Official
Cert Guide

Learn, prepare, and practice for exam success

CCNP Security VPN
642-647

- Master **CCNP Security VPN 642-647** 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

ciscopress.com

HOWARD HOOPER, CCIE® No. 23470

CCNP Security VPN 642-647

Official Cert Guide

Howard Hooper, CCIE No. 23470

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCNP Security VPN 642-647
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

First Printing July 2011

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

ISBN-13: 978-1-58714-256-7

ISBN-10: 1-58714-256-2

Warning and Disclaimer

This book is designed to provide information for the Cisco CCNP Security VPN 642-647 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 regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail 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

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact: International Sales 1-317-581-3793 international@pearsontechgroup.com

We greatly appreciate your assistance.

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

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Managing Editor: Sandra Schroeder

Editorial Assistant: Vanessa Evans

Executive Editor: Brett Bartow

Book Designer: Gary Adair

Indexer: Tim Wright

Copy Editor: Keith Cline

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editors: James Risler, Cristian Matei

Compositor: Mark Shirar

Development Editor: Kimberley Debus

Proofreader: Water Crest Publishing, Inc.

Senior Project Editor: Tonya Simpson

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 for his companies SYNCom Ltd. and 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.

About the Technical Reviewers

James Risler, CCIE No. 15412, is a systems engineer education specialist for Cisco Systems. His focus is on security technology and training development. James has more than 18 years of experience in IP internetworking, including the design and implementation of enterprise networks. Before joining Cisco Systems, James provided Cisco security training and consulting for Fortune 500 companies and government agencies. He holds two Bachelor degrees from University of South Florida and is currently working on his MBA at the University of Tampa.

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, 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 grandfather, Geoffrey, for becoming my father figure and teaching me what I consider to be one of the most important lessons I received early on in my life: that you must work and work hard for what you want. You are forever missed and never forgotten.

My mother, Sally, for providing me with the greatest example of personal strength and determination anyone could ever hope to possess. You scaled mountains to make sure we always had everything we needed and were protected; we are only here because of you.

My son, Ridley, for giving me the reason I need at times to carry on and the drive to become better at everything I do. Even though I cannot be there all the time, Daddy loves you very much.

I hope I have and will always go on to make you proud of me. I would not be the man I am today without you, for that I thank you.

Acknowledgments

When writing a book, a small army of people back you up and undertake 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 Kimberley Debus, who transformed my words into human-readable form and kept me on track. I know she worked many late nights and weekends to help complete this book, and I shall miss our "conversations through the comments." I will be forever grateful to both of you.

Thanks must also go out to the two technical reviewers, Cristian Matei and James Risler. Your comments and suggestions have been brilliant throughout the entire book. Your help and input has definitely made this book better.

Last, but by no means least, I want thank my family and co-workers for their support during the writing of this book. Without that support, this would not have been possible, and as soon as I have caught up on sleep again, I will be conscious enough to thank you personally.

Contents at a Glance

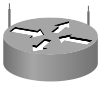
Part VI Cisco IPsec Site-to-Site VPN Solutions

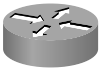
Part VII Exam Preparation

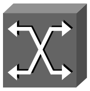
Part VIII Appendixes

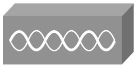
Contents

Icons Used in This Book


Wireless Router

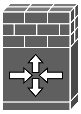

Router

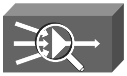

ATM/FastGb Eitherswitch

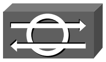

Access Point

Switch

Secure Switch

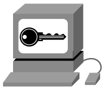

Cisco IOS Firewall

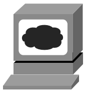

CS-MARS


IPS

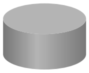
SSL VPN Gateway

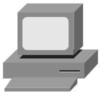
IP Phone

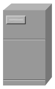

AAA Server


Web Server

Secure Endpoint

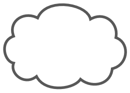

Database


PC


File/ Application Server

Laptop

Wireless Connection


Network Cloud

Ethernet Connection

Introduction

This book is designed to help you prepare for the Cisco VPN certification exam. The VPN 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 23 chapters. Each chapter tends to build upon 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, "Evaluation of the ASA Architecture":** This chapter reviews the ASA operation and 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 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 4, "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 Public Key Infrastructure (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 5, "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 6, "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 DAPs and how their configuration can be used to enhance the authorization process.
- **Chapter 7, "AnyConnect Integration with Cisco Secure Desktop and Optional Modules":** This chapter reviews the Cisco Secure Desktop (CSD) environment and associated modules. We also introduce you to the optional AnyConnect modules that are available for installation either as standalone components or deployed through client profiles.
- **Chapter 8, "AnyConnect High Availability and Performance":** This chapter reviews the different types of redundancy and high availability that can be deployed on the ASA device through configuration of the AnyConnect client or with external hardware.
- **Chapter 9, "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 10, "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 11, "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 PKI and of double-authentication mechanisms.
- **Chapter 12, "Advanced Authorization Using Dynamic Access Policies":** 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 13, "Clientless SSL VPN with Cisco Secure Desktop":** This chapter reviews the Cisco Secure Desktop environment and associated modules. In addition, we cover how to deploy the CSD with a clientless SSL VPN solution.
- **Chapter 14, "Clientless SSL VPN High Availability and Performance Options":** This chapter reviews the available HA and performance enhancements that can be deployed when working with clientless SSL VPN solutions.
- **Chapter 15, "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 16, "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 17, "Advanced Authentication and Authorization Using Easy VPN":** In this chapter, we review the configuration of PKI and its subsequent implementation with Easy VPN deployments. We also cover certificate mappings and their role when used for advanced authentication purposes.
- **Chapter 18, "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 19, "High Availability and Performance for Easy VPN":** This chapter describes the mechanisms that can be put in place to provide an HA solution that will protect an organization from outages alongside an Easy VPN deployment.
- **Chapter 20, "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 21, "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 22, "High Availability and Performance Strategies for IPSec Site-to-Site VPNs":** In this chapter, we discuss 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 23, "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, "642-647 CCNP Security VPN 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 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/9781587142567.

- **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 a good tool for last-minute preparation just before taking the exam.
- **Practice exam on CD-ROM:** 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 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 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, 15, 16, 21
Choose the correct ASA model and license to implement HLD based on given performance requirements	1, 3, 8, 15, 16, 21
Choose the correct ASA VPN features to implement HLD based on given corporate security policy and network requirements	1–5, 8–10, 15–17, 20, 21
Integrate ASA VPN solutions with other security technology domains (CSD, ACS, device managers, cert servers, and so on)	1–5, 8–10, 15–21
Complex Operations Support	
Optimize ASA VPN performance, functions, and configurations	3–5, 7–10, 15–22
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, RA VPN, certificates, QoS, and so on to meet security policy requirements	3–10, 15–22
Create complex ASA network security rules using such features as ACLs, DAP, VPN profiles, certificates, MPF, and so on to meet the corporate security policy	4–6, 10–12, 15, 17, 18, 20
Advanced Troubleshooting	
Perform advanced ASA VPN configuration and troubleshooting	4–6, 8, 10–12, 14, 15, 17–19, 22

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. You can view the current exam topics on any current Cisco certification exam by visiting its website at Cisco.com, 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/9781587142567. 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 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 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, you will want to 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 professional-ism 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 or router is not normally something to play with. That is to say that after you have it properly configured, you will tend to leave it alone until there is a problem or you need to make some other configuration change. This is the reason that the question mark (?) is probably the most widely used Cisco IOS and Cisco ASA software command. Unless you have constant exposure to this equipment, it can be difficult to remember the numerous commands required to configure devices and troubleshoot problems. Most engineers remember enough to go in the right direction but will use the ? 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 could have chosen to use 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 will want 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/9781587142567. 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 subjects:

- **Policies and Their Relationships:** In this section, we review the available policies that can be applied during a VPN connection and how they work together to form the overall policy applied to a remote user.
- **Understanding Connection Profiles:** In this section, we discuss the role of connection profiles, their configuration elements, and how they are applied to remote users.
- **Understanding Group Policies:** In this section, we discuss the role of group policies for attribute assignment and control of your remote users.
- **Configure User Attributes:** In this section, we review the creation of a user account and take a look at the available parameters and attributes that can be assigned to an individual remote user.
- **Using External Servers for AAA and Policy Assignment:** In this section, we discuss the role of AAA servers and briefly cover their configuration and how we can deploy policies through them.

Configuring Policies, Inheritance, and Attributes

An important part of the deployment of a Secure Sockets Layer (SSL) or IPsec virtual private network (VPN) connection is the use of policies to allow access to resources through the VPN tunnel and the ability to control the access granted to those resources, whether this is based on the user and their internal group membership or department, the site and specific resources they are accessing, or role in the company.

We are given a wide range of options that can be configured and specified using the available policy set in the Adaptive Security Appliance (ASA), allowing us to take a very granular approach to allow or deny access based on a user's attributes. Furthermore, if a user is a member of multiple groups in the business, we can assign multiple policies, resulting in the inheritance of higher-level policies and only the more specific attributes being directly assigned.

In this chapter, we take a look at the methods available for policy assignment both in real-life scenarios and throughout this book. We then review how these policy methods work together if more than one is assigned to a user through the inheritance mode.

"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 2-1 details the major topics discussed in this chapter and their corresponding quiz sections.

Table 2-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Policies and Their Relationships	2
Understanding Connection Profiles	1, 3
Understanding Group Policies	4, 5
Using External Servers for AAA and Policy Assignment	6

1. Which of the following are available methods of assigning a connection profile? (Choose all that apply.)

   a. User connection profile lock

   b. Certificate to connection profile maps

   c. User choice using a menu in either clientless or full-tunnel VPN

   d. All of the above

2. Which of the following policy types take precedence over all others configured based on the ASA policy hierarchy?

   a. DAPs

   b. Group policy

   c. Connection profile

   d. User attributes

3. Which two of the following are the default connection profiles that exist on the ASA device?

   a. DefaultRAGroup

   b. DefaultWebVPNGroup

   c. DefaultL2LGroup

   d. DefaultAnyConnectGroup

4. Which of the following objects can be used for post-login policy assignment? (Choose all that apply.)

   a. Connection profiles

   b. User attributes

   c. Group policies

   d. DAPs

5. Which of the following are valid group policy types?

   a. External

   b. Internal

   c. Local

   d. Remote

6. When configuring external group policies, which AAA protocols or servers can you use for authorization?

   a. RADIUS

   b. SDI

   c. TACACS+

   d. LDAP

Foundation Topics

Policies and Their Relationships

User policy and connection parameter enforcement is an important part of any VPN deployment. Without it, we cannot provide login parameters, authorization methods, or resource access for our users, which control what they can or cannot access and when.

Key Topic

An important part of policy assignment is the ability to provide flexibility and scalability to both administrators configuring them and the remote users using them.

- Flexibility is achieved through being able to assign the same security or network settings to any user or group regardless of their connection type.
- Scalability is achieved through modularity and policy inheritance, limiting the amount of duplicate configuration items required by policy reuse among groups or individual users.

All remote users must go through two phases before they can successfully connect and start to access resources made available through your VPN connection:

- **The prelogin phase** is achieved through the use of connection profiles (also known as tunnel groups). In connection profiles, we can carry out the assignment of connection attributes and parameters (for example, authentication, authorization, and accounting [AAA] and IP address assignment) and define the available connection methods (for example, IKEv1 and IKEv2 SSL), allowing our users to start the login process.
- **The post-login phase** is achieved through the use of group policy objects, Dynamic Access Policies (DAPs), and user-specific attributes. These may include such items as IPv4 or IPv6 access lists, Domain Name System (DNS) servers, access hours, split tunneling, and so on. Group policies offer a great deal of flexibility when assigning attributes to users, either individually in a user account or groupwide by assignment to a connection profile. DAPs provide an advanced policy assignment method based on user AAA attributes or client device posture assessment. We discuss DAPs, their configuration, and deployment in later chapters.

Different policy types, although they include their own specific attributes, are really just containers that can be used to hold multiple configuration items that might have been used multiple times already in different policies. For example, we can configure an access control list (ACL) (we'll call it Server_Access) to only allow access between remote client A and corporate server A. We assign it to the group policy object AnyConnect, limiting internal resource access for our AnyConnect users. Later, we create a new group policy for our IPsec VPN users and assign our Server_Access ACL to this group policy, as well.

In our example, we have two groups of users accessing our corporate network through their own protocol-specific connection profiles (AnyConnect and IPsec). Each of the two connection profiles has its own group policy objects, both using our Server_Access ACL.

If we want to reduce the amount of configuration we have to carry out but still allow each connection group to have its specific attributes (for example, IP address pools and DNS servers), we can create a single group policy object using our Server_Access ACL and apply this to each connection profile.

Furthermore, if we want to really minimize the amount of configuration we have on our device, and the only difference between these two groups of users is their connection type (that is, they do not require any further attribute or parameter assignments between them), we can create a single connection profile allowing multiple connectivity types and attach the single group policy that uses our Server_Access ACL. Later, if one of our users requires access to corporate server B, we can create a custom ACL and apply it directly to their user account, or create a user-specific group policy object and assign this directly to our user.

Key Topic

We can be as specific as we like or as needs require for our particular environment, either sharing multiple policies between multiple groups, reusing multiple attributes in multiple policies, using multiple groups connecting to one connection profile, or configuring each group to have its own specific connection profiles, policies, and attributes. The choice is, well, yours.

As we create our connection profiles and policies, we might end up with a user who has been assigned the same attributes multiple times by separate policies. These might have been applied because of the user's group or department membership, connection type, or location. Regardless of the reason for these assignments, the result is that our user's policies are merged and assigned in a hierarchical fashion.

The hierarchal policy model shown in Figure 2-1 works from top to bottom with any attributes set within policy assignment methods toward the top of the list (DAPs), taking precedence over any conflicting attributes assigned within methods toward the end of the list (default group policy object).

Each connection entry has its own default group policy object. As shown in Figure 2-1, the default group policy is at the end of the policy hierarchy. As a result, any attributes/settings that have not been configured within policies already assigned to a user are applied using the attribute assignment of the default group policy.

The same applies to other policy types within the policy hierarchy. However, if two policy types contain different values for the same attribute or property, the user is assigned the attribute set within the policy type that is higher in the hierarchy. For example, if IP pool A has been assigned to the group policy applied to the connection profile and IP pool B has been assigned to the user account directly, the user is assigned an IP address from IP pool B.

Understanding Connection Profiles

As you saw earlier, connection profiles provide our users with the necessary prelogin policies that must successfully establish a connection to our ASA device. We can also use connection profiles to separate our connecting users into the relevant groups that may require separate methods of access (for example, clientless SSL VPN, AnyConnect VPN sessions, or even separate AAA methods).

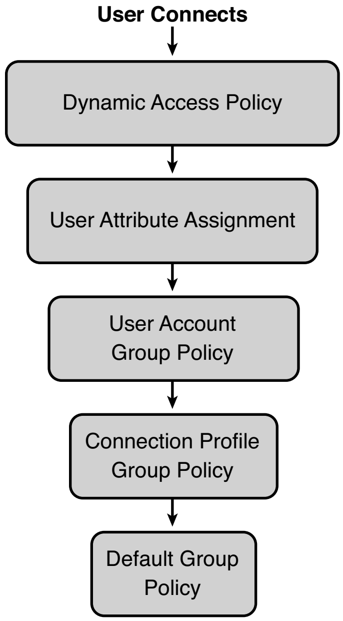

User Connects
Dynamic Access Policy
User Attribute Assignment
User Account Group Policy
Connection Profile Group Policy
Default Group Policy

Figure 2-1 *ASA VPN Policy Enforcement Hierarchy*

Consider the following scenario. You have two groups of users connecting into your environment: guests and corporate employees. Guests connecting into your organization do not require the same level of access as your employees. In fact, they only require access to an internal intranet portal. On the other hand, your corporate employees require access to internal file servers and email. Based on the level of access required by each group, we could create two connection profiles, aptly named Guests and Corporate for our discussion. Our Guests connection profile would only allow access for incoming clientless SSL VPNs and authenticate connecting users with a shared guest internal username and password. A group policy (covered in greater depth during the next section) would be applied to our connection profile containing the relevant bookmarks needed for browsing our company's intranet in the SSL VPN portal. However, our Corporate connection profile would allow access for incoming AnyConnect SSL, IKEv2, and IKEv1 (IPsec VPN clients), and an IP address would be assigned per remote user from an existing IP address pool. Authentication and authorization would be carried out using a combination of a one-time password (OTP) and internal Windows Active Directory server. A group policy would be applied to the connection profile to provide users with split-tunnel lists and access lists, restricting communication to only those internal subnets and devices that are required.

A few methods are available for allowing our users to select/connect to the appropriate connection profile they require. Depending on the authentication scheme we have configured for our users and their chosen login method (clientless SSL VPN, AnyConnect, IPsec client), they can either select a connection profile manually from a list of those available or have it selected for them automatically, based on one of the following methods:

Key Topic

- Group URL
- Group alias
- Certificate to connection profile mapping
- Per-user connection profile lock

Group URL

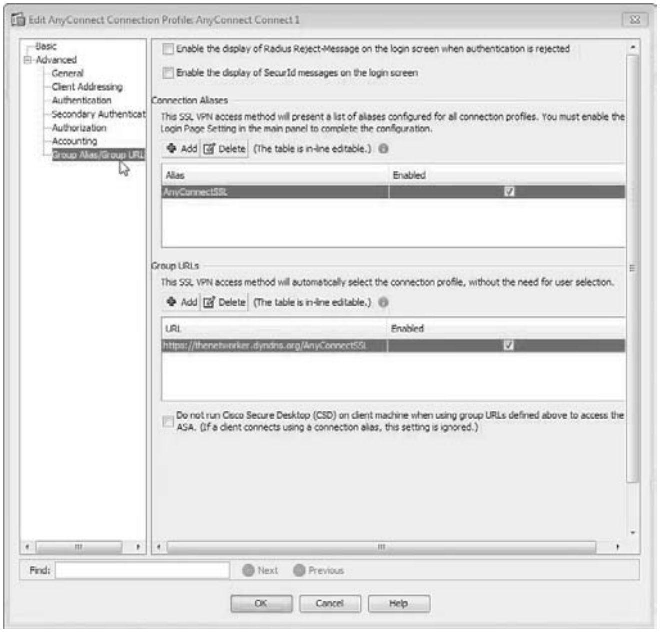
Group URLs allow remote users to select a connection profile by entering the direct URL configured for the profile they require. An example of a configured group URL is either of the following:

https://<ASA IP address>/<connection profile>

https://<ASA FQDN>/<connection profile>

Group Alias

Group aliases allow clientless SSL VPN users to select the appropriate connection profile from a list at the portal login page and AnyConnect users to select a connection profile in the client software. Both scenarios occur before a user has logged in and are covered in greater detail in Chapter 3, "Deploying an AnyConnect Remote-Access VPN Solution," and Chapter 9, "Deploying a Clientless SSL VPN Solution." As shown in Figure 2-2, the configuration of both a group alias and group URL is carried out in the Group Alias/Group URL pane of a connection profiles properties window. We navigate to **Configuration > Remote Access VPN > Network (Client) Access | Clientless SSL VPN Access > AnyConnect Connection Profiles | Connection Profiles**, select the connection profile, click **Edit**, and then use the menu on the left side to select **Advanced > Group Alias/Group URL**.



□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Alias	Enabled
AnyConnectSSL	☑

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

(The table is in-line editable.)

URL	Enabled
https://thenetworker.dyndns.org/AnyConnectSSL	☑

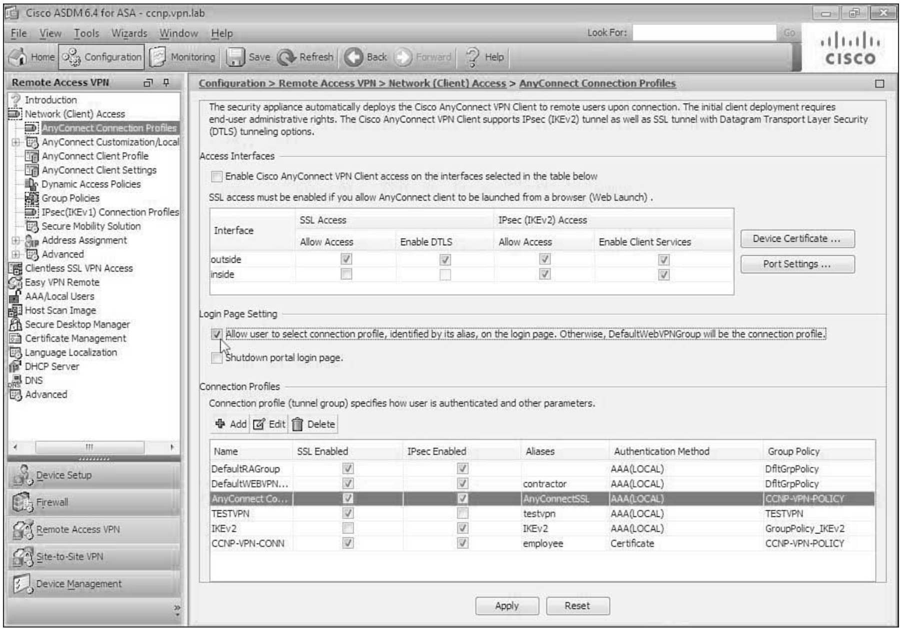
□ Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)

Figure 2-2 *Connection Profile Group URL and Alias Configuration*

As you will also see in later chapters, before our remote users can select a connection profile by group alias, we must first enable this feature on the ASA in the respective connection profiles pane of the Adaptive Security Device Manager (ASDM), as shown in Figure 2-3.

For example, we can enable our AnyConnect and clientless SSL VPN users to select a connection profile in their client software or from the portal login page using the following steps:

- **AnyConnect Users:** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.** In the Login Page Setting section of the window, select **Allow User to Select Connection Profile**, **Identified by Its Alias.**
- **Clientless SSL VPN Users:** Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.** In the Login Page Setting section of the window, select **Allow User to Select Connection Profile**, **Identified by Its Alias.**



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

□ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☑	☑
inside	□	□	☑	☑

Device Certificate ...
Port Settings ...

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

□ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

Add Edit Delete

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPN...	☑	☑	contractor	AAA(LOCAL)	DfltGrpPolicy
AnyConnect Co...	☑	☑	AnyConnectSSL	AAA(LOCAL)	CCNP-VPN-POLICY
TESTVPN	☑	□	testvpn	AAA(LOCAL)	TESTVPN
IKEv2	□	☑	IKEv2	AAA(LOCAL)	GroupPolicy_IKEv2
CCNP-VPN-CONN	☑	☑	employee	Certificate	CCNP-VPN-POLICY

Apply Reset

Figure 2-3 *Connection Profile Pane: Allow Group Alias Selection*

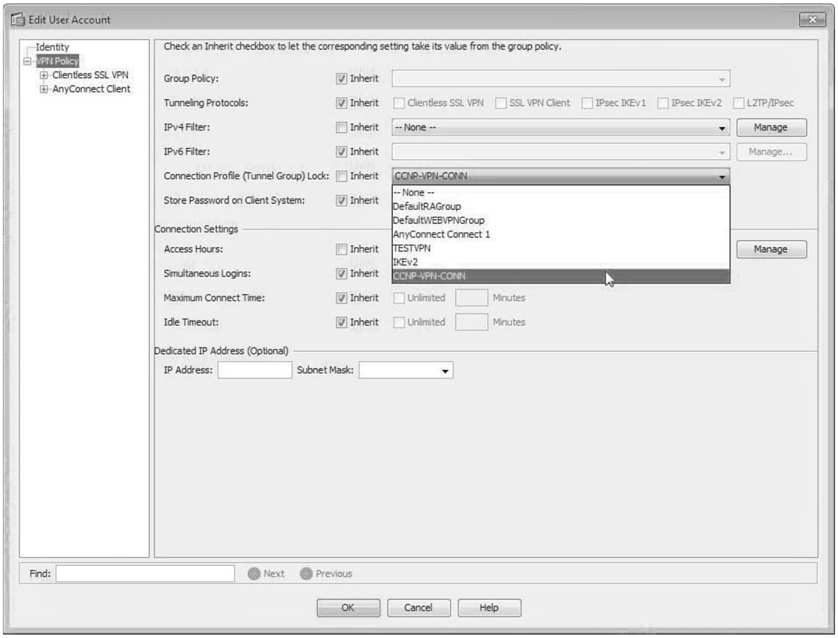
Certificate to Connection Profile Mapping

If you have chosen to use digital certificate authentication for your connection profiles, the distinguished name (DN) values in a remote user's certificate can be used to select the appropriate connection profile. For example, if the remote user initiating a connection is a member of the Accounts team, his certificate DN value may equal OU=Accounts. Using certificate-to-connection profile maps, the ASA can be configured to match any connecting users with the value of OU=Accounts to a custom connection profile created for Accounts department personnel. You can apply the same actions to any DN values held in your user certificates (as discussed in Chapter 9 and Chapter 4, "Advanced Authentication and Authorization of AnyConnect VPNs").

Per-User Connection Profile Lock

We can also assign a connection profile directly to remote users on an individual basis. For example, we might have a specific connection profile for our VPs and want to make the process of connecting as seamless as possible for them without their having to first enter or select a connection profile.

The process of assigning a connection profile directly to a user can be achieved in the properties menu of the user's account, as shown in Figure 2-4.



Edit User Account

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy: ☑ Inherit

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

IPv4 Filter: □ Inherit -- None --

IPv6 Filter: ☑ Inherit

Connection Profile (Tunnel Group) Lock: □ Inherit CCNP-VPN-CONN

Store Password on Client System: ☑ Inherit

Connection Settings

Access Hours: □ Inherit

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited Minutes

Idle Timeout: ☑ Inherit □ Unlimited Minutes

Dedicated IP Address (Optional)

IP Address: Subnet Mask:

Figure 2-4 *Configuring Per-User Connection Profile Lock*

We begin by selecting the user account to edit from **Configuration > Device Management > Users/AAA > User Accounts**, and then click **Edit**. In the Edit User Account window, select **VPN Policy** from the menu on the left, and in the pane on the right side, uncheck the **Connection Profile (Tunnel Group) Lock Inherit** check box. Using the drop-down list, select the appropriate connection profile to be assigned to this user.

We see a great deal more of connection profiles and their use in the chapters that follow. It is important to note at this stage that we can only allow clientless SSL VPN and client-based (AnyConnect) VPN remote users the option to select a connection profile. As discussed in Chapter 15, "Deploying and Managing the Cisco VPN Client," when we work with IPsec remote-access VPNs, the connection profile name is configured in the client software as the group name and must match before a successful connection can occur.

Default Connection Profiles

Besides our own custom connection profiles, default connection profiles are applied to a user's session if the various connection parameters in manually configured connection profiles are not satisfied and the user is not allowed to select the connection profile before login.

Three default connection profiles are configured on the ASA, as listed here. These cannot be removed, but they can be modified, allowing us to change the settings to match our environment:

- **DefaultRAGroup:** Used for client-based (AnyConnect) SSL VPNs and IPsec remote-access VPNs.
- **DefaultWEBVPNGroup:** Used for clientless SSL VPNs.
- **DefaultL2LGroup:** Used for IPsec LAN-to-LAN connections.

The default connection profiles, as mentioned earlier, are used mainly for global property assignment or a catchall mechanism for users that may only require a basic VPN portal (webmail and so on) and are not able to or allowed to select a connection profile. It is recommended that your own custom connection profiles be created for your specific VPN deployments, instead of relying on the default connection profiles for remote user connection establishment.

By default, when using plain old username and password-based authentication for remote user authentication, users are automatically connected to the appropriate default connection profile based on their connection method (that is, clientless SSL, IPsec, and so on). We can overcome this problem by providing our remote users with the means to select a connection profile before authenticating (either from a drop-down list in the clientless SSL portal or the AnyConnect client). If we have deployed username and password-based authentication (no certificates) for our clientless SSL and AnyConnect VPNs, however, and we have configured our ASA to provide our remote users with the ability to select a connection profile, users must select an available connection profile from the list in order to continue. If they do not select a connection profile, they are mapped to their default connection profile.

When using certificate-based authentication the game changes, and the default connection profile is used only if predefined fields within a user's certificate do not match the values we configure in Certificate to Connection Profile Mapping Rules for automatic connection profile assignment.

The process that occurs when using the Cisco IPsec VPN client is different from that just described for both clientless and full-tunnel connections, again depending on the type of authentication method in use. As you will see later in Chapter 15, "Deploying and Managing the Cisco VPN Client," when deploying IPsec remote-access connections using preshared key authentication, the connection profile name must be entered exactly into the client software (in the Group Name field). If the connection process fails, the client is not assigned to the default connection profile for the specific method of connection (DefaultRAGroup). Instead, the connection fails.

If we are using certificate-based authentication with the Cisco IPsec VPN client, we are not given the option of selecting or entering a connection profile/group name. Instead, we must either configure our own certificate to connection profile mappings, or by default, the ASA attempts to match the OU field value of the certificate to an available connection profile with the same name. If one or both of these methods fail, unlike with the pre-shared key method, the remote user is mapped to the DefaultRAGroup connection profile instead of being disconnected.

The DefaultL2LGroup acts as a catchall for any LAN-to-LAN IPsec VPN sessions that do not match on a manually administrator-configured connection profile, regardless of its authentication type, pre-shared-key, or if it is certificate based.

Note that, by default, neither DefaultWEBVPNGroup nor DefaultRAGroup allows for AnyConnect sessions, because these connection profiles have the DfltGrpPolicy group policy attached, which only permits clientless SSL VPN, IPsec VPN, and L2TP/IPsec sessions. These settings can, of course, be modified.

As you move through the rest of the book, you will many more uses of connection profiles with all available types of connectivity offered by the ASA device, in addition to many advanced features that are available within a connection profile.

Connection profiles are created by first navigating to **Configuration > Remote Access VPN** or **Site-to-Site VPN**. Depending on the chosen method of connectivity (whether this be clientless SSL, IKEv1, IKEv2, or so forth), select one of the following options in the Remote Access VPN or Site-to-Site VPN areas to continue:

Remote Access VPN:

- **Network (Client) Access:** Use for AnyConnect (full tunnel) SSL and IKEv2, Cisco IPsec VPN client, and IKEv1 connections.
- **Clientless SSL VPN:** Use for browser-based clientless SSL VPN connections.

Site-to-Site VPN:

- **Connection Profiles:** Use for all site-to-site connection profiles.

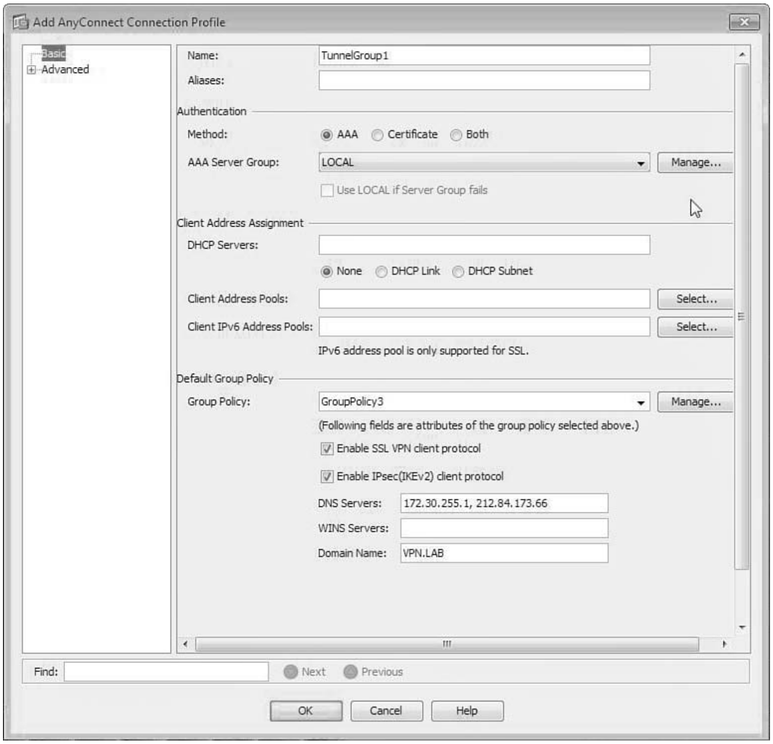
After navigating to the appropriate area, create a connection profile by selecting **Add** on the right side of the window. The Add Connection Profile window appears, as shown in Figure 2-5.

In this window, the connection profile is given a name, the authentication method selected, and custom attributes assigned (such as IP address pools, Dynamic Host Configuration Protocol (DHCP) servers, group policies, and so on). These settings are described in detail in later chapters.

Understanding Group Policies

Key Topic

As you saw earlier, a group policy object is a container for the various attributes and post-login parameters that can be assigned to VPN users, and to endpoints such as IPv4 and IPv6 ACLs, DHCP servers, address pools, and so on.



Add AnyConnect Connection Profile

Name: TunnelGroup1

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL Manage...

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: Select...

Client IPv6 Address Pools: Select...

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: GroupPolicy3 Manage...

(Following fields are attributes of the group policy selected above.)

☑ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

DNS Servers: 172.30.255.1, 212.84.173.66

WINS Servers:

Domain Name: VPN.LAB

Find: ○ Next ○ Previous

Figure 2-5 *Connection Profile Creation*

Group policies can simplify the configuration required by allowing for their assignment to multiple users or connection profiles. This provides a greater level of scale, flexibility, and management when working with multiple connection methods and remote users.

Group policies may be internal (local) or external (remote). Both internal and external group policies are configured on the ASA. However, unlike internal policies, which hold their configured attributes and parameters locally on the ASA, external group policy attributes and parameters are configured and stored on external AAA servers. During a login attempt, the configured AAA authorization servers are contacted and send back the relevant policy attributes and parameters, based on the connecting user's policy assignment.

For more information about external group policy objects, see Chapter 4, "Advanced Authentication and Authorization of AnyConnect VPNs." For the remainder of this section, we focus only on the deployment and configuration of local group policies.

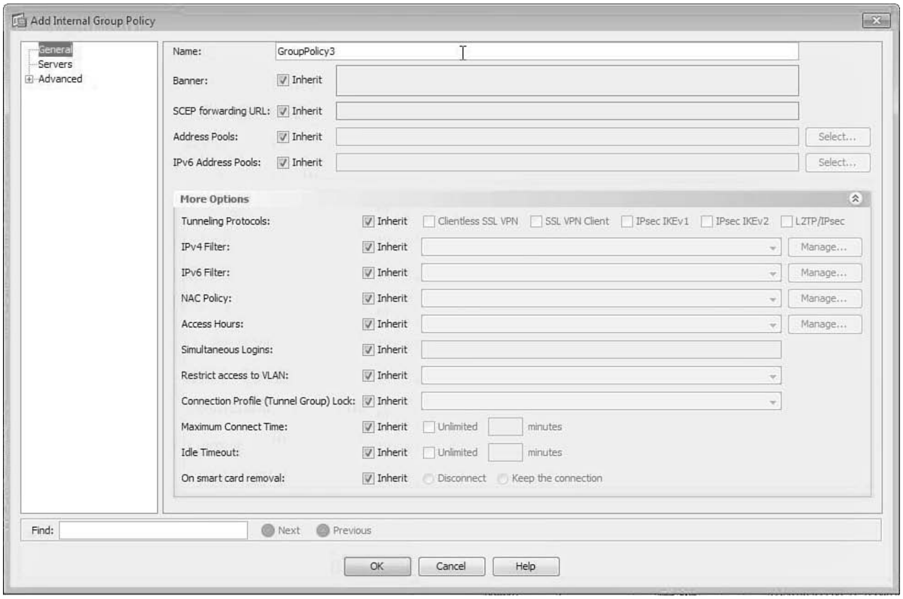
Group policies, as previously mentioned, are applied to either a connection profile or a user account directly. They do not provide any function while they are unassigned.

Although we can select the connection method that a group policy can apply to (for example, IKEv1, IKEv2, or AnyConnect SSL), unlike connection profiles, group policy objects are not locally specific to a connection profile type. If we create a group policy in the Network (Client) Access area of the ASDM for our AnyConnect or IPsec remote-access clients, the same group policy is globally available among the other connection types, and we can select, edit, or delete it within the Group Policies section of the Site-to-Site or Clientless SSL VPN areas of the ASDM. This enables us to reuse our group policy objects, not just by multiple connection profiles of the same type, but by all connection profile types and remote users regardless of their connection method (depending on the configured protocols in the group policy itself). However, not all configuration areas or items may be available, depending on the configuration area you are using to add or edit your group policy object. For example, when configuring a site-to-site group policy object, there is no need for us to be able to see all the remote user-specific attributes and parameters that might be assigned, because they are unavailable for use in the connection type being configured.

Group policy objects are configured in any one of these three areas:

- **Configuration > Remote Access VPN > Network (client) Access > Group Policies**
- **Configuration > Remote Access VPN > Clientless SSL VPN > Group Policies**
- **Configuration > Site-to-Site VPN > Group Policies**

Select **Add > Internal Group Policy**, and the window shown in Figure 2-6 appears.



Name: GroupPolicy3

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

Tunneling Protocols: ☑ Inherit □ Clientless SSL VPN □ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

IPv4 Filter: ☑ Inherit

IPv6 Filter: ☑ Inherit

NAC Policy: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

On smart card removal: ☑ Inherit ○ Disconnect ○ Keep the connection

Figure 2-6 *Internal Group Policy Creation*

We begin by giving our group policy object a name, a banner, and address pools. If we expand the **More Options** section of the window, we are presented with a greater list of parameters that may be configured to further tailor the experience our remote users have when connecting to our VPN deployment. All these options are covered in later chapters. For now, it is just important to at least know they exist and how to get to them.

You might have noticed also in Figure 2-6 that all the fields in the Add Internal Group Policy window have the Inherit option in front of them. Similar to connection profiles, the ASA also has a default group policy object DfltGrpPolicy that cannot be deleted. However, its properties can be modified and indirectly applied to our configured group policies, as they all by default inherit the settings configured in DfltGrpPolicy.

Configure User Attributes

We have several choices of which users to use. We can use local users or remote users that have been created specifically for our deployment on RADIUS, TACACS+, or other remote AAA servers. We can also use an existing database of users. For example, a company might want to use their existing Microsoft Windows Active Directory deployment for the management of new users and allow their internal users to connect into their environment remotely.

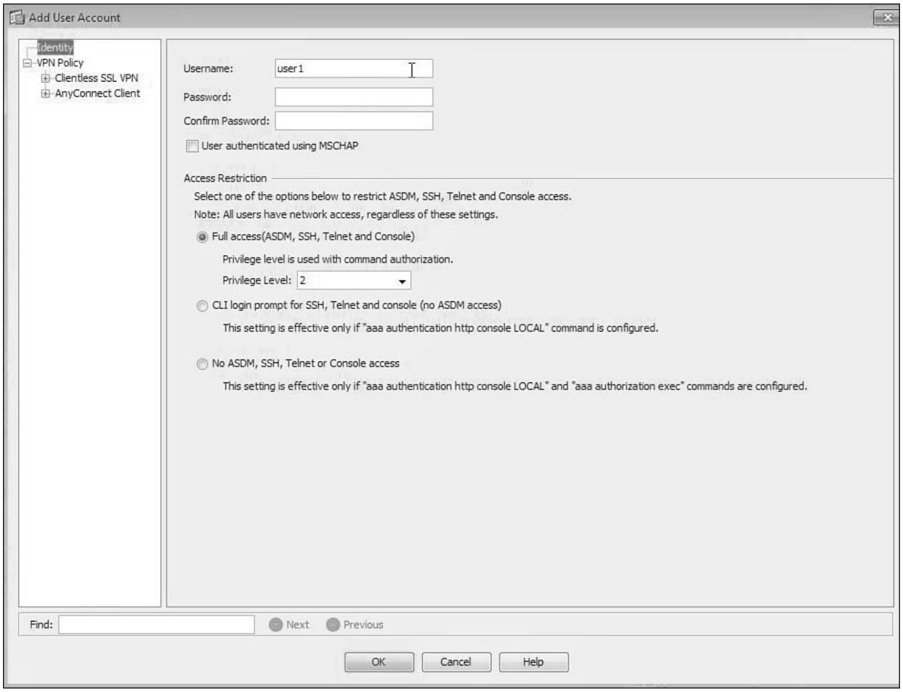
Many of the examples in this book use the internal user database (local users) available on the ASA. The policies and parameters we can assign to either local or remote users are the same by using either connection profiles or group policy objects. However, in a locally configured user, we can also assign attributes and policy objects directly to their user account using the various properties available. (For example, in the preceding sections we discussed the assignment of group policies and connection profiles to a user account directly.)

Local user accounts are configured on the ASA device in the **Device Management > Users/AAA > User Accounts** area of the ASDM. Begin by creating a new user account, shown in Figure 2-7, by selecting **Add**.

We enter a username, password, and the type of management access our user will have to the ASA device (for example, telnet, Secure Shell [SSH], ASDM). Depending on the type of user account we are creating (VPN User, Management Only, VPN User with Management Functions), select the appropriate level of management access to the ASA to grant the user. By default, any new user accounts created are given the option of Full Access to the ASA. However, if our users are only created for the purposes of connecting to our VPNs, there is no requirement for them to have management access to the ASA, and this option should be changed to **No ASDM**, **SSH**, **Telnet, or Console Access** instead.

We can further customize the user experience during their VPN connection by assigning the various options available, either when connecting through a clientless SSL VPN session or AnyConnect full-tunnel session (for example, bookmark lists, Smart Tunnel applications and access, manual or automatic download of the AnyConnect client). However, it is recommended if you have multiple users in your VPN deployment that all have similar parameters and settings attached to their account. Assignment of these attributes should be carried out using group policy objects or connection profiles for ease of management.

As you continue through this book, you will see the creation of local user accounts in detail, along with the advanced attributes that are available to them and the results that occur after their assignment.



Username: user1

Password:

Confirm Password:

☐ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

○ No ASDM, SSH, Telnet or Console access

This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Figure 2-7 *ASDM Local User Account Creation*

Using External Servers for AAA and Policies

As briefly discussed earlier, not only can we use remote AAA servers for the purposes of user creation and management, we can also use them for the purposes of policy assignment using external group policies.

The use of an external AAA server for the purposes of policy assignment is recommended. This provides centralized policy storage and management where a VPN deployment might have more than one ASA device available (for example, when using two or more ASA devices in a VPN cluster).

Key Topic

The ASA device supports the following external AAA server types and protocols for authorization purposes:

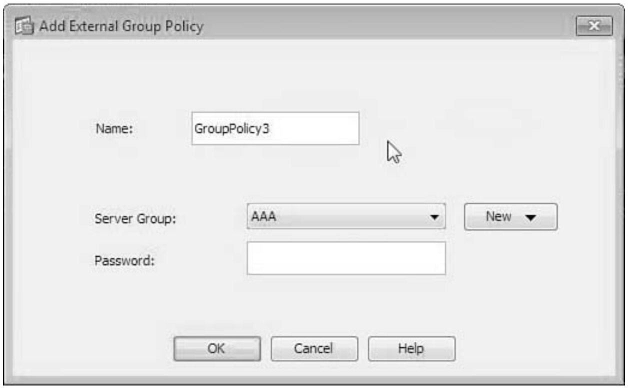
- RADIUS
- TACACS+
- LDAP
- NT Domain
- SDI
- Kerberos
- HTTP Form

Only two of the protocols are available for use with external group policy assignment: RADIUS and Lightweight Directory Access Protocol (LDAP). In earlier ASA releases, TACACS+ was also available for external policy assignment. However, because of the lack of support offered by the protocol for the purposes of policy assignment compared to the parameters offered by RADIUS and LDAP, TACACS+ has been removed for this purpose. (TACACS+ support has been removed for use with external group policy assignment only; the protocol still exists for use as an AAA server for user authentication purposes.)

To create a new external group policy object whose name will exist on the ASA device (although all attributes that are stored in the group policy exist only on the configured RADIUS or LDAP server), navigate to one of the following locations:

- **Configuration > Remote Access VPN > Network (client) Access > Group Policies**
- **Configuration > Remote Access VPN > Clientless SSL VPN > Group Policies**
- **Configuration > Site-to-Site VPN > Group Policies**

Select **Add > External Group Policy** to begin the configuration process, shown in Figure 2-8.



Name: GroupPolicy3

Server Group: AAA

Password:

Figure 2-8 *ASDM Local User Account Creation*

The ASA asks for very few parameters in comparison to when creating an internal group policy, because we are only creating the container or name for the group policy on the ASA and specifying the AAA server that will store the policy attributes along with the password the ASA uses to authenticate against it.

Table 2-2 lists the available RADIUS attributes, attribute number, type, and values, respectively, which you may configure on an external RADIUS or LDAP server for the purposes of user policy assignment.

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
Access-Hours	1	String	Name of the time range (for example, Work Time)
Simultaneous-Logins	2	Integer	A number between 0 and 2,147,483,647
Primary-DNS	5	String	IP address
Secondary-DNS	6	String	IP address
Primary-WINS	7	String	IP address
Secondary-WINS	8	String	IP address
SEP-Card-Assignment	9	Integer	Not used
Tunneling-Protocols	11	Integer	1 = PPTP 2 = L2TP 4 = IPsec 8 = LT2P/IPsec 16 = WebVPN 4 and 8, mutually exclusive 0–11 and 16–27, legal values
IPsec-Sec-Association	12	String	Name of SA
IPsec-Authentication	13	Integer	0 = None 1 = RADIUS 2 = LDAP (auth only) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS with expiry 7 = Kerberos/AD
Banner1	15	String	Banner string
IPsec-Allow-Passwd-Store	16	Boolean	0 = Disabled 1 = Enabled
Use-Client-Address	17	Boolean	0 = Disabled 1 = Enabled

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
PPTP-Encryption	20	Integer	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required 15 = 40/128-Encr/Stateless-Req
L2TP-Encryption	21	Integer	Bitmap: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-required 15 = 40/128-Encr/Stateless-Req
Group-Policy Pre 8.2 use IETF-RADIUS-Class	25	String	Use one of the following formats <group policy name> OU=<group policy name>
IPsec-Split-Tunnel-List	27	String	Name of the ACL used for split tunneling
IPsec-Default-Domain	28	String	Client default domain name. Enter 1–255 characters.
IPsec-Split-DNS-Names	29	String	Client secondary default domain name. Enter 1–255 characters.
IPsec-Tunnel-Type	30	Integer	1 = LAN-to-LAN 2 = Remote access
IPsec-Mode-Config	31	Boolean	0 = Disabled 1 = Enabled
IPsec-User-Group-Lock	33	Boolean	0 = Disabled 1 = Enabled
IPsec-Over-UDP	34	Integer	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	35	Integer	4001–49151 Default = 10000
Banner2	36	String	If configured banner string is concatenated to banner1

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
PPTP-MPPC-Compression	37	Integer	0 = Disabled 1 = Enabled
L2TP-MPPC-Compression	38	Integer	0 = Disabled 1 = Enabled
IPsec-IP-Compression	39	Integer	0 = Disabled 1 = Enabled
IPsec-IKE-Peer-ID-Check	40	Integer	1 = Required 2 = If supported by peer certificate 3 = Do not check
IKE-Keep-Alive	41	Boolean	0 = Disabled 1 = Enabled
IPsec-Auth-On-Rekey	42	Boolean	0 = Disabled 1 = Enabled
Required-Client-Firewall-Vendor-Code	45	Integer	1 = Cisco Systems (with Cisco integrated client) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems (with Cisco IPS agent)
Required-Client-Firewall-Product-Code	46	Integer	Cisco Systems Products: 1 = Cisco IPS Agent or CIC Zone Labs Products: 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE Product: 1 = BlackICE Defender/Agent Sygate Products: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Client-Firewall-Description	47	String	Enter a description

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
Require-HW-Client-Auth	48	Boolean	0 = Disabled 1 = Enabled
Required-Individual-User-Auth	49	Integer	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	50	Integer	1–35,791,394 minutes
Cisco-IP-Phone-Bypass	51	Integer	0 = Disabled 1 = Enabled
IPsec-Split-Tunneling-Policy	55	Integer	0 = No split tunneling 1 = Split tunneling 3 = Local LAN permitted
IPsec-Required-Client-Firewall-Capability	56	Integer	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server
IPsec-Client-Firewall-Filter-Name	57	String	Enter the name of the firewall policy filter
IPsec-Client-Firewall-Filter-Optional	58	Integer	0 = Required 1 = Optional
IPsec-Backup-Servers	59	String	1 = Use client-configured list 2 = Disable and clear client list 3 = Use backup server list
IPsec-Backup-Server-List	60	String	Server addresses (space, delimited)
DHCP-Network-Scope	61	String	IP address
Intercept-DHCP-Configure-Msg	62	Boolean	0 = Disabled 1 = Enabled
MS-Client-Subnet-Mask	63	Boolean	IP address
Allow-Network-Extension-Mode	64	Boolean	0 = Disabled 1 = Enabled

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
Authorization-Type	65	Integer	0 = None 1 = RADIUS 2 = LDAP
Authorization-Required	66	Integer	0 = No 1 = Yes
Authorization-DN-Field	67	String	Possible values: UID, OU, O, CN, L, SP, C, EA, T, N, SN, I, GENQ, DNQ, SER, use-entire-name
IKE-Keepalive-Confidence-Interval	68	Integer	10–300 seconds
WebVPN-Content-Filter-Parameters	69	Integer	1 = JAVA ActiveX 2 = JavaScript 3 = Image 4 = Cookies in images
WebVPN-URL-List	71	String	Url-list-name
WebVPN-Port-Forward-List	72	String	Port-forward list name
WebVPN-Access-List	73	String	Access list name
Cisco-LEAP-Bypass	75	Integer	0 = Disabled 1 = Enabled
WebVPN-Homepage	76	String	Enter the URL of the home page
Client-Type-Version-Limiting	77	String	IPsec VPN version number string
WebVPN-Port-Forwarding-Name	79	String	Example: “Company Apps” replaces the Application Access string on the clientless SSL VPN portal page
IE-Proxy-Server	80	String	IP address
IE-Proxy-Server-Policy	81	Integer	0 = No Modify 1 = No Proxy 2 = Auto Detect 3 = Use Concentrator Setting
IE-Proxy-Exception-List	82	String	Newline (\n) separated list of DNS domains

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
IE-Proxy-Bypass-Local	83	Integer	0 = None 1 = Local
IKE-Keepalive-Retry-Interval	84	Integer	2–10 seconds
Tunnel-Group-Lock	85	String	Name of the tunnel group or None
Access-list-inbound	86	String	Access list ID
Access-list Outbound	87	String	Access list ID
Perfect-Forward-Secret-Enable	88	Boolean	0 = No 1 = Yes
NAC-Enable	89	Integer	0 = No 1 = Yes
NAC-Status-Query-Timer	90	Integer	30–1,800 seconds
NAC-Revalidation-Timer	91	Integer	300–86,400 seconds
NAC-Default-ACL	92	String	Access-list
WebVPN-URL-Entry-Enable	93	Integer	0 = Disabled 1 = Enabled
WebVPN-File-Access-Enable	94	Integer	0 = Disabled 1 = Enabled
WebVPN-File-Server-Entry-Enable	95	Integer	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	96	Integer	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Enable	97	Integer	0 = Disabled 1 = Enabled
WebVPN-Outlook-Exchange-Proxy-Enable	98	Integer	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	99	Integer	0 = Disabled 1 = Enabled

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
WebVPN-Auto-Applet-Download-Enable	100	Integer	0 = Disabled 1 = Enabled
WebVPN-Citrix-Metaframe-Enable	101	Integer	0 = Disabled 1 = Enabled
WebVPN-Apply ACL	102	Integer	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Enable	103	Integer	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	104	Integer	0 = Disabled 1 = Enabled
WebVPN-SSL-Client-Keep-Installation	105	Integer	0 = Disabled 1 = Enabled
SVC-Keepalive	107	Integer	0 = Off 15–600 seconds
SVC-DPD-Interval-Client	108	Integer	0 = Off 5–3600 seconds
SVC-DPD-Interval-Gateway	109	Integer	0 = Off 5–3600 seconds
SVC-Rekey-Time	110	Integer	0 = Disabled 1–10,080 minutes
WebVPN-Deny-Message	116	String	Valid string (up to 500 characters)
Extended-Authentication-On-Rekey	122	Integer	0 = Disabled 1 = Enabled
SVC-DTLS	123	Integer	0 = False 1 = True
SVC-MTU	125	Integer	MTU value 256–1,406 in bytes
SVC-Modules	127	String	String (name of module)
SVC-Profiles	128	String	String (name of profile)

Table 2-2 *Supported RADIUS Attributes and Values*

Attribute Name	Attribute Number	Type	Value
SVC-Ask	131	String	0 = Disabled 1 = Enabled 3 = Enabled default service 5 = Enable default clientless
SVC-Ask-Timeout	132	Integer	5–120 seconds
IE-Proxy-PAC-URL	133	String	PAC address
Strip-Realm	135	Boolean	0 = Disabled 1 = Enabled
Smart-Tunnel	136	String	Name of Smart Tunnel
WebVPN-ActiveX-Relay	137	Integer	0 = Disabled Otherwise = Enabled
Smart-Tunnel-Auto	138	Integer	0 = Disabled 1 = Enabled 2 = AutoStart
Smart-Tunnel-Auto-Signon-Enable	139	String	Name of Smart Tunnel auto sign-on list appended by domain name
VLAN	140	Integer	0–4094
NAC-Settings	141	String	Name of NAC policy
Member-Of	145	String	Comma-separated string (for example, Engineering, Sales)
Address-Pool	217	String	Name of IP local pool
IPv6-Address-Pool	218	String	Name of IP local pool
IPV6-VPN-Filter	219	String	ACL name
Privilege-level	220	Integer	Enter between 0 and 15
WebVPN-Macro-Value1	223	String	Unbounded. See the SSL VPN Deployment Guide at Cisco.com for examples.
WebVPN-Macro-Value-2	224	String	Unbounded. See the SSL VPN Deployment Guide at Cisco.com for examples.

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 memory tables in Appendix C, Chapter 23, "Final Exam Preparation," and the exam simulation questions on the CD-ROM.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 2-3 lists a reference of these key topics and the page numbers on which each is found.

Table 2-3 *Key Topics*

Key Topic Element	Description	Page
Bulleted List	The benefits of the modular policy assignment of the ASA	49
List	ASA policy inheritance	50
Bulleted List	Available connection profile selection and assignment methods	52
Bulleted List	Default connection profiles	55
Topic	Understanding group policies	56
Bulleted List	Available AAA server types and protocols	60

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:

connection profile, internal group policy, external group policy

Index