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

Copyright © 2012 Pearson Education, Inc.

Published by:

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

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.

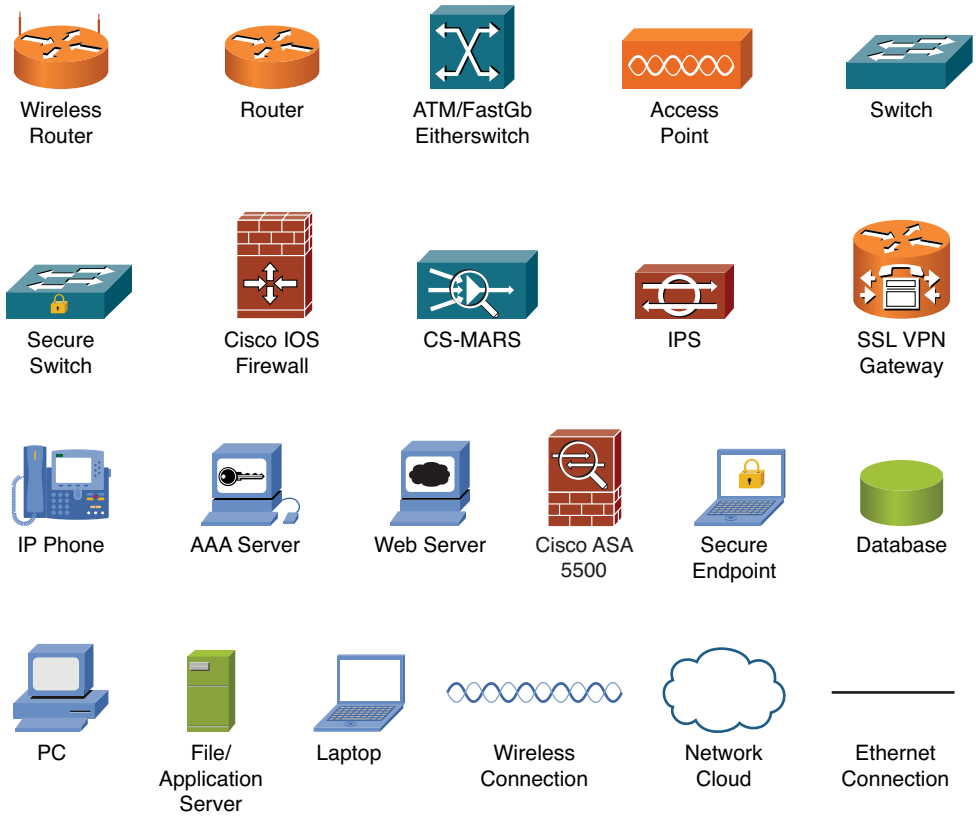
Thanks must also go out to the two technical reviewers, Chris Turpin and Cristian Matei. Your comments and suggestions have been a great help throughout the entire book. Your input has definitely made this version of the book better.

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

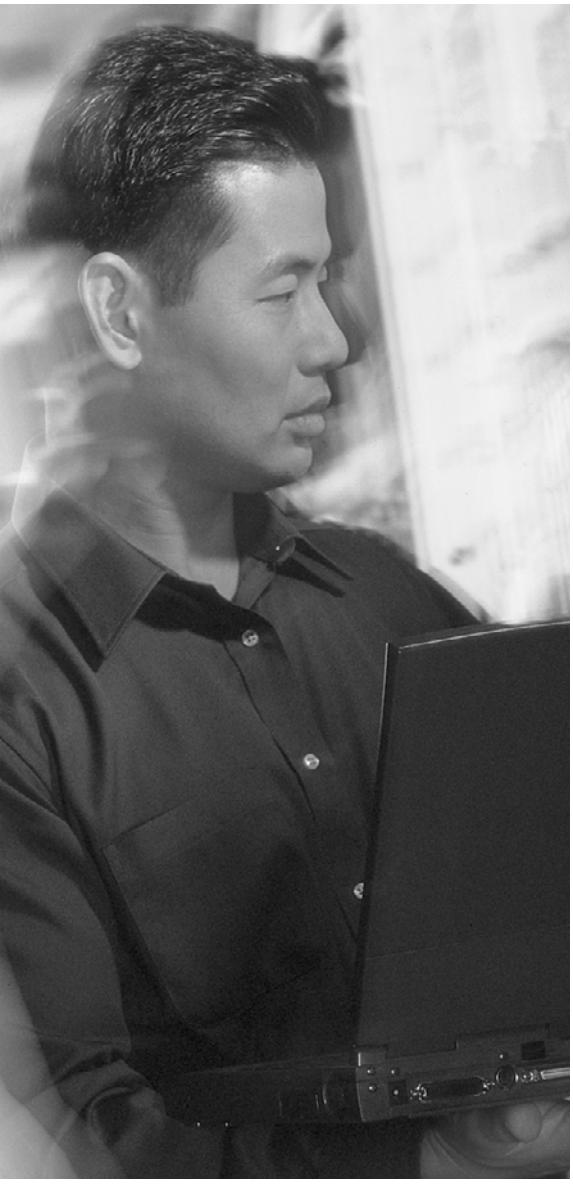
The VPN exam is a computer-based exam, with multiple-choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (www.pearsonvue.com) testing center. Your testing center can tell you the exact length of the exam. Be aware that when you register for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

- **Introducing the Virtual Private Network:** In this section, you learn what a VPN is and the role it can play within and outside of an organization. In addition, VPN methods available on the ASA are discussed and compared.
- **Meet the Protocols:** This section introduces you to the all-important protocols that operate either independently or together to enable a VPN connection to successfully establish. As you move through the rest of this book, you might want to refer to this section to remind yourself of protocol-specific details.
- **ASA Packet Processing:** This section discusses the process that is followed by the ASA device for a packet traveling through it both inbound toward your internal environment and outbound away from it.
- **The Good, the Bad, and the Licensing:** This section discusses the overall licensing model used by the ASA, the implementation of optional features, and licensing requirements that might apply.

CHAPTER 1

Examining the Role of VPNs and the Technologies Supported by the ASA

So, you just received your first brand-new *Adaptive Security Appliance (ASA)* device and have unpacked the box. Your heart and mind fill with excitement as you stare at the shining rectangular, rack-mountable beacon of near-endless security possibilities. You let out a faint giggle as the flick of the rear power switch causes a rush of cool air to escape from the built-in fan mechanisms, and the intense flash of the front and rear LEDs suggests that your new friend shares your enthusiasm to start building a new secure future. You decide the first thing you want to do is to give the ASA an IP address so that you and the ASA can start to communicate with each other properly, but how? You then realize that you have purchased the *CCNP Security VPN Certification Guide* and not the ASA all-in-one how-to book you really need.

Yes, the preceding paragraph might provide some of you with the warm feeling of nostalgia and others with a cringe-like sensation. However, you have learned an important piece of information: This book is *not* a how-to-do-everything-on-an-ASA manual. Instead, as we work through the various information, facts, and examples together, I am assuming you already have a good understanding of the various *virtual private network (VPN)* and ASA architectures.

This chapter serves as a review for much of the ASA and its overall operation. However, as we move through the chapter, we start to explore more VPN-specific information in the form of their security, the protocols used, and their operation. We then finish the discussion with a look at the various licenses available on the ASA device and which ones you might need for the successful deployment and operation of the technologies we explore throughout this book.

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

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

Foundation Topics Section	Questions
Examining ASA Control Fundamentals	4, 5, 6
Routing the Environment	3
Address Translations and Your ASA	2
ASA VPN Technology Comparison	1
Managing Your ASA Device	7
ASA Packet Processing	8, 9

1. Which of the following are available VPN connection methods on the ASA? (Choose all that apply.)
   - **a.** Clientless SSL
   - **b.** AnyConnect IKEv2
   - **c.** Easy VPN IKEv2
   - **d.** AnyConnect SSL
2. Which of the following are processes achieved by secure VPNs? (Choose all that apply.)
   - **a.** Authentication
   - **b.** Antireplay
   - **c.** Hashing
   - **d.** Integrity
3. Which of the following are valid encryption protocols? (Choose all that apply.)
   - **a.** 3DES
   - **b.** DES
   - **c.** MD5
   - **d.** Diffie-Hellman
4. Which of the following are valid characterizations of key encryption protocols? (Choose all that apply.)
   - **a.** Asymmetric
   - **b.** Bidirectional
   - **c.** Symmetric
   - **d.** One-Way

5. Which of the following would be considered a valid type of VPN? (Choose all that apply.)
   a. VLAN
   b. X.25
   c. Ethernet
   d. IPsec site-to-site
6. What is the key size used by the DES encryption protocol?
   a. 168
   b. 256
   c. 56
   d. 64
7. What are the two IKE methods used by the IPsec protocol for secure tunnel negotiation? (Choose all that apply.)
   a. IKEv1
   b. IKE-New
   c. IKEv2
   d. IKEng
8. Which of the following is not a valid packet-processing action taken by the ASA for flows traveling from the inside interface to the outside interface?
   a. NAT host check
   b. Route lookup
   c. IP options lookup (MPF)
   d. NAT (RPF)
9. Which of the following is the recommended tool for viewing the path a packet takes through the ASA device?
   a. Traceroute
   b. Ping
   c. Packet Tracer
   d. SNMP

Foundation Topics

Introducing the Virtual Private Network

Although you might not have noticed, *virtual private networks (VPN)* have been used within and between many organizations for some time now. When the term *VPN* is used, many people immediately think of an IPsec site-to-site or remote-access VPN providing private connectivity between or into organizations. Although both of these methods are valid types of VPN connectivity, there are also many other technologies that because of their use and function can be characterized as a VPN type or method, including the following:

- *Virtual local area networks (VLAN)* are a common VPN type that achieve the privacy and segmentation of networks by means of a tag or encapsulation method applied to network data.
- *Multiprotocol Label Switching (MPLS)* VPNs operate by appending multiple labels to a data packet to provide private connectivity throughout or between networks across a WAN.
- *Generic routing encryption (GRE)* or IP-in-IP tunneling methods create a private connection between devices by appending header information to an assembled packet for the formation of a point-to-point tunnel.
- Legacy VPN types that were commonly used to provide WAN connectivity between organizations (for example, X.25, Frame Relay, and ATM).

This list of VPN types above is not exhaustive, but it does give you a good idea about the various roles VPNs play. Put simply, VPNs provide private connectivity between devices operating over a shared infrastructure and can generally be categorized in two types: those that offer privacy through various isolation methods (VLANs, MPLS VPNs), and those that offer both privacy and security (IPsec/*Secure Sockets Layer [SSL]* VPNs). The security provided for VPNs is achieved by the implementation of cryptographic protocols (for example, IPsec, SSL, and Transport Layer Security [TLS], to name a few). This book focuses on the VPN methods that provide both privacy and security between both remote sites and remote users and a central site. VPNs of this sort provide three basic benefits:

- **Authentication:** This can be achieved through the use of usernames and passwords, *pre-shared keys (PSK)*, *one-time passwords (OTP)* or tokens, *public key infrastructure (PKI)* and digital certificates, or a combination of these. The primary purpose of authentication is to make sure you are who you say you are.
- **Confidentiality:** Provided by encrypting user data before transmission through the established VPN tunnel with the aim of preventing any data that may be captured by an attacker.

- **Integrity:** Provides a means to ensure data has not been tampered with along the path between the source and destination (for example, by an attacker attempting to perform a man-in-the-middle attack).
- **Antireplay:** The sending device can add sequence numbers to each packet sent through the VPN tunnel and thus allow the receiving end (ASA) to determine whether, in an effort to overcome the security measures provided by the VPN, a packet has been duplicated.

Although the process of encrypting (and therefore, hiding) data is often assumed with VPN operation, all functions just listed are optional and are carried out by a specific protocol.

The secure VPN methods covered within this book are those capable of providing connectivity either between organizations (site to site) or between remote users and an organization (remote access). The CCNP Security VPN exam covers the following VPN methods and their associated protocols supported by the ASA:

- IPsec remote access (IKEv1)
- Easy VPN Remote client and server (IKEv1)
- Easy VPN Remote hardware client (ASA 5505 only)
- Clientless SSL remote access
- AnyConnect SSL remote access (SSL/TLS)
- AnyConnect IKEv2 remote-access (SSL/TLS and *Datagram Transport Layer Security [DTLS]*)
- IPsec site to site (IKEv1 and IKEv2) (ASA 8.4 allows for *LAN-to-LAN [L2L]* tunnels using both IKEv1 and IKEv2.)

Table 1-2 lists the methods and their typical deployment scenarios, IP addressing, feature support, and so on.

Table 1-2 *Advantages and Limitations of Available ASA VPN Methods*

	IPsec Remote Access	Easy VPN	Clientless SSL
Protocol	IPsec/IKEv1	IPsec/IKEv1	SSL/TLS
Client based/ remote access/site to site	Cisco IPsec VPN client	ASA 5505 hardware client Site to site/remote access on supported client device	Clientless browser based
Client IP addressing	Supported	Supported	Not supported All traffic tunneled

	IPsec Remote Access	Easy VPN	Clientless SSL
High availability (HA) support	Stateful	Stateful	Stateless
Management/ deployment overhead	Configuration on the ASA required Manual installation and distribution of Cisco IPsec VPN client software	Configuration on the local and remote ASA device Basic configuration required on ASA 5505 Policy deployed during connection	Configuration on the ASA required
Policy update/ configuration change method	Manual configuration for client authentication changes and so on in the Cisco IPsec VPN client	Automatic policy download and update during connection establishment	Requires client to log out and back in to the web interface for updates to portal to take effect
Client authentication methods	XAUTH (AAA or ASA local user authentication). Certificates. Hybrid SDI can be used with PSK only.	XAUTH (AAA or ASA local user authentication). Additionally for hardware client SUA and IUA.	AAA or ASA local user authenticaton cDigital Certificates. SDI.
LAN extension	Yes	Yes	No (unless smart tunnels are configured)
Standards-based access method/ protocols	Yes	Proprietary	Yes

Key Topic

Table 1-2 Continued *Advantages and Limitations of Available ASA VPN Methods*

	AnyConnect SSL	AnyConnect IKEv2	IPsec Site to Site
Protocol	SSL/TLS/DTLS	IKEv2	IPsecIKEv1/IKEv2
Client based/remote access/site to site	AnyConnect Secure Mobility Client	AnyConnect Secure Mobility Client	Remote router, firewall, or concentrator device
Remote client IP addressing	Supported	Supported	N/A
HA support	Stateful	Stateful	Stateful

	AnyConnect SSL	AnyConnect IKEv2	IPsec Site to Site
Management/ deployment overhead	Configuration on the ASA required Automatic download and installation/upgrade of AnyConnect client software	Configuration on the ASA required Automatic download and installation/ upgrade of AnyConnect client software	Configuration on the ASA required and matching configuration on remote devices
Policy update/ configuration change method	Automatic download and installation of policy updates during connection establishment	Automatic download and installation of policy updates during connection establishment	Remote devices must manually update their policies/settings to match
Client authentication methods	User AAA or local ASA user based, certificates, SDI	AAA or ASA local user authentication. Certificates. *Standards-based Extensible Access Protocol (EAP)* methods. Cisco proprietary EAP	N/A
LAN extension (full tunnel)	Yes	Yes	Yes
Standards-based access method/protocols	Yes	Yes	Yes

Based on the information shown in the preceding table, it is safe to assume that if you require a site-to-site VPN providing LAN extension services between two Cisco devices, an Easy VPN client/server deployment should meet your requirements. However, if you have the same requirements but the remote endpoint is a checkpoint or other third-party device, you need to use a standard IKEv1/IKEv2 IPsec site-to-site VPN connection.

If you concentrate on the remote-access VPN methods, a clientless SSL VPN-based deployment may meet the needs of your remote users based on ease of deployment and policy update procedures. However, if your remote users also require full LAN extension (that is, to be able to seamlessly access internal resources and servers as though working from in the office), an AnyConnect SSL or IKEv2 VPN should be implemented because of the minimal support for this access method offered with the browser-based clientless SSL VPN.

You may choose to deploy a clientless SSL VPN if your remote users operate a number of web-based applications that do not require their remote devices to have an IP address or use complicated dynamic protocols for access to internal resources. However, as

discussed in later chapters, a degree of application and server access can be provided to remote users through the implementation of smart tunnels, port forwarding, and plug-ins.

One benefit provided by the ASA is the device's ability to provide multiple VPN connectivity methods simultaneously. For example, you may have one or more site-to-site IKEv1/IKEv2 IPsec VPN tunnels established between your ASA and remote ASAs and at the same time allow clientless SSL, full-tunnel (client-based) SSL, and IPsec remote-access VPN connections, as shown in Figure 1-1. In addition, the ASA can provide multiple sessions per connectivity method (the limit depending on the ASA platform chosen). For example, if your organization has a requirement to establish a secure site-to-site VPN connection between one or more remote sites, depending on the number of tunnels that are required between your organization and others the ASA may be able to terminate all the sessions simultaneously instead of just one at a time.

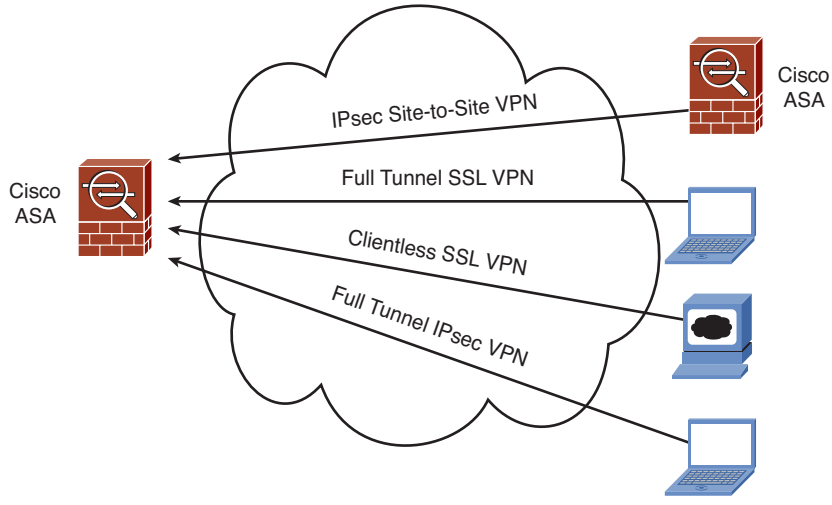


Figure 1-1 *Available VPN Methods on the ASA*

Later in this chapter, the "Meet the Protocols" section introduces you to the various underlying protocols that are used along with the VPN methods discussed earlier.

VPN Termination Device (ASA) Placement

When implementing a new device for the purposes of VPN termination within your organization, you need to decide whether to place the device within your existing topology. This is usually somewhere near or at the perimeter of your network. The following three common design methodologies are recommended and used when deploying a VPN termination device into an existing network:

- In parallel with a firewall device, as shown in Figure 1-2
- Inline with a firewall device, as shown in Figure 1-3

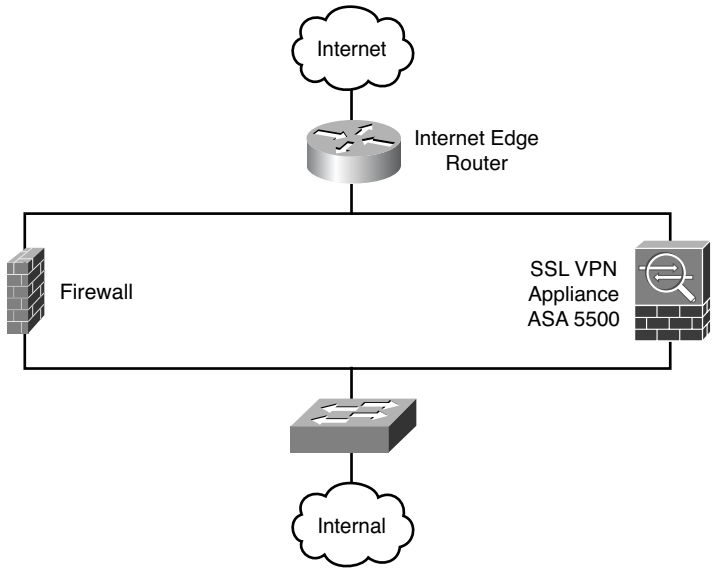


Figure 1-2 *VPN Appliance Parallel Topology*

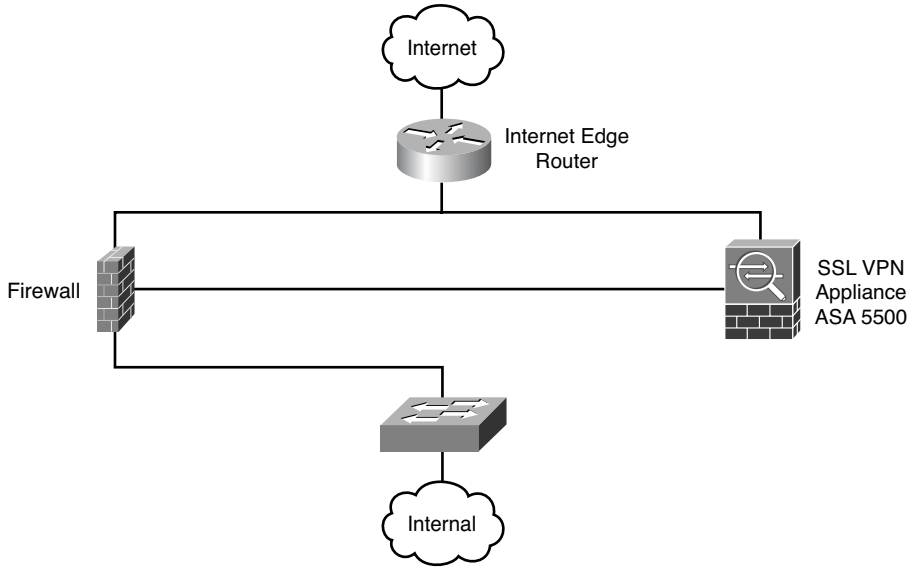


Figure 1-3 *VPN Appliance Inline Topology*

- Inside a *demilitarized zone (DMZ)* for greater segregation from your network, as shown in Figure 1-4

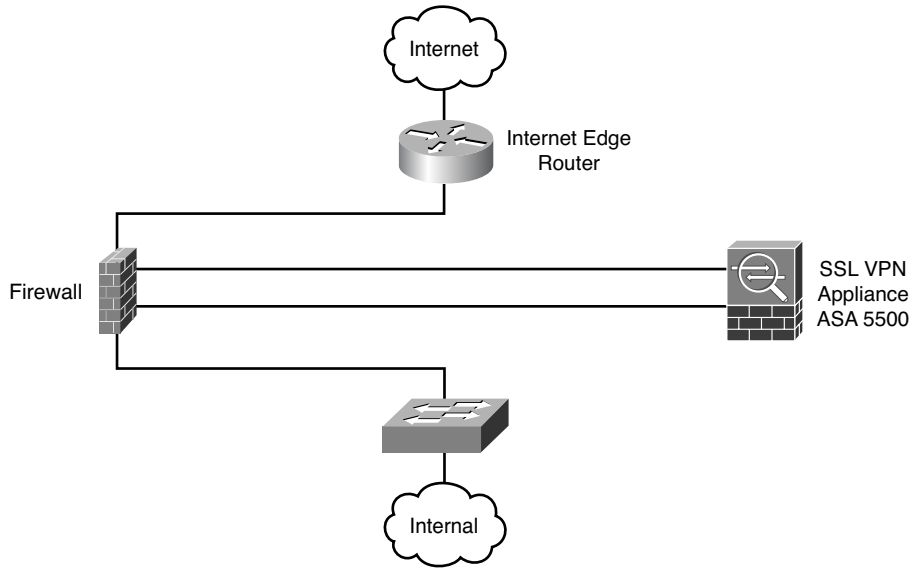


Figure 1-4 *VPN Appliance DMZ Topology*

The most popular design is to place the VPN appliance into its own DMZ, allowing for greater scale and ease of management. Unlike the parallel design, this removes the threat of attackers from the Internet being able to have direct public access to your device without first having to pass through a firewall. It also removes the possibility of inbound traffic being checked by the firewall twice, which can happen when using the inline design.

It is also important to remember that ASA 5500 devices are also firewall devices. If you are designing the topology for a *small to medium business (SMB)* network, you also have the possibility of "collapsing" the two roles (SSL VPN termination and firewall) into the same physical device to minimize the overall cost of deployment.

Meet the Protocols

As the title of this section suggests, the information that follows introduces the various protocols that work either independently or in collaboration to provide a secure tunnel and means of data transmission for the purposes of providing remote users and sites access to your internal resources. However, this access is provided in a manner without compromising your internal security policies. As you move through the remaining chapters and configuration examples in this book, notice the role of each protocol and how they operate to provide the overall method of VPN connectivity.

Symmetric and Asymmetric Key Algorithms

The sections that follow cover the operation of IPsec, SSL/TLS, and DTLS. Before these protocols can establish a secure communications tunnel (VPN) between two endpoints,

they generate, exchange, and use keys as a means to authenticate/encrypt the information used to create a secure tunnel that is sent between both parties. As you read on through the later sections in this chapter, note that each protocol goes through specific stages when establishing a secure tunnel. Depending on the stage they are at in their negotiations, either a symmetric or asymmetric encryption protocol is used.

So, what are symmetric and asymmetric key algorithms? Well, without noticing, you've probably come across them, heard of them, and no doubt have used them without even knowing (when shopping online, for example).

During their operation, symmetric key algorithms generate and use a single key for the purposes of encrypting and decrypting data. Examples of symmetric key algorithms include *Digital Encryption Standard (DES)*, *Triple DES (3DES)*, *and Advanced Encryption Standard (AES)*. The downside with using a single key for both encryption and decryption is just that: If attackers gain access to the key used for encrypting sensitive data, they are automatically able to decrypt and read it. Some argue that symmetric key algorithms are subject to brute-force attacks (given enough computing power), whereby attackers attempt to "guess" the key by literally trying number after number against an encrypted piece of data. However, efforts have been made to overcome this problem, mainly by the introduction of a larger key size. Examples of symmetric algorithms and their key sizes include the following:

- DES uses a key size of 56 bits.
- 3DES uses a key size of 168 bits.
- AES offers 128, 192, 256 key sizes.

Symmetric encryption algorithms are prone to a specific problem: the process of key exchange. As mentioned earlier, for two parties to be able to encrypt and decrypt data they must both be in possession of the same key. However, this means the encryption/decryption key must be exchanged somehow, which leaves it open to potential attackers if, for example, the key is exchanged in an email. Therefore, asymmetric encryption protocols are commonly used to set up a secure communications path for the purpose of exchanging the symmetric key.

Instead of using one single key to perform the encryption/decryption operation, asymmetric key algorithms use a key pair, one key for encryption and one key for decryption. Because of a mathematical relationship of the two keys generated, a piece of information or data that has been encrypted can be decrypted only by the key that belongs to the corresponding key pair of the encryption key used. You might have heard of the terms *public* and *private key* before. These terms refer to the keys used by asymmetric key algorithms. Usually, a public key is distributed to people who expect to receive the encrypted data (commonly using digital certificates), and a private key is kept and known only to the person encrypting the data. Public/private key pairs are also easier to distribute than keys used with symmetric algorithms. For example, if you were to send the key used by a symmetric key algorithm to decrypt some information to a host across the Internet, an attacker could likely intercept this key and the messages sent between the source and destination and could then freely decrypt and read them.

Public/private key pairs commonly use digital certificates as a method of key distribution. Internet shopping and other sites often use SSL/TLS as a way to secure transactions on their websites. In this case, you usually receive a copy of the server's digital certificate. Within the certificate is a copy of the server's public key. By using this public key, the host and server can set up a secure communications path (because the server has a corresponding private key). Examples of asymmetric key algorithms include the following:

- *Rivest, Shamir, and Adleman (RSA)*
- *Diffie-Hellman (DH)*

When working with VPNs, you will often see asymmetric key algorithms used (for example, DH used to encrypt and securely exchange symmetric keys). The sending and receiving hosts at either end of the VPN exchange symmetric keys to encrypt and decrypt any data sent. Their use is popular because of the simplicity of symmetric encryption protocols in terms of mathematics and the ability to run them within hardware at a very fast rate. However, asymmetric encryption algorithms often use larger key sizes and more-sophisticated and processor-intensive mathematical functions such as discrete logarithms or factoring large prime numbers, so their use is limited mainly to key exchange or for authentication purposes (RSA tokens).

Note Recall that symmetric and asymmetric protocols and the methods used by each to encrypt data (for example, block ciphers, stream ciphers, *Electronic Code Book [ECB]* and *Cipher Block Chaining [CBC]* used by DES) are explained in great detail within the *CCNA Security Official Exam Certification Guide* (Cisco Press).

IPsec

IPsec is composed of a collection of underlying protocols that together provide the overall operation of parameter negotiation, connection establishment, tunnel maintenance, data transmission, and connection teardown.

Three protocols are used in the IPsec architecture to provide key exchange in addition to the integrity, encryption, authentication, and antireplay features discussed earlier:

- IKEv1 or IKEv2 is used by IPsec for the exchange of parameters used for key negotiation, the exchange of the derived authentication/encryption keys, and overall establishment of *security associations (SA)*.
- *Encapsulating Security Payload (ESP)* provides a framework for the data integrity, encryption, authentication, and antireplay functions of an IPsec VPN.
- *Authentication Header (AH)* provides a framework for the data integrity, authentication, and antireplay functions. (No encryption is provided when using AH.)

IKEv1

IKEv1 provides a framework for the parameter negotiation and key exchange between VPN peers for the correct establishment of an SA.

However, the actual processes of key exchange and parameter negotiation are carried out by two protocols used by IKEv1:

- *Internet Security Association and Key Management Protocol (ISAKMP)*
- Oakley

ISAKMP takes care of parameter negotiation between peers (for example, DH groups, lifetimes, encryption [if required], and authentication). The process of negotiating these parameters between peers is required for the successful establishment of SAs. After an SA has been established, ISAKMP defines the procedures followed for correct maintenance and removal of the SA during connection termination.

Oakley provides the key-exchange function between peers using the DH protocol. DH is an asynchronous protocol, meaning each peer uses its own set of keys for communications establishment and operation between peers. However, the keys are never exchanged, providing a much higher level of security than synchronous protocols (DES, 3DES, and so on) that require both peers to use the same keys for operation. After both peers have established their shared communication path, they can proceed to exchange the keys used by the various synchronous protocols for authentication and encryption purposes.

Note You will often find the terms *ISAKMP* and *IKE* used interchangeably in earlier versions of ASA (pre 8.4) and IOS to reference IKEv1 functions and parameters. However, as discussed when working with ASA 8.4 and later, any references to IKE now include the respective version number (for example, IKEv1 or IKEv2).

Two mandatory IKEv1 phases (aptly named IKEv1 Phase 1 and IKEv1 Phase 2) must be followed by each peer before a communications tunnel can be established between them and they are ready for successful data transmission:

- **IKEv1 Phase 1:** During this phase, both peers negotiate parameters (integrity and encryption algorithms, authentication methods) to set up a secure and authenticated tunnel. This is also called a management channel because no user data is flowing through it (and it is actually a bidirectional IKE SA). Its sole scope is to handle secure Phase 2 negotiations. It is called bidirectional because both peers use only one session key to secure both incoming and outgoing traffic. Peer authentication can be carried out by one of the following methods:
  - Pre-shared keys
  - Digital certificates

- **IKEv1 Phase 2:** This second mandatory phase uses the negotiated parameters in Phase 1 for secure IPsec SA creation. However, unlike the single bidirectional SA created within Phase 1, the IPsec SAs are unidirectional, meaning a different session key is used for each direction (one for inbound, or decrypted, traffic, and one for outbound, or encrypted, traffic). This is applicable for any administrator-configured source-destination network pair. Therefore, you might end up with four unidirectional IPsec SAs if you have two source-destination network pairs defined in a VPN policy. (IPsec VPN policy configuration is discussed in later chapters.)

IKEv1 uses either IKEv1 Main mode or IKEv1 Aggressive mode in Phase 1 to carry out the actions required to build a bidirectional tunnel. It then uses IKEv1 Quick mode for Phase 2 operations.

IKEv1 Main mode (Phase 1) uses three pairs of messages (making six in total) between peers:

- **Pair 1 consists of the IKEv1 security policies configured on the device:** One peer (initiator) begins by sending one or more IKEv1 policies, and the receiving peer responds (responder) with its choice from the policies.
- **Pair 2 includes DH public key exchange:** DH creates shared secret keys using the agreed upon DH group/algorithm exchanged in pair 1 and encrypts nonces (a randomly generated number) that begin life by first being exchanged between peers. They are then encrypted by the receiving peer and sent back to the sender and decrypted using the generated keys.
- **Pair 3 is used for ISAKMP authentication:** Each peer is authenticated and their identity validated by the other using pre-shared keys or digital certificates. These packets and all others exchanged from now on during the negotiations are encrypted and authenticated using the policies exchanged and agreed upon in pair 2.

IKEv1 Aggressive mode (Phase 1) uses just three messages rather than the six used with Main mode. The same information is exchanged between peers. However, the process is abbreviated by carrying out the following actions:

- The initiator sends DH groups signed nonces (randomly generated numbers), identity information, IKEv1 policies, and so on.
- The responder authenticates the packet and sends back accepted IKEv1 policies, nonces, key material, and an identification hash that are required to complete the exchange.
- The initiator authenticates the responder's packet and sends the authentication hash.

Note Of the two available modes, Main mode is the preferred due to the lack of encryption used between hosts in Aggressive mode. Therefore, Aggressive mode makes it possible for an attacker to sniff the packets and discover peer identity information. Aggressive mode is used by default on ASAs when configuring an IPsec VPN because of the slower operation of Main mode.

During IKEv1 Quick mode (Phase 2), IKEv1 transform sets (a list of encryption and hashing protocols) used for IPsec policy negotiation and unidirectional SA creation are exchanged between peers. Regardless of the parameters/attributes selected within a transform set, the same five pieces of information are always sent:

- IPsec encryption algorithm (DES, 3DES, AES)
- IPsec authentication algorithm (MD5, SHA-1)
- IPsec protocol (AH or ESP)
- IPsec SA lifetime (seconds or kilobytes)
- IPsec mode (Tunnel, Transport)

An optional *Extended Authentication (XAUTH)* phase can also take place after successful Phase 1 SA creation. XAUTH carries out the process of end host/device authentication before a user can use the VPN connection. Be careful not to confuse this optional step with the peer authentication carried out within IKEv1 Phase 1. The difference is IKEv1 Phase 1 carries out the authentication of the VPN peers used to terminate each end of the SA, whereas XAUTH is used for the authentication of users or devices that will be transmitting and receiving data across the established VPN tunnel. This phase can occur in remote-access or Easy VPN scenarios, but not in site-to-site VPNs. XAUTH authentication can be achieved by using either of the following:

- Static username and passwords
- *One-time passwords (OTP)*

Authentication Header and Encapsulating Security Payload

Both AH and ESP operate at the network layer of the OSI model and, as a result, have their own protocol numbers for protocol identification carried out by devices in the VPN path. (The protocol numbers assigned are 51 and 50, respectively.) As mentioned earlier, ESP can provide the optional encryption function for data traversing the VPN connection. Therefore, ESP is the preferred choice for use with IPsec. The data encryption function provided by ESP is carried out by one of the following symmetric key algorithms:

- *Digital Encryption Standard (DES)*
- *Triple DES (3DES)*
- *Advanced Encryption Standard (AES)* (preferred)

The origin authentication, provided by both AH and ESP, can be carried out by one of the following hash algorithms:

- *Message digest 5 algorithm (MD5)*
- *Secure Hash (SHA)* (and only for IKEv2: SHA256, SHA384, SHA512)

AH is unavailable for use on the ASA because of the lack of an encryption option. Therefore, when configuring a VPN, only ESP is available to us.

Because ESP and AH operate at the network layer, as illustrated in Figure 1-5, the original host and destination IP addresses remain in the packet throughout the network, exposing them to potential attackers of the VPN connection. However, which IPsec mode (either Transport or Tunnel) is chosen determines the amount of the original packet to be hidden.

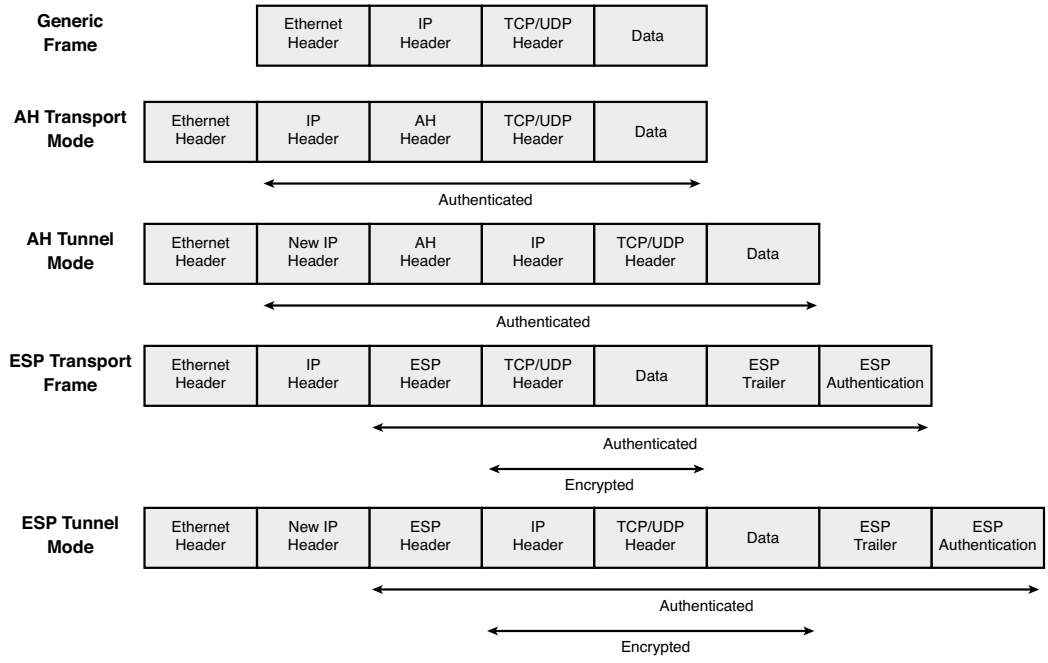


Figure 1-5 *ESP and AH Transport and Tunnel Frame Formats*

As shown in Figure 1-5, in both AH and ESP Transport mode, the original IP addresses remain untouched and are visible to potential attackers. However, when operating within Tunnel mode, the AH and ESP headers are placed after the original IP header, and a new IP header is added. This header contains the IP addresses of the VPN endpoints (ASA, PIX, concentrator, or router), which are generally public IP addresses and contain no information, thus not allowing an attacker to determine any valuable information about the internal network. ASA, as a VPN tunnel endpoint, supports only Tunnel mode. Even if Transport mode is configured on the ASA, the resulting VPN tunnel negotiates and uses Tunnel mode. This is also the case for Cisco routers running IOS. However, this restriction applies only to native IPsec functionality, Transport mode is supported on IOS routers (for example, when *generic routing encapsulation [GRE]* tunneling is used along with IPsec, but not on the ASA, which does not support GRE termination).

A feature often used with remote-access IPsec VPNs, which you will see more of later, is *NAT Traversal (NAT-T)*. As you might have noticed already, *Network Address Translation (NAT)* and *Port Address Translation (PAT)* play a large and important role

in many organizations and general Internet connectivity. The original idea behind NAT was to provide a temporary solution to the growing decline in available IPv4 addresses. However, many organizations have also seen the benefit of using NAT/PAT to mask/hide the IP address information of the internal network from external attackers. Also, home users and *small to medium business (SMB)* remote users typically use NAT and PAT to translate many internal hosts or devices to only one or two public IP addresses. However, ESP and AH are not PAT aware, cannot be PAT'ed because these protocols do not have the notion of port numbers, and run on top of IP with their own protocol numbers. To resolve this problem, a similar approach to adding a new IP header can be taken by adding a new transport header.

AH cannot operate with NAT-T because changing the authenticated IP address in the outer header will break the integrity check when the packet reaches the remote VPN endpoint, unlike ESP, which does not perform authentication of the outer header, thus allowing for the IP address to be changed without breaking communications.

For ESP to pass across PAT devices on Cisco ASA, the following options are available:

- Standard-based NAT-T, which encapsulates ESP into *User Datagram Protocol (UDP)* port 4500 only if NAT/PAT device is detected along the path between the two VPN endpoints. This method is supported for all IKEv1 IPsec VPN types, but only in Tunnel mode.
- Cisco proprietary UDP or TCP encapsulation, which always encapsulates ESP into UDP or TCP, even though no NAT/PAT device exists along the path. If UDP encapsulation is being used, IKEv1 negotiation still uses UDP port 500, but ESP is encapsulated into UDP. (By default, port 10000 is used.) With TCP encapsulation, both IKEv1 and ESP are encapsulated into TCP, and by default, port 10000 is used. This method is available only for remote-access IKEv1 IPsec VPNs in Tunnel mode.

Figure 1-6 shows the resulting packet format with the addition of the new TCP or UDP transport layer headers that can be added for NAT-T operation.

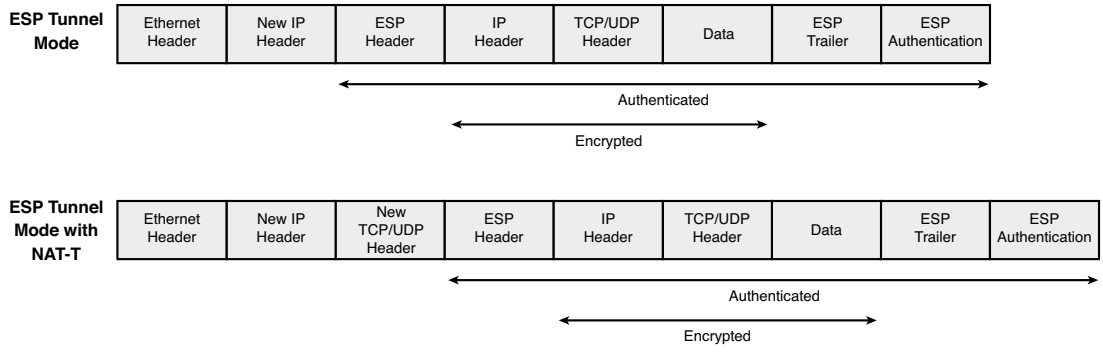


Figure 1-6 *ESP and ESP with NAT-T Frame Format*

IKEv2

The original IKEv1 protocol has been around for many years and enjoys widespread deployment in site-to-site VPN tunnels and remote-access VPNs. The Cisco IPsec VPN client supports the IKEv1 protocol for the purposes of establishing an IPsec remote-access connection. However, difficulties were encountered with the complexity of IKEv1 and its implementation. In addition, the protocol lacked initial support for the extended capabilities required by remote clients (for example, NAT-T), which ultimately led to many vendors implementing their own versions of required features, even though additional standards had later been created to provide for a standardized application of NAT-T, legacy authentication, and remote-address acquisition.

Both IKEv1 and IKEv2 use UDP for the encapsulation and transmission of information between peers. Although the header format used by both protocol implementations is similar enough to allow them to simultaneously use the same UDP port (500), the two protocols cannot interoperate with each other.

IKEv2 (RFC 5996) was created to simplify and streamline the processes and architecture of IKEv1. So, IKEv2 (RFC 5996) combines the contents of the ISAKMP (RFC 2408), IKE (RFC 2409), Internet Domain of Interpretation (RFC 2407), NAT-T, legacy authentication, and remote-address acquisition, which had previously been documented separately.

IKEv2 has streamlined the original IKEv1 packet exchanges during Phase 1 and Phase 2 operation (Main mode, Aggressive mode, and Quick mode) used to create IKE and IPsec SAs for a secure communications tunnel. IKEv1 uses either nine messages (Main mode = 6 + Quick mode = 3) or six messages (Aggressive mode = 3 + Quick mode = 3) for successful operation. However, IKEv2 introduces a new packet-exchange process using just four messages most of the time. A successful message exchange involves a pair of messages. IKEv2 uses the following new exchange types (which are used either for Phase 1 or Phase 2 operation) to replace the IKEv1 Main mode, Aggressive mode, and Quick modes:

- IKE_SA_INIT (Phase 1)
- IKE_AUTH (Phase 1 and 2)

The first exchange, IKE_SA_INIT, is used to negotiate the security parameters by sending IKEv2 proposals, including the configured encryption and integrity protocols, DH values, and nonces (random) numbers. At this point, the two peers generate SKEYSEED (a seed security key value) from which all future IKE keys are generated. The messages that follow in later exchanges are encrypted and authenticated using keys also generated from the SKEYSEED value.

The second exchange, IKE_AUTH, operates over the IKE_SA created by the IKE_SA_INIT exchanges and is used to validate the identity of the peers and negotiate the various encryption, authentication, and integrity protocols to establish the first CHILD_SA for use by ESP or AH in which IPsec communication occurs. Peers are validated using pre-shared keys, certificates, or *Extensible Authentication Protocol (EAP)* (allowing for legacy authentication methods between peers). Figure 1-7 shows these two exchanges.

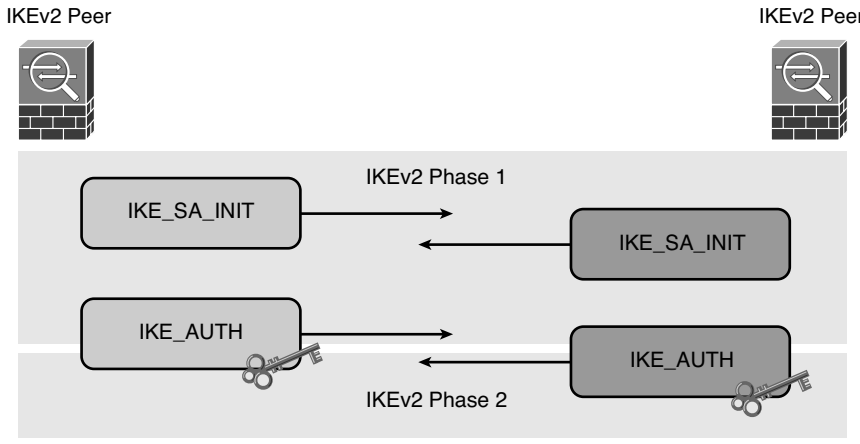


Figure 1-7 *IKEv2 Message Exchange and Tunnel Creation Between Peers*

The first CHILD_SA created in the second exchange is commonly the only SA created for IPsec communication. However, if an application or peer requires the use of additional SAs to secure traffic through an encrypted tunnel, IKEv2 uses the CREATE_CHILD_SA exchange. During the CREATE_CHILD_SA exchange, new DH values may be generated and cryptographic protocols used. (That is, there is no requirement for later SAs to use the same key material created during the initial IKE_SA_INIT exchange.) This behavior is similar in function to the use of *Perfect Forwarding Secrecy (PFS)*, whereby during an IKEv1 Quick mode exchange new DH values may be used to prevent the reuse of key material created in the previous Phase 1 exchanges. You'll usually have multiple CREATE_CHILD_SA exchanges to create multiple SAs for securing data traffic, if you do not want to multiplex multiple source/destination traffic pairs over the same SA.

IKEv2 also implements a fourth exchange type: INFORMATIONAL. This message type is used to exchange error and management information between peers.

As mentioned earlier, IKEv2 was created to combine many of the existing standards used by IKEv1. For example, NAT-T is now a part of the IKEv2 standard and is a "built-in" function of the protocol, as is a keepalive function between peers allowing for an IKEv2 peer to recognize when a tunnel is down and facilitate the regeneration of the tunnel.

IKEv2 can also reduce the overhead experienced by VPN peers. For example, multiple subnets and networks may be included into an exchange and an SA created for all of them, whereas IKEv1 requires a separate SA for each subnet/network source and destination pair.

SSL/TLS

Originally developed by Netscape in 1994, the SSL protocol quickly became dominant for use in applications and servers when transferring secured data across the Internet. Back then, during the consumer infancy of the Internet, the World Wide Web Consortium decided that a secure way to transfer web traffic across the Internet was needed to encourage e-commerce providers onto the Internet. Initially, the consortium

voted in favor of using *Secure Hypertext Transfer Protocol (S-HTTP)*, a protocol that had also been developed for secure Internet communication during the mid-1990s. However, because Netscape was already using its own secure implementation (SSL) in their browser and Microsoft had adopted the use of the SSL protocol within its operating systems, the decision was made to use *Hypertext Transfer Protocol Secure (HTTPS)*, a combination of the SSL and HTTP protocols. The standard was later created for HTTPS and is defined in RFC 2818.

TLS is a standards-based implementation of SSL 3.0 (known as SSL 3.1). Because SSL is a proprietary protocol, the *Internet Engineering Task Force (IETF)* published the standard in 1999, details of which you can find in RFC 2246. (The most recent version of the standard is RFC 6176 TLS 1.2.) Although SSL and TLS are similar, significant differences exist so that the protocols do not interoperate. Three versions of the SSL protocol are available, as are two versions of the TLS protocol:

- SSL 1.0 (deprecated)
- SSL 2.0 (not recommended for use in production environments)
- SSL 3.0
- TLS 1.1 (SSL 3.1)
- TLS 1.2

SSL provides message authentication, confidentiality, and integrity through the combination of the underlying cryptographic protocols (reviewed earlier in this chapter). SSL sits between the application and transport layers of the OSI model, as shown in Figure 1-8, and includes no mechanism for reliable packet delivery. Therefore, the protocol relies on other higher-layer protocols within the OSI model and the VPN termination device for ordered and guaranteed delivery of packets. For these reasons, TCP is the transport layer of choice for this situation, with its sequencing, reordering, and reliable delivery functionality.

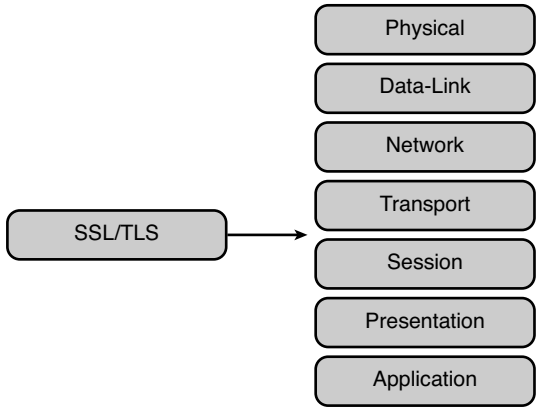


Figure 1-8 *SSL's OSI Layer Position*

Within an SSL packet is the Record protocol responsible for packaging the lower-level messages to be transmitted. For example, the Record protocol fragments, assembles, applies, and removes MAC hashing and compression schemes and encrypts or decrypts the messages encapsulated within it. The overall hash, encryption algorithms, and compression schemes are negotiated by the lower-level protocols it encapsulates, as you will see in a moment.

Figure 1-9 shows the format of a Record protocol message.

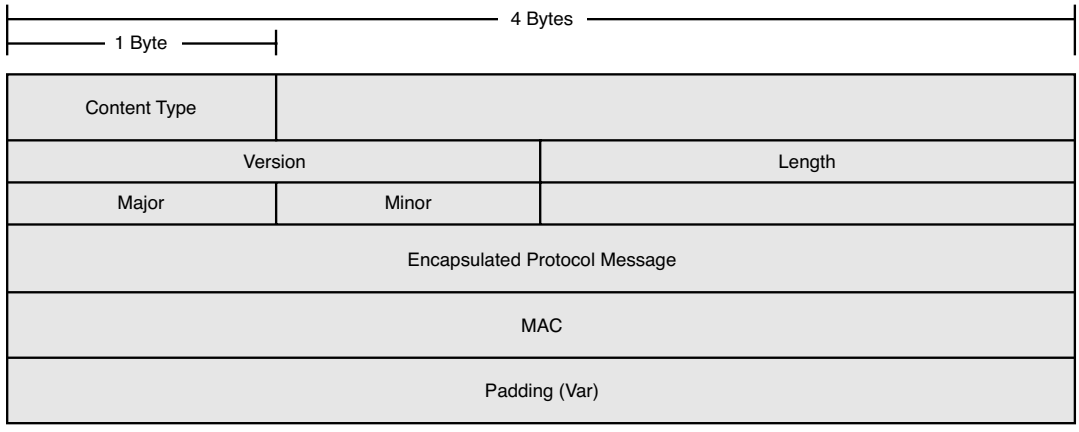


Figure 1-9 *SSL Record Protocol Format*

- **Content Type:** Indicates the message encapsulated in this record. The message can be one of four values:
  - **Handshake:** 22
  - **ChangeCipherSpec:** 20
  - **Application:** 23
  - **Alert:** 21
- **Version:** Indicates the version of the protocol. For example:
  - **SSL 2.0:** Major 2, Minor 0
  - **SSL 3.0:** Major 3, Minor 0
  - **TLS 1.0:** Major 3, Minor 1 (known as SSL 3.1)
- **Length:** The length of this record.
- **Encapsulated Protocol Message:** Carries the messages or application data sent between client and server during a conversation. After the authentication, encryption, and hash parameters have been negotiated, this field may be encrypted.
- **MAC:** The MAC calculated for the application data held in the encapsulated protocol message. The protocol used for the MAC is negotiated between client and server using the ClientHello and ServerHello messages.

- **Padding:** Used alongside MAC protocols that operate as block ciphers to pad the message length to an even block size. This field is not required with stream ciphers.

SSL Tunnel Negotiation

SSL establishes a connection between both the client (typically the user's web browser or the Cisco AnyConnect client) and server by sending a number of messages encapsulated within the Record protocol described in the preceding section. This section walks you through the SSL tunnel negotiation process, the messages involved, and their parameters and use, which all occur during a phase called the handshake. The handshake is one of two phases involved in the building blocks of an SSL tunnel, the second being the application phase, during which the transmission of data between the client and server takes place.

As shown in Figure 1-10 and the following list, a number of messages are sent between the client and server within the handshake phase:

- **ClientHello:** Sent from the client to the server, the first message to be sent
- **ServerHello:** Sent from the server to the client as the server's response to the ClientHello
- **Certificate:** Sent from the server to the client, and used by the client to authenticate the server and obtain a copy of the server's public key
- **ServerHelloDone:** Sent from the server to the client to indicate that all information the server has or expects to send has been
- **ClientKeyExchange:** Sent from the client to the server containing information used to create a master key
- **ChangeCipherSpec:** Sent by the client after successful negotiation of all parameters have completed to indicate all messages from this point onward will be encrypted
- **Finish:** Sent by the client to indicate the completion of its part in the tunnel-establishment phase
- **ChangeCipherSpec:** Sent by the server after successful negotiation of all parameters have completed to indicate all messages from this point onward will be encrypted
- **Finish:** Sent by the server to indicate the completion of its part in the tunnel-establishment phase

Handshake

During the handshake stage, various parameters are negotiated between the client and server. The client starts the conversation by sending a ClientHello packet to the server, as shown in Figure 1-10.

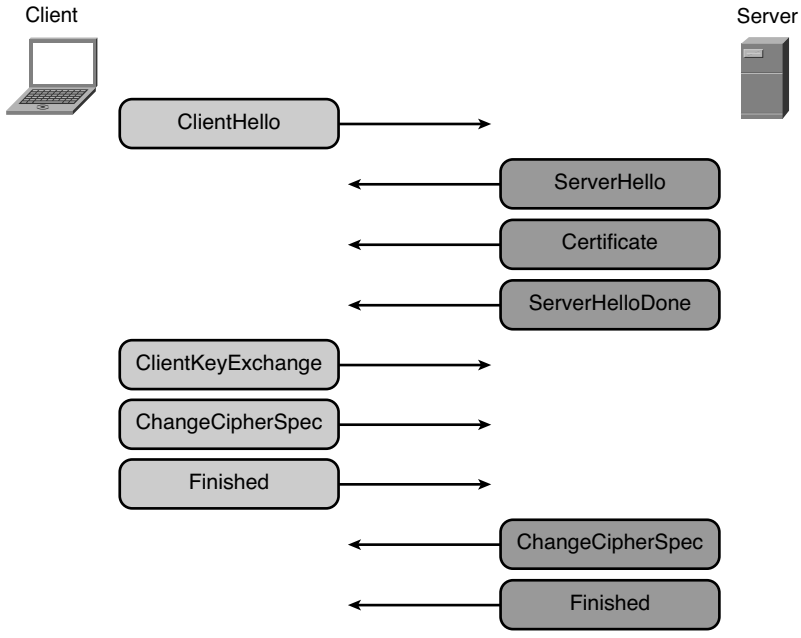


Figure 1-10 *SSL/TLS Handshake Process*

The ClientHello packet contains the fields shown in Figure 1-11.

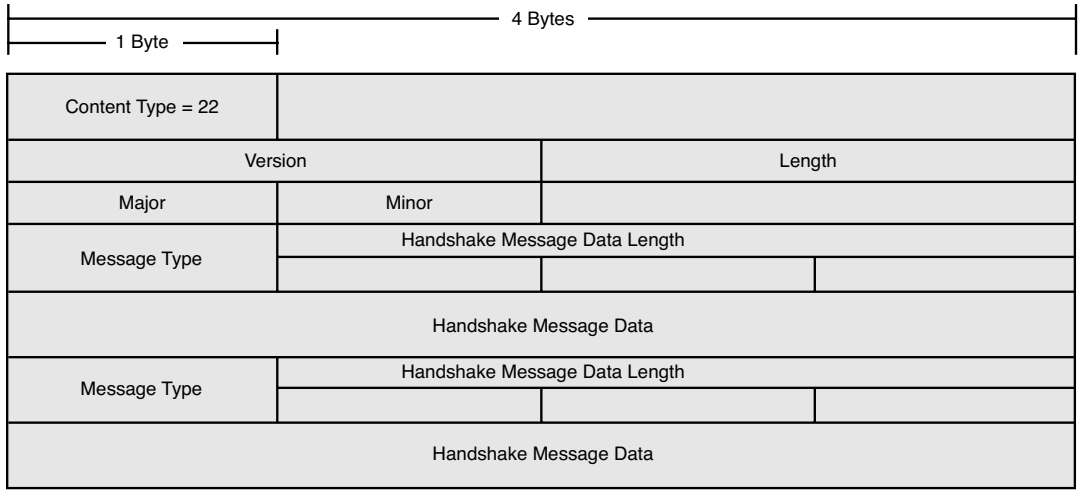


Figure 1-11 *SSL/TLS ClientHello/ServerHello Packet Format*

The following list describes the data included within the Handshake Message Data field of the ClientHello packet:

- **The cipher suite** lists the available protocols for encryption and their key lengths. Protocols used for message hashing and integrity checks (for example, an available cipher) are listed in the form of TLS_RSA_WITH_DES_CBC_SHA.

- **A random number** is used to construct the master key. The random number is a 4-byte field created with a combination of the client's configured date and time and a 28-byte pseudorandom number.
- **The protocol version:** The higher value is preferred. For example, if TLS is available, it is the preferred protocol, then SSL 3.0, then SSL 2.0. (A few vendors have already removed SSL 2.0 support from their browsers.) Common version numbers include the following:
  - **3.1:** TLS
  - **3:** SSL 3.0
  - **2:** SSL 2.0
- **Any compression schemes** supported by the client are included.
- **A session ID:** If this is a new conversation, the session ID is null. If the client is trying to reconnect to an existing session, the ID is placed into the session ID during this stage.

After the server has received the ClientHello message, it responds with its own ServerHello message. This packet is similar in construction to the original ClientHello message. However, the server generates and includes its own random number for creation of the master key and chooses a compression scheme from the list of supported schemes it receives from the client.

Instead of the server sending the client a list of the cipher suites it supports, the server chooses from the highest supported version of protocols it has, based on the list it received from the client. For example, if the client had sent a cipher suite including *Advanced Encryption Standard 256 (AES-256)* and *Secure Hash 1 (SHA-1)*, and the server could not find an entry for any protocol version higher (more secure) but had these protocols installed, it would choose to use these and send the name of the cipher back to the client to confirm its choice. As mentioned earlier, the client also sends the server a session ID in its ClientHello message. If the session ID is null, the server generates a new session ID and includes this in its ServerHello to the client. If the session ID received from the client is not null and that of an existing session, however, the server restarts the existing session where possible.

At this stage, after the ClientHello and ServerHello messages have been sent and received, and the protocol, encryption, hash, and authentication algorithms have been negotiated, the server sends its certificate to the client, which contains a copy of the server's public key, as shown in Figure 1-12.

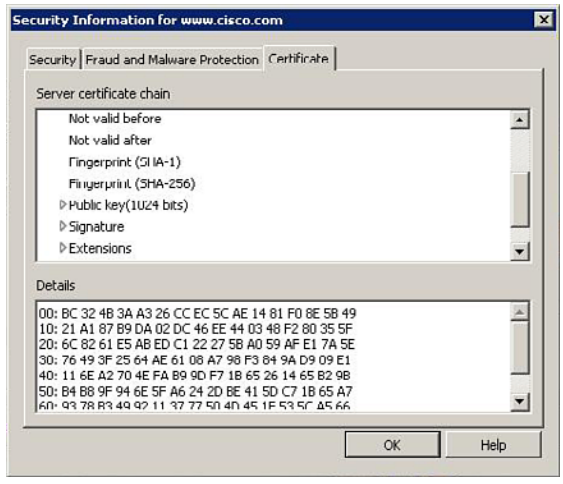


Figure 1-12 *A Server Certificate Displaying the Server's Attached Public Key*

The client, upon receiving the server's certificate, checks to see whether the name of the root *certificate authority (CA)* exists in its own trusted root CA store, retrieves the root CA's public key, and validates the digital signature using it. The client then moves on to validating the server by inspecting the name of the server it is connecting to against the name held in the certificate file, the current date and time against the certificates valid from-to values, and the *certificate revocation list (CRL)*.

At this point in the tunnel negotiation, the server sends the client the ServerHelloDone message, indicating to the client that the server has finished sending the information it has.

The client now sends a ClientKeyExchange message to the server, which includes the protocol version number originally sent in the ClientHello message and a pre_master secret used by both the server and client, to generate the master secret for encryption. Depending on the cipher suite negotiated in earlier messages, the pre_master secret can vary in length and the information carried within it. The pre_master secret is typically composed of the client's SSL/TLS version number and a string of random bytes, and before being transmitted it is encrypted using the server's public key. The client sends the protocol version again to prevent a rollback attack (attacks that attempt to fool the server and client into using a lower version of the protocol).

The server then decrypts the pre_master secret using its private key matching the public key from its certificate. Both client and server now use the pre_master secret along with both random numbers to generate the master key, which is then used to create the symmetric keys used for message encryption, key seed identification and integrity-checking purposes.

The client now sends a *ChangeCipherSpec (CCS)* message to the server as a sign that everything sent from now on will be encrypted using the keys and protocols as established in the earlier messages, followed by a Finish message. The server also sends the client a CCS message to indicate the same state, followed by a Finish message. The diagram

in Figure 1-13 illustrates the packet format of the CCS message. The CCS protocol type is currently set to 1 because it is the only available protocol type in a CCS message.

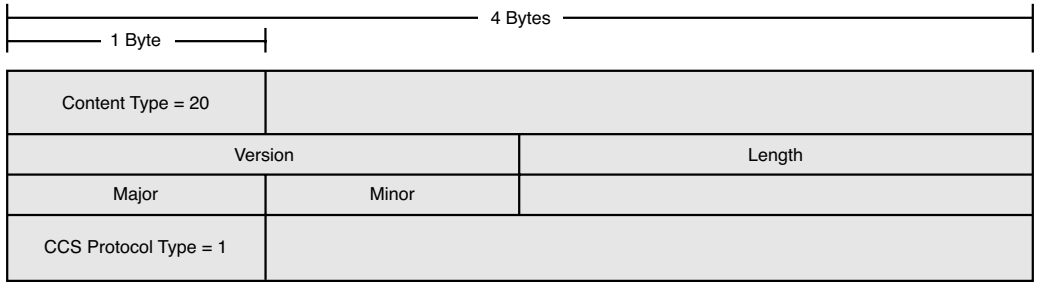


Figure 1-13 *ChangeCipherSpec Packet Format*

As you will see in later configuration examples of this book, in addition to the server using a digital certificate for authentication purposes, the client (remote site or user) can also use their own digital certificate during the SSL/TLS handshake process for them to be authenticated by the ASA.

If you recall, after the ServerHello and ClientHello packets are sent and received, the server sends its certificate and optionally can prompt for a user certificate by sending the CertificateRequest message followed by the ServerHelloDone message. The client responds to the CertificateRequest with its own Certificate message containing its digital certificate, and optionally the certificate chain that includes the list of CAs responsible for issuing the certificate.

After sending the server a copy of its certificate, the client then sends another new message, this time of the type CertificateVerify. This message (which is encrypted using its private key) contains the signature/hash, which is then computed over all the messages sent up to this point. The server receives the CertificateVerify message, and with the corresponding public key (which was sent with the client's certificate file) decrypts the information. Successful decryption verifies that the certificate belongs to the client.

The handshake process then continues. The client and server each use the parameters received in earlier messages to generate the master secret. Figure 1-14 shows the SSL handshake process, including the messages that are used when client authentication is in operation.

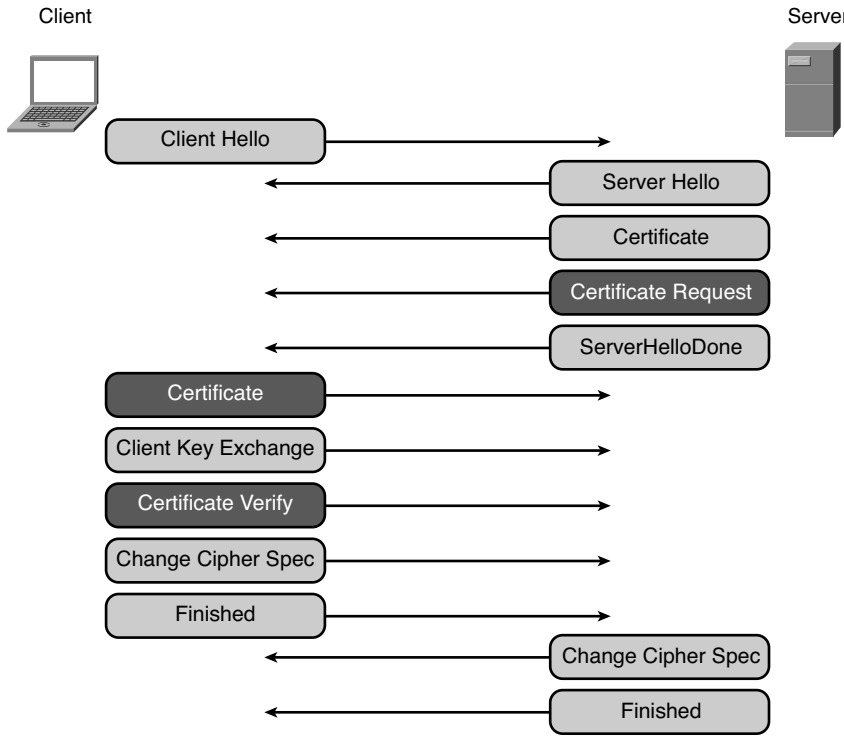


Figure 1-14 *SSL Handshake Process with Client Authentication*

DTLS

Recall that TCP is used by SSL/TLS because of the need for support for message reordering, retransmission, and reliable delivery purposes. However, for many delay-sensitive protocols (for example, voice and video), the benefits of TCP are often sacrificed to make way for faster transmission of data using UDP, so a problem surfaced when network designers and engineers needed to send delay-sensitive applications through an SSL/TLS tunnel. For this reason, DTLS (RFC 6347) was born. DTLS is based on the original implementation of TLS, but instead operates using the UDP transport protocol for faster packet delivery. Additional parameters, fields, and functions allow it to provide reliable message delivery, message reordering, fragmentation, and antireplay natively.

To provide the functions of message reordering and reliable delivery, the DTLS protocol has added two new fields to the TLS record layer format: the Sequence Number and the Epoch. The sequence number increments for each packet sent between the client and server. DTLS also uses a windowing system for antireplay purposes, providing the protocol to be able to distinguish between packets that are yet to be received and should be

processed further and packets that have already been received. (Any packets containing sequence numbers in this range should be dropped.)

Unlike the implicit sequence number used by TCP, the sequence number in DTLS is defined explicitly. Therefore, there is a potential for a client or server taking part in many DTLS conversations and encountering DTLS packets from different conversations using the same sequence number. For this reason, the Epoch field is used to distinguish the different conversations that may be occurring at the same time. The Epoch field begins at zero during the handshake process and increments each time a ChangeCipherSpec packet is sent. Although the Epoch is reset to zero each time the handshake occurs between client and server, it is suggested that because of the minimal number of conversations that will require a "re-handshake," this should not pose much of an overlapping-conversations problem.

In addition to the changes DTLS makes to the TLS protocol, as described previously, the protocol can also prevent potential *denial-of-service (DoS)* attacks by using an optional authentication cookie mechanism that is inserted into the handshake phase. Using an authentication cookie allows the server to validate the identity of the client by replying to the client with a HelloVerifyRequest message after receiving a ClientHello message. The HelloVerifyRequest message contains the authentication cookie generated by the server. Upon receipt of the HelloVerifyRequest packet, the client sends the server another ClientHello that this time contains the received authentication cookie using a new "cookie" field created explicitly by DTLS in the ClientHello packet for carrying the authentication cookie. The server can now confirm the identity of the client on receiving and validating the authentication cookie, as shown in Figure 1-15.

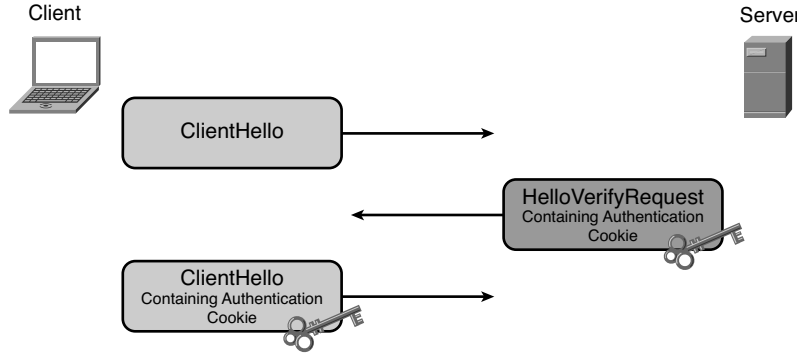


Figure 1-15 *DTLS Authentication Cookie Client Identity Verification Process (DoS Mitigation)*

Although this process describes the use of the HelloVerifyRequest packet sent by the server for sending the authentication cookie, this packet has also been added to the existing TLS handshake phase for providing state information. For example, DTLS prevents against packet loss using timers on the client and server. After the client has started a new handshake by sending the ClientHello packet to a server, it starts a timer (based loosely on the TCP RTT). Upon receipt of the ClientHello, the server replies to the client with a HelloVerifyRequest packet, and the client resets the timer. If the original

ClientHello message had been dropped because of congestion in the path between the client and server, the server does not receive a packet and therefore does not respond to the client. The client's timer will expire, resulting in the client sending a new ClientHello message to the server.

So, you can see that in addition to using UDP to overcome the speed limitations that can be imposed on delay-sensitive applications with TCP, DTLS has extended TLS to provide for similar functions carried out by TCP but still allows delay-sensitive applications to enjoy the faster transmission offered by using UDP without additional overhead.

The Cisco AnyConnect client supports the use of DTLS with the addition of a native TLS tunnel. If at any point during communications the DTLS tunnel is torn down between the client and server, the AnyConnect client can fall back to the established TLS tunnel for data transmission.

ASA Packet Processing

When processing incoming and outgoing packets from internal and external networks, the ASA device goes through a flow of operations in which it performs routing lookups, enforces host limits, inspects the packet against any configured *access control lists (ACL)*, and so on.

When configuring available features and settings of a VPN, it is important to understand the flow of operations that ASA devices engage in on both an incoming and outgoing path. Understanding this information can also save you a great deal of time when troubleshooting a configuration error or even a suspected error on the ASA.

However, depending on the incoming interface (direction of traffic), the ASA processes the operations in a different order. The following list shows the order of operations the ASA goes through upon receiving a packet from an inside interface destined to a host on the outside interface:

- **Received packet from interface:** Inside.
- **Flow lookup:** Does this packet belong to an existing flow entry?
- **Route lookup:** Perform a longest prefix match route lookup for the destination IP address in the packet against the information held within the ASA's routing table.
- **Access list:** Check the packet against any access lists configured on the incoming path.
- **IP options (Modular Policy Framework [MPF]):** Check the packet against MPF configured policies (*quality of service (QoS)*, embryonic limits, and so on).
- **VPN crypto match?:** Is this packet destined for a host through a VPN tunnel?
- **NAT:** Perform NAT translation against the fields in the packet based on any configured NAT rules.
- **NAT host limit:** Is this packet subject to any limits imposed that might cause it to be discarded (for example, half-open connections)?

- **IP options (MPF):** Check the packet against MPF configured policies (QoS, embryonic limits, and so on).
- **Flow creation:** If this packet is a new flow, create a new flow entry for it here.
- **Send packet out of interface:** Outside.

The following is the order of operations taken by the ASA upon receiving a packet on the outside interface destined for a host connected to a network on the inside interface:

- Received packet from interface: Outside.
- Flow lookup
- Route lookup
- Access list
- IP options (MPF)
- VPN crypto match?
- NAT (Reverse Path Forwarding [RPF]): Is the best path in the routing table toward the source IP address in the packet through the interface in which it came into the ASA?
- NAT host limit
- NAT lookup
- Send packet out of interface: Inside.

We can also use the available Packet Tracer tool as a visual guide to how a packet will be treated by our ASA device, by specifying the source and destination IP address, ports, protocol, and the incoming interface the packet may be received on.

Figure 1-16 shows the Packet Tracer utility available from the Tools menu along the top of the ASDM window. This tool can prove invaluable when troubleshooting a problem if, for example, you are experiencing packet loss or drops and suspect the problem might be caused by something configured on your ASA device.

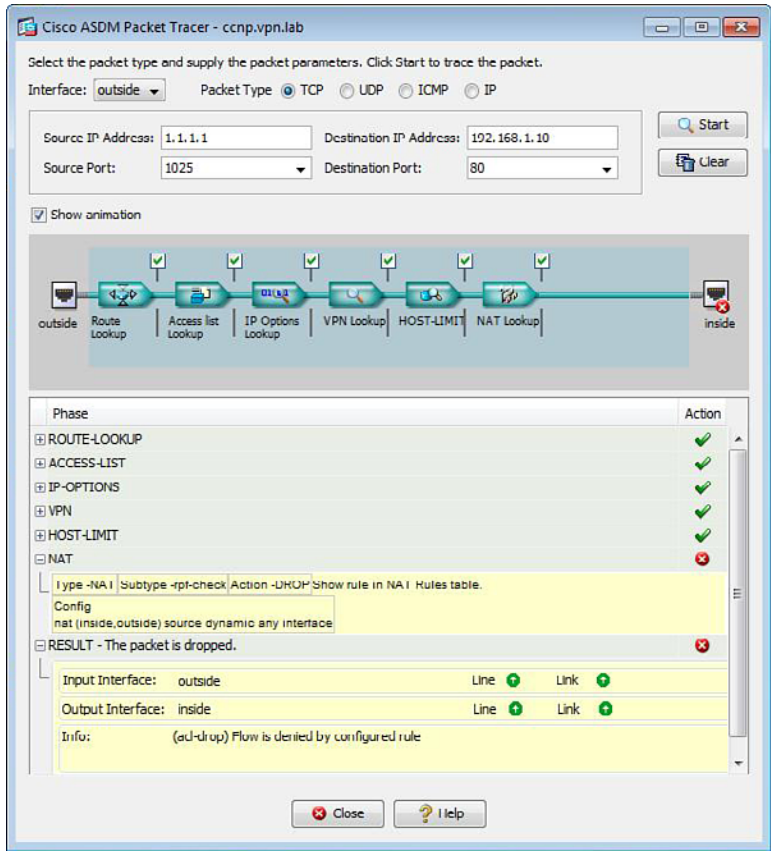


Figure 1-16 *ASA Packet Tracer Utility*

The Packet Tracer tool assesses the IP, port, protocol, and interface information you enter against any configured access lists, MPF, NAT rules, and so on and provides you with the results of its step-by-step check.

The Good, the Bad, and the Licensing

Now that you have reviewed the available VPN connectivity methods provided by the ASA, their comparison and the path taken by a packet through the ASA device, it is time to take a look at the licensing models available. When it comes to licensing on the ASA, a lot of information is involved. I suggest using the following information as a handy reference instead of trying to memorize all of it. You might be required to know the result of combining two matching licenses (for example, on two devices during a failover configuration). However, the majority of the information provided here is for your information only and will not be included on the exam.

You can view your currently installed and active licenses on the ASA by navigating to **Configuration > Device Management > Licensing > Activation Key** within the ASDM, or by issuing the **show version** command when working from the *command-line interface (CLI)*.

The license information available includes the combination of all permanent and time-based licenses. (Time-based licenses are explained in greater detail in the next section.)

Tables 1-3 to 1-8 include the model-specific licensing information available for the ASA 5505 to ASA 5580.

Table 1-3 *ASA 5505 License Features*

ASA 5505	Base License	Security Plus
Firewall Licenses		
Botnet Traffic Filter	Disabled *(Optional time-based license available)*	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	10 K	25 K
GTP/GPRS	No support	No support
Intercompany Media Engine	Disabled *(Optional license available)*	Disabled *(Optional license available)*
UC Phone Proxy Sessions	2 *(Optional license upgrade: 24)*	2 *(Optional license upgrade: 24)*
VPN Licenses		
Adv. Endpoint Assessment	Disabled *(Optional license available)*	Disabled *(Optional license available)*
AnyConnect Essentials	Disabled *(Optional license available)*	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*	Disabled *(Optional license available)*
AnyConnect Premium SSL VPN Edition (sessions)*	2 *(Optional permanent or time-based licenses: 10 or 25 sessions)*	2 *(Optional permanent or time-based licenses: 10 or 25 sessions)*
IPsec VPN (sessions)	10 (max. 25 combined IPsec and SSL VPN)	25 (max. 25 combined IPsec and SSL VPN)
VPN load balancing	No support	No support

ASA 5505	Base License	Security Plus
General Licenses		
Encryption	Base (DES) *(Optional license: Strong [3DES/AES])*	Base (DES) *(Optional license: Strong [3DES/AES])*
Failover	No support	Active/standby (no stateful failover)
Security contexts	No support	No support
Users, concurrent	10 *(Optional licenses: 50 or unlimited)*	10 *(Optional licenses: 50 or unlimited)*
VLANs/zones, maximum	3 (2 regular zones and 1 restricted zone)	20
VLAN trunk, maximum	No support	8 trunks

Table 1-4 *ASA 5510 License Features*

ASA 5510	Base License	Security Plus
Firewall Licenses		
Botnet Traffic Filter	Disabled *(Optional time-based license available)*	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	50 K	130 K
GTP/GPRS	No support	No support
Intercompany Media Engine	Disabled *(Optional license available)*	Disabled *(Optional license available)*
Unified Comm. Sessions	2 *(Optional licenses available: 24, 50, or 100 sessions)*	2 *(Optional licenses available: 24, 50, or 100 sessions)*
VPN Licenses		
Adv. Endpoint Assessment	Disabled *(Optional license available)*	Disabled *(Optional license available)*

ASA 5510	Base License	Security Plus
AnyConnect Essentials	Disabled *(Optional license available)*	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*	Disabled *(Optional license available)*
AnyConnect Premium SSL VPN Edition (sessions)	2 *(Optional permanent or time-based licenses available: 10, 20, 50, 100, or 250 sessions)* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*	2 *(Optional permanent or time-based licenses available: 10, 20, 50, 100, or 250 sessions)* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*
IPsec VPN (sessions)	250 (max. 250 combined IPsec and SSL VPN)	250 (max. 250 combined IPsec and SSL VPN)
VPN Load Balancing	No support	Supported
General Licenses		
Encryption	Base (DES) *Optional license available: Strong (3DES/AES)*	Base (DES) *Optional license available: Strong (3DES/AES)*
Failover	No support	Active/Standby or Active/Active
Interface Speed	All: Fast Ethernet	Ethernet 0/0 and 0/1: Gigabit Ethernet Ethernet 0/2, 0/3, and 0/4 (and any others): Fast Ethernet
Security Contexts	No support	2 *Optional licenses: 5*
VLANs, Maximum	50	100

Table 1-5 *ASA 5520 License Features*

ASA 5520	Base License
Firewall Licenses	
Botnet Traffic Filter	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	280 K
GTP/GPRS	Disabled *(Optional license available)*
Intercompany Media Engine	Disabled *(Optional license available)*
Unified Communications Proxy Sessions	2 *(Optional licenses available: 24, 50, 100, 250, 500, 750, or 1000 sessions)*
VPN Licenses	
Adv. Endpoint Assessment	Disabled *(Optional license available)*
AnyConnect Essentials	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*
AnyConnect Premium SSL VPN Edition (sessions)	2 *(Optional permanent or time-based licenses available: 10, 25, 50, 100, 250, 500, or 750 sessions)* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*
IPsec VPN (sessions)	750 (max. 750 combined IPsec and SSL VPN)
VPN Load Balancing	Supported
General Licenses	
Encryption	Base (DES) *Optional license available: Strong (3DES/AES)*
Failover	Active/standby or active/active

ASA 5520	Base License
Security Contexts	2 *(Optional licenses available: 5, 10, or 20)*
VLANs, Maximum	150

Table 1-6 *ASA 5540 License Features*

ASA 5540	Base License
Firewall Licenses	
Botnet Traffic Filter	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	400 K
GTP/GPRS	Disabled *(Optional license available)*
Intercompany Media Engine	Disabled *(Optional license available)*
Unified Communications Proxy Sessions	2 *(Optional licenses available: 24, 50, 100, 250, 500, 750, 1000, or 2000 sessions)*
VPN Licenses	
Adv. Endpoint Assessment	Disabled *(Optional license available)*
AnyConnect Essentials	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*
AnyConnect Premium SSL VPN Edition (sessions)	2 *Optional permanent or time-based licenses available: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*

ASA 5540	Base License
IPsec VPN (sessions)	5000 (max. 5000 combined IPsec and SSL VPN)
VPN Load Balancing	Supported
General Licenses	
Encryption	Base (DES) *(Optional license available: Strong [3DES/AES])*
Failover	Active/standby or active/active
Security Contexts	*2* *(Optional licenses available: 5, 10, 20, 50)*
VLANs, Maximum	200

Table 1-7 *ASA 5550 License Features*

ASA 5550	Base License
Firewall Licenses	
Botnet Traffic Filter	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	650 K
GTP/GPRS	Disabled *(Optional license available)*
Intercompany Media Engine	Disabled *(Optional license available)*
Unified Communications Proxy Sessions	2 *(Optional licenses available: 24, 50, 100, 250, 500, 750, 1000, 2000, or 3000 sessions)*
VPN Licenses	
Adv. Endpoint Assessment	Disabled *(Optional license available)*
AnyConnect Essentials	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*

ASA 5550	Base License
AnyConnect Premium SSL VPN Edition (sessions)	2 *Optional permanent or time-based licenses available: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*
IPsec VPN (sessions)	5000 (max. 5000 combined IPsec and SSL VPN)
VPN Load Balancing	Supported
General Licenses	
Encryption	Base (DES) *(Optional license available: Strong [3DES/AES])*
Failover	Active/standby or active/active
Security Contexts	2 *(Optional licenses available: 5, 10, 20, 50)*
VLANs, Maximum	400

Table 1-8 *ASA 5580 License Features*

ASA 5580	Base License
Firewall Licenses	
Botnet Traffic Filter	Disabled *(Optional time-based license available)*
Firewall Conns, Concurrent	5580-20: 1000 K 5580-40: 2000 K
GTP/GPRS	Disabled *(Optional license available)*
Intercompany Media Engine	Disabled *(Optional license available)*

ASA 5580	Base License
Unified Communications Proxy Sessions	2 *Optional licenses available: 24, 50, 100, 250, 500, 750, 1000, 2000, 3000, 5000, or 10,000 sessions*
VPN Licenses	
Adv. Endpoint Assessment	Disabled *(Optional license available)*
AnyConnect Essentials	Disabled *(Optional license available)*
AnyConnect Mobile	Disabled *(Optional license available)*
AnyConnect Premium SSL VPN Edition (sessions)	2 *Optional permanent or time-based licenses available: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000* *Optional shared licenses: Participant or Server. For the Server, these licenses are available:* *500–50,000 in increments of 500* *50,000–545,000 in increments of 1000*
IPsec VPN (sessions)	5000 (max. 5000 combined IPsec and SSL VPN)
VPN Load Balancing	Supported
General Licenses	
Encryption	Base (DES) *(Optional license available: Strong [3DES/AES])*
Failover	Active/standby or active/active
Security Contexts	2 *Optional licenses available: 5, 10, 20, 50*
VLANs, Maximum	1024

Table 1-9 includes the VPN-specific licensing information. By default, the ASA includes two AnyConnect Premium licenses. You cannot mix an AnyConnect Premium and AnyConnect Essentials license on the same device. You can have only one or the other.

Table 1-9 *VPN Licensing and Compatibility*

Supported With	Enable One of the Following Licenses	
	AnyConnect Essentials	AnyConnect Premium SSL VPN Edition
AnyConnect Mobile	Yes	Yes
Advanced Endpoint Assessment	No	Yes
AnyConnect Premium SSL VPN Edition Shared	No	Yes
Client-based SSL VPN	Yes	Yes
Browser-based (clientless) SSL VPN	No	Yes
IPsec VPN	Yes	Yes
VPN load balancing	Yes	Yes
Cisco Secure Desktop	No	Yes

Note IKEv1 IPsec sessions are not licensed, and the maximum number of sessions available equal the maximum number available for the ASA platform used. IKEv2 site-to-site VPNs are not licensed either.

IKEv2 IPsec remote-access VPN sessions are available for use only with the AnyConnect client and as such are licensed using the same AnyConnect Essentials or AnyConnect Premium licenses used with SSL VPNs.

Time-Based Licenses

You might have noticed in these tables the inclusion of an optional time-based license available from Cisco for the particular feature you are enabling. Time-based licenses are usually purchased from Cisco to allow your device to handle temporary surges of use for a particular feature. For example, if you are performing a failover of your production traffic to a secondary device during a weekend, but your secondary device does not have enough installed licenses to support the number of SSL VPN sessions required, a time-based license could be installed to cover your requirements for the weekend but only last, say, 90 days.

The timer for a time-based license starts to count down as soon as the license has been activated on your ASA and continues to count down even if your device is shut down for a period of time and then turned on again. It is possible to install multiple time-based licenses. However, only one license can be active on your device at any one time. For example, if you were to install a 250 Clientless SSL VPN time-based license and then a 500 Clientless SSL VPN time-based license, only one of these licenses would be active.

When Time-Based and Permanent Licenses Combine

Depending on the feature you are purchasing or have installed, a time-based license for the resulting combination of your permanent and time-based licenses will differ. For example:

- **SSL VPN Sessions (Client and Clientless):** The license with the higher value is used. For example, if you have a time-based license with a 1000-session limit and a permanent license with a 500-session limit, the time-based license is used, and you have 1000 sessions available.
- **Unified Communications Proxy Sessions:** The time-based and permanent licenses are combined up to the platform limit. For example, if you have a time-based license with a 1000-session limit and a permanent license with a 2000-session limit, you have 3000 sessions available.
- **Security Contexts:** The time-based and permanent licenses are combined up to the platform limit. For example, if you have a time-based license with a 20-context limit and a permanent license with a 5-context limit, you have 25 contexts available.
- **Botnet Traffic Filter:** There is no permanent license for this feature. The time-based license is always used.
- **All remaining licensed features:** The license with the higher limit is used.

Note It is not advisable to install a time-based license with a lower license limit than your current permanent licenses because features that use the license with the higher limit will continue to use your permanent license.

Shared SSL VPN Licenses

Instead of purchasing device-specific license bundles, it is also possible to set up a shared SSL VPN server if you are running two or more ASA devices (Version 8.2+). Licenses are purchased from Cisco in large numbers and entered onto the ASA and will be configured with the role of the shared SSL VPN License server. The other ASA devices contact the SSL VPN License server running on the ASA and request licenses in blocks of 50 to allow for them to cope with the current connections they have.

The ASA devices can contact the SSL VPN License server and keep requesting licenses. However, they can only install and use up to the platform limit locally.

Failover Licensing

Beginning with ASA Version 8.3(1), the two devices in a failover pair no longer require matching licenses to operate. Instead, the primary failover device typically has a license installed and the secondary device inherits this license.

If both devices have licenses installed, however, they merge to become one large failover interface, allowing for the combination of licensed VPN session numbers up to the platform-specific maximum.

Both ASA 5505 and ASA 5510 devices require the Security Plus license before they can operate in Failover mode.

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 1-10 lists a reference of these key topics and the page numbers on which each is found.

Table 1-10 *Key Topics*

Key Topic Element	Description	Page
Bulleted list	Available VPN methods on the ASA	7
Table 1-2	Advantages and limitations of various VPN methods	7-8
Subtopic	SSL tunnel negotiation	24
Topic	ASA packet processing	31
Topic	Time-based licenses	42

Complete Tables and Lists from Memory

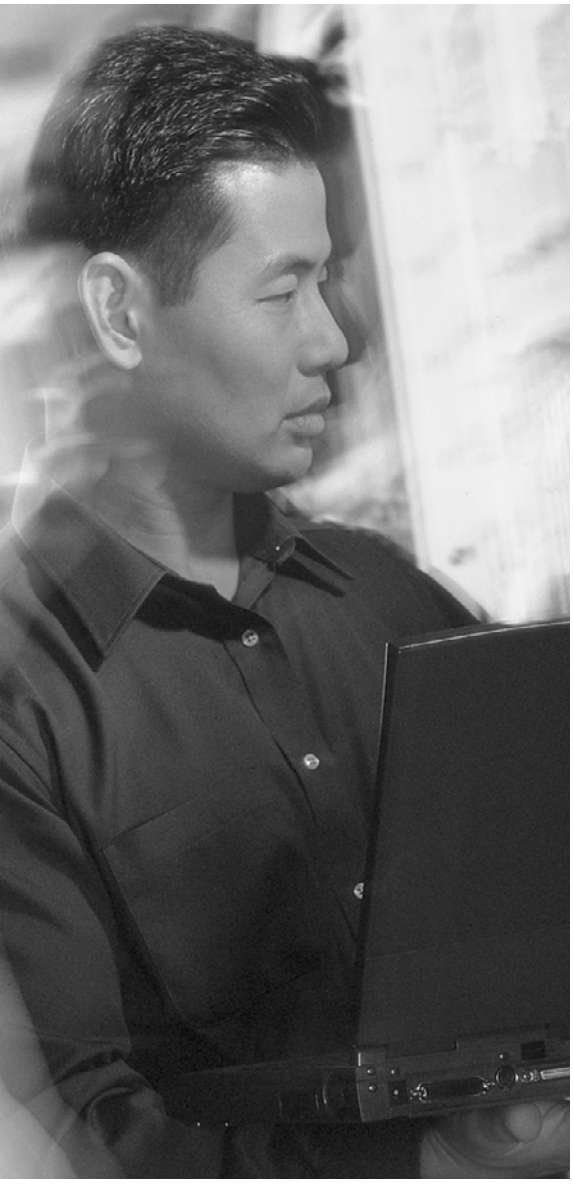
Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Define Key Terms

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

DES, 3DES, AES, Diffie-Hellman, IPsec, SSL, TLS, DTLS

This page intentionally left blank



This chapter covers the following subjects:

- **Policies and Their Relationships:** This section reviews the available policies you can apply during a VPN connection and how they work together to form the overall policy applied to a remote user.
- **Understanding Connection Profiles:** This section discusses the role of connection profiles, their configuration elements, and how they are applied to remote users.
- **Understanding Group Policies:** This section discusses the role of group policies for attribute assignment and control of your remote users.
- **Configure User Attributes:** This section reviews the creation of a user account and looks at the available parameters and attributes that you can assign to an individual remote user.
- **Using External Servers for AAA and Policy Assignment:** This section discusses the role of AAA servers and briefly covers their configuration and how to deploy policies through them.

CHAPTER 2

Configuring Policies, Inheritance, and Attributes

Not only is allowing remote access to resources through a *virtual private network (VPN)* important, you must also be able to control the access granted to those resources. In this chapter, you learn how the *Adaptive Security Appliance (ASA)* achieves the role of access control through policy assignment, whether this be through the use of *dynamic access policies (DAP)*, connection profiles (also known as tunnel groups), group policies, or direct user assignment.

In addition to the available policy assignment methods, you are introduced to the inheritance model that takes place between these methods and learn how they interact with each other when attributes set within them contain different values.

"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

For a successful VPN deployment, you must be able to enforce user policy and connection parameters. Without them, you cannot provide login parameters, authorization methods, or resource access for users, and thus control what they can or cannot access and how they can access them and when.

Note that before remote users can build a successful connection into an organization through a VPN, they must first go through the following two phases:

- **The prelogin phase** is achieved through the use of connection profiles (also known as tunnel groups). In connection profiles, you 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, IKEv2, and *Secure Sockets Layer [SSL]*), allowing users to move on to the login process.
- **The post-login phase** is achieved through the use of group policy objects, 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.

In this chapter, with the exception of DAPs, we discuss the various policy types and attributes that may be applied within either the prelogin phase or the post-login phase. Of the available VPN methods on the *Adaptive Security Appliance (ASA)*, the clientless SSL, full-tunnel SSL (AnyConnect), and full-tunnel IPsec (Cisco Easy VPN IKEv1, AnyConnect IKEv2) remote-access methods all follow the same process to classify and log in a remote user, as illustrated in Figure 2-1.

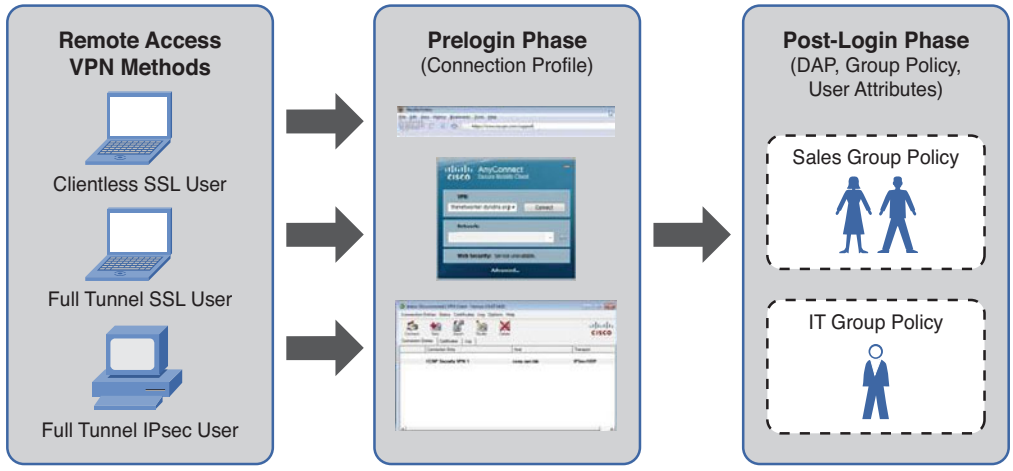


Figure 2-1 *Remote VPN User Prelogin and Post-Login Phases*

As the number of VPN connections you roll out increases, the following two key points are an important part of the policy assignment methodology:

Key Topic

- **Flexibility:** Flexibility is achieved through being able to assign the same security or network settings to any user or group regardless of their method of VPN connectivity (clientless SSL, AnyConnect, and so on).
- **Scalability:** Scalability is achieved through modularity and policy inheritance. Inheritance can limit the amount of duplicate configuration items that may be required (for example, by assigning policies containing "global" attributes to multiple connections or groups and policies containing specific role-oriented attributes directly to individual groups or users). You see later in this chapter how to use inheritance to your advantage when assigning policies to users, groups, or connection profiles.

To give a bit of perspective on how both flexibility and scalability are achieved through policy and attribute assignment on the ASA, suppose you have two departments in your organization called sales and engineering. Each department contains users who need to access resources in the office when working remotely. Two connection profiles have been created, aptly named Sales and Engineering, allowing users from the sales department to connect using a clientless SSL VPN and users from the engineering department to connect using a full-tunnel SSL VPN (AnyConnect). Later you create a new time range called Office_Hours allowing users to log in during office hours only and assign it to the sales department by creating a new group policy called sales_gp and attaching it to the sales connection profile. However, you have now been asked to also assign the Office_Hours time range to the engineering department. You decide to add the time range to the default group policy object instead so that it applies to both of your connection profiles (and thus the respective departments) and remove it from the sales_gp.

Note Configuring the default group policy (DfltGrpPolicy) to contain connection-specific properties is generally frowned upon because its intended use is a systemwide policy used to provide global settings to remote users of what may be multiple connectivity types. The systemwide default group policy (DfltGrpPolicy) is discussed in more detail in the "Understanding Group Policies" section, later in this chapter.

You can be as specific as you like or as needs require for any 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 yours.

In the earlier scenario, you had a number of choices, depending on the level of granularity, control, and specificity you aim to have on the policies configured and their specific assignments. For example, instead of assigning the Office_Hours time range using the default group policy object, you could have just assigned the sales_gp group policy object to the Engineering connection profile. Despite the fact that you would have confused any remaining and future technical staff in your organization by placing a sales object onto an engineering object (the two seldom work well together anyway), you would lose the ability to add specific attributes and settings to the engineering department's connectivity without potentially affecting the sales department. Sure, you could assign specific attributes to the engineering users' accounts individually without modifying the group policy object applied to both connection profiles, but that's just no fun, even if you do have only 20 engineering users. In time, as your employee numbers increase, the environment could quickly turn into a support nightmare.

As you can probably guess, your overall and ongoing policy configuration should be an item on your list that is given a good deal of thought and preparation. You will see in a moment how the different policy objects behave and the results that occur when they are configured together. As a rule of thumb, it is a whole lot easier to assign global attributes and settings further away from the object you are assigning them to and more specific attributes and settings closer or even directly to the object you are assigning them to. For example, use default group policies for companywide login or welcome banners that need to apply to all users and their respective connection profiles, while assigning group policies that contain specific user attributes or settings to groups of users (departments/organizational units) or users directly.

As you start to create many connection profile policies and begin assigning attributes, you may 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 the user's policies are merged and assigned in a hierarchical fashion.

The hierarchal policy model shown in Figure 2-2 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). In contrast, any unassigned attributes inherit their settings from the lower-level policy methods.

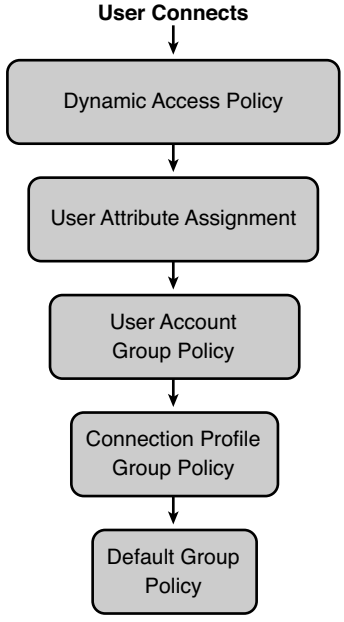


Figure 2-2 *ASA VPN Policy Enforcement Hierarchy*

If users attempt to create a new VPN connection into your organization and pass the prelogin phase, the post-login phase begins, and their session assigns attributes using one of the available policy methods. The list begins with DAPs. Any particular attributes or settings configured within a DAP are applied to the user's session and the process continues by moving on to check for any attributes configured within the users account. After this phase, the process checks for attributes to be applied within the group policy object assigned to the user account. Then the group policy object assigned to the connection profile used during the prelogin phase, and finally any remaining attributes that have not been set or used, are assigned using the default group policy configuration.

If at any time during this process conflicting attributes are found between policy methods in the hierarchy, attributes contained within the preceding policy method are used based on the hierarchical model shown in Figure 2-2.

Understanding Connection Profiles

Connection profiles, or tunnel groups as they are more commonly known, provide the necessary prelogin policy criteria required to enable remote users to successfully establish a VPN connection to the ASA device. Connection profiles are typically used to separate remote users into the relevant groups (commonly departments) that may require separate methods of access or login (for example, clientless SSL VPN, AnyConnect VPN sessions, username and password, or certificate-based authentication) and provide

these groups with general connectivity settings such as AAA, DNS, DHCP servers, and IP address pools. In addition to access methods and general settings, you can assign each connection profile a group policy object specific to the connecting remote users, containing filters, access times, proxy settings, and so on (as discussed in the "Understanding Group Policies" section, later in this chapter).

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. However, your corporate employees require access to internal file servers and email. Based on the level of access required by each group, you could create two connection profiles, aptly named Guests and Corporate for this discussion. The 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 more detail in the "Understanding Group Policies" section) would be applied to the connection profile containing the relevant bookmarks needed for browsing your company's intranet using the SSL VPN portal. However, your 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 users to select and connect to the appropriate connection profile. Depending on the authentication scheme configured for users and the 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:

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

Group URL

Group URLs allow remote users connecting through a clientless SSL VPN session to select a connection profile by entering the direct URL in their browser that has been configured for the profile they require. An example of a configured group URL would be either of the following:

https://*ASA IP address*/*connection profile name*

https://*ASA FQDN*/*connection profile name*

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 a Clientless SSL VPN Solution," and Chapter 8, "Deploying an AnyConnect Remote-Access VPN." As shown in Figure 2-3, the configuration of both a group alias and group URL can be achieved on the Group Alias/Group URL pane of a connection profiles properties window available at **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.**

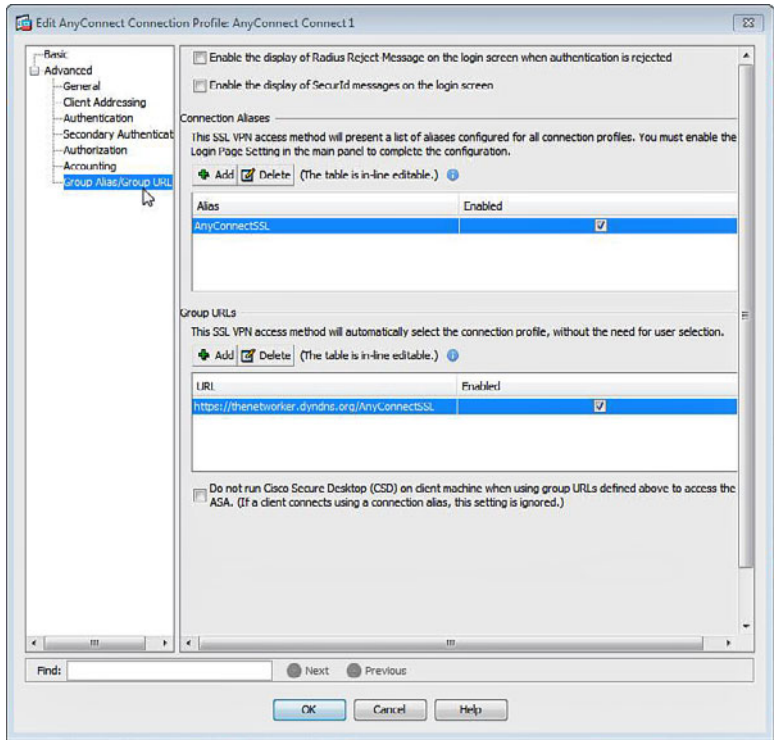


Figure 2-3 *Connection Profile Group URL and Alias Configuration*

You can complete the same configuration via the command-line interface, as shown in Example 2-1.

Example 2-1 *Cisco ASA Group Alias and Group URL Commands*

```
CCNPSec(config)# tunnel-group SSLVPN webvpn-attributes
CCNPSec(config-tunnel-webvpn)# group-alias SSL enable
CCNPSec(config-tunnel-webvpn)# group-url https://ccnp.vpn.com/SSL enable
```

Note The **group-url** can accept a URL entry with either an http:// or https:// prefix.

As you will also see in later chapters, before remote users can select a connection profile by group alias, you must first enable this feature on the ASA either using the CLI or in the respective connection profiles pane of the *Adaptive Security Device Manager (ASDM)*, as shown in Figure 2-4.

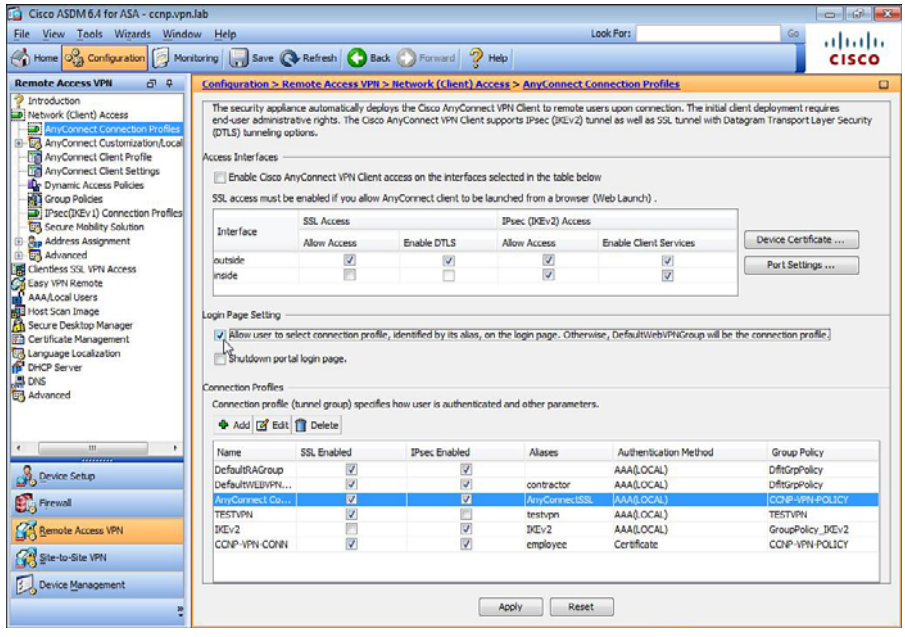


Figure 2-4 *Connection Profile Pane: Allow Group Alias Selection*

For example, you can enable 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 within the ASDM:

- **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**.

Alternatively, just enter the **tunnel-group-list enable** command when in global webvpn configuration mode, as shown in Example 2-2.

Example 2-2 *Enabling the Use of Group URLs or Aliases via the CLI*

```
CCNPSec(config)# webvpn
CCNPSec(config-webvpn)# tunnel-group-list enable
```

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, you can configure the ASA 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 6, "Clientless SSL VPN Advanced Authentication and Authorization," and Chapter 9, "Advanced Authentication and Authorization of AnyConnect VPNs").

Per-User Connection Profile Lock

You can also assign a connection profile directly to remote users on an individual basis. For example, you might have a specific connection profile for sales users 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.

You can assign a connection profile directly to a user using the ASDM (in the properties menu of the user's account), as shown in Figure 2-5.

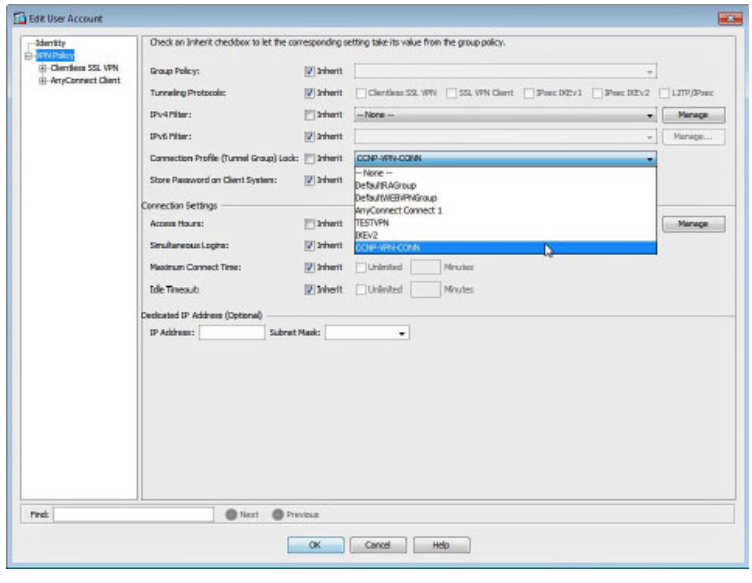


Figure 2-5 *Configuring Per-User Connection Profile Lock*