advantage

of SNMP is that it is vendor-neutral, meaning that a common SNMP architecture can be used for many vendors' products. There are three main elements to the SNMP architecture:

- ▶ **Manager.** Network Management System (NMS). Can retrieve (*get*) information from agents or change (*set*) information in the MIB on agents.
- ▶ **Agent.** Managed Node. Agents can send traps when system events occur and respond to *sets* (configuration commands) and *gets* (information queries).
- ▶ **MIB.** Management Information Base. This is the database of information contained on the agent.

Referring to Figure 4.1, the Cisco Catalyst switch and Cisco IOS firewall could be SNMP agents. The NMS is configured OOB in its own VLAN on an inside network protected by the stateful Cisco IOS firewall.

SNMP v1 and v2 Community Strings

One of the vulnerabilities of SNMP v1 and v2 architecture is that messages are authenticated using cleartext community strings. Community strings have the following attributes:

- ▶ Essentially used for password-only authentication of messages between the NMS and the agent.
- ▶ Read-only (RO) strings are used to *get* information only from an agent's MIB.
- ▶ Read-write (RW) strings are used to *set* and *get* information on an agent.

SNMP Version 3 Architecture

SNMP Version 3 has the following improvements relative to SNMP Version 1 and 2:

- ▶ Messages may be encrypted to ensure confidentiality.
- ▶ Messages may be hashed to ensure integrity.
- ▶ Messages may be authenticated to ensure authenticity.

SNMP v1, v2, and v3 Security Models and Levels

Here is some other useful terminology that should be understood when deploying SNMP:

- ▶ **Security Model.** The security strategy used by an SNMP agent.
- ▶ **Security Level.** Provides a level of granularity within the security model. It is the permitted level of security within the security model.

Let’s look at an example: Referring to Table 4.2, find the *noAuthNoPriv* security level within SNMPv3.

TABLE 4.2 SNMP Security Models and Levels

SNMP Ver	Security Level	Authentication	Encryption	Note
1	noAuthNoPriv	Community String	No	Authenticates with community string.
2c	noAuthNoPriv	Community String	No	Authenticates with community string.
3	noAuthNoPriv	Username	No	Authenticates with username.
3	authNoPriv	MD5 or SHA	No	Authenticates with HMAC-SHA or HMAC-MD5.
3	authPriv	MD5 or SHA	Yes	Authenticates with HMAC-SHA or HMAC-MD5. Encrypts with DES, 3DES, or AES ciphers.

At the *noAuthNoPriv* security level, SNMP v3 uses a username. SNMP v3 is downward-compatible with SNMP v1 and v2 if the username only is used. The username remains cleartext, as is the case with the community string in SNMP v1 and v2.

NOTE

HMAC = Hashing Message Authentication Code. SHA (Secure Hashing Algorithm) and MD5 (Message Digest 5) are examples. DES (Date Encryption Standard), 3DES (Triple-DES), and AES (Advanced Encryption Standard) are all examples of encryption algorithms or ciphers. We examine these in Chapter 6, “Introducing Cryptographic Services.”

Enabling and Configuring SNMP with Cisco SDM

To enable the SNMP agent on the IOS router and configure it to respond to SNMP gets, follow these steps in the Cisco SDM:

1. Choose **Configure->Additional Tasks->Router Properties->SNMP** starting at the SDM homepage.
2. Click the **Edit** button, as shown in Figure 4.4.

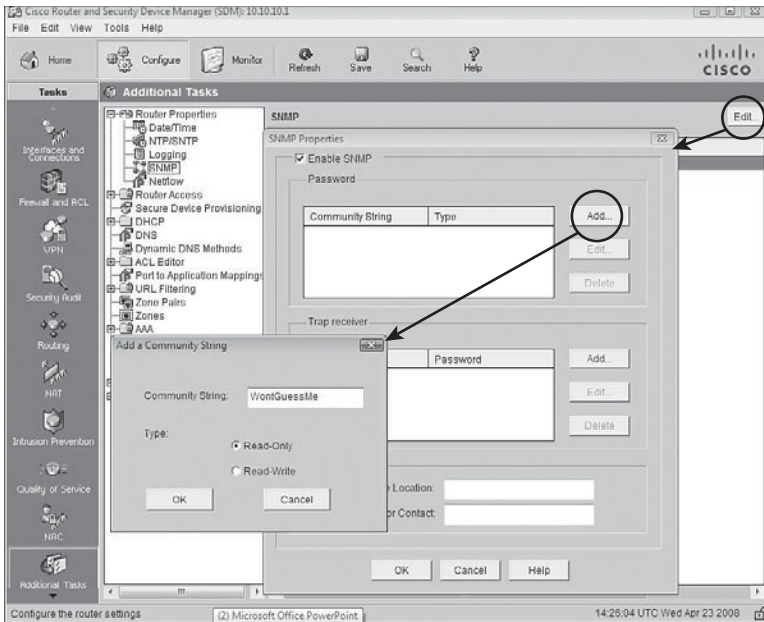


FIGURE 4.4 Enabling and configuring SNMP with Cisco SDM.

3. Check the **Enable SNMP** checkbox in the SNMP Properties pane.
4. As shown in Figure 4.4, click **Add** and fill in the Community String in the **Community String** dialog box. Click either the **Read-Only** or **Read-Write** radio buttons.
5. Click **OK**.

NOTE

SNMP v3 cannot be configured with the Cisco SDM.

Adding an SNMP Trap Receiver

While we're at the SNMP settings page, we can set up a trapping receiver for unsolicited SNMP messages to an SNMP server:

1. Starting at the SNMP pane in Cisco SDM, click **Edit**. The SNMP Properties window displays, as shown in Figure 4.5.
2. Click **Add** to add a new trap receiver in the Trap Receiver section of the SNMP Properties window.

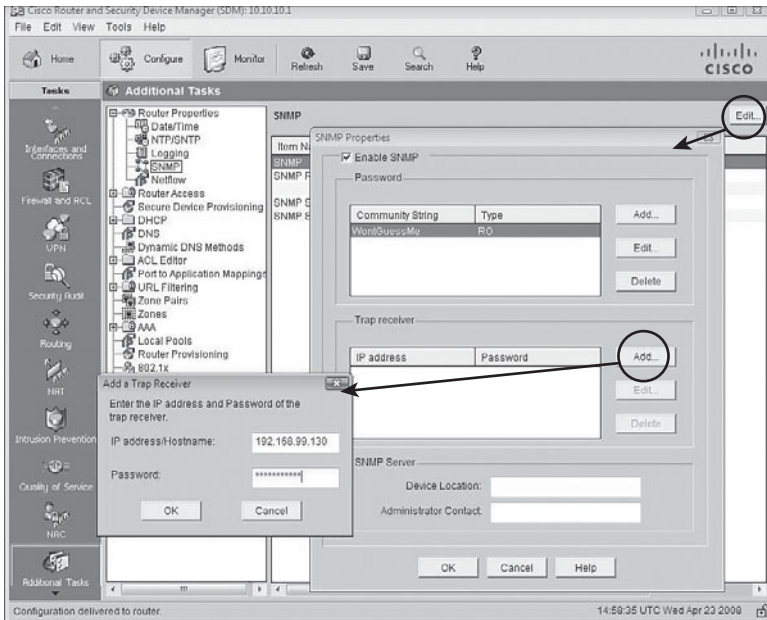


FIGURE 4.5 Adding an SNMP trap receiver using Cisco SDM.

3. Enter the IP address (or hostname) and password of the NMS, which is acting as the trap receiver.
4. Click **OK** to finish adding the trap receiver.

NOTE

The following CLI command results from following the preceding steps:

```
snmp-server host 192.168.99.130 WontGuessMe
```

Configuring the SSH Daemon

In order to ensure that management sessions to the router are confidential, Secure Shell (SSH) is recommended. With respect to the reference architecture in Figure 4.1, SSH could be used to the Catalyst switch and the IOS firewall.

SSH is essentially encrypted Telnet. As such, it should be used instead of Telnet wherever possible, particularly where in-band management of a device is required. There are two versions of SSH:

- ▶ **Version 1.** Cisco IOS Release 12.1(1)T and later.
- ▶ **Version 2.** Cisco IOS Release 12.3(4)T and later. This is more secure than version 1.

NOTE

Beginning with Cisco IOS Release 12.1(3)T, the router can act both as a server and a client. The **ssh** command can be used to launch a client SSH session to an SSH server.

Enabling SSH Using Cisco SDM

The following are prerequisite tasks for enabling SSH using Cisco SDM:

- ▶ Ensure that you have the right release of the Cisco IOS Software image. Only images that contain the IPsec feature set will support the SSH daemon.

NOTE

Typically, IOS images whose names have the string “k8” or “k9” in them are crypto images that support cryptosystems such as IPsec VPNs and the SSH daemon. There are a number of ways that you can determine the image name. One way is the **show flash** command:

```
ciscoISR#show flash
```

```
28672K bytes of processor board System flash (Intel Strataflash)
```

```
Directory of flash:/
```

```
  2 -rwx  18929780 May 15 2008 21:15:14 -04:00 c870-advipservicesk9-  
mz.124-15.T5.bin
```

- ▶ The target systems must be configured with AAA (either local or external) because SSH requires the use of a username and password.
- ▶ Ensure that target systems have unique fully-qualified domain names (FQDNs) if you are using the device's FQDN to SSH to.
- ▶ The domain name must also be set on any device running the SSH daemon because the RSA keys (see the following steps) will not generate without the domain name set.

Using the Cisco SDM, follow these steps to enable SSH on the IOS router:

1. Choose **Configure->Additional Tasks->Router Access->SSH**.
2. If the **Generate RSA Key** button is grayed out (as shown in Figure 4.6), this means that the RSA key exists and SSH is enabled on the router. If the **Generate RSA Key** button is available, press it and follow the prompts to generate a key with a modulus between 512 and 2048 in 64-bit increments. The larger the modulus, the longer it will take to generate the key.

Press this button to generate the RSA keys.

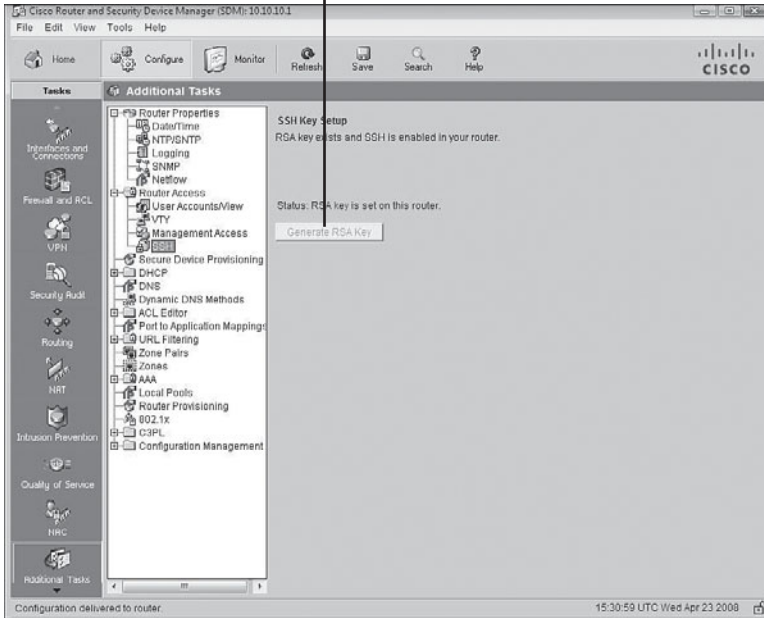


FIGURE 4.6 Enabling the SSH daemon using the Cisco SDM.

3. Click **OK**.

NOTE

SSH is enabled by default on the LAN interface on Cisco IOS routers that ship with the Cisco SDM pre-installed.

Rivest-Shamir-Adleman (RSA) keys are discussed in Chapter 6.

4. Now that we have the SSH daemon operational, we should be able to SSH to it, right? Wrong! Remember what we do with policies; we have to apply them somewhere. SSH has to be enabled on the vty lines. This is accomplished in the Cisco SDM by choosing **Configure->Additional Tasks->Router Access->VTY**. Figure 4.7 shows the Edit VTY Lines dialog box.

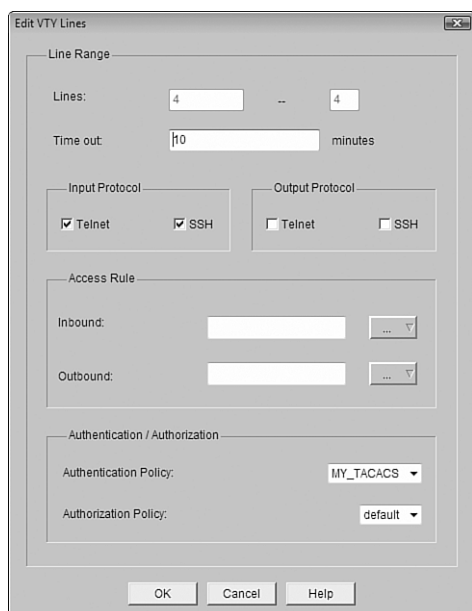


FIGURE 4.7 Edit VTY lines in the Cisco SDM.

Here are the equivalent CLI commands:

```
CiscoISR(config)#ip domain-name example.com
CiscoISR(config)#crypto key zeroize rsa
```

% All RSA keys will be removed.

% All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no]: **yes**

```
CiscoISR(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: CiscoISR.example.com
```

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
CiscoISR(config)#ip ssh time-out 120
CiscoISR(config)#ip ssh authentication-retries 4
CiscoISR(config)#line vty 0 4
CiscoISR(config-line)#transport input ssh
CiscoISR(config-line)#end
CiscoISR#
```


Configuring Time Features

The Cisco SDM enables you to manually:

- ▶ Synchronize the router's clock to the local PC clock.
- ▶ Edit the router's date and time.

Network Time Protocol

Assuming that our security policy requires that all of our network devices have their clocks synchronized to a single, recognized time source, manual setting of the router clock is not an option. We will choose to set the router's clock with a Network Time Protocol (NTP) source. An organization can set up its own master time source (preferably OOB) or synchronize from a public time server on the Internet.

A few important notes:

- ▶ NTP uses UDP port 123 and is considered secure.
- ▶ Simple Network Time Protocol (SNTP) is a simpler and less secure version of NTP.
- ▶ NTP version 3 (NTPv3) and above implement cryptography and authentication between NTP peers (client and server).

You must be careful when synchronizing from an NTP server. Rules of evidence might require you to prove that you are using an unimpeachable source of information to synchronize your devices' clocks if you want to use your logs in the course of a criminal proceeding. This makes using Internet time sources problematic. This might be mitigated somewhat by using your own master time server, but if you are synchronizing it from an Internet time source, you are back to where you started. Therefore, your master time server may need to be synchronized by radio or satellite to meet the security standards required by the security policy.

Figure 4.8 illustrates the steps to add an NTP server using the SDM. Starting at the Cisco SDM homepage, here are the steps required to add an NTP server:

1. Choose **Configure->Additional Tasks->Router Properties->NTP/SNTP**.
2. Click **Add** to add a new NTP server. The Add NTP Server Details window appears.

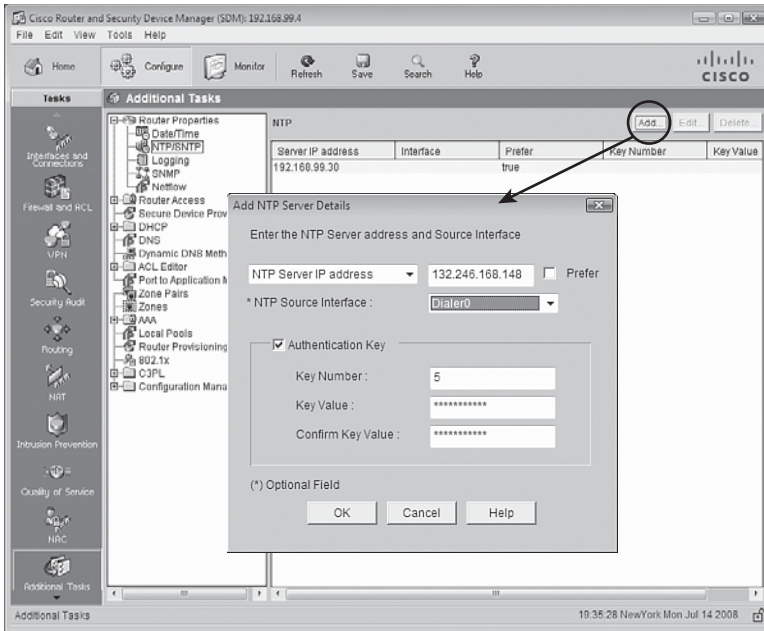


FIGURE 4.8 Configuring NTP in the Cisco SDM.

3. Fill in the details about your NTP server in the Add NTP Server Details window.
 - ▶ (optional) You can select the source interface for your NTP packets from the **NTP Source Interface** drop-down box.
 - ▶ (optional) If this is the preferred NTP server, check the **Prefer** check box. This server will be checked before other servers. You can have more than one preferred server.
4. Check the **Authentication Key** check box if the NTP server requires authentication and fill in the values.
5. To finish adding the server, click **OK**.

NOTE

The CLI command generated by the Cisco SDM in the preceding example would be as follows:
ntp server 192.168.99.30 key cisco123 source vlan2 prefer

Using Cisco SDM and CLI Tools to Lock Down the Router

Cisco routers come with services enabled on them by default that make them great routers, but not necessarily great security devices. The reasons for these default services are various, but generally speaking, they are there more for historical reasons than anything else and would not likely be the defaults were these devices to be given a rethink in the context of current security knowledge. In this section, we quickly summarize some of these default services, their security risk in the context of the router's responsibilities as a perimeter defense device, and (more importantly) what to do about it. As we will see, the router has a number of CLI and SDM tools that can first audit and secondly secure these vulnerabilities.

Router Services and Interface Vulnerabilities

The following is a list of general recommendations for router services and interfaces that are vulnerable to network attacks. They can be grouped into seven categories, as follows:

- ▶ Disable unnecessary services and interfaces.
- ▶ Disable commonly configured management services.
- ▶ Ensure path integrity.
- ▶ Disable probes and scans.
- ▶ Ensure terminal access security.
- ▶ Disable gratuitous and proxy ARP.
- ▶ Disable IP directed broadcasts.

Table 4.3 outlines Cisco's recommendations for disabling vulnerable router services and interfaces.

TABLE 4.3 Recommendations for Vulnerable Router Services and Interfaces
Disable these unnecessary services and interfaces:

Unused router interfaces	Cisco Discovery Protocol
BOOTP server	Configuration autoloading
FTP server	TFTP server
NTP service	PAD service
TCP and UDP minor services	DEC MOP service
Disable commonly configured management services:	
SNMP	HTTP or HTTPs configuration and monitoring
DNS	
Ensure path integrity:	
ICMP redirects	IP source routing
Disable probes and scans:	
Finger	ICMP unreachable notifications
ICMP mask reply	
Ensure terminal access security:	
IP identifications service	TCP keepalives
Disable gratuitous and proxy ARP:	
GARP	Proxy ARP
Disable IP directed-broadcast	

A detailed explanation of the vulnerabilities presented by these features will not be attempted. What follows is a quick summary of the services and their respective vulnerabilities as well as security recommendations.

Disable Unnecessary Services and Interfaces

The following are Cisco’s recommendations for disabling unnecessary services and interfaces:

- ▶ **Router Interfaces.** Disabling unused router interfaces will limit unauthorized access to both the router and the network.
Recommendation: Disable unused open router interfaces.
- ▶ **Bootstrap Protocol (BOOTP).** This service is enabled by default. It allows other devices to obtain IP addresses and other configuration information automatically.
Recommendation: This service is rarely needed and should be disabled.

- ▶ **Cisco Discovery Protocol.** Enabled by default. This protocol allows the router to discover information about directly connected neighbor Cisco devices.

Recommendation: This service is not required once a network has been constructed and tested. Disable.

- ▶ **Configuration Autoloading.** Disabled by default. It allows the autoloading of configuration files from a network server.

Recommendation: Disable unless needed.

- ▶ **FTP Server.** Disabled by default. Allows the router to act as an FTP server and serve files from flash memory to FTP clients.

Recommendation: Disable unless needed.

- ▶ **TFTP Server.** Disabled by default. Allows the router to act as a TFTP server and serve files from flash memory to TFTP clients.

Recommendation: Disable unless needed

- ▶ **Network Time Protocol (NTP) Service.** This protocol was discussed in the last section, as were recommendations for its use.

Recommendation: Disable unless needed.

- ▶ **TCP and UDP Minor Services.** These services are disabled by default in Cisco IOS Software Release 11.3 and later. They are small daemons that have a diagnostic purpose but are rarely needed.

Recommendation: Disable this service explicitly.

- ▶ **Maintenance Operation Protocol (MOP) Service.** Enabled by default on most Ethernet interfaces. It is a legacy Digital Electronic Corporation (DEC) maintenance protocol.

Recommendation: Disable this service explicitly when it is not in use.

Disable and Restrict Commonly Configured Management Services

The following are Cisco's recommendations for disabling and restricting commonly configured management services:

- ▶ **Simple Network Management Protocol (SNMP).** Enabled by default. This protocol's vulnerabilities (SNMP versions 1 and 2) were discussed in a previous section in this chapter.

Recommendation: Disable this service when it is not required.

- ▶ **HTTP or HTTPS Configuration and Monitoring.** Default operation is device-dependent. Used for monitoring and configuring the device using a web browser and/or Cisco SDM.

Recommendation: Disable if not in use or restrict access using ACLs.

- ▶ **Domain Name System (DNS).** Enabled by default. Also by default, the DNS client broadcasts its request to destination IP address 255.255.255.255. This makes it vulnerable to spoofed responses, possibly leading to session-hijacking.

Recommendation: Disable if not required. If it is required, set the DNS lookup service with the unicast address of specific DNS servers.

Ensure Path Integrity

The following are Cisco's recommendations for ensuring path integrity. Path integrity ensures that the path that data packets take through the network is not somehow redirected or otherwise compromised by an exploit:

- ▶ **Internet Control Message Protocol (ICMP) redirects.** Enabled by default. When a router receives an ICMP redirect on an interface, it is required to resend the packet out the same interface that it was received. If this is an Internet-facing interface, an attacker could use the resent information to redirect packets to an untrusted device, a classic session hijacking exploit.

Recommendation: Disable this service if it is not required.

- ▶ **IP source routing.** Enabled on interfaces by default. Routing is normally destination-based, but a IP host can indicate which path it would prefer to take through a network by specifying IP source-routing options in the IP packet header. Routers would be forced to honor this path. This can be exploited by an attacker as a carefully crafted attack that would take the attacker's choice of path through an unprotected network rather than the best path indicated in the routing table.

Recommendation: Disable this service on all interfaces unless it is required.

Disable Probes and Scans

The following are Cisco's recommendations for disabling probes and scans of the network and the router itself:

- ▶ **Finger Service.** Enabled by default. Finger service allows a reconnaissance of the router to determine a list of users currently using a particular device, among other information.

Recommendation: Disable this service if it is not required.

- **ICMP Unreachable Notifications.** Enabled by default. This service notifies users of unreachable IP hosts and networks. It can be used during a reconnaissance attack to map out a network's topology because if the attacker doesn't receive an ICMP unreachable notification in reply to an ICMP request, they can infer that the network is reachable.

Recommendation: An attacker can infer all they want! Turn off ICMP unreachable notifications on all interfaces facing untrusted networks unless they are required.

- **ICMP Mask Reply.** Disabled by default. Same general vulnerabilities as ICMP unreachables.

Recommendation: Turn off ICMP mask replies on all interfaces facing untrusted networks unless they are required.

Ensure Terminal Access Security

The following are Cisco's recommendations for ensuring terminal access security. These recommendations will mitigate the possibility that an attacker can identify the device and launch certain DoS attacks against the device itself:

- **IP Identification (IDENT) Service.** Enabled by default. Useful in reconnaissance attacks. When TCP port 113 is probed, the identity of the device is obtained.

Recommendation: Disable explicitly.

- **TCP Keepalives.** Disabled by default. This service is a reaper service that polls TCP sessions to see if they are still active. If a response isn't received, the connection is closed, thereby freeing up resources on the router and preventing certain DoS attacks.

Recommendation: Should be enabled globally.

Disable Gratuitous and Proxy Address Resolution Protocol (ARP)

The following are Cisco's recommendations for disabling gratuitous and proxy address resolution protocol (ARP) messages.

- **Gratuitous ARP (GARP).** Enabled by default. It is commonly used in ARP poisoning attacks. It is gratuitous in that they are ARP replies that don't match ARP requests. The intent is to fool IP hosts to cache these

replies in their ARP tables so that the host will send packets to the attacker versus the legitimate hosts whose IP addresses and MAC addresses the attacker has spoofed.

Recommendation: Should be disabled on each interface unless it is needed.

- **Proxy ARP.** Enabled by default. This service allows the router to reply to an ARP request by proxy with its own MAC address where an IP address resolves to a remote segment.

Recommendation: Should be disabled unless the router is acting as a layer 2 LAN bridge.

Disable IP Directed-broadcasts

This service is disabled by default in Cisco IOS Release 12.0 and later. IP directed-broadcasts are used in smurf and other related DoS attacks.

Recommendation: This service should be disabled if not required.

Performing a Security Audit

Now that we have identified the specific vulnerabilities that may be present on the router, we will perform a security audit of the router using the Cisco SDM, as well as some CLI tools.

The Cisco SDM Security Audit, shown in Figure 4.9, is based on the Cisco IOS AutoSecure feature (also accessible by the CLI, as we will see later), which is an automated, interactive script that checks for vulnerabilities and recommends how they might be remediated. As we will see, the Cisco SDM Security Audit has *almost* all the feature of the Cisco AutoSecure functions.

The Security Audit Wizard can be reached by choosing **Configure->Security Audit** from the Cisco SDM homepage. There are two modes of operation, as indicated in Figure 4.9:

- **Security Audit Wizard.** Once vulnerabilities are discovered, the wizard gives you a choice as to which vulnerabilities you want to secure. Press the **Perform security audit** button if you want this.
- **One-Step Lockdown.** This configures the router with a set of defined security features with recommended settings in one step and without further user interaction. Press the **One-step lockdown** button if you want this.

Let's examine the Cisco SDM Security Audit Wizard first.

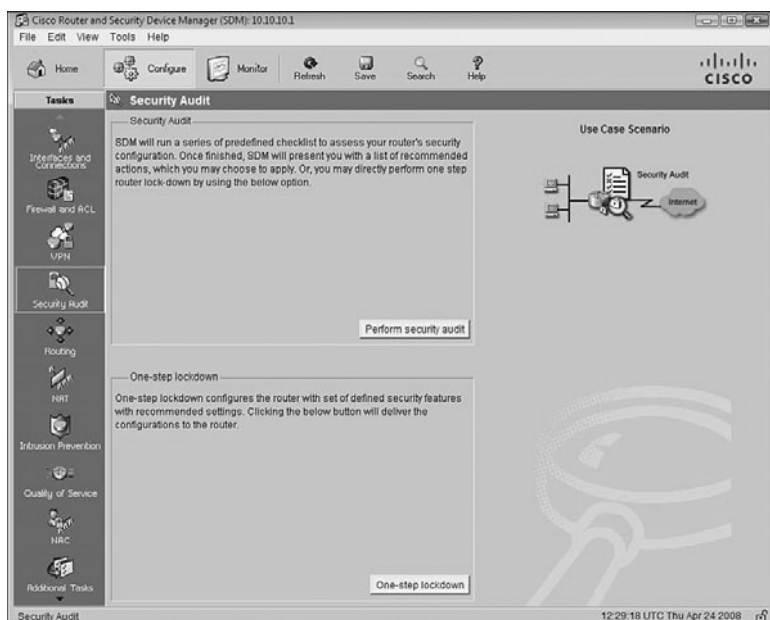


FIGURE 4.9 The Cisco SDM Security Audit homepage.

Cisco SDM Security Audit Wizard

In the last section, we identified the specific vulnerabilities that may be present on the router. Now we will use the Cisco SDM Security Audit Wizard to determine whether they are present and give us the option to remedy them.

To perform a security audit, follow these steps from the Cisco SDM homepage:

1. Choose **Configure->Security Audit**.

NOTE

The figures in this series of steps are based on a Cisco 800 Series ISR whose inside interface is *Vlan1* and whose outside interface is *FastEthernet4*.

2. Click the **Perform Security Audit** button. The Welcome Page of the Security Audit Wizard appears.
3. Click **Next** to bring up the Security Audit Interface Configuration page as shown in Figure 4.10.

6. If you want to save the report to a file, click **Save Report**.
7. To continue with fixing the identified security issues, click **Close**.
8. The Security Audit Wizard window appears, as shown in Figure 4.12. If you want to fix the security problems identified, you can either check the **Fix it** check box in the Action column beside each identified security problem you want to fix, or you can click the **Fix All** button, which checks all the boxes for you.

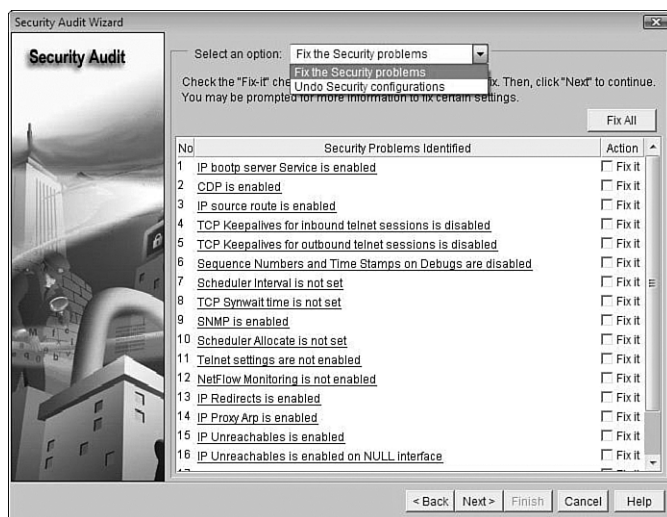


FIGURE 4.12 Security Audit Wizard window.

If you want to undo security problems that have been identified as “Passed” in the Security Audit report window (refer to Step 5), you can choose **Undo Security configurations** in the **Select an option** drop-down list at the top of the Security Audit window. The resulting Security Audit Wizard window will allow you to check off **Undo** in the Action column beside each enabled security configuration you want to undo.

NOTE

Interestingly, each security problem identified is a hyperlink that, if selected, will pop up a description of the problem from the SDM's built-in context-sensitive help feature. This will help the administrator decide on a course of action for that specific vulnerability.

9. Click **Next**.

10. Depending on which security vulnerabilities you have chosen to fix, you might be asked to enter more information on the subsequent screens. Enter the required information and click **Next** as indicated until you arrive at the Summary screen.
11. Click **Finish** to deliver the changes to the router.

Cisco SDM One-Step Lockdown

The Cisco one-step lockdown feature can be executed using either the Cisco SDM or the CLI command, **auto secure**. Complete the following steps to perform a one-step lockdown using the Cisco SDM, starting at the SDM home-page:

1. Choose **Configure->Security Audit->One-step lockdown**.
2. An SDM Warning dialog appears, as shown in Figure 4.13. Click **Yes** if you are sure you want to lock down the router. A one-step lockdown window appears with a check mark beside all the items that will be fixed.

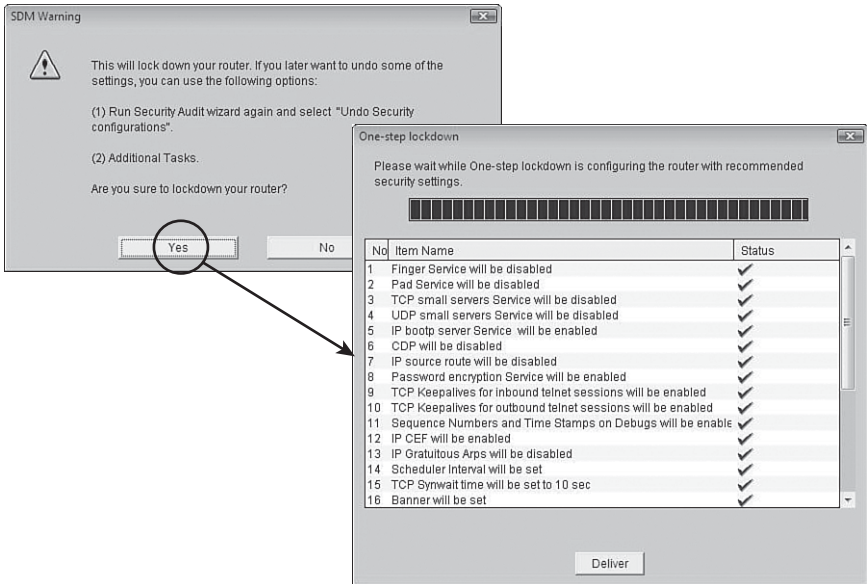


FIGURE 4.13 Cisco SDM one-step lockdown.

3. Click **Deliver** to deliver the configuration changes to the router.
4. Click **OK** to exit back to the Security Audit window.

Using the Cisco AutoSecure Feature to Lock Down a Router

Cisco AutoSecure is a feature that is initiated from the CLI and executes a script, which first makes recommendations for fixing security vulnerabilities, and then modifies the security configuration of the router. The syntax of the command is as follows:

```
auto secure [no-interact]
```

It can be executed in either of two modes:

- **Interactive Mode.** Prompts the user with recommendations for enabling and disabling specific services. This is the default mode. Use the **auto-secure** command with no options.
- **Non-Interactive Mode.** Automatically executes the Cisco AutoSecure command with Cisco's recommended default settings. Use the **auto secure no-interact** form of the command.

Here is what the opening dialog looks like. This example is using the interactive mode:

```
ciscoISR#auto secure
-- AutoSecure Configuration --
```

```
***AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks***
```

```
AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
```

```
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
```

```
Gathering information about the router for AutoSecure
```

```
Is this router connected to internet? [no]:yes
[output omitted]
Securing Management plane services...
```

```
Disabling service finger
Disabling service pad
Disabling udp&tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
```

Disabling the cdp protocol

Disabling the bootp server

Disabling the http server

Disabling the finger service

Disabling source routing

Disabling gratuitous arp

Configure NTP Authentication? [yes]:**no**

Configuring AAA local authentication

Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport

Securing device against Login Attacks

Configure the following parameters

Blocking Period when Login Attack detected: **120**

At the end of the AutoSecure interactive dialog, the recommended running-config with the changes to be applied is displayed. You are then asked:

Apply this configuration to running-config? [yes]:**yes**

NOTE

Once applied to the running-config, if you lose connectivity to the router or something stops working, you can always reboot the router because the changes will not have been saved to the startup-config. This sounds strange, but many security texts recommend this procedure. Essentially if you don't know what a service does, turn it off. If something important stops working as a result, you now know what it does. Locking down a network device, despite the excellent features such as AutoSecure, is often a trial-and-error approach.

You should consider testing these changes in a lab environment first, and only make changes on a production network when you are absolutely sure of what you are doing.

Caveats: Cisco AutoSecure Versus Cisco SDM Security Audit

There are some notable limitations and differences between Cisco AutoSecure and the Cisco SDM Security Audit:

- ▶ Cisco SDM does not implement the following Cisco AutoSecure features:
 - ▶ Disabling NTP
 - ▶ Configuring AAA
 - ▶ Setting SPD values
 - ▶ Enabling TCP intercepts
 - ▶ Configuring anti-spoofing ACLs on outside-facing interfaces

- ▶ Cisco SDM implements some Cisco AutoSecure features differently:
 - ▶ SNMP is disabled but will not configure SNMPv3 (varies with router).
 - ▶ SSH is enabled and configured with Cisco IOS images that support this feature.
 - ▶ Curiously, Secure Copy Protocol (SCP) is not enabled and unsecure FTP is.

Exam Prep Questions

1. Which of the following is *not* a consideration for setting up technical controls in support of secure logging?
 - ☐ A. How can the confidentiality of logs as well as communicating log messages be assured?
 - ☐ B. How do you log events from several devices in one central place?
 - ☐ C. What are the most critical events to log?
 - ☐ D. What are the most important logs?
 - ☐ E. None of the above.

2. Fill in the blank with the correct term from the choices.

One communication path between management hosts and the devices they manage is _____, meaning that the traffic flows within a network separate from the production network.

 - ☐ A. In-band
 - ☐ B. Inter-vlan
 - ☐ C. Private
 - ☐ D. Out-of-band
 - ☐ E. Intranet

3. True or false. A general management guideline is to ensure that clocks on network devices are not synchronized with an external time source because this is a known vulnerability.

4. Indicate the number for each logging level:
 - ▶ Debugging: _____
 - ▶ Alerts: _____
 - ▶ Emergencies: _____
 - ▶ Notifications: _____
 - ▶ Critical: _____
 - ▶ Informational: _____
 - ▶ Warnings: _____

5. To what menus do you have to navigate to setup logging in the SDM?
 - ☐ A. Configure->Router Management->Additional Tasks->Logging
 - ☐ B. Configure->Additional Tasks->Router Properties->Logging

- ☐ C. Monitor->System Properties->Configure->Syslog
- ☐ D. Configure->Additional Tasks->Router Properties->Syslog
- ☐ E. Monitor->Logging Options->Syslog Setup

6. Match the following SNMP terms with their definitions:

- 1. MIB: ____
- 2. Agent: ____
- 3. NMS: ____

- A. Responds to sets and gets
- B. Sends sets and gets
- C. Information database

7. True or false. Secure Network Time Protocol (SNTP) is more secure than regular NTP as it requires authentication.

8. Which of the following is part of Cisco's list of seven categories of vulnerable router services and interfaces? (Choose all that apply.)

- ☐ A. Disable unnecessary services and interfaces.
- ☐ B. Disable commonly configured management services.
- ☐ C. Ensure path integrity.
- ☐ D. Disable probes and scans.
- ☐ E. All of the above.

9. Fill in the blank with the correct term from the choices.

The Cisco SDM Security Audit Wizard and One-Step Lockdown tools are based on the Cisco _____ feature.

- ☐ A. Auto-Initiate
- ☐ B. SafeAudit
- ☐ C. AuditMany-SecureOnce
- ☐ D. AutoSecure
- ☐ E. None of the above.

10. True or false. SNMPv3 is implemented in the Cisco SDM Security Audit Wizard but not in the auto secure CLI command.

Answers to Exam Prep Questions

1. Answer E is correct because all the choices are valid considerations.
2. The right answer is D, out-of-band (OOB). A design goal for a secure network is to try to separate management traffic from the production networks wherever possible. Answer A is the opposite. The other answers are incorrect because they are not used in this context.
3. False. This is a bit of a trick question. Yes, there are some known vulnerabilities with synchronizing clocks with external time sources, but these are outweighed by the advantage of having all network devices' clocks synchronized to a single time source.
4. The logging levels are the following:
 - ▶ Debugging: 7
 - ▶ Alerts: 1
 - ▶ Emergencies: 0
 - ▶ Notifications: 5
 - ▶ Critical: 2
 - ▶ Informational: 6
 - ▶ Warnings: 4
5. The correct answer is B. The other choices, although they look vaguely correct, do not represent real choices.
6. The correct answers are: 1—C; 2—A; 3—B. MIB stands for Management Information Base and resides on an agent. The information in this database can be queried (get) or configured (set) by a Network Management System (NMS).
7. False. SNTP stands for Simple Network Time Protocol and is considered less secure than NTP. NTPv3, on the other hand, is more secure because it implements cryptography and authentication between NTP peers.
8. Answer E is correct. The complete list is as follows:
 - ▶ Disable unnecessary services and interfaces.
 - ▶ Disable commonly configured management services.
 - ▶ Ensure path integrity.
 - ▶ Disable probes and scans.
 - ▶ Ensure terminal access security.
 - ▶ Disable gratuitous and proxy ARP.
 - ▶ Disable IP directed broadcasts.
9. Answer D is correct. The other choices are made up and don't appear in any context with Cisco network security.
10. False. SNMPv3 is not part of the Cisco SDM Security Audit Wizard.

Index

NUMBERS

3DES (3Data Encryption Standard), 264-265, 304

A

AAA (Authentication, Authorization and Accounting), 114

- aaa accounting command, 140
- aaa authentication login default local command, 120
- aaa local authentication attempts max-fail command, 120
- aaa new-model command, 119
- accounting configuration, 139-140
- administrative access, 115
- clear aaa local user lockout command, 121
- configuration snapshots, 141
- debug aaa command, 120
- exec authentication policies, creating, 136

- login authentication policies, creating, 134-135
- network authentication policies, creating, 138
- no aaa new-model command, 119
- RADIUS, 125, 129-130, 140-141
- remote user network access, 115
- router implementation
 - external AAA, 115-116, 122, 127-140
 - local AAA, 115-120
 - reasons for, 114
 - types of router access, 116
- show aaa local user lockout command, 120
- show aaa sessions command, 121
- show aaa user all command, 121
- TACACS+, 125, 129-131, 140-141
- troubleshooting, local AAA, 140-141

AAA Client Hostname field (Secure ACS Network Configuration page), 130

AAA Client IP Address field (Secure ACS Network Configuration page), 130

AAA clients. *See* NAS

academic hackers, 31

access (physical), best practice against network attacks, 46

access-class command, 102

access-list command, 99

accounting (AAA)

- administrative access, 115
- configuration snapshots, 141
- configuring, 139-140
- remote user network access, 115
- router implementation
 - external AAA, 115-116
 - local AAA, 115-120
 - reasons for, 114
 - types of router access, 116
- troubleshooting, local AAA, 140-141

ACE (Application Control Engine), 77

ACL (Access Control Lists), 203

- best practices, 208
- common services, filtering, 216-217
- configuring via Cisco SDM, 209-211
- crypto ACL
 - Step-by-Step Setup mode (Site-to-Site VPN Wizard), 333-334
 - traffic-defining
 - crypto ACL, creating in IPsec VPN, 319-320
 - verifying, 325
- Firewall and ACL Wizard (SDM), 110
- ICMP, filtering, 216-217
- identifying, 205
- inbound IP address spoofing, 204, 213-214
- IPsec VPN compatibility, 315-316
- named ACL, 205
- network services, filtering, 212
- numbered ACL, 205
- outbound IP address spoofing, 204, 215
- router service traffic, filtering, 217
- static packet-filtering firewalls, creating, 204-217
- usage examples, 205-208
- ZPF, 220

ACS (Access Control Servers). *See* Secure ACS**Add AAA Server dialog (SDM), 131****Add Server window (SDM), Server IP or Host field, 131****Additional Tasks menu (SDM), 111-112****administrative access (AAA), 115****administrative access (routers), 91**

- banner messages, 104
- CLI role-based access, configuring, 98-100
- IOS resilient configuration feature (Cisco), 101-102
- line interfaces, 92-93
- passwords
 - best practices, 94
 - configuring, 94-97
 - console
 - passwords, 94
 - enable passwords, 95
 - minimum length configuration, 96
 - recovering, 97
 - secret passwords, 95
 - service password encryption, 95
 - timeouts, 96
 - username
 - security, 96
 - virtual passwords, 95
- privilege levels, setting, 97
- view creation, 98-100
- virtual login security, 102-103

administrative controls

- attributes of, 23
- best practices against network attacks, 45

administrative law, prosecuting computer crimes, 27**AES (Advanced Encryption Standard), 253-255, 265-266, 304****AES Homepage website, 505****age metric (data classification), 22****AH (Authentication Headers), IKE Phase II, 312-313****AIM-VPN (Advanced Integration Module-Virtual Private Networks), 300****alarms (signature), security levels, 359-360****answers (practice exams)**

- exam 1, 461-469
- exam 2, 487-496

anti-replay, site-to-site VPN, 303**AnyConnect VPN Client, 300****application inspection firewalls, 199-200****Application Layer (OSI Layers 5-7), encryption, 249****application layer gateways, 194-195****application servers, VoIP, 412****applications, software security, 398****ARP (Address Resolution Protocol)**

- disabling, 172
- GARP, disabling, 171

ASA 5500 Series Adaptive Security appliances, 202, 299**ASR (Aggregation Service Routers), web resources, 90**

assets, defining (network security policies), 62

asymmetric key encryption algorithms, 251, 275

- authentication via, 277
- DH, 255
- length of, 253
- private key algorithms, 276
- public key algorithms, 276
- speed of, 253
- trusted algorithms, 255
- types of, 253

atomic signatures, 358

attacks (network)

- availability attacks, 42
 - botnets, 43
 - computer environment attacks, 44
 - DDoS attacks, 44
 - DoS attacks, 43
 - electrical power attacks, 44
 - ICMP floods, 43
 - MAC floods, 45
 - physical environment attacks, 44
 - SYN floods, 44
- best practices against
 - administrative controls, 45
 - education, 45
 - encryption, 46
 - environmental control, 46
 - hardware, 46
 - passwords, 46
 - patches, 45
 - physical access, 46
 - physical controls, 46
 - security policies, 45
 - TCP ports, 46

- technical controls, 46
- UDP ports, 46
- unnecessary services, 46

confidentiality attacks, 36

- covert channel attacks, 37
- dumpster diving, 37
- emanation capturing, 37
- identity theft, 38
- overt channel attacks, 37
- packet sniffing (protocol analysis) attacks, 37
- pharming attacks, 38
- phishing attacks, 38
- ping sweeps, 37
- port scanning attacks, 37
- protocol analysis (packet sniffing) attacks, 37
- social engineering attacks, 37

DDoS attacks, 36

Defense in Depth philosophy, 33-34

DoS attacks, 36
exploits, defining, 30
external threats

- examples of, 16
- protecting against, 17

hackers

- motivations of, 31
- specializations of, 31
- thought process of, 32
- types of, 31

integrity attacks

- data diddling, 39
- password attacks, 39

- port redirection attacks, 40
- salami attacks, 39
- session hijacking, 39
- trust exploits, 39

internal threats

- best practices against, 17
- examples of, 16
- seriousness of, 17

IP spoofing, 34-36

MiM attacks, 36

risks, defining, 30

seven steps for compromising targets and applications, 32

vulnerabilities, categories of, 30

audits (security). See Security Audit Wizard (SDM)

AUP (Acceptable Use Policies), 64

Authenticate Using drop-down list (Secure ACS Network Configuration page), 131

authentication (AAA), 19, 114

- administrative access, 115
- applications requiring authentication list, 40
- asymmetric key encryption algorithms, 277
- certificate-based authentication, 283-284
- configuration snapshots, 141
- exec authentication policies, creating, 136
- login authentication policies, creating, 134-135

authentication (AAA)

- network authentication policies, creating, 138
- remote user network access, 115
- router implementation
 - external AAA, 115-116, 122, 127-140
 - local AAA, 115-120
 - reasons for, 114
 - types of router access, 116
- site-to-site VPN, 295, 303, 306
- troubleshooting, local AAA, 140-141

authorization (AAA)

- administrative access, 115
- configuration snapshots, 141
- remote user network access, 115
- router implementation
 - external AAA, 115-116
 - local AAA, 115-120
 - reasons for, 114
 - types of router access, 116
- troubleshooting, local AAA, 140-141

auto secure command, 103**autoloading configurations, disabling, 169****auxiliary line interfaces, 93****Availability (CIA triad), 19-20****availability attacks, 42**

- botnets, 43
- computer environment attacks, 44
- DDoS attacks, 44
- DoS attacks, 43
- electrical power attacks, 44

- ICMP floods, 43
- MAC floods, 45
- physical environment attacks, 44
- SYN floods, 44

AVS (Application Velocity System), 60, 77

B

bandwidth

- broadcast traffic limitations, 437
- multicast traffic limitations, 437
- unicast traffic limitations, 438

banner messages, 104**Basic Firewall Wizard (SDM), ZPF configuration, 224-233****BCP (Business Continuity Planning)**

- categories of disruption, 60
- phases of, 59

BID (Bridge IDs), 426**birthday attacks, 250****black hat hackers, 31****blind spoofing attacks, 36****block ciphers, 254, 263****blue hat hackers, 31****BOOTP (Bootstrap Protocol), disabling, 168****botnets, 43****BPDU (Bridge Protocol Data Units), STP manipulation attacks, 426****BPDU Guard, mitigating STP manipulation attacks, 427-428****broadcast storms, 436-437****broadcast traffic, bandwidth limitations, 437****browsers (web)**

- SDM requirements, 108
- Secure ACS support, 127

brute force attacks, 249**buffer overflows, endpoint security, 399-400**

C

CA (Certificate Authorities)

- central (single-root) CA topology, 279
- CRL, 280
- cross-certified CA, 279
- defining, 277
- hierarchical CA topology, 279

call agents, VoIP, 412**call policies, VoIP, 416****CAM (Content Addressable Memory), table overflow attacks, 428-429****Category window (IPS Policies Wizard), 369****CBC (Cipher Block Chaining) mode, block ciphers, 263****CCP (Cisco Configuration Professional), 105****CD-ROM**

- installing, 500-501
- system requirements, 500
- test modes
 - certification mode, 499
 - custom mode, 500
 - study mode, 499

central (single-root) CA topology, 279**Certicom VPN client, 300**

certificates, 279

- authentication via, 283-284
- defining, 277
- enrollment process, 282-283
- issuing, 283
- OSI application layer, viewing at, 285
- retrieving, 283
- uses of, 285

certification exams

- exam cram usage strategies, 12
- self-assessment, 5-9
- topics of, 10-11

certification mode (CD-ROM), 499**CFB (Cipher Feedback) mode, stream ciphers, 263****chain of custody, 26****Change and Configuration Controls operations security principle, 54****chosen-ciphertext attacks, 250****chosen-plaintext attacks, 250****CIA triad (Confidentiality, Integrity, Availability), 303**

- Availability, 19-20
- Confidentiality, 18-20
- Integrity, 19-20

ciphers

- block ciphers, 254, 263
- defining, 246
- DES cipher, 250
- stream ciphers, 254-255, 263

ciphertext

- chosen-ciphertext attacks, 250

- ciphertext-only attacks, 249

- defining, 246

Cisco ASA 5500 Series Adaptive Security appliances, 202**Cisco AutoSecure feature, 177-179****Cisco Discovery Protocol, disabling, 169****Cisco Host Security Strategy, 397-398****Cisco IOS firewalls, 201****Cisco IOS IPS (Intrusion Prevention Systems)**

- benefits of, 362-363
- configuration verification, 384-385
- configuring via
 - CLI, 377
 - SDM, 364-372, 375-376
- feature blend, 362
- interface verification, 386
- IPS Policies Wizard, 367, 369-370
- IPS Rule Wizard, 367
- policy verification, 384
- SDEE support, 381-383
- settings verification, 386
- signatures
 - configuring, 378-380
 - integration, 363

Cisco IOS resilient configuration feature, 101-102**Cisco PIX 500 Series firewalls, 201****Cisco Security Center website, 504****Cisco Security Manager, 78****Cisco Security MARS. *See* MARS****Cisco Self-Defending Networks**

- firewalls role in, 190
- website, 504

civil law, prosecuting computer crimes, 27**class maps, ZPF configurations, 235****classifying data, 21**

- age metric, 22
- criteria for, 22
- custodian role, 22
- owner role, 22
- personal association metric, 22
- personnel classification via, 22
- private sector classification, 22
- public sector classification, 21
- useful life metric, 22
- user role, 22
- value metric, 22

clear aaa local user lockout command, 121**cleartext (plaintext)**

- chosen-plaintext attacks, 250
- defining, 246
- known-plaintext attacks, 249
- ACL usage examples, 205-208

CLI (Command-Line Interface)

- IOS IPS configuration, 377
- IPsec implementation on site-to-site VPN
 - ACL compatibility, 315-316
- crypto ACL verification, 325

- crypto map
 - creation, 320
- IKE Phase II SA verification, 322-324
- IPsec transform set configuration, 318-319
- ISAKMP (IKE Phase I) policy sets, 316-318
- ISAKMP SA verification, 324
- traffic-defining
 - crypto ACL creation, 319-320
- troubleshooting, 321
- verifying, 321-325
- role-based access, configuring, 98-100
- client mode (SSL VPN), 296**
- clientless mode (SSL VPN), 296**
- Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, The, 505*
- cold site backups, 61**
- common services, filtering via ACL, 216-217**
- community strings, SNMP, 158**
- compromising targets, seven steps for, 32**
- computer crimes, prosecuting**
 - administrative law, 27
 - civil law, 27
 - complications in, 26
 - criminal law, 27
 - ethics, 27
 - investigations, 25
 - liability, 28
 - U.S. government regulations, 28-29
- computer environment, attacks on, 44**
- Computer Fraud and Abuse Act, 29**
- computer security hackers, 31**
- concept of least privilege, 72**
- confidential data classification level, 21-22**
- confidentiality, 294, 302-305**
- Confidentiality (CIA triad), 18-20**
- confidentiality attacks, 36**
 - covert channel attacks, 37
 - dumpster diving, 37
 - emanation capturing, 37
 - identity theft, 38
 - overt channel attacks, 37
 - packet sniffing (protocol analysis) attacks, 37
 - pharming attacks, 38
 - phishing attacks, 38
 - ping sweeps, 37
 - port scanning attacks, 37
 - protocol analysis (packet sniffing) attacks, 37
 - social engineering attacks, 37
- Config Location window (IPS Policies Wizard), 369**
- Configuration Autoloading, disabling, 169**
- Configuration Interceptor (CSA), 406**
- configure command, 97**
- Configure mode (SDM), 110**
- configuring**
 - AAA, configuration snapshots, 141
 - accounting (AAA), 139-140
 - ACL via SDM, 209-211
 - banner messages, 104
 - CLI role-based access, 98-100
 - endpoints, VoIP, 417
 - external AAA on routers via Secure ACS, 122, 127
 - AAA client additions, 129-130
 - AAA network configuration, 129-132
 - AAA server additions on IOS routers, 131-132
 - traffic identification, 133-140
 - user configuration, 132
 - IOS resilient configuration feature (Cisco), 101-102
 - IPS, 360-361
 - IOS IPS via CLI, 377
 - IOS IPS via SDM, 364-372, 375-376
 - signatures, 378-380
 - IPsec transform sets, 318-319
 - IPsec VPN
 - IKE Phase I, 307-311
 - IKE Phase II, 311-314
 - local AAA on routers, 116, 119
 - enabling/disabling AAA, 118
 - user account configuration, 117
 - verifying configurations, 120

- passwords, 94-97
- port security, 429
 - basic settings, 430
 - optional settings, 430-432
 - violation mode, 431
- SDM, advanced configurations, 111-112
- secure management/
 - reporting time features, NTP, 165
- servers, VoIP, 417
- SNMB, SDM configurations, 159-160
- SSH daemons, 161-164
- user accounts, local
 - AAA configuration on routers, 117
- ZPF manually via
 - SDM, 233
 - class map
 - creation, 235
 - policy map creation, 236
 - zone creation, 234
 - zone pair
 - creation, 237
- ZPF via Basic Firewall Wizard (SDM), 224-233
- console line interfaces, 93**
- console passwords, 94**
- covert channel attacks, 37**
- crackers, 31**
- criminal law, prosecuting computer crimes, 27**
- CRL (Certificate Revocation Lists), 280**
- cross-certified CA (Certificate Authorities), 279**
- cryptanalysis, defining, 246**

crypto ACL (Access Control Lists)

- Step-by-Step Setup mode (Site-to-Site VPN Wizard), defining in, 333-334
- traffic-defining ACL, creating in IPsec VPN, 319-320
- verifying, 325

crypto ipsec transform-set command, 319

crypto isakmp key command, 317

crypto isakmp policy command, 316

crypto map command, 321

crypto maps, site-to-site IPsec VPN, 320

cryptographic hashing algorithms, 256, 268

- HMAC, 270-272
- MD5, 269-271
- SHA-1, 269, 272

cryptographic keys. *See* encryption keys

cryptography

- asymmetric key encryption algorithms, 251, 275
 - authentication
 - via, 277
 - length of, 253
 - private key
 - algorithms, 276
 - public key
 - algorithms, 276
 - speed of, 253
 - trusted
 - algorithms, 255
 - types of, 253
- birthday attacks, 250
- block ciphers, 254, 263

- brute force attacks, 249
- chosen-ciphertext attacks, 250
- chosen-plaintext attacks, 250
- ciphertext-only attacks, 249
- cryptographic hashing algorithms, 256, 268
 - HMAC, 270-272
 - MD5, 269-271
 - SHA-1, 269, 272
- defining, 246
- digital signatures
 - DSS, 275
 - process example, 274
 - uses for, 272
- ECC, 256
- encryption algorithms
 - desirable features
 - of, 251
 - selection criteria, 255
- encryption keys
 - keyspaces, 257-258
 - lengths of, 258
 - managing, 256-257
- known-plaintext attacks, 249
- MiM attacks, 250
- SSL VPN, 259-260
- stream ciphers, 254-255, 263
- symmetric key encryption algorithms, 251, 261
 - 3DES, 264-265
 - AES, 253-255, 265-266
 - DES, 263
 - DH, 255
 - key length, 262
 - RC, 267

- SEAL, 266
- trusted
 - algorithms, 255
 - types of, 252
- web resources, 505

cryptography

- defining, 246
- example of, 247

cryptosystems, defining, 246-247**CSA (Cisco Security Agent)**

- buffer overflows, 400
- Configuration
 - Interceptor, 406
- endpoint protection, 397
- endpoint security, 406
- Execution Space
 - Interceptor, 406
- File System
 - Interceptor, 406
- HIPS, 351-355
- Network
 - Interceptor, 406

CSM (Cisco Security Manager), IPS management, 350**custodian role (data classification), 22****custom mode (CD-ROM), 500****custom threats, rise of, 18****D****data classification**

- age metric, 22
- criteria for, 22
- custodian role, 22
- owner role, 22
- personal association
 - metric, 22
- personnel classification
 - via, 22
- private sector
 - classification, 22

- public sector
 - classification, 21
 - useful life metric, 22
 - user role, 22
 - value metric, 22

data diddling, 39**data integrity, HMAC, 271****Data Link Layer (OSI Layer 2), encryption, 248****data packets, ensuring path integrity, 170****DDOS (Distributed Denial of Service) attacks, 36, 44****debug aaa authentication command, 120, 140-141****debug crypto ipsec command, 322****debug crypto isakmp command, 322****decryption (deciphering), defining, 246****Defense in Depth philosophy, 33-34****Deny Attacker Inline action (IPS attack responses), 348****Deny Connection Inline action (IPS attack responses), 348****Deny Packet Inline action (IPS attack responses), 348****DES (Data Encryption Standard), 250, 263, 304****design, simplicity of, 72****detective type (security controls), 24****deterrent type (security controls), 24****DH (Diffie-Hellman) key exchange algorithm, 255, 276, 305****dial plans (UCM), 414****diddling data, 39****digital signatures**

- DSS, 275
- process example, 274
- uses for, 272

Discovery Protocol (Cisco), disabling, 169**DMVPN (Dynamic Multipoint Virtual Private Networks), 298****DNS (Domain Name System), disabling, 170****DoS (Denial of Service) attacks, 36, 43**

- causes of, 20
- IP-address broadcasts,
 - disabling, 172
- terminal access security,
 - ensuring, 171
- VoIP, 413

double-tagging (VLAN hopping), 424-425**drop action (ZPF), 221****DRP (Disaster Recovery Procedures)**

- categories of
 - disruption, 60
- phases of, 59

DSA (Digital Signature Algorithm), 275-276**DSS (Digital Signature Standard), 275****dual operator control (SoD operations security principle), 55****due care (liability), 28****due diligence (liability), 28****dumpster diving, 37****dynamic packet-filtering firewalls, 196-198**

E

Easy VPN (Virtual Private Networks), 298-299

eavesdropping attacks, VoIP, 414

ECB (Electronic Code Block) mode, block ciphers, 263

ECC (Elliptic Curve Cryptography), 256

ECDSA (Elliptic Curves Digital Signature Algorithm), 275

Economic Espionage Act of 1996, 29

education, best practices against network attacks, 45

electrical power attacks, 44

ElGamal, 276

Elliptic Curve, 276

email, digital signatures, 273

emanation capturing, 37

enable passwords, 95

enable view command, 101

encryption (enciphering), 248

3DES, VPN, 304

AES, 253-255, 304

Application Layer (OSI Layers 5-7), 249

asymmetric key encryption algorithms, 251, 275

authentication via, 277

length of, 253

private key algorithms, 276

public key algorithms, 276

speed of, 253

trusted algorithms, 255

types of, 253

best practices against network attacks, 46

cryptographic hashing algorithms, 256, 268

HMAC, 270-272

MD5, 269-271

SHA-1, 269, 272

Data Link Layer (OSI Layer 2), 248

defining, 246

DES, VPN, 304

DH, 255, 305

digital signatures

DSS, 275

process example, 274

uses for, 272

ECC, 256

encryption algorithms

block ciphers, 254, 263

desirable features of, 251

encryption keys with, 251

selection criteria, 255

stream ciphers, 254-255, 263

encryption keys, 248

distributing, 252

encryption algorithms with, 251

keyspaces, 257-258

lengths of, 258

managing, 256-257

hardware-accelerated encryption, 300

Network Layer (OSI Layer 3), 249

RSA, VPN, 305

SEAL, VPN, 305

service password encryption, 95

site-to-site IPsec VPN, 303-305

symmetric key encryption algorithms, 251, 261

3DES, 264-265

AES, 253-255, 265-266

DES, 263

DH, 255

key length, 262

RC, 267

SEAL, 266

trusted algorithms, 255

types of, 252

Transport Layer (OSI Layer 4), 249

encryption keys, DH key exchanges, 305

end systems, 396

end-user policies, 65

endpoint protection (Cisco Security Agent), 397

endpoint security

best practices, 407

buffer overflows, 399-400

CSA, 397, 406

IronPort, 403

NAC, 397, 403-405

NIC, 397

Trojan horses, 399-402

viruses, 399-401

VoIP, 417

worms, 399-402

ENGINE_BUILDING messages, IPS, 373

ENGINE_BUILDS_STARTED messages, IPS, 373

ENGINE_READY messages, IPS, 373

entrapment, defining, 27

environmental control, best practices against network attacks, 46

ESP (Encapsulating Security Payloads), IKE Phase II, 313-314**ethics, prosecuting computer crimes, 27****exams (certification)**

- exam cram usage strategies, 12
- self-assessment, 5-9
- topics of, 10-11

exams (practice)

- exam 1
 - answers, 461-469
 - questions, 444-455, 458-460
- exam 2
 - answers, 487-496
 - questions, 472-485
- MeasureUp, 500-501
- tips for taking, 443, 471

exchange one (IKE Phase I main mode exchanges), 310**exchange two (IKE Phase I main mode exchanges), 310-311****exec authentication policies, creating, 136****Exec banner messages, 104****exec-timeout command, 96****Execution Space Interceptor (CSA), 406****exploits, defining, 30****external AAA (Authentication, Authorization and Accounting), router configuration via Secure ACS, 115-116, 122, 127**

- AAA client additions, 129-130
- AAA network configuration, 129-132

- traffic identification, 133-140
- user configuration, 132

external threats

- examples of, 16
- protecting against, 17

F

FAC (Forced Authorization Codes), UCM, 414**false negative signature alarms, 359****false positive signature alarms, 359****FCIP (Fiber Channel over IP), SAN, 408****Federal Information Security Management Act of 2002 (FISMA), 29****Fiber Channel (SAN), 408****File System Interceptor (CSA), 406****Finger service, disabling, 170****FIPS 197, Advanced Encryption Standard (AES) website, 505****Firewall and ACL Wizard (SDM), 110****firewalls**

- advantages of, 189
- application inspection firewalls, 199-200
- application layer gateways, 194-195
- Basic Firewall Wizard (SDM), ZPF configuration via, 224-233
- best practices, 202
- characteristics of, 189
- Cisco ASA 5500 Series Adaptive Security appliances, 202

Cisco IOS firewalls, 201**Cisco PIX 500 Series firewalls, 201****Cisco Self-Defending Networks, role in, 190****defining, 188****disadvantages of, 190****dynamic packet-filtering firewalls, 196-198****layered defense strategies, role in, 190****perimeters, defining, 188****static packet-filtering firewalls, 191-192****advantages of, 193****creating via ACL, 204-217****disadvantages of, 194****transparent firewalls, 200****VAC+, 300****VoIP, 415-416****ZPF, 218****ACL, 220****actions of, 221****advantages of, 220****configuration overview, 219****configuring manually via SDM, 233-237****configuring via Basic Firewall Wizard (SDM), 224-233****features of, 221****monitoring, 238-240****zone behavior in, 221-223****FISMA (Federal Information Security Management Act of 2002), 29**

five P's of worm attacks, 402

flash file system (routers), required SDM operation files, 106-107

fraud

- Theft and Toll Fraud, VoIP, 414

- UCM protection features, 414

- vishing attacks, VoIP, 414

FTP servers, disabling, 169

G - H

GARP (Gratuitous Address Resolution Protocol), disabling, 171

gatekeepers, VoIP, 411

gateways, VoIP, 412

GLBA (Gramm-leach-Bliley Act of 1999), 28

governing policies, 64

gray hat hackers, 31

guidelines (network security policies), 66

H.323 protocol, 412

hackers

- custom threats, rise of, 18

- motivations of, 31

- specializations of, 31

- thought process of, 32

- types of, 31

Hacking Exposed, 5th Edition, 504

hacktivists, 31

HAGLE (Hash, Authentication, Group, Lifetime, Encryption) memory aid, 308, 328

Handbook of Applied Cryptography, 505

hard zoning, SAN, 410

hardware, best practices against network attacks, 46

hardware-accelerated encryption, 300

hashing algorithms, 256, 268

- HMAC, 270-272

- MD5, 269-271

- SHA-1, 269, 272

- site-to-site IPsec VPN, 305

headers, TCP segment headers, 196

Health Insurance Portability and Accountability Act of 2000 (HIPAA), 28

help, technical support, 502

hierarchical CA topology, 279

high security level (signature alarms), 360

HIPAA (Health Insurance Portability and Accountability Act of 2000), 28

HIPS (host-based Intrusion Protection Systems), 351-355

HMAC (Hashed Message Authentication Code), 270-272, 305

hobby hackers, 31

honey pots, defining, 347

hopping attacks (VLAN), 422

- double-tagging, 424-425

- rogue trunks, 423-424

hot (mirror) sites, backups, 61

HTTP (Hypertext Transfer Protocol), disabling configuration/monitoring service, 170

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer), disabling configuration/monitoring service, 170

I

ICMP (Internet Control Message Protocol)

- ACL, filtering via, 216-217

- floods, 43

- mask replies, disabling, 171

- redirects, 170

- unreachable notifications, disabling, 171

IDENT (IP Identification) service, disabling, 171

identity theft, 38

IDM (IPS (Device Manager), IPS management, 350

IDS (Intrusion Detection Systems)

- categories of, 343-344

- custom threats, handling, 18

- IPS versus, 342, 345-346

- sensor types, 346-347

- signatures

- alarms, 359-360

- micro-engines, 357-358

IEV (IPS Event Viewer), IPS management, 350-351

IKE (Internet Key Exchange)

IPsec VPN

configuration

Phase I, 307-311,
316-318

Phase II, 311-314

Phase I, 307-311

ISAKMP policy sets,
316-318

ISAKMP SA verification,
324

main mode
exchanges,
310-311

Phase II, 311

AH, 312-313

ESP, 313-314

SA verification,
322-324

Step-by-Step Setup
mode (Site-to-Site
VPN Wizard),
defining proposals in,
331-332

implementation, simplicity of, 72**in-band administrative access (routers). *See* remote administrative access (routers)****in-band interfaces, 93****in-band traffic, 152****inbound IP address spoofing, 204, 213-214****incident response**

chain of custody, 26
complications in, 26
investigations, 25

Incoming banner messages, 104**informational security level (signature alarms), 360*****Inside Internal Security, What Hackers Don't Want You to Know, 504*****inspect action (ZPF), 221****installing**

CD-ROM, 500-501

Secure ACS, Windows
requirements, 124

integrity, site-to-site VPN, 294, 303-305**Integrity (CIA triad), 19-20****integrity attacks**

data diddling, 39

password attacks, 39

port redirection
attacks, 40

salami attacks, 39

session hijacking, 39

trust exploits, 39

interactive mode (Cisco AutoSecure feature), 177**Interface and Connection Wizard (SDM), 110****interface command, 99****interfaces**

GARP, disabling, 171

in-band interfaces, 93

line interfaces

auxiliary line
interfaces, 93

console line
interfaces, 93

reviewing, 92-93

virtual line
interfaces, 93

out-of-band
interfaces, 93

router interfaces,
disabling, 168

vulnerable interfaces,
disabling, 167-169

vulnerabilities, 167

intermediate systems, 396**internal threats**

best practices against, 17

examples of, 16

seriousness of, 17

Internet Denial of Service, Attack and Defense Mechanisms, 504***Introduction to Security Policies, Four-Part Series, 503*****intrusion notification, switch security, 434-435****Intrusion Prevention Wizard (SDM), 111****IOS firewalls (Cisco), 201****IOS IPS (Intrusion Prevention Systems)**

benefits of, 362-363

configuration verification,
384-385

configuring via

CLI, 377

SDM, 364-372,
375-376

feature blend, 362

interface
verification, 386

IPS Policies Wizard,
367-370

IPS Rule Wizard, 367

policy verification, 384

SDEE support,
381, 383

settings verification, 386

signatures

configuring,
378-380

integration, 363

IOS resilient configuration feature (Cisco), 101-102**IOS routers**

deploying, 88-90

DF, 367-369

DMVPN, 298

Easy VPN, 298

IPsec stateful
failover, 298

V3PN, 298

VPN features, 298

IP (Internet Protocol)

- IP-directed broadcasts, disabling, 172
- phones, VoIP, 411
- source routing, 170
- VoIP
 - call policies, 416
 - components of, 411-412
 - DoS attacks, 413
 - eavesdropping attacks, 414
 - endpoint configuration, 417
 - firewalls, 415-416
 - inspecting, 416
 - MIM attacks, 414
 - protocols of, 412
 - rate limits, 416
 - reconnaissance attacks, 413
 - registration, 416
 - security, 415-417
 - server configuration, 417
 - SIP vulnerabilities, 414
 - SPIT, 413
 - standards compliance, 416
 - Theft and Toll Fraud, 414
 - vishing attacks, 414
 - VPN, 416-417
 - VVLAN, 415

IP addresses

- end systems, 396
- FCIP (Fiber Channel over IP), 408
- intermediate systems, 396
- spoofing, 34-35, 204
 - blind attacks, 36
 - inbound, 213-214
 - nonblind attacks, 36
 - outbound, 215

ip ips command, 377**ip ips config location command, 377****ip ips name command, 377****ip ips notify command, 377****ip ips signature-category command, 377****ip verify unicast reverse-path command, 216****ip virtual-reassembly, 377****IPS (Intrusion Prevention Systems)**

- attack responses, 348
- best practices, 360-361
- categories of, 343-344
- Cisco appliances, 356
- configuration verification, 384-385
- configuring, 360-361
- custom threats, handling, 18
- ENGINE_BUILDING messages, 373
- ENGINE_BUILDS_STARTED messages, 373
- ENGINE_READY messages, 373
- event management/monitoring, 349-350
- HIPS, 351-355
- IDS versus, 342, 345-346

- interface verification, 386

IOS IPS

- benefits of, 362
- CLI configuration, 377
- configuration verification, 384-385
- feature blend, 362
- interface verification, 386

- policy verification, 384
- SDEE support, 381-383
- SDM configuration, 364-372, 375-376
- settings verification, 386
- signature configuration, 378-380
- signature integration, 363
- IPS Policies Wizard, 367-370
- IPS Rule Wizard, 367
- network IPS, 354-355
- policy verification, 384
- SDEE support, 381, 383
- sensor types, 346-347
- settings verification, 386
- signatures
 - alarms, 359-360
 - configuring, 378-380
- IOS IPS integration, 363
- micro-engines, 357-358

IPS Policies Wizard, 367-370**IPS Rule Wizard, 367****IPsec (Internet Protocol Security)**

- crypto maps, site-to-site IPsec VPN, 320
- stateful failover, 298
- strengths of, 307
- transform sets, 329
 - configuring, 318-319
- Step-by-Step Setup mode (Site-to-Site VPN Wizard), defining in, 332-333
- verifying, 322

transport mode, 314

tunnel mode, 314

IPsec VPN (Internet Protocol Security over Virtual Private Networks)

AES, 255

Certicom client, 300

certificate-based

authentication, 283

configuring

IKE Phase I,

307-311

IKE Phase II,

311-314

DH, 255

IPsec VPN SPA, 300

PKI, 280

site-to-site VPN

anti-replay, 303

authentication,

303, 306

CLI implementa-

tion, 315-325

confidentiality,

302-305

DH key

exchanges, 305

integrity, 303-305

SDM implementa-

tion, 325-326,

329-336

SSL VPN versus,

301-302

IPsec VPN SPA (Shared Port Adapters), 300

IronPort, endpoint security, 403

ISAKMP (IKE Phase I)

policy sets, IPsec VPN

implementation via

CLI, 316-318

SA verification, 324

iSCSI (SCSI over TCP/IP), SAN, 408

ISR (Integrated Service Routers), 80, 90

J - K - L

keepalives (TCP), disabling, 171

keys (encryption), DH key exchanges, 305

keyspaces (encryption keys), 257-258

known-plaintext attacks, 249

law, prosecuting computer crimes

administrative law, 27

civil law, 27

complications in, 26

criminal law, 27

ethics, 27

investigations, 25

liability, 28

U.S. government
regulations, 28-29

layer 2 security

best practices, 438

CAM table overflow
attacks, 428-429

intrusion notification,
434-435

MAC address spoofing
attacks, 429

port security, 429

basic settings, 430

optional settings,
430-432

verification, 433-434

violation mode con-
figuration, 431

SPAN, 435

storm control, 436-437

STP manipulation
attacks, 425

BPDU Guard,
427-428

portfast mode,
426-427

root guard, 428

VLAN hopping
attacks, 422

double-tagging,
424-425

rogue trunks,
423-424

layered defense strategies, firewalls role in, 190

least privilege, concept of, 72

liability, prosecuting computer crimes, 28

line interfaces

auxiliary line
interfaces, 93

console line
interfaces, 93

reviewing, 92-93

virtual line
interfaces, 93

local AAA (Authentication, Authorization and Accounting), 115

router configuration,
116, 119-120

enabling/disabling
AAA, 118

user account config-
uration, 117

verifying configura-
tions, 120

troubleshooting,
140-141

local administrative access (routers), 91

banner messages, 104

CLI role-based access
configuration, 98-100

IOS resilient configura-
tion feature (Cisco),
101-102

line interfaces, 92-93

passwords

best practices, 94

configuring, 94-97

- console
 - passwords, 94
- enable passwords, 95
- minimum length
 - configuration, 96
- recovering, 97
- secret passwords, 95
- service password
 - encryption, 95
- timeouts, 96
- username security, 96
- virtual terminal passwords, 95
- privilege levels,
 - setting, 97
- view creation, 98-100
- virtual login security,
 - 102-103

Log Attacker Packets action (IPS attack responses), 348

Log Pair Packets action (IPS attack responses), 348

Log Victim Packets action (IPS attack responses), 348

logs

- authentication policies,
 - creating, 134-135
- banner messages, 104
- configuration verification, 103
- Syslog login detection
 - messages,
 - generating, 103
- virtual login security,
 - 102-103

logs

- how to log, 150
- messages
 - formats of, 156
 - security levels, 155
 - sending, 154-155
- what to log, determining, 149-150

low security level (signature alarms), 360

LUN (Logical Unit Numbers), 408

M

MAC addresses

- spoofing attacks, 429
- sticky learning, 432

MAC floods, 45

mac-address-table notification command, 435

main mode exchanges (IKE Phase I), 310-311

maps, ZPF configurations

- class maps, 235
- policy maps, 236

MARS (Monitoring, Analysis, and Response System), 78, 154, 350

mask replies (ICMP), disabling, 171

MCU (Multipoint Control Units), VoIP, 412

MD5 (Message Digest 5), 269, 271, 305

means (computer crime investigations), 25

MeasureUp practice tests, 500-501

medium security level (signature alarms), 360

memory, CAM table overflow attacks, 428

message logs, viewing

- SDEE logs, 382
- Syslog logs, 383

message tampering, SIP, 414

MGCP (Media Gateway Control Protocol), 412

MiM (Man-in-the-Middle) attacks, 36, 250, 414

mirror (hot) site backups, 61

Monitor mode (SDM), 110, 113

MOP (Maintenance Operation Protocol), disabling, 169

MOTD (Message-Of-The-Day) banner messages, 104

motive (computer crime investigations), 25

multi-string signatures, 358

multicast traffic, bandwidth limitations, 437

N

NAA (NAC Application Agent), 404

NAC (Network Admission Control), 397

- endpoint security,
 - 403-405

- NAA, 404

- NAC Appliance, 404

- NAC Framework, 403

- NAM, 404

- NAS, 404

- rule-set updates, 404

NAC Wizard (SDM), 111

NAM (NAC Application Manager), 404

named ACL (Access Control Lists), 205

NAS (Network Access Servers), 115, 404

NAT Wizard (SDM), 111

navigation bar (Secure ACS), 127, 130

network attacks

- availability attacks, 42
- botnets, 43
- computer environment attacks, 44
- DDoS attacks, 44
- DoS attacks, 43
- electrical power attacks, 44
- ICMP floods, 43
- MAC floods, 45
- physical environment attacks, 44
- SYN floods, 44
- best practices against
 - administrative controls, 45
 - education, 45
 - encryption, 46
 - environmental control, 46
 - hardware, 46
 - passwords, 46
 - patches, 45
 - physical access, 46
 - physical controls, 46
 - security policies, 45
 - TCP ports, 46
 - technical controls, 46
 - UDP ports, 46
 - unnecessary services, 46
- confidentiality attacks, 36
 - covert channel attacks, 37
 - dumpster diving, 37
 - emanation capturing, 37
 - identity theft, 38
 - overt channel attacks, 37

- packet sniffing (protocol analysis) attacks, 37
- pharming attacks, 38
- phishing attacks, 38
- ping sweeps, 37
- port scanning attacks, 37
- protocol analysis (packet sniffing) attacks, 37
- social engineering attacks, 37
- DDOS attacks, 36
- Defense in Depth philosophy, 33-34
- DoS attacks, 36
- exploits, defining, 30
- external threats
 - examples of, 16
 - protecting against, 17
- hackers
 - motivations of, 31
 - specializations of, 31
 - thought process of, 32
 - types of, 31
- integrity attacks
 - data diddling, 39
 - password attacks, 39
 - port redirection attacks, 40
 - salami attacks, 39
 - session hijacking, 39
 - trust exploits, 39
- internal threats
 - best practices against, 17
 - examples of, 16
 - seriousness of, 17
- IP spoofing, 34-36
- MiM attacks, 36
- risks, defining, 30

- seven steps for compromising targets and applications, 32
- vulnerabilities, categories of, 30

network authentication policies, creating, 138**Network Configuration page (Secure ACS)**

- AAA Client Hostname field, 130
- AAA Client IP Address field, 130
- accessing, 130
- Authentication Using drop-down list, 131
- Shared Secret field, 130

Network Interceptor (CSA), 406**network IPS (Intrusion Protection Systems), 354-355****Network Layer (OSI Layer 3), encryption, 249****network probes, disabling, 170****network scans, disabling, 170****network security**

- perimeters, determining, 73-74
- policies
 - assets, defining, 62
 - AUP, 64
 - end-user policies, 65
 - governing policies, 64
 - guidelines, 66
 - principles of, 70-72
 - procedures, 66
 - reasons for having, 63
 - responsibility for, 66
 - RFC 2196, 61-62
 - risk management, 67-69

SDLC, 62
standards, 66
technical policies, 65
web resources, 503

practices, web
resources, 504

scanners, 56
Nmap, 57
SuperScan, 57-58

Self-Defending
Networks
collaborative sys-
tems, 75
integrated security
portfolio, 79-80
Operational Control
and Policy
Management com-
ponent, 76-78
principles of, 75
Secure
Communications
component, 76-77
Secure Network
Platform compo-
nent, 76
Threat Control and
Containment com-
ponent, 76-77

sensors, 56

testing
techniques, 55-56
tools list, 56

**network services, filtering
ACL via, 212**

**NIC (Network Infection
Containment), 397**

Nmap, features of, 57

**no aaa new-model com-
mand, 119**

**no service password-recov-
ery command, 97**

**non-interactive mode (Cisco
AutoSecure feature), 177**

**nonblind spoofing
attacks, 36**

**notifications (intrusion),
switch security, 434-435**

**NTP (Network Time
Protocol)**
disabling, 169
secure management/
reporting time fea-
tures, configuring, 165

**numbered ACL (Access
Control Lists), 205**

O

**OFB (Output Feedback)
mode, stream ciphers,
263**

off-site backup facilities, 61

**One-Step Lockdown feature
(Security Audit Wizard),
172, 176**

**OOB (Out-Of-Band)
traffic, 152**

**Operational Control and
Policy Management com-
ponent (Self-Defending
Networks), 76-78**

operations security
BCP, phases of, 59-60
Change and
Configuration
Controls principle, 54
DRP
categories of disrup-
tion, 60
phases of, 59
network security
Nmap, 57
scanners, 56
sensors, 56
SuperScan, 57-58
testing techniques,
55-56
testing tools list, 56

Rotation of Duties
principle, 54
SDLC, 52
SoD principle, 54-55
Trusted Recovery prin-
ciple, 54

**opportunity (computer
crime investigations), 25**

**origin authentication,
19, 271**

**OS (operating systems),
software security, 397-398**

**OSI application layer, view-
ing certificates at, 285**

out-of-band interfaces, 93

**outbound IP address spoof-
ing, 204, 215**

overt channel attacks, 37

**owner role (data classifica-
tion), 22**

P

packets (data)
packet sniffing
(protocol analysis)
attacks, 37
path integrity, 170

**parser view feature, view
creation, 98-100**

partitioning (UCM), 414

pass action (ZPF), 221

passwords
attacks, 39
best practices, 94
best practices against
network attacks, 46
configuring, 94-97
console passwords, 94
enable passwords, 95
minimum length, con-
figuring, 96
recovering, 97

passwords

- secret passwords, 95
- service password encryption, 95
- timeouts, setting, 96
- username security, 96
- virtual terminal passwords, 95

patches, best practices against network attacks, 45

path integrity, ensuring, 170

Perform Security Audit button (Security Audit Wizard), 173

perimeters (network security)

- defining, 188
- determining, 73-74

personal association metric (data classification), 22

pharming attacks, 38

phishing attacks, 38

phone phreaks, 31

phreakers, 31

physical access, best practices against network attacks, 46

physical controls, 23-24, 46

physical environment, attacks on, 44

ping sweeps, 37

PIX 500 Series firewalls (Cisco), 201

PKCS (Public Key Cryptography Standards), PKI, 281

PKI (Public-Key Infrastructures)

- areas of, 278
- CA
 - central (single-root) CA topology, 279
 - CRL, 280

- cross-certified CA, 279
- defining, 277
- hierarchical CA topology, 279
- certificates, 279
 - authentication via, 283-284
 - defining, 277
 - enrollment process, 282-283
 - issuing, 283
 - retrieving, 283
 - uses of, 285
 - viewing at OSI application layer, 285

- defining, 277
- encryption key management, 257
- IPsec VPN, 280
- PKCS, 281
- RA, offloading tasks to, 280
- SCEP, 281
- usage keys, 279
- X.509 v3 standard, 281

plaintext (cleartext)

- chosen-plaintext attacks, 250
- defining, 246
- known-plaintext attacks, 249

policies

- best practices against network attacks, 45
- end-user policies, 65
- governing policies, 64
- network security
 - assets, defining, 62
 - AUP, 64
 - end-user policies, 65
 - governing policies, 64
 - guidelines, 66

- principles of, 70-72
- procedures, 66
- reasons for having, 63
- responsibility for, 66
- RFC 2196, 61-62
- risk management, 67-69
- SDLC, 62
- standards, 66
- technical policies, 65
- web resources, 503
- technical policies, 65

policy maps, ZPF configurations, 236

policy sets

- ISAKMP (IKE Phase I) policy sets, IPsec VPN implementation via CLI, 316-318
- transform sets versus, 311
- VPN, 310

port security

- CAM table overflow attacks, mitigating, 429
- configuring, 429
 - basic settings, 430
 - optional settings, 430-432
- MAC address spoofing attacks, mitigating, 429
- show port-security address command, 434
- show port-security command, 433
- show port-security interface command, 433-434
- switchport port-security aging command, 432
- switchport port-security mac-address command, 432

switchport port-security maximum command, 431

verifying, 433-434

violation mode, configuring, 431

portfast mode, mitigating STP manipulation attacks, 426-427

ports

redirection attacks, 40

scanning attacks, 37

TCP ports, best practices against network attacks, 46

UDP ports, best practices against network attacks, 46

practice exams

exam 1

answers, 461-469

questions, 444-455, 458-460

exam 2

answers, 487-496

questions, 472-485

MeasureUp, 500-501

tips for taking, 443, 471

preventative type (security controls), 24

Privacy Act of 1974, 29

private data classification level, 22

private key encryption algorithms, 276

private sector data classification, 22

privilege levels (administrative access), setting, 97

privilege, concept of least, 72

probes (network), disabling, 170

procedures (network security policies), 66

Produce Alert action (IPS attack responses), 348

Produce Verbose Alert action (IPS attack responses), 348

prosecuting computer crimes

administrative law, 27

civil law, 27

complications in, 26

criminal law, 27

ethics, 27

investigations, 25

liability, 28

U.S. government regulations, 28-29

protocol analysis (packet sniffing) attacks, 37

Proxy ARP (Address Resolution Protocol), disabling, 172

PSK (Pre-Shared Keys), site-to-site IPsec VPN, 306

public data classification level, 22

public key encryption algorithms, 276

public sector data classification, 21

PVST+ (Per VLAN Spanning Tree Plus), 426

Q - R

qualitative risk analysis, 67

Quality of Service Wizard (SDM), 111

quantitative risk analysis, 67, 69

questions (practice exams)

exam 1, 444-455, 458-460

exam 2, 472-485

Quick Setup mode (Site-to-Site VPN Wizard), 325-326, 329

quiet mode (virtual login security), 102

RA (Registration Authorities), offloading PKI tasks to, 280

RADIUS (Remote Dial-In User Services)

AAA implementation, 125, 129-130

default port numbers for, 126

TACACS+ versus, 125-126

troubleshooting, 140-141

rate limits, VoIP, 416

RBAC (Role-Based Access Controls), creating, 78

RC (Rivest Ciphers), 267

reconnaissance attacks, VoIP, 413

recovery, passwords, 97

redirection attacks (ports), 40

Refresh mode (SDM), 110

registration

hacks, SIP, 414

VoIP, 416

remote administrative access (routers), 91

auxiliary line interfaces, 93

banner messages, 104

CLI role-based access configuration, 98-100

remote administrative access (routers)

console line
interfaces, 93

IOS resilient configuration feature (Cisco),
101-102

passwords

best practices, 94

configuring, 94-97

console
passwords, 94

enable passwords, 95

minimum length
configuration, 96

recovering, 97

secret passwords, 95

service password
encryption, 95

timeouts, 96

username security, 96

virtual passwords, 95

privilege levels,
setting, 97

reviewing, 92-93

view creation, 98-100

virtual line
interfaces, 93

virtual login security,
102-103

**remote user network
access, AAA, 115**

**remote-access VPN (Virtual
Private Networks), 295**

Cisco product position-
ing, 297-298

Easy VPN, 298-299

VPN 3002 Hardware
Client, 300

Web VPN, 299

**Request Block Connection
action (IPS attack
responses), 348**

**Request Block Host action
(IPS attack responses),
348**

**Request SNMP Trap action
(IPS attack responses), 348**

**Reset TCP Connection
action (IPS attack
responses), 348**

resources (web)

cryptography, 505

network security

policies, 503

practices, 504

**RFC (Request for Comment)
2196, network security
policies, 61-62**

risks

analyzing, 67-69

avoidance, 69

defining, 30

managing, 67-69

**rogue trunks (VLAN hop-
ping), 423-424**

**ROMMON (ROM Monitor)
mode, password
recovery, 97**

**root guard, mitigating STP
manipulation attacks, 428**

**Rotation of Duties opera-
tions security principle, 54**

**Router Security Strategies,
Security IP Network Traffic
Planes, 504**

router services

vulnerable services, dis-
abling, 167

commonly config-
ured management
services, 169-170

unnecessary services,
168-169

vulnerabilities of, 167

routers

administrative access, 91

auxiliary line inter-
faces, 93

banner messages, 104

CLI role-based
access configura-
tion, 98-100

console line inter-
faces, 93

console passwords, 94

enable passwords, 95

IOS resilient config-
uration feature
(Cisco), 101-102

minimum password
length configura-
tion, 96

password best
practices, 94

password configura-
tion, 94-97

password recovery, 97

privilege levels, 97

reviewing line inter-
faces, 92-93

secret passwords, 95

service password
encryption, 95

timeouts, 96

username security, 96

view creation,
98-100

virtual line inter-
faces, 93

virtual login security,
102-103

virtual passwords, 95

AIM-VPN, 300

ASR, web resources, 90

Cisco AutoSecure
feature, 177-178

flash file system,
required SDM opera-
tion files, 106-107

interfaces, disabling, 168

IOS routers

deploying, 88-90

DMVPN, 298

Easy VPN, 298

IPsec stateful
failover, 298

- SDF, 367-369
- V3PN, 298
- VPN features, 298
- IPsec VPN SPA, 300
- ISR, 80, 90
- path integrity, ensuring, 170
- Proxy ARP, disabling, 172
- SDM
 - launching, 108
 - required operation files, 106-107
- SDM Express, 107
- “self” zones, 223
- service traffic, filtering via ACL, 217
- timeouts, setting, 96
- traffic destined to, ZPF zone behavior, 223
- traffic flowing through, ZPF zone behavior, 222
- traffic originating from, ZPF zone behavior, 223

Routing Wizard (SDM), 111

RSA (Rivest, Shamir and Adleman) encryption algorithm, 275-276, 305-306

RTCP (RTP Control Protocol), 413

RTP (Real-Time Transport Protocol), 412

rule-set updates (NAC), 404

S

SA (Security Associations), verifying

- IKE Phase II SA, 322-324
- ISAKMP (IKE Phase I) SA, 324

SAFE (Security and Freedom Through Encryption Act of 1997), 29

salami attacks, 39

SAN (Storage Area Networks)

- advantages of, 407
- FCIP (Fiber Channel over IP), 408
- Fiber Channel, 408
- iSCSI (SCSI over TCP/IP), 408
- LUN, 408
- security storages, 409
- VSAN, 409
- WWN, 409
- zoning, 410

Sarbanes-Oxley Act of 2002 (SOX), 29

Save mode (SDM), 110

SBU (Sensitive but Unclassified) data classification level, 21

scanners, 56

- Nmap, features of, 57
- SuperScan, features of, 57-58

scans (network), disabling, 170

SCCP (Skinny Client Control Protocol), 413

SCEP (Simple Certificate Enrollment Protocol), PKI, 281

script kiddies, 31

SCSI (Small Computer Systems Interface), 408

SDEE (Security Device Event Exchange)

- IOS IPS support for, 381-383
- message log, viewing, 382

SDF (Signature Definition Files), 367-369

SDLC (System Development Life Cycle), 52, 62

SDM (Security Device Manager), 105

AAA

- enabling/disabling, 119
- router configuration, 120

ACL configuration, 209-211

Add AAA Server dialog, 131

Add Server window, Server IP or Host field, 131

Additional Tasks menu, 111-112

advanced configurations, 111-112

authentication methods, applying, 135

Basic Firewall Wizard, ZPF configuration, 224-233

browser software requirements, 108

Configure mode, 110

files required for operation from router, 106-107

Firewall and ACL Wizard, 110

Interface and Connection Wizard, 110

Intrusion Prevention Wizard, 111

IOS IPS configuration, 364-372, 375-376

IPS management, 350

IPS Policies Wizard, 367-370

IPS Rule Wizard, 367

IPsec implementation
on site-to-site VPN

Quick Setup mode
(Site-to-Site
VPN Wizard),
325-326, 329

Step-by-Step Setup
mode (Site-to-Site
VPN Wizard),
329-336

launching, 108

Monitor mode,
110, 113

NAC Wizard, 111

NAT Wizard, 111

Quality of Service
Wizard, 111

Refresh mode, 110

Routing Wizard, 111

Save mode, 110

Security Audit
Wizard, 111

Cisco AutoSecure
feature versus,
178-179

One-Step
Lockdown feature,
172, 176

Perform Security
Audit button, 173

Security Audit
Interface
Configuration
page, 174

Security Audit
report window,
174-175

smart wizards, list of,
110-111

SNMB, configuring,
159-160

SSH daemon configu-
ration, 162-164

Syslog logging,
enabling, 156-157

user accounts, configu-
ring via, 117

VPN Wizard, 110

web resources, 106

ZPF

configuring manual-
ly, 233-237

monitoring, 238-240

SDM Express, 107

**SEAL (Software Encryption
Algorithm), 266, 305**

**secret data classification
level, 21**

secret passwords, 95

**Secure ACS (Access Control
Servers)**

browser support for, 127

external AAA router
configuration,
122, 127

AAA client addi-
tions, 129-130

AAA network confi-
guration, 129-132

traffic identification,
133-140

user configura-
tion, 132

features of, 123

navigation bar, 127, 130

Network Configuration
page

AAA Client
Hostname
field, 130

AAA Client IP
Address field, 130

accessing, 130

Authentication
Using drop-down
list, 131

Shared Secret
field, 130

prerequisites for,
126-127

reasons for using, 123

solution engine versus
Secure ACS
Express, 125

Windows installation
requirements, 124

Secure ACS Express, 125

**secure boot-config
command, 101**

**Secure Communications
component (Self-
Defending Networks),
76-77**

**secure management/
reporting, 148**

guidelines for, 153

logs

determining what to
log, 149-150

how to log, 150

message formats, 156

security levels, 155

sending messages,
154-155

MARS, 154

reference architecture
for, 151-152

SNMP, 157

architecture of, 158

community
strings, 158

SDM configuration,
159-160

security levels,
158-159

security models,
158-159

trap receivers, 160

versions of, 158

SSH daemons, config-
uring, 161-164

Syslog, 153-157

time feature configura-
tion, NTP, 165

Secure Network Platform component (Self-Defending Networks), 76

Security and Freedom Through Encryption Act of 1997 (SAFE), 29

Security Audit Interface Configuration page (Security Audit Wizard), 174

Security Audit report window (Security Audit Wizard), 174-175

Security Audit Wizard (SDM), 111

Cisco AutoSecure feature versu, 178-179

One-Step Lockdown feature, 172, 176

Perform Security Audit button, 173

Security Audit Interface Configuration page, 174

Security Audit report window, 174-175

security controls

administrative controls, 23

detective type, 24

deterrent type, 24

physical controls, 23-24

preventative type, 24

technical controls, 23

Security Manager (Cisco), 78

Security MARS (Cisco). *See* MARS

security passwords min-length command, 96

security policies

assets, defining, 62

AUP, 64

best practices against network attacks, 45

end-user policies, 65

governing policies, 64

guidelines, 66

principles of, 70

concept of least privilege, 72

design simplicity, 72

implementation simplicity, 72

realistic

assumptions, 71

security awareness, 72

procedures, 66

reasons for having, 63

responsibility for, 66

RFC 2196, 61-62

risk management, 67-69

SDLC, 62

standards, 66

technical policies, 65

segment hearers (TCP), 196

“self” zones (routers), 223

self-assessment (certification exams), 5-9

self-contained AAA. *See* local AAA

Self-Defending Networks

collaborative systems, 75

firewalls role in, 190

integrated security portfolio, 79-80

Operational Control and Policy Management component, 76-78

principles of, 75

Secure Communications component, 76-77

Secure Network Platform component, 76

Threat Control and Containment component, 76-77

sensitive data classification level, 22

sensors, 56

SEP-E (Scalable Encryption Processor-Enhanced), 300

Server IP or Host field (SDM Add Server window), 131

servers

FTP servers, disabling, 169

NAS, 115

TFTP servers, disabling, 169

VoIP configuration, 417

services

DNS, disabling, 170

HTTP configuration/monitoring service, disabling, 170

HTTPS configuration/monitoring service, disabling, 170

IDENT, disabling, 171

MOP, disabling, 169

NTP, disabling, 169

password encryption, 95-96

router services

disabling vulnerable services, 167-170

vulnerabilities of, 167

signatures, 358

SNMP, disabling, 169

TCP, disabling, 169

UDP, disabling, 169

unnecessary services, best practices against network attacks, 46

session hijacking, 39

session tear-down, SIP, 414

seven steps for compromising targets and applications, 32

SHA-1 (Secure Hashing Algorithm 1), 269, 272, 305

Shared Secret field (Secure ACS Network Configuration page), 130

shortcuts (MeasureUp practice tests), creating, 501

show aaa local user lockout command, 120

show aaa sessions command, 121

show aaa user all command, 121

show access-list 101 command, 214

show access-list command, 322

show crypto ipsec sa command, 322

show crypto ipsec transform-set command, 322

show crypto isakmp policy command, 318, 322

show crypto isakmp sa command, 322

show crypto isakmpsa command, 324

show crypto map command, 321-322

show flash command, 101

show ip interface command, 208

show ip ips all command, 386

show ip ips configuration command, 384-386

show ip ips interfaces command, 386

show ip ips signatures count command, 375-376

show logging command, 157

show login command, 103

show parser view command, 100

show policy-map type inspect zone-pair session command, 238-240

show port-security address command, 434

show port-security command, 433

show port-security interface command, 433-434

show privilege command, 97

show secure bootset command, 102

show version command, SEAL, 266

Signature File and Public Key window (IPS Policies Wizard), 367

signatures

alarms, security levels, 359-360

atomic signatures, 358

IDS

alarms, 359-360

micro-engines, 357-358

IPS

alarms, 359-360

configuring, 378-380

IOS IPS signature integration, 363

micro-engines, 357-358

micro-engines, 357-358

multi-string signatures, 358

service signatures, 358

string signatures, 358

SIP (Session Initiation Protocol), 412-414

Site Security Handbook, RFC 2196, 503

site-to-site VPN (Virtual Private Networks), 294

anti-replay, 303

authentication, 295, 303, 306

Cisco product positioning, 297-298

confidentiality, 294, 302-305

DH key exchanges, 305

DMVPN, 298

integrity, 294, 303-305

IPsec stateful failover, 298

IPsec VPN

anti-replay, 303

authentication, 303, 306

CLI implementation, 315-325

confidentiality, 302-305

integrity, 303-305

SDM implementation, 325-326, 329-336

Site-to-Site VPN Wizard

Quick Setup mode, 325-326, 329

Step-by-Step Setup mode, 329

defining connection settings, 330

defining IKE proposals, 331-332

defining IPsec transform sets, 332-333

defining protected traffic (Crypto ACL), 333-334

reviewing configurations, 334

troubleshooting configurations, 335-336

SLA (Service-Level Agreements), backups, 60

SLIP-PPP (Serial Line Internet Protocol-Point-to-Point Protocol) banner messages, 104

smart wizards (SDM), list of, 110-111

smurf attacks, disabling IP-directed broadcasts, 172

SNMP (Simple Network Management Protocol), 157

architecture of, 158

community strings, 158

disabling, 169

SDM, configuring via, 159-160

security levels, 158-159

security models, 158-159

trap receivers, 160

versions of, 158

social engineering attacks, 37

sockets, components of, 197

SoD (Separation of Duties) operations security principle, 54-55

soft zoning, SAN, 410

software security, 397-398

source routing (IP), 170

SOX (Sarbanes-Oxley Act of 2002), 29

SPAN (Switched Port Analyzers), switch security, 435

SPIT (Spam over Telephony), VoIP, 413

spoofing attacks

IP addresses, 34, 204

blind attacks, 36

inbound, 213-214

nonblind attacks, 36

outbound, 215

MAC addresses, 429

SRTP (Secure RTP), 413

SSH (Secure Shell)

daemons, configuring, 161-164

SSL VPN (Secure Socket Layer Virtual Private Networks), 259-260

AnyConnect VPN Client, 300

client mode, 296

clientless mode, 296

compatibility, 297

disadvantages of, 296

IPsec VPN versus, 301-302

standards (network security policies), 66

standards compliance, VoIP, 416

state tables, 197

stateful failover (IPsec), 298

static packet-filtering firewalls, 191-193

ACL, creating via, 204-217

advantages of, 193

disadvantages of, 194

steganography, 37

Step-by-Step Setup mode (Site-to-Site VPN Wizard), 329

configuration review, 334

connection settings, defining, 330

IKE proposals, defining, 331-332

IPsec transform sets, defining, 332-333

protected traffic (Crypto ACL), defining, 333-334

troubleshooting configurations, 335-336

sticky learning, MAC addresses, 432

storm control, 436-437

STP (spanning tree protocol), manipulation attacks, 425

BPDU Guard, 427-428

portfast mode, 426-427

root guard, 428

stream ciphers, 254-255, 263

strings

community strings, SNMP, 158

signatures, 358

study mode (CD-ROM), 499

Summary window (IPS Policies Wizard), 370

SuperScan, features of, 57-58

switch security

best practices, 438

CAM table overflow attacks, 428-429

intrusion notification, 434-435

MAC address spoofing attacks, 429

port security, 429

basic settings, 430

optional settings, 430-432

verification, 433-434

violation mode configuration, 431

SPAN, 435

storm control, 436-437

STP manipulation attacks, 425

BPDU Guard,
427-428

portfast mode,
426-427

root guard, 428

VLAN hopping
attacks, 422

double-tagging,
424-425

rogue trunks,
423-424

switchport port-security
aging command, 432

switchport port-security
mac-address
command, 432

switchport port-security
maximum command, 431

symmetric key encryption
algorithms, 251, 261

3DES, 264-265

AES, 253-255, 265-266

DES, 263

key length, 262

RC, 267

SEAL, 266

trusted algorithms, 255

types of, 252

SYN floods, 44

Syslog, 153-155

login detection mes-
sages, generating, 103

message log,
viewing, 383

SDM, enabling logging
via, 156-157

**system requirements, CD-
ROM installations, 500**

T

TACACS+ (Terminal Access Control Access Control Server Plus)

AAA implementation,
125, 129-131

RADIUS versus,
125-126

troubleshooting,
140-141

TCP (Transfer Control Protocol)

disabling, 169

keepalives, disabling, 171

segment headers, 196

TCP ports, best practices against network attacks, 46

TCP/IP (Transfer Control Protocol/Internet Protocol)

end systems, 396

intermediate
systems, 396

iSCSI (SCSI over
TCP/IP), 408

technical controls, 23, 46

technical policies, 65

technical support, 502

**TEMPEST U.S. government
standard, 38**

term monitor command, 373

**terminal access security,
ensuring, 171**

**terminal monitor command,
120**

test modes (CD-ROM)

certification mode, 499

custom mode, 500

study mode, 499

tests (certification)

exam cram usage strate-
gies, 12

self-assessment, 5-9

topics of, 10-11

tests (practice)

MeasureUp, 500-501

test 1

answers, 461-469

questions, 444-455,
458-460

test 2

answers, 487-496

questions, 472-485

TFTP servers, disabling, 169

**Theft and Toll Fraud,
VoIP, 414**

**Threat Control and
Containment component
(Self-Defending
Networks), 76-77**

**threat identification (risk
management), 67**

**timeouts, setting in router
lines, 96**

**top secret data classifica-
tion level, 21**

tort law. *See* civil law

traffic

external AAA router
configuration, identi-
fying for, 133-140

in-band traffic, 152

OOB traffic, 152

router services, filtering
via ACL, 217

router traffic, ZPF zone
behavior, 222-223

transform sets

IPsec transform sets, 329

configuring, 318-319

defining in Step-by-Step Setup mode (Site-to-Site VPN Wizard), 332-333

verifying, 322

policy sets versus, 311

transparent firewalls, 200

Transport Layer (OSI Layer 4), encryption, 249

transport mode (IPsec) versus tunnel mode, 314

trap receivers (SNMP), 160

Trojan horses, endpoint security, 399-402

troubleshooting

IPsec site-to-site VPN, CLI implementations, 321-322

local AAA, 140-141

RADIUS, 140-141

TACACS+, 140-141

VPN, Step-by-Step Setup mode (Site-to-Site VPN Wizard), 335-336

true negative signature alarms, 359

true positive signature alarms, 359

trust exploits, 39

Trusted Recovery operations security principle, 54

tunnel mode (IPsec) versus transport mode, 314

two-man control (SoD operations security principle), 55

U

U.S. government regulations, computer crime prosecution, 28-29

UCM (Unified Communications Manager), fraud protection features, 414

UDP (User Datagram Protocol), disabling, 169

UDP ports, best practices against network attacks, 46

unclassified data classification level, 21

Understanding PKI: Concepts, Standards and Deployment Considerations, 505

unicast traffic, bandwidth limitations, 438

unnecessary services, best practices against network attacks, 46

unreachable notifications (ICMP), disabling, 171

USA PATRIOT Act, 29

useful life metric (data classification), 22

user accounts, local AAA configuration on routers, 117

user role (data classification), 22

usernames, password security, 96

V

V3PN (Voice and Video Enabled VPN), 298

VAC+ (VPN Accelerator Card +), 300

value metric (data classification), 22

videoconference stations, VoIP, 412

views, creating, 98-100

violation mode (port security), configuring, 431

virtual line interfaces, 93

virtual login security

blocking login systems, 102

delays between logins, 103

login configuration verification, 103

quiet mode, 102

Syslog login detection messages, generating, 103

virtual terminal passwords, 95

viruses, endpoint security, 399-401

vishing attacks, VoIP, 414

VLAN (Virtual Local Area Networks), hopping attacks, 422

double-tagging, 424-425

rogue trunks, 423-424

VoIP (Voice over Internet Protocol)

call policies, 416

components of, 411-412

DoS attacks, 413

eavesdropping attacks, 414

inspecting, 416

MIM attacks, 414

protocols of, 412

rate limits, 416

reconnaissance attacks, 413

registration, 416

security

endpoint configura-
tion, 417

firewalls, 415-416

server configura-
tion, 417

VPN, 416-417

VVLAN, 415

SIP, 414

SPIT, 413

standards

compliance, 416

Theft and Toll

Fraud, 414

vishing attacks, 414

VPN (Virtual Private Networks)

AIM-VPN, 300

ASA 550 Series adap-
tive security appli-
ances, 299

benefits of, 293

Certicom client, 300

Cisco product position-
ing, 297-298

Cisco products list, 293

defining, 292

Easy VPN, 298-299

encryption algorithms,
304-305

hashing algorithms, 305

IOS routers, VPN
features of, 298

IPsec VPN

AES, 255

certificate-based
authentication, 283

configuring, 307-314

DH, 255

IKE Phase I,
307-311

IKE Phase II,
311-314

PKI, 280

SSL VPN versus,
301-302

IPsec VPN SPA, 300

policy sets, 310

PSK, 306

remote-access VPN, 295

Easy VPN, 298-299

VPN 3002

Hardware
Client, 300

Web VPN, 299

RSA encrypted
nonces, 306

RSA signatures, 306

SEP-E, 300

site-to-site VPN

anti-replay, 303

authentication, 295,
303, 306

CLI implementa-
tion, 315-325

confidentiality, 294,
302-305

DH key
exchanges, 305

DMVPN, 298

integrity, 294,
303-305

IPsec stateful
failover, 298

SDM implementa-
tion, 325-326,
329-336

SSL VPN, 259-260

AnyConnect VPN
Client, 300

client mode, 296

clientless mode, 296

compatibility, 297

disadvantages
of, 296

IPsec VPN versus,
301-302

troubleshooting, Step-
by-Step Setup mode
(Site-to-Site VPN
Wizard), 335-336

V3PN, 298

VAC+, 300

VoIP, 416-417

VPN Software Client,
300

Web VPN, 299

VPN 3002 Hardware Client, 300

VPN Software Client, 300

VPN Wizard (SDM), 110

VSAN (Virtual Storage Area Networks), 409

vulnerabilities, categories of, 30

VVLAN (Voice VLANs), 415

W

warm site backups, 61

web resources

cryptography, 505

network security
policies, 503
practices, 504

Web VPN (Virtual Private Networks), 299

white hat hackers, 31

wildcard masks, 214

Windows, Secure ACS installation require- ments, 124

wizards

Basic Firewall Wizard
(SDM), ZPF configu-
ration, 224-233

Firewall and ACL
Wizard (SDM), 110

Interface and
Connection Wizard
(SDM), 110

- Intrusion Prevention Wizard (SDM), 111
- IPS Policies Wizard, 367, 369-370
- IPS Rule Wizard, 367
- NAC Wizard (SDM), 111
- NAT Wizard (SDM), 111
- Quality of Service Wizard (SDM), 111
- Routing Wizard (SDM), 111
- Security Audit Wizard (SDM), 111
 - Cisco AutoSecure feature versus, 178-179
 - One-Step Lockdown feature, 172, 176
 - Perform Security Audit button, 173
 - Security Audit Interface Configuration page, 174
 - Security Audit report window, 174-175
- Site-to-Site VPN Wizard
 - Quick Setup mode, 325-326, 329
 - Step-by-Step Setup mode, 329-336
- smart wizards (SDM), list of, 110-111
- VPN Wizard (SDM), 110

worms

- endpoint security, 399-402
- five p's of worm attacks, 402

write mem command, 99

WWN (World Wide Names), 409

X-Y-Z

X.509 v3 standard, PKI, 281

zoning, SAN, 410

ZPF (Zone-based Policy Firewalls), 218

- ACL, 220
- actions of, 221
- advantages of, 220
- Basic Firewall Wizard (SDM), configuring via, 224-233
- configuring, 219
- features of, 221
- manual configuration via SDM, 233
 - class map creation, 235
 - policy map creation, 236
 - zone creation, 234
 - zone pair creation, 237
- monitoring, 238-240
- zone behavior in, 221
 - traffic destined to routers, 223
 - traffic flowing through routers, 222
 - traffic originating from routers, 223
- zone pairs, creating for, 237