Official
Cert Guide

Learn, prepare, and practice for exam success

CCNP Security VPN 642-648

- Master **CCNP Security VPN 642-648** 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

HOWARD HOOPER, CCIE® No. 23470

ciscopress.com

CCNP Security VPN 642-648

Official Cert Guide

Howard Hooper, CCIE No. 23470

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCNP Security VPN 642-648 Official Cert Guide

Howard Hooper CCIE No. 23470

Published by:

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

Printed in the United States of America

Second Printing September 2013

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

ISBN-13: 978-1-58720-447-0

ISBN-10: 1-58720-447-9

Warning and Disclaimer

This book is designed to provide information for the Cisco CCNP Security VPN 642-648 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

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 about 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.

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

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.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Compositor: Mark Shirar

Proofreader: Sarah Kearns

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editors: Chris Turpin, Cristian Matei

Development Editor: Eleanor C. Bru

Copy Editor: Keith Cline

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 Author

Howard Hooper, CCIE No. 23470, CCNP, CCNA, CCDA, JNCIA, works as a network consultant and trainer for Transcend Networks Ltd., specializing in network design, installation, and automation for enterprise and government clients. He has worked in the network industry for 10 years, starting his career in the service provider field as a support engineer, before moving on to installations engineer and network architect roles, working on small, medium, enterprise, and service provider networks. In his spare time, Howard is a professional skydiver and Cisco Academy instructor. When he is not freefalling from more than 13,500 feet at his local drop zone, he is teaching the CCNA syllabus at his local Cisco Academy.

About the Technical Reviewers

Chris Turpin, CCIE No. 17170, is a senior network consultant for Tomorrows Networks Limited. Chris has more than 15 years of experience in networking across a varied range of disciplines, including IP telephony, security, wireless, LAN switching, data center networking, and WANs. More recently, he has been responsible for the design and planning of secure, large-scale IP and MPLS networks worldwide, including in Australia, Europe, and the United States, with a particular focus on financial and service provider networks. He earned his Master's degree in astronomy and astrophysics from Newcastle University.

Cristian Matei, CCIE No. 23684, is a senior security consultant for Datanet Systems, Cisco Gold Partner in Romania. He has designed, implemented, and maintained multiple large enterprise networks covering the Cisco security, routing, switching, and wireless portfolio of products. Cristian started this journey back in 2005 with Microsoft technology and finished MCSE Security and MCSE Messaging tracks. He then joined Datanet Systems, where he quickly obtained his Security CCIE, among other certifications and specializations such as CCNP, CCSP, and CCDP. Since 2007, Cristian has been a Cisco Certified Systems Instructor (CCSI) teaching CCNA, CCNP, and CCSP curriculum courses. In 2009, he was awarded by Cisco with Cisco Trusted Technical Advisor (TTA) and got certified as Cisco IronPort Certified Security Professional on Email and Web (CICSP). That same year, he started his collaboration with Internetwork Expert as technical editor on the CCIE Routing & Switching and Security Workbook series. In 2010, Cristian earned his ISACA Certified Information Security Manager (CISM) certification. He is currently preparing for Routing & Switching, Service Provider CCIE tracks and can be found as a regular active member on Internetwork Expert and Cisco forums.

Dedications

I dedicate this book to my family and friends, without whom I would not be in the position that I am and have the opportunities I currently enjoy.

In particular, I want to say special thanks to the following:

My grandmother, Mary, for always taking the time to be there for others, making sure we always had what we needed and were happy, many times at her own personal sacrifice. I still miss you and miss being able to talk to you. I hope you would be proud of who I have become; one day we will meet again.

My stepfather, Nigel, one of the hardest working and knowledgeable people I know, for taking us in, providing for us, and becoming a father figure. Without you, I would not have been lucky enough to have the opportunities I have today or know the things I know. For this, I will always be thankful.

My sister, Angela, and brother in-law, Stuart, you have always been there day and night and have helped in a way that no one could even begin to imagine. For this, I will be eternally grateful and one day I hope I can repay the many favors.

My son, Ridley, I hope one day you can understand why I'm not around as much as I'd like to be. I want you to understand, though, that the times we have together are the ones I look forward to the most. Your happiness will always be the most important thing in my world. Daddy misses you and loves you very much.

Acknowledgments

When writing a book, a small army of people backs you up and undertakes a huge amount of work behind the scenes. I want to thank everyone involved who helped with the writing, reviewing, editing, and production of this book. In particular, I want to acknowledge Brett Bartow for giving me this fantastic opportunity and for his help with the many deadline extensions and obstacles that presented themselves along the way. I also want to acknowledge and thank Eleanor Bru, who worked tirelessly with myself and the technical reviewers to transform this manuscript into a book. I haven't made it easy and have kept you waiting; for this I apologize, but I thank you and will be forever grateful to both of you.

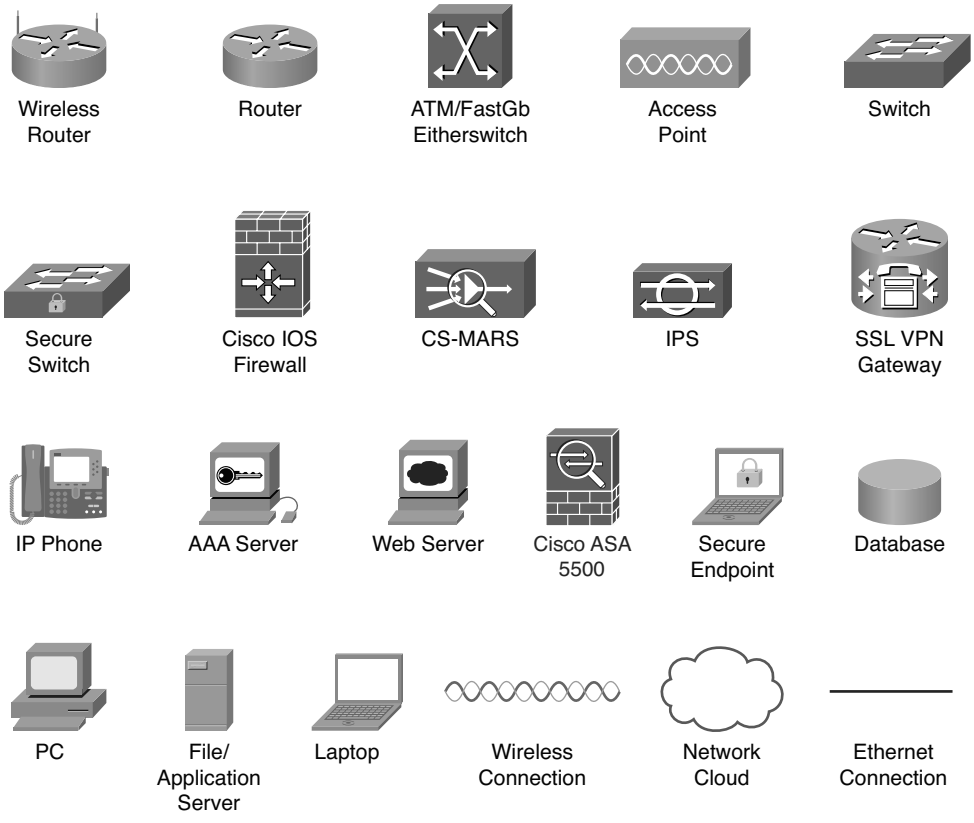
Thanks must also go out to the two technical reviewers, Chris Turpin and Cristian Matei. Your comments and suggestions have been a great help throughout the entire book. Your input has definitely made this version of the book better.

Last, but by no means least, I want to thank my family and co-workers for their support during the writing of this book. Without that support, this would not have been possible.

Contents at a Glance

Contents

Icons Used in This Book



Introduction

This book is designed to help you prepare for the CCNP Security VPN exam. This 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 Cisco IOS routers, switches, and *virtual private network (VPN)* devices.

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 VPN program was developed to introduce the remote-access and site-to-site VPN products associated with or integrated into the Cisco Adaptive Security Appliance (ASA) and available client software, explain how each product is applied, and explain how it can increase the security of your network. The VPN 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 22 chapters. Each chapter builds on the chapter that precedes it. The chapters that cover specific commands and configurations include case studies or practice configurations.

The chapters of the book cover the following topics:

- **Chapter 1, "Examining the Role of VPNs and the Technologies Supported by the ASA":** This chapter reviews the VPN operation and ASA architecture. It is this core of understanding that provides a good base for the other chapters.
- **Chapter 2, "Configuring Policies, Inheritance, and Attributes":** This chapter reviews the different methods used to apply policies and their contained attributes for controlling and ultimately securing our remote users. The policy inheritance model is also introduced to help network security personnel understand the results of having multiple policy types configured.
- **Chapter 3, "Deploying a Clientless SSL VPN Solution":** This chapter introduces you to the Cisco clientless *Secure Sockets Layer (SSL)* VPN implementation. In addition, we look at the configuration required for a basic deployment of an SSL VPN.
- **Chapter 4, "Advanced Clientless SSL VPN Settings":** This chapter reviews the advanced settings that are available for our clientless SSL VPN deployment and the available application access methods and their configuration.

- **Chapter 5, "Customizing the Clientless Portal":** This chapter reviews the available customization options we have when approaching the task of customizing our clientless SSL VPN environment for our remote users. We also discuss the implementation of *public key infrastructure (PKI)* and of double-authentication mechanisms.
- **Chapter 6, "Clientless SSL VPN Advanced Authentication and Authorization":** This chapter reviews the implementation and configuration of group policies and the available attributes contained within. We also discuss the available logging and accounting methods on the ASA.
- **Chapter 7, "Clientless SSL High Availability and Performance":** This chapter reviews the available HA and performance enhancements that can be deployed when working with clientless SSL VPN solutions.
- **Chapter 8, "Deploying an AnyConnect Remote-Access VPN Solution":** This chapter introduces you to the Cisco AnyConnect remote-access VPN configuration and client software. You learn how to configure a basic AnyConnect remote-access connection, along with the configuration required basic remote user authentication.
- **Chapter 9, "Advanced Authentication and Authorization of AnyConnect VPNs":** This chapter reviews the available mechanisms that can be configured to successfully authenticate your remote users. We take a closer look at PKI technology and its implementation as a standalone authentication mechanism, along with the steps required for successful deployment of PKI and username/password-based authentication (doubling up on authentication).
- **Chapter 10, "Advanced Deployment and Management of the AnyConnect Client":** This chapter reviews the various methods of the AnyConnect client deployment and installation available. In addition, we explore the various modules that are available and their benefits.
- **Chapter 11, "AnyConnect Advanced Authorization Using AAA and DAPs":** This chapter describes the role and implementation of advanced authorization, which enables us to maintain complete control over the resources our remote users can or cannot access before and during their connection to our VPN deployment. In addition, we review the role of *dynamic access policies (DAP)* and how their configuration can be used to enhance the authorization process.
- **Chapter 12, "AnyConnect High Availability and Performance":** This chapter reviews the different types of redundancy and high availability that you can deploy on the ASA device through configuration of the AnyConnect client or with external hardware.
- **Chapter 13, "Cisco Secure Desktop":** This chapter reviews the *Cisco Secure Desktop (CSD)* environment and associated modules for use with both the AnyConnect client and the clientless SSL VPN.
- **Chapter 14, "Deploying and Managing the Cisco VPN Client":** This chapter introduces you to the Cisco IPsec VPN client and its available methods of installation, configuration, and advanced customization.

- **Chapter 15, "Deploying Easy VPN Solutions":** This chapter introduces you to the Cisco Easy VPN client and server architecture. In addition, we review the configuration steps required for a basic Easy VPN deployment, XAUTH configuration, IP address assignment, and so on.
- **Chapter 16, "Advanced Authentication and Authorization Using Easy VPN":** This chapter covers the configuration of PKI and its subsequent implementation with Easy VPN deployments. It also covers certificate mappings and their role when used for advanced authentication purposes.
- **Chapter 17, "Advanced Easy VPN Authorization":** This chapter describes the implementation of group policies and the attributes that can be included to provide advanced authorization of our remote users. In addition, this chapter describes logging and accounting methods and their use with Easy VPN deployments.
- **Chapter 18, "High Availability and Performance for Easy VPN":** This chapter describes the mechanisms that can be put in place to provide a *high-availability (HA)* solution that will protect an organization from outages alongside an Easy VPN deployment.
- **Chapter 19, "Easy VPN Operation Using the ASA 5505 as a Hardware Client":** This chapter introduces you to the Easy VPN hardware client capabilities of the ASA 5505 device and the configuration required for successful deployment.
- **Chapter 20, "Deploying IPsec Site-to-Site VPNs":** This chapter introduces you to the IPsec site-to-site VPN solution available on the ASA devices and the configuration procedures required for a successful deployment.
- **Chapter 21, "High Availability and Performance Strategies for IPsec Site-to-Site VPNs":** This chapter examines the available HA mechanisms for use when providing hardware- and software-level redundancy with an IPsec site-to-site VPN deployment. We also review the available *quality of service (QoS)* mechanisms on the ASA and their associated configuration.
- **Chapter 22, "Final Exam 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, "642-648 CCNP Security VPN Exam Updates, Version 1.0":** This appendix provides you with updated information when 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 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/9781587204470.

- **Appendix C, "Memory Tables" (CD only):** This appendix, which you will find in PDF form on the CD accompanying this book, provides a series of tables that highlight some of the key topics in each chapter. Each table provides some cues and clues that will enable you to complete the table and test your knowledge about the table topics.
- **Appendix D, "Memory Tables Answer Key" (CD only):** This appendix, which you will find in PDF form on the CD accompanying this book, provides the completed memory tables from Appendix C so that you can check your answers. In addition, you can use this appendix as a standalone study tool to help you prepare for the exam.
- **Glossary:** 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 about 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 refers you to the memory tables appendixes, and 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, memory tables, and key terms, although they are good tools for last-minute preparation just before taking the exam.
- **Practice exam on the CD-ROM:** This book includes a CD-ROM containing an interactive practice exam. It is recommended that you continue to test your knowledge and test-taking skills by using this exam. 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. If you want to practice with additional questions, check out the Premium Edition eBook and Practice Test version of this book, which contains both eBook files and two additional practice exams. See the offer in the CD sleeve for more details.

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 they are published by Cisco. Coincidentally, these are the same topics required for you to be proficient when configuring Cisco security devices. 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 painful detail. The goal of this book is to prepare you as well as possible for the CCNP Security VPN 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 about a specific topic, feel free to surf. Table I-1 lists each exam topic along with a reference to the chapter that covers the topic.

Table I-1 *VPN Exam Topics and Chapter References*

Exam Topic	Chapter Where Topic Is Covered
Preproduction Design	
Choose ASA VPN technologies to implement *high-level design (HLD)* based on given requirements	1, 3, 8, 14, 15, 20
Choose the correct ASA model and license to implement HLD based on given performance requirements	1, 3, 8, 14, 15, 20
Choose the correct ASA VPN features to implement HLD based on given corporate security policy and network requirements	1–5, 8–10, 14–16, 19, 20
Integrate ASA VPN solutions with other security technology domains (CSD, ACS, device managers, cert servers, and so on)	1–5, 8–10, 14–20
Complex Operations Support	
Optimize ASA VPN performance, functions, and configurations	3–5, 7–10, 14–21
Configure and verify complex ASA VPN networks using features such as DAP, CSD, smart tunnels, AnyConnect SSL VPN, clientless SSL VPN, site-to-site VPN, remote-access VPNs, certificates, QoS, and so on to meet security policy requirements	3–10, 14–21

Exam Topic	Chapter Where Topic Is Covered
Create complex ASA network security rules using such features as access control lists (ACL), DAP, VPN profiles, certificates, Modular Policy Framework (MPF), and so on to meet the corporate security policy	4–6, 10–12, 14, 16, 17, 19
Advanced Troubleshooting	
Perform advanced ASA VPN configuration and troubleshooting	4–6, 8, 10–12, 14–21

You will notice that not all the chapters map to a specific exam topic. This is because of the selection of evaluation topics for each version of the certification exam. Our goal is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. To do this, we cover all the topics that have been addressed in different versions of this exam (past and present). Network security can (and should) be extremely complex and usually results in a series of interdependencies between systems operating in concert. This book shows you how one system (or function) relies on another, and each chapter of the book provides insight into topics in other chapters. 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 overall goal is to become a qualified network security professional.

Note that because security vulnerabilities and preventive measures continue apace, Cisco Systems 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 the Cisco Systems website to verify the actual list of topics to ensure that you are prepared before taking an exam. 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/9781587204470. It is 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 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 CCNP Security exam will give you a solid foundation that you can expand upon and use when working in the network security field.

The requirements for and explanation of the CCNP Security certification are outlined at the Cisco Systems website. Go to Cisco.com, hover over Training & Events, and select CCNP Security from the Certifications list.

Taking the VPN Certification Exam

As with any Cisco certification exam, it is best to be thoroughly prepared before taking the exam. There is no way to determine exactly which questions will appear 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 information available about Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking CCNP Security 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 re-sources, labs, and practice tests. This guide has integrated some practice questions and labs to help you better prepare. It is encouraged that you have hands-on experience with the Cisco ASA devices. There is no substitute for experience, and it is much easier to understand the commands and concepts when you can actually work with Cisco ASA devices. If you do not have access to a Cisco ASA device, you can choose from among a variety of simulation packages available for a reasonable price. Last, but certainly not least, Cisco.com provides a wealth of information about the Cisco ASA device, all the products that operate using Cisco ASA software, and the products that interact with Cisco ASA devices. No single source can adequately prepare you for the VPN exam unless you already have extensive experience with Cisco products and a background in networking or network security. At a minimum, use this book combined with the Technical Support and Documentation site resources (www.cisco.com/cisco/web/support/index.html) to prepare for this exam.

Assessing Exam Readiness

After completing a number of certification exams, we have found that you do not actually know whether you are adequately prepared for the exam until you have completed about 30 percent of the questions. At this 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. 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. You cannot go into a data center or server room without seeing some Cisco equipment. 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 clout. Cisco certifications demonstrate to potential employers and contract holders a certain professionalism and the dedication required to complete a goal. Face it, if these certifications were easy to acquire, everyone would have them.

Cisco ASA Software Commands

A firewall is not normally something to play with. That is, after you have it properly configured, you will tend to leave it alone until there is a problem or until you need to make some other configuration change. This is why the question mark (**?**) is probably the most widely used Cisco IOS and Cisco ASA software command. Unless you have constant exposure to this equipment, you might find it difficult to remember the numerous commands required to configure devices and troubleshoot problems. Most engineers remember enough to go in the right direction, but still use **?** to help them use the correct syntax. This is life in the real world. Unfortunately, the question mark is not always available in the testing environment.

Rules of the Road

We have always found it confusing when different addresses are used in the examples throughout a technical publication. For this reason, we use the address space defined in RFC 1918. We understand that these addresses are not routable across the Internet and are not normally used on outside interfaces. (Even with the millions of IP addresses available on the Internet, there is a slight chance that we might have used an address that the owner did not want published in this book.)

It is our hope that this will assist you in understanding the examples and the syntax of the many commands required to configure and administer Cisco ASA devices.

Exam Registration

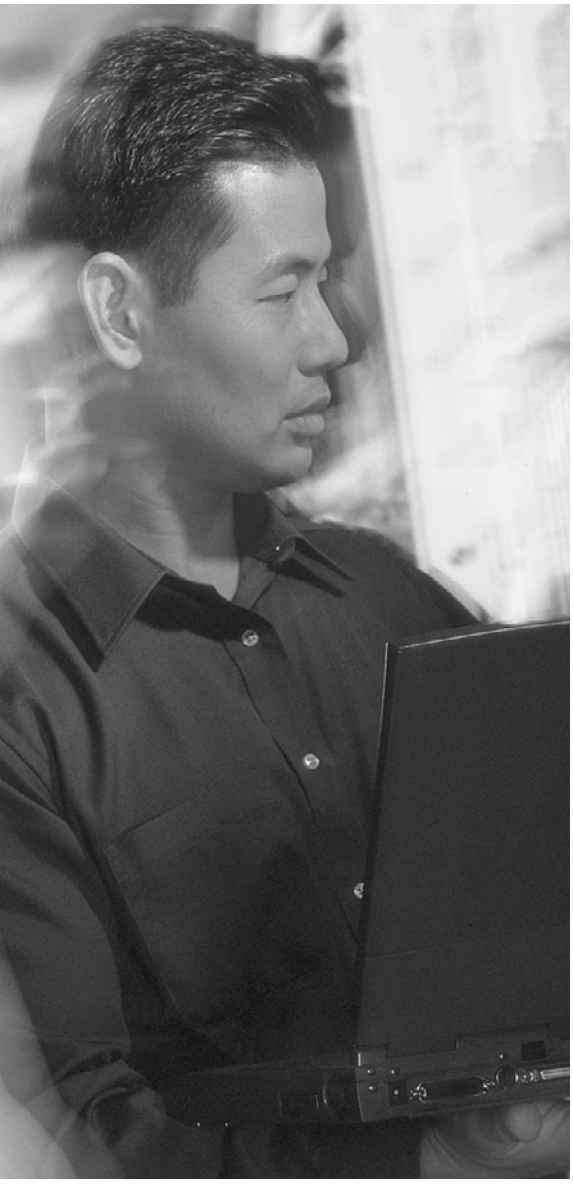
The VPN exam is a computer-based exam, with multiple-choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (www.pearsonvue.com) testing center. Your testing center can tell you the exact length of the exam. Be aware that when you register for 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 wants you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco Systems 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/9781587204470. 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.

Premium Edition eBook and Practice Test

This Cert Guide contains a special offer for a 70% discount off the companion *CCNP Security VPN 642-648 Official Cert Guide Premium Edition* eBook and practice test. The Premium Edition combines an eBook version of the text with an enhanced Pearson IT Certification practice test. By purchasing the Premium Edition, you get access to two eBook versions of the text: a PDF version and an ePUB version for reading on your tablet, eReader, or mobile device. You also get an enhanced practice test that contains an additional two full practice tests of unique questions. In addition, all the practice test questions are linked to the PDF eBook, allowing you to get more detailed feedback on each question instantly. To take advantage of this offer, you will need the coupon code included on the paper in the CD sleeve. Just follow the purchasing instructions that accompany the code to download and start using your Premium Edition today!



This chapter covers the following subjects:

- **Configuration Procedures, Deployment Strategies, and Information Gathering:** This section covers what to consider when deciding whether to deploy an internal AAA server for authorization.
- **Configuring Local and Remote Group Policies:** This section discusses the differences between ASA local and remote group policies and the configuration required on the ASA for the deployment of each.
- **Accounting Methods for Operational Information:** This section reviews the accounting methods available on the ASA for connection and user information gathering.

CHAPTER 17

Advanced Easy VPN Authorization

In earlier chapters, you learned how to plan for and configure the various authentication mechanisms available on the *Adaptive Security Appliance (ASA)* to allow remote users access into your environment. Now that you have given them access, you need to control and account for it.

The information in this chapter will enable you to prepare for the deployment of an advanced authorization scheme for your remote users, allowing you to control the level of access granted to them based on such information as their internal department, username, IP address, and so on, using the familiar local group policies that are configured on the ASA device. This chapter also introduces you to remote group policies, their configuration on the ASA, and their remote server requirements.

After the various ways to authorize remote users into your environment has been explored, the discussion moves on to review the accounting methods available on the ASA device that enable you to track the success or failure of specific authorization settings and connections.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you determine your level of knowledge on this chapter's topics before you begin. Table 17-1 details the major topics discussed in this chapter and their corresponding quiz sections.

Table 17-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Configuring Local and Remote Group Policies	1, 2, 3, 4
Accounting methods for Operational Information	5, 6, 7

1. Which of the following are available group policy types on the ASA? (Choose all that apply.)
   a. Internal
   b. External
   c. Active
   d. Standby
2. Which of the following are legitimate ways to assign a group policy? (Choose all that apply.)
   a. DAP
   b. Direct user assignment
   c. Connection profile
   d. AAA
3. In what format are the attributes stored in an external group policy?
   a. Text files
   b. A/V pairs
   c. CSV files
   d. XML files
4. Which of the following remote user types are external group policy objects available on? (Choose all that apply.)
   a. LDAP
   b. TACACS+
   c. SDI
   d. RADIUS

5. By default, where is ASA syslog information stored?

   a. External syslog server

   b. Internal syslog server

   c. NetFlow collection service

   d. ASA internal buffer

6. When configuring an AAA server on the ASA, which communication protocol when configured allows for secure (SSL/TLS) communication between the AAA server and the ASA?

   a. UDP

   b. SCEP

   c. SMTP

   d. TCP

7. Which of the following are available actions used for NetFlow flow information creation? (Choose all that apply.)

   a. Created

   b. Denied

   c. Torn down

   d. Dropped

Foundation Topics

Configuration Procedures, Deployment Strategies, and Information Gathering

The role of authorization in any *virtual private network (VPN)* deployment is an important one. With it, you can control which of your remote users can or cannot access corporate servers, email, financial and personnel records, and even the Internet. However, not only can you control the level of access each remote user has in your corporate environment, you can also control the user's connection experience through maximum connection times, timeout settings, simultaneous logins, portal customization, and so on.

You can restrict or allow access to specific internal resources from remote users using the available policy options on the ASA device, whether you allow full access from all remote users to all of your internal resources (really not recommended) or, as shown in Figure 17-1, you provide remote users access to only the internal resources they require. (For example, Client A can access the corporate finance server and file server but not the corporate email server, but Client B can access the corporate email server and file server but not the corporate finance server.) Specifically, this chapter focuses on the role of group policies for user authorization purposes, and as you will see in the next section, you can assign IPv4 and IPv6 access lists in group policy objects that allow or deny access to internal servers for a particular group, access hours, maximum connection time, and so on.

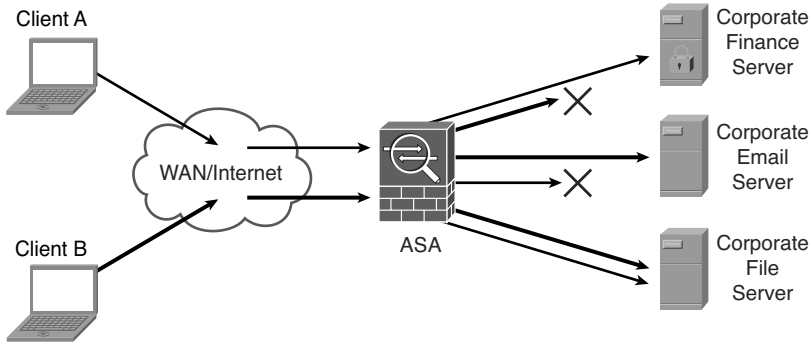


Figure 17-1 *ASA Authorizing (or Not) Remote Users*

In addition to the available authorization attributes that can be applied by local group policies to remote users, you can extend the role of authorization to a remote (internal) *authentication, authorization, and accounting (AAA)* server. After the remote user has been authenticated, the remote AAA server is queried for the authorization attributes that should be applied to their session.

Configuring Local and Remote Group Policies

Via group policies, you can assign attributes to users and groups based on their individual user account, group membership, or the connection profile used to connect to the ASA device.

Using group policy objects, you can define the following user authorization settings (and many more, as discussed momentarily):

- Set the maximum connection time applied to remote users before they are required to carry out the connection process and reauthenticate.
- Control the number of simultaneous logins that can be made using the particular user account.
- Restrict access only to the internal resources and subnets using IPv4 filters (*access control lists [ACL]*).
- Define the networks used for split tunneling.
- Control remote user access hours (the time they can and cannot log in).

Recall from the information shown in Chapter 2, "Configuring Policies, Inheritance, and Attributes," covering group policies, you can configure two types of group policy objects. The location of the policy attributes contained in them dictates the type of policy it is:

- **Local group policies** (also known as internal group policies) are policy objects that have been configured locally on the ASA along with the attributes they contain. They are assigned either to local users directly (local user accounts configured on the ASA) or in connection profiles.
- **Remote group policies** (also known as external group policies) are applied either to remote users or groups. The attributes contained in a remote group policy are configured on a remote (typically internal) AAA server (for example, RADIUS or *Lightweight Directory Access Protocol [LDAP]*) in the form of *attribute/value (A/V)* pairs. However, the remote group policy container (name) must also be configured on the ASA device, even though authorization attributes are imported from the AAA server.

Local group policy and the remote group policy containers are both configured on the ASA using the **group-policy** *name* [**internal | external**] global configuration command via the *command-line interface (CLI)* or within **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** if you have chosen to use the *Adaptive Security Device Manager (ASDM)* for configuration purposes. Within the ASDM, begin by clicking **Add**. Then, from the Add menu, choose either **Internal Group Policy** or **External Group Policy**. For this example, as shown in Figure 17-2, the Add External Group Policy option was selected.

Figure 17-2 *External Group Policy Configuration*

In the Add External Group Policy window, enter the following details:

- **Name:** Enter a name for the group policy object. This is the actual username used by the ASA and configured within the RADIUS server's database for authentication purposes between the ASA and the RADIUS server.
- **Server Group:** Choose an existing AAA server group or create a new one.
- **Password:** Enter a password to be used for authentication with the AAA servers. This is the password configured for the previously defined username also used for the group policy name.

The group policy object is then used as a container for the A/V attributes received from the internal AAA server. Example 17-1 displays the configuration of an external group policy object when working from the CLI.

Example 17-1 *External Group Policy Object Configuration*

```
CCNPSec# conf t
CCNPSec(config)# group-policy Remote_EzVPN_Policy external server-group
 RADIUS password security
```

If you want to create a new AAA server group instead of selecting an existing one, you can choose **New > New RADIUS Server Group** or **New > New LDAP Server Group** in the ASDM's Add External Group Policy window. After choosing the appropriate server group type to create, enter the following information into the Add AAA Server Group window:

- **Server Group:** Enter a name for the server group.
- **Protocol:** Uneditable. This displays either RADIUS or LDAP depending on your chosen group.

- **Accounting Mode:** Choose either Simultaneous (the ASA sends accounting data to all servers in the group) or Single (the ASA sends accounting data to only one server); this option is not available for LDAP server groups.
- **Reactivation Mode:** Choose either Depletion (servers that have failed in the group are only reactivated when all other servers in the group are inactive) or Timed (failed servers are reactivated after 30 seconds). If you choose Depletion, you can also modify the dead timer (default 10 minutes), which is time that elapses between disabling the last server in the group and the reenabling of all servers.
- **Max Failed Attempts:** Enter the maximum number of attempts that will be used to connect to a server configured in the server group until declaring it dead; the default is 3.
- **Enable Interim Accounting Update:** Choose this option to enable multisession accounting for both AnyConnect and clientless *Secure Sockets Layer (SSL)* VPNs.
- **Enable Active Directory Agent mode:** Not relevant for VPN configuration, but it is related to the identify firewall feature.
- **VPN3K Compatibility:** Choose Do Not Merge (to disable merging of RADIUS downloadable ACLs with received A/V pair ACLs), Place the Downloadable ACL After the Cisco AV Pair ACL, or Place the Downloadable ACL Before the Cisco AV Pair ACL.

After creating your new AAA server group, you then need to add AAA servers to it in the AAA Server Groups window (**Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**), as shown in Figure 17-3. Note that for this configuration to be fully usable and valid, configurations on the remote LDAP or RADIUS servers need to be performed. (LDAP and RADIUS configuration is beyond the scope of this book.)

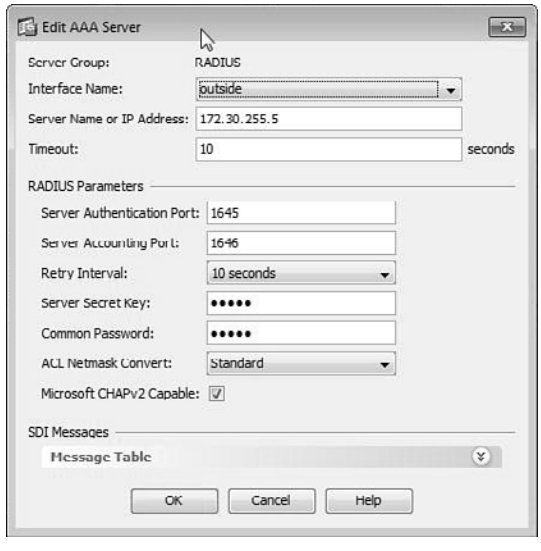


Figure 17-3 *AAA Server Configuration*

Example 17-2 displays the commands required to create a new AAA server group and add a new external server to the group.

Example 17-2 *Creating a New AAA Server Group and Adding an External Radius Server*

```
CCNPSec# !!First create your new AAA server group ready to add your exter-
 nal AAA server!!
CCNPSec# conf t
CCNPSec(config)# aaa-server RADIUS protocol radius
CCNPSec(config-aaa-server-group)# !!Now enter the details of your AAA
 server and add it to the new group!!
CCNPSec(config-aaa-server-group)# exit
CCNPSec(config)# aaa-server RADIUS (outside) host 172.30.255.5
CCNPSec(config-aaa-server-host)# key security
CCNPSec(config-aaa-server-host)# radius-common-pw security
```

When creating a new internal group policy object using the CLI, use the global configuration command **group-policy** *name* **internal from** *name*. The **from** *name* options available with the command are optional enable you to specify an existing group policy object that can be used as a template and its settings copied from. After you create the group policy object, you can enter the **group-policy** *name* **attributes** to set any specific attributes required using the commands shown in Table 17-2 in group policy attributes configuration mode.

When using the ASDM, click **Add > Add Internal Group Policy** to open the Add Internal Group Policy window, shown in Figure 17-4. As you can see, many more options are available for this configuration, because all attributes of the group policy are configured and stored on the ASA. Begin by giving the policy a name, which is the only mandatory attribute required when configuring a new policy. All other attributes are by default inherited from the default group policy object (DfltGrpPolicy).

Table 17-2 lists the General window fields and values that you can use to configure the remaining general attributes you want to set explicitly. In addition, the table includes the corresponding CLI commands in case you have chosen to configure your ASA using the CLI. Note that before configuration is possible, you must uncheck the respective field's **Inherit** option. However, you do not have to do so when you are using the CLI to configure the attributes; as soon as you configure a setting, the default inheritance is overridden.

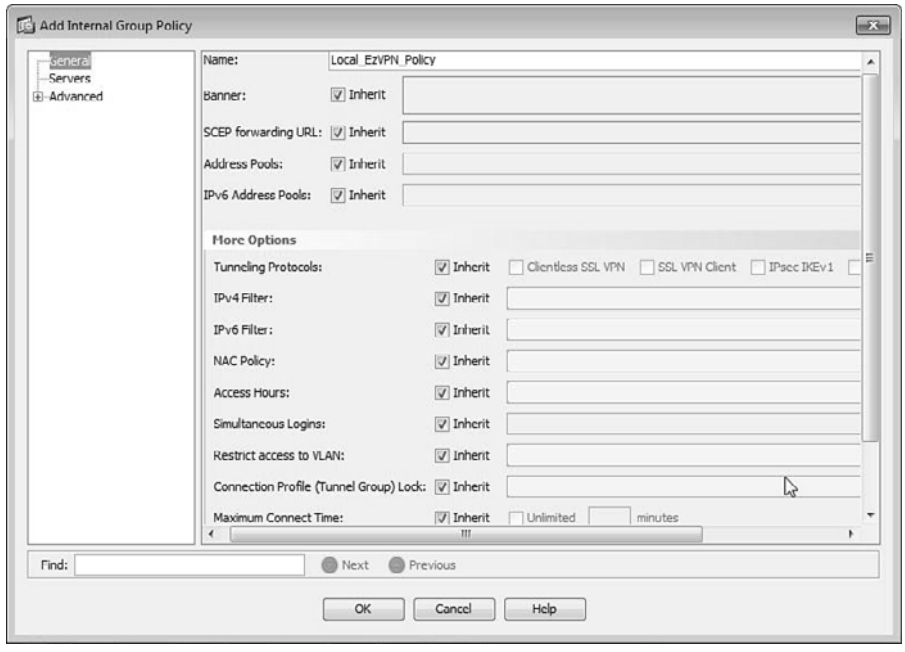


Figure 17-4 *Internal Group Policy Configuration*

Table 17-2 *Internal Group Policy Attributes*

Field	CLI Commands	Value
Banner	**banner value** *enter up to 500 characters*	Enter a banner that will be displayed to users as they attempt to connect to the VPN.
SCEP Forwarding URL	**scep-forwarding-url value** *url*	Enter the URL that users of this group policy will use to automatically request digital certificates (if using certificate-based authentication).
Address Pools	**address-pools value** *enter up to 6 address pools separated by a space*	Choose an IP address pool from the list. An IP address will be assigned to users for use during their connection.
IPv6 Address Pools	**ipv6-address-pools value** *enter up to 6 address pools separated by a space*	Select an IPv6 address pool from the list. An IP address will be assigned to users for use during their connection.
Tunneling Protocols	**vpn-tunnel-protocol [ikev1 | ikev2 | l2tp-ipsec | ssl-client | ssl-clientless]**	Choose from the available tunneling protocols that this group policy object will apply to.

Field	CLI Commands	Value
IPv4 Filter	**vpn-filter value** *acl name*	Select an IPv4 ACL from the list to restrict network access during the user's connection to only the networks/hosts the user requires.
IPv6 Filter	**ipv6-vpn-filter value** *ipv6 acl name*	Choose an IPv6 ACL from the list to restrict network access during the user's connection to only the networks/hosts the user requires.
NAC Policy	**nac-policy** *policy name*	Select a *Network Access Control (NAC)* policy from the list of those configured. The NAC policy is used to perform posture assessment and validation for the connecting user.
Access Hours	**vpn-access-hours value** *time-range name*	Choose a time range from those previously configured if you only allow access to this connection during specific times (for example, regular business hours).
Simultaneous Logins	**vpn-simultaneous-logins** *0-2147483647*	Enter the number of simultaneous logins that can appear for this user account. (The default is 3.) A value of 0 prevents any logins from occurring, and remote users are unable to gain VPN access.
Restrict Access to VLAN (5505 Only)	**vlan** *vlan id*	Choose the only VLAN (Inside, Outside, DMZ) you will allow this connecting user access to. The default value is None.
Connection Profile (Tunnel Group) Lock	**group-lock value** *connection profile*	Choose the connection profile from the list. This group policy object will only be assigned to the selected connection profile. This setting basically makes the group policy usable only by a certain connection profile.
Maximum Connect Time	**vpn-session-timeout** {**none** | *1-4473924*}	Choose either Unlimited or enter the number of minutes the user is allowed to be connected before being automatically disconnected. (The default is Unlimited or None.)
Idle Timeout	**vpn-idle-timeout** {**none** | *1-35791394*}	Choose either Unlimited (value of None) or enter the number of minutes the user's connection can be idle before being automatically disconnected. (The default is 30 minutes.)
On Smart Card Removal	**smartcard-removal-disconnect** [**enable** | **disable**]	Choose the option to either keep the user's connection connected or disconnect the connection upon the user removing her smart card.

After setting the specific general attributes required in your local group policy, you can assign the policy either directly to a local user account or globally to all users of a connection in the connection profile's properties.

Assigning a Group Policy to a Local User Account

Begin this task by entering the user attributes configuration mode using the **username** *name* **attributes** global configuration command. Within this mode, you can apply the group policy using the **vpn-group-policy** *policy name* command, as shown in Example 17-3.

Example 17-3 *Assigning a Group Policy Directly to a User*

```
CCNPSec# conf t
CCNPSec(config)# username EzUser1 attributes
CCNPSec(config-username)# vpn-group-policy EasyVPN
```

When using the ASDM, start by opening your user's account properties in **Configuration > Remote Access VPN > AAA/Local Users > User Accounts**. In the User Accounts window, choose the local user account to apply the group policy object to and click **Edit**.

As shown in Figure 17-5, in the Edit User Account window that opens, we choose **VPN Policy** from the menu on the left and uncheck the **Inherit** check box next to the Group Policy section. Using the drop-down list, we then choose the group policy object we want applied to the user account.

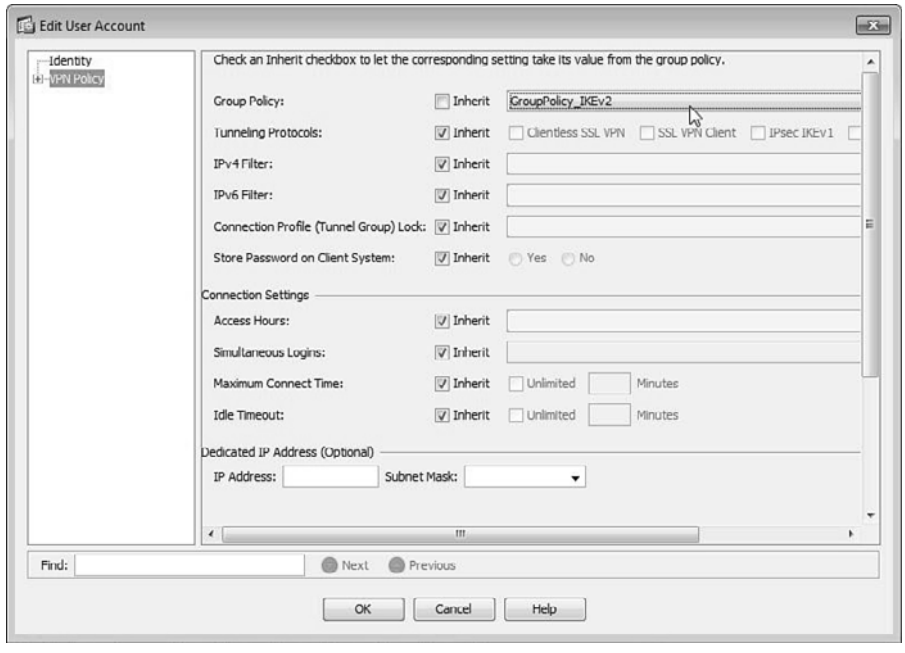


Figure 17-5 *Assigning a Group Policy Directly to a User*

Assigning a Group Policy to a Connection Profile

Key Topic

You can assign a group policy object to a connection profile using the CLI of ASDM. Via the CLI, issue the **default-group-policy** *policy name* command within tunnel-group general-attributes configuration mode. Alternatively, open the ASDM connection profile properties window by navigating to **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv1) Connection Profiles**. Select the connection profile to assign the group policy object to from the list and click **Edit.**

In the Edit IPsec Remote Access Connection Profile *Name* window, use the drop-down list in the Default Group Policy section of the window to select the group policy object to be applied, as shown in Figure 17-6.

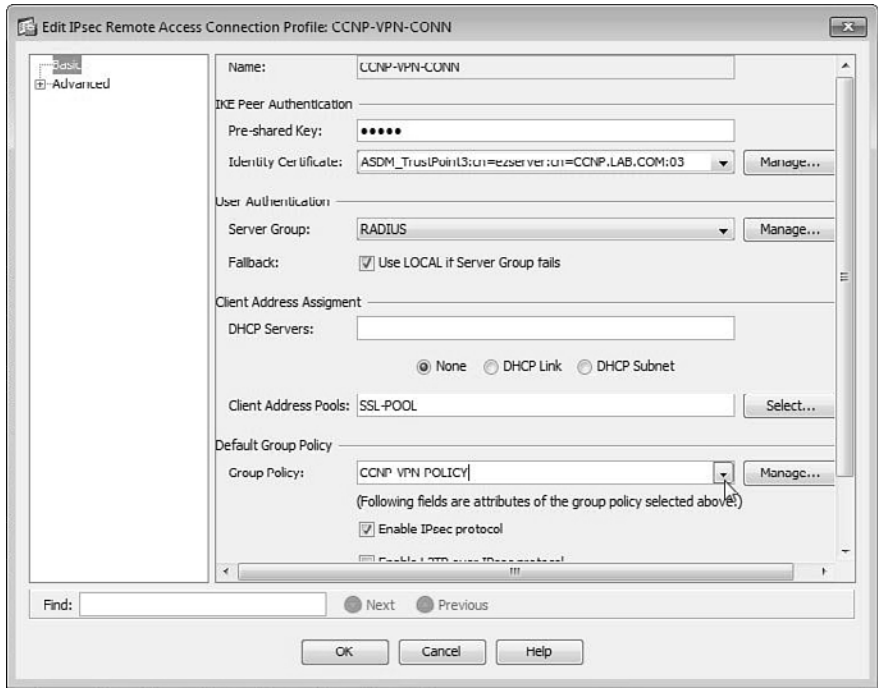


Figure 17-6 *Assigning a Group Policy to a Connection Profile*

In addition to the more general properties that you can assign using a group policy object, you can assign advanced properties (for example, split-tunneling exceptions and rules).

The configuration in Figure 17-7 shows the split-tunneling properties located in the **Advanced > Split Tunneling** section of the Edit Internal Group Policy - *Name* window.

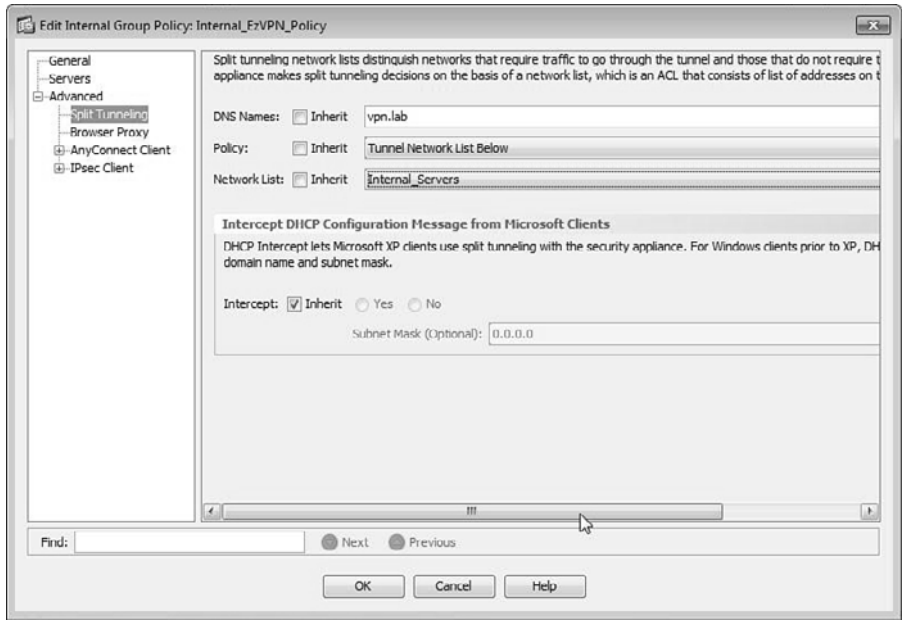


Figure 17-7 *Group Policy Split-Tunneling Configuration*

For this example, the domain name vpn.lab has been added as a *Domain Name System (DNS)* name, indicating to the Easy VPN clients that any requests for DNS information for hosts in this domain should be tunneled (for example, secretfiles.vpn.lab). In addition to the configuration of DNS names, the option to tunnel only the list specified in the preconfigured ACL Internal_Servers by using the Policy and Network List fields has been configured. Example 17-4 displays the same configuration achieved via the CLI.

Example 17-4 *Configuring Split Tunneling*

```
CCNPSec# conf t
CCNPSec(config)# group-policy Internal-EzVPN-POLICY attributes
CCNPSec(config-group-policy)# split-tunnel-policy tunnelspecified
CCNPSec(config-group-policy)# split-tunnel-network-list value Internal_
 Servers
CCNPSec(config-group-policy)# default-domain value VPN.LAB
```

The configuration shown in Figure 17-7 and Example 17-4 results in DNS requests for devices in the domain name vpn.lab, or traffic matching that of the ACL Internal_Servers, to be sent by Easy VPN clients through the VPN tunnel to the ASA and on to the corporate network. All other traffic (for example, the remote user device's LAN or Internet data) travels directly to the destination rather than through the VPN tunnel.

Accounting Methods for Operational Information

You have at your disposal the following logging mechanisms on the ASA to monitor remote user activity and connection state:

Key Topic

- Syslog
- NetFlow 9
- RADIUS accounting
- *Simple Network Management Protocol (SNMP)*

Syslog can provide a large amount of information for statistics-based analysis or information regarding the current ASA's health and the status of our remote connections. In addition to being able to send syslog (debugging, informational, and so on) information to remote servers for offline inspection, you can choose to store it in a local buffer on the ASA for later viewing when working on the device.

Figure 17-8 shows the ASDM's Logging Setup window available via **Configuration > Device Management > Logging > Logging Setup**. To enable logging, just check the **Enable Logging** check box. You can also optionally include debugging information when troubleshooting a feature/error on the ASA by checking the **Send Debug Messages as Syslogs** check box.

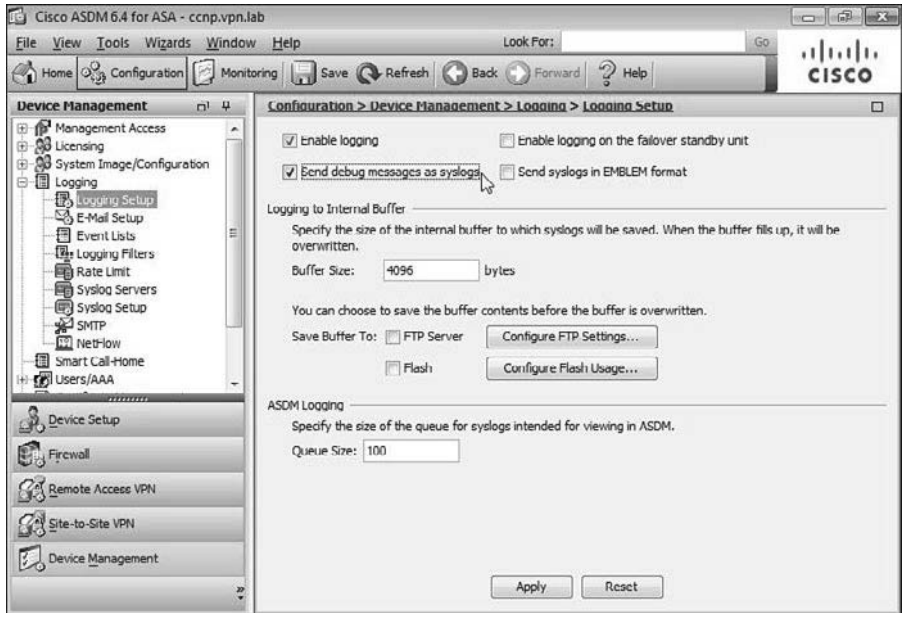


Figure 17-8 *Enable Logging in the ASDM and Specify Location*

In the Logging Setup window, you can also enable logging on the failover device if you are running two ASAs in a hardware failover pair, and you can select to send your syslog

information in EMBLEM format. (This is required if you are running CiscoWorks software as applications. For example, *RME [Resource Manager Essentials]* processes syslog information in EMBLEM format.) In addition to these options, in the Logging to Internal Buffer section of the window, you can increase or decrease the size of the internal buffer used to store the logging information (default is 4096 bytes) on the ASA. The internal buffer is a rolling log, meaning as soon as it becomes full, any new information starts to overwrite the older information in the buffer. For example, if your ASA device is logging a large amount of information while you are trying to troubleshoot an error, it is worthwhile to increase the size of the logging buffer to prevent the information you might require being overwritten before you have had a chance to look at it. In this section, you can also configure the ASA to store the buffer information in a file on the ASA's flash device or upload it to an FTP server when it reaches a specific size. This can also prevent your valuable log information from being overwritten. In the final section of the window, you can select the amount of information that is written to the ASDM log viewer (visible on the home page). The default is 100 messages.

After you have enabled logging on the ASA device, you can navigate to **Configuration > Device Management > Logging > Syslog Servers** and configure the remote servers to which the ASA will send its generated syslogs.

Figure 17-9 shows the Syslog Servers window and the Add Syslog Server window that opens when you click **Add**. In the Add Syslog Server window, select the interface your server is available on, enter the IP address of the server, and select either TCP or UDP (default) and the port (514 by default). In addition, you can check to enable the option Log Messages in Cisco EMBLEM Format (UDP only) or the option to Enable Secure Syslog Using *SSL/TLS (Secure Sockets Layer/Transport Layer Security)*. (This latter option is available only when using TCP for communications between the ASA and server.)

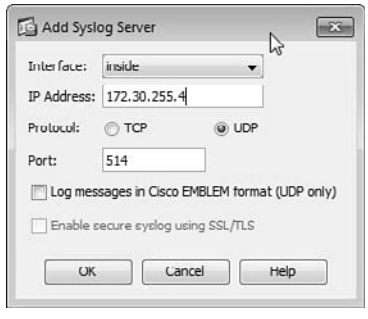


Figure 17-9 *Creating a New Syslog Entry*

After you have entered your syslog servers, you need to then specify the level of logging information that will be sent to our syslog server. In **Configuration > Device Management > Logging > Logging Filters**, you can choose from the following:

Key Topic

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

As shown in Figure 17-10, you can choose the level of logging per function on the ASA. For example, you might want to send informational messages to the console but debugging information to the ASA's internal buffer.

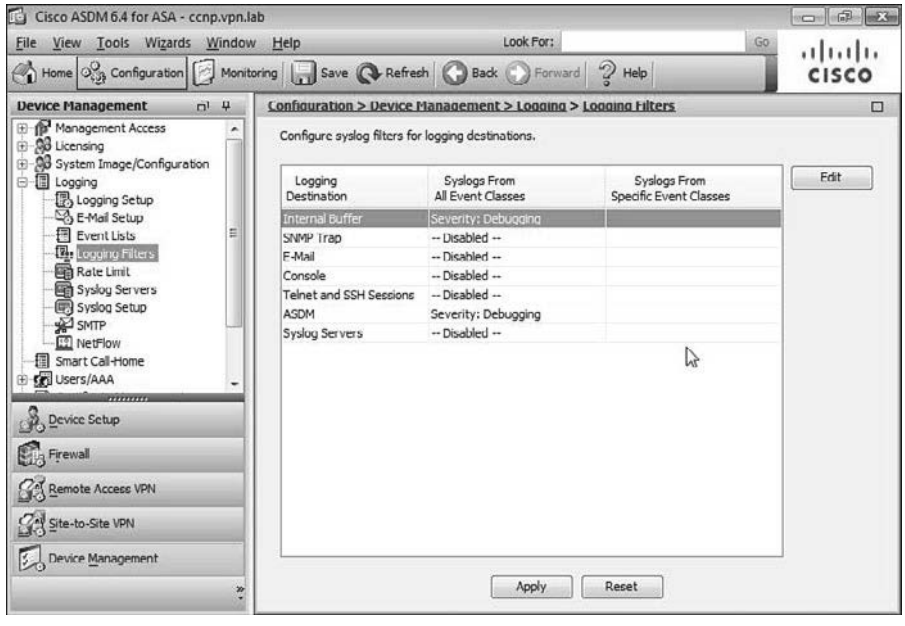


Figure 17-10 *Choose the Logging Level per Function*

And that's it! Well... not quite. At the moment, enough options have been selected and enough information entered for the ASA to be able to log to the internal buffer, syslog, and servers. Now you can start to get really granular with the control you have over syslog information. For example, if you are interested in only a particular log message or set of messages, you can create a filter in the Event Lists window. After creating a filter, you can select this in the Logging Filters window instead of selecting a predefined logging level.

You can optionally rate limit the number of log messages sent per second per logging level, or even per log message, in the Rate Limit window. You can set up a dedicated facility per logging level, if you want to view or filter the different logging levels easily on our syslog server. And in the E-Mail Setup and SMTP windows, you can set up the parameters and options used to send syslog information to a recipient via email.

The process of configuring logging on your ASA when working from the CLI is, as you can imagine, a lot faster because you do not have to open and close all the different windows or check on uncheck any of the options. However, which method you choose to use to configure your ASA is up to you, although for the exam it is a good idea to have an understanding of the various CLI commands that are available and their corresponding ASDM locations and values.

For example, to enable informational logging to the local buffer of the ASA, you can enter the following commands in enable mode:

```
logging buffered informational
logging enable
```

For logging to become operational, the latter command *must* be issued.

Similarly, to set up logging to an external server, you can enter the following enable mode commands:

```
logging trap informational
logging host [nameif] {hostname | ip address} port [format emblem]
```

Again, you can use the **format emblem** keywords along with the command to enable the use of the EMBLEM format when working with a supported RADIUS server. When configuring logging to a destination or the local buffer, the same logging levels are available (for example, notifications, emergencies, debugging) as shown in Example 17-5. You have the choice of either entering the name of the level (for example, **informational**) or the corresponding severity level (**6**); both achieve the same result.

Example 17-5 *Available CLI Logging Severities*

```
CCNPSec(config)# logging buffered ?

configure mode commands/options:
  <0-7>          Enter syslog level (0 - 7)
  WORD           Specify the name of logging list
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
```

You can view logging information held in the ASA's internal buffer in **Monitoring > Logging > Log Buffer**. Alternatively, you can enter the **show logging** command when using the CLI. Choose the logging level you are interested in viewing and click **View**. Figure 17-11 shows an example of the log buffer contents in the internal logging buffer viewed using the ASDM.

Note To clear the local buffer of all logs, enter **clear logging buffer** in privileged EXEC (enable) mode.

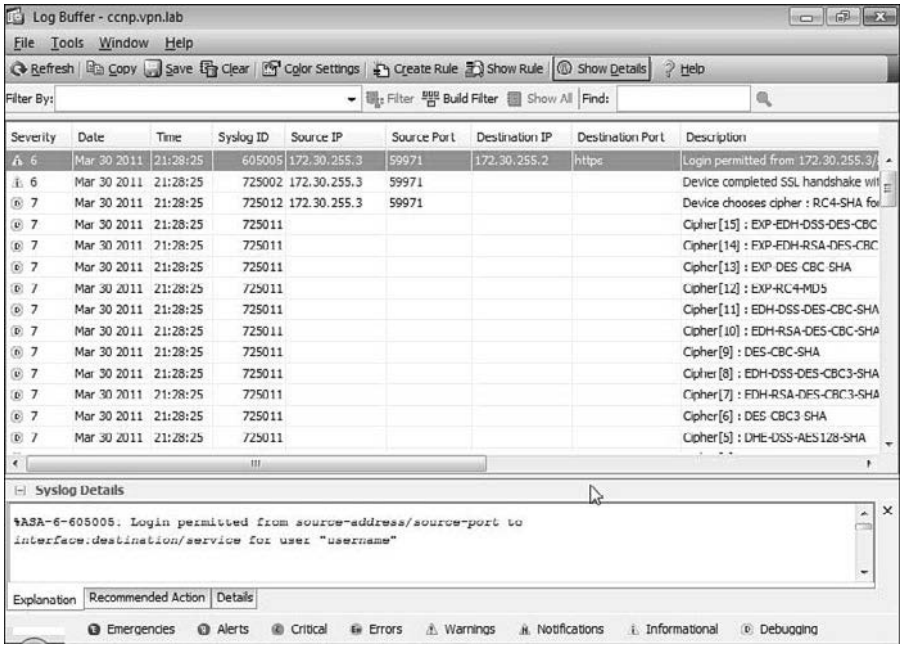


Figure 17-11 *ASA Internal Log Buffer*

NetFlow 9

With NetFlow logging, you can view information on a flow-by-flow basis based on Layer 3 and Layer 4 information of a conversation. Unlike sending information to a collector in tuple format (which can lead to limitations in the amount of information sent in any one packet, like its predecessor NetFlow 5), NetFlow 9 uses a template-based method of transferring information to a server running the NetFlow collector service. The template is sent to the server at specific intervals (30 minutes) and is used to format the information it receives from the ASA.

The ASA can send NetFlow 9 information to a server running the NetFlow 9 collector service (all other versions are incompatible) based on the following packet-flow actions occurring:

- Created
- Denied (excluding flows denied by Ethertype ACLs).
- Torn down

Figure 17-12 shows the configuration of NetFlow on the ASA device using the ASDM.

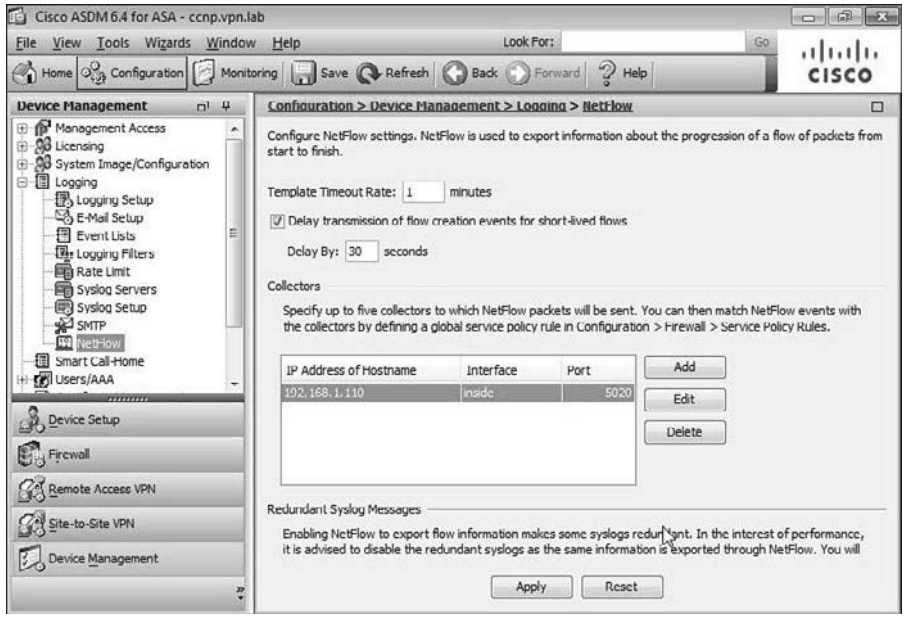


Figure 17-12 *ASA NetFlow Configuration*

In the NetFlow window (**Configuration > Device Management > Logging > NetFlow**), you can enter a value in minutes for the interval used to send the Version 9 template to the collection service running on your remote server (default 30). Optionally, you can choose to delay the sending of flow-creation events by a specific time you enter in seconds (which can help minimize the amount of information sent at any one time if, for example, a lot of flows are created at once on the ASA device). You also enter your flow collector's (server) IP address, the interface they are available on, and the UDP port that will be used for the communication of NetFlow information to them. After entering this information, you can then specify the type of event for which NetFlow information is sent to the servers. As shown in Figure 17-12, three events can cause the information to be sent. You can specify the event using a service policy that, if you recall from earlier chapters, you have already seen when used to create *quality of service (QoS)* policies on the ASA.

However, unlike QoS policies, NetFlow policies can be applied only globally, not per interface. By default, the ASA has an existing default service policy that is applied globally to the ASA. However, you cannot edit this in the ASDM, so you must create a new global service policy and either use an access list to define the IP addresses for which your NetFlow flow information will be generated or use the class-default class of your policy.

To configure NetFlow via the CLI, enter **flow-export** *option* global configuration command (with the exception of service policy configuration, which is shown in a moment). Table 17-3 lists the options/values available for this command. Notice how these are also the same options that are available when using the ASDM.

Table 17-3 **flow-export** *CLI Commands*

CLI Commands	Value
flow-export delay flow-create *1-180*	Enter the delay in seconds between 1 and 180 after which flow creation information will be exported.
flow-export destination [**nameif**] {*hostname* | *ip address*} *port*	Enter the interface, hostname/IP address, and optionally a port that will be used to export information to a destination host.
flow-export template timeout-rate *1-3600*	Enter the time in minutes (default 30) that template information will be re-sent.

In this example, a new global service policy is created using the class-default class to match all traffic for NetFlow flow information. Begin by opening the service policy in the ASDM Service Policy Rules window (**Configuration > Firewall > Service Policy Rules**) and clicking **Add**. Then choose **Add Service Policy Rule.** In the Add Service Policy Rule Wizard - Service Policy window, choose **Global - Applies to All Interfaces** and click **Next.**

On the next screen, Add Service Policy Rule Wizard - Traffic Classification Wizard, choose the **Use Class-Default as the Traffic Class** and click **Next.**

Then, in the Add Service Policy Rule Wizard - Rule Actions window, open the **NetFlow** tab. On this tab, click **Add.** In the new Add Flow Event window that opens, shown in Figure 17-13, choose the event that will trigger the sending of NetFlow information from the Flow Event Type drop-down box and check the box next to the host for which you want to enable this rule. Finally, click **OK** and **Finish** to apply the new rule.

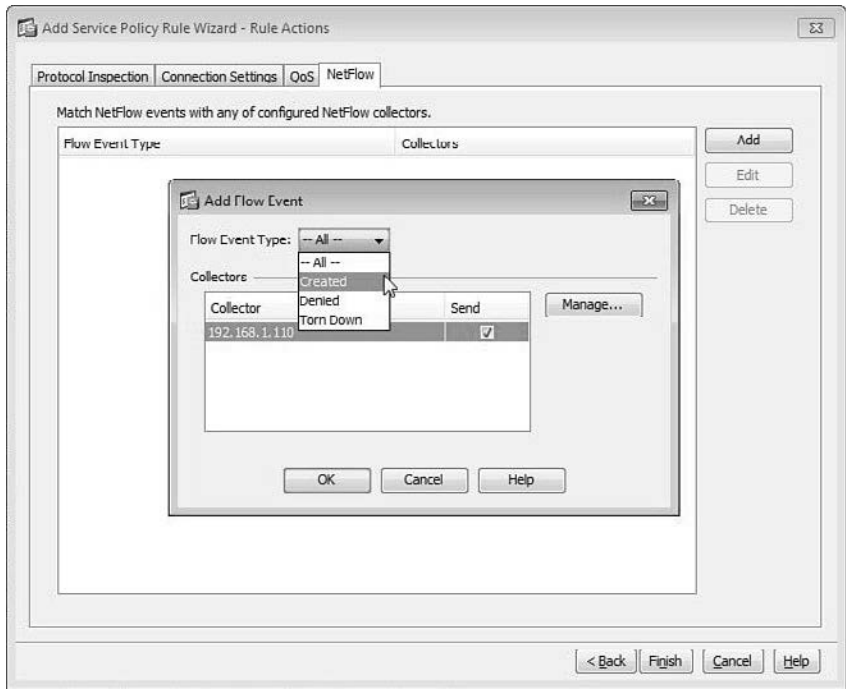


Figure 17-13 *ASA NetFlow Service Policy Configuration*

Example 17-6 displays the same configuration as the earlier ASDM example, but this time configured using the CLI.

Example 17-6 *NetFlow Export Configuration*

```
CCNPSec(config)# flow-export destination inside 192.168.1.100 5010
CCNPSec(config)# policy-map global_policy
CCNPSec(config-pmap)# class class-default
CCNPSec(config-pmap-c)# flow-export event-type flow-create destination
 192.168.1.100
```

RADIUS VPN Accounting

You can enable RADIUS accounting information so that your support representatives can interrogate the RADIUS logging information to see whether a VPN connection has succeeded or failed (and if failed, why).

To enable RADIUS accounting in a connection profile, as shown in Figure 17-14, navigate to **Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv1) Connection Profiles**. Choose your connection profile from the list and click **Edit**. In the Edit IPsec Remote Access Connection Profile: *Name* window, choose **Advanced > Accounting** from the menu on the left. In the Accounting window, from the drop-down list choose the RADIUS server group that contains the RADIUS servers

to which the ASA will be sending its accounting information. You can also create a new server group by clicking **Manage** if no groups are currently available.

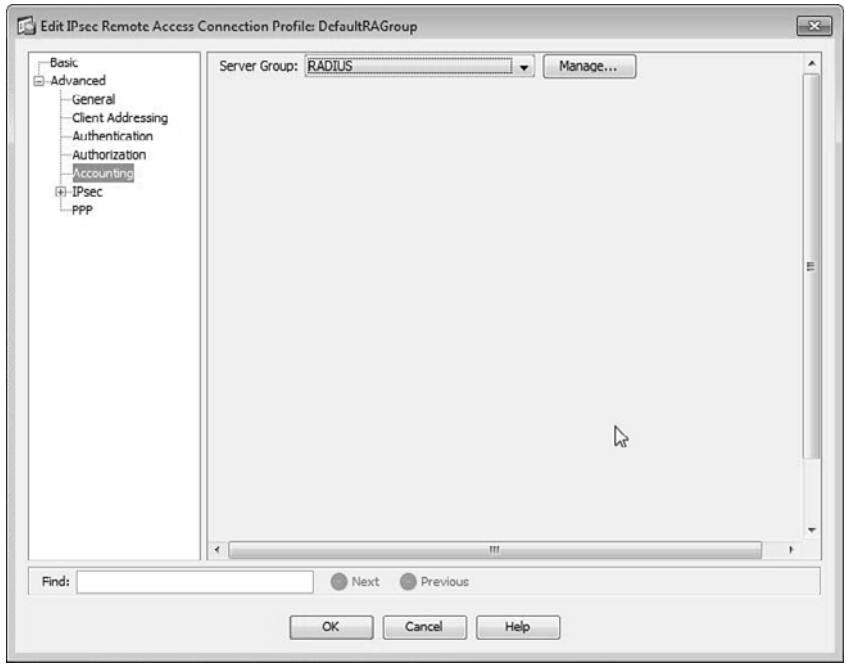


Figure 17-14 *IKEv1 Connection Profile RADIUS Accounting Configuration*

The CLI configuration is just as simple. You configure the accounting servers within the now familiar tunnel-group general-attributes configuration mode with **accounting-server-group** *name*, as shown in Example 17-7.

Example 17-7 *Connection Profile Accounting Server Configuration*

```
CCNPSec(config)# tunnel-group DefaultRAGroup general-attributes
CCNPSec(config-tunnel-general)# accounting-server-group RADIUS
```

After configuring RADIUS accounting servers in a connection profile, you can inspect the received RADIUS accounting information on your RADIUS server implementation using the various logging options that are available.

SNMP

The ASA can support access for device and statistical interrogation using SNMP Version 1, Version 2c, and Version 3. Many texts and books already explain the differences between these versions, so to save you from reading it all again, this discussion assumes that you know enough about SNMP already to have made the decision that if Version 3 is available on a device, you use Version 3 to access it.

You configure the various SNMP options (traps, location, global community string, and hosts) in **Configuration > Device Management > Management Access > SNMP**, as shown in Figure 17-15.

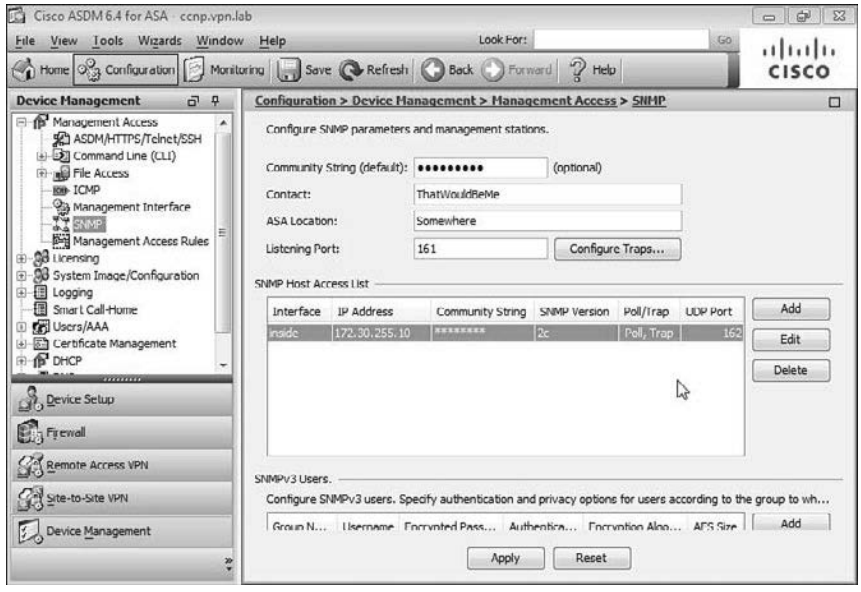


Figure 17-15 *ASA SNMP Configuration*

In the SNMP window, you can configure all the familiar options for the protocol, such as the community string, contact, location, and listening port (UDP 161 by default). You can configure the criteria for trap information to be sent by clicking **Configure Traps** and choosing from the available options in the SNMP Trap Configuration window that opens.

In addition, in the SNMP window, in the SNMP Host Access List section, you can explicitly enter the addresses of your servers that will be accessing your ASA device. You can also create the users and groups that will be used for SNMPv3 access in the SNMPv3 Users section of the window.

To configure SNMP hosts, options, and attributes via the CLI, enter the **snmp-server** *option* global configuration mode command. Table 17-4 describes the configuration options you have for this command. Note that these are the same as those available within the ASDM SNMP window shown earlier in Figure 17-15.

Table 17-4 **snmp-server** *CLI Commands*

CLI Commands	Value
snmp-server community *string*	Enter the community string used for authentication with SNMP versions earlier than Version 3.
snmp-server contact *value*	Enter the contact information that will be held within the SNMP MIB object sysContact.

CLI Commands	Value
snmp-server enable traps *option*	Enter the trap option that will enable the appropriate amount and detail of information you require to be sent to the SNMP server. The available options are as follows: **all**—Enable all traps. **connection-limit-reached**—Enable connection limit traps. **cpu**—Enable CPU utilization-related traps. **entity**—Enable ENTITY MIB notifications. **ikev2**—Enable IKEv2 traps. **interface-threshold**—Enable interface threshold reached traps. **ipsec**—Enable IPSec traps. **memory-threshold**—Enable memory threshold reached traps. **nat**—Enable *Network Address Translation (NAT)*-related traps. **remote-access**—Enable remote-access traps. **snmp**—Enable SNMP traps. **syslog**—Enable syslog traps.
snmp-server group *name* **v3** [**auth** | **priv** | **noauth**]	Enter this command to configure a group for use with Version 3 servers and the purposes of authentication (**auth**) or encryption (**priv**) of SNMP information.
snmp-server host [**nameif**] *hostname/ip address* [**community** *value*] [**udp-port** *port*] [**poll**] [**trap**] [**version 1** | **2c** | **3**]	Use this command to enter the location, hostname/IP address and port number of an SNMP server used to send SNMP information to/from the ASA. You can also optionally enter a community value and SNMP version, and you can use the **trap** keyword to send traps to only the specified host or use the **poll** keyword to allow polling to occur only from this host.
snmp-server listen-port *value*	Enter the port that will be used by the local SNMP engine on the ASA to listen for incoming SNMP requests (default 161).
snmp-server location *value*	Use this command to enter the value for the MIB object sysLocation (for example, Floor1East).
snmp-server user *username groupname* **v3** [**auth** {**md5** | **sha**} *password*] [**priv des** | **3des** | **aes** {**256** | **192** | **128**} *password*]	Use this command to create a local SNMP user account for use with Version 3. Note that you must first configure the group the user will belong to on the ASA by entering the **snmp-server group** *name* command.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a few choices for exam preparation: Chapter 22, "Final Exam Preparation," Appendix C, "Memory Tables" (CD only), and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 17-5 lists a reference of these key topics and the page numbers on which each is found.

Table 17-5 *Key Topics*

Key Topic Element	Description	Page
Bulleted list	Group policy types	627
Subtopic	Assigning a group policy to a user account	633
Subtopic	Assigning a group policy to a connection profile	634
Bulleted list	Available accounting methods	636
Bulleted list	Available logging levels	638
Bulleted list	NetFlow flow-creation actions	641

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

external group policy, internal group policy, NetFlow, SNMP (Simple Network Management Protocol)

Index

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