cisco

Official Cert Guide

Learn, prepare, and practice for exam success

- Master **CCNP Security FIREWALL 642-617** exam topics
- Assess your knowledge with **chapter-opening quizzes**
- Review key concepts with **exam preparation tasks**
- Practice with **realistic exam questions** on the CD-ROM

CCNP Security FIREWALL 642-617

DAVID HUCABY, CCIE® No. 4594
DAVE GARNEAU
ANTHONY SEQUEIRA, CCIE No. 15626

ciscopress.com

CCNP Security FIREWALL 642-617

Official Cert Guide

David Hucaby
Dave Garneau
Anthony Sequeira

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCNP Security FIREWALL 642-617 Official Cert Guide

David Hucaby
Dave Garneau
Anthony Sequeira

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

Printed in the United States of America

First Printing September 2011

Library of Congress Cataloging-in-Publication Data is on file.

ISBN-13: 978-1-58714-279-6

ISBN-10: 1-58714-279-1

Warning and Disclaimer

This book is designed to provide information for the Cisco CCNP Security 642-617 FIREWALL v1.0 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

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

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. 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@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Composition: Mark Shirar

Proofreader: Sarah Kearns

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Senior Development Editor: Christopher Cleveland

Technical Editors: Doug McKillip, Martin Walshaw

Copy Editor: Bill McManus

Book Designer: Gary Adair

Indexer: Tim Wright

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Authors

David Hucaby, CCIE No. 4594, is a network architect for the University of Kentucky, where he works with healthcare networks based on the Cisco Catalyst, ASA, FWSM, and Unified Wireless product lines. David has a bachelor of science degree and master of science degree in electrical engineering from the University of Kentucky. He is the author of several Cisco Press titles, including *Cisco ASA, PIX, and FWSM Firewall Handbook,* Second Edition; *Cisco Firewall Video Mentor; Cisco LAN Switching Video Mentor;* and *CCNP SWITCH Exam Certification Guide*.

David lives in Kentucky with his wife, Marci, and two daughters.

Dave Garneau is a senior member of the Network Security team at Rackspace Hosting, Inc., a role he started during the creation of this book. Before that, he was the principal consultant and senior technical instructor at The Radix Group, Ltd. In that role, Dave trained more than 3000 students in nine countries on Cisco technologies, mostly focusing on the Cisco security products line, and worked closely with Cisco in establishing the new Cisco Certified Network Professional Security (CCNP Security) curriculum. Dave has a bachelor of science degree in mathematics from Metropolitan State College of Denver (now being renamed Denver State University). Dave lives in San Antonio, Texas with his wife, Vicki.

Anthony Sequeira, CCIE No. 15626, is a Cisco Certified Systems Instructor and author regarding all levels and tracks of Cisco Certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies. Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company KnowledgeNet, and Anthony trained there for many years. Anthony is currently pursuing his second CCIE in the area of Security and is a full-time instructor for the next generation of KnowledgeNet, StormWind Live.

About the Technical Reviewers

Doug McKillip, P.E., CCIE No. 1851, is an independent consultant specializing in Cisco Certified Training in association with Global Knowledge, a Training Partner of Cisco Systems. He has more than 20 years of experience in computer networking and security. Doug provided both instructional and technical assistance during the initial deployment of MCNS Version 1.0, the first Cisco Security training class, which debuted in early 1998, and has been a lead instructor for the security curriculum ever since. He holds bachelor's and master's degrees in chemical engineering from MIT and a master's degree in computer and information sciences from the University of Delaware. He resides in Wilmington, Delaware.

Martin Walshaw, CCIE No. 5629, CISSP, is a senior systems engineer working for F5 Networks in South Africa. His areas of expertise span multiple different areas, but over the past few years he has focused specifically on security and application delivery. During the past 20 years or so, Martin has dabbled in many different areas of IT, ranging from RPG III to PC sales. When Martin is not working or doing sports, he likes to spend all of his available time with his extremely patient wife, Val, and his two awesome sons, Joshua and Callum. Without their support, patience, and understanding, projects such as this would not be possible.

Dedications

From David Hucaby:

As always, this book is dedicated to the most important people in my life: my wife, Marci, and my two daughters, Lauren and Kara. Their love, encouragement, and support carry me along. I'm so grateful to God, who gives endurance and encouragement (Romans 15:5), and who has allowed me to work on projects like this.

From Dave Garneau:

I am also dedicating this book to the most important person in my life: my wife, Vicki. Without her love and support, I doubt I would succeed in any major endeavor, much less one of this magnitude. Additionally, I want to dedicate this book to my mother, Marian, who almost 40 years ago believed a very young version of myself when he declared he would one day grow up and write a book. I am glad I was finally able to live up to that promise.

From Anthony Sequeira:

This book is dedicated to the many, many students I have had the privilege of teaching over the past several decades. I hope that my passion for technology and learning has conveyed itself and helped to motivate, and perhaps even inspire.

Acknowledgments

It has been my great pleasure to work on another Cisco Press project. I enjoy the networking field very much, and technical writing even more. And more than that, I'm thankful for the joy and inner peace that Jesus Christ gives, making everything more abundant and worthwhile.

I've now been writing Cisco Press titles continuously for over 10 years. I always find it to be quite fun, but other demands seem to be making writing more difficult and time consuming. That's why I am so grateful that Dave Garneau and Anthony Sequeira came along to help tote the load. It's also been a great pleasure to work with Brett Bartow and Chris Cleveland. I'm glad they put up with me yet again, especially considering how much I let the schedule slip.

I am very grateful for the insight, suggestions, and helpful comments that the technical editors contributed. Each one offered a different perspective, which helped make this a more well-rounded book and me a more educated author.

—David Hucaby

The creation of this book has certainly been a maelstrom of activity. I was originally slated to be one of the technical reviewers, but became a coauthor at David Hucaby's request.

Right after accepting that challenge, I started a new job, moved to a new city, and built a new house. Throughout all the resulting chaos, Brett Bartow and Christopher Cleveland demonstrated the patience of Job, while somehow keeping this project on track. Hopefully, their patience was not exhausted, and I look forward to working with them again on future projects.

I am also thankful to our technical reviewers for their meticulous attention to detail. Doug McKillip, whom I count as a close friend, was able to step into the role I left to become a coauthor. The extremely thorough reviews provided by Doug and Martin definitely improved the quality of the material for the end readers.

—Dave Garneau

Brett Bartow is a great friend, and I am so incredibly thankful to him for the awesome opportunities he has helped me to achieve with the most respected line of IT texts in the world, Cisco Press. I am also really thankful that he continues to permit me to participate in his fantasy baseball league.

It was such an honor to help on this text with the incredible David Hucaby and Dave Garneau. While they sought out a third author named David, it was so kind of them to make a concession for an Anthony.

I cannot thank David Hucaby enough for the assistance he provided me in accessing the latest and greatest Cisco ASAs for the lab work and experimentation that was required for my chapters of this text.

Finally, thanks to my family, Joette and Annabella and the dog Sweetie, for understanding all of the hours I needed to spend hunched over a keyboard. And that reminds me, thanks also to my chiropractor, Dr. Paton.

—Anthony Sequeira

Contents at a Glance

Contents

Icons Used in This Book

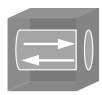

Cisco ASA

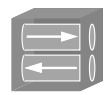

IPS


Content Services Module


AAA Server


CA


SSL VPN Gateway


IPsec VPN Gateway


Router


Layer 3 Switch

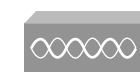

Layer 2 Switch


PC


IP Phone


Server


Network Cloud


Access Point


Wireless Connection

Ethernet Connection

Introduction

This book is designed to help you prepare for the Cisco FIREWALL v1.0 certification exam. The FIREWALL exam is one in a series of exams required for the Cisco Certified Network Professional Security (CCNP Security) certification. This exam focuses on the application of security principles with regard to the Cisco Adaptive Security Appliance (ASA) device.

Who Should Read This Book

Network security is a complex business. It is important that you have extensive experience in and an in-depth understanding of computer networking before you can begin to apply security principles. The Cisco FIREWALL program was developed to introduce the ASA security products, explain how each product is applied, and explain how it can be leveraged to increase the security of your network. The FIREWALL program is for network administrators, network security administrators, network architects, and experienced networking professionals who are interested in applying security principles to their networks.

How to Use This Book

The book consists of 16 chapters. Each chapter tends to build upon the chapter that precedes it. Each chapter includes case studies or practice configurations that can be implemented using both the command-line interface (CLI) and Cisco Adaptive Security Device Manager (ASDM).

The chapters of the book cover the following topics:

- **Chapter 1, "Cisco ASA Overview":** This chapter discusses basic network security and traffic filtering strategies. It also provides an overview of ASA operation, including the ASA feature set, product licensing, and how various ASA models should be matched with the environments they will protect.
- **Chapter 2, "Working with a Cisco ASA":** This chapter reviews the basic methods used to interact with an ASA and to control its basic operation. Both the CLI and ASDM are discussed.
- **Chapter 3, "Configuring ASA Interfaces":** This chapter explains how to configure ASA interfaces with the parameters they need to operate on a network.
- **Chapter 4, "Configuring IP Connectivity":** This chapter covers the ASA features related to providing IP addressing through DHCP and to exchanging IP routing information through several different dynamic routing protocols.
- **Chapter 5, "Managing a Cisco ASA":** This chapter reviews the configuration commands and tools that can be used to manage and control an ASA, both locally and remotely.

- **Chapter 6, "Recording ASA Activity":** This chapter describes how to configure an ASA to generate logging information that can be collected and analyzed. The logging information can be used to provide an audit trail of network and security activity.
- **Chapter 7, "Using Address Translation":** This chapter describes how IP addresses can be altered or translated as packets move through an ASA. The various types of Network Address Translation (NAT) and Port Address Translation (PAT) are covered.
- **Chapter 8, "Controlling Access Through the ASA":** This chapter reviews access control lists and host shunning, and how these features can be configured to control traffic movement through an ASA.
- **Chapter 9, "Inspecting Traffic":** This chapter covers the Modular Policy Framework, a method used to define and implement many types of traffic inspection policies. It also covers ICMP, UDP, TCP, and application protocol inspection engines, as well as more advanced inspection tools such as botnet traffic filtering and threat detection.
- **Chapter 10, "Using Proxy Services to Control Access":** This chapter discusses the features that can be leveraged to control the authentication, authorization, and accounting of users as they pass through an ASA.
- **Chapter 11, "Handling Traffic":** This chapter covers the methods and features that can be used to handle fragmented traffic, to prioritize traffic for QoS, to police traffic rates, and to shape traffic bandwidth.
- **Chapter 12, "Using Transparent Firewall Mode":** This chapter reviews transparent firewall mode and how it can be used to make an ASA more stealthy when introduced into a network. The ASA can act as a transparent bridge, forwarding traffic at Layer 2.
- **Chapter 13, "Creating Virtual Firewalls on the ASA":** This chapter discusses the multiple context mode that can be used to allow a single physical ASA device to provide multiple virtual firewalls or security contexts.
- **Chapter 14, "Deploying High Availability Features":** This chapter covers two strategies that can be used to implement high availability between a pair of ASAs.
- **Chapter 15, "Integrating ASA Service Modules":** This chapter explains the basic steps needed to configure an ASA to work with the AIP and CSC Security Services Modules (SSM), which can be used to offload in-depth intrusion protection and content handling.
- **Chapter 16, "Final Preparation":** This short chapter lists the exam preparation tools useful at this point in the study process and provides a suggested study plan now that you have completed all the earlier chapters in this book.
- **Appendix A, "Answers to the 'Do I Know This Already?' Quizzes":** This appendix provides the answers to the "Do I Know This Already?" quizzes that you will find at the beginning of each chapter.

- **Appendix B, "CCNP Security 642-617 FIREWALL Exam Updates: Version 1.0":** This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you will need to consult the new edition of the book for the updated content. This additional content about the exam will be posted as a PDF document on this book's companion website, at www.ciscopress.com/title/9781587142796.
- **Appendix C, "Traffic Analysis Tools":** This appendix discusses two troubleshooting tools that you can use to test and confirm packet movement through an ASA.
- **Glossary of Key Terms:** This glossary defines the key terms that appear at the end of each chapter, for which you should be able to provide definitions on your own in preparation for the exam.

Each chapter follows the same format and incorporates the following tools to assist you by assessing your current knowledge and emphasizing specific areas of interest within the chapter:

- **"Do I Know This Already?" Quiz:** Each chapter begins with a quiz to help you assess your current knowledge of the subject. The quiz is divided into specific areas of emphasis that enable you to best determine where to focus your efforts when working through the chapter.
- **Foundation Topics:** The foundation topics are the core sections of each chapter. They focus on the specific protocols, concepts, or skills that you must master to successfully prepare for the examination.
- **Exam Preparation:** Near the end of each chapter, the Exam Preparation section highlights the key topics from the chapter and the pages where you can find them for quick review. This section also provides a list of key terms that you should be able to define in preparation for the exam. It is unlikely that you will be able to successfully complete the certification exam by just studying the key topics and key terms, although they are a good tool for last-minute preparation just before taking the exam.
- **Command References:** Each chapter ends with a series of tables containing the commands that were covered. The tables provide a convenient place to review the commands, their syntax, and the sequence in which they should be used to configure a feature.
- **CD-ROM-based practice exam:** This book includes a CD-ROM containing several interactive practice exams. It is recommended that you continue to test your knowledge and test-taking skills by using these exams. You will find that your test-taking skills will improve by continued exposure to the test format. Remember that the potential range of exam questions is limitless. Therefore, your goal should not be to "know" every possible answer but to have a sufficient understanding of the subject matter so that you can figure out the correct answer with the information provided.

Certification Exam and This Preparation Guide

The questions for each certification exam are a closely guarded secret. The truth is that if you had the questions and could only pass the exam, you would be in for quite an embarrassment as soon as you arrived at your first job that required these skills. The point is to know the material, not just to successfully pass the exam.

We do know which topics you must know to successfully complete this exam because Cisco publishes them as "642-617 Deploying Cisco ASA Firewall Solutions Exam Topics (Blueprint)" on the Cisco Learning Network. Table I-1 lists each FIREWALL v1.0 exam topic listed in the blueprint, along with a reference to the chapter that covers the topic. These are the same topics you should be proficient in when configuring the Cisco ASA in the real world.

Table I-1 *FIREWALL v1.0 Exam Topics and Chapter References*

Exam Topic	Chapter Where Topic Is Covered
Pre-Production Design	
Choose ASA Perimeter Security technologies/features to implement HLD based on given security requirements	Chapter 1
Choose the correct ASA model to implement HLD based on given performance requirements	Chapter 1
Create and test initial ASA appliance configurations using CLI	Chapters 2–15
Determine which ASA licenses will be required based on given requirements	Chapter 1
Complex Operations Support	
Optimize ASA Perimeter Security features performance, functions, and configurations	Chapters 2–15
Create complex ASA security perimeter policies such as ACLs, NAT/PAT, L3/L4/L7 stateful inspections, QoS policies, cut-through proxy, threat detection, and botnet detection/filter using CLI and/or ASDM	Chapters 7–11
Perform initial setup on the AIP-SSM and CSC-SSM using CLI and/or ASDM	Chapter 15
Configure, verify, and troubleshoot High Availability ASAs (A/S and A/A FO) operations using CLI and/or ASDM	Chapter 14
Configure, verify, and troubleshoot static routing and dynamic routing protocols on the ASA using CLI and/or ASDM	Chapter 4

Table I-1 *FIREWALL v1.0 Exam Topics and Chapter References*

Exam Topic	Chapter Where Topic Is Covered
Pre-Production Design	
Configure, verify, and troubleshoot ASA transparent firewall operations using CLI	Chapter 12
Configure, verify, and troubleshoot management access/protocols on the ASA using CLI and/or ASDM	Chapters 5 and 6
Describe Advanced Troubleshooting	
Advanced ASA security perimeter configuration/software/hardware troubleshooting using CLI and/or ASD fault finding and repairing	Chapters 2–15

Notice that not all the chapters map to a specific exam topic. Each version of the exam can have topics that emphasize different functions or features, while some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. In order to do this, all possible topics that have been addressed in different versions of this exam (past and present) are covered. Many of the chapters that do not specifically address exam topics provide a foundation that is necessary for a clear understanding of network security. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified network security professional.

It is also important to understand that this book is a "static" reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.

This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information available at Cisco.com that covers each topic in great detail. The goal of this book is to prepare you as well as possible for the FIREWALL exam. Some of this is completed by breaking a 600-page (average) implementation guide into a 30-page chapter that is easier to digest. If you think that you need more detailed information on a specific topic, you should read the Cisco documentation that focuses on that topic.

Note that because security vulnerabilities and preventive measures continue to develop, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics listed in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, hovering over Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book at www.ciscopress.com/title/9781587142796. It's a good idea to check the website a couple of weeks before taking your exam to be sure that you have up-to-date content.

Overview of the Cisco Certification Process

The network security market is currently in a position where the demand for qualified engineers vastly surpasses the supply. For this reason, many engineers consider migrating from routing/networking over to network security. Remember that "network security" is just "security" applied to "networks." This sounds like an obvious concept, but it is actually an important one if you are pursuing your CCNP Security certification. You must be familiar with networking before you can begin to apply the security concepts. For example, the skills required to complete the CCNA or CCNP will give you a solid foundation that you can expand into the network security field.

Taking the FIREWALL Certification Exam

As with any Cisco certification exam, you should strive to be thoroughly prepared before taking the exam. There is no way to determine exactly what questions are on the exam, so the best way to prepare is to have a good working knowledge of all subjects covered on the exam. Schedule yourself for the exam and be sure to be rested and ready to focus when taking the exam.

The best place to find out the latest available Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking CCNP Status

You can track your certification progress by checking www.cisco.com/go/certifications/login. You must create an account the first time you log in to the site.

How to Prepare for an Exam

The best way to prepare for any certification exam is to use a combination of the preparation resources, labs, and practice tests. This guide has integrated some practice questions and example scenarios to help you better prepare. If possible, you should get some hands-on experience with the Cisco ASA. There is no substitute for real-world experience; it is much easier to understand the commands and concepts when you can actually work with a live ASA device.

Cisco.com provides a wealth of information about the ASA and its software and features. No single source can adequately prepare you for the FIREWALL exam unless you already have extensive experience with Cisco products and a background in networking or network security. At a minimum, you will want to use this book combined with the Support and Downloads site resources (www.cisco.com/cisco/web/support/index.html) to prepare for the exam.

Assessing Exam Readiness

Exam candidates never really know if they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the "Do I Know This Already?" quizzes at the beginning of each chapter, review the foundation and key topics presented in each chapter, and review the command reference tables at the end of each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Cisco Security Specialist in the Real World

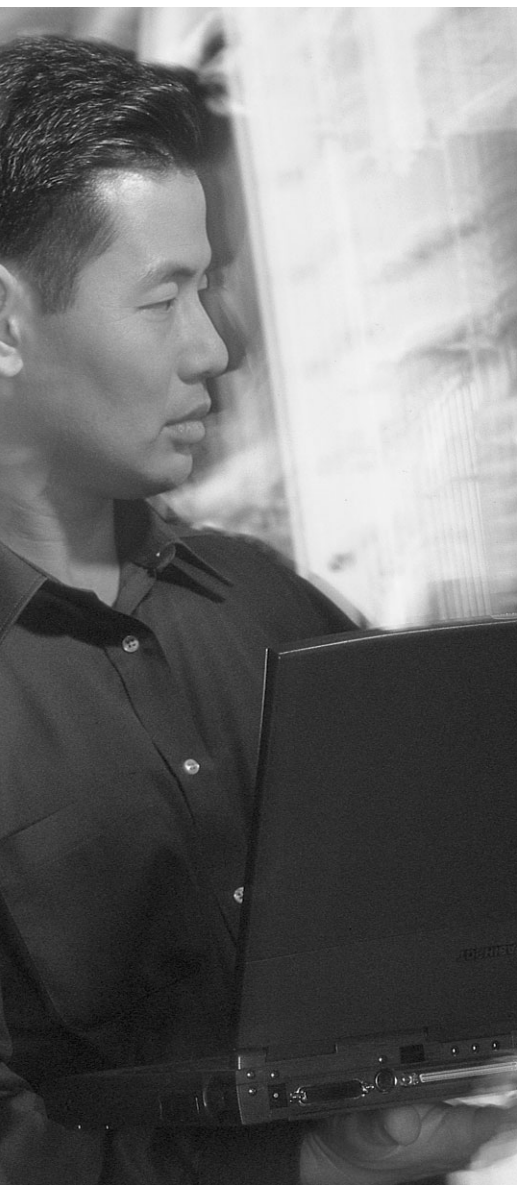
Cisco has one of the most recognized names on the Internet. Cisco Certified Security Specialists can bring quite a bit of knowledge to the table because of their deep understanding of the relationship between networking and network security. This is why the Cisco certification carries such high respect in the marketplace. Cisco certifications demonstrate to potential employers and contract holders a certain professionalism, expertise, and dedication required to complete a difficult goal. If Cisco certifications were easy to obtain, everyone would have them.

Exam Registration

The FIREWALL exam is a computer-based exam, with around 60 to 70 multiple choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (www.pearsonvue.com) testing center. According to Cisco, the exam should last about 90 minutes. Be aware that when you register for the exam, you might be told to allow a certain amount of time to take the exam that is longer than the testing time indicated by the testing software when you begin. This discrepancy is because the testing center will want you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco occasionally updates exam topics without notice, Cisco Press might post additional preparatory content on the web page associated with this book at www.ciscopress.com/title/9781587142796. It is a good idea to check the website a couple of weeks before taking your exam, to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Cisco Press website to view any errata or supporting book files that may be available.



This chapter covers the following topics:

- **System Time:** This section describes configuration of system time, both locally on the Cisco Adaptive Security Appliance and through the use of NTP.
- **Managing Event and Session Logging:** This section gives an overview of the security appliance logging subsystem, including event destinations, severity levels, and NetFlow support.

Note: The terms Cisco Adaptive Security Appliance, ASA, and security appliance are used interchangeably.

- **Configuring Event and Session Logging:** This section describes the configuration of logging on the security appliance. It covers the setting of global parameters, the creation of event lists and filters, and the details on configuring a number of event destinations.
- **Verifying Event and Session Logging:** This section covers commands used to verify proper functioning of logging on the security appliance.
- **Troubleshooting Event and Session Logging:** This section covers commands used to troubleshoot logging functionality.

CHAPTER 6

Recording ASA Activity

Effective troubleshooting of network or device activity, from the perspective of the security appliance, requires accurate information. Many times, the best source of accurate and complete information will be various logs, if logging is properly configured to capture the necessary information. A Cisco security appliance has many potential destinations to which it can send logging information.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 6-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 6-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
System Time	1–4
Managing Event and Session Logging	5–7
Configuring Event and Session Logging	8–12
Verifying Event and Session Logging	13
Troubleshooting Event and Session Logging	14

Caution: The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which are two of the most important reasons for ensuring accurate time on the security appliance? (Choose two.)
   a. Synchronization with AAA servers
   b. Use of digital certificates
   c. Time-based Modular Policy Framework rules
   d. Time stamps in log messages
2. Where in ASDM do you configure NTP authentication and servers?
   a. **Configuration > Device Setup > System Time > NTP**
   b. **Configuration > Device Management > System Time > NTP**
   c. **Configuration > Device Management > System Time > NTP > Parameters**
   d. **Configuration > Device Setup > System Time > NTP > Parameters**
3. Consider the following command:
   ```
   ntp authentication-key 1 md5 UEB34mid@#9C
   ```
   What does this command mean?
   a. This is the first authentication key in a key ring, and the MD5 hash value is the value UEB34mid@#9C.
   b. The key number is 1, which will be sent by the NTP server in all packets. The key of UEB34mid@#9C is used to create an MD5 keyed hash value to verify the server message.
   c. The key number is 1, which is locally significant and allows the creation of multiple trusted keys per server. The key of UEB34mid@#9C is used to create an MD5 keyed hash value to verify the server message.
   d. None of these answers are correct. This is not a valid command string.
4. Consider the following command:
   ```
   ntp server 10.0.0.5 key 1 source inside prefer
   ```
   What is the meaning of the word "prefer" in this command?
   a. This NTP server is preferred over all other time sources.
   b. The security appliance prefers the use of NTP authentication key 1 over other keys in the key ring.
   c. The security appliance prefers the use of NTP authentication using key 1, but is willing to accept unauthenticated NTP messages from this server.
   d. This NTP server is preferred over other time sources of similar accuracy, but can be overridden by a more accurate time source.
   e. None of these answers are correct. This is not a valid command string.
5. What are the two major classifications of security appliance events? (Choose two.)
   a. System events
   b. Security events
   c. Network events

d. Syslog events

e. None of these answers are correct. This is not a valid command string.

6. Consider the following partial event message:

```
Jan 5 2011 09:27:16 FIREWALL : %ASA-6-725002: Device completed ...
```

What is the severity level of this event message?

a. Notifications

b. Informational

c. Warnings

d. Debugging

e. Errors

7. Which version of NetFlow is supported by the security appliance?

a. 9

b. 2

c. 7.2

d. 5

8. If the internal buffer logging destination becomes full, which two locations can its contents be copied to, to ensure no loss of information?

a. An HTTP server

b. An FTP server

c. Internal flash memory

d. A TFTP server

e. An SCP server

9. How are time stamps enabled/disabled for logging event messages to destinations?

a. Once, globally, by navigating to **Configuration > Device Management > Logging > Syslog Setup**

b. Once, globally, by navigating to **Configuration > Device Management > Logging > Logging Setup**

c. Once, globally, but this can be done only from the CLI

d. Per log destination, by navigating to **Configuration > Device Management > Logging >** *screen for destination being configured*

e. Per log destination, but this can be done only from the CLI interface

10. You want to change the level at which message 106018 is logged to Notifications, from its default setting. The message will be sent to your syslog server destination. Which of the following is the correct command syntax?

a. **logging trap message 106018 level Notifications**

b. **message 106018 syslog level Notifications**

c. **logging message 106018 level Notifications**

d. **logging level Notifications message 106018**

e. **logging message 106018 new level Notifications**

11. What is an event list? (Choose all that apply.)

a. A grouping of messages, based on which logging subsystem generated the events in the list.

b. A reusable group of messages, selected by a combination of event class, event severity, and separately by message IDs.

c. A filter, used to determine which messages generated by the logging subsystem are forwarded to a particular log destination.

d. All of these answers are correct.

12. You want to configure logging so that email messages are sent to administrators when events of maximum level Errors are generated by the system. Which of the following is the correct syntax for the command you need to use?

a. **logging smtp Errors**

b. **logging trap smtp Errors**

c. **logging email Errors**

d. **logging trap email Errors**

e. **logging mail Errors**

f. **logging trap mail Errors**

13. You want to verify that the security appliance is sending NetFlow v9 records to the configured NetFlow collector. Which of these items will do that?

a. Use the **show logging** command and look for a non-zero number as **messages logged** for the NetFlow destination.

b. Use the **show logging** command and look for a non-zero number as **packets sent** for the NetFlow destination.

c. Use the **show flow-export counters** command and look for a non-zero number as **messages logged**.

d. Use the **show flow-export counters** command and look for a non-zero number as **packets sent**.

14. You suspect your syslog server is not receiving all messages generated by the security appliance, possibly due to excessive logging leading to a queue overflow. What command would you use to verify your suspicions?

a. **show logging**

b. **show logging queue**

c. **show logging drops**

d. **show logging queue drops**

Foundation Topics

This chapter discusses methods for gathering information on network or device activity, including the use of system event logs. It also discusses how to ensure accurate time on the system clock, because accurate time stamps on gathered information are critical to properly analyzing that information.

System Time

Having a correct time set on a Cisco ASA is important for a number of reasons. Possibly the most important reason is that digital certificates compare this time to the range defined by their Valid From and Valid To fields to define a specific validity period. Having a correct time set is also important when logging information with the **timestamp** option. Whether you are sending messages to a syslog server, sending messages to an SNMP monitoring station, or performing packet captures, time stamps have little usefulness if you cannot be certain of their accuracy.

The default ASA time is set to UTC (Coordinated Universal Time), but you can add local time zone information so that the time displayed by the ASA is more relevant to those who are viewing it. Even if you set local time zone information, the ASA internally tracks time as UTC, so if it is interacting with hosts in other time zones (which is fairly common when using digital certificates for VPN connectivity, for example), they have a common frame of reference.

To set the time locally on the ASA (that is, not using Network Time Protocol [NTP]), first navigate to **Configuration > Device Setup > System Time > Clock** to display the Clock settings window, shown in Figure 6-1. If you want to set the clock to UTC time, simply enter a new date and time, as UTC is the default time zone. If you prefer to set the clock using your local time zone, choose that time zone from the drop-down list before you enter a new date and time (Figure 6-1 shows the North American Central Time Zone being selected).

You can then set the date and time accordingly. Time is set as hours, minutes, and seconds, in 24-hour format. Optionally, you can click the Update Displayed Time button to update the time shown in the bottom-right corner of the Cisco ASDM status bar. The current time updates automatically every ten seconds. Click **Apply** to complete the setting of the internal clock.

The configured time is retained in memory when the power is off, by a battery on the security appliance motherboard.

NTP

Of course, to ensure precise synchronization of the ASA's clock to the rest of your network, you should configure the ASA to obtain time information from a trusted NTP server. To do so, navigate to **Configuration > Device Setup > System Time > NTP**. The NTP settings window opens. To define a new NTP time source, click **Add** to open the Add

NTP Server Configuration dialog box, shown in Figure 6-2. Define the IP address of the new NTP time source, the ASA interface through which this NTP server can be reached, and any information relevant to the use of authenticated NTP communication.

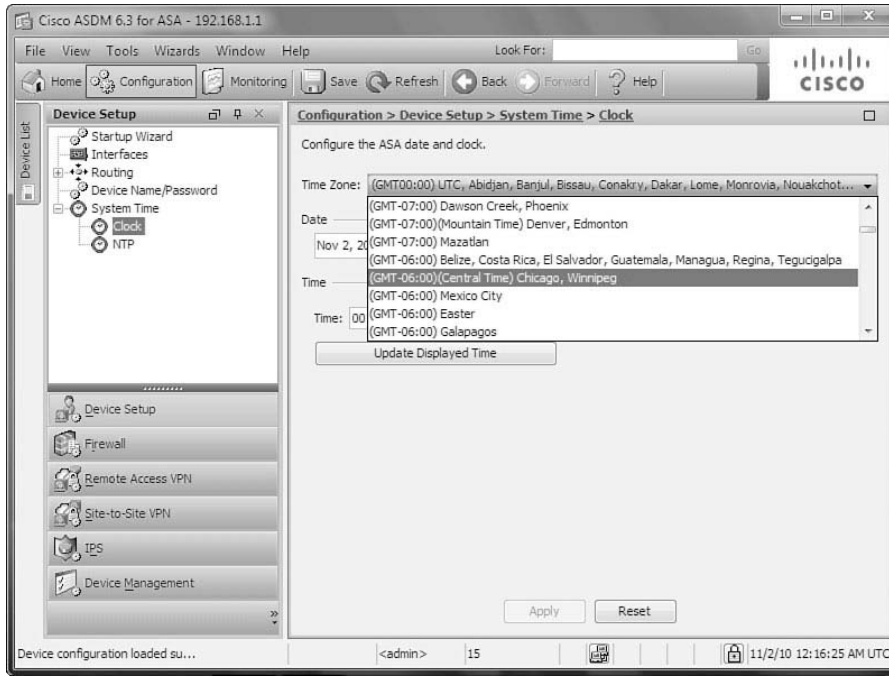


Figure 6-1 *Setting Local Time Parameters*

Figure 6-2 shows the configuration of an internal NTP server, 10.0.0.5, which is preferred to other NTP sources and uses NTP authentication for added security. To use NTP authentication, both the server and any clients must be configured with the same trusted key number and key (effectively, a password). The key number must be included in NTP packets from the server in order for the ASA to accept synchronization to that server. The key is used to create a keyed hash for verification that NTP advertisements are from an authorized source, and have not been tampered with. You must check the **Trusted** check box for the configured key ID for authentication to work. You must also check the **Enable NTP Authentication** box at the bottom of the NTP server window (shown in the background in Figure 6-2).

Note: The security appliance can act only as an NTP client, not as an NTP server.

You can configure additional NTP servers (a minimum of three associations is recommended for optimal accuracy and redundancy). Figure 6-3 shows the result of configuring TIME.NIST.GOV as an additional NTP server (it is not set as preferred, and does not use authentication). Note that, although the **name** command was used in Chapter 5 to map TIME.NIST.GOV to the IP address 192.43.244.18, if you tried to configure

TIME.NIST.GOV in the server field, it will result in an Invalid IP Address error. You can enter IP addresses only when defining NTP servers.

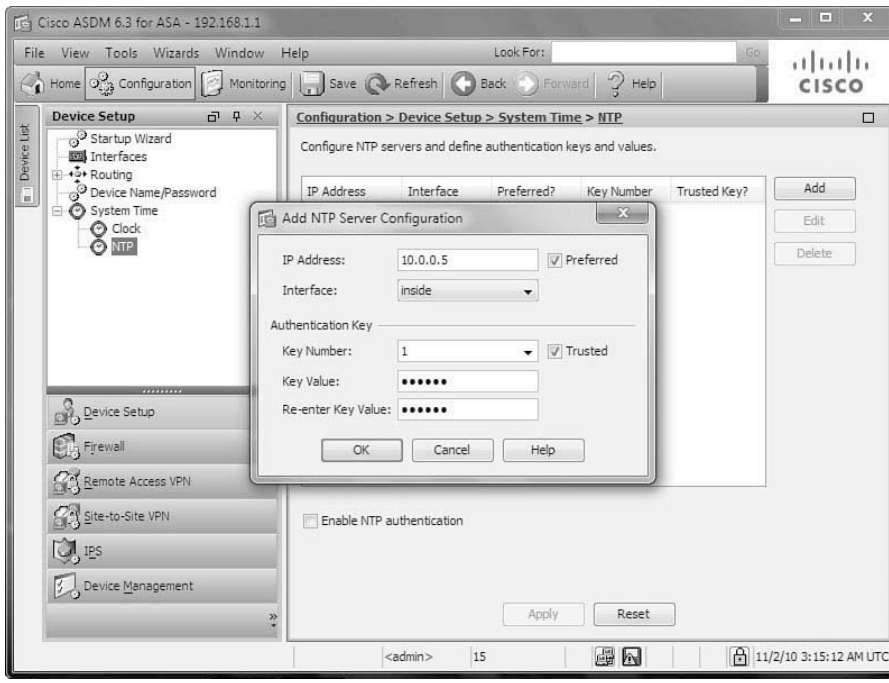


Figure 6-2 *Configuring an NTP Server*

Using an NTP server reachable through the outside interface, and not using authentication, is inherently subject to potential compromise, so it should be done only as a backup to an internal NTP server, if available. Note also that, because NTP Authentication is enabled on this ASA, time would not currently be accepted from the TIME.NIST.GOV server, because it is not configured for authenticated NTP messaging. Thus, the addition of this server is for example purposes only.

Key Topic

Time derived from an NTP server overrides any time set manually in the Clock pane. However, in the unlikely event of an extended period of unavailability of any configured NTP servers, the local clock can serve as a fallback mechanism for maintaining time on the security appliance. Setting a server as preferred does not guarantee that the ASA will accept the time advertised by such a server. The security appliance will choose the NTP server with the lowest stratum number and synchronize to that server. (A stratum number indicates the distance from the reference clock, so a lower stratum number implies that a server is more reliable than others with a higher stratum number. The atomic clock at NIST, for instance, is considered stratum 0.) If several servers have similar accuracy, the preferred server is used. If another server is significantly more accurate than the preferred server, however, the ASA uses the more accurate one.

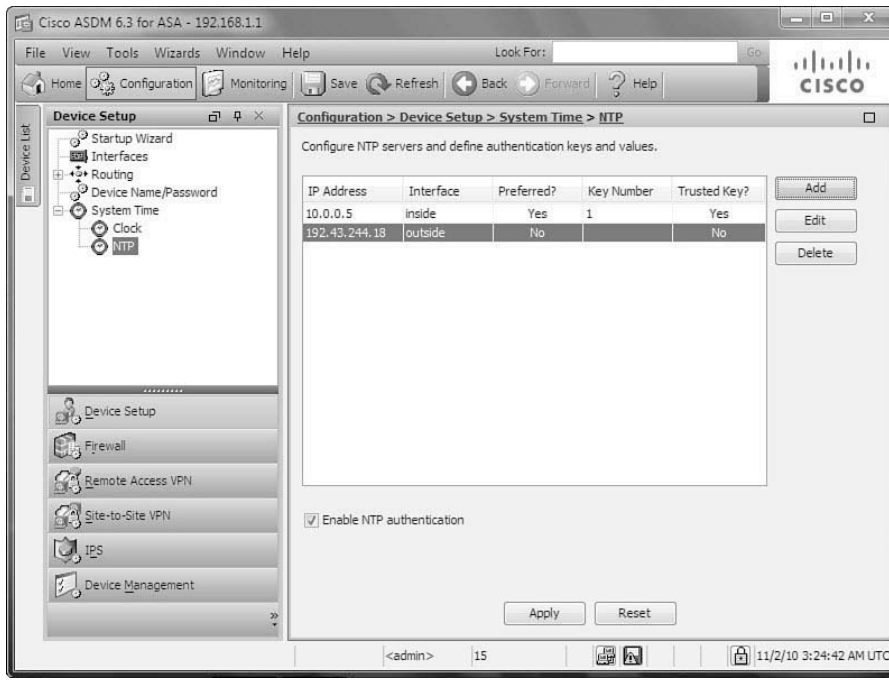


Figure 6-3 *Configuring Multiple NTP Servers*

The CLI commands generated by the changes made are as follows:

```
clock set 21:24:37 NOV 1 2010
clock timezone CST -6 0
clock summer-time CDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 60
ntp server 10.0.0.5 key 1 source inside prefer
ntp server 192.43.244.18 source outside
ntp authenticate
ntp authentication-key 1 md5 UEB34mid@#9C
ntp trusted-key 1
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode (the **clock set** command can actually be entered from privileged mode as well).

Note that if you set the time zone using ASDM, the use of Daylight Saving Time (DST) is automatically enabled, if appropriate, with the correct date and time parameters for the selected time zone. To alter the start and end dates of DST, should they be incorrect, you would need to make the change from the CLI.

The **clock set** command is used to manually set the security appliance date and time information. It can be used from the CLI in privileged EXEC mode (use of configuration mode is not necessary). When setting from the CLI, the date can be specified as MONTH DAY YEAR or DAY MONTH YEAR, whichever you prefer.

The **clock timezone** command defines a name for your local time zone (in Standard Time) as well as its offset from UTC in hours (the -6 in the example), and in minutes (the 0 in the example) if you live in a time zone with an offset that is not in whole hours.

The **clock summer-time** command defines a name for your local time zone (in DST), and uses the keyword **recurring** to set a recurring range, defined as a day and time of a given month, rather than a specific date, so that you do not need to alter the setting yearly. Use it to set the beginning and ending days and times for DST in your time zone (in the example, DST begins on the second Sunday in March at 2 a.m., and ends on the first Sunday of November at 2 a.m.) and the DST offset from Standard Time (in the example, 60 minutes).

The **ntp server** command defines a server to be used as a time source by the security appliance. This command sets the server IP address, authentication key number (if used), source interface, and whether or not it is a preferred server.

To enable authentication with an NTP server, you must use the **ntp authenticate** command from global configuration mode. The **ntp authentication-key** command ties the key number to the specific key used to create an MD5 keyed hash for source validation and integrity check. For NTP authentication to succeed, any key ID to be accepted by the security appliance must be defined as trusted. This is done using the **ntp trusted-key** command.

Verifying System Time Settings

Security appliance time can be verified using two commands, **show clock** and **show ntp associations**. Both have an optional keyword of **detail**. Example 6-1 shows the use of both the standard and detailed version of the **show clock** command.

Example 6-1 *Verifying System Time with* **show clock**

```
FIREWALL# show clock

10:09:16.309 CDT Tue Nov 2 2010
FIREWALL# show clock detail

10:03:55.129 CDT Tue Nov 2 2010
Time source is NTP
Summer time starts 02:00:00 CST Sun Mar 14 2010
Summer time ends 02:00:00 CDT Sun Nov 7 2010
```

As shown in the example, using the **detail** keyword with the **show clock** command adds information on the time source, and the local time zone DST information. Note the source of NTP in this example.

Example 6-2 shows the use of the **show ntp associations** command, which displays the configured NTP server and whether the security appliance is successfully synced.

Example 6-2 *Verifying System Time with* **show ntp associations**

```
FIREWALL# show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
*~10.0.0.5          127.0.0.1        3    87  1024  377     2.5   -0.23     1.8
-~192.43.244.18     .ACTS.           1   147  1024  377    41.5   -1.08    16.5
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Managing Event and Session Logging

The Cisco Adaptive Security Appliance supports a full audit trail of system log messages that describe its activities and security events. The two major classifications of events are *system events*, such as resource depletion, and *network events*, such as denied sessions or packets. These messages are used to create log files, which can be filtered and sent to a number of differing destinations for storage, display, or analysis.

Figure 6-4 provides a graphical illustration of the Cisco ASA logging subsystem, showing the two major event classifications as sources, and the eight possible destinations.

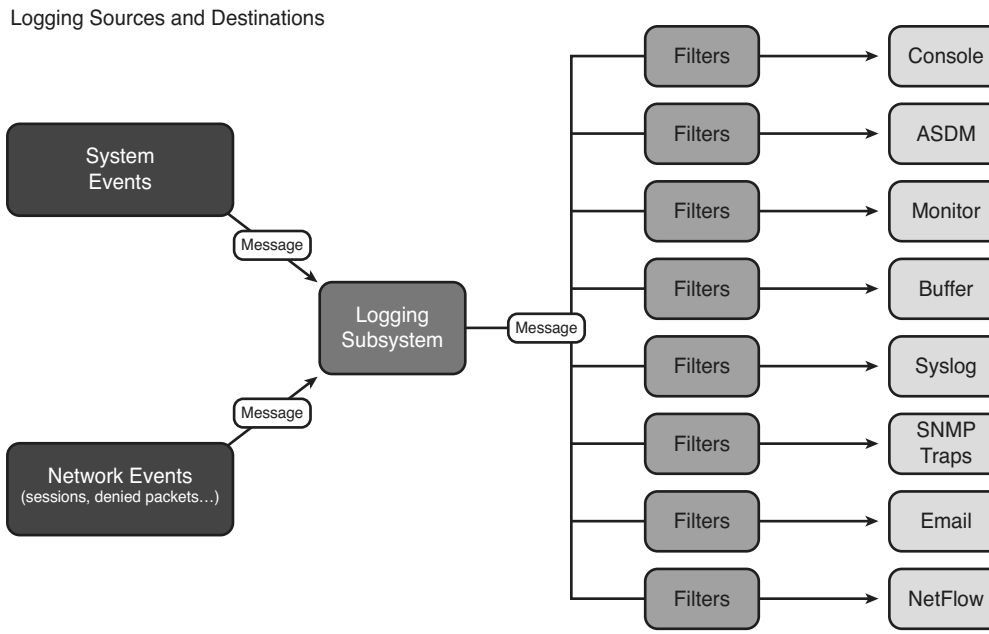


Figure 6-4 *The Cisco ASA Logging Subsystem*

The security appliance supports sending log messages to the following destinations:

- **Console:** The security appliance console, a low-bandwidth serial connection to which messages can be sent for display on a console CLI session. This mode is useful for limited debugging, or in production environments with limited traffic or a lack of centralized management tools.
- **ASDM:** The ASDM graphical user interface, which provides a powerful real-time event viewer useful for troubleshooting issues or monitoring network activity.
- **Monitor:** Telnet or SSH administrative sessions. This mode is useful to receive real-time debugging information when troubleshooting.
- **Buffered:** The internal in-memory buffer on the security appliance. Although useful for storage and analysis of recent activity, the internal buffer is limited in size, and it is not persistent, by default, across appliance reboots. The buffer can optionally be archived to an external FTP server or to the security appliance's internal flash memory.
- **Host:** Remote syslog servers, using the standard syslog protocol. Use the **logging host** command in conjunction with the **logging trap** command to define both a destination server and a logging level.
- **SNMP:** Remote network management servers, using the standard Simple Network Management Protocol (SNMP) Trap to send event messages. This mode is configured with the **snmp-server enable traps syslog** command, rather than directly with a **logging** *destination* command.
- **Mail:** Remote email systems, using the standard Simple Mail Transfer Protocol (SMTP) to send event messages to a defined SMTP server, or set of SMTP servers.
- **Flow-export-syslogs:** Remote NetFlow collectors, using the standard NetFlow v9 protocol to send event messages to the defined collector.

NetFlow Support

Cisco NetFlow efficiently provides a key set of services for IP applications, including network traffic accounting, usage-based network billing, network planning, security, denial-of-service monitoring capabilities, and network monitoring. NetFlow provides valuable information about network users and applications, peak usage times, and traffic routing.

The basic output of NetFlow is known as a flow record. Several different formats for flow records have existed as NetFlow has evolved and matured. The current version of NetFlow formatting is known as NetFlow version 9. The Cisco ASA supports providing NetFlow Secure Event Logging (NSEL), beginning with version 8.2(1). NSEL allows specific, high-volume, traffic-related events to be exported from the security appliance in a more efficient and scalable manner than that provided by standard syslog logging. You may use any NetFlow v9–capable collector to receive ASA NetFlow data.

The ASA implementation of NSEL is a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status, and are triggered by the events that cause state changes. Examples of events

that are tracked include flow-create, flow-teardown, and flow-denied (excluding flows that are denied by EtherType ACLs, which are discussed in Chapter 12, "Using Transparent Firewall Mode"). Each NSEL record has an event ID and an extended event ID field, which describe the flow event.

The Cisco ASA supports multiple NetFlow export destinations and can therefore store its NetFlow information on multiple NetFlow collectors.

For a detailed discussion on Cisco ASA NetFlow event generation, consult the "Cisco ASA 5500 Series Implementation Note for NetFlow Collectors, 8.2," at www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html.

Logging Message Format

Most Cisco ASA messages generated by the logging subsystem are simple text messages that conform to a particular message format, as demonstrated here:

```
Jan 5 2011 09:27:16 FIREWALL : %ASA-6-725002: Device completed SSL handshake with
  client management:192.168.1.8/49287
```

This message consists of the following:

- An optional **timestamp** (disabled by default)
- An optional **device-id** (disabled by default), which can include the interface name, IP address, hostname, context name, or a custom string up to 16 characters, if configured
- A message identifier (**%ASA-6-725002** in the example), which identifies the device type (ASA), the message severity level (6, Informational), and the event message number (725002)
- The message text (**Device completed SSL handshake...**)

Additional data may be added to the message, depending on its destination. For example, a time stamp and hostname may be added for the syslog destination.

Message Severity

Each log message is assigned a severity level that indicates its relative importance. Lower numbers are of higher severity than higher numbers. Possible number and string values for message severity are shown in Table 6-2.

Table 6-2 *Message Severity Levels*

Numeric Level	Equivalent String	Definition
0	Emergencies	Extremely critical "system unusable" messages
1	Alerts	Messages that require immediate administrator action
2	Critical	A critical condition
3	Errors	An error message (also the level of many access list deny messages)

Table 6-2 *Message Severity Levels*

Numeric Level	Equivalent String	Definition
4	Warnings	A warning message (also the level of many other access list deny messages)
5	Notifications	A normal but significant condition (such as an interface coming online)
6	Informational	An informational message (such as a session being created or torn down)
7	Debugging	A debug message or very detailed accounting message

Note: Take care in setting the severity level of messages being sent to various destinations, particularly the console. Too low a severity (a high number), when coupled with a lot of traffic, can severely impact system performance, or potentially exhaust system resources, and make it difficult or impossible to regain access to the device CLI. It is important to remember that the security appliance will send all messages of the selected level and all higher severity (lower number) messages, not just messages of the configured level.

Configuring Event and Session Logging

Configuring event and session logging consists of some or all of the following tasks:

- Globally enabling system logging and configuring global logging properties
- Optionally, disabling logging of specific messages
- Optionally, changing the level of specific messages
- Optionally, configuring message event filters that will govern which system messages to send to particular destinations
- Configuring event destinations and specifying message filters that apply to each of those destinations

Configuring Global Logging Properties

To globally enable system logging and set general logging properties, navigate in ASDM to **Configuration > Device Management > Logging > Logging Setup**. The Logging Setup pane opens, as shown in Figure 6-5. In this pane, you can set several global logging properties.

In Figure 6-5, the Enable Logging check box is selected. This is necessary because, by default, all logging on the security appliance is disabled. Options within this same pane, none of which are selected in the figure, are as follows:

- **Enable logging on the failover standby unit:** Check this box to enable logging for a standby security appliance, if one exists. By default, if this box is not checked, only

severity level 1 messages are available on the standby unit (severity level 1 messages on the standby unit are related to failover events). Failover configurations are discussed in a later chapter.

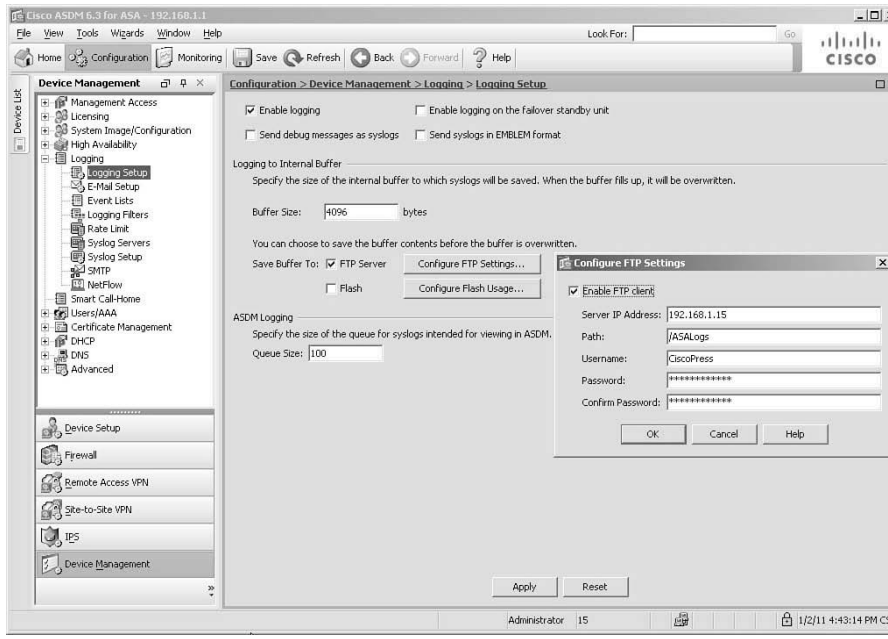


Figure 6-5 *Setting Global Logging Parameters*

- **Send debug messages as syslogs:** Check this box to redirect all debug output to system logs. By default, debug output is not included in system log messages. Checking this box redirects debug messages to logs as syslog message 711001, with severity level 7.
- **Send syslogs in EMBLEM format:** Check this box to enable Cisco EMBLEM format for all log destinations other than syslog servers. EMBLEM format is designed to be consistent with the Cisco IOS format. Many event management solutions will not recognize EMBLEM format messages, however. It is used primarily for the CiscoWorks Resource Manager Essentials (RME) Syslog Analyzer.

In Figure 6-5, the Buffer Size setting is left at the default of 4096 bytes (valid sizes are from 4096 to 1048576 bytes). This pertains to the internal buffer, maintained in memory. When this buffer gets full, it is overwritten in circular fashion, with each new message overwriting the oldest message in the buffer. If you do not want to lose information to these overwrites, there are two options for preserving buffered log messages: sending the buffer contents to an FTP server or saving them to internal flash memory. In Figure 6-5, the check box for FTP Server is checked, and the Configure FTP Settings button has been clicked, opening the Configure FTP Settings dialog box on the right side of the figure.

To enable saving of buffer contents to an FTP server, in the Configure FTP Settings dialog box, check the **Enable FTP Client** check box and configure information on the FTP server

address, directory path for storing buffer log contents, and a username and password used to log in to the FTP server. In Figure 6-5, a server is defined in the out-of-band (OOB) management network, at IP address 192.168.1.15; the /ASALogs directory of the FTP server is used for storage; the username is set to CiscoASA; and a password of CCNPSecurity is entered twice, the second time to verify it is entered correctly. Clicking OK would complete the FTP server definition.

If you were saving buffered log contents to internal flash memory, you would need to define two parameters: the maximum amount of flash memory to be used for storing log information, and the minimum free space to be preserved in flash memory. Selecting this option creates a directory named "syslog" on the device disk on which messages are stored.

Finally, Figure 6-5 leaves the default queue size of 100 for messages retained in the ASDM log buffer. The ASDM log buffer is a different buffer than the internal log buffer.

Once the FTP server window is completed and saved, clicking Apply in the Logging Setup pane will send the new settings to the security appliance.

The CLI commands generated by the changes made are as follows:

```
logging enable
logging ftp-bufferwrap
logging ftp-server 192.168.1.15 /ASALogs CiscoPress CCNPSecurity
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode.

Two other settings that are global for syslog messages are the syslog Facility Code and whether messages carry a time stamp when sent by the security appliance. These settings are not made in the same pane in which the other settings are made.

To modify these settings, navigate to **Configuration > Device Management > Logging > Syslog Setup**. This pane is shown in Figure 6-6. In the Syslog Format area, at the top of the pane, you can set the Facility Code and enable/disable time stamps.

In Figure 6-6, the default syslog Facility Code of LOCAL4(20) is left unchanged. Syslog Facility Codes are included in messages sent to syslog servers. The codes are used by syslog servers to organize event messages as they arrive. Eight logging facilities are available, LOCAL0 to LOCAL7 (if set in decimal only, 16–23). LOCAL4(20) is the default setting for all Cisco ASA syslog events. In the figure, the check box to enable time stamps is selected. Click **Apply** to send the change to the security appliance.

The CLI command generated by the change is as follows:

```
logging timestamp
```

If you are configuring the security appliance from the CLI, you can enter this command directly in global configuration mode.

Altering Settings of Specific Messages

Sometimes a default system message does not contain any useful information, or the default severity assigned to a message is not suitable to a particular environment. In such

cases, you can tune individual system messages by globally suppressing them or by altering their default severity. You tune these aspects in the Syslog Setup pane, also.

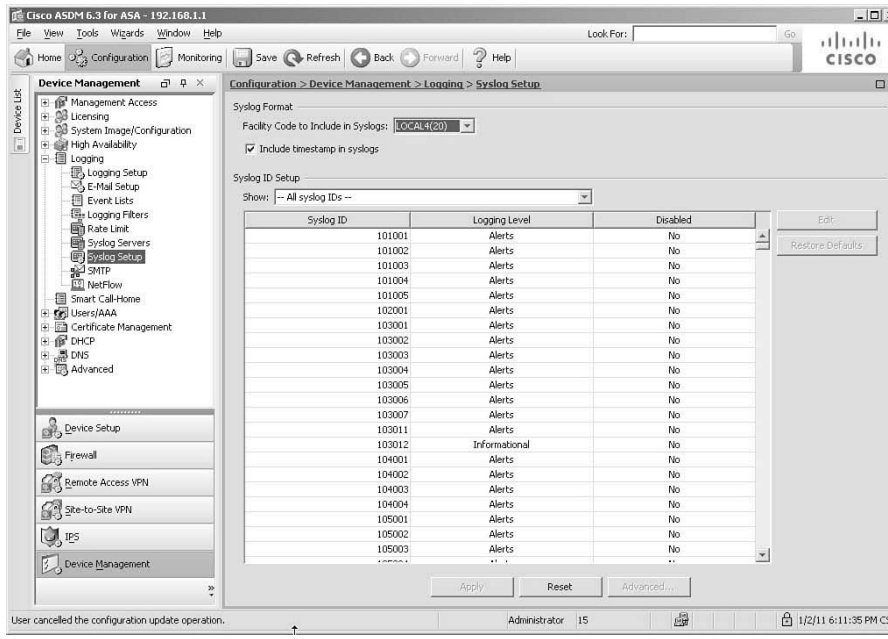


Figure 6-6 *The Syslog Setup Pane*

The Syslog ID Setup area comprises most of the Syslog Setup pane. The first option available is to change what message IDs are displayed in the main portion of this area. The default option is the display of all syslog message IDs. Other options available in the Show drop-down list are as follows:

- **Disabled syslog IDs:** Display only message IDs that have been explicitly suppressed.
- **Syslog IDs with changed logging:** Display only message IDs with severity levels that have been changed from their default values.
- **Syslog IDs that are suppressed or with a changed logging level:** Display all message IDs that have been modified by being suppressed or having their default level modified.

To modify a specific message ID, click the message to select it, and then click the **Edit** button to open the Edit Syslog ID Settings dialog box, shown in Figure 6-7. In this dialog box, you can suppress (disable) a particular message or change its configured logging level.

In Figure 6-7, message ID 113007 has been selected for editing, and the Disable Messages check box has been selected. Clicking OK will configure global suppression of this particular message. Message 113007 is generated when a locked user account is unlocked by an administrator, and in this scenario, it has been decided that this information is unimportant—what is important is to log when an account is locked for excessive incorrect password attempts.

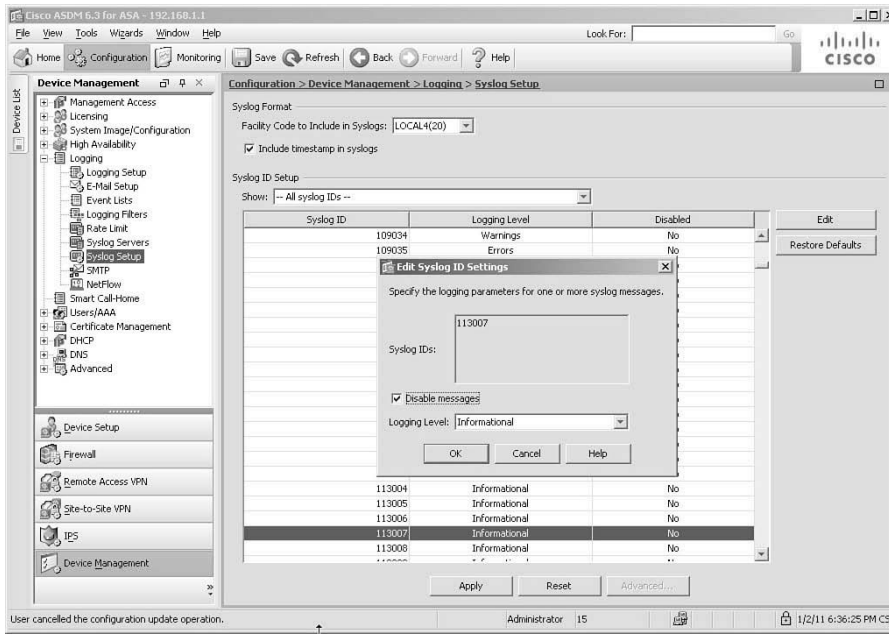


Figure 6-7 *Disabling a Message ID*

Note: There is a difference between suppressing a message ID and filtering it (covered later). If a message ID is disabled, the security appliance will not generate that particular message to any logging destination. Filtering a message is a means of not delivering a particular message to a particular logging destination, but the security appliance still generates the message, and can deliver it to other destinations.

There are also times when you may want to log a particular message ID, but alter the severity level at which it is reported. You do so from the same Edit Syslog ID Settings dialog box. Click a message to select it, and then click the **Edit** button. Figure 6-8 shows an example of modifying the severity level of a syslog message.

In Figure 6-8, message ID 106018 has been selected for modification. As you can see in the background, the default setting for this message ID is Critical (2). This particular message is generated if an ICMP packet is denied by an outgoing access list. Because outgoing filters do not exist by default on the security appliance, this means an administrator explicitly configured the security appliance to block such packets. However, given that an internal user generating a ping that is dropped by the security appliance would generate such a message, in this scenario it has been decided to alter the level from Critical to Notifications (5). Click **OK** to complete the modification of this message, and then click **Apply** to send these changes to the security appliance.

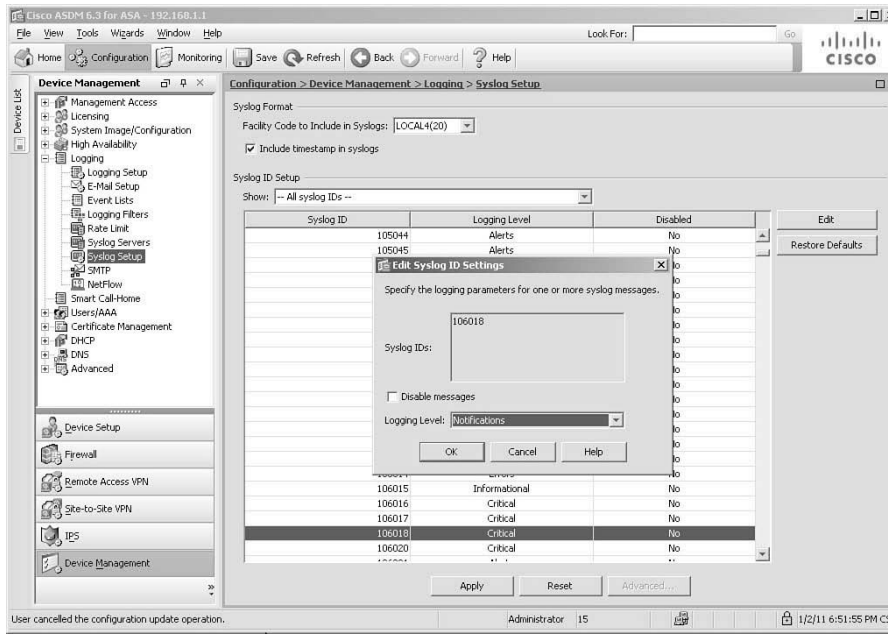


Figure 6-8 *Modifying a Syslog Message Severity Level*

The CLI commands generated by the changes made are as follows:

```
logging message 106018 level Notifications
no logging message 113007
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode.

Configuring Event Filters

For each logging destination, you can configure filters (known as *event lists*) that determine which subset of all generated messages will be forwarded to that destination. You can configure such filters based on the following:

- **Event (message) severity only:** For example, by specifying a maximum severity of 4 (Warnings), all messages with a severity of Warnings or higher (severity levels 0 to 4) would be forwarded to the logging destination. All messages with severities of 5 to 7 would be dropped.
- **Event classes:** All system messages are grouped into event classes based on the subsystem that created the messages. For example, there is an event class for the Authentication subsystem.
- **A combination of event class and event severity:** For example, all Authentication messages with a maximum severity of 4 (Warnings).
- **The message ID:** Each message has a unique message ID. Therefore, you can select individual messages for forwarding to particular logging destinations.

Event lists are reusable groups of messages, which can be selected by a combination of event class and severity, or individually by message ID. When you create an event list, you can apply that same event list to multiple logging destinations, thus simplifying the configuration of message filters.

To create an event list, navigate to **Configuration > Device Management > Logging > Event Lists**. Click **Add** to create a new event list. This opens the Add Event List dialog box, which is shown in Figure 6-9. You assign a unique name to each event list, and then configure the parameters that define your desired filter.

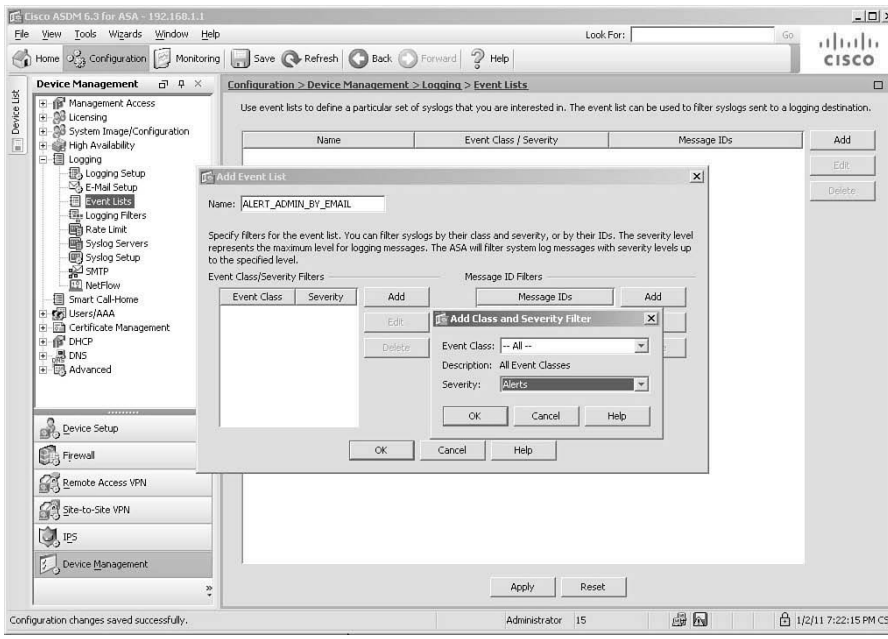


Figure 6-9 *Configuring an Event List*

In Figure 6-9, a name of ALERT_ADMIN_BY_EMAIL has been defined. The Add button in the Event Class/Severity Filters area was clicked to open the Add Class and Severity Filter dialog box, in which a specific class and severity can be defined. In this example, All Event Classes has been selected, and a severity level of Alerts (1) has been selected. In this scenario, it has been determined that any syslog message of severity 0 or 1 should generate an immediate email notification to an administrator (setup of the SMTP log destination is covered in the "Email" section of this chapter). This event list will accommodate such a configuration. Click **OK** twice to complete the configuration of the event class filter and the creation of the event list. Finally, click **Apply** to send the configuration to the security appliance.

The CLI command generated by the change is as follows:

```
logging list ALERT_ADMIN_BY_EMAIL level Alerts
```

If you are configuring the security appliance from the CLI, you can enter this command directly in global configuration mode.

Configuring Individual Event Destinations

After you have enabled logging globally, optionally set up global logging properties, and optionally configured event lists, you can configure the security appliance to send logging messages to one or more logging destinations. For each destination, you specify a filter that will select a subset of generated messages to be forwarded to that destination.

To configure logging destinations and filters, navigate to **Configuration > Device Management > Logging > Logging Filters**. In the Logging Filters pane that opens, you can activate logging to any of the eight available destinations and configure filters that determine which generated messages are forwarded to each.

Internal Buffer

The first example will be to configure the internal buffer as a logging destination. In the Logging Filters pane, select the **Internal Buffer** destination, and click **Edit** to open the Edit Logging Filters dialog box, shown in Figure 6-10.

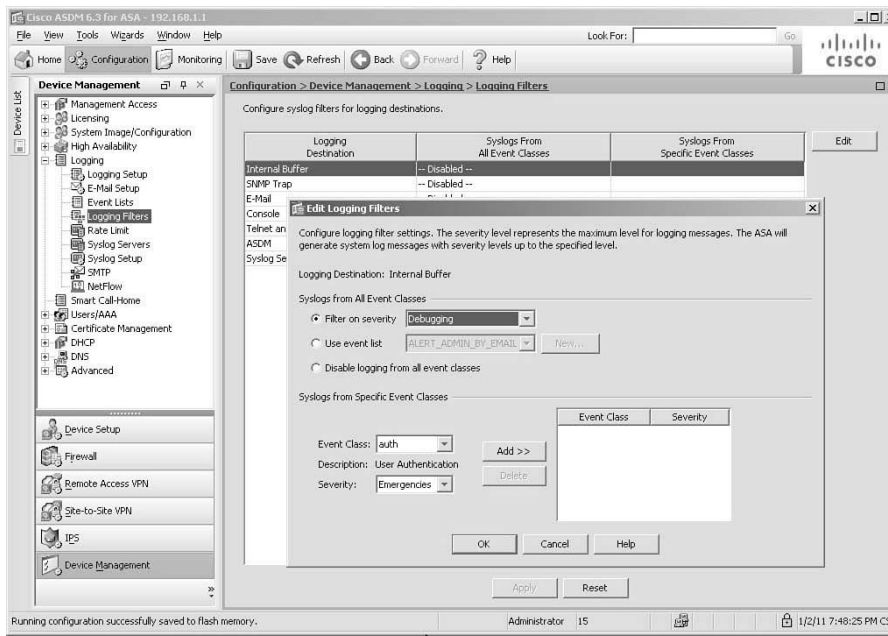


Figure 6-10 *Configuring the Internal Buffer Logging Filter*

As you can see in Figure 6-10, you have several options for determining the logging filter for a particular log destination. To create a filter that applies to all event classes, choose one of the following radio buttons in the top, Syslogs from All Event Classes area:

- **Filter on severity:** Filters system log messages by their severity level, and allows you to specify the level of messages that should be forwarded to the log destination. In Figure 6-10, this choice is selected, and the filter level is set to Debugging, which sends all system messages to the destination being configured (internal buffer). Depending on traffic, this particular choice can overwhelm the destination service (especially the console) or the user attempting to analyze events. You should carefully consider the impact of your choice before applying the configuration to the security appliance. If you wish to log all messages from all severity levels, it is strongly recommended that you do so to the internal buffer, and never to the console. In fact, it is generally recommended to leave console logging disabled.
- **Use event list:** Filters system log messages based on a previously defined event list, and allows you to specify which event list to use, or create a new event list.
- **Disable logging from all event classes:** Disables all forwarding of system messages to the destination being configured.

You can also create specific logging filters in this dialog box by entering the filter criteria in the Syslogs from Specific Event Classes area. This is equivalent to creating an event list for just this specific logging destination.

Click **OK** to complete the configuration of a logging filter to the internal buffer logging destination. Click **Apply** to send the modified settings to the security appliance.

The CLI command generated by the change made is as follows:

```
logging buffered Debugging
```

If you are configuring the security appliance from the CLI, you can enter this command directly in global configuration mode.

Note: A full log buffer can be saved to flash memory or transmitted to an FTP server for retention, as discussed in the earlier section "Configuring Global Logging Properties."

ASDM

Cisco ASDM contains a powerful event viewer that you can use to display a real-time message feed from the security appliance. This event viewer is particularly useful when you are troubleshooting security appliance software and configuration issues, or when you are monitoring real-time activity over the security appliance.

You enable logging to the internal ASDM event viewer by configuring the ASDM logging destination and specifying a logging filter, in the same manner as for other logging destinations. Messages are forwarded to ASDM over the HTTPS session and are displayed in a log viewer window at the bottom of the ASDM Home page.

This example assumes that the ASDM logging destination has been configured to receive messages from all event classes, containing a maximum severity level of Informational. Click **Apply** to send the modified settings to the security appliance.

The CLI command generated by the change made is as follows:

```
logging asdm Informational
```

If you are configuring the security appliance from the CLI, you can enter this command directly in global configuration mode.

Key Topic

To use the full event viewer functionality, start the viewer by navigating in ASDM to **Monitoring > Logging > Real-Time Log Viewer**, selecting a logging level, and clicking the **View** button. The ASDM Real-Time Log Viewer opens in a dedicated window and starts displaying log messages as selected by the configured message filter. Figure 6-11 shows an example of the Real-Time Log Viewer.

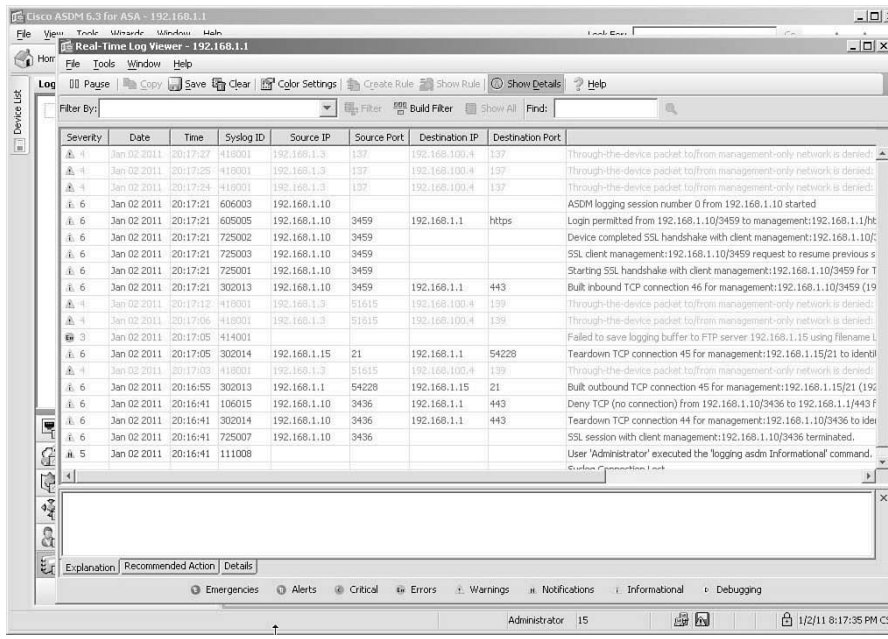


Figure 6-11 *Real-Time Log Viewer*

In the Real-Time Log Viewer, you can set additional keyword-based filtering by entering a keyword in the Filter By field in the log viewer toolbar. Above this field are toolbar icons that can be used to pause, resume, and clear the event display, copy individual messages to the clipboard, and set message colors.

The log viewer interface also allows you to select a particular message, and invoke various options by right-clicking it. You can, for example, show or even create specific access rules based on log messages. For example, if a log message showed that a packet had been denied by an access rule, you could immediately create a rule to allow such packets in the future. Or, for all session-related messages, you could right-click the interface and select Show Access Rule to jump immediately to the table of access rules and to the exact rule permitting or denying this particular connection.

At the bottom of the Real-Time Log Viewer, a context-sensitive help window shows message descriptions, recommends actions to administrators, and offers full message details. This is the only tool in ASDM that provides an administrator with such detailed explanations of log messages. Additionally, the suggestion of remedies is an invaluable aid in rapid troubleshooting and resolution of identified problems.

You can also use ASDM to view a snapshot of the current appliance internal log buffer, by navigating to **Monitor > Logging > Log Buffer**, selecting a maximum severity level, and clicking View.

Syslog Server(s)

Probably the most common destination to configure for log messages is one or more syslog servers in your network. Configuring the security appliance to send logs to syslog servers enables you to easily archive logs, limited only by the available disk space on the remote syslog server. You can specify up to 16 syslog servers as log destinations. Further, the security appliance can deliver syslog messages to servers using either UDP (standard syslog) or TCP (specialized for firewall syslog) as transport protocols.

Prior to ASA software version 8.0, all syslog messages were transferred in clear text. Beginning with software version 8.0(2), support was introduced for secure logging, using a SSL/TLS transport layer between the security appliance and syslog servers. Certificate-based authentication and encrypted data transfer help mitigate security threats to the logging service when messages are crossing an untrusted network. To use secure logging, you must set up an SSL/TLS connection between the security appliance and a remote syslog server supporting SSL/TLS. Also, the SSL syslog server must be added to the ASA as a certificate trust point. Configuration of secure logging is not covered in this book, but more information can be obtained from the *Cisco ASDM User Guide* available at Cisco.com.

When a security appliance is configured to use TCP-based syslog to at least one syslog server, by default, the security appliance will block all traffic attempting to go through the appliance if the TCP-based syslog server is down or unable to record further messages in its logs (that is, it is out of disk space). This feature is designed to prevent traffic from traversing a security appliance that is unable to log events, a common requirement in high-security networks. Use this feature if your local security policy requires this level of risk control.

To configure (non-SSL/TLS) syslog servers as log destinations, navigate to **Configuration > Device Management > Logging > Syslog Servers**. In the Syslog Servers pane, click **Add** to define a new syslog server log destination. The Add Syslog Server dialog box opens, as shown in Figure 6-12. Here, you define which interface the security appliance uses to reach the server, the server's IP address, whether to use TCP or UDP as the transport protocol, the destination port on the server, and, optionally, the use of EMBLEM format (only if using UDP) or SSL/TLS encryption (only if using TCP).

In Figure 6-12, a syslog server is defined, reachable through the management interface (in the OOB management network), using IP address 192.168.1.7, and standard UDP-based syslog transport to port 514 (the default UDP port; the default TCP port is 1470). Click **OK** to complete the configuration of this server.

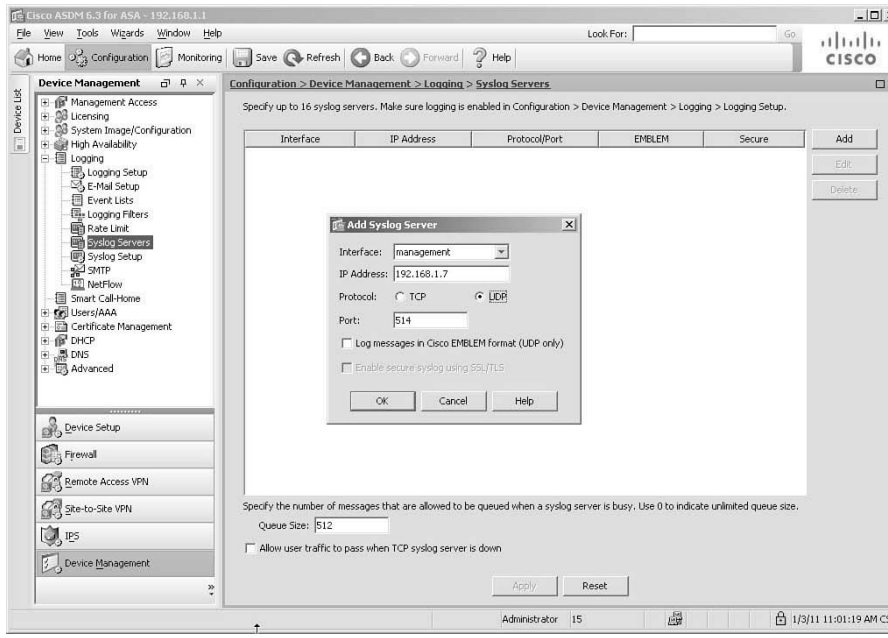


Figure 6-12 *Adding a Syslog Server Destination*

If you are using TCP-based syslog, you have the option to allow user traffic to traverse the ASA even when the TCP syslog server is down. To do so, in the main Syslog Servers pane, check the **Allow User Traffic to Pass when TCP Syslog Server Is Down** check box and then click **Apply** to send the new server definitions to the security appliance. Selecting this option generates the **logging permit-hostdown** command in the security appliance configuration.

After you have defined one or more syslog servers, you must configure a logging filter for the destination syslog servers, before the security appliance actually sends event messages to the configured servers. You do this the same way as covered previously. This example assumes that you have configured a logging filter to send all event classes, with a maximum severity of Warnings (4) to the logging destination of syslog servers.

The CLI commands generated by the changes made are as follows:

```
logging trap Warnings
logging host management 192.168.1.7
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode.

In most cases, using remote syslog servers as the primary method of reporting events to a central repository is recommended, as syslog is a widely supported and easily deployed logging protocol. Because UDP transport does not guarantee delivery, and should be used only over trusted or OOB networks, you should consider the use of TCP-based syslog when operating over a congested network subject to frequent packet loss. Also, consider

the use of SSL/TLS if you are using untrusted ("sniffable") transport networks between the security appliance and the syslog server.

Email

Sending log messages to an email system is useful, as it provides a simple way to integrate event notification with many messaging solutions, including simple email, mobile email, and SMS or pager systems, using appropriate gateways.

Configuring the security appliance to send email notifications is similar to configuring syslog servers, in that you must first define how the security appliance reaches intended recipients (sender and receiver addresses, SMTP servers, and so on), and then create a logging filter instructing the security appliance to use email as a logging destination and what events to send.

To configure email sender and recipient addresses, navigate to **Configuration > Device Management > Logging > E-Mail Setup**. Enter a source email address in the provided field, and then click the **Add** button to add recipient information. Figure 6-13 shows an example, where a source address of ASA@CiscoPress.CCNP has been entered in the Source E-Mail Address field.

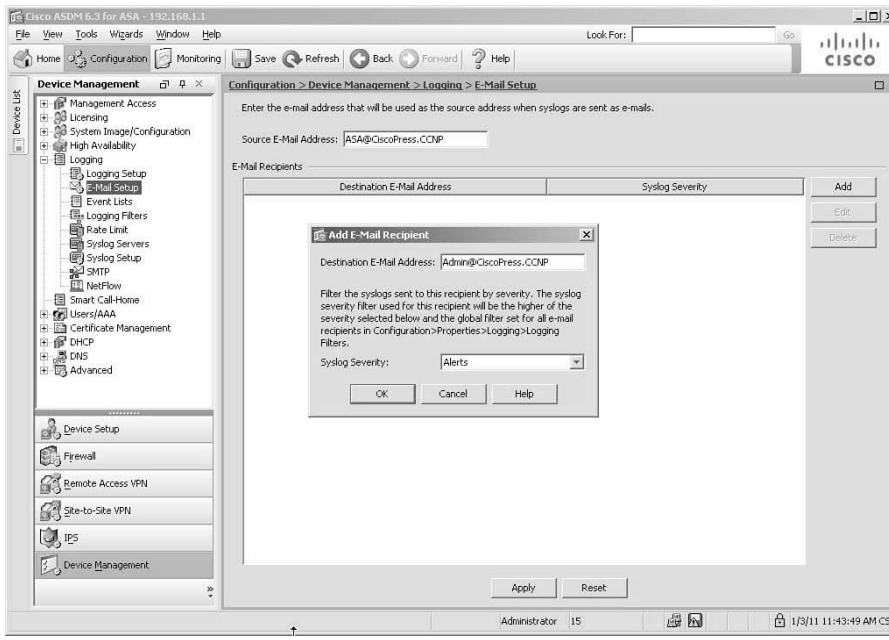


Figure 6-13 *Adding an Email Recipient*

In the Add E-Mail Recipient dialog box, the Destination E-Mail Address field has been completed with Admin@CiscoPress.CCNP as the recipient. Finally, the maximum severity of event messages that should generate an email to this recipient is configured in the Syslog Severity field, as Alerts.

After you have configured recipients, you must configure the security appliance with information about the SMTP server(s) through which the security appliance will send notifications. To do this, navigate to **Configuration > Device Management > Logging > SMTP**. The SMTP pane, as shown in Figure 6-14, is where you configure a primary and, optionally, secondary SMTP server address for the security appliance to send email through.

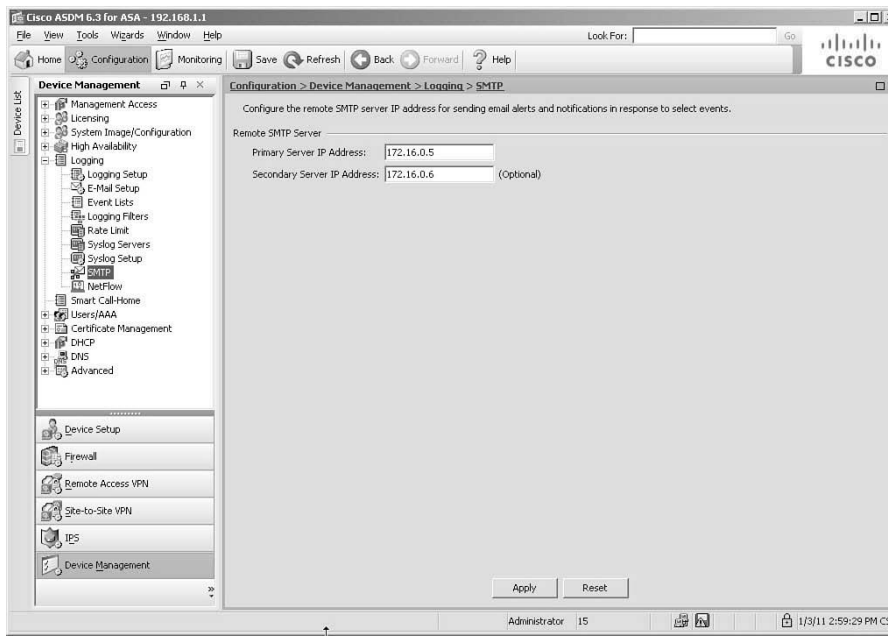


Figure 6-14 *Defining SMTP Servers*

Figure 6-14 shows an example where two SMTP servers on the DMZ network—172.16.0.5 as primary and 172.16.0.6 as secondary—are configured.

After configuring sender and recipient addresses and SMTP servers, you configure email notifications just like any other logging destination. In this example, however, rather than simply set a maximum severity for all event classes, Figure 6-15 shows the configuration of a logging filter for the E-Mail destination, using the previously created event list named ALERT_ADMIN_BY_EMAIL.

It is important to limit the amount of notifications sent via email, so use this destination only for exceptional events of critical importance. In this example, recall that event list ALERT_ADMIN_BY_EMAIL was defined with a maximum severity level of Alerts (1). This example might be overly restrictive, so use an appropriate level based on your local security policy.

Click **OK** in the Edit Logging Filters dialog box, and then click **Apply** in the Logging Filters pane, to complete the configuration of email as a logging destination.

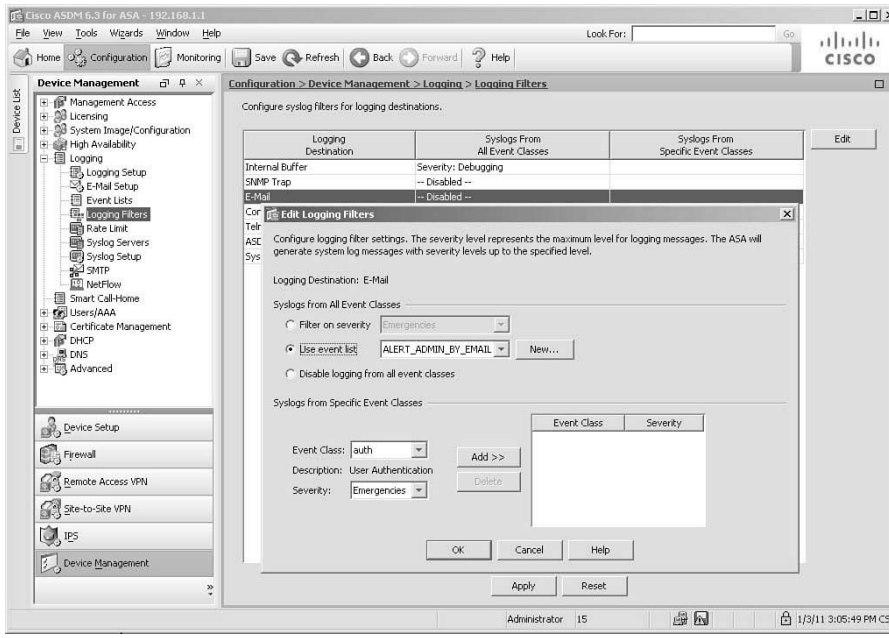


Figure 6-15 *Configuring Email Logging Filter*

The CLI commands generated by the changes made are as follows:

```
logging mail ALERT_ADMIN_BY_EMAIL
smtp-server 172.16.0.5 172.16.0.6
logging from-address ASA@CiscoPress.CCNP
logging recipient-address Admin@CiscoPress.CCNP level Alerts
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode.

NetFlow

To configure NSEL in the security appliance, you must first configure NetFlow export destinations by defining the location of NetFlow collectors. To do so, navigate to **Configuration > Device Management > Logging > NetFlow**. In the NetFlow pane, shown in Figure 6-16, you can configure NetFlow destinations, and also some options that might impact performance with NetFlow export enabled.

In Figure 6-16, a NetFlow collector has been defined through the management interface, with IP address 192.168.1.13, and the default NetFlow port of UDP 2055. Additionally, the option Delay Transmission of Flow Creation Events for Short-Lived Flows has been enabled, and the delay set to 10 seconds. Finally, because use of NetFlow makes some syslog messages redundant, the option to Disable Redundant Syslog Messages has been selected. (Neither of the preceding options is enabled by default.)

Defining flows to be exported to NetFlow collectors is unique among logging destinations. With NSEL, you can granularly select which flows through the security appliance

are exported using NetFlow, based on flow properties such as IP addresses, protocols, and ports. You configure this selection using Cisco Modular Policy Framework (MPF) service policies, which are covered in a later chapter.

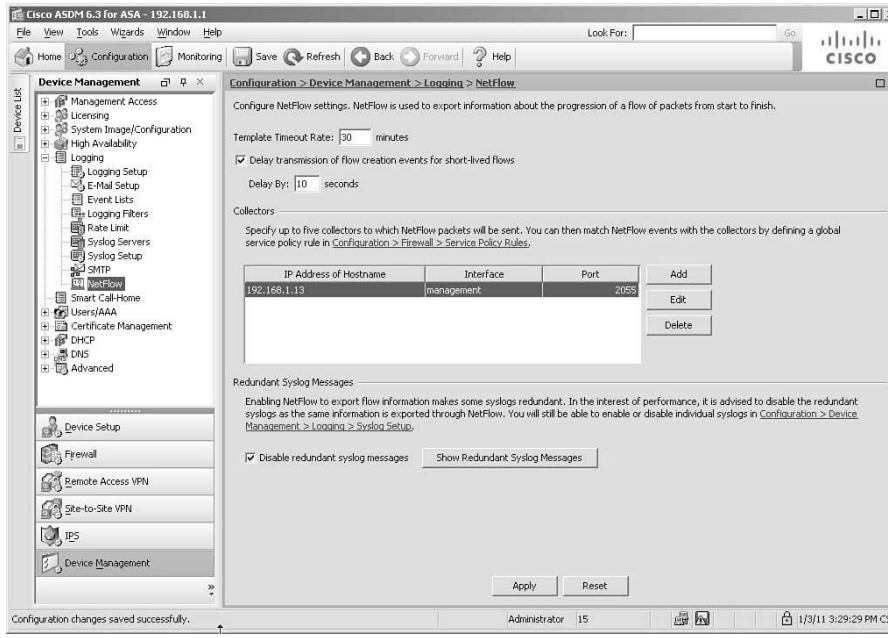


Figure 6-16 *Configuring NetFlow Settings*

The CLI commands generated by the changes made are as follows:

```
no logging message 106015
no logging message 106023
...output omitted...
flow-export delay flow-create 10
flow-export destination management 192.168.1.13 2055
```

If you are configuring the security appliance from the CLI, you can enter these commands directly in global configuration mode.

Telnet or SSH Sessions

To enable the security appliance to display system event messages in Telnet or SSH sessions, you can configure a logging filter for the Telnet and SSH Sessions destination, like any other destination. This generates the **logging monitor** command in the security appliance's configuration file. Although these messages are sent to the Telnet or SSH session, the user must also use the **terminal monitor** command to see the messages displayed in their remote terminal session.

Verifying Event and Session Logging

Only a few commands are used to verify the configuration and functionality of logging. Example 6-3 shows the use of the **show logging** command to see a summary of the logging configuration, along with any internally buffered log messages.

Example 6-3 *Verifying Logging*

```
FIREWALL# show logging

Syslog logging: enabled

    Facility: 20
    Timestamp logging: enabled

    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled

    Monitor logging: disabled
    Buffer logging: level debugging, 5548 messages logged
    Trap logging: level warnings, facility 20, 2145 messages logged
        Logging to management 192.168.1.7
    History logging: disabled
    Device ID: hostname "FIREWALL"
    Mail logging: list ALERT_ADMIN_BY_EMAIL, 0 messages logged
    ASDM logging: level informational, 802 messages logged
Jan 03 2011 16:10:13 FIREWALL : %ASA-7-609001: Built local-host
  management:192.168.1.15
Jan 03 2011 16:10:19 FIREWALL : %ASA-4-418001: Through-the-device packet to/from
  management-only network is denied: tcp src management:192.168.1.3/50388 dst out-
  side:192.168.100.4/22
Jan 03 2011 16:10:23 FIREWALL : %ASA-7-609002: Teardown local-host manage-
  ment:192.168.1.15 duration 0:00:10
...output omitted...
```

The output shows several important pieces of information, which are shaded for easy reference. Logging is globally enabled. Timestamps are enabled. Console logging is disabled, as it should be on production devices, except in rare circumstances. For each configured destination, you can see the number of logged messages. Additionally, if you are using a TCP syslog server, the connection from the ASA to the syslog server will be shown.

At the end of the configuration summary, you will see the full contents of the internal log buffer. This output is truncated here.

To verify NetFlow export operation, use the **show flow-export counters** command, as shown in Example 6-4. A non-zero packet count will prove that the security appliance is sending NetFlow v9 records to the configured NetFlow collector.

Example 6-4 *Verifying NetFlow Export*

```
FIREWALL# show flow-export counters

destination: management 192.168.1.13 2055
  Statistics:
    packets sent                                          14327
  Errors:
    block allocation failure                                0
    invalid interface                                       0
    template send failure                                   0
    no route to collector                                   0
```

Implementation Guidelines

When implementing event and session logging, consider the following implementation guidelines:

- Depending on the requirements of your local security policy, some events can be deleted, archived, or partially archived. This depends on the amount of event history available for online retrieval, the need for long-term reporting, and regulatory and legal requirements, which might require a specific retention period or, conversely, not allow certain types of personal information to be stored in an event database or event archives. Therefore, you should create a log retention policy that will enable you to store appropriate logs for an appropriate amount of time.
- It is generally best to log too much information as opposed to too little. Gathering too much information typically is harmless, unless it causes performance or capacity issues, whereas gathering too little information might prevent you from having information necessary to respond effectively to incidents or to meet regulatory requirements.
- Tune logging to exclude duplicate information. Some events might be redundant or not needed in your local environment. Make sure you analyze the event feed thoroughly to review and confirm these duplicates.
- Use multiple destinations for logging, to increase reliability of the information gathered.
- Try to handle boundary conditions, such as excessive event rate and lack of storage space, appropriately and without interruptions to service. Monitoring should be regularly tested and validated for accuracy, to ensure that changes to the system have not disabled desired functionality.
- Synchronize the security appliance clock to a reliable time source, to ensure trustworthy logging of time stamps.
- Transport events over the network using reliable and secure channels, if possible. Use a trusted network, or at least authenticate and verify the integrity of messages. To

ensure reliability and no packet loss, consider using TCP transport for log messages to remote servers.

- To provide the most scalable remote event export in high-connection-rate environments, consider using NetFlow instead of syslog to report on network events.
- Limit access to the security appliance logging subsystem (so that logging cannot be disabled without detection), the central event database, and long-term event archives. Implement mechanisms to prevent or detect changes to stored event data.
- Consider using an appliance-based logging server, especially when output from multiple sources will be collected, or where real-time event parsing along with event correlation might be required.

Troubleshooting Event and Session Logging

The recommended troubleshooting task flow when troubleshooting remote logging is as follows:

- For remote logging, verify mutual connectivity between the security appliance and the server using **ping**, **traceroute**, or similar tools.
- If you are using a TCP syslog server with a fail-closed policy (the default), use the **show logging** command (shown in Example 6-3) to determine if the host is reachable.
- Use **show logging** on the security appliance to determine the configuration of the event source. Verify logging filters to ensure that they are not filtering out desired event messages. You can also use the **capture** command to verify that events are actually being sent through security appliance interfaces. On the remote log destination, view stored logs and consider running a network analyzer to determine if events are arriving properly at the destination.
- Finally, there could be a performance problem at the security appliance that prevents it from sending messages to a destination. Use **show logging queue** (detailed in the next section) to examine the logging queue length and any drops, to determine if such a problem exists.

Troubleshooting Commands

Oversubscription of the logging queue indicates local performance issues. If you encounter oversubscription, consider logging less, rate-limiting a logging destination, tuning the logging queue, or using alternative logging methods such as NetFlow.

Example 6-5 shows the use of the **show logging queue** command to look for performance issues. A large number of discarded event messages is indicative of a logging subsystem performance problem.

Example 6-5 *Verifying Logging Queue Performance*

```
FIREWALL# show logging queue

        Logging Queue length limit : 512 msg(s)
        412366 msg(s) discarded due to queue overflow
        10 msg(s) discarded due to memory allocation failure
        Current 216 msg on queue, 512 msgs most on queue
```

The logging queue is where messages wait to be dispatched to their destinations. This queue is 512 messages long by default, but can be made larger or smaller. Rare drops due to queue overflow might not be indicative of a serious problem. Frequent drops due to queue overflow is a sign that the security appliance is not able to keep up with the number of messages being generated, and cannot dispatch them all to their intended destinations. If this occurs, first consider extending the size of the logging queue, using rate-limiting or more efficient logging methods (such as NetFlow), and reducing the amount of information being logged.

You can use the **logging queue** command to extend the size of the queue. Valid values range from 0 to 8192 messages. The following command doubles the size of the queue from the default value of 512 to a new value of 1024:

```
FIREWALL (config)# logging queue 1024
```

If a TCP-based syslog server is being used as a destination, with a fail-closed policy, and the server is not reachable, this will be indicated in the output of the **show logging** command, and will also appear as a recurring syslog message in an available destination (such as Internal Buffer or ASDM):

```
Jan 03 2011 18:49:56 FIREWALL : %ASA-3-414003: TCP Syslog Server manage-
ment:192.168.1.7/1470 not responding, New connections are denied based on logging
permit-hostdown policy
```

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 16, "Final Preparation," and the exam simulation questions on the CD-ROM.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-3 lists a reference of these key topics and the page numbers on which each is found.

Table 6-3 *Key Topics for Chapter 6*

Key Topic Element	Description	Page Number
Paragraph	Describes the NTP preference hierarchy	239
Paragraph	Explains how to configure NTP authentication	241
Section	Explains logging message format, including options	244
Table 6-2	Lists and defines message severity levels	244
Paragraph/Figure 6-6	Demonstrates how to enable logging time stamps	247–248
Paragraph	Explains use of the ASDM Real-Time Log Viewer	254
Paragraph	Explains use of TCP-based syslog servers	255

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It is not necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands, cover the right side of Tables 6-4 and 6-5 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

The FIREWALL exam focuses on practical, hands-on skills that are used by a networking professional. Therefore, you should be able to identify the commands needed to configure and test an ASA feature.

Table 6-4 *ASA Time-Related Commands*

Task	Command Syntax
Set system time	ciscoasa# **clock set** *hh:mm:ss* {*month day* | *day month*} *year*
Set system time zone	ciscoasa(config)# **clock timezone** *zone* [-]*hours* [*minutes*]
Set Daylight Saving Time parameters	ciscoasa(config)# **clock summer-time** *zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*] OR ciscoasa(config)# **clock summer-time** *zone date* {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]
Configure an NTP server	ciscoasa(config)# **ntp server** *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]
Enable NTP authentication	ciscoasa(config)# **ntp authenticate**
Set a key to authenticate with an NTP server	ciscoasa(config)# **ntp authentication-key** *key_id* **md5** *key*
Specify that a key is trusted (required for NTP authentication)	ciscoasa(config)# **ntp trusted-key** *key_id*
Display system time	ciscoasa# **show clock** [**detail**]
Display NTP associations	ciscoasa# **show ntp associations** [**detail**]

Table 6-5 *ASA Logging Configuration Commands*

Task	Command Syntax
Globally enable logging	ciscoasa(config)# **logging enable**
Configure save of buffered log to an FTP server before wrapping, and define an FTP server	ciscoasa(config)# **logging** ftp-bufferwrap ciscoasa(config)# **logging ftp-server** *ftp_server path username* [*0* | *8*] *password*
Include a time stamp on logged messages	ciscoasa(config)# **logging timestamp**
Include a device identifier on logged messages	ciscoasa(config)# **logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}
Disable a system message	ciscoasa(config)# **no logging message** *syslog_id*
Change the severity level of a system message	ciscoasa(config)# **logging message** *syslog_id* **level** *level*

Table 6-5 *ASA Logging Configuration Commands*

Task	Command Syntax
Create a logging list to be used with other commands	ciscoasa(config)# **logging list** *name* {**level** *level* [**class** *event_class*] | **message** *start_id* [*-end_id*]}
Log event messages to a particular destination	ciscoasa(config)# **logging** [**asdm** | **buffered** | **console** | **mail** | **monitor** | **trap**] [*logging_list* | *level*]
Define a syslog server	ciscoasa(config)# **logging host** *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**] [**permit-hostdown**]
Define an SMTP server	ciscoasa(config)# **smtp-server** {*primary_server*} [*backup_server*]
Configure source and destination email addresses	ciscoasa(config)# **logging from-address** *from-email-address* ciscoasa(config)# **logging recipient-address** *address* [**level** *level*]
Delay export of NetFlow flow-create events	ciscoasa(config)# **flow-export delay flow-create** *seconds*
Define a NetFlow collector	ciscoasa(config)# **flow-export destination** *interface-name ipv4-address | hostname udp-port*
Display log settings and buffered messages	ciscoasa# **show logging**
Display NetFlow counters	ciscoasa# **show flow-export counters**
Display logging queue statistics	ciscoasa# **show logging queue**
Adjust logging queue size	ciscoasa(config)# **logging queue** [*size*]

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q-R

S

T

U

V

W-X-Y-Z